HP Data Protector 8.00
インストールおよびライセンスガイド

HP 部品番号: N/A
2013 年 6 月
第 3 版

目次

出版履歴....9
本書について....10
対象読者....10
ドキュメントセット....10
ヘルプ....10
ガイド....10
ドキュメントマップ....13
略称....13
対応表....14
統合....15
表記上の規則および記号....15
Data Protector グラフィカルユーザーインタフェース....16
一般情報....17
HP テクニカルサポート....17
メールニュース配信サービス....17
HP Web サイト....17
ドキュメントに関する意見....18
1 インストール手順の概要....19
インストール手順の概要....19
リモートインストールの概念....21
Data Protector のインストール DVD-ROM....22
Cell Manager システムの選択....23
Data Protector ユーザーインタフェースシステムの選択....24
Data Protector グラフィカルユーザーインタフェース....24
2 ネットワークへの Data Protector のインストール....26
Data Protector Cell Manager およびインストールサーバーのインストール....26
UNIX 用 Cell Manager のインストール....27
カーネルパラメーターの設定....28
インストール手順....28
HP-UX および Linux システムにインストールされるディレクトリの構造....29
自動での起動とシャットダウンの構成....30
環境変数の設定....31
この次に行う作業....31
Windows 用 Cell Manager のインストール....32
インストール手順....33
インストール後の状態....36
トラブルシューティング....37
この次に行う作業....37
インストールサーバーのインストール....37
UNIX システム用のインストールサーバーのインストール....38
Windows システム用のインストールサーバーのインストール....39
Data Protector クライアントのインストール....42
Data Protector コンポーネント....44
Windows 用クライアントのインストール....47
ローカルインストール....48
Windows システムへのバックアップデバイスの接続....50
HP-UX クライアントのインストール....51
HP-UX のカーネル構成のチェック....52
HP-UX システムへのバックアップデバイスの接続....53
Solaris 用クライアントのインストール....54

インストール後の構成.....55
Solaris システムへのバックアップデバイスの接続.....59
Linux クライアントのインストール.....60
Linux システムへのバックアップデバイスの接続.....62
ESX Server クライアントのインストール.....63
Mac OS X クライアントのインストール.....63
IBM AIX クライアントのインストール.....64
AIX クライアントへのバックアップデバイスの接続.....65
HP OpenVMS クライアントのインストール.....65
リモートインストール.....70
セキュアシェルを使用したリモートインストール.....71
クライアントのセルへの追加.....73
クライアントへのコンポーネントの追加.....74
UNIX および Mac OS X システムのローカルインストール.....76
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.....79
ライブラリドライブの接続.....79
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.....79
ADIC/GRAU ライブラリ用の Media Agent のインストール.....80
StorageTek ライブラリを使用する Data Protector クライアントの準備作業.....83
StorageTek ライブラリ用の Media Agent のインストール.....84
Data Protector 統合クライアントのインストール.....84
リモートインストール.....86
ローカルインストール.....86
クラスター対応統合ソフトウェアのインストール.....87
Microsoft Exchange Server クライアント.....87
Data Protector Microsoft Exchange Server 2007 用統合ソフトウェア.....87
Data Protector Microsoft Exchange Server 2010 用統合ソフトウェア.....88
Data Protector Microsoft Exchange Server Single Mailbox 用統合ソフトウェア.....88
Data Protector Microsoft ボリュームシャドウコピーサービス用統合ソフトウェア.....88
Microsoft Exchange Server 向け Data Protector Granular Recovery Extension.....89
Microsoft SQL Server クライアント.....89
Microsoft SharePoint Server クライアント.....89
Data Protector Microsoft SharePoint Server 2007/2010 用統合ソフトウェア.....89
Data Protector Microsoft SharePoint Server 2007/2010 VSS ベースソリューション.....90
Data Protector Microsoft ボリュームシャドウコピーサービス用統合ソフトウェア.....90
Microsoft SharePoint Server 向け Data Protector Granular Recovery Extension.....90
Microsoft ボリュームシャドウコピーサービスクライアント.....91
Sybase Server クライアント.....91
Informix Server クライアント.....91
IBM HACMP Cluster.....92
SAP R/3 クライアント.....92
SAP MaxDB クライアント.....92
Oracle Server クライアント.....92
IBM DB2 UDB クライアント.....93
Lotus Notes/Domino Server クライアント.....93
Lotus Domino Cluster.....93
VMware クライアント.....93
Data Protector 仮想環境統合ソフトウェア.....94
Data Protector VMware(レガシー) 用統合ソフトウェア.....94
VMware vSphere 向け Data Protector Granular Recovery Extension.....94
Microsoft Hyper-V クライアント.....96
Data Protector 仮想環境統合ソフトウェア.....96
Data Protector Microsoft ボリュームシャドウコピーサービス用統合ソフトウェア.....96
NDMP Server クライアント.....97
HP P4000 SAN ソリューション クライアント.....97

HP P6000 EVA ディスクアレイファミリ クライアント....97
HP P6000 EVA ディスクアレイファミリ と Oracle Server の統合....98
HP P6000 EVA ディスクアレイファミリ と SAP R/3 の統合....99
HP P6000 EVA ディスクアレイファミリ と Microsoft Exchange Server の統合....101
HP P6000 EVA ディスクアレイファミリ と Microsoft SQL Server の統合....102
HP P9000 XP ディスクアレイファミリ クライアント....102
HP P9000 XP ディスクアレイファミリ と Oracle Server の統合....103
HP P9000 XP ディスクアレイファミリ と SAP R/3 の統合....104
HP P9000 XP ディスクアレイファミリ と Microsoft Exchange Server の統合....106
HP P9000 XP ディスクアレイファミリ と Microsoft SQL Server の統合....107
HP 3PAR StoreServ Storage クライアント....107
EMC Symmetrix クライアント....108
EMC Symmetrix 用統合ソフトウェアと Oracle の組み合わせ....108
EMC Symmetrix 用統合ソフトウェアと SAP R/3 との組み合わせ....109
EMC Symmetrix 用統合ソフトウェアと Microsoft SQL Server との組み合わせ....111
各国語版 Data Protector ユーザーインタフェースのインストール....111
トラブルシューティング....112
各国語版 Data Protector マニュアルのインストール....112
Windows システムへの各国語版 Data Protector マニュアルのインストール....112
UNIX システムへの各国語版 Data Protector マニュアルのインストール....113
Data Protector シングルサーバー版のインストール....114
Windows 用 SSE の制限....114
SSE へのアップグレード (HP-UX) での制限事項....114
Data Protector Web Reporting のインストール....115
MC/ServiceGuard への Data Protector のインストール....116
クラスター対応 Cell Manager のインストール....116
インストールサーバーのクラスターノードへのインストール....116
クラスター対応クライアントのインストール....116
Microsoft Cluster Server への Data Protector のインストール....117
クラスター対応 Cell Manager のインストール....117
クラスター対応クライアントのインストール....123
Veritas Cluster への Data Protector クライアントのインストール....125
クラスター対応クライアントのインストール....125
Data Protector の IBM HACMP Cluster へのインストール....125
クラスター対応クライアントのインストール....126
Microsoft Hyper-V クラスターでの Data Protector のインストール....126
3 インストールの保守....127
Data Protector 保守モード....127
保守モードの開始....127
保守モードの終了....128
セルへのクライアントのインポート....129
セルへのインストールサーバーのインポート....130
セルへのクラスター対応クライアントのインポート....131
Microsoft Cluster Server....131
その他のクラスター....132
セルからのクライアントのエクスポート....133
セキュリティについて....135
セキュリティ層....135
クライアントの保護....135
Data Protector ユーザー....135
Cell Manager の保護....136
その他のセキュリティ保護について....136
クライアントの保護設定....137
allow_hosts ファイルと deny_hosts ファイル....141

inet.log ファイルに大量のログが記録される....141
厳密なホスト名チェック....142
機能を使用可能にする....143
セキュアな通信の有効化....143
[バックアップ仕様を開始] ユーザー権限....145
バックアップ仕様の内容にアクセスできないようにする....145
ホストの信頼....145
保護イベントのモニター....146
Data Protector パッチの管理....146
パッチのインストール....146
Data Protector パッチバンドルのインストールと削除....147
UNIX システムでの Data Protector パッチバンドルのインストールと削除....147
Windows システムでの Data Protector パッチバンドルのインストールと削除....147
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....148
GUI を使用した Data Protector パッチの確認....148
CLI を使用した Data Protector パッチの確認....149
Data Protector ソフトウェアのアンインストール....149
Data Protector クライアントのアンインストール....150
Cell Manager とインストールサーバーのアンインストール....150
Windows システムからのアンインストール....151
HP-UX システムからのアンインストール....151
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ーのアンインストール....152
Linux システムからのアンインストール....153
UNIX での Data Protector ソフトウェアの手動による削除....155
Data Protector ソフトウェアコンポーネントの変更....156
Windows システムの場合....156
HP-UX システムの場合....157
Linux システムの場合....157
その他の UNIX システムの場合....158
4 Data Protector 8.00 へのアップグレード....159
アップグレードの概要....159
アップグレード手順....160
Data Protector A.06.11、6.20、および 7.00 からのアップグレード....161
UNIX 用 Cell Manager とインストールサーバーのアップグレード....161
Cell Manager のアップグレード....161
インストールサーバーのアップグレード....163
Windows Cell Manager とインストールサーバーのアップグレード....163
構成の変更のチェック....166
Data Protector 8.00 へのアップグレード後の内部データベースの変更....168
詳細カタログバイナリファイル (DCBF) の移行....168
IDB 変換期間および IDB サイズと構造の変更....169
レガシー NDMP メディアのインポート....169
セッション ID の序数....169
クライアントのアップグレード....170
Oracle 用統合ソフトウェアのアップグレード....171
ユーザールートは不要....171
インスタントリカバリのための Oracle インスタンスの構成....172
データストレージ用に HP P6000 EVA ディスクアレイファミリ を使用した Oracle ASM の構成....172
SAP R/3 用統合ソフトウェアのアップグレード....172
SAP 対応 ZDB セッション....172
インスタントリカバリのための Oracle インスタンスの構成....172
Microsoft ボリュームシャドウコピーサービス用統合ソフトウェアのアップグレード....173

HP Data Protector HP A.06.11、HP Data Protector 6.20、または Data Protector 7.00 からのアップグレード後のインスタントリカバリが有効なバックアップセッション....173
HP P6000 EVA ディスクアレイファミリ 用統合ソフトウェアのアップグレード....173
仮想環境統合ソフトウェアのアップグレード....173
他の統合ソフトウェアのアップグレード....173
MoM 環境でのアップグレード....174
シングルサーバー版からのアップグレード....174
旧バージョンの SSE から Data Protector 8.00 SSE へのアップグレード....174
Data Protector 8.00 SSE から Data Protector 8.00 へのアップグレード....174
Cell Manager のアップグレード....175
複数のシステムからのアップグレード....175
Cell Manager の異なるプラットフォームへの移行....175
PA-RISC HP-UX システムから Intel Itanium HP-UX システムへの移行....175
32 ビット/64 ビット Windows から 64 ビット Windows/Windows Server 2008 への移行...176
Solaris から Linux への移行....176
MoM 固有の手順....177
インストールサーバー 固有の手順....177
MC/ServiceGuard 上で構成されている Cell Manager のアップグレード....177
Microsoft Cluster Server 上で構成されている Cell Manager のアップグレード....180
5 Data Protector ライセンス....183
概要....183
ライセンスチェック機能とレポート機能....183
Cell Manager 関連ライセンス....184
エンティティーベースのライセンス....184
容量ベースのライセンス....184
使用容量の計算....185
アドバンストバックアップ使用権....186
容量ベースのライセンスの例....187
必要に応じたライセンスレポートの作成....189
Data Protector 8.00 以前のライセンスのチェックとレポート....190
マルチドライブサーバー使用権のレポート....190
以前のオンラインライセンスのレポート....192
NDMP ダイレクトバックアップ使用権のレポート....192
スロットライブラリ使用権のレポート....193
以前の ZDB および IR のライセンスのレポート....193
Data Protector パスワード....195
恒久パスワードの取得とインストール....196
パスワードの検証....198
インストール済みライセンスの数を調べる....198
他の Cell Manager システムへのライセンスの移動....198
集中型ライセンス....199
Data Protector 8.00 の製品構成とライセンス....199
パスワードについて....202
Data Protector 8.00 へのライセンス移行....203
Data Protector ライセンスフォーム....203
6 インストールのトラブルシューティングとアップグレード....205
Windows 用 Cell Manager インストール時の名前解決に関する問題....205
Data Protector セル内の DNS 接続の確認....205
omnicheck コマンドの使用....206
共通の問題のトラブルシューティング....207
UNIX システムでのインストールのトラブルシューティング....208
Windows システムでのインストールのトラブルシューティング....209
Data Protector クライアントのインストール結果の確認....210
アップグレードのトラブルシューティング....211

Windows システムでのリモートアップグレードのトラブルシューティング.....215
UNIX システムでのローカルアップグレードの手動処理.....215
ログファイルの使用.....215
ローカルインストール.....215
リモートインストール.....216
Data Protector ログファイル.....216
インストール実行トレースの作成.....217
A UNIX システムネイティブツールを使用した Data Protector のインストールとアップグレード.....218
ネイティブツールを使用した、HP-UX および Linux システムへのインストール.....218
swinstall を使用した HP-UX システムへの Cell Manager のインストール.....218
rpm を使用した Linux システムへの Cell Manager のインストール.....219
swinstall を使用した HP-UX システムへのインストールサーバーのインストール.....220
rpm を使用した Linux システムへのインストールサーバーのインストール.....221
クライアントのインストール.....223
ネイティブツールを使用した、HP-UX および Linux システムでのアップグレード.....223
swinstall を使用した HP-UX システムでの Data Protector のアップグレード.....223
rpm を使用した Linux システムでの Data Protector のアップグレード.....224
B システムの準備と保守作業.....226
UNIX システムでのネットワーク構成.....226
TCP/IP 設定をチェックする.....226
デフォルトの Data Protector ポートの変更.....227
デフォルトの Data Protector Inet ポートの変更.....227
UNIX システムでデフォルトの Data Protector IDB ポートおよびユーザーアカウントを変更する.....228
Data Protector インストールのための Windows Server 2008 または Windows Server 2012 上で実行する Microsoft サーバークラスターの準備.....229
Veritas Volume Manager がインストールされた Microsoft Cluster Server への Data Protector のインストール.....231
NIS サーバーの準備.....231
Cell Manager 名の変更.....232
C デバイスとメディア関連タスク.....233
Windows システムでのテープドライバーおよびロボティクスドライバーの使用.....233
Windows システム上でのデバイスファイル (SCSI アドレス) の作成.....234
HP-UX システム上の SCSI ロボティクス構成.....235
HP-UX システム上のデバイスファイルの作成.....238
SCSI コントローラーのパラメーターの設定.....240
HP-UX システム上の未使用の SCSI アドレスの取得.....240
Solaris システム上の未使用の SCSI ターゲット ID の取得.....241
Solaris システム上でのデバイスおよびドライバー構成の更新.....242
構成ファイルの更新.....242
デバイスファイルの作成とチェック.....244
Windows システム上の未使用の SCSI ターゲット ID の取得.....245
HP 330fx ライブラリでの SCSI ID の設定.....245
バックアップデバイスの接続.....246
HP 24 スタンドアロンデバイスの接続.....248
HP DAT オートローダーの接続.....249
HP DLT ライブラリ 28/48 スロットの接続.....250
Seagate Viper 200 LTO Ultrium テープドライブの接続.....253
D Data Protector 8.00 へのアップグレード後のコマンドラインの変更.....255
索引.....269
用語集.....279

出版履歴

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

表 1 出版履歴

製品番号	ガイド版	製品
N/A	2013 年 6 月	Data Protector リリース 8.00
N/A	2013 年 6 月 (第 2 版)	Data Protector リリース 8.00
N/A	2013 年 6 月 (第 3 版)	Data Protector リリース 8.00

本書について

本書では、以下について説明します。

- 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に満たす必要がある前提条件
- アップグレードとライセンス

対象読者

本書は、環境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としています。

Data Protector の概念については、『HP Data Protector コンセプトガイド』を参照してください。Data Protector に関する基礎知識とモデルについてよく理解するためにも、一読することをお勧めします。

ドキュメントセット

ヘルプおよびその他のガイドには、関連情報が記載されています。

注記: このドキュメントセットは HP サポートの Web サイト (http://support.openview.hp.com/selfsolve/manuals) で利用できます。ドキュメントセットには最新の更新情報と修正情報が記載されています。

ヘルプ

Data Protector は、Windows および UNIX の各プラットフォーム用にヘルプトピックとコンテキスト依存ヘルプ (F1 キー) を備えています。ヘルプのインストールは、Data Protector のセットアップ時に、Windows システムの場合は英語のドキュメント（ガイド、ヘルプ）インストールコンポーネント、UNIX システムの場合は `OB2-DOCS` インストールコンポーネントを選択することで行います。一度インストールされると、ヘルプは、以下のディレクトリに格納されます。

Windows システムの場合: *`Data_Protector_home`*`\help\enu`

UNIX システムの場合: `/opt/omni/help/C/help_topics`

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

Windows システムの場合: `DP_help.chm` を開きます。

UNIX システムの場合: 圧縮された tar ファイル `DP_help.tar.gz` をアンパックし、`DP_help.htm` を開きます。

ガイド

Data Protector のガイドは、電子的な PDF 形式で提供されます。PDF ファイルのインストールは、Data Protector のセットアップ時に、Windows システムの場合は英語のドキュメント（ガイド、ヘルプ）インストールコンポーネント、UNIX システムの場合は `OB2-DOCS` インストールコンポーネントを選択することで行います。一度インストールされると、マニュアルは、以下のディレクトリに格納されます。

Windows システムの場合: *`Data_Protector_home`*`\docs`

UNIX システムの場合: `/opt/omni/doc/C`

マニュアルには、以下からもアクセスできます。

- Data Protector グラフィカルユーザーインタフェースの [ヘルプ] メニューから

- http://support.openview.hp.com/selfsolve/manuals にある HP サポートの Web サイト (この Web サイトには最新バージョンのマニュアルが用意されています)

Data Protector マニュアルの内容は、以下のとおりです。

- 『HP Data Protector スタートアップガイド』

  このマニュアルでは、Data Protector を使用して操作をすぐに開始するための情報を記載しています。インストールの前提条件を一覧し、基本的なバックアップ環境のインストールと構成の手順、およびバックアップと復元の実行手順を記載しています。また、詳細な情報を記載しているリソースについても一覧しています。

- 『HP Data Protector コンセプトガイド』

  このガイドでは、Data Protector のコンセプトを解説するとともに、Data Protector の動作原理を詳細に説明しています。これは、タスクごとのヘルプとともに使用するように作成されています。

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

  このガイドでは、Data Protector ソフトウェアのインストール方法をオペレーティングシステムおよび環境のアーキテクチャーごとに説明しています。また、Data Protector のアップグレード方法や、環境に適したライセンスの取得方法についても説明しています。

- 『HP Data Protector トラブルシューティングガイド』

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

- 『HP Data Protector ディザスタリカバリガイド』

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

- 『HP Data Protector Command Line Interface Reference』

  このガイドでは、Data Protector コマンドラインインタフェース、コマンドオプション、使用方法を、基本コマンドラインの例とともに説明しています。このマニュアルは以下のディレクトリにあります。

  Windows システムの場合: *Data_Protector_home*\docs\MAN

  UNIX システムの場合: /opt/omni/doc/C/

  UNIX システムの場合、omniintroman ページを使用して、使用できる Data Protector コマンドの一覧を表示できます。man *CommandName* コマンドを実行すると、各 Data Protector コマンドについての情報を取得できます。

- 『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』

  このガイドでは、HP Data Protector 8.00 の新機能について説明しています。また、インストール要件、必要なパッチ、および制限事項に関する情報に加えて、既知の問題と回避策についても提供します。

- 『HP Data Protector インテグレーションガイド』

  これらのガイドでは、さまざまなデータベースやアプリケーションをバックアップおよび復元するための、Data Protector の構成方法および使用法を説明します。このマニュアルは、バックアップ管理者およびオペレーターを対象としています。6 種類のガイドがあります。

  - 『HP Data Protector インテグレーションガイド - Microsoft アプリケーション: SQL Server、SharePoint Server、Exchange Server』

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

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

  このガイドでは、Oracle Server、SAP R/3、SAP MaxDB に対応する Data Protector の統合ソフトウェアについて説明します。

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

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

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

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

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

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

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

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

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

  このガイドでは、Data Protector ゼロダウンタイムバックアップとインスタントリカバリのコンセプトについて解説するとともに、ゼロダウンタイムバックアップ環境における Data Protector の動作原理を詳細に説明します。手順を中心に説明している『HP Data Protector ゼロダウンタイムバックアップ管理者ガイド』および『HP Data Protector ゼロダウンタイムバックアップインテグレーションガイド』とあわせてお読みください。

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

  このガイドでは、HP P4000 SAN ソリューション 、HP P6000 EVA ディスクアレイファミリ 、HP P9000 XP ディスクアレイファミリ 、HP 3PAR StoreServ Storage、EMC Symmetrix Remote Data Facility および TimeFinder に対応する Data Protector 統合ソフトウェアの構成方法および使用法を説明します。このガイドは、バックアップ管理者やオペレーターを対象としています。ファイルシステムとディスクイメージのゼロダウンタイムバックアップ、インスタントリカバリ、および復元についても説明します。

- 『HP Data Protector ゼロダウンタイムバックアップインテグレーションガイド』

  このガイドでは、Oracle Server、SAP R/3、Microsoft Exchange Server、Microsoft SQL Server の各データベースに対して、そのゼロダウンタイムバックアップ、インスタントリカバリ、標準復元を実行するための Data Protector の構成方法および使用方法について説明します。

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

  このマニュアルでは、Data Protector Granular Recovery Extension for Microsoft Exchange Server の構成方法および使用法について説明します。Microsoft Exchange Server 用の Data Protector Granular Recovery Extension のグラフィカルユーザーインタフェースは、Microsoft 管理コンソールに組み込まれます。このガイドは、Microsoft Exchange Server 管理者および Data Protector バックアップ管理者を対象としています。

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

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

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

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

- 『HP Data Protector Deduplication』

  この技術ホワイトペーパーでは、基本的なデータの重複排除のコンセプト、ディスクへのバックアップデバイスとの HP Data Protector の統合の原理とその重複排除の使用について説明しています。また、Data Protector バックアップ環境での重複排除の構成方法と使用方法についても説明しています。

- 『HP Data Protector Autonomy IDOL Server との統合』

  この技術ホワイトペーパーでは、統合のコンセプト、インストールと構成、Data Protector バックアップイメージのインデックス作成、フルコンテンツ検索ベースの復元、トラブルシューティングなど、Autonomy IDOL Server と Data Protector の統合についてのあらゆる側面について説明しています。

- 『HP Data Protector Autonomy LiveVault との統合』

  この技術ホワイトペーパーでは、統合のコンセプト、インストールと構成、バックアップポリシー管理、クラウンドバックアップ、クラウド復元、トラブルシューティングなど、Autonomy LiveVault と Data Protector の統合についてのあらゆる側面について説明しています。

ドキュメントマップ

略称

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

略称	ドキュメント項目
CLI	Command Line Interface Reference
Concepts	コンセプトガイド
DR	ディザスタリカバリガイド
GS	スタートガイド
GRE Exchange	Granular Recovery Extension User Guide for Microsoft Exchange Server
GRE SPS	Granular Recovery Extension ユーザーガイド - Microsoft SharePoint Server
GRE VMware	Granular Recovery Extension User Guide for VMware vSphere
Help	ヘルプ
Install	インストールおよびライセンスガイド

略称	ドキュメント項目
IG IBM	IBM アプリケーション用インテグレーションガイド - Informix、DB2、および Lotus Notes/Domino
IG MS	Microsoft アプリケーション用インテグレーションガイド - SQL Server、SharePoint Server、および Exchange Server
IG VSS	Microsoft Volume Shadow Copy Service
IG O/S	インテグレーションガイド - Oracle、SAP
IG Var	インテグレーションガイド - Sybase および Network Data Management Protocol Server
IG VirtEnv	インテグレーションガイド - 仮想環境
IG IDOL	Autonomy IDOL Server との統合
IG LV	Autonomy LiveVault との統合
PA	製品案内、ソフトウエアノートおよびリファレンス
Trouble	トラブルシューティングガイド
ZDB Admin	ZDB 管理者ガイド
ZDB Concepts	ZDB コンセプトガイド
ZDB IG	ZDB インテグレーションガイド

対応表

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

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

統合

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

ソフトウェアアプリケーション	ガイド
Autonomy IDOL Server	IG IDOL
Autonomy LiveVault	IG LV
IBM DB2 UDB	IG IBM
Informix Server	IG IBM
Lotus Notes/Domino Server	IG IBM
Microsoft Exchange Server	IG MS, ZDB IG、GRE Exchange
Microsoft Hyper-V	IG VirtEnv
Microsoft SharePoint Server	IG MS、ZDB IG、GRE SPS
Microsoft SQL Server	IG MS, ZDB IG
Microsoft Volume Shadow Copy Service (VSS)	IG VSS
Network Data Management Protocol (NDMP) Server	IG Var
Oracle Server	IG O/S, ZDB IG
SAP MaxDB	IG O/S
SAP R/3	IG O/S、ZDB IG
Sybase Server	IG Var
VMware vCloud Director	IG VirtEnv
VMware vSphere	IG VirtEnv、GRE VMware

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

ディスクアレイファミリ	ガイド
EMC Symmetrix	すべての ZDB
HP P4000 SAN ソリューション	ZDB Concepts、ZDB Admin、IG VSS
HP P6000 EVA ディスクアレイファミリ	すべての ZDB、IG VSS
HP P9000 XP ディスクアレイファミリ	すべての ZDB、IG VSS
HP 3PAR StoreServ Storage	ZDB Concepts、ZDB Admin、IG VSS

表記上の規則および記号

表 2 表記上の規則

規則	要素
青色のテキスト:「表記上の規則」 (15 ページ)	クロスリファレンスリンクおよび電子メールアドレス
青色の下線付きテキスト:http://www.hp.com	Web サイトアドレス

表 2 表記上の規則 (続き)

規則	要素
太字テキスト	• 押すキー • ボックスなど GUI 要素に入力するテキスト • メニュー、リストアイテム、ボタン、タブ、およびチェックボックスなどクリックまたは選択する GUI 要素
斜体テキスト	テキスト強調
等幅テキスト	• ファイルおよびディレクトリ名 • システム出力 • コード • コマンド、引数、および引数の値
等幅、斜体テキスト	• コード変数 • コマンド変数
等幅、太字テキスト	強調された等幅テキスト

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

⊘ **重要:** 詳細情報または特定の手順を示します。

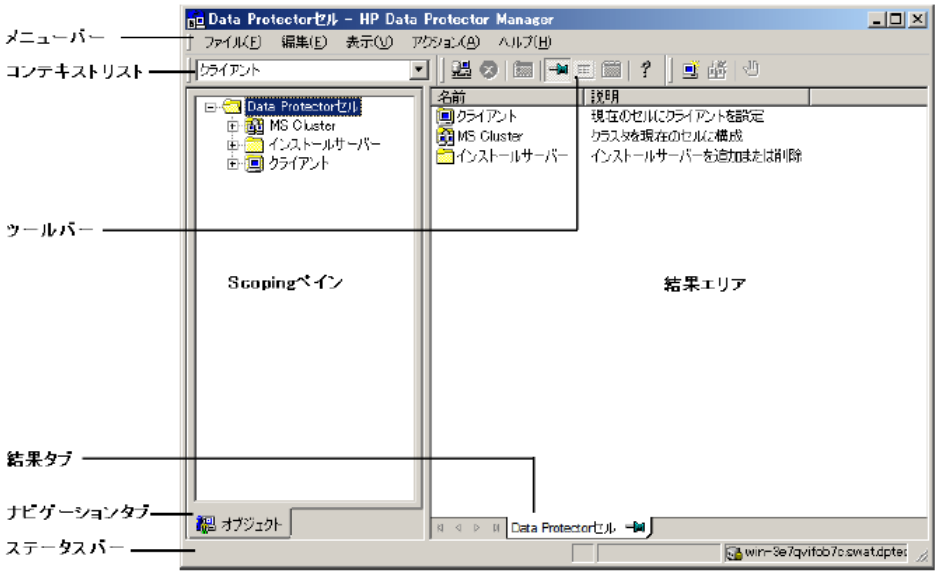
注記: 補足情報を示します。

ヒント: 役に立つ情報やショートカットを示します。

Data Protector グラフィカルユーザーインタフェース

Data Protector では、Microsoft Windows オペレーティングシステム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 グラフィカルユーザーインタフェースに関する詳細は、『HP Data Protector ヘルプ』を参照してください。

図 1 Data Protector グラフィカルユーザーインタフェース



一般情報

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

HP テクニカルサポート

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

http://www.hp.com/support

HP に問い合わせる前に、以下の情報を集めておいてください。

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

メールニュース配信サービス

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

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

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

HP Web サイト

その他の情報については、次の HP Web サイトを参照してください。

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

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

ドキュメントに関する意見

HP では、皆さまのご意見をお待ちしております。

製品ドキュメントに関するご意見やお気づきの点があれば、Data Protector ドキュメントに対する意見という件名で AutonomyTPFeedback@hp.com までメッセージを送信してください。お知らせいただいた内容は、すべて HP に帰属することになります。

1 インストール手順の概要

この章では、Data Protector のインストール手順の概要およびインストールに関する概念を説明します。また、この章では、Data Protector Cell Manager および Data Protector ユーザーインタフェースについても説明します。

インストール手順の概要

Data Protector のバックアップ環境は、 同じタイムゾーンに所属し、同じ LAN または SAN 上に存在する複数のシステムで構成されます。これらのシステムでは、共通のバックアップ方針が適用されます。このネットワーク環境を Data Protector **セル**と呼びます。通常、セルは 1 つの Cell Manager、複数のインストールサーバー、クライアント、およびバックアップデバイスから構成されています。

Cell Manager は、 セルを集中管理するメインシステムです。Cell Manager は、Data Protector 内部データベース (IDB) を含み、Data Protector のコアソフトウェアおよび Session Manager を実行します。

IDB には、バックアップしたファイルとセルの構成が記録されます。

インストールサーバーは、 クライアントのリモートインストールに使用される Data Protector ソフトウェアレポジトリを含む、別のシステムまたは Cell Manager コンポーネントです。この Data Protector の機能によって、特にリモートクライアントのソフトウェアのインストール手順が容易になります。

通常、セルは、1 つの Cell Manager と複数のクライアントから構成されています。Data Protector ソフトウェアコンポーネントがコンピューターシステムにインストールされると同時に、そのシステムは、Data Protector **クライアント**になります。システムにインストールされるクライアントコンポーネントは、バックアップ環境におけるシステムの役割によって異なります。Data Protector コンポーネントは、1 台のシステムにローカルに、またはインストールサーバーから複数のシステムにインストールすることができます。

ユーザーインタフェースコンポーネントは、 Data Protector 機能にアクセスするために必要です。すべての構成作業および管理作業は、ユーザーインタフェースを使用して行われます。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システムにインストールする必要があります。Data Protector には、グラフィカルユーザーインタフェース (GUI) とコマンドラインインタフェース (CLI) があります。

バックアップが必要なディスクがあるクライアントシステムには、適切な Data Protector **Disk Agent** 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。Disk Agent では、クライアントディスクからのデータのバックアップまたはその復元ができます。

バックアップデバイスに接続されているクライアントシステムには、**Media Agent** 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。このソフトウェアでは、バックアップデバイスおよびメディアを管理します。Data Protector には、**General Media Agent** および **NDMP Media Agent** という 2 つの Media Agent があります。NDMP Media Agent は、NDMP サーバーのバックアップを制御するクライアントシステム (NDMP 専用ドライブを制御するクライアントシステム) にのみ必要です。それ以外の場合は、これらの 2 つの Media Agent は置き換え可能です。

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。

- Cell Manager がインストールされるシステム。サポートされるオペレーティングシステムおよびバージョンについては、最新のサポート一覧 (http://support.openview.hp.com/selfsolve/manuals) を参照してください。

  セルごとに設定できる Cell Manager は 1 つだけです。Cell Manager がインストールされていないと、Data Protector は実行できません。

- ユーザーインタフェースを介して、Data Protector の機能へのアクセスに使用されるシステム。これらのシステムには、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。
- バックアップされるシステム。これらのシステムには、ファイルシステムのバックアップ用の Disk Agent コンポーネント、およびオンラインデータベース統合用の関連 Application Agent 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。
- バックアップデバイスの接続先となるシステム。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。
- Data Protector インストールサーバーをインストールする 1 つまたは複数のシステム。ソフトウェアのリモートインストールには、UNIX クライアントと Windows クライアント用の 2 つのタイプのインストールサーバーを使用できます。

  インストールサーバーとして選択するシステムは、Cell Manager および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です。Cell Manager およびインストールサーバーは、同じシステム上、または別々のシステムにインストールできます。

  1 つのインストールサーバーを複数の 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ーは、Windows システム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ーは、HP-UX または Linux システムにインストールする必要があります。サポートされるオペレーティングシステムのバージョンについては、最新のサポート一覧 (http://support.openview.hp.com/selfsolve/manuals) を参照してください。

重要: Data Protector クライアントを Solaris システムにインストールする場合は、`/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。Data Protector をインストールすると、`/usr/omni` ディレクトリのすべてのファイルは削除されます。

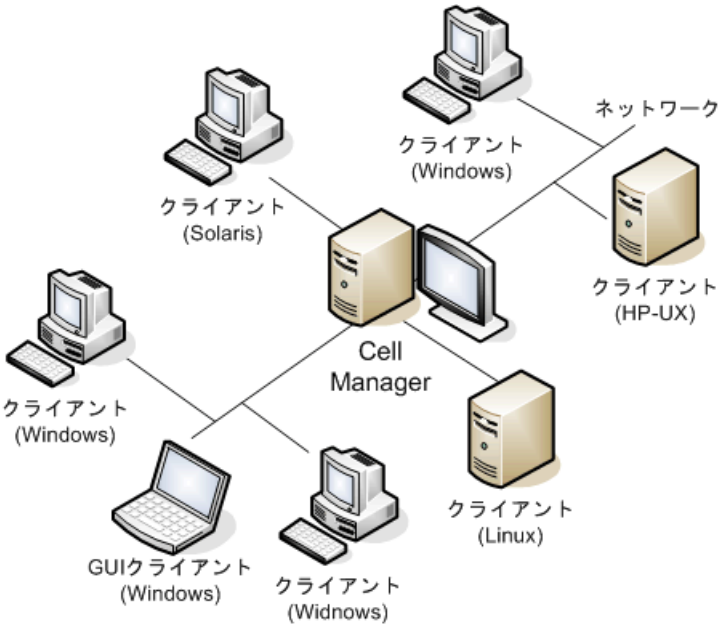
Data Protector セル内における各システムの役割を決定したら、インストール作業を行います。一般的な手順は以下のとおりです。

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ーおよびユーザーインタ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でインストールするか (推奨)、またはインストール 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ー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ー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 Data Protector Windows 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。[カスタムセットアップ] 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ーコンポーネントをすべて選択してください。

リモートインストールは、Windows XP Home Edition、HP OpenVMS クライアントでも実行できません。ローカルにインストールする必要があります。

図 2 Data Protector セル



リモート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ー (UNIX、Windows ともに少なくとも 1 台のインストールサーバーが必要) をインストールすると、リモートインストールがサポートされているオペレーティングシステムを使用して、Data Protector ソフトウェアをクライアントに配布できます。（「Data Protector のインストールの概念」(22 ページ) を参照）。

リモートインストールを実行するたびに、GUI を介してインストールサーバーにアクセスします。ユーザーインタフェースコンポーネントは Cell Manager にインストールできますが、これは前提条件ではありません。さまざまな場所から Cell Manager にアクセスできるように、ユーザーインタフェースを複数のシステムにインストールすることをお勧めします。

クライアントソフトウェアは、Windows 用のインストールサーバーから、Windows XP Home Edition 以外の Windows システムに配布できます。

Windows XP Home Edition クライアントシステムは、Data Protector の Windows 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。

クライアントソフトウェアは、HP-UX、Solaris、Linux、AIX、およびその他のサポートされている UNIX オペレーティングシステムに、UNIX システム用のインストールサーバーからリモートでインストールできます。サポートされるプラットフォームの一覧は、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。インストールサーバーはクライアントのローカルインストールには必要ありませんが、パッチを適用してクライアントを最新の状態を保つためには必要です。

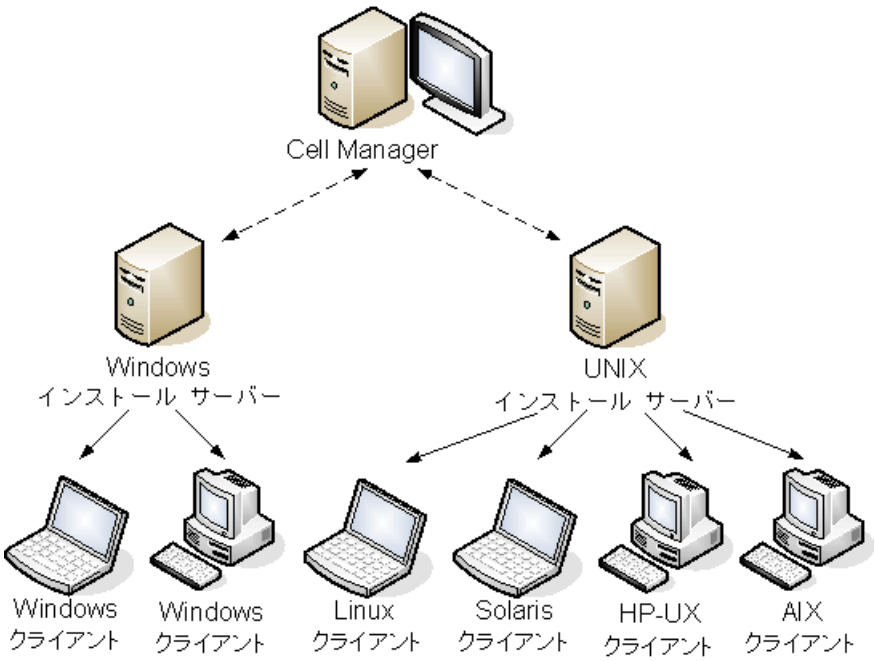
インストール先のシステムがリモートインストールをサポートしていない UNIX オペレーティングシステムである場合や、UNIX 用のインストールサーバーをインストールしていない場合は、Data Protector の UNIX 用インストール DVD-ROM を使用して、UNIX クライアントをローカルにインストールできます。

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、「Data Protector クライアントのインストール」(42 ページ) を参照してください。

UNIX クライアントのローカルアンインストールの手順は、「UNIX および Mac OS X システムのローカルインストール」(76 ページ) を参照してください。

図 3 Data Protector のインストールの概念



Data Protector のインストール DVD-ROM

Data Protector では、さまざまなオペレーティングシステムおよび複数のプロセッサーアーキテクチャーがサポートされています。すべてのプラットフォームに対応するために、DVD-ROM が 3 枚用意されています。DVD-ROM に収録されているコンポーネントの一覧は、「Data Protector DVD-ROM の一覧」 (22 ページ) を参照してください。

注記: Windows Vista、Windows 7、Windows 8、Windows Server 2008、Windows Server 2012 システム用の Data Protector インストールファイルは、Data Protector によってデジタル署名されています。

表 3 Data Protector DVD-ROM の一覧

DVD 番号	DVD-ROM のタイトル	内容
1	Data Protector Starter Pack for Windows および HP OpenVMS クライアント用のエージェントが含まれています。	• Windows 64 ビット (AMD64/Intel EM64T) システム用の Cell Manager およびインストールサーバー • PDF 形式の英語版マニュアル一式 (DOCS ディレクトリ) • 64 ビット版 Windows クライアント • HP OpenVMS クライアント (Alpha および Itanium システム) • 製品情報 • HP ソフトウェア統合パッケージ
2	Data Protector スターターパック (HP-UX 用) 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。	• HP-UX システム用の Cell Manager、インストールサーバー、およびクライアント • その他の UNIX システムのクライアント • Mac OS X システム用のクライアント • PDF 形式の英語版マニュアル一式 (DOCS ディレクトリ) • HP ソフトウェア統合パッケージ
3	Data Protector Starter Pack for Linux	• Linux 用の Cell Manager、インストールサーバー、およびクライアント

表 3 Data Protector DVD-ROM の一覧 (続き)

DVD 番号	DVD-ROM のタイトル	内容
	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。	• その他の UNIX システムのクライアント • Mac OS X システム用のクライアント • PDF 形式の英語版マニュアル一式 (DOCS ディレクトリ) • HP ソフトウェア統合パッケージ

Cell Manager システムの選択

Cell Manager は、Data Protector セル内のメインシステムです。Cell Manager はセルを集中管理します。Cell Manager の機能は次のとおりです。

- Data Protector のコアソフトウェアを実行します。
- Data Protector 内部データベース (IDB) サーバーをホストします。
- Data Protector セッションに関する情報があるデータを収集および維持します。
- Session Manager を実行します。Session Manager は、各種の Data Protector を開始および停止するほか、関連する情報を 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。

- 対応プラットフォーム

  Cell Manager は、Windows、HP-UX、または Linux プラットフォームにインストールできます。

  これらのプラットフォームのサポートされるバージョンまたはリリースの詳細は、最新のサポート一覧 (http://support.openview.hp.com/selfsolve/manuals) を参照してください。

- 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 が正常に動作していないとバックアップや復元を実行できなくなるため、お使いの環境では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の増加および 必要なディスクスペース

  Cell Manager は、Data Protector 内部データベース (IDB) を保持しています。IDB には、バックアップ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ます。環境によっては、IDB のサイズがかなり増加する可能性があります。たとえば、バックアップの大部分がファイルシステムバックアップの場合は、標準的な IDB のサイズは、バックアップされたデータに使用されるディスクスペースの 2% となります。

  データベースのサイズおよび拡張に関する計画および管理の詳細は、『HP Data Protector ヘルプ』の索引「IDB のサイズ増加とパフォーマンス」を参照してください。

  IDB に必要な最小ディスクスペースについては、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。

注記: Cell Manager を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 Cell Manager システムと Data Protector ユーザーインタフェースコンポーネントを、Windows プラットフォームを使用した別のシステムにインストールできます。

この次に行う作業

「Data Protector Cell Manager およびインストールサーバーのインストール」 (26 ページ) を参照して、将来の Cell Manager システムの最小要件を決定します。

Data Protector ユーザーインタフェースシステムの選択

Data Protector には、グラフィカルユーザーインタフェース (GUI) とコマンドラインインタフェース (CLI) の 2 種類のユーザーインタフェースがあります。GUI は Windows プラットフォームで使用でき、CLI は Windows、HP-UX、Solaris、および Linux プラットフォームで使用できます。両方のユーザーインタフェースは、単一の Data Protector ソフトウェアコンポーネントとして提供され、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ー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ー環境では、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、異種混合環境では、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。

ユーザーインタフェースに対してサポートされているオペレーティングシステム（リリース、バージョン、エディション）の詳細は、http://support.openview.hp.com/selfsolve/manuals で最新のサポート一覧を参照してください。ローカル言語サポート、およびファイル名に非 ASCII 文字を使用することについては、『HP Data Protector ヘルプ』の索引「言語設定、カスタマイズ」を参照してください。

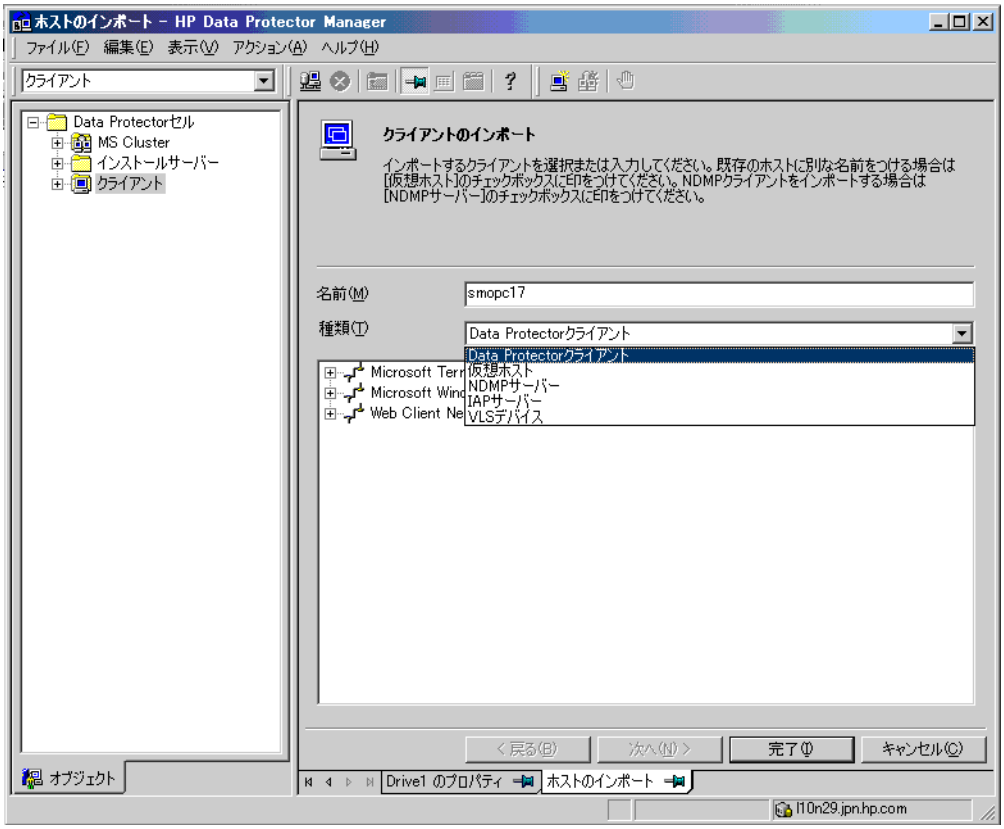
セル内のシステムにユーザーインタフェースをインストールすると、そのシステムから Cell Manager にリモートでアクセスできます。Cell Manager でグラフィカルユーザーインタフェースシステムを使用する必要はありません。

Data Protector グラフィカルユーザーインタフェース

Data Protector GUI は高機能ユーザーインタフェースであり、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]、[オブジェクト操作]、[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] などのビューがあり、関連するすべての作業をこれらのビューで行うことができます。

たとえば、[クライアント] ビューでは、すべての対象システム、および指定したインストールサーバーに送られるインストールパスとオプションを指定することによって、クライアントをリモートでインストール (追加) できます。クライアントでセットアップが稼動している場合は、インストール固有のメッセージがモニターウィンドウに表示されます。

図 4 Data Protector グラフィカルユーザーインタフェース



「Data Protector グラフィカルユーザーインタフェース」 (17 ページ) も参照してください。
Data Protector GUI の主な領域について説明しています。

2 ネットワークへの Data Protector のインストール

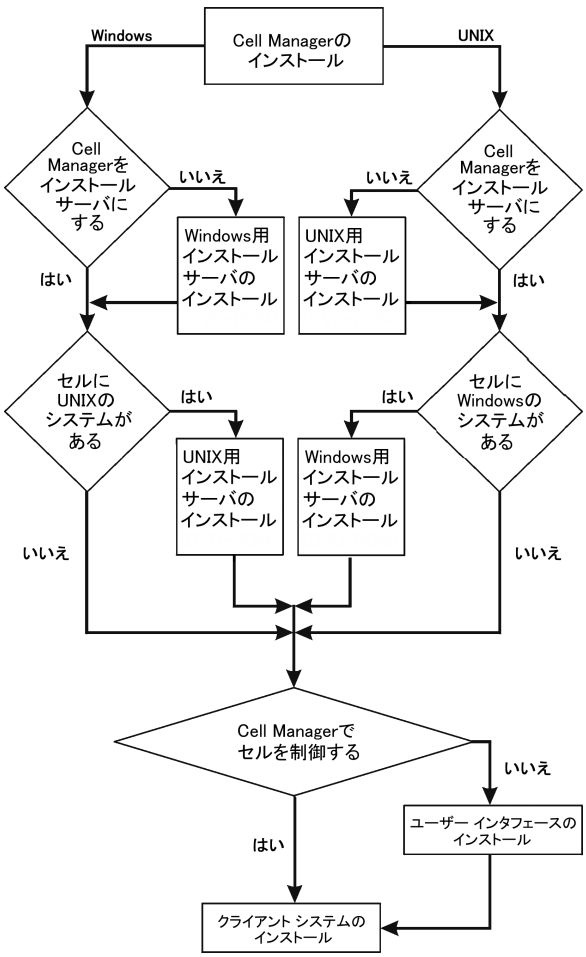
この章では、以下の各作業について詳細な手順を示します。

- Data Protector Cell Manager およびインストールサーバーのインストール
- Data Protector クライアントのインストール
- Data Protector 統合クライアントのインストール
- 各国語版 Data Protector マニュアルのインストール
- Data Protector シングルサーバー版のインストール
- Data Protector Web Reporting のインストール
- クラスターへの Data ProtectorCell Manager、インストールサーバー、およびクライアントのインストール: MC/ServiceGuard
- クラスターへの Data Protector Cell Manager およびクライアントのインストール: Microsoft Cluster Server
- クラスターへの Data Protector クライアントのインストール: Veritas クラスター、IBM HACMP クラスター、Microsoft Hyper-V クラスター

Data Protector Cell Manager およびインストールサーバーのインストール

インストール手順については、「インストール手順」 (26 ページ) を参照してください。

図 5 インストール手順



Cell Manager とインストールサーバー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。

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、「Windows 用 Cell Manager のインストール」 (32 ページ) を参照してください。

前提条件

- インストールで使用するユーザーアカウントには、選択したターゲットシステムに対する管理者 (`root`) 権限が付与されている必要があります。
- Cell Manager となるシステムは、以下の条件を満たしていなければなりません。
  - サポート対象の UNIX 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 でサポートしているオペレーティングシステムのリストについては、『http://support.openview.hp.com/selfsolve/manuals 』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。
  - 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。詳細については、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』の「インストールの要件」を参照してください。

    リンクディレクトリを使用することで、空きディスクスペースの不足を解決できます。リンクを作成する場合は、事前に「HP-UX および Linux システムにインストールされるディレクトリの構造」 (29 ページ) を参照してください。
  - Data Protector 内部データベース (IDB) 用の十分な空きディスクスペースがあること。詳細については、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』の「インストールの要件」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。
  - NIS サーバーを使用する場合は、Cell Manager システムを認識するように構成されていること。「NIS サーバーの準備」 (231 ページ) を参照してください。
  - 以下のポートが使用可能であること。
    - 5555 — Data Protector 通信用のデフォルトポート
    - 7112 — 内部データベースサービスポート
    - 7113 — 内部データベース接続プーラー (IDB CP) ポート
    - 7116 — アプリケーションサーバー (HTTPS AS) ポート
    - 9999 — アプリケーションサーバー管理ポート

    デフォルトの通信ポート番号を変更する場合は、「デフォルトの Data Protector Inet ポートの変更」 (227 ページ) を参照してください。デフォルトの IDB ポートとアプリケーションサーバーポートを変更する場合は、「UNIX システムでデフォルトの Data Protector IDB ポートおよびユーザーアカウントを変更する」 (228 ページ) 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` *`DirectoryPath`* コマンドを実行します。
- `inetd` または `xinetd` デーモンが正常に稼働していること。
- ユーザーグループ `hpdp` と、このユーザーグループ内の専用ユーザーアカウント `hpdp` が Data Protector で使用できるように構成されていること。デフォルトのユーザーアカウントを変更するには、「UNIX システムでデフォルトの Data Protector IDB ポートおよびユーザーアカウントを変更する」 (228 ページ) を参照してください。

クラスター対応 Cell Manager

クラスター対応 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。「クラスター対応 Cell Manager のインストール」 (116 ページ) 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。

推奨事項

- HP では、Data Protector 内部データベースおよび 2 GB を超える可能性がある DC バイナリファイルを格納するファイルシステムではラージファイルサポート (LFS) を使用することをお勧めします。

カーネルパラメーターの設定

HP-UX システムの場合:

- カーネルパラメーター `shmmax`(共有メモリーセグメントの最大サイズ) は、2.5GB 以上に設定します。構成をチェックするには、以下のコマンドを実行します。

  ```
  kcusage shmmax
  ```

- HP は、カーネルパラメーター `maxdsiz` または `maxdsiz_64`(最大データセグメントサイズ) を 134217728 バイト (128MB) 以上に設定し、カーネルパラメーター `semmnu`(セマフォのアンドゥ構造の数) を 256 以上に設定することをお勧めします。これらの変更が完了したら、カーネルを再コンパイルしシステムを再起動してください。

Linux システムの場合:

- カーネルパラメーター `shmmax`(共有メモリーセグメントの最大サイズ) は、2.5GB 以上に設定します。構成をチェックするには、以下のコマンドを実行します。

  ```
  cat /proc/sys/kernel/shmmax
  ```

インストール手順

ヒント: Cell Manager とインストールサーバー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 Data Protector Command Line Interface Reference』を参照してください。

HP-UX または 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. 適切な UNIX インストール DVD-ROM(HP-UX または Linux 用) をマウントポイントに挿入してマウントします。

   DVD-ROM ファイルシステムは Rock Ridge 拡張を使用します。

   必要に応じて、DVD-ROM からローカルディスクに次のディレクトリをコピーします。

   `LOCAL_INSTALL`

   `platform_dir``/DP_DEPOT`

   ここで、*`platform_dir`* には、以下のいずれかの値を指定します。

`hpux`	HP-UX システムの場合
`linux_x86_64`	Linux システムの場合

2. `LOCAL_INSTALL` ディレクトリに移動して、以下のコマンドを実行します。

   `./omnisetup.sh -CM`

   `omnisetup.sh` コマンドの詳細は、『HP Data Protector Command Line Interface Reference』を参照してください。

UNIX 用のインストールサーバーを 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、「UNIX システム用のインストールサーバーのインストール」 (38 ページ) を参照してください。

HP-UX および Linux システム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ーは`/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 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/`

`/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。

`/opt/omni/bin`	ユーザーコマンド
`/opt/omni/help/C`	ヘルプ
`/opt/omni/lbin`	管理コマンド、コマンドラインユーティリティ
`/opt/omni/sbin`	管理コマンド、コマンドラインユーティリティ
`/opt/omni/sbin/install`	インストール用スクリプト
`/etc/opt/omni`	構成データ
`/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`	電子的な PDF 形式のガイド
`/var/opt/omni/log /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`	man ページ
`/var/opt/omni/tmp`	一時ファイル
`/var/opt/omni/server/db80`	IDB ファイル

	詳細は、『HP Data Protector ヘルプ』の索引「IDB、ディレクトリの位置」の内容を参照してください。
/opt/omni/AppServer	HP Data Protector アプリケーションサーバー。
/opt/omni/idb	HP Data Protector の内部データベース
/opt/omni/jre	Data Protector で使用する Java ランタイム環境

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 システムの場合:

/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 パラメーターが格納されます。このパラメーターは、以下のいずれかの値をとります。

omni=1	システムの再起動時に 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。
omni=0	システムの再起動時に Data Protector の自動停止および自動起動を行いません。

Linux システムの場合:

/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、および 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 システムの場合:

/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 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。

`/opt/omni/lbin/mmd`

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 `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。

`/opt/omni/lbin/kms`

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 `Key Management Server (KMS)` サービスが実行されます。KMS は、Data Protector 暗号化機能のキーを管理します。

`/opt/omni/idb/bin/postgres`

Data Protector 内部データベースサービス `(hpdp-idb)` は、IDB を実行するサービスです。内部データベースサービスは、内部データベースからの情報を必要とするプロセスによって Cell Manager 上でローカルにアクセスされます。このサービスがリモートでアクセスされるのは、Cell Manager 上の IDB から Manager-of-Manager(MoM) 上の IDB への転送に関するメディア管理情報の場合のみです。

`/opt/omni/idb/bin/pgbouncer`

Data Protector 内部データベース接続プーラー `(hpdp-idb-cp)` サービスは、hpdb-idb への開いた接続のプールを提供します。要求時に接続プールを使用することで、要求のたびに新しい接続を開く必要がなくなるため、hpdp-idb 接続の拡張性が確保されます。このサービスは、Cell Manager 上で実行され、ローカルプロセスによってのみアクセスされます。

`/opt/omni/AppServer/bin/standalone.sh`

Data Protector アプリケーションサーバー `(hpdp-as)` サービスは、HTTPS 接続 (Web サービス) を介した IDB への GUI 接続に使用されます。このサービスは Cell Manager 上で実行され、hpdp-idb-cp サービスへのローカル接続があります。

環境変数の設定

Data Protector を使用する場合は、事前にお使いのオペレーティングシステム構成の環境変数の値を追加してください。

- Data Protector man ページをどこからでも閲覧できるようにするには、`/opt/omni/lib/man` を `MANPATH` 変数に追加します。
- Data Protector コマンドをどのディレクトリからでも実行できるようにするには、コマンドの場所を `PATH` 変数に追加します。Data Protector ドキュメントの手順は、変数値が追加されていることを前提とします。コマンドの場所については、『HP Data Protector Command Line Interface Reference』の `omniintro` のリファレンスページ、および `omniintro` の man ページを参照してください。

この次に行う作業

この段階で、Cell Manager(および選択した場合は UNIX システム用のインストールサーバー)がインストールされています。準備が整ったら、以下の作業を実施します。

1. UNIX 用のインストールサーバーを同一システム上にインストールしなかった場合は、「UNIX システム用のインストールサーバーのインストール」 (38 ページ) を参照してください。
2. 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する場合は、Windows 用のインストールサーバーをインストールします。「Windows システム用のインストールサーバーのインストール」 (39 ページ) 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。「Data Protector クライアントのインストール」 (42 ページ) を参照してください。

Windows 用 Cell Manager のインストール

前提条件

- インストールで使用するユーザーアカウントは、以下の条件を満たす必要があります。
  - 選択したターゲットシステムに対する管理者 (`Administrator`) 権限が付与されていること。
  - ネットワークアクセスユーザー権限が Windows ローカルセキュリティポリシー内に設定されていること。
- Data Protector Inet サービスはデフォルトで、Windows ローカルユーザーアカウント SYSTEM で実行されます。ただし、さまざまな理由から Inet サービスが Windows ドメインユーザーアカウントで実行されている場合は、さらに次の Windows オペレーティングシステムのセキュリティポリシー特権も付与される必要があります。
  - 認証後にクライアントを偽装
  - プロセスレベルトークンの置き換え

  詳細は、『HP Data Protector ヘルプ』の索引「Inet ユーザーの成り済まし」を参照してください。
- Cell Manager となるシステムは、以下の条件を満たしていなければなりません。
  - 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 でサポートしているオペレーティングシステムのリストについては、『http://support.openview.hp.com/selfsolve/manuals 』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。
  - 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。詳細については、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』の「インストールの要件」を参照してください。
  - Data Protector 内部データベース (IDB) 用の十分な空きディスクスペースがあること。詳細については、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』の「インストールの要件」を参照してください。
  - 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。コンピューターの名前とホスト名は同じでなければなりません。
  - 固定 IP アドレスが割り当てられていること。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、その IP アドレスが変更されます。そのため、システムに恒久 DNS を割り当てる (再構成する) か、DHCP サーバーでシステムの静的 IP アドレス (IP アドレスはシステムの MAC アドレスにバインドされる) を構成する必要があります。
  - 以下のポートが使用可能であること。
    - 5555 — Data Protector 通信用のデフォルトポート
    - 7112 — 内部データベースサービスポート
    - 7113 — 内部データベース接続プーラー (IDB CP) ポート
    - 7116 — アプリケーションサーバー (HTTPS AS) ポート
    - 9999 — アプリケーションサーバー管理ポート

    IDB およびアプリケーションサーバーサービスポートはインストール時に変更できます。デフォルトの通信ポート番号を変更する場合は、「デフォルトの Data Protector Inet ポートの変更」 (227 ページ) を参照してください。

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。
  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ー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

- DC バイナリファイルが 2 GB よりも大きくなると思われる場合 (DC バイナリファイルのサイズは、ファイルシステムの設定でのみ制限可) は、NTFS ファイルシステムの使用をお勧めします。

クラスター対応 Cell Manager

クラスター対応 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。「クラスター対応 Cell Manager のインストール」 (117 ページ) を参照してください。

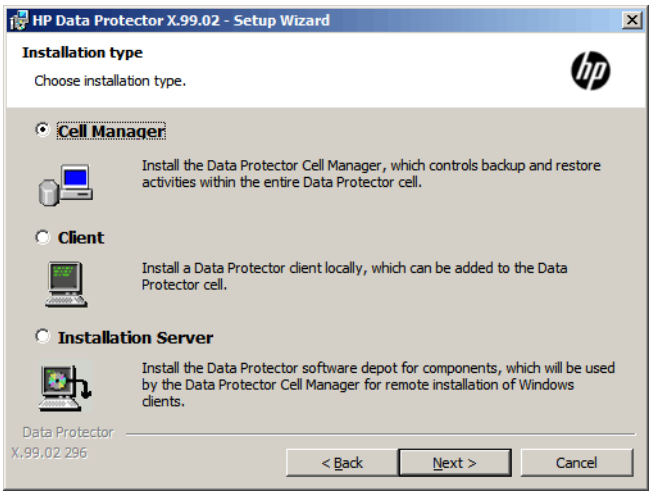
インストール手順

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ます。

   [ユーザーアカウント制御] ダイアログが表示されます。[続行] をクリックしてインストールを続けます。
2. HP Data Protector ウィンドウで **[Data Protector** のインストール**]** を選択し、Data Protector のセットアップ用ウィザードを開始します。
3. セットアップウィザードに従い、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。
4. [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 6 インストールの種類の選択



5. 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。

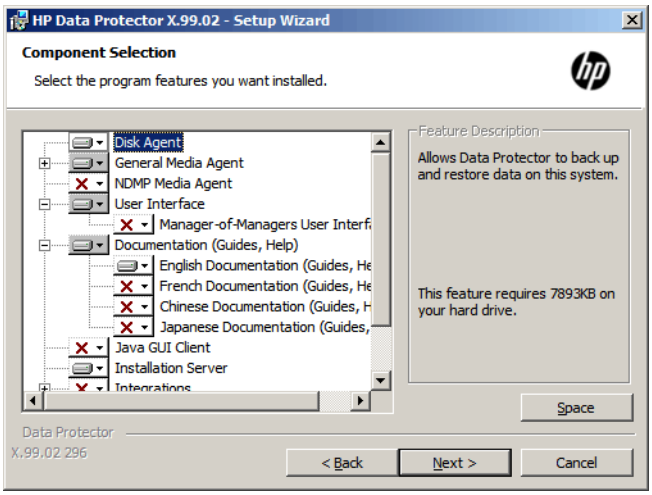
   [Next] をクリックし、次に進みます。

6. Data Protector をデフォルトのフォルダーにインストールする場合は、**[Next]** をクリックします。

   それ以外の場合は、**[Change]** をクリックして [Change Current Destination Folder] または [Change Current Program Data Destination Folder] ダイアログボックスを開き、必要に応じてインストールフォルダーを変更します。プログラムデータインストールフォルダーへのパスは 80 文字以内に制限されます。

7. [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、「Data Protector コンポーネント」 (44 ページ) を参照してください。

図 7 ソフトウェアコンポーネントの選択

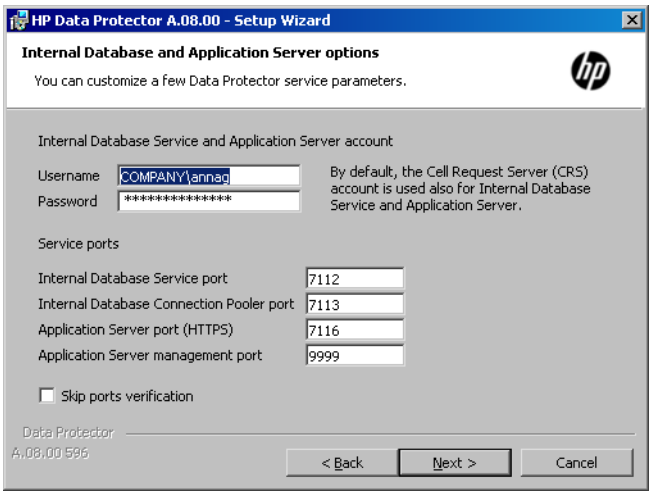


Disk Agent、**General Media Agent**、ユーザーインタフェース、および インストールサーバーがデフォルトで選択されています。**[Next]** をクリックします。

8. 必要に応じて、Data Protector IDB およびアプリケーションサーバーで使用するユーザーアカウントと、これらのサービスで使用するポートを変更します。

   [次へ] をクリックします。

図 8 IDB およびアプリケーションサーバーオプションの変更



9. Data Protector がシステムで Windows ファイアウォールを検出した場合、[Windows Firewall configuration] ページが表示されます。Data Protector セットアップにより、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

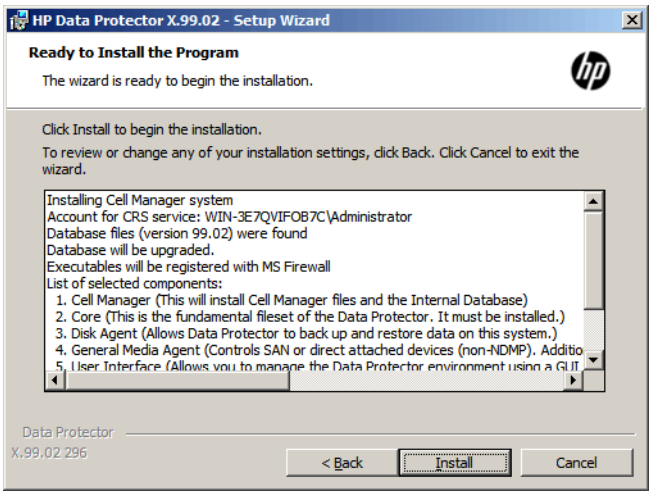
います。この時点で、Data Protector によってポートがオープンされないようにするには、オプションを選択解除します。ただし、Data Protector を適切に機能させるには、実行可能ファイルを有効にする必要があります。

自動生成されるのはインバウンドファイアウォールルールのみであり、アウトバウンドファイアウォールルールは手動で作成する必要があるので注意してください。必要なポート範囲については、『HP Data Protector ヘルプ』の索引「ファイアウォールのサポート」で表示される内容を参照してください。

[Next] をクリックします。

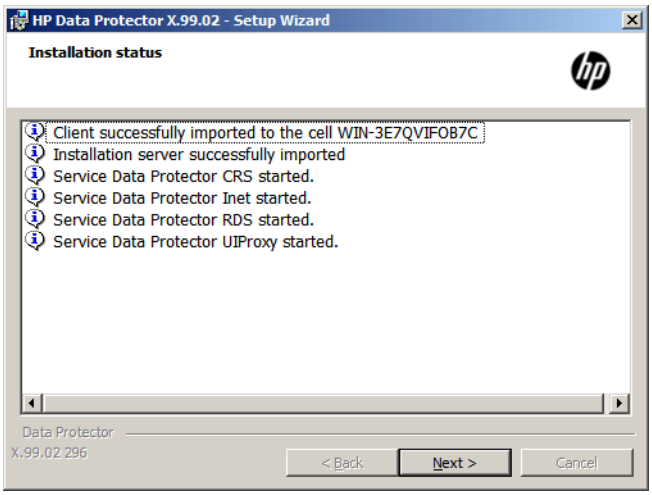
10. コンポーネントのサマリーリストが表示されます。**[Install]** をクリックして、選択したコンポーネントのインストールを開始します。この処理には、数分かかる場合があります。

図 9 コンポーネントのサマリーリスト



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

図 10 [Installation status] ページ



12. ユーザーインタフェースコンポーネントをインストールした場合に、セットアップ直後に Data Protector GUI を使用して操作を開始するには **[Data Protector GUI** の起動**]** を選択します。

英語版ドキュメント（ガイド、ヘルプ）コンポーネントをアップグレードしたか、または新しくインストールした場合に、セットアップ直後に『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を表示するには、**[Open the Product Announcements, Software Notes, and References]** を選択します。

[Finish] をクリックします。

インストール後の状態

Cell Manager ファイルは、*Data_Protector_home* ディレクトリおよび *Data_Protector_program_data* 内にあります。

ソフトウェアデポは、*Data_Protector_program_data*\Depot ディレクトリ内にあります。

Data Protector コマンドは、ディレクトリに格納されます。コマンドの場所については、『HP Data Protector Command Line Interface Reference』の omniintro のリファレンスページ、および omniintro の man ページを参照してください。

重要: HP では、お使いのオペレーティングシステム構成の適切な環境変数の値にコマンドの場所を追加して、どのディレクトリからでも Data Protector コマンドを実行できるようにすることをお勧めしています。Data Protector ドキュメントの手順は、環境変数の値が追加されていることを前提とします。

以下のプロセスが Cell Manager システムで実行します。

crs.exe	Data Protector Cell Request Server (CRS) サービスは Cell Manager システム上で実行され、Cell Manager ソフトウェアがシステムにインストールされると開始します。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。*Data_Protector_home*\bin ディレクトリで実行されます。
mmd.exe	Data Protector Media Management Daemon (MMD) サービスは Cell Manager システム上で実行され、Cell Manager ソフトウェアがシステムにインストールされると起動されます。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。*Data_Protector_home*\bin ディレクトリで実行されます。
OmniInet.exe	Cell Manager が他のシステムでエージェントを起動できるようにする Data Protector クライアントサービス。Data ProtectorInet 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。*Data_Protector_home*\bin ディレクトリで実行されます。
kms.exe	Data Protector Key Management Server (KMS) サービスは Cell Manager システム上で実行され、Cell Manager ソフトウェアがシステムにインストールされると開始します。KMS は、Data Protector 暗号化機能のキーを管理します。*Data_Protector_home*\bin ディレクトリで実行されます。
hpdp-idb	Data Protector 内部データベースサービス (hpdp-idb) は、IDB を実行するサービスです。内部データベースサービスは、内部データベースからの情報を必要とするプロセスによって Cell Manager 上でローカルにアクセスされます。このサービスは、Cell Manager 上の IDB から Manager-of-Manager(MoM) 上の IDB への転送に関するメディア管理情報に対してのみリモートでアクセスされます。
hpdp-idb-cp	Data Protector 内部データベース接続プーラー (hpdp-idb-cp) サービスは、hpdb-idb への開いた接続の

	プールを提供します。これにより、すべての要求に対して新しい接続が開かれるのではなく要求時に使用できるようになるため、hpdp-idb 接続の拡張性が確保されます。このサービスは、Cell Manager 上で実行され、ローカルプロセスによってのみアクセスされます。
`hpdp-as`	Data Protector アプリケーションサーバー (`hpdp-as`) サービスは、HTTPS 接続 (Web サービス) を介した IDB への GUI 接続に使用されます。このサービスは Cell Manager 上で実行され、hpdp-idb-cp サービスへのローカル接続があります。

注記: 複数のプラットフォームにまたがるバックアップや復元を Data Protector ユーザーインタフェースから実行する場合は、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照して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。手順の詳細については、オペレーティングシステムのドキュメントを参照してください。

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前提条件を検証し、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。「前提条件」 (32 ページ) を参照してください。

セットアップがチェックする前提条件を以下に示します。

- Service Pack のバージョン
- `nslookup` により、Data Protector がホスト名を展開できることが確認されていること
- ディスクスペース
- 管理者権限

この次に行う作業

この段階で、Cell Manager がインストールされます。また、選択した場合は Windows 用のインストールサーバーもインストールされます。準備が整ったら、以下の作業を実施します。

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 用インストールサーバーをインストールします。「インストールサーバーのインストール」 (37 ページ) を参照してください。なお、UNIX システム用のインストールサーバーが不要な場合は、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。「Data Protector クライアントのインストール」 (42 ページ) を参照してください。

インストールサーバーのインストール

インストールサーバーは、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ー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、http://support.openview.hp.com/selfsolve/manuals 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ーを配置する場合は、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 システム用のインストールサーバーのインストール

前提条件

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

- HP-UX または 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ーでサポートされているオペレーティングシステムの詳細は、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。
- `inetd` または `xinetd` デーモンが稼働していること。
- 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、「デフォルトの Data Protector Inet ポートの変更」 (227 ページ) 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 Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。
- DVD-ROM ドライブにアクセスできること。
- Data Protector セル内の Cell Manager は、バージョン 8.00 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/`

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ます。

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ー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ーを HP-UX 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. 適切な UNIX インストール DVD-ROM(HP-UX または Linux 用) をマウントポイントに挿入してマウントします。

   DVD-ROM ファイルシステムは Rock Ridge 拡張を使用します。

   必要に応じて、DVD-ROM からローカルディスクに次のディレクトリをコピーします。

   `LOCAL_INSTALL`

   `platform_dir``/DP_DEPOT`

   ここで、*`platform_dir`* には、以下のいずれかの値を指定します。

`hpux`	HP-UX システムの場合
`linux_x86_64`	Linux システムの場合

2. `LOCAL_INSTALL` ディレクトリに移動して、以下のコマンドを実行します。

   `./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、または DVD-ROM の*Mount_point*/DOCS/C/MAN ディレクトリにある『HP 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ーのすべてのパッケージがインストールされます。パッケージのサブセットのみをインストールするには、swinstall (HP-UX の場合) または rpm (Linux の場合) を使用する必要があります。「ネイティブツールを使用した、HP-UX および Linux システムへのインストール」 (218 ページ) 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ーをインストールしない場合は、UNIX インストール DVD-ROM (HP-UX または Linux 用) 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。さらに、Data Protector クライアント上のコンポーネントはパッチできなくなります。

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ー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、以下の作業を実施します。

1. インストールサーバーを 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。「セルへのインストールサーバーのインポート 」 (130 ページ) を参照してください。

   注記: インストールサーバーをインポートすると、Cell Manager 上の/etc/opt/omni/server/cell/installation_servers が更新されて、インストール済みのリモートインストールパッケージが一覧表示されます。CLI からこのファイルを使用して、使用可能なリモートインストール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、リモートインストールパッケージをインストールまたは削除したときは必ずインストールサーバーのエクスポートと再インポートを実行してください。これは、インストールサーバーを 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 システムがある場合は、Windows 用のインストールサーバーをインストールします。「Windows システム用のインストールサーバーのインストール」 (39 ページ) 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。「Data Protector クライアントのインストール」 (42 ページ) を参照してください。

Windows システム用のインストールサーバーのインストール

前提条件

インストールサーバー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ー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、http://support.openview.hp.com/selfsolve/manuals を参照してください。
- 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 Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。
- 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。コンピューターの名前とホスト名は同じでなければなりません。

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ー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。

重要: ネットワーク上に Windows 用インストールサーバーをインストールしない場合は、DVD-ROM からすべての Windows 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。

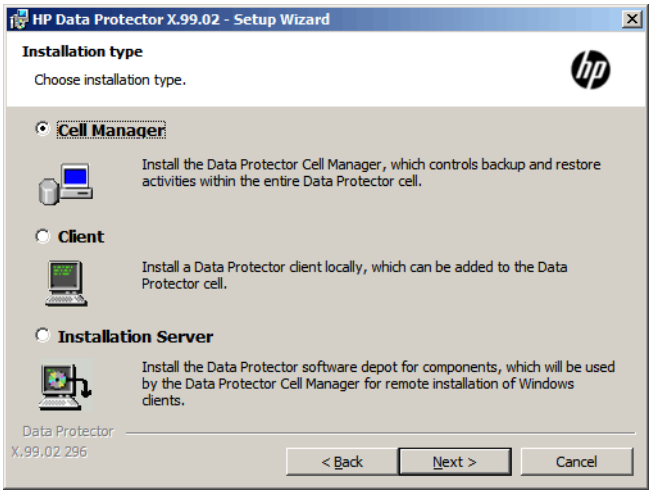
注記: インストールサーバーのインストール後、Windows システムには Data Protector クライアントをリモートでインストールすることはできません。同一システム上にインストールサーバーとクライアントコンポーネントをインストールする場合は、クライアントをローカルにインストールする必要があります。この場合はインストール手順の中で、必要なクライアントコンポーネントとインストールサーバーコンポーネントをすべて選択してください。
「Windows 用クライアントのインストール」 (47 ページ) を参照してください。

インストール手順

Windows システム用のインストールサーバー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ます。
   [ユーザーアカウント制御] ダイアログが表示されます。**[**続行**]** をクリックしてインストールを続けます。
2. HP Data Protector ウィンドウで **[Data Protector** のインストール**]** を選択し、Data Protector のセットアップ用ウィザードを開始します。
3. セットアップウィザードに従い、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。
4. **[Installation Type]** ページで、**[**インストールサーバー**]** 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 11 インストールの種類の選択



5. Data Protector をデフォルトフォルダーにインストールする場合には、**[Next]** をクリックします。
   それ以外の場合は、**[Change]** をクリックして [Change Current Destination Folder] ウィンドウを開き、別のパスを入力します。
6. Data Protector がシステムで Windows ファイアウォールを検出した場合、[Windows Firewall configuration] ページが表示されます。Data Protector セットアップにより、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**

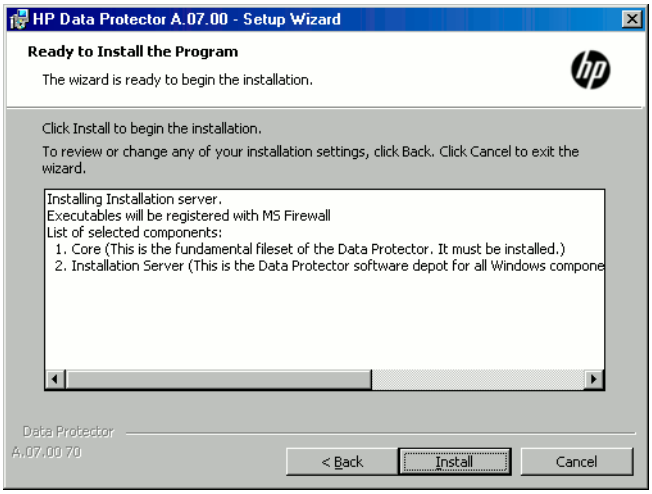
newly registered Data Protector binaries to open ports as needed] オプションが選択されています。この時点で、Data Protector によってポートがオープンされないようにするには、オプションを選択解除します。ただし、Data Protector を適切に機能させるには、実行可能ファイルを有効にする必要があります。

自動生成されるのはインバウンドファイアウォールルールのみであり、アウトバウンドファイアウォールルールは手動で作成する必要があるので注意してください。必要なポート範囲については、『HP Data Protector ヘルプ』の索引「ファイアウォールのサポート」で表示される内容を参照してください。

[Next] をクリックします。

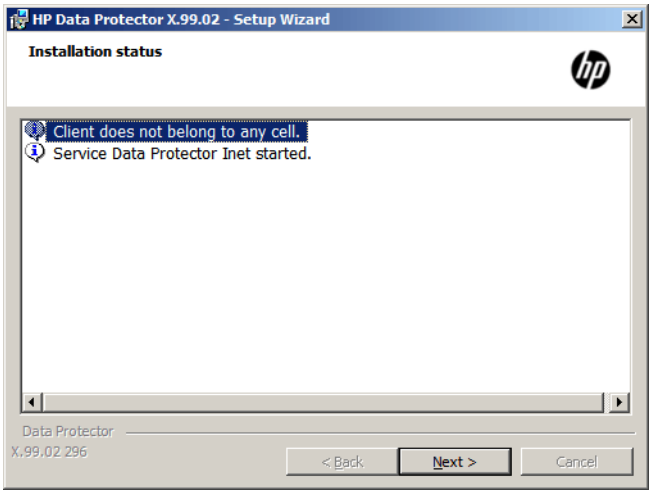
7. コンポーネントのサマリーリストが表示されます。**[Install]** をクリックして、選択したコンポーネントのインストールを開始します。この処理には、数分かかる場合があります。

図 12 コンポーネント選択サマリーページ



8. インストールステータスのページが表示されます。**[Next]** をクリックします。

図 13 [Installation Status] ページ



9. **[Finish]** をクリックします。

インストールが完了すると、ソフトウェアはデフォルトで *Data_Protector_program_data*\Depot ディレクトリにインストールされます。ソフトウェアは共有されるため、ネットワーク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ー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。

1. 独立した形で (たとえば、Cell Manager とは別のシステムに) インストールサーバー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) する必要があります。「セルへのインストールサーバーのインポート」 (130 ページ) を参照してください。
2. 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 システムまたは Linux システム上に、UNIX 用のインストールサーバーをインストールします。「UNIX システム用のインストールサーバーのインストール」 (38 ページ) 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。「Data Protector クライアントのインストール」 (42 ページ) 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ー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、「Data Protector のインストール DVD-ROM」 (22 ページ) を参照してください。

クライアントのインストールが完了したら、各クライアントの適切な環境変数にコマンドの場所を追加して、どのディレクトリからでも Data Protector コマンドを実行できるようにすることをお勧めします。Data Protector ドキュメントの手順は、変数値が追加されていることを前提とします。コマンドの場所については、『HP Data Protector Command Line Interface Reference』の `omniintro` のリファレンスページ、および `omniintro`man ページ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、セル内にインポートした後には、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、「Data Protector クライアントのインストール結果の確認 」 (210 ページ) を参照してください。セキュリティ保護の詳細については、「セキュリティについて」 (135 ページ) を参照してください。

「Data Protector クライアントのインストール」 (42 ページ) 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 4 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	インストールの種類とリファレンス
Windows	リモートおよびローカルインストール。「Windows 用クライアントのインストール」 (47 ページ) を参照してください。
HP-UX	リモートおよびローカルインストール。「HP-UX クライアントのインストール」 (51 ページ) を参照してください。
Solaris	リモートおよびローカルインストール。「Solaris 用クライアントのインストール」 (54 ページ) を参照してください。
Linux	リモートおよびローカルインストール。「Linux クライアントのインストール」 (60 ページ) を参照してください。
ESX Server	リモートおよびローカルインストール。「ESX Server クライアントのインストール」 (63 ページ) を参照してください。
Mac OS X	リモートおよびローカルインストール。「Mac OS X クライアントのインストール」 (63 ページ) を参照してください。
IBM AIX	リモートおよびローカルインストール。「IBM AIX クライアントのインストール」 (64 ページ) を参照してください。

表 4 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	インストールの種類とリファレンス
HP OpenVMS	ローカルインストール。「HP OpenVMS クライアントのインストール」 (65 ページ) を参照してください。
その他の UNIX システム	ローカルインストール。「UNIX および Mac OS X システムのローカルインストール」 (76 ページ) を参照してください。
DAS Media Agent クライアント	リモートおよびローカルインストール。「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」 (79 ページ) を参照してください。
ACS Media Agent クライアント	リモートおよびローカルインストール。「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」 (79 ページ) を参照してください。

統合

Data Protector 用統合ソフトウェアとは、Data Protector でデータベースアプリケーションをバックアップするソフトウェアコンポーネントです。MS Exchange Server データベースのバックアップには `MS Exchange 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や 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、「統合ソフトウェアのインストール」 (43 ページ) を参照してください。

表 5 統合ソフトウェアのインストール

ソフトウェアアプリケーションまたはディスクアレイファミリ	リファレンス
Microsoft Exchange Server	「Microsoft Exchange Server クライアント」 (87 ページ) を参照してください。
Microsoft SQL Server	「Microsoft SQL Server クライアント」 (89 ページ) を参照してください。
Microsoft SharePoint Server	「Microsoft SharePoint Server クライアント」 (89 ページ) を参照してください。
Microsoft ボリュームシャドウコピーサービス (VSS)	「Microsoft ボリュームシャドウコピーサービスクライアント」 (91 ページ) を参照してください。
Sybase Server	「Sybase Server クライアント」 (91 ページ) を参照してください。
Informix Server	「Informix Server クライアント」 (91 ページ) を参照してください。
SAP R/3	「SAP R/3 クライアント」 (92 ページ) を参照してください。
SAP MaxDB	「SAP MaxDB クライアント」 (92 ページ) を参照してください。
Oracle Server	「Oracle Server クライアント」 (92 ページ) を参照してください。
IBM DB2 UDB	「IBM DB2 UDB クライアント」 (93 ページ) を参照してください。
Lotus Notes/Domino Server	「Lotus Notes/Domino Server クライアント」 (93 ページ) を参照してください。
VMware	「VMware クライアント」 (93 ページ) を参照してください。
Microsoft Hyper-V	「Microsoft Hyper-V クライアント」 (96 ページ) を参照してください。
Network Data Management Protocol (NDMP) Server	「NDMP Server クライアント」 (97 ページ) を参照してください。
HP P4000 SAN ソリューション	「HP P4000 SAN ソリューション クライアント」 (97 ページ) を参照してください。
HP P6000 EVA ディスクアレイファミリ	「HP P6000 EVA ディスクアレイファミリ クライアント」 (97 ページ) を参照してください。
HP P9000 XP ディスクアレイファミリ	「HP P9000 XP ディスクアレイファミリ クライアント」 (102 ページ) を参照してください。

表 5 統合ソフトウェアのインストール (続き)

ソフトウェアアプリケーションまたはディスクアレイファミリ	リファレンス
HP 3PAR StoreServ Storage	「HP 3PAR StoreServ Storage クライアント」 (107 ページ) を参照してください。
EMC Symmetrix	「EMC Symmetrix クライアント」 (108 ページ) を参照してください。

表 6 他のインストール

インストール	リファレンス
各国語版ユーザーインタフェース	「各国語版 Data Protector ユーザーインタフェースのインストール」 (111 ページ) を参照してください。
Web レポート	「Data Protector Web Reporting のインストール」 (115 ページ) を参照してください。
MC/ServiceGuard	「MC/ServiceGuard への Data Protector のインストール」 (116 ページ) を参照してください。
Microsoft Cluster Server	「Microsoft Cluster Server への Data Protector のインストール」 (117 ページ) を参照してください。
Veritas Cluster Server	「Veritas Cluster への Data Protector クライアントのインストール」 (125 ページ) を参照してください。
IBM HACMP Cluster	「Data Protector の IBM HACMP Cluster へのインストール」 (125 ページ) を参照してください。
Microsoft Hyper-V クラスター	「Microsoft Hyper-V クラスターでの Data Protector のインストール」 (126 ページ) を参照してください。

Data Protector コンポーネント

サポート対象プラットフォームの最新情報は、HP Data Protector のホームページ (http://support.openview.hp.com/selfsolve/manuals) でご確認ください。

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には、Data Protector のグラフィカルユーザーインタフェース (Windows システム) とコマンドラインインタフェースの一部 (Windows システムおよび Unix システム) が含まれます。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する必要があります。

注記: Data Protector コマンドラインインタフェースの特定のコマンドは、他の Data Protector コンポーネントに含まれています。詳細は、『HP Data Protector Command Line Interface Reference』を参照してください。

異種混合環境で Data Protector のユーザーインタフェースを使用する前に、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照して制限事項を確認してください。

英語版マニュアル (ガイド、ヘルプ)

Data Protector の英語版マニュアルファイルセットです。

フランス語版マニュアル (ガイド、ヘルプ)

Data Protector のフランス語版マニュアルファイルセットです。

日本語版マニュアル (ガイド、ヘルプ)	Data Protector の日本語版マニュアルファイルセットです。
簡体字中国語版マニュアル (ガイド、ヘルプ)	Data Protector の簡体字中国語版マニュアルファイルセットです。
Manager-of-Managers ユーザーインタフェース	Manager-of-Managers ユーザーインタフェースには、Data Protector のグラフィカルユーザーインタフェースが含まれます。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。Manager-of-Managers ユーザーインタフェースと Manager ユーザーインタフェースは、共通アプリケーションとして使用できます。
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システム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システムか、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システムにインストールする必要があります。
自動ディザスタリカバリ	自動ディザスタリカバリコンポーネントは、自動ディザスタリカバリ手法を使用して復旧を行うシステムと、拡張自動ディザスタリカバリ (EADR) またはワンボタンディザスタリカバリ (OBDR) で使用する DR CD ISO イメージを作成することによってディザスタリカバリを自動化するシステムに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システム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 MaxDB 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。
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システムにインストールする必要があります。
VMware 用統合ソフトウェア (レガシー)	VMware 用統合ソフトウェア (レガシー) コンポーネントは、VirtualCenter システム (存在する場合)、および Data Protector でバックアップを行うすべての ESX Server システムにインストールする必要があります。また、VCBfile または VCBimage のバックアップ方法を採用する場合は、統合ソフトウェアコンポーネントをバックアッププロキシーシステムにもインストールする必要があります。
仮想環境統合ソフトウェア	仮想環境統合ソフトウェアのコンポーネントは、Data Protector の仮想環境統合ソフトウェアを使って仮想マシンのバックアップおよび復元を制御する際にバックアップホストとして使用するシステム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 があるシステム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システム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システムにインストールする必要があります。
MS Exchange 用統合ソフトウェア	MS Exchange 用統合ソフトウェアコンポーネントは、Data Protector Microsoft Exchange Server 2007 用統合ソフトウェアまたは Data Protector Microsoft Exchange Single Mailbox 用統合ソフトウェアを使用してバックアップを行う Microsoft Exchange Server 2007 システムにインストールする必要があります。 また、Data Protector Microsoft Exchange Single Mailbox 用統合ソフトウェアを使用してバックアップを行う Microsoft Exchange Server 2010 システムにもインストールする必要があります。
MS Exchange Server 2010+ 用統合ソフトウェア	MS Exchange Server 2010+ 用統合ソフトウェアコンポーネントは、Data Protector Microsoft Exchange Server 2010 用統合ソフトウェアを使用してバックアップを行う Microsoft Exchange Server 2010 または Microsoft Exchange Server 2013 システムにインストールする必要があります。
MS SQL 用統合ソフトウェア	MS SQL 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 SQL Server 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 SharePoint Server 2007/2010 用統合ソフトウェア	MS SharePoint 2007/2010 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 SharePoint Server 2007/2010 システムにインストールする必要があります。
MS ボリュームシャドウコピー用統合ソフトウェア	MS ボリュームシャドウコピー用統合ソフトウェアコンポーネントは、ボリュームシャドウコピーサービスによるバックアップを実行する Windows Server システムにインストールする必要があります。
HP P4000 Agent	HP P4000 Agent コンポーネントは、HP P4000 SAN ソリューション 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の両方にインストールする必要があります。
HP P6000/HP 3PAR SMI-S Agent	HP P6000/HP 3PAR SMI-S Agent コンポーネントは、Data Protector を HP P6000 EVA ディスクアレイファミリ と統合する場合、またはアプリケーションシステムとバックアップシステムが HP-UX システムである構成で Data Protector を HP 3PAR StoreServ Storage と統合する場合、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インストールする必要があります。
HP P9000 XP Agent	HP P9000 XP Agent コンポーネントは、Data Protector を HP P9000 XP ディスクアレイファミリ 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の両方にインストールする必要があります。

HP 3PAR VSS Agent	HP 3PAR VSS Agent コンポーネントは、アプリケーションシステムとバックアップシステムが Windows システムである構成で Data Protector を HP 3PAR StoreServ Storage と統合する場合、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、Data Protector を EMC Symmetrix 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の両方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 サーバーを介して 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システム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を実行する Lotus Notes/Domino Server データベースがあるすべてのシステムにインストールする必要があります。
MS Exchange Granular Recovery Extension	Data Protector Granular Recovery Extension for Microsoft Exchange Server は、Granular Recovery 機能を有効化するために、各 Microsoft Exchange Server システムにインストールする必要があります。Microsoft Exchange Server Database Availability Group (DAG) 環境では、DAG 内の任意の Exchange Server システムにインストールする必要があります。
MS SharePoint Granular Recovery Extension	Microsoft SharePoint Server 向け Data Protector Granular Recovery Extension は、Microsoft SharePoint Server サーバーの全体管理システムにインストールする必要があります。
VMware Granular Recovery Extension Web Plug-In	VMware 仮想マシンを細かな単位で復旧するには、Data Protector VMware Granular Recovery Extension Web Plug-In コンポーネントを VMware Virtual Server システムに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のみがサポートされています。
VMware Granular Recovery Extension Agent	VMware 仮想マシンの復元と、細かな単位での復旧を行うには、Data Protector VMware Granular Recovery Extension Agent コンポーネントをマウントプロキシシステムに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のみがサポートされています。

注記: General Media Agent と NDMP Media Agent を同じシステム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るプラットフォームとコンポーネントの詳細は、http://support.openview.hp.com/selfsolve/manuals 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 権限が必要です。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。

- 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 Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。

- 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。コンピューターの名前とホスト名は同じでなければなりません。
- ネットワークアクセスユーザー権限が、インストールを実行するアカウントの Windows ローカルセキュリティポリシーの下に設定されていることを確認します。

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ー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 XP Home Edition 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。
- Windows Vista、Windows 7、Windows 8、Windows Server 2008、または Windows Server 2012 にクライアントをリモートでインストールするときは、次のいずれかのアカウントを使用する必要があります。
  - リモートシステム上の組み込み管理者アカウント。このアカウントは、**管理者承認モード**を無効にした状態で有効にしておく必要があります。
  - ドメインユーザーアカウント。このアカウントは、リモートシステムのローカル管理者ユーザーグループのメンバーです。

自動ディザスタリカバリ

自動ディザスタリカバリコンポーネントは、拡張自動ディザスタリカバリ (EADR)、ワンボタンディザスタリカバリ (OBDR)、自動システム復旧 (ASR) のいずれかを使用して復旧を行うシステムと、EADR または OBDR で使用する DR CD ISO イメージを作成するシステム上にインストールする必要があります。

クラスター対応クライアント

クラスター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。詳細は、「クラスター対応クライアントのインストール」(123 ページ)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、「Data Protector コンポーネント」(44 ページ)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 を使用して、ローカルにインストールできます。

1. DVD-ROM を挿入します。

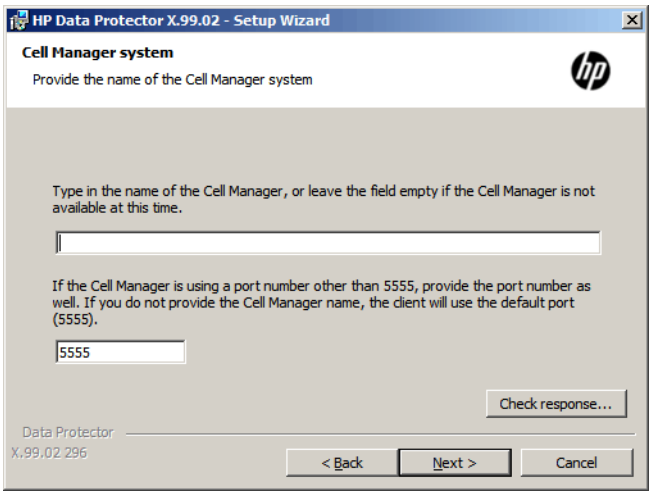
   Windows Vista、Windows 7、Windows 8、Windows Server 2008、Windows Server 2012 の場合は、[ユーザーアカウント制御] ダイアログボックスが表示されます。**[**続行**]** をクリックしてインストールを続けます。
2. HP Data Protector ウィンドウで **[Data Protector** のインストール**]** を選択し、Data Protector のセットアップ用ウィザードを開始します。
3. セットアップウィザードに従い、ライセンス契約を十分にお読みください。記載内容に同意する場合は、**[Next]** をクリックして次に進みます。
4. **[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。

5. Cell Manager の名前を入力します。「Cell Manager の選択」 (49 ページ) 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 14 Cell Manager の選択



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

   それ以外の場合は、**[Change]** をクリックして [Change Current Destination Folder] ページを開き、パスを入力します。

7. 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、「Data Protector コンポーネント」 (44 ページ) を参照してください。

   [Next] をクリックします。

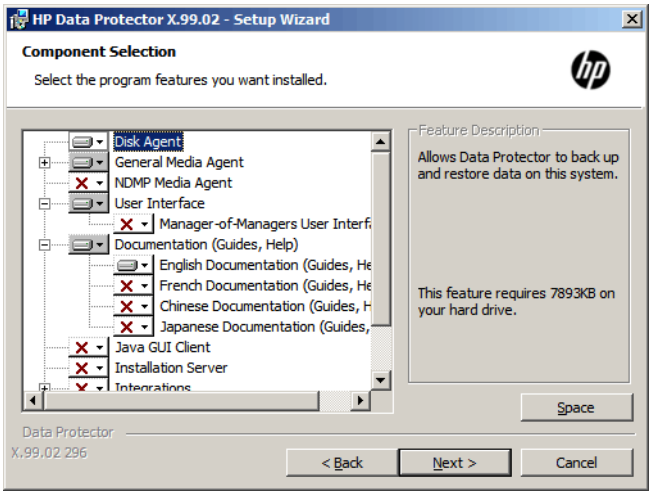
8. Data Protector がシステムで Windows ファイアウォールを検出した場合、[Windows Firewall configuration] ページが表示されます。Data Protector セットアップにより、必要なすべての Data Protector 実行可能ファイルが登録されます。デフォルトでは、**[Initially, enable newly registered Data Protector binaries to open ports as needed]** オプションが選択されています。この時点で、Data Protector によってポートがオー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。

   自動生成されるのはインバウンドファイアウォールルールのみであり、アウトバウンドファイアウォールルールは手動で作成する必要があるので注意してください。必要なポート範囲については、『HP Data Protector ヘルプ』の索引「ファイアウォールのサポート」で表示される内容を参照してください。

   [Next] をクリックします。

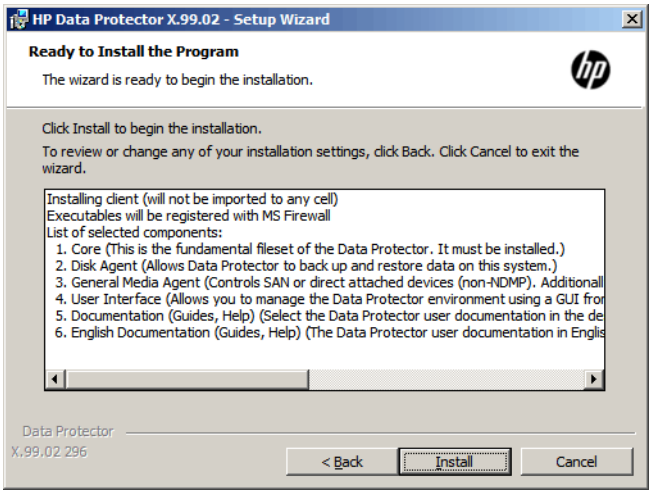
9. コンポーネント選択サマリーページが表示されます。**[Install]** をクリックして、選択したコンポーネントをインストールします。

図 15 コンポーネント選択サマリーページ



10. インストールステータスのページが表示されます。**[Next]** をクリックします。

図 16 インストールサマリーページ



11. ユーザーインタフェースコンポーネントをインストールした場合に、セットアップ直後に Data Protector GUI を使用して操作を開始するには **[Data Protector GUI** の起動**]** を選択します。

    英語版ドキュメント（ガイド、ヘルプ）コンポーネントをアップグレードしたか、または新しくインストールした場合に、セットアップ直後に『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を表示するには、**[Open the Product Announcements, Software Notes, and References]** 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)。「Windows システム上の未使用の SCSI ターゲット ID の取得」 (245 ページ) 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://support.openview.hp.com/selfsolve/manuals を参照してください。

3. コンピューターの電源を切り、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ー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ーがロードされている場合。

     ```
     HP:C1533A
     tape3:0:4:0
     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、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ー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ーをロードまたはアンロードする方法は、「Windows システムでのテープドライバーおよびロボティクスドライバーの使用」(233 ページ)を参照してください。デバイスファイル名の作成の詳細は、「Windows システム上でのデバイスファイル (SCSI アドレス) の作成」(234 ページ)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。構成タスクに関する情報については、『HP Data Protector ヘルプ』の索引「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。" バックアップデバイスの構成 "

HP-UX クライアントのインストール

HP-UX クライアントのインストールは、UNIX 用インストールサーバーを使用したリモートインストール、または UNIX インストール DVD-ROM (HP-UX または Linux 用) を使用したローカルインストールが可能です。

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、「Data Protector コンポーネント」(44 ページ)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、プロセッサー、および Data Protector コンポーネントについては、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。
- この時点で、Cell Manager および UNIX 用のインストールサーバー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。インストールが完了していない場合は、「Data Protector Cell Manager およびインストールサーバーのインストール」 (26 ページ) を参照してください。
- インストールを実行するには、**root** ユーザーによるアクセスか、または **root** ユーザーの権限付きのアカウントが必要です。

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ー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の詳細は、「リモートインストール」 (70 ページ) 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ー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。

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ーがインストールされていない場合、UNIX 用インストール DVD-ROM (HP-UNIX または Linux 用) 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。詳しい手順は、「UNIX および Mac OS X システムのローカルインストール」 (76 ページ) 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。「セルへのクライアントのインポート 」 (129 ページ) を参照してください。

クラスター対応クライアント

クラスター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。詳細は、「クラスター対応クライアントのインストール」 (116 ページ) を参照してください。

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。カーネルを手動でビルドする方法の詳細は、「HP-UX システム上の SCSI ロボティクス構成」 (235 ページ) 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構成をビルドするには、以下の手順に従ってください。

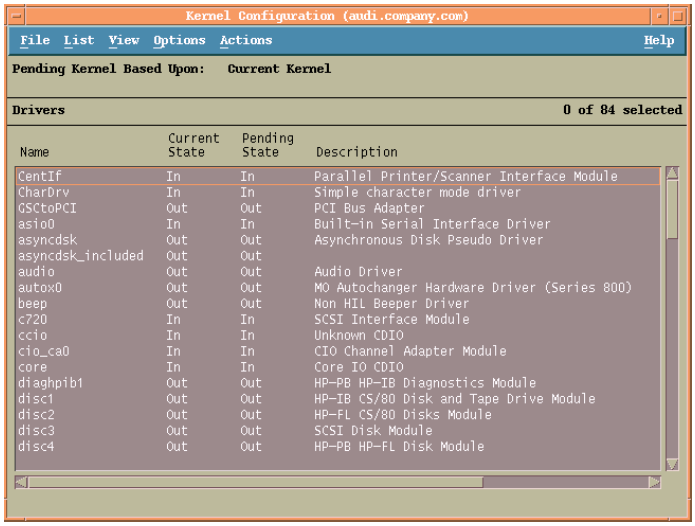
1. `root` ユーザーとしてログインし、端末を開いて `sam` と入力します。
2. **[System Administration Manager]** ウィンドウで **[Kernel Configuration]** と **[Drivers]** を順にダブルクリックします。
3. **[Kernel Configuration]** ウィンドウで、以下の条件が満たされていることを確認します。
   - 使用するデバイスのドライバーがインストール済みドライバーのリストに含まれていること。「[Kernel Configuration] ウィンドウ」 (53 ページ) を参照してください。目

的のドライバー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。たとえば、次のものが必要です。

- テープデバイスにはテープデバイスドライバーが必要です。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ー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 ドライバーは DLT や LTO などの汎用的な SCSI テープドライブで使用され、tape2 ドライバーは DDS デバイスで使用されます。
- 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ー (sctl または spt) か、オートチェンジャロボティクスドライバー (schgr) が必要です。

  詳細は、「HP-UX システム上の SCSI ロボティクス構成」 (235 ページ) を参照してください。

図 17 [Kernel Configuration] ウィンドウ



- **[Current State]** 列でドライバーのステータスが **[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。
  1. リスト内のドライバーを選択します。**[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 **[In]** に設定されている各ドライバーに対して繰り返します。
  2. **[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。

必要なドライバー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ーに接続してください。

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、「HP-UX システム上の未使用の SCSI アドレスの取得」 (240 ページ) 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://support.openview.hp.com/selfsolve/manuals を参照してください。
3. デバイスをコンピューターに接続し、デバイスとコンピューター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。「HP-UX システム上のデバイスファイルの作成」 (238 ページ) を参照してください。

インストール手順が完了し、バックアップデバイスが正しくシステムに接続されたら、『HP Data Protector ヘルプ』の索引「構成、バックアップデバイス」を参照して、デバイスおよびメディアプールまたは Data Protector のその他の構成タスクの詳細を確認してください。

Solaris 用クライアントのインストール

Solaris クライアントのインストールは、UNIX 用インストールサーバーを使用したリモートインストール、または UNIX インストール DVD-ROM (HP-UX または Linux 用) を使用したローカルインストールが可能です。

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、「Data Protector コンポーネント」 (44 ページ) 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、および Data Protector コンポーネントについては、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。
- この時点で、Cell Manager および UNIX 用のインストールサーバー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。詳しい手順は、「Data Protector Cell Manager およびインストールサーバーのインストール」 (26 ページ) 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。

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ー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の詳細は、「リモートインストール」 (70 ページ) 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をインストールする場合は、コンポーネントを使用する前に環境変数を更新する必要があります。詳細は、「環境変数の設定」 (31 ページ) 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。

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。

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ーがインストールされていない場合、UNIX 用インストール DVD-ROM (HP-UNIX または Linux 用) 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。詳しい手順は、「UNIX および Mac OS X システムのローカルインストール」(76 ページ) を参照してください。

クラスター対応クライアント

クラスター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。詳細は、「クラスター対応クライアントのインストール」(125 ページ) を参照してください。

インストール後の構成

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、使用するプラットフォームとデバイスの種類に応じて構成をチェックし、必要な変更作業を確認してください。

- パッチ適用済みの Solaris 9 または Solaris 10 システム環境の場合、テープデバイスドライバーはデフォルトでデバイスをサポートしている可能性があります。サポートの有無のチェックには、`strings` コマンドを実行します。

  たとえば、追加で構成作業を行わずに HP DAT-72 デバイスが使用可能かどうかをチェックするには、次のコマンドを実行します。

  Solaris (SPARC) システムの場合:

  ```
  strings /kernel/drv/sparcv9/st | grep HP
  ```

  Solaris (x86、x64) システムの場合:

  ```
  strings /kernel/drv/st | grep HP
  ```

  コマンド出力を確認します。デバイスが存在する場合、追加の手順は必要ありません。存在しない場合、次の手順を実行します。

- 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に記述してください。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す。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。

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.templ` 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。

- 使用したい各テープドライブについて、`/kernel/drv/st.conf` ファイルに次の行が存在することを確認し、必要に応じて追加します。*ID* プレースホルダーを、デバイスのアドレスで置換します。

  SCSI デバイス:

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

  ファイバチャネルデバイス:

```
name="st" parent="fp" target=ID
```

parent パラメーターの値は、テープデバイスによって異なる場合があります。詳細は、テープデバイスのマニュアルを参照してください。

- Solaris 9 以前のバージョンで SCSI エクスチェンジャーデバイスを制御する場合は、SCSI パススルードライバーを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ー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 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 ビット版 Solaris 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. /etc/devlink.tab ファイルに以下の行を追加します。

     重要: /etc/devlink.tab 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. 制御する各 SCSI エクスチェンジャーデバイスについて、/kernel/drv/sst.conf ファイルに次の行が含まれていることを確認し、必要に応じて挿入します。*ID* プレースホルダーを、デバイスのアドレスで置換します。

     SCSI デバイス:

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

     ファイバチャネルデバイス:

     ```
     name="sst" parent=”lpfc” class="scsi" target=ID lun=0;
     ```

     parent パラメーターの値は、テープデバイスによって異なる場合があります。詳細は、テープデバイスのマニュアルを参照してください。

  4. 以下のコマンドを入力して、システムにドライバーをインストールします。

     ```
     add_drv sst
     ```

  5. 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ー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、まず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 (Solaris (SPARC) 専用の手順)。

     ```
     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 デバイスを使用する準備として、次の例で示す手順を実行します。

a. `/kernel/drv/st.conf` を編集し、割り当てられた SCSI ポートを使用するためにデバイスパラメーターを設定します。詳細は、デバイス付属のドキュメントを参照してください。テープデバイスドライバーがデフォルトではデバイスをサポートしない場合のみ、`tape-config-list` パラメーターを変更します。

b. `/usr/kernel/drv/sgen.conf` 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 SCSI エクスチェンジ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;
```

- Solaris 10 (SPARC、x86、x64) で SCSI エクスチェンジデバイスを制御するには、付属の `sgen` ドライバーを構成してから SCSI デバイスをインストールします。以下の手順に従ってください。

1. `/kernel/drv/sgen.conf` ファイルを開きます。

   ファイルで `device-type-config-list` パラメーターが指定されている場合、その行にチェンジャーデバイスの参照を追加します。次に例を示します。

   ```
   device-type-config-list=”scanner”, "changer";
   ```

   パラメーターが定義されていない場合、次の行を追加します。

   ```
   device-type-config-list="changer";
   ```

2. 制御する SCSI エクスチェンジャーデバイスについて、`/kernel/drv/sgen.conf` ファイルに次の行が含まれていることを確認し、必要に応じて挿入します。*`ID`* プレースホルダーを、デバイスのアドレスで置換します。

   ```
   name="sgen" class="scsi" target=ID lun=0;
   ```

3. 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ー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、まず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 (SPARC システム専用の手順)。

   ```
   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 デバイスを使用する準備として、次の例で示す手順を実行します。

   a. `/kernel/drv/st.conf` を編集し、割り当てられた SCSI ポートを使用するためにデバイスパラメーターを設定します。詳細は、デバイス付属のドキュメントを参照してください。テープデバイスドライバーがデフォルトではデバイスをサポートしない場合のみ、`tape-config-list` パラメーターを変更します。

   b. `/kernel/drv/sgen.conf` 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 SCSI エクスチェンジドライブに関して以下のデータを`/kernel/drv/sgen.conf` ファイルに追加します。

   ```
   name="sgen" 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 (Solaris 9 以前のバージョン) または/kernel/drv/sgen.conf ファイル (Solaris 10) の変更が完了したら、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。

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、コンピューター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。

   サポート対象のデバイスの詳細は、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、テープドライバーは、未定義の状態となり、システムの再起動が必要になります。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. Solaris (SPARC) システムの場合、システムの電源を投入し、Stop-A キーを押して起動プロセスを中断します。
4. 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。
5. 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 9 以前のバージョン (特に 64 ビット版 Solaris の場合) では、SCSI 制御デバイス (ピッカー) へのリンクが自動生成されないことがあります。Solaris 10 では、このリンクは生成されません。このような場合、シンボリックリンクを作成し、/dev/rsst*Num* (*Num* は任意の数字) にデバイスファイルを追加します。以下に例を示します。

   sst の場合:

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

   sgen の場合:

   ```
   ln -s /devices/pci@1e,600000/QLGC,qla@3/sgen@8,2:changer /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 エクスチェンジャーデバイス (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/lbin/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/lbin/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、テープドライブには/dev/rmt/0h ではなく/dev/rmt/0cbn 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

インストール手順が完了し、バックアップデバイスを Solaris クライアントに正しく接続したら、バックアップデバイスやメディアプールの構成、その他構成タスクの追加情報について、『HP Data Protector ヘルプ』の索引「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のインストールは、UNIX 用インストールサーバーを使用したリモートインストール、または UNIX インストール DVD-ROM (HP-UX または Linux 用) を使用したローカルインストールが可能です。

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、「Data Protector コンポーネント」 (44 ページ) 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、および Data Protector コンポーネントについては、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。
- この時点で、Cell Manager および UNIX 用のインストールサーバー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。詳しい手順は、「Data Protector Cell Manager およびインストールサーバーのインストール」 (26 ページ) を参照してください。
- 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。
- Data Protector コンポーネントを**リモートシステム**にインストールする場合は、リモートシステム上で以下の前提条件を満たしている必要があります。
  - inetd または xinetd サービスが実行またはセットアップされ、Data Protector が開始可能である。
  - ssh サービス、または ssh がインストールされていない場合には rexec サービスが有効になっている。
- カーネルが SCSI デバイス (SCSI support、SCSI tape support、SCSI generic support の各モジュール) をサポートしていることを確認してください。パラメーター Probe all LUNs on each SCSI device は省略可能です。

  Linux カーネルでの SCSI サポートの詳細は、お使いの Linux ディストリビューションまたは Linux カーネルのマニュアル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。「デフォルトの Data Protector Inet ポートの変更」 (227 ページ) を参照してください。

自動ディザスタリカバリ

自動ディザスタリカバリコンポーネントは、拡張自動ディザスタリカバリ (EADR) またはワンボタンディザスタリカバリ (OBDR) を使用して復旧を行うシステムと、EADR または OBDR で使用する DR CD ISO イメージを作成するシステム上にインストールする必要があります。

MC/ServiceGuard クラスター

MC/ServiceGuard クラスターの場合は、Data Protector エージェント (Disk Agent、Media Agent) を、共有ディスク上ではなく、**各クラスターノード** (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) はクラスター上で、クラスターの**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。

インストールサーバーのインストールにパッシブノードを使用できます。

Novell Open Enterprise Server (OES)

Novell OES システムの場合は、Data Protector によって OES 対応の Disk Agent が自動的にインストールされます。ただし、次のような Novell OES 固有の状況がいくつかあります。

- Novell OES を 32 ビット SUSE Linux Enterprise Server 9.0 (SLES) にインストールする場合は、Data Protector Linux クライアントをシステムにインストールした後に、Data Protector クライアントもアップグレードする必要があります。

  アップグレード処理中に、新しい Novell OES 対応 Disk Agent がクライアントシステムにリモートでインストールされます。

- Novell OES コンポーネントを SLES から削除する場合は、Data Protector クライアントを再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

Linux クライアントシステムは、UNIX 用のインストールサーバーから 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、「リモートインストール」 (70 ページ) 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。

リモートインストールの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` を編集します。`exec` サービスと `shell` サービスの定義を見つけ、これらの 2 つのサービスの定義に次の行を追加します。

   ```
   server_args = -h
   ```

   以下に例を示します。

   ```
   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 ファイルを作成して次のエントリを追加します。

   MyInstallationServerHostname root

   これにより、インストールサーバーから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、ステップ 2で示す 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 man ページを参照してください。問題が発生した場合は、「UNIX および Mac OS X システムのローカルインストール」(76 ページ) 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ーがインストールされていない場合、UNIX 用インストール DVD-ROM (HP-UNIX または Linux 用) 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。詳しい手順は、「UNIX および Mac OS X システムのローカルインストール」(76 ページ) 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://support.openview.hp.com/selfsolve/manuals を参照してください。
3. デバイスをコンピューターに接続し、デバイスとコンピューター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 Enterprise Linux システムの場合は、コンピューター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 が起動します。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
   ```

   たとえば、次のように入力してください。

   ```
   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は sga、sgb、sgc、... sgh で、ドライブ用のデバイスファイルは st0、st1、... st7 です。

この次に行う作業

インストール手順が完了し、バックアップデバイスが正しく Linux クライアントシステムに接続されたら、『HP Data Protector ヘルプ』の索引「構成、バックアップデバイス」を参照して、バックアップデバイスおよびメディアプール、またはその他の構成タスクの詳細を確認してください。

ESX Server クライアントのインストール

ESX Server は、Modified Linux オペレーティングシステムです。ESX Server システムに Data Protector コンポーネントをインストールする方法については、「Linux クライアントのインストール」 (60 ページ) を参照してください。

Mac OS X クライアントのインストール

Mac OS X クライアントのインストールは、UNIX 用インストールサーバーを使用したリモートインストール、または UNIX インストール DVD-ROM (HP-UX または Linux 用) を使用したローカルインストールが可能です。

Disk Agent(DA) のみがサポートされています。

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 OS バージョン、および Data Protector コンポーネントについては、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。
- この時点で、Cell Manager および UNIX 用のインストールサーバー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。詳しい手順は、「Data Protector Cell Manager およびインストールサーバーのインストール」 (26 ページ) を参照してください。

推奨事項

- デフォルトのブロックサイズを増やす場合は、カーネルパラメーター kern.sysv.shmmax(共有メモリーセグメントの最大サイズ) を 32MB に設定することをお勧めします。

リモートインストール

Mac OS X 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ーからクライアン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の詳細は、「リモートインストール」 (70 ページ) 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ーがインストールされていない場合、UNIX 用インストール DVD-ROM (HP-UNIX または Linux 用) 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。詳しい手順は、「UNIX および Mac OS X システムのローカルインストール」(76 ページ) 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。

IBM AIX クライアントのインストール

AIX クライアントのインストールは、UNIX 用インストールサーバーを使用したリモートインストール、または UNIX インストール DVD-ROM (HP-UX または Linux 用) を使用したローカルインストールが可能です。

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、「Data Protector コンポーネント」(44 ページ) 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、および Data Protector コンポーネントについては、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。
- この時点で、Cell Manager および UNIX 用のインストールサーバー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。詳しい手順は、「Data Protector Cell Manager およびインストールサーバーのインストール」(26 ページ) 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。

IBM HACMP Cluster

IBM High Availability Cluster Multi-processing environment for AIX の場合、すべてのクラスターノードに Data Protector `Disk Agent` コンポーネントをインストールします。クラスター対応アプリケーションデータベースがインストールされたクラスター環境に Data Protector をインストールする方法については、「Data Protector 統合クライアントのインストール」(84 ページ) を参照してください。

インストールが終了したら、クラスターノードと**仮想サーバー** (仮想環境パッケージの IP アドレス) を Data Protector セルにインポートします。

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ー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の詳細は、「リモートインストール」(70 ページ) 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ーがインストールされていない場合、UNIX 用インストール DVD-ROM (HP-UNIX または Linux 用) 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。詳しい手順は、「UNIX および Mac OS X システムのローカルインストール」(76 ページ) 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. コンピューター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://support.openview.hp.com/selfsolve/manuals を参照してください。
2. コンピューターの電源を投入し、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: 巻き戻しなし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

インストール手順が完了し、バックアップデバイスが正しく AIX システムに接続されたら、『HP Data Protector ヘルプ』の索引「構成、バックアップデバイス」を参照して、バックアップデバイス、メディアプール、または Data Protector のその他の構成タスクの詳細を確認してください。

HP OpenVMS クライアントのインストール

OpenVMS クライアントのインストール手順は、サポートされている OpenVMS システムでローカルに行う必要があります。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、およびそのユーザーインタフェース (コマンドラインインタフェースのみ) は、OpenVMS 7.3-2/IA64 8.2-1 を実行しているシステムにインストールできます。また、Oracle Integration コンポーネントは、OpenVMS 7.3-2 以上を実行している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、「Data Protector コンポーネント」(44 ページ) を参照してください。

サポート対象デバイス、OpenVMS プラットフォームのバージョン、制限事項、既知の問題および回避策の詳細は、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。

OpenVMS 固有の詳細情報については、`SYS$COMMON:[SYSHLP]DPA0800.RELEASE_NOTES` など、OpenVMS のデフォルトのヘルプドキュメントのディレクトリにある『OpenVMS リリースノート』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、以下を確認してください。

- HP 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。

- `SYS$MANAGER:UTC$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。
- HP OpenVMS クライアントのインストールパッケージを収録した Data Protector のインストール 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 インストールは、インストールサーバーの機能の一部ではないこと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、ステップ 2に進みます。PCSI インストールファイルを取得するには、OpenVMS サーバーにインストール DVD-ROM をマウントし、ターゲットロケーションにコピーしてください。Windows システムから PCSI ファイルを FTP で取得することもできます。
2. 以下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 A08.00-xx
   Layered Product Do you want to continue?[YES]
   ```
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。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 IA64VMS DP A08.00-xx:HP OpenVMS IA64 Data Protector V8.00
   COPYRIGHT HEWLETT-PACKARD COMPANY 2013
   Do you want the defaults for all options?[YES] NO
   Do you wish to install Disk Agent for this client node?
   [YES] YES
   Do you wish to install Media Agent for this client node?
   [YES] YES
   Do you wish to install Command Language Interface for this client
   node?
   [YES] YES
   Do you wish to install Oracle Integration Agent for this client
   node?
   [YES] YES
   Do you want to review the options?
   [NO] YES
   ```

```
HP IA64VMS DP X08.00-xx:HP OpenVMS IA64 Data Protector V8.00
[Installed]

Do you wish to install Disk Agent for this client node?

YES

Do you wish to install Media Agent for this client node?

YES

Do you wish to install Command Language Interface for this client
node?

YES

Do you wish to install Oracle Integration Agent for this client
node?

[YES] 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]
```

このディレクトリには、OpenVMS クライアントに常に表示される 4 つのファイルと、CLI オプションを選択した場合にのみ存在する 5 つ目のファイルがあります。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。
- `SYS$STARTUP:OMNI$SYSTARTUP.COM`: `OMNI$ROOT` の論理名を定義するためのコマンドプロシジャです。このクライアントに必要な他の論理名も、このコマンドプロシジャに追加できます。
- `SYS$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ーに対して、`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. `SYS$MANAGER:SYSTARTUP_VMS.COM` に以下の行を挿入します。

   ```
   @sys$startup:omni$startup.com
   ```

6. `SYS$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 の可能なすべての TCP/IP のエイリアスに接続できることを確認してください。
8. 「セルへのクライアントのインポート」(129 ページ) の手順に従って、Data Protector の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 の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。

注記: OpenVMS 8.3 以降では、Data Protector インストールで次のメッセージが表示されます。

```
%PCSI-I-CANNOTVAL, cannot validate [PATH]HP-AXPVMS-DP-A0800
-XXX-1.PCSI;1 -PCSI-I-NOTSIGNED, product kit
is not signed and therefore has no manifest file
```

警告が表示されないようにするには、製品のインストールコマンドに /OPTION=NOVALIDATE_KIT を指定します。

クラスター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。

クラスターの TCP/IP エイリアス名を使用する場合で、クラスター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、クラスター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 の Data Protector Disk Agent は、マウントされた FILES-11 ODS-2 および ODS-5 のディスクボリュームをサポートしています。OpenVMS Disk Agent を構成する必要はありません。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仕様は、ODS-5 ディスクに常駐するファイル以外は大文字小文字を区別しません。

例

OpenVMS のファイル仕様

```
$1$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: 暗黙に使用される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、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 とハードウェアマニュアルをガイドとして使用して、OpenVMS システム上のデバイスを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
```

内容は以下のとおりです。

- `c` = K (直接接続型の SCSI テープライブラリの場合)
- `a` = A、B、C、...(SCSI コントローラーのアダプターの文字)
- `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。

テープライブラリに接続された SAN の場合、SAN のガイドラインに従って SAN ドライブを構成すると、OpenVMS にテープドライブとロボットデバイス名が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 コントローラー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。

クラスターの Media Agent

クラスター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ー内で、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。`TZ89_A` を使用してノード B でバックアップを実行すると、Data Protector によりデータがノード B からノード A のデバイスに移動されます。`TZ89_B` を使用してノード B でバックアップを実行すると、OpenVMS MSCP サーバーによりデータがノード B からノード A のデバイスに移動されます。

注記: クラスター内の MSCP により機能するテープデバイスで、HSx コントローラーまたはファイバーチャネルを介して接続されるすべてのテープデバイスの場合、『HP Data Protector ヘルプ』の索引「SAN、デバイスの構成」の SAN 構成のガイドラインに従ってください。

コマンドラインインタフェース

OpenVMS で Data Protector のコマンドラインインタフェースを使用する前に、以下のように CLI コマンドのセットアップ手順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 コマンドの説明については、『HP 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 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" -nlsset 159 -nlsId 12172 -flags
0x7 -ntpath "" -uxpath "" -version 8.00
```

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

その他の構成タスクに関する情報については、『HP Data Protector ヘルプ』の索引 "HP OpenVMS" で表示される内容を参照してください。

リモートインストール

この項では、インストールサーバーを使って 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。

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。

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、「Data Protector クライアントシステムのインストール 」 (42 ページ) および 「統合ソフトウェアのインストール」 (43 ページ) に示すとおりです。
- サポート対象プラットフォーム、Data Protector コンポーネント、ディスクスペース要件については、http://support.openview.hp.com/selfsolve/manuals と『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。

- 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ー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。
- クリーンリモートインストールの場合、Windows 用のインストールサーバーは、ネットワーク上の他のコンピューター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。

推奨事項

- **UNIX システムの場合:** セキュリティ上の理由から、Data Protector リモートインストールにはセキュアシェルを使用することをお勧めします。セキュアシェルを使用できない場合は、従来の UNIX ツールである `rsh` および `rexec` が Data Protector のリモートインストールで自動的に使用されます。

  セキュアシェルを使用するには、クライアントおよびインストールサーバーの両方に OpenSSH をインストールしてセットアップします。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ー上に keychain をインストールしてセットアップします。「セキュアシェルを使用したリモートインストール」 (71 ページ) 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ーがある場合は、それ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。

セキュアシェルを使用した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ー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ー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 システムでのみサポートされています。

OpenSSH のセットアップ

クライアントおよびインストールサーバーの両方に OpenSSH をインストールしてセットアップします。

1. OpenSSH がシステムにインストールされていることを確認します。詳細は、お使いのオペレーティングシステムまたはディストリビューションのマニュアルを参照してください。

   OpenSSH パッケージがお使いの OS ディストリビューションに含まれていない場合は、OpenSSH を http://www.openssh.org からダウンロードして、Data Protector クライアントとインストールサーバー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場所は `/opt/ssh` です。

2. インストールサーバー上で、`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ー上に維持します。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

バー上に 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「keychain のセットアップ」 (72 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 パラメーターの設定を変更します。

1. **インストールサーバーの場合:**

   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。

2. **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) によって使用されます。

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. 次のコマンドを実行して、インストールサーバー上の $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ー上で、omnirc オプション OB2_SSH_ENABLED を 1 に設定します。omnirc オプションの詳細は、『HP Data Protector トラブルシューティングガイド』を参照してください。

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. http://www.gentoo.org/proj/en/keychain/index.xml からインストールサーバーに keychain を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 および Solaris システムの場合:

   keychain_install_directory/keychain-*keychain_version*/keychain $HOME/.ssh/*private_key*

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

   Linux システムの場合:

   /usr/bin/keychain $HOME/.ssh/*private_key*

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

3. インストールサーバー上で、omnirc オプション `OB2_ENCRYPT_PVT_KEY` を `1` に設定します。`omnirc` オプションの詳細は、『HP Data Protector トラブルシューティングガイド』を参照してください。

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 (「クライアントのセルへの追加」 (73 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ーについては、『HP 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、警告メッセージが表示されます。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。

クライアントのセルへの追加

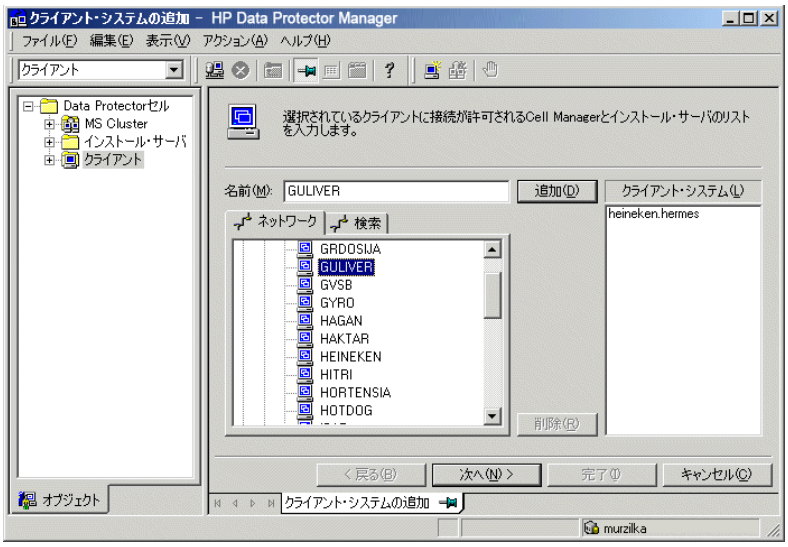
クライアントのセルへの追加

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. **[スタート]** → **[プログラム]** → **[HP Data Protector]** → **[Data Protector Manager]** を順にクリックして、Data Protector GUI を起動します。

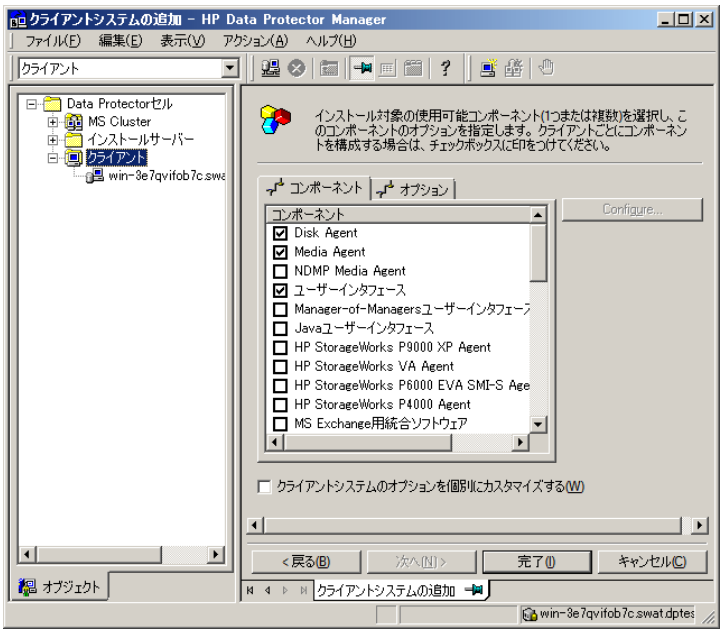
   Data Protector のグラフィカルユーザーインタフェースの詳細については、「Data Protector グラフィカルユーザーインタフェース」 (24 ページ) と『HP Data Protector ヘルプ』を参照してください。
2. [Data Protector Manager] で **[クライアント]** コンテキストを選択します。
3. Scoping ペインで **[クライアント]** を右クリックし、**[クライアントの追加]** をクリックします。
4. 複数のインストールサーバーが構成されている場合は、インストールするクライアントのプラットフォーム (UNIX または 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ーを選択します。**[次へ]** をクリックします。
5. クライアントの名前を直接入力するか、Windows GUI を使用している場合はインストールするクライアントを検索することもできます (「クライアントの選択」 (73 ページ) を参照してください)。**[次へ]** をクリックします。

図 18 クライアントの選択



6. 「コンポーネントの選択 」 (74 ページ) 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。「Data Protector コンポーネント」 (44 ページ) を参照してください。

図 19 コンポーネントの選択



インストール用のデフォルトアカウントとターゲットディレクトリ (Windows 上のみ) を変更するには、[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、[各クライアントのコンポーネントを個別に指定] 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。

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へのアクセスに必要なデータ (ユーザー名、パスワード。Windows の場合はドメイン) を入力し、**[OK]** をクリックします。

システムに Data Protector ソフトウェアがインストールされ、Data Protector セルに追加されるとすぐに、Data Protector クライアントとなります。

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、『HP Data Protector 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が完了すると、GUI を使用して **[Actions]** および **[Restart Failed Clients]** をクリックすることにより、失敗したインストール手順を再開できます。インストールが再度失敗する場合は、「インストールのトラブルシューティングとアップグレード」 (205 ページ) 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と Cell Manager には、追加の Data Protector ソフトウェアコンポーネントをインストールできます。コンポーネントは、リモートまたはローカルに追加できます。ローカルインストールについては、「Data Protector ソフトウェアコンポーネントの変更」 (156 ページ) を参照してください。

MC/ServiceGuard クライアント

MC/ServiceGuard クラスター環境では、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ーが利用可能である必要があります。

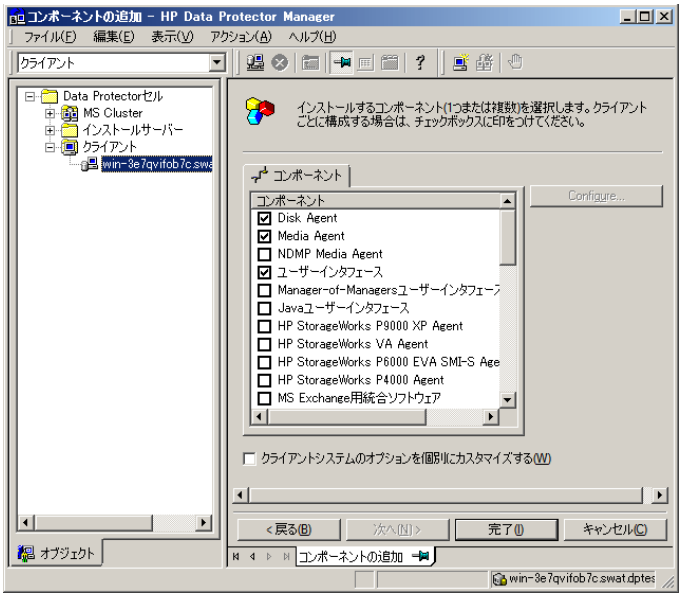
Data Protector セル内のクライアントに Data Protector ソフトウェアを配布するには、以下の手順に従ってください。

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 ペインで [クライアント] を展開し、クライアントを右クリックし、[コンポーネントの追加] をクリックします。
3. 複数のインストールサーバー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ーを選択します。[次へ] をクリックします。
4. 「クライアントの選択」 (75 ページ) に示すように、コンポーネントをインストールするクライアントを選択します。[次へ] をクリックします。

図 20 クライアントの選択

5. 「コンポーネントの選択」 (76 ページ) で示すように、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。「Data Protector コンポーネント」 (44 ページ) を参照してください。

図 21 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、[各クライアントのコンポーネントを個別に指定] 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。

UNIX および Mac OS X システム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ーがインストールされていない場合、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、UNIX 用インストール DVD-ROM (HP-UX または Linux 用) 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、「Data Protector コンポーネント」 (44 ページ) 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、プロセッサー、および Data Protector コンポーネントについては、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。
- 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。
- インストールには、POSIX シェル (`sh`) が必要です。

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 および Mac OS X 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 (HP-UX または Linux 用) をドライブに挿入してマウントします。

   DVD-ROM ファイルシステムは Rock Ridge 拡張を使用します。

2. *MountPoint*/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*]

   内容は以下のとおりです。

   - *directory* には、インストール DVD-ROM 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 またはインストールサーバー上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。

   - *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 パラメーターを指定しなければ、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: クライアントのアップグレードでは、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コンポーネントと同じコンポーネントモデル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。コンポーネントの説明については、「Data Protector コンポーネント」 (44 ページ) を参照してください。

表 7 Data Protector 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
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
oracle8	Oracle 用統合ソフトウェア
vmware	VMware 用統合ソフトウェア (レガシー)
vepa	仮想環境統合ソフトウェア
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 7 Data Protector 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
smisa	HP P6000/HP 3PAR SMI-S Agent
ssea	HP P9000 XP Agent
autodr	自動ディザスタリカバリ
docs	英語版マニュアル (ガイド、ヘルプ)
fra_ls	フランス語版マニュアル (ガイド、ヘルプ)
jpn_ls	日本語版マニュアル (ガイド、ヘルプ)
chs_ls	簡体字中国語版マニュアル (ガイド、ヘルプ)

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 用統合ソフトウェアの各コンポーネントを、Cell Manager computer.company.com を使用してセルに自動的にインポートされるクライアントにインストールする方法を示しています。

```
./omnisetup.sh -server computer.company.com -install da,ma,cc,informix
```

3. インストールが完了している場合や、クライアントが Data Protector セルにインポートされている場合は、そのことを示すメッセージが表示されます。

   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 をお使いのコンピューターにコピーして、UNIX および Mac OS X クライアントのインストールまたはアップグレードをハードディスクから実行するには、少なくとも hpux/DP_DEPOT ディレクトリと LOCAL_INSTALL ディレクトリをコピーしてください。

注記: Linux デポではローカルインストールはサポートされません。Linux システムの場合も HP-UX デポのコピーが必要です。

たとえば、インストールパッケージを/var/dp80 にコピーする場合、ディレクトリは/var/dp62 のサブディレクトリでなければなりません。

```
# pwd
/var/dp80
# ls
DP_DEPOT
LOCAL_INSTALL
```

これをハードディスクにコピーした後、LOCAL_INSTALL ディレクトリに変更してから、次のコマンドを実行します。

```
omnisetup.sh [-server name] [-install component_list]
```

たとえば、次のように入力します。

```
./omnisetup.sh -install da
```

ディスク容量の制約などにより、DP_DEPOT ディレクトリを別のディレクトリにコピーした場合は、-source オプションも必要になります。

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。詳しい手順は、「セルへのクライアントのインポート」(129 ページ)を参照してください。追加の構成タスクの詳細は、『HP Data Protector ヘルプ』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、専用の ADIC/GRAU と StorageTek ACS ライブラリが用意されています。ポリシーは、Data Protector バックアップデバイスとしての ADIC/GRAU ライブラリ または StorageTek ACS ライブラリの構成に使用されます。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ーに接続される構成を意味します。

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、「Data Protector ライセンス」(183 ページ)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 または STK ライブラリの詳細は、http://support.openview.hp.com/selfsolve/manuals を参照してください。

システムにバックアップデバイスを物理的に接続する方法については、「HP-UX クライアントのインストール」(51 ページ)と、ADIC/GRAU または StorageTek ライブラリ付属のマニュアルを参照してください。

サポート対象 Windows システムにバックアップデバイスを物理的に接続する方法については、「Windows 用クライアントのインストール」(47 ページ)と、ADIC/GRAU または StorageTek ライブラリ付属のマニュアルを参照してください。

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 サーバーが 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 サーバーコンピューター上の 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. Data Protector Media Agent がインストールされ、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各クライアント上で、omnirc ファイルを編集して以下のオプションを設定します。

DAS_CLIENT	DAS サーバー上に定義される一意な GRAU クライアント名です。たとえば、クライアントの名前が “DP_C1” の場合、omnirc ファイルの該当する行は DAS_CLIENT=DP_C1 です。
DAS_SERVER	DAS サーバー名です。

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。割り当てポリシーのタイプ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 オプション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。「Data Protector Cell Manager およびインストールサーバーのインストール」 (26 ページ) を参照してください。
- DAS サーバー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 サーバーに送信されます。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 サーバーが 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は、1 つのメディアタイプのみ処理できます。挿入/取り出し領域のそれぞれに所属するメディアの種類を把握しておくことが重要です。このデータは、後で Data Protector ライブラリ用の挿入/取り出し領域を構成するときに必要になります。
  - 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、「HP-UX システムへのバックアップデバイスの接続」 (53 ページ) 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、「Windows システムへのバックアップデバイスの接続」 (50 ページ) 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。

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ーを使って、クライアントに Media Agent コンポーネントを配布します。「リモートインストール」 (70 ページ) 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` 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。

次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。

Windows システムの場合: *`Data_Protector_home`*`\bin\devbra -dev`

HP-UX システムの場合: `/opt/omni/lbin/devbra -dev`

AIX システムの場合: `/usr/omni/bin/devbra -dev`

ライブラリドライブが正しく接続されていると、ライブラリドライブ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 がインストールされ、ADIC/GRAU ライブラリが物理的にシステムに接続されたら、『HP Data Protector ヘルプ』索引「構成、バックアップデバイス」を参照して、その他の構成タスク (バックアップデバイスやメディアプールの構成など) の詳細を確認してください。

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。「Data Protector Cell Manager およびインストールサーバーのインストール」 (26 ページ) 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*ホスト名*。
  - 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、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、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 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、「HP-UX システムへのバックアップデバイスの接続」 (53 ページ) 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、「Windows システムへのバックアップデバイスの接続」 (50 ページ) を参照してください。
- Data Protector で使用するドライブがオンライン状態になっていることを確認します。ドライブがオンライン状態になっていない場合は、ACSLS ホスト上で次のコマンドを実行して状態を切り替えます。`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 がオンライン状態になっていない場合は、次のコマンドを実行して状態を切り替えます。

  ```
  vary cap cap_id online
  ```

  CAP が手動操作モードになっていない場合は、次のコマンドを実行してモードを切り替えます。

  ```
  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 システム用インストールサーバーを使って、クライアントに Media Agent コンポーネントを配布します。「リモートインストール」 (70 ページ) 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。詳細については、ACS のドキュメント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、システムを再起動すると、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` サービスをインストールし終えたら、`libattach\bin` ディレクトリがシステムパスに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. 次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、Solaris、および Linux 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が正しく接続されていると、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 アドレスがリストに表示されます。

この次に行う作業

Media Agent がインストールされ、StorageTek ライブラリが物理的にシステムに接続されたら、『HP Data Protector ヘルプ』の索引「構成、バックアップデバイス」を参照して、その他の構成タスク (バックアップデバイスやメディアプールの構成など) の詳細を確認してください。

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 Server や Microsoft Exchange Server 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 用統合ソフトウェアは、HP P6000 EVA ディスクアレイファミリ などのディスクアレイを使用してゼロダウンタイムバックアップおよびインスタントリカバリ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を実行しているシステムは、**統合クライアントと呼ばれ、**バックアップとデータの保存に ZDB ディスクアレイを使用するシステムは **ZDB 統合クライアントと呼ばれます。**これらのクライアントは、Windows や UNIX システム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、Microsoft Exchange Server データベースのバックアップには `MS Exchange` 用統合ソフトウェアコンポーネント、HP P6000 EVA ディスクアレイファミリ による ZDB および IR には `HP P6000/HP 3PAR 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、プロセッサー、および Data Protector コンポーネントについては、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。
- 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。ライセンスの詳細は「Data Protector 8.00 の製品構成とライセンス」 (199 ページ) 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ー (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。詳しい手順は、「Data Protector Cell Manager およびインストールサーバーのインストール」 (26 ページ) 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、「Data Protector コンポーネント」 (44 ページ) 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ー (Oracle Server や Microsoft 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。
  - ファイルシステムまたはディスクイメージのゼロダウンタイムバックアップを実行する。
  - 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 サーバーを介して 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。

統合ソフトウェアクライアントのインストールは、Windows 用または UNIX 用インストールサーバーを使用したリモートインストール、Windows または UNIX インストール DVD-ROM (HP-UX または Linux 用) を使用したローカルインストールが可能です。

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」 (87 ページ)
- 「Microsoft SQL Server クライアント」 (89 ページ)
- 「Microsoft SharePoint Server クライアント」 (89 ページ)
- 「Microsoft ボリュームシャドウコピーサービスクライアント」 (91 ページ)
- 「Sybase Server クライアント」 (91 ページ)
- 「Informix Server クライアント」 (91 ページ)
- 「SAP R/3 クライアント」 (92 ページ)
- 「SAP MaxDB クライアント」 (92 ページ)
- 「Oracle Server クライアント」 (92 ページ)
- 「IBM DB2 UDB クライアント」 (93 ページ)
- 「Lotus Notes/Domino Server クライアント」 (93 ページ)
- 「VMware クライアント」 (93 ページ)
- 「Microsoft Hyper-V クライアント」 (96 ページ)
- 「NDMP Server クライアント」 (97 ページ)
- 「HP P4000 SAN ソリューション クライアント」 (97 ページ)
- 「HP P6000 EVA ディスクアレイファミリ クライアント」 (97 ページ)
- 「HP P9000 XP ディスクアレイファミリ クライアント」 (102 ページ)
- 「HP 3PAR StoreServ Storage クライアント」 (107 ページ)
- 「EMC Symmetrix クライアント」 (108 ページ)

統合クライアントのインストールが完了したら、各クライアントの適切な環境変数にコマンドの場所を追加して、どのディレクトリからでも Data Protector コマンドを実行できるようにすることをお勧めします。Data Protector ドキュメントの手順は、変数値が追加されていることを前提とします。コマンドの場所については、『HP Data Protector Command Line Interface Reference』の `omniintro` のリファレンスページ、および `omniintro` のマンページを参照してください。

インストール後に Data Protector 統合クライアントを構成する場合は、『HP Data Protector インテグレーションガイド』、『HP Data Protector ゼロダウンタイムバックアップ管理者ガイド』、または『HP Data Protector ゼロダウンタイムバックアップインテグレーションガイド』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ー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の詳細は、「リモートインストール」 (70 ページ) 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。

ローカルインストール

ユーザー環境のオペレーティングシステム用のインストールサーバーがない場合は、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。詳しい手順は、

「Windows 用クライアントのインストール」 (47 ページ) または「UNIX および Mac OS X システムのローカルインストール」 (76 ページ) 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。「セルへのクライアントのインポート 」 (129 ページ) を参照してください。

クラスター対応統合ソフトウェアのインストール

Data Protector クラスター対応統合クライアントは、各クラスターノードで、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 P6000/HP 3PAR SMI-S Agent` など) をインストールしてください。

Data Protector Cell Manager には、クラスター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ー環境により、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ー化に関する項を参照してください。

- 「MC/ServiceGuard への Data Protector のインストール」 (116 ページ)
- 「Microsoft Cluster Server への Data Protector のインストール」 (117 ページ)
- 「Microsoft Hyper-V クラスターでの Data Protector のインストール」 (126 ページ)
- 「Veritas Cluster への Data Protector クライアントのインストール」 (125 ページ)
- 「Data Protector の IBM HACMP Cluster へのインストール」 (125 ページ)

クラスタリングの詳細については、『HP Data Protector ヘルプ』の索引「クラスター、MC/ServiceGuard」および『HP 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、『HP 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

Microsoft Exchange Server システムにインストールする必要がある Data Protector コンポーネントは、使用するバックアップおよび復元のソリューションによって異なります。次のソリューションから選択することができます。

- 「Data Protector Microsoft Exchange Server 2007 用統合ソフトウェア」 (87 ページ)
- 「Data Protector Microsoft Exchange Server 2010 用統合ソフトウェア」 (88 ページ)
- 「Data Protector Microsoft Exchange Server Single Mailbox 用統合ソフトウェア」 (88 ページ)
- 「Data Protector Microsoft ボリュームシャドウコピーサービス用統合ソフトウェア」 (88 ページ)
- 「Microsoft Exchange Server 向け Data Protector Granular Recovery Extension」 (89 ページ)

Data Protector Microsoft Exchange Server 2007 用統合ソフトウェア

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できるようにするには、Microsoft Exchange Server システムに `MS Exchange` 用統合ソフトウェアコンポーネントをインストールします。

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 用統合ソフトウェアコンポーネントの一部としてインストールされます。

Data Protector Microsoft Exchange Server 2010 用統合ソフトウェア

ここでは、Microsoft Exchange Server 環境が正しく動作していることが前提となります。

Microsoft Exchange Server 2010 データベースまたは Microsoft Exchange Server 2013 データベースをバックアップできるようにするには、すべての Microsoft Exchange Server システムに次の Data Protector コンポーネントをインストールします。

- MS Exchange Server 2010+ 用統合ソフトウェア
- MS ボリュームシャドウコピー用統合ソフトウェア
- 適切な Data Protector ディスクアレイエージェント (Microsoft Exchange Server データがディスクアレイに存在する場合)

注記: VSS トランスポータブルバックアップセッションでは、バックアップシステムに MS ボリュームシャドウコピー用統合ソフトウェアコンポーネントと適切な Data Protector ディスクアレイエージェントもインストールする必要があります。

DAG 環境では、DAG 仮想システム (ホスト) も Data Protector セルにインポートする必要があります。Data Protector セルにクライアントをインポートする方法については、『HP Data Protector ヘルプ』の索引「インポート、クライアントシステム」を参照してください。

注記:

- Data Protector の MS Exchange Server 2010 用統合ソフトウェアは VSS 技術に基づいているため、MS Exchange Server 2010+ 統合ソフトウェアコンポーネントのインストール時に、自動的に MS ボリュームシャドウコピー用統合ソフトウェアコンポーネントがインストールされます。MS ボリュームシャドウコピー用統合ソフトウェアコンポーネントがすでにインストールされている場合は、アップグレードされます。
- MS Exchange Server 2010+ 統合ソフトウェアコンポーネントをシステムから削除しても、MS ボリュームシャドウコピー用統合ソフトウェアコンポーネントは自動的に削除されません。MS Exchange Server 2010+ 統合ソフトウェア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 MS ボリュームシャドウコピー用統合ソフトウェアコンポーネントを削除することはできないので注意してください。

Data Protector Microsoft Exchange Server Single Mailbox 用統合ソフトウェア

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 のメールボックスフォルダーとパブリックフォルダーの項目をバックアップできるようにするには、Microsoft Exchange Server システムに MS Exchange 用統合ソフトウェアコンポーネントをインストールします。DAG 環境では、DAG の一部に含まれるすべての Microsoft Exchange Server システムにこのコンポーネントをインストールします。

Microsoft Exchange Server 2007 システムの場合、追加パッケージをインストールして、Data Protector Microsoft Exchange Single Mailbox 用統合ソフトウェアの機能を有効にする必要があります。パッケージは、Microsoft Exchange Server MAPI クライアントおよび Collaboration Data Objects (ExchangeMapiCdo.EXE) という名前で、Microsoft Web サイト http://www.microsoft.com/downloads/Search.aspx?DisplayLang=en から無料でダウンロードできます。

Data Protector Microsoft ボリュームシャドウコピーサービス用統合ソフトウェア

「Microsoft ボリュームシャドウコピーサービスクライアント」 (91 ページ) を参照してください。

Microsoft Exchange Server 向け Data Protector Granular Recovery Extension

Microsoft Exchange Server メールボックス項目を復元できるようにするには、Data Protector 拡張を使用します。Microsoft Exchange Server 環境の構成に応じて、対応する Data Protector コンポーネントを以下のシステムにインストールしてください。

- 単一の Microsoft Exchange Server システム: 本システム
- 複数の Microsoft Exchange Server システム: メールボックスサーバーロールが構成されている各 Exchange Server システム
- Microsoft Exchange Server Database Availability Group (DAG) 環境: DAG 内にある任意の Exchange Server システム

前提条件

- 選択した Microsoft Exchange Server システムに次のコンポーネントをインストールします。
  - Data Protector `MS Exchange Server 2010+` 統合ソフトウェアコンポーネント
  - Data Protector ユーザーインタフェースコンポーネント
  - Data Protector 以外の必要なコンポーネントすべて

    詳細は、『HP Data Protector Granular Recovery Extension User Guide for Microsoft Exchange Server』のインストールの章を参照してください。
- 選択した Microsoft Exchange Server システム上の TCP/IP ポート 60000 (デフォルト) を空きポートにしておきます。

Data Protector `MS Exchange Granular Recovery Extension` コンポーネントをローカルまたはリモートにインストールする手順は、『HP Data Protector ヘルプ』の索引キーワード「インストール、クライアントシステム」を参照してください。

Microsoft SQL Server 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できるようにするには、インストール手順で `MS SQL` 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 SharePoint Server クライアント

Microsoft SharePoint Server 環境にインストールする必要がある Data Protector コンポーネントは、使用するバックアップおよび復元のソリューションによって異なります。次のソリューションから選択することができます。

- 「Data Protector Microsoft SharePoint Server 2007/2010 用統合ソフトウェア」 (89 ページ)
- 「Data Protector Microsoft SharePoint Server 2007/2010 VSS ベースソリューション」 (90 ページ)
- 「Data Protector Microsoft ボリュームシャドウコピーサービス用統合ソフトウェア」 (90 ページ)
- 「Microsoft SharePoint Server 向け Data Protector Granular Recovery Extension」 (90 ページ)

Data Protector Microsoft SharePoint Server 2007/2010 用統合ソフトウェア

ここでは、Microsoft SharePoint Server インスタンスと関連する Microsoft SQL Server インスタンスが正しく動作していることが前提となります。

Microsoft SharePoint Server オブジェクトをバックアップできるようにするには、次の Data Protector コンポーネントをインストールします。

- MS SharePoint 2007/2010 用統合ソフトウェア – Microsoft SharePoint Server システム上 (Microsoft SQL Server システムは除外されます)
- MS SQL 統合 – Microsoft SQL Server システム上

注記: システムに Microsoft SQL Server と Microsoft SharePoint Server の両方がインストールされている場合、システムに両方の Data Protector コンポーネントをインストールします。

Data Protector Microsoft SharePoint Server 2007/2010 VSS ベースソリューション

ここでは、Microsoft SharePoint Server インスタンスと関連する Microsoft SQL Server インスタンスが正しく動作していることが前提となります。

Microsoft SharePoint Server オブジェクトをバックアップできるようにするには、次の Data Protector コンポーネントをインストールします。

- MS ボリュームシャドウコピー用統合ソフトウェア - Microsoft SharePoint Server システムおよび Microsoft SQL Server システム上にインストールします。少なくとも次のサービスのいずれか 1 つが有効である必要があります。

  Microsoft Office SharePoint Server 2007:

  - Windows SharePoint Services Database
  - Windows SharePoint Service ヘルプ検索
  - Office SharePoint Server Search

  Microsoft SharePoint Server 2010:

  - SharePoint Foundation Database
  - SharePoint Foundation Help Search
  - SharePoint Server Search

- Data Protector ユーザーインタフェースコンポーネント - Data Protector MS ボリュームシャドウコピー用統合ソフトウェアコンポーネントがインストールされた Microsoft SharePoint Server の 1 つ、およびバックアップを構成し開始する予定の Microsoft SharePoint Server にインストールします。

Data Protector Microsoft ボリュームシャドウコピーサービス用統合ソフトウェア

「Microsoft ボリュームシャドウコピーサービスクライアント」 (91 ページ) を参照してください。

Microsoft SharePoint Server 向け Data Protector Granular Recovery Extension

ここでは、Microsoft SharePoint Server インスタンスと関連する Microsoft SQL Server インスタンスが正しく動作していることが前提となります。

Microsoft SharePoint Server の各オブジェクトを復元できるようにするには、Microsoft SharePoint Server の全体管理システムに MS SharePoint Granular Recovery Extension をインストールします。

- コンポーネントをローカルにインストールすると、Data Protector インストールウィザードに MS SharePoint GRE オプションのダイアログボックスが表示されます。ファーム管理者のユーザー名とパスワードを指定します。
- このコンポーネントをリモートにインストールするには、[MS SharePoint Granular Recovery Extension] を選択して [構成] をクリックし、MS SharePoint GRE オプションのダイアログボックスにファーム管理者ユーザー名とパスワードを指定します。

注記:

- Granular Recovery Extension をインストールできるのは、Microsoft SharePoint Server がインストールされているシステムのみです。
- Microsoft SharePoint Server データをバックアップするために必要な Data Protector コンポーネントも Microsoft SharePoint Server 環境にインストールされていることを確認します。

Microsoft ボリュームシャドウコピーサービスクライアント

VSS ライター、または VSS を使用したファイルシステムのみをバックアップするには、アプリケーションシステム (**ローカルバックアップ**の場合)、また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 (**トランスポータブルバックアップ**の場合) に、以下の Data Protector ソフトウェアをインストールします。

- `MS` ボリュームシャドウコピー用統合ソフトウェア
- ディスクアレイを (ハードウェアプロバイダーとともに) 使用する場合は、適切なディスクアレイエージェント: `HP P4000 Agent`、`HPP6000/HP 3PAR SMI-S Agent`、`HP P9000 XP Agent`、または `HP 3PAR VSS Agent`

VSS 用統合ソフトウェアをインストールした後、ディスクへの ZDB セッションおよびディスク + テープへの ZDB セッション (インスタントリカバリが有効なセッション) を実行する場合は、アプリケーションシステム上のソースボリュームを解決する必要があります。セルの VSS クライアントからの解決操作は、以下のように実行します。

```
omnidbvss -resolve {-apphost ApplicationSystem | -all}
```

ただし、アプリケーションシステムを解決しないか解決に失敗する場合、`omnirc` ファイル内で `OB2VSS_DISABLE_AUTO_RESOLVE` オプションが `0` (デフォルト) に設定されていれば、アプリケーションシステムが自動で解決されます。この場合、複製作成のバックアップ時間が長くなります。

詳細は、『HP Data Protector ゼロダウンタイムバックアップインテグレーションガイド』を参照してください。

Sybase Server 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。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。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。

IBM HACMP Cluster

If Informix Server が IBM HACMP クラスター環境にインストールされている場合は、すべてのクラスターノードに `Informix` 用統合ソフトウェアコンポーネントをインストールします。

SAP R/3 クライアント

前提条件

- 次の Oracle ソフトウェアがインストールされて構成されていることを確認します。
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net8 ソフトウェア
  - SQL*Plus
- 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
- `Disk Agent`

  Data Protector では、Disk Agent をバックアップサーバー (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 MaxDB クライアント

SAP MaxDB サーバーはすでに実行されているものとします。

SAP MaxDB 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 MaxDB 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 MaxDB 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 Server 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。

HP OpenVMS

HP OpenVMS では、Oracle 用統合ソフトウェアをインストールして構成した後 (『HP Data Protector インテグレーションガイド - Oracle、SAP』を参照)、`-key Oracle8` エントリが `OMNI$ROOT:[CONFIG.CLIENT]omni_info` に表示されていることを確認します。次に例を示します。

```
-key oracle8 -desc "Oracle Integration" -nlsset 159 -nlsId 12172 -flags 0x7 -ntpath "" -uxpath "" -version 8.00
```

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。

IBM DB2 UDB 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。

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。

Lotus Domino Cluster

Install the `Lotus` 用統合ソフトウェアおよび `Disk Agent` のコンポーネントを、バックアップに使用する Domino サーバーにインストールします。また、Domino データベースをこのデータベースの複製を含む他の Domino サーバーに復元する場合は、これらの Domino サーバーにもコンポーネントをインストールします。

VMware クライアント

VMware システムへのインストールが必要になる Data Protector コンポーネントは、使用するバックアップと復元ソリューションによって異なります。次のソリューションから選択することができます。

- 「Data Protector 仮想環境統合ソフトウェア」 (94 ページ)
- 「Data Protector VMware(レガシー) 用統合ソフトウェア」 (94 ページ)

- 「VMware vSphere 向け Data Protector Granular Recovery Extension」 (94 ページ)

Data Protector 仮想環境統合ソフトウェア

コンポーネントのインストール先となるシステムがすべて稼働状態であることが前提となります。

バックアップおよび復元セッションを制御するシステム (**バックアップホスト**) に次の Data Protector コンポーネントをインストールします。

- 仮想環境統合ソフトウェア
- `Disk Agent`

注記:

- `Disk Agent` コンポーネントをインストールすると、バックアップホスト上にあるディレクトリへの復元時に [参照] ボタンが表示されます。このコンポーネントをインストールしない場合は、ターゲットディレクトリを入力する必要があります。
- VMware Consolidated Backup (VCB) ソフトウェアがインストールされているクライアントは、バックアップホストとして使用**できません**。

Data Protector VMware(レガシー) 用統合ソフトウェア

VirtualCenter Server システム (存在する場合) および ESX Server システムはすでに実行されているものとします。VMware クライアントをインストールできるようにするには、最初に OpenSSH を設定します。詳細は、『HP Data Protector ヘルプ』の索引「インストール、クライアントシステム」を参照してください。

Data Protector `VMware` 用統合ソフトウェア（レガシー）コンポーネントを以下のクライアントにインストールします。

- 仮想マシンをバックアップするすべての ESX Server システム
- VirtualCenter システム (存在する場合)
- バックアッププロキシーシステム (**VCBfile** および **VCBimage** バックアップ方式を使用する場合)
- 仮想マシンのファイルシステムを復元する Windows システム (物理または仮想)

注記: Data Protector `VMware` 用統合ソフトウェア（レガシー）コンポーネントは、ESXi Server システムにはインストールできません。そのため、ESXi Server システム上で実行している仮想マシンに使用できないバックアップおよび復元機能が存在します。

クラスター

クラスター内の ESX Server システムまたは VirtualCenter システムの有無に関係なく、`VMware` 用統合ソフトウェア（レガシー）コンポーネントを両方のクラスターノードにインストールします。

VMware vSphere 向け Data Protector Granular Recovery Extension

Data Protector 仮想環境統合ソフトウェアが『HP Data Protector インテグレーションガイド - 仮想環境』の手順に従ってインストールおよび構成されていることと、復元を行う仮想マシンに VMware ツール 4.x 以降がインストールされていることが前提となります。

制限事項

- VMware vSphere 向け Data Protector Granular Recovery Extension では、リモートインストールのみがサポートされています。

マウントプロキシーシステム:

マウントプロキシーシステムに、次の Data Protector コンポーネントをリモートインストールします。

- 仮想環境統合ソフトウェア
- `VMware Granular Recovery Extension Agent`

インストール手順については、『HP Data Protector ヘルプ』の検索キーワード「インストール、クライアントシステム」を参照してください。

vCenter Server (VirtualCenter Server):

1. vCenter Server 上に Data Protector コンポーネントがインストールされていない場合は、このシステムに Data Protector `Disk Agent` コンポーネントをリモートインストールします。
2. vCenter Server を Data Protector セルに Data Protector クライアントとしてインポートします。詳細は、『HP Data Protector ヘルプ』の索引「インポート、クライアントシステム」を参照してください。

   以下の手順に従ってください。

   a. クライアントのインポートウィザードで、**[**種類**]** ドロップダウンリストから **[VMware vCenter]** を選択します。
   b. クライアントのインポートウィザードで、ログインの資格情報を次のように指定します。
      - **[**ポート**]**:VMware vSphere が使用しているポートを指定します。デフォルトでは、VMware vSphere はポート 443 を使用します。
      - **[**ユーザー名**]** および **[**パスワード**]**:以下の VMware vSphere アクセス権を持つオペレーティングシステムのユーザーアカウントを指定します。

        [Web サービスのルート**]**

        オプションで、Web サービスのエントリポイント URI を変更します。デフォルト:`/sdk`.

3. 以下の手順に従ってください。

   vCenter Server 5.1:

   - VMware Web Server の自動デプロイ機能を使用してインストールを実行するには、以下の手順に従います。
     a. VMware Web Server フォルダーの `installation_directory`(デフォルトパス: `C:\Program Files\VMware\Infrastructure\tomcat`) の `conf` サブフォルダーにある構成ファイル `server.xml` を開きます。
     b. ホストノードで、`autoDeploy` パラメーターの値を、`false` から `true` に変更します。
     c. [コントロールパネル] の [管理ツール] の下で、[サービス] を開き [VMware VirtualCenter Management Webservices] サービスを再起動します。
     d. `VMware Granular Extension Web Plug-In` コンポーネントを vCenter Server にリモートインストールします。
   - VMware Web Server の自動デプロイ機能を使用しないでインストールを実行するには、以下の手順に従います。
     a. `VMware Granular Extension Web Plug-In` コンポーネントを vCenter Server にリモートインストールします。

     VMware GRE インストール後スクリプトは失敗します。

b. VMware Web Server フォルダーの `installation_directory` の `webapps` サブフォルダーにある `VMWareGRE.war` ファイルを、`VMWareGRE` という名前 (大文字と小文字を区別する) の新しいディレクトリに抽出します。

c. `Data_Protector_home\bin` フォルダーから、次のコマンドを実行します。

```
perl -I "..\lib\perl" vmwgre_wp.pl -install
```

d. [コントロールパネル] の [管理ツール] の下で、[サービス] を開き [VMware VirtualCenter Management Webservices] サービスを再起動します。

vCenter Server の以前のバージョン:

Data Protector `VMware Granular Extension Web Plug-In` コンポーネントを vCenter Server にリモートインストールします。

Microsoft Hyper-V クライアント

Microsoft Hyper-V システムにインストールする必要がある Data Protector コンポーネントは、使用するバックアップおよび復元のソリューションによって異なります。次のソリューションから選択することができます。

- 「Data Protector 仮想環境統合ソフトウェア」 (94 ページ)
- 「Data Protector Microsoft ボリュームシャドウコピーサービス用統合ソフトウェア」 (96 ページ)

Data Protector 仮想環境統合ソフトウェア

コンポーネントのインストール先となるシステムがすべて稼働状態であることが前提となります。

バックアップおよび復元セッションを制御するシステム (**バックアップホスト**) に次の Data Protector コンポーネントをインストールします。

- 仮想環境統合ソフトウェア
- `MS` ボリュームシャドウコピー用統合ソフトウェア
- `Disk Agent`

注記: `Disk Agent` コンポーネントをインストールすると、バックアップホスト上にあるディレクトリへの復元時に [参照] ボタンが表示されます。このコンポーネントをインストールしない場合は、ターゲットディレクトリを入力する必要があります。

Microsoft Hyper-V システムに次の Data Protector コンポーネントをインストールします。

- `MS` ボリュームシャドウコピー用統合ソフトウェア

注記: Microsoft Hyper-V システムをクラスター内で構成する場合、クラスター対応クライアントとしてインストールする必要があります。詳細は、「Microsoft Hyper-V クラスターでの Data Protector のインストール」 (126 ページ) を参照してください。

バックアップシステム (VSS トランスポータブルバックアップ) に次の Data Protector コンポーネントをインストールします。

- `MS` ボリュームシャドウコピー用統合ソフトウェア

注記: **バックアップホスト**と**バックアップシステム**は、同じシステムではありません。

Data Protector Microsoft ボリュームシャドウコピーサービス用統合ソフトウェア

Microsoft Hyper-V システムにインストールする必要があるコンポーネントの詳細については、「Microsoft ボリュームシャドウコピーサービスクライアント」 (91 ページ) を参照してください。

NDMP Server 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。

HP P4000 SAN ソリューション クライアント

HP P4000 SAN ソリューション 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。

- `MS` ボリュームシャドウコピー用統合ソフトウェア
- `HP P4000 Agent`

ディスクとテープへの ZDB セッションまたはテープへの ZDB セッションを実行するには、次の Data Protector ソフトウェアコンポーネントをバックアップシステムに追加でインストールする必要があります。

- `General Media Agent`

HP P6000 EVA ディスクアレイファミリ クライアント

HP P6000 EVA ディスクアレイファミリ 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 P6000/HP 3PAR 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`

  `Disk Agent` コンポーネントは、ファイルシステムまたはディスクイメージのゼロダウンタイムバックアップを実行する場合に、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 バックアップ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。

重要: Microsoft Windows Server 2008 システムでは、Data Protector HP P6000 EVA ディスクアレイファミリ 用統合ソフトウェアを正常に動作させるために、2 つの Windows Server 2008 修正プログラムをインストールする必要があります。必要な修正プログラムのパッケージは、Microsoft の Web サイト http://support.microsoft.com/kb/952790 および http://support.microsoft.com/kb/971254 からダウンロードしてください。

この追加要件は、Windows Server 2008 R2 システムには適用されません。

クラスターへのインストール

HP P6000 EVA ディスクアレイファミリ 用統合ソフトウェアは、クラスター環境にインストールできます。サポート対象のクラスター構成とインストール要件の詳細は、『HP Data Protector ゼロダウンタイムバックアップ管理者ガイド』を参照してください。

他のアプリケーションの統合

HP P6000 EVA ディスクアレイファミリ 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 P6000 EVA ディスクアレイファミリ 用統合ソフトウェアは、Oracle Server、SAP R/3、Microsoft Exchange Server、Microsoft SQL Server、および Microsoft ボリュームシャドウコピーサービスと組み合わせてインストールできます。

HP P6000 EVA ディスクアレイファミリ と Oracle Server の統合

前提条件

- アプリケーションシステムと、バックアップセット ZDB の方法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 Net Services
  - 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ーを使用して、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。
- 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 Oracle 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 Oracle 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 Oracle 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` omnirc オプションを設定します。詳細は、『HP Data Protector ゼロダウンタイムバックアップインテグレーションガイド』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。

Oracle データファイルの一部がシンボリックリンクにインストールされている場合、バックアップシステムにもこれらのリンクを作成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。このカタログデータベースは、非ミラー化ディスク上の個々のシステムにインストールすることをお勧めします。リカバリカタログは、登録しない状態で残しておきます。データベースのインストール方法については、Oracle のマニュアルを参照してください。
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 P6000/HP 3PAR 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
   - `Oracle` 用統合ソフトウェア – 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

注記:

- バックアップシステムの Data Protector `Oracle` 用統合ソフトウェアコンポーネントは、バックアップセット ZDB 方式にのみ必要です。プロキシーコピー ZDB 方式の場合は必要ありません。
- RAC クラスター環境の場合、Oracle アプリケーションデータベースは、複数の Oracle インスタンスによりアクセスされます。そのため、Oracle インスタンスを実行するすべてのシステムに Data Protector `Oracle` 用統合ソフトウェアおよび `HP P6000/HP 3PAR SMI-S Agent` コンポーネントをインストールしてください。
- Oracle リカバリカタログデータベースが個々のシステムにインストールされている場合は、そこに Data Protector ソフトウェアコンポーネントをインストールする必要はありません。

HP P6000 EVA ディスクアレイファミリ と SAP R/3 の統合

前提条件

- アプリケーションシステムには、以下の Oracle ソフトウェアがインストールされている必要があります。
  - Oracle Enterprise Server (RDBMS)
  - Oracle Net Services
  - SQL*Plus
- SAP 準拠の ZDB セッション (アプリケーションシステムではなくバックアップシステムで開始された BRBACKUP) を実行する場合、バックアップシステムを構成します。詳細は、Oracle 用の SAP データベースガイド (スプリットミラーバックアップ、ソフトウェア構成) を参照してください。
- 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 のデータファイルは、ディスクアレイに配置する必要があります。
  - オンラインバックアップの場合、オンラインの REDO ログをディスクアレイに配置する必要はありません。オンライン SAP 対応 ZDB セッションは例外です。コントロールファイルはディスクアレイに配置する必要があります。
  - オフラインバックアップの場合、コントロールファイルとオンラインの REDO ログはディスクアレイに配置する必要があります。

- アーカイブされた REDO ログファイルは、ディスクアレイに配置する必要はありません。

Oracle 制御ファイル、オンライン REDO ログファイル、および Oracle SPFILE を、Oracle データファイルと**同じ** LVM ボリュームグループまたはソースボリュームに配置する場合、Data Protector の `ZDB_ORA_NO_CHECKCONF_IR`、`ZDB_ORA_INCLUDE_CF_OLF`、`ZDB_ORA_INCLUDE_SPF` `omnirc` オプションを設定します。設定しないと、ZDB–to–disk セッションと ZDB–to–disk+tape セッションを実行できません。詳細は、『HP Data Protector ゼロダウンタイムバックアップインテグレーションガイド』を参照してください。

注記: Oracle データファイルの一部がシンボリックリンクにインストールされている場合、バックアップシステムにもリンクを作成します。

UNIX システムの場合: Oracle データベースが raw パーティション (raw ディスクまたは raw 論理ボリューム) にインストールされている場合、アプリケーションシステムとバックアップシステムでのボリューム/ディスクグループ名が同じであることを確認してください。

- UNIX システムの場合、アプリケーションシステムに以下のユーザーが存在しているかどうかを確認します。
  - プライマリグループが `dba` の `ora`*`ORACLE_SID`*
  - UNIX グループ `sapsys` に属する*`ORACLE_SID`*`adm`
- 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)

    `c:\Oracle\`*`ORACLE_SID`*`\sys\exe\run` (Windows システム)

注記: インスタントリカバリを行う場合、sapbackup、saparch、および sapreorg の各ディレクトリが、Oracle データファイルとは異なるソースボリュームに存在していることを確認します。

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にない場合、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 PRO の場合、/usr/sap/PRO/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 orapro dba 4598276 Apr 17  2011 brarchive
-rwsr-xr-x   1 orapro dba 4750020 Apr 17  2011 brbackup
-rwsr-xr-x   1 orapro dba 4286707 Apr 17  2011 brconnect
-rwsr-xr-x   1 proadm sapsys 430467 Apr 17  2011
brrestore
-rwsr-xr-x   1 orapro dba 188629 Apr 17  2011 brtools
```

インストール手順

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、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 P6000/HP 3PAR SMI-S Agent
   - SAP R/3 用統合ソフトウェア
   - Disk Agent

注記: SAP R/3 Integration は、バックアップシステムで BRBACKUP が開始される SAP 対応 ZDB セッションを実行する場合にのみインストールする必要があります。

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。

HP P6000 EVA ディスクアレイファミリ と Microsoft Exchange Server の統合

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 P6000/HP 3PAR SMI-S Agent` – アプリケーションとバックアップシステムの両方
- `MS Exchange` 用統合ソフトウェア – アプリケーションシステムのみ

HP P6000 EVA ディスクアレイファミリ と Microsoft SQL Server の統合

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 P6000/HP 3PAR SMI-S Agent` – アプリケーションとバックアップシステムの両方
- `MS SQL` 用統合ソフトウェア – アプリケーションシステムのみ

HP P9000 XP ディスクアレイファミリ クライアント

HP P9000 XP ディスクアレイファミリ 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 P9000 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、ファイルシステムまたはディスクイメージのゼロダウンタイムバックアップを実行する場合に、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 バックアップ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。

重要: Microsoft Windows Server 2008 システムでは、Data Protector HP P9000 XP ディスクアレイファミリ 用統合ソフトウェアを正常に動作させるために、2 つの Windows Server 2008 修正プログラムをインストールする必要があります。必要な修正プログラムのパッケージは、Microsoft の Web サイト http://support.microsoft.com/kb/952790 および http://support.microsoft.com/kb/971254 からダウンロードしてください。

この追加要件は、Windows Server 2008 R2 システムには適用されません。

クラスターへのインストール

HP P9000 XP ディスクアレイファミリ 用統合ソフトウェアは、クラスター環境にインストールできます。サポート対象のクラスター構成とインストール要件の詳細は、『HP Data Protector ゼロダウンタイムバックアップ管理者ガイド』を参照してください。

他のアプリケーションの統合

HP P9000 XP ディスクアレイファミリ 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 P9000 XP ディスクアレイファミリ 用統合ソフトウェアは、Oracle Server、SAP R/3、Microsoft Exchange Server、Microsoft SQL Server、および Microsoft ボリュームシャドウコピーサービスと組み合わせてインストールできます。

HP P9000 XP ディスクアレイファミリ と Oracle Server の統合

前提条件

- アプリケーションシステムと、バックアップセット ZDB の方法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 Net Services
  - 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ーを使用して、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。
- アプリケーションシステム上の Oracle データファイルは、バックアップシステムにミラーリングされる HP P9000 XP ディスクアレイファミリ LDEV にインストールする必要があります。

  バックアップセット方法を使用する場合で、Oracle データファイルの一部がシンボリックリンクにインストールされている場合、バックアップシステムにもこれらのリンクを作成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 Oracle 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 Oracle 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 Oracle 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` omnirc オプションを設定します。詳細は、『HP Data Protector ゼロダウンタイムバックアップインテグレーションガイド』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。このカタログデータベースは、非ミラー化ディスク上の個々のシステムにインストールすることをお勧めします。リカバリカタログは、登録しない状態で残しておきます。データベースのインストール方法については、Oracle のマニュアルを参照してください。
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 P9000 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
   - `Oracle` 用統合ソフトウェア–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

注記:

- バックアップシステムの Data Protector `Oracle` 用統合ソフトウェアコンポーネントは、バックアップセット ZDB 方式にのみ必要です。プロキシーコピー ZDB 方式の場合は必要ありません。
- RAC クラスター環境の場合、Oracle アプリケーションデータベースは、複数の Oracle インスタンスによりアクセスされます。そのため、Oracle インスタンスを実行するすべてのシステムに Data Protector `Oracle` 用統合ソフトウェアおよび `HP P9000 XP Agent` コンポーネントをインストールしてください。
- Oracle リカバリカタログデータベースが個々のシステムにインストールされている場合は、そこに Data Protector ソフトウェアコンポーネントをインストールする必要はありません。

HP P9000 XP ディスクアレイファミリ と SAP R/3 の統合

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 Net Services
  - SQL*Plus
- SAP 準拠の ZDB セッション (アプリケーションシステムではなくバックアップシステムで開始された BRBACKUP) を実行する場合、バックアップシステムを構成します。詳細は、Oracle 用の SAP データベースガイド (スプリットミラーバックアップ、ソフトウェア構成) を参照してください。
- 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 のデータファイルは、ディスクアレイに配置する必要があります。
  - オンラインバックアップの場合、オンラインの REDO ログをディスクアレイに配置する必要はありません。オンライン SAP 対応 ZDB セッションは例外です。コントロールファイルはディスクアレイに配置する必要があります。
  - オフラインバックアップの場合、コントロールファイルとオンラインの REDO ログはディスクアレイに配置する必要があります。
  - アーカイブされた REDO ログファイルは、ディスクアレイに配置する必要はありません。

Oracle 制御ファイル、オンライン REDO ログファイル、および Oracle SPFILE を、Oracle データファイルと**同じ** LVM ボリュームグループまたはソースボリュームに配置する場合、Data Protector の `ZDB_ORA_NO_CHECKCONF_IR`、`ZDB_ORA_INCLUDE_CF_OLF`、`ZDB_ORA_INCLUDE_SPF omnirc` オプションを設定します。設定しないと、ZDB–to–disk セッションと ZDB–to–disk+tape セッションを実行できません。詳細は、『HP Data Protector ゼロダウンタイムバックアップインテグレーションガイド』を参照してください。

注記: Oracle データファイルの一部がシンボリックリンクにインストールされている場合、バックアップシステムにもリンクを作成します。

UNIX システムの場合: Oracle データベースが raw パーティション (raw ディスクまたは raw 論理ボリューム) にインストールされている場合、アプリケーションシステムとバックアップシステムでのボリューム/ディスクグループ名が同じであることを確認してください。

- UNIX システムの場合、アプリケーションシステムに以下のユーザーが存在しているかどうかを確認します。
  - プライマリグループが `dba` の `ora`*`ORACLE_SID`*
  - UNIX グループ `sapsys` に属する*`ORACLE_SID`*`adm`
- 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)

    `ORACLE_HOME``\database` (Windows システム) - Oracle および SAP R/3 プロファイル
  - *`ORACLE_HOME`*`/bin` (UNIX システム) または

    `ORACLE_HOME``\bin` (Windows システム) - Oracle バイナリ
  - *`SAPDATA_HOME`*`/sapbackup` (UNIX システム)

    `SAPDATA_HOME``\sapbackup` (Windows システム) -

    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)

    `SAPDATA_HOME``\saparch` (Windows システム) - 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)

    `SAPDATA_HOME``\sapreorg` (Windows システム)
  - *`SAPDATA_HOME`*`/sapcheck` (UNIX システム)

    `SAPDATA_HOME``\sapcheck` (Windows システム)
  - *`SAPDATA_HOME`*`/saptrace` (UNIX システム)

    `SAPDATA_HOME``\saptrace` (Windows システム)

- /usr/sap/*ORACLE_SID*/SYS/exe/run (UNIX システム)
  c:\Oracle*ORACLE_SID*\sys\exe\run (Windows システム)

注記: インスタントリカバリを行う場合、sapbackup、saparch、および sapreorg の各ディレクトリが、Oracle データファイルとは異なるソースボリュームに存在していることを確認します。

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にない場合、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 PRO の場合、/usr/sap/PRO/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 orapro dba 4598276 Apr 17  2011 brarchive
-rwsr-xr-x   1 orapro dba 4750020 Apr 17  2011 brbackup
-rwsr-xr-x   1 orapro dba 4286707 Apr 17  2011 brconnect
-rwsr-xr-x   1 proadm sapsys 430467 Apr 17  2011
brrestore
-rwsr-xr-x   1 orapro dba 188629 Apr 17  2011 brtools
```

インストール手順

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、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 P9000 XP Agent
   - SAP R/3 用統合ソフトウェア
   - Disk Agent

注記: SAP R/3 Integration は、バックアップシステムで BRBACKUP が開始される SAP 対応 ZDB セッションを実行する場合にのみインストールする必要があります。

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。

HP P9000 XP ディスクアレイファミリ と Microsoft Exchange Server の統合

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 P9000 XP ディスクアレイファミリ 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、HP BC P9000 XP または HP CA P9000 XP 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 P9000 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
- `MS Exchange` 用統合ソフトウェア – アプリケーションシステムのみ

HP P9000 XP ディスクアレイファミリ と Microsoft SQL Server の統合

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 P9000 XP Agent`
- `MS SQL` 用統合ソフトウェア

HP 3PAR StoreServ Storage クライアント

HP 3PAR StoreServ Storage 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お使いのオペレーティングシステムに応じて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。

Windows システムの場合:

- `MS` ボリュームシャドウコピー用統合ソフトウェア
- `HP 3PAR VSS Agent`

HP-UX(Itanium) システムの場合:

- `HP P6000/HP 3PAR SMI-S Agent`

オペレーティングシステムに関係なく、ディスクとテープへの ZDB セッションまたはテープへの ZDB セッションを実行するには、次の Data Protector ソフトウェアコンポーネントをバックアップシステムに追加でインストールする必要があります。

- `General Media Agent`

HP-UX システムでは、インスタントリカバリを使用できないため、テープへの ZDB セッションしか実行できません。

EMC Symmetrix クライアント

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)`

  `EMC Symmetrix Agent` コンポーネントをリモートでインストールする前に、次の 2 つの EMC コンポーネントをインストールします。

  - EMC Solution Enabler
  - EMC Symmetrix TimeFinder または EMC Symmetrix Remote Data Facility (SRDF) マイクロコードとライセンス

- `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 バックアップ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。

クラスターへのインストール

EMC Symmetrix 用統合ソフトウェアは、クラスター環境にインストールできます。サポート対象のクラスター構成とインストール要件の詳細は、『HP Data Protector ゼロダウンタイムバックアップ管理者ガイド』を参照してください。

他のアプリケーションの統合

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 Net Services
  - SQL*Plus

- 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。このカタログデータベースは、非ミラー化ディスク上の個々のシステムにインストールすることをお勧めします。リカバリカタログは、登録しない状態で残しておきます。データベースのインストール方法については、Oracle のマニュアルを参照してください。
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
   - `Oracle` 用統合ソフトウェア – 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

   注記:

   - バックアップシステムの Data Protector `Oracle` 用統合ソフトウェアコンポーネントは、バックアップセット ZDB 方式にのみ必要です。プロキシーコピー ZDB 方式の場合は必要ありません。
   - RAC クラスター環境の場合、Oracle アプリケーションデータベースは、複数の Oracle インスタンスによりアクセスされます。そのため、Oracle インスタンスを実行するすべてのシステムに Data Protector `Oracle Integration` および `EMC Symmetrix Agent` コンポーネントをインストールしてください。
   - Oracle リカバリカタログデータベースが個々のシステムにインストールされている場合は、そこに Data Protector ソフトウェアコンポーネントをインストールする必要はありません。

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
- SAP 準拠の ZDB セッション (アプリケーションシステムではなくバックアップシステムで開始された BRBACKUP) を実行する場合、バックアップシステムを構成します。詳細は、

Oracle 用の SAP データベースガイド (スプリットミラーバックアップ、ソフトウェア構成) を参照してください。

- 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 のデータファイルは、ディスクアレイに配置する必要があります。
  - オンラインバックアップの場合、オンラインの REDO ログをディスクアレイに配置する必要はありません。オンライン SAP 対応 ZDB セッションは例外です。コントロールファイルはディスクアレイに配置する必要があります。
  - オフラインバックアップの場合、コントロールファイルとオンラインの REDO ログはディスクアレイに配置する必要があります。
  - アーカイブされた REDO ログファイルは、ディスクアレイに配置する必要はありません。

注記: Oracle データファイルの一部がシンボリックリンクにインストールされている場合、バックアップシステムにもリンクを作成します。

UNIX システムの場合: Oracle データベースが raw パーティション (raw ディスクまたは raw 論理ボリューム) にインストールされている場合、アプリケーションシステムとバックアップシステムでのボリューム/ディスクグループ名が同じであることを確認してください。

- UNIX システムの場合、アプリケーションシステムに以下のユーザーが存在しているかどうかを確認します。
  - プライマリグループが `dba` の `ora`*`ORACLE_SID`*
  - UNIX グループ `sapsys` に属する*`ORACLE_SID`*`adm`
- 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`

注記: インスタントリカバリを行う場合、`sapbackup`、`saparch`、および `sapreorg` の各ディレクトリが、Oracle データファイルとは異なるソースボリュームに存在していることを確認します。

最後の 6 つのディレクトリが前述の場所にない場合は、適切なリンクを作成してください。

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 PRO の場合、/usr/sap/PRO/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 orapro dba 4598276 Apr 17  2011 brarchive
-rwsr-xr-x   1 orapro dba 4750020 Apr 17  2011 brbackup
-rwsr-xr-x   1 orapro dba 4286707 Apr 17  2011 brconnect
-rwsr-xr-x   1 proadm sapsys 430467 Apr 17  2011 brrestore
-rwsr-xr-x   1 orapro dba 188629 Apr 17  2011 brtools
```

インストール手順

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、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。
   - EMC Symmetrix Agent
   - SAP R/3 用統合ソフトウェア
   - Disk Agent

注記: SAP R/3 Integration は、バックアップシステムで BRBACKUP が開始される SAP 対応 ZDB セッションを実行する場合にのみインストールする必要があります。

EMC Symmetrix 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。

- EMC Symmetrix Agent
- MS SQL 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 8.00 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。ユーザーインタフェースとしては、Data Protector GUI および Data Protector CLI のメッセージと通知がローカライズされています。各国語番のドキュメントも用意されています。各国語版にローカライズされた Data Protector ドキュメントセットについては、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。

注記: デフォルトでは、Data Protector のインストール時に、サポートされるすべての言語の言語サポートがインストールされ、システムの地域設定にあわせて Data Protector ユーザーインタフェースが起動されます。

Linux システムでは、Data Protector CLI のメッセージと通知は英語でしか表示されません。

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、英語版の Data Protector GUI 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:

   Data_Protector_home\bin\OmniFra.dll

   日本語のサポートの場合:

   Data_Protector_home\bin\OmniJpn.dll

   簡体字中国語のサポートの場合:

   Data_Protector_home\bin\OmniChs.dll

2. システムの地域設定を確認します。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。

各国語版 Data Protector マニュアルのインストール

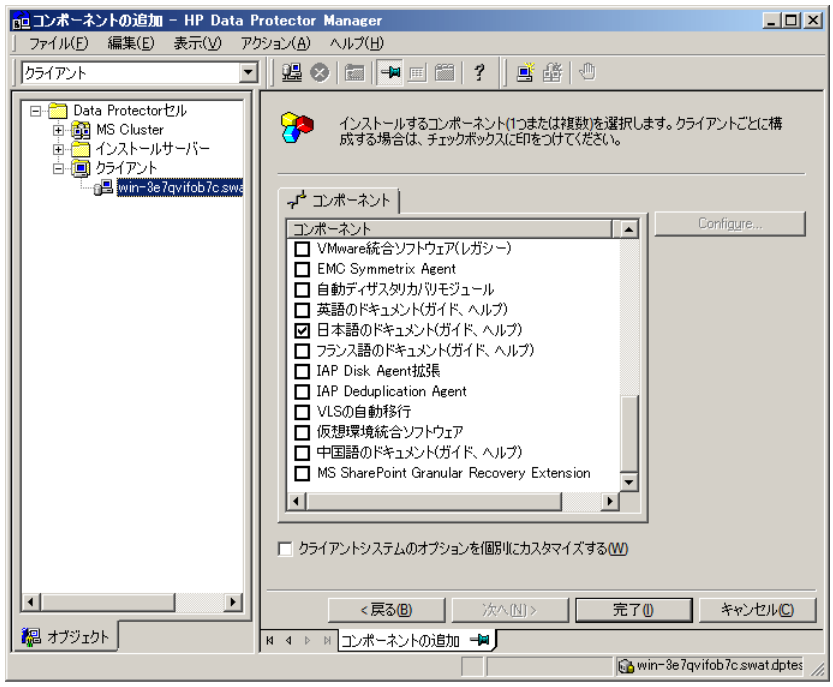
Windows システムへの各国語版 Data Protector マニュアルのインストール

リモートインストール

インストールサーバーを利用して Data Protector 各国語版マニュアルをリモートで配布するには、コンポーネントの追加ウィザードの [コンポーネント選択] ページで、必要な各国語版マニュアルを選択します。「各国語版マニュアルのリモートでのインストール」(113 ページ) 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、「リモートインストール」 (70 ページ) を参照してください。

図 22 各国語版マニュアルのリモートでのインストール

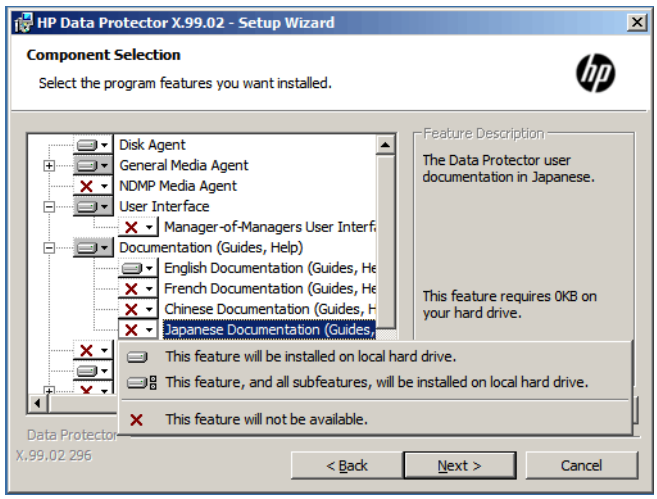


ローカルインストール

Windows システムに各国語版 Data Protector マニュアルをローカルにインストールするには、セットアップウィザードの [カスタムセットアップ] ページで、必要なコンポーネントを選択します。「セットアップ時の各国語版マニュアルの選択 」 (113 ページ) を参照してください。

ローカルインストール手順については、「Data Protector Cell Manager およびインストールサーバーのインストール」 (26 ページ) を参照してください。

図 23 セットアップ時の各国語版マニュアルの選択



UNIX システムへの各国語版 Data Protector マニュアルのインストール

リモートインストール

インストールサーバーを利用して Data Protector 各国語版マニュアルをリモートで配布するには、コンポーネントの追加ウィザードの [コンポーネント選択] ページで、必要な各国語版マニュアルを選択します。「各国語版マニュアルのリモートでのインストール」 (113 ページ) 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、「リモートインストール」 (70 ページ) を参照してください。

ローカルインストール

日本語、フランス語または簡体字中国語のマニュアル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`、`fra_ls`、または `chs_ls` ソフトウェアコンポーネントを指定してください。詳細な手順は、「UNIX および Mac OS X システムのローカルインストール」 (76 ページ) 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ーのインストールに `swinstall`、`pkgadd`、または `rpm` ユーティリティを使用している場合は、英語版のマニュアルしかインストールできません。各国語版 Data Protector マニュアルを Cell Manager またはインストールサーバーと同じシステムにインストールしたい場合は、それらの言語パックをリモートでインストールする必要があります。

Data Protector シングルサーバー版のインストール

Data Protector のシングルサーバー版 (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。シングルサーバー版は、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 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ーをインストールする手順は、「Data Protector Cell Manager およびインストールサーバーのインストール」 (26 ページ) 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ー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。
- 拡張製品を SSE に追加することはできません。
- SSE でクラスター化を行うことはできません。
- SSE でディザスタリカバリ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。

サポート対象デバイスについては、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。

SSE へのアップグレード (HP-UX) での制限事項

- 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、サーバーのバックアップはできません。UNIX、Windows、および Solaris 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 でクラスター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。

サポート対象デバイスについては、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。

パスワードのインストール

Cell Manager にパスワードをインストールする詳しい手順は、「Data Protector パスワード」(195 ページ) を参照してください。

Data Protector Web 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 サーバー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 Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。

インストール

Data Protector Web Reporting を Web サーバー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 ファイルをサーバーにコピーします。コピー先のサーバーは、Data Protector クライアントでなくてもかまいません。システムに Data Protector ユーザーインタフェースコンポーネントをインストールしている場合は、これらのファイルは以下のディレクトリにあります。

   Windows システムの場合:

   Data_Protector_home\java\bin

   UNIX システムの場合:

   /opt/omni/java/bin

2. ブラウザーで WebReporting.html ファイルを開くと、Data Protector Web 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。

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。Cell Manager にパスワードを設定して、Web レポートへのアクセスを制御することを強くお勧めします。手順については、『HP Data Protector ヘルプ』の索引「Web レポート、アクセスの制限」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、『HP Data Protector ヘルプ』の索引「Web レポートのインタフェース、通知の構成」を参照して、構成上の問題および独自のレポートを作成する方法を確認してください。

MC/ServiceGuard への Data Protector のインストール

Data Protector は、HP-UX および Linux 用の MC/ServiceGuard (MC/SG) をサポートしています。サポートされているオペレーティングシステムの詳細は、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。

Cell Manager をクラスター対応にする場合は、ライセンスで仮想サーバー IP アドレスを使用する必要があります。

クラスター対応 Cell Manager のインストール

前提条件

MC/SeviceGuard 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、クラスター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、クラスター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、一次ノードと各二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。「Data Protector Cell Manager およびインストールサーバーのインストール」(26 ページ) を参照してください。
- ユーザーグループ `hpdp` と、専用のユーザーアカウント `hpdp` には、両方のノードで同じ ID を割り当てる必要があります。

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。Data Protector で MC/ServiceGuard を構成する際の詳細は、『HP Data Protector ヘルプ』の索引「クラスター、MC/ServiceGuard」で表示される内容を参照してください。

インストールサーバーのクラスターノードへのインストール

インストールサーバーを二次 MC/ServiceGuard ノードにインストールし、リモートインストールに利用できます。「UNIX システム用のインストールサーバーのインストール」(38 ページ) .

クラスター対応クライアントのインストール

重要: Data Protector クラスター対応クライアントは、クラスター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。詳細は、「HP-UX クライアントのインストール」(51 ページ) と「Linux クライアントのインストール」(60 ページ) 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、仮想サーバー (クラスター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。「セルへのクラスター対応クライアントのインポート」(131 ページ) を参照してください。

バックアップデバイスとメディアプールの構成方法、または追加の Data Protector 構成タスクについては、『HP Data Protector ヘルプ』の索引「構成」を参照してください。

Microsoft Cluster Server への Data Protector 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は、http://support.openview.hp.com/selfsolve/manuals の最新のサポート一覧を参照してください。

注記:

Cell Manager をクラスター対応にする場合は、Cell Manager の仮想サーバー IP アドレスをライセンスに使用する必要があります。

クラスター対応 Cell Manager のインストール

前提条件

クラスター対応の Data Protector Cell Manager 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。

- すべてのクラスターノード上にクラスター機能が正しくインストールされていること。たとえば、ディスク共有の問題なしに、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。
- クラスター内に以下の名前を持つリソースが存在しないこと。

  `OBVS_MCRS`、`OBVS_HPDP_AS`、`OBVS_HPDP_IDB`、`OBVS_HPDP_IDB_CP`、および `OmniBack_Share`

  Data Protector では、これらの名前が Data Protector 仮想サーバーに使用されます。そのようなリソースが存在する場合は、削除するか名前を変更してください。

  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**]** > **[**クラスターアドミニストレーター**]** をクリックします。
  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。
- クラスター内の最低 1 つのグループにファイルクラスターリソースが定義されていること。Data Protector は、このファイルクラスターリソースの一部のデータファイルを指定したフォルダーにインストールします。

  データファイルはインストール時にユーザーが選択した共有フォルダーの下にある *`File Server`* リソースにインストールされます。

  ファイルクラスターリソースを定義する方法については、各クラスターのマニュアルを参照してください。ファイルクラスター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。
- ファイルクラスターリソースと同じグループ内に仮想サーバーが存在しない場合は、登録済みの 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ーを作成し、これをネットワーク名と関連付けます。
- Data Protector のインストール先となるファイルクラスターリソースの `IP` アドレス、ネットワーク名、および物理ディスクが、ファイルクラスターリソースの依存関係に含まれていること。これで Data Protector クラスターグループが、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ことを確認できます。
- クラスター管理者だけがファイルクラスターリソースの共有フォルダーへのアクセス権 (フルアクセス権限) を持つことを確認します。
- Data Protector は、すべてのクラスターノード上で同じ場所 (ドライブとパス名) にインストールされます。これらのインストール場所に空きがあることを確認してください。
- クラスター対応 Cell Manager のインストールをネットワーク共有から開始する場合、すべてのクラスターノードからこの共有にアクセスする必要があります。

- あらゆるクラスターノードで、その他の Microsoft インストーラーベースのインストールが実行されていないことを確認してください。
- クラスターの各システム (ノード) が適切に稼動していること。
- Windows Server 2008 上で Microsoft Cluster Service (MSCS) が実行されているサーバークラスターに、クラスター対応の Data Protector Cell Manager をインストールできるようにするには、「Data Protector インストールのための Windows Server 2008 または Windows Server 2012 上で実行する Microsoft サーバークラスターの準備」 (229 ページ) で説明されている手順を実行します。

留意事項

- ファイルクラスターリソースの共有フォルダーに直接アクセスできるように、ファイルクラスターリソースがアクティブになっているシステム (ノード) 上のクラスターサービスアカウントでセットアップを起動すること。リソースのオーナー (リソースがアクティブになっているシステム) は、クラスター管理ユーティリティを使うと確認できます。
- クラスター対応 Data Protector Cell Manager をインストールおよび構成するために、インストール時に以下のユーザー権限のドメインアカウントを用意すること。
  - Cell Manager システムに対する管理者権限を付与します。
  - クラスター内でのクラスター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。

重要: Microsoft Cluster Server をインストールするには、すべてのクラスターシステム (ノード) 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必要があります。そうしなかった場合は、Data Protector のサービスが、クラスター対応モードではなく通常のモードで稼動することになります。

- Inet サービスで使用する Windows ドメインユーザーアカウントには、すべてのクラスターノードで以下の Windows オペレーティングシステムのセキュリティポリシー特権が付与される必要があります。
  - 認証後にクライアントを偽装
  - プロセスレベルトークンの置き換え

  『HP Data Protector ヘルプ』の索引「Inet ユーザーの成り済まし」を参照してください。

ローカルインストール手順

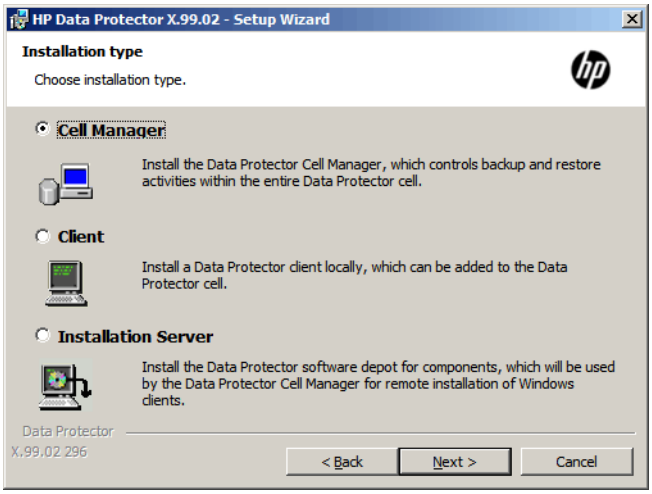
クラスター対応 Data Protector Cell Manager は、DVD-ROM からローカルにインストールする必要があります。この場合、以下の手順を実行します。

1. Windows 用インストール DVD-ROM をドライブに挿入します。

   [ユーザーアカウント制御] ダイアログが表示されます。**[**続行**]** をクリックしてインストールを続けます。
2. HP Data Protector ウィンドウで **[Data Protector** のインストール**]** を選択し、Data Protector のセットアップ用ウィザードを開始します。
3. セットアップウィザードに従い、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。

4. [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 24 インストールの種類の選択



5. セットアップはクラスター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、クラスターセットアップを有効にします。

   クラスターグループ、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ファイルクラスター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 はクラスター対応には**なりません**。「Windows 用 Cell Manager のインストール」 (32 ページ) を参照してください。

図 25 Windows Server 2008 でのクラスターリソースの選択

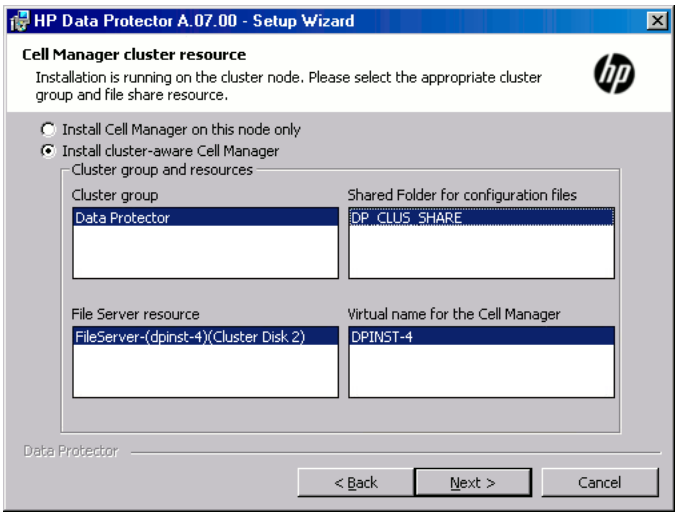
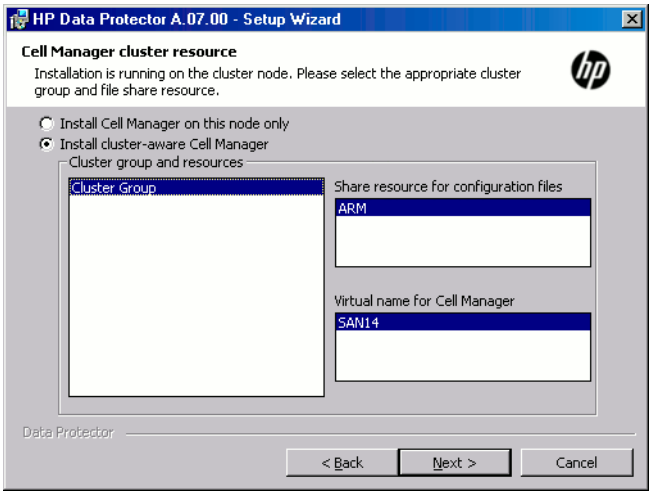
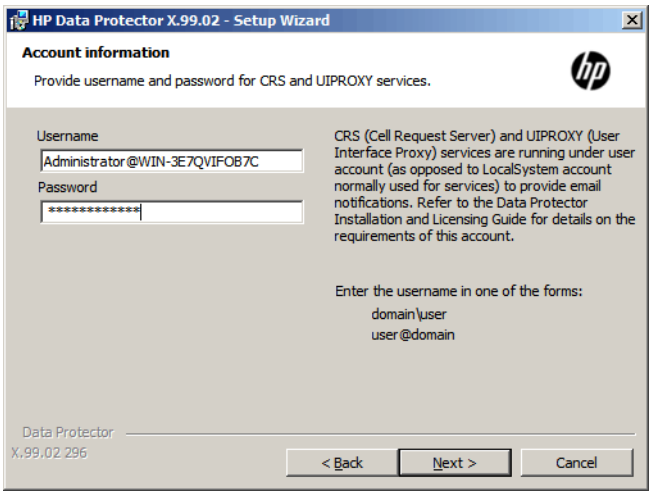


図 26 Windows システムでのクラスターリソースの選択



6. 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 27 アカウント情報の入力



7. Data Protector をデフォルトのフォルダーにインストールする場合は、**[Next]** をクリックします。

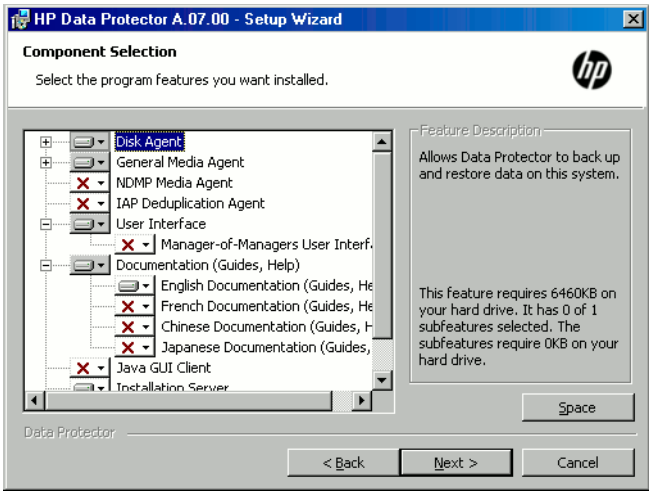
   それ以外の場合は、**[Change]** をクリックして [Change Current Destination Folder] または [Change Current Program Data Destination Folder] ダイアログボックスを開き、必要に応じてインストールフォルダーを変更します。プログラムデータインストールフォルダーへのパスは 80 文字以内に制限されます。

8. [Component Selection] ウィンドウで、すべてのクラスターノードおよびクラスター仮想サーバー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 Support ファイルが自動的にインストールされます。

   選択されたコンポーネントは、クラスター内のすべてのノードにインストールされます。

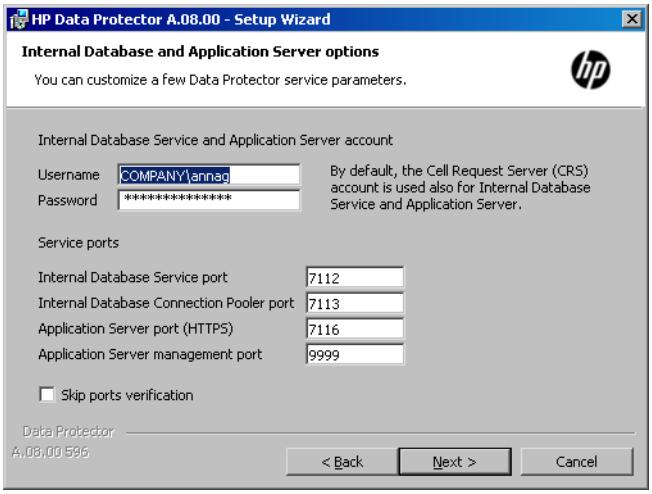
図 28 コンポーネント選択ページ



9. また、Data Protector サービスの内部データベースサービスおよびアプリケーションサーバーで使用するユーザーカウントやポートも変更できます。

   ［**Next**］をクリックします。

図 29 IDB およびアプリケーションサーバーオプションの変更



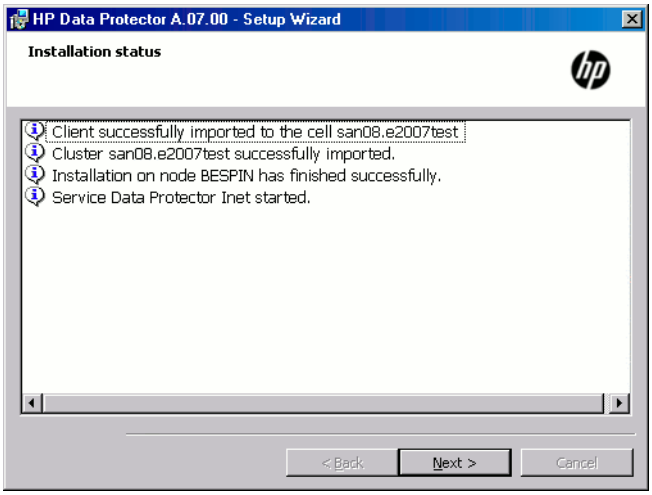
10. Data Protector がシステムで Windows ファイアウォールを検出した場合、[Windows Firewall configuration] ページが表示されます。Data Protector セットアップにより、必要なすべての Data Protector 実行可能ファイルが登録されます。デフォルトでは、**[Initially, enable newly registered Data Protector binaries to open ports as needed]** オプションが選択されています。この時点で、Data Protector によってポートがオ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。

    自動生成されるのはインバウンドファイアウォールルールのみであり、アウトバウンドファイアウォールルールは手動で作成する必要があるので注意してください。必要なポート範囲については、『HP Data Protector ヘルプ』の索引「ファイアウォールのサポート」で表示される内容を参照してください。

    [Next] をクリックします。

11. 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。
12. [Installation setup] ページが表示されます。**[Next]** をクリックします。

図 30 [Installation Status] ページ



13. ユーザーインタフェースコンポーネントをインストールした場合に、セットアップ直後に Data Protector GUI を使用して操作を開始するには **[Data Protector GUI の起動]** を選択します。

    英語版ドキュメント（ガイド、ヘルプ）コンポーネントをアップグレードしたか、または新しくインストールした場合に、セットアップ直後に『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を表示するには、**[Open the Product Announcements, Software Notes, and References]** を選択します。

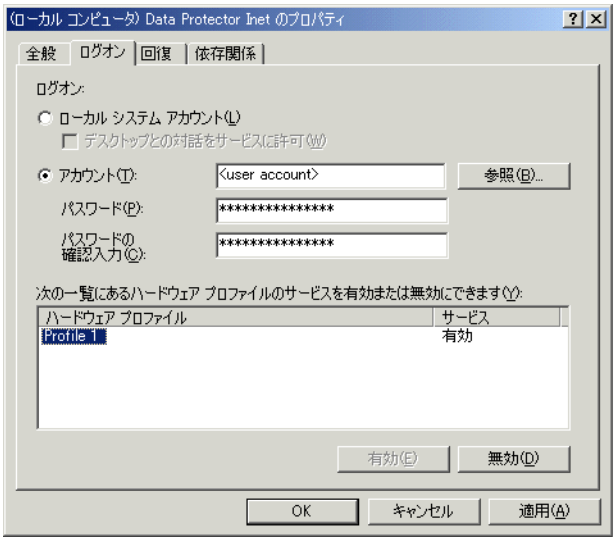
14. **[Finish]** をクリックしてインストールを完了します。

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. クラスターサービスアカウントが各クラスターノードの 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の種類は、「Data Protector ユーザーアカウント」(122 ページ)で示すように、［アカウント］に設定する必要があります。

図 31 Data Protector ユーザーアカウント



2. 次のコマンドを実行します。

   `omnirsh host INFO_CLUS`

   host には、クラスター仮想サーバーの名前を指定します。このコマンドを実行すると、クラスター内のシステムの名前のリストと仮想サーバーの名前が表示されます。`0 "NONE"` のような出力が表示された場合は、Data Protector がクラスター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。

Data Protector Inet サービスと CRS サービス

必要に応じて、Data Protector `Inet` サービスと `CRS` サービスを実行しているアカウントを変更してください。

クラスター対応クライアントのインストール

前提条件

クラスター対応の 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。

- すべてのクラスターノード上にクラスター機能が正しくインストールされていること。たとえば、ディスク共有の問題なしに、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。
- クラスターの各システムが適切に稼動していること。
- Windows Server 2008 または Windows Server 2012 上で Microsoft Cluster Service (MSCS) が実行されているサーバークラスターに、クラスター対応の Data Protector クライアントをインストールできるようにするには、「Data Protector インストールのための Windows Server 2008 または Windows Server 2012 上で実行する Microsoft サーバークラスターの準備」 (229 ページ) で説明されている手順を実行します。

ローカルインストール手順

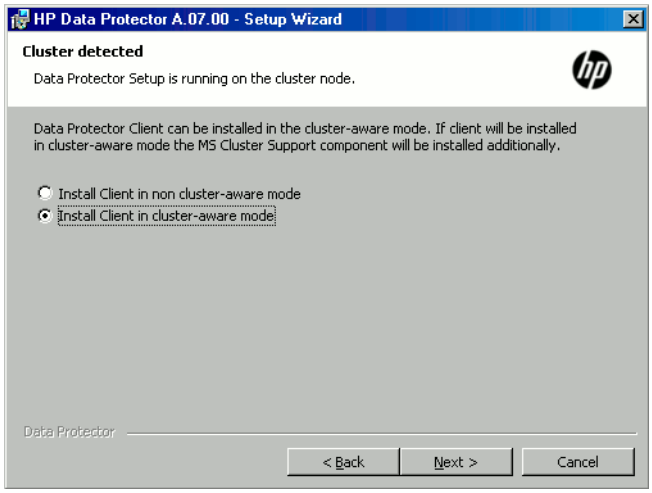
クラスター対応の Data Protector クライアントは、各クラスターノードで、DVD-ROM からローカルにインストールする必要があります。クラスターノード (Data Protector クラスタークライアント) は、インストールプロセス中に指定したセルにインポートされます。その後、仮想サーバー名をインポートする必要があります。

インストールを実行する際には、クラスター管理者のアカウントが必要です。この点を除けば、クラスタークライアントのセットアップは、通常の Windows クライアントのセットアップと同じです。MS Cluster Support ファイルが自動的にインストールされます。

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の詳細は、「Windows 用クライアントのインストール」 (47 ページ) を参照してください。

Data Protector インストールでは、クラスターが検出されたことが通知されます。**[Install client in cluster-aware mode]** を選択します。

図 32 クラスター対応インストールモードの選択



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ーノード上と仮想サーバー上で実行する必要があります。

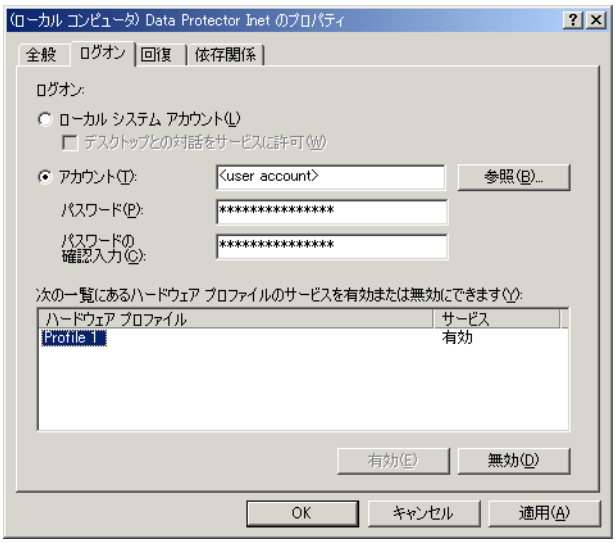
注記: クラスター対応クライアントは、標準の Cell Manager が管理する Data Protector セル、またはクラスター対応の Cell Manager が管理する Data Protector セルのどちらにでもインポートできます。

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. クラスターサービスアカウントが各クラスターノードの 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の種類は、「Data Protector ユーザーアカウント」 (124 ページ) で示すように、[アカウント] に設定する必要があります。

図 33 Data Protector ユーザーアカウント



2. 以下を実行します。

   `omnirsh` *`host`* `INFO_CLUS`

host には、クラスタークライアントシステムの名前を指定します。クラスター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" のような出力が表示された場合は、Data Protector がクラスター対応モードでインストールされていません。

Veritas Volume Manager

クラスター上に 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「Veritas Volume Manager がインストールされた Microsoft Cluster Server への Data Protector のインストール」 (231 ページ) 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、仮想サーバーのホスト名 (クラスター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。「セルへのクラスター対応クライアントのインポート」 (131 ページ) を参照してください。

バックアップデバイスとメディアプールの構成方法、または追加の Data Protector 構成タスクについては、『HP Data Protector ヘルプ』の索引「構成」を参照してください。

Inet アカウントと CRS アカウントの変更

必要に応じて、Data Protector `Inet` サービスと `CRS` サービスを実行しているアカウントを変更してください。

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、クラスター外にある 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す。

共有ディスクまたはクラスター対応アプリケーションをバックアップする場合は、仮想サーバーの IP アドレスをライセンスに使用する必要があります。

重要: Data Protector の場合、フェイルオーバー時のクラスター対応バックアップは サポートされていません。

クラスター対応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。詳細は、「Solaris 用クライアントのインストール」 (54 ページ) 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。

- 仮想サーバーをバックアップする場合は、仮想サーバーをセルにインポートする必要があります。
- 物理ノードをバックアップする場合は、物理ノードもセルにインポートする必要があります。

（「セルへのクラスター対応クライアントのインポート」 (131 ページ) を参照）。バックアップデバイスとメディアプールの構成方法、または追加の Data Protector 構成タスクについては、『HP Data Protector ヘルプ』の索引「構成」を参照してください。

Data Protector の IBM HACMP Cluster へのインストール

Data Protector は、IBM High Availability Cluster Multi-processing for AIX をサポートしています。

重要: Data Protector Disk Agent コンポーネントをすべてのクラスターノードにインストールします。

クラスター対応クライアントのインストール

Data Protector コンポーネントをクラスターノードにインストールするには、Data Protector を標準構成の UNIX システムにインストールする場合と同じ手順を使用します。詳細については、「リモートインストール」 (70 ページ) または「UNIX および Mac OS X システムのローカルインストール」 (76 ページ) を参照してください。

この次に行う作業

インストールが終了したら、クラスターノードと仮想サーバー (仮想環境パッケージの IP アドレス) を Data Protector セルにインポートします。「セルへのクラスター対応クライアントのインポート」 (131 ページ) を参照してください。

バックアップデバイスとメディアプールの構成方法、または追加の Data Protector 構成タスクについては、『HP Data Protector ヘルプ』の索引「構成」を参照してください。

Microsoft Hyper-V クラスターでの Data Protector のインストール

Microsoft フェールオーバークラスタリング機能を使用するクタスター内で構成した Microsoft Hyper-V システムに Data Protector をインストールする手順は、Data Protector を Microsoft Cluster Server にインストールする手順に類似しており、Microsoft Hyper-V システムは Data Protector クラスター対応クライアントとして構成する必要があります。詳細は、「Microsoft Cluster Server への Data Protector のインストール」 (117 ページ) を参照してください。

注記: Microsoft Hyper-V システムをクラスター対応クライアントとして構成すると、追加の Data Protector コンポーネントを Data Protector インストールサーバーでリモートインストールできるようになります。

3 インストールの保守

この章では、バックアップ環境の構成を変更するために最も頻繁に実行される手順について説明します。以降の項では、以下の情報を提供します。

- 保守モードを使用する方法と使用のタイミング
- 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
- 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ーをセルにインポートする方法
- 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ーや仮想サーバーをインポートする方法
- 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
- 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
- Data Protector パッチバンドルを管理し、インストールした Data Protector パッチを識別する方法
- Data Protector ソフトウェアをアンインストールする方法
- 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

Data Protector 保守モード

Cell Manager で保守タスクを実行する場合、Data Protector は保守モードに入る必要があります (この間、内部データベースへの書き込み操作は避けてください)。このようなタスクには、Data Protector インストールのアップグレードや、パッチと重要な修正プログラムのインストール、ハードウェアまたはオペレーティングシステムのアップグレードがあります。保守モードは、この章で説明する特定の手順に対してのみ必要ですが、他の章で説明するタスクに対しても適用されます。

保守モードに入るプロセスを実行すると、スケジューラーの停止やバックアップ仕様ディレクトリの名前変更、実行中のプロセスの中止、ロックされたリソースの解放などの一連のタスクが自動的に開始されます。保守モードは、個々のセル、および MoM とクラスター環境でサポートされています。

保守モードの開始

保守モードは、管理者権限を持つユーザーがコマンドラインインタフェースを使用して開始できます。保守モードを開始するには、以下を実行します。

個々のセルの場合:

```
omnisv -maintenance [GracefulTime]
```

MoM 環境の場合:

```
omnisv -maintenance -mom
```

実行中のセッションは Cell Manager によって同時にすべてを停止するように指示されますが、MoM 環境内のセルは個別に保守モードに入ります。

Cell Manager が保守モードに入る方法をカスタマイズするには、適切なグローバルオプションを変更します。`MaintenanceModeGracefulTime` は、実行しているセッションを中止するために Data Protector サービスに指定された秒数を示しますが、`MaintenanceModeShutdownTime` オプションは、セッションが中止するまでに待機する秒数を示します。両方のオプションのデフォルト値は 300 です。*`GracefulTime`* オプションを使用すると、`MaintenanceModeGracefulTime` グローバルオプションより優先されます。このオプションの値を超えてもまだ復元セッションが実行されていると、保守モードの開始が失敗します。

MoM 環境内のセルが保守モードに入ることができないと、保守モードは元の状態に戻ります。

Data Protector が保守モードで実行されているかをチェックするには、`omnisv -status` を実行して CRS サービスのステータスを確認するか、GUI ステータスバーをチェックしてください。GUI が保守モードであることを正確に示すことができるのは Cell Manager に接続しているときのみです。Cell Manager は通常のモードに切り替わった後もステータスバーに保守モードを示す場合があるので注意してください。

保守モード中、Cell Manager は、新しいデバイスの作成、バックアップと復元セッションまたはそれらのプレビュー、削除、コピー、集約セッションなどの IDB へのデータ書き込みを行うすべての操作を拒否します。

クラスター環境では、保守モードがアクティブな場合、クラスターパッケージのシャットダウンや Data Protector サービスの停止、手動によるボリュームのマウントなど、手動クラスター関連アクティビティしか実行できません。

保守モードがアクティブな場合、読み取り専用 IDB 操作すべてを実行できます。Data Protector サービスはすべて正しく動作します。Data Protector が保守モードである間、セルまたは MoM に接続できるのは Data Protector の管理者権限を持つユーザーだけです。

保守モードの終了

Cell Manager で CLI を使用して保守モードを終了するには、以下を実行します。

- 個々のセルの場合:

  ```
  omnisv -maintenance -stop
  ```

- MoM 環境の場合:

  ```
  omnisv -maintenance -mom_stop
  ```

MoM 環境では、個々のセルは保守モードを終了できません。MoM の保守は MoM サーバーからしか起動できません。

GUI を使用して保守モードを終了するには、以下を実行します。

1. コンテキストリストで、**[**クライアント**]** を選択します。
2. **[**アクション**]** メニューの **[**保守モードの停止**]** をクリックします。

通常モードが再開したら、中止されたセッションと拒否されたセッションを再起動できます。これらは以下の `maintenance.log` に記録されています。

Windows システムの場合: *`Data_Protector_program_data`*`\log\maintenance.log`

UNIX システムの場合: `/var/opt/omni/log/maintenance.log`

次の 2 つの例では、中止されたセッションと拒否されたセッションの `maintenance.log` エントリを示しています。

```
10.5.2013 10:52:45  OMNISV.2492.9936 ["/cli/omnisv/omnisv.c $Rev: 22709
 $ $Date:: 2013-03-22 18:00:03":247] X.99.01 b2
Session was aborted - graceful period expired!
session id:         2013/05/10-8
session type:       0
datalist:           large_backup
start date:         2013-05-10 10:52:45
owned by:           JOHN.JOHNSON@company.com

10.5.2013 10:48:45  CRS.7620.3308 ["/cs/mcrs/sessions.c $Rev: 22709 $
$Date:: 2013-03-22 18:00:03":142] X.99.01 b2
CRS is in maintenance mode - session rejected
session id:         R-2013/05/10-200
session type:       dbsm
session desc:       Database
```

```
start date:          2013-05-10 10:48:45
owned by:            .@ pid=0
```

保守モードがアクティブであった場合にセッションの開始を試みると、セッションは「中止されたセッション」として記録されます。中止されたセッションを後で実行するには、以下を実行します。

1. コンテキストリストで [内部データベース] をクリックします。
2. Scoping ペインで [セッション] を展開します。
3. セッションを右クリックして、コンテキストメニューから [失敗したオブジェクトの再開] を選択します。

Cell Manager が保守モードに入っている場合にセッションの開始を試みると、セッションは「拒否されたセッション」として記録されます。拒否されたセッションを後から実行する場合は、手動で各セッションを再起動します。

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ーを使用してソフトウェアコンポーネントをクライアントに配布すると、クライアントシステムが自動的にセルに追加されます。リモートインストールが完了すると、クライアントはセルのメンバーになります。

いつインポートを行うか

インストール DVD-ROM からローカルにインストールされた HP OpenVMS、Windows XP Home Edition など一部のクライアントは、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セルにシステムを手動で追加することを意味します。システムを Data Protector セルに追加すると、このシステムは Data Protector クライアントとして機能します。システムがセルのメンバーになると、この新しいクライアントに関する情報は、Cell Manager 上の IDB に書き込まれます。

クライアントがメンバーになれるのは、1 つのセルだけです。クライアントを他のセルに移動する場合は、まずクライアントを現在のセルから**エクスポート**してから、新しいセルに**インポート**します。クライアントをエクスポートする手順は、「セルからのクライアントのエクスポート」 (133 ページ) を参照してください。

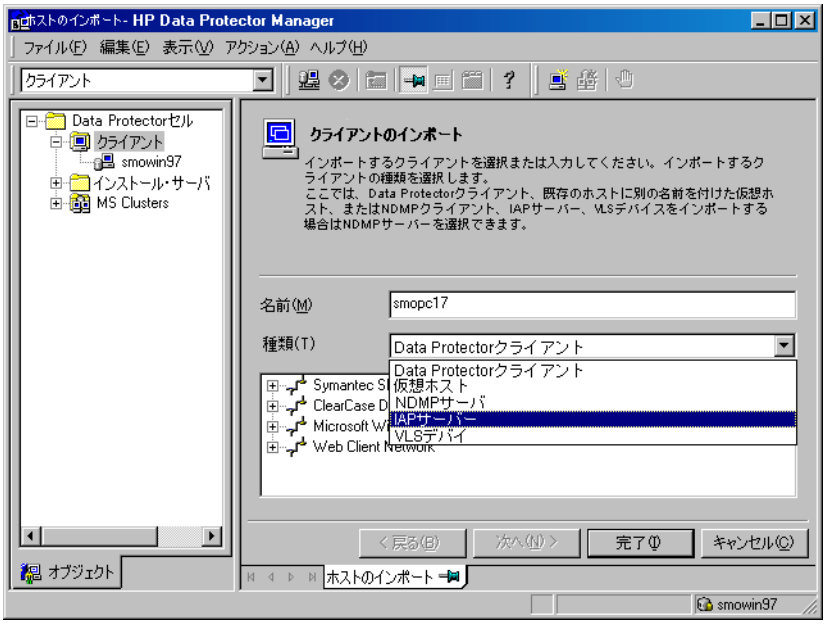
重要: Data Protector クライアントのインストール、およびクライアントのセルへのインポートが完了したら、不要なセル権限によるアクセスからクライアントを保護することを、強くお勧めします。「クライアントの保護設定」 (137 ページ) を参照してください。

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 ペインで [クライアント] を右クリックし、[クライアントのインポート] をクリックします。
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。「セルへのクライアントのインポート」 (130 ページ) を参照してください。

図 34 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ます。このオプションにより、同一システムに割り当てられている複数のホスト名をすべてインポートします。

NDMP クライアントをインポートする場合は、**[NDMP** サーバー**]** オプションを選択し、[次へ] をクリックします。NDMP Server に関する情報を指定します。

HP 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。

VLS デバイスをインポートする場合は、**VLS** デバイスオプションを選択して、[次へ] をクリックします。VLS デバイスの情報を指定します。

Data Protector の Microsoft Exchange Server 2010 用統合ソフトウェアで使用する Microsoft Exchange Server DAG 仮想ホストをインポートする場合は、[仮想ホスト] を選択します。

Data Protector の仮想環境統合ソフトウェアで使用するクライアントをインポートする場合は、**[VMware ESX(i)]**(スタンドアロンの ESX(i) Server システムの場合)、**[VMware vCenter]**(VMware vCenter Server システムの場合)、**[Hyper-V]**(Microsoft Hyper-V システムの場合) のいずれかを選択します。[次へ] をクリックし、ログイン資格情報を入力します。

[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ーのインポート

いつ追加を行うか

次の場合、インストールサーバーをセルに追加する必要があります。

- 独立した形で、たとえば Cell Manager とは別のシステム上に UNIX インストールサーバーをインストールした場合。

  この場合、インストールサーバー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は実行できません。

- Cell Manager にインストールしているが、他のセルでもリモートインストールを実行する場合。この場合は、他のセルの Cell Manager に接続された GUI を使用して、他のセルにも追加する必要があります。

クライアントとは異なり、インストールサーバーは複数のセルのメンバーにすることができます。したがって、インストールサーバーは、いずれかのセルから削除(エクスポート)しなくても、他のセルに追加 (インポート) できます。

追加方法

インストールサーバーのインポートプロセスは、クライアントのインポートプロセスに似ています。この作業は、インストールサーバーを追加するセルの Cell Manager に接続された Data Protector GUI を使用して、以下の手順に従って実行します。

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 ペインで、**[**インストールサーバー**]** を右クリックし、**[**インストールサーバーのインポート**]** をクリックして、ウィザードを起動します。「セルへのクライアントのインポート」 (130 ページ) 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または選択します。**[**完了**]** をクリックしてインストールサーバーをインポートします。

セルへのクラスター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ー対応クライアント上にローカルにインストールした後、そのクラスター対応クライアントを表す仮想サーバーを Data Protector セルにインポートします。

前提条件

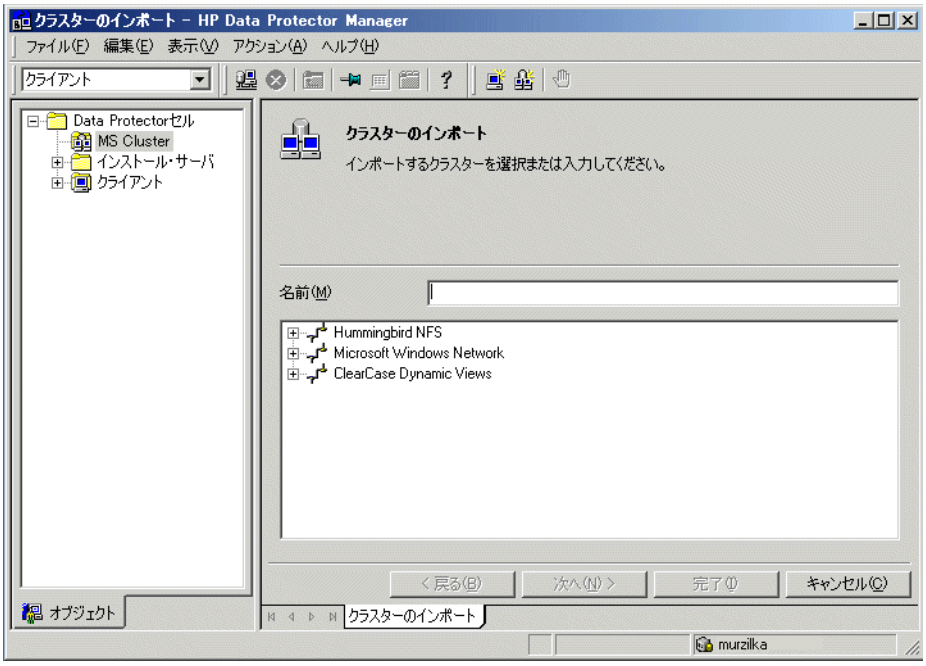
- すべてのクラスターノード上に Data Protector がインストールされていること。
- クラスター内ですべてのクラスターパッケージが実行されていること。

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]** を右クリックし、**[**クラスターのインポート**]** をクリックします。
3. インポート対象のクラスタークライアントを表す仮想サーバーの名前を入力するか、ネットワークをブラウズして仮想サーバーを選択します。「セルへの Microsoft Cluster Server クライアントのインポート」 (132 ページ) を参照してください。

図 35 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イアントをインポートします。

ヒント: 特定のクラスターノードまたは仮想サーバーをインポートするには、Scoping ペインでそのクラスターを右クリックし、[クラスターノードのインポート] または [クラスター仮想サーバーのインポート] をクリックします。

その他のクラスター

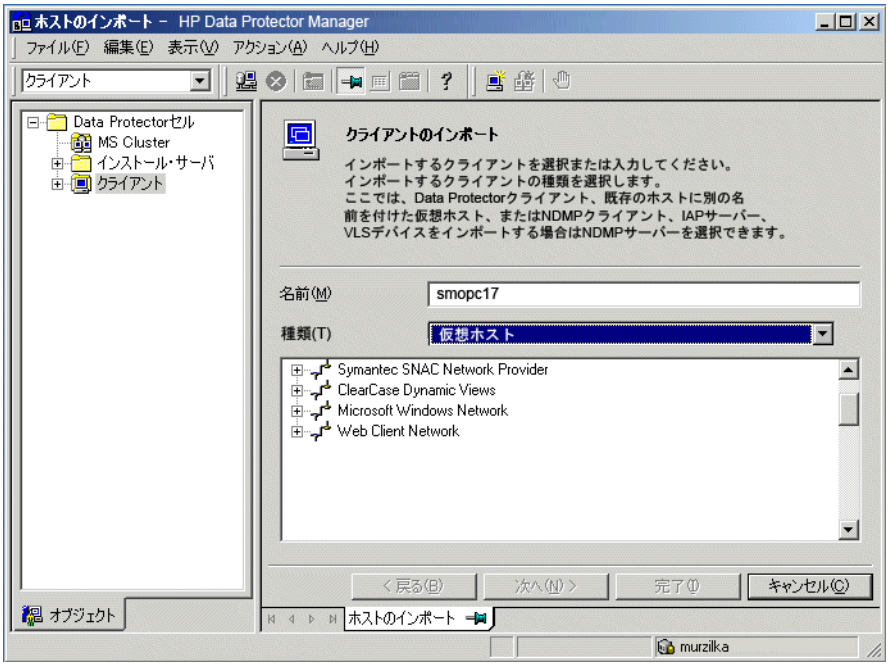
手順

MC/ServiceGuard、Veritas、または IBM HACMP Cluster 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 Protector Manager] で [クライアント] コンテキストを選択します。
2. Scoping ペインで [クライアント] を右クリックし、[クライアントのインポート] をクリックします。
3. 仮想サーバーのホスト名をアプリケーションクラスター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ーを選択することもできます。

   [仮想ホスト] オプションを選択し、これがクラスター仮想サーバーであることを示します。「MC/ServiceGuard または Veritas クライアントのセルへのインポート」 (133 ページ) を参照してください。
4. [完了] をクリックして仮想サーバーをインポートします。

図 36 MC/ServiceGuard または Veritas クライアントのセルへのインポート



ヒント: クラスター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ーノードをインポートする必要があります。詳しい手順は、「セルへのクライアントのインポート」(129 ページ)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 セルからのクライアントの**エクスポート**とは、クライアントからソフトウェアをアンインストールすることなく、クライアントへの参照を Cell Manager の IDB から削除することを意味します。この作業は、Data Protector GUI を使用して行います。

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。
- ライセンシングに関連する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。

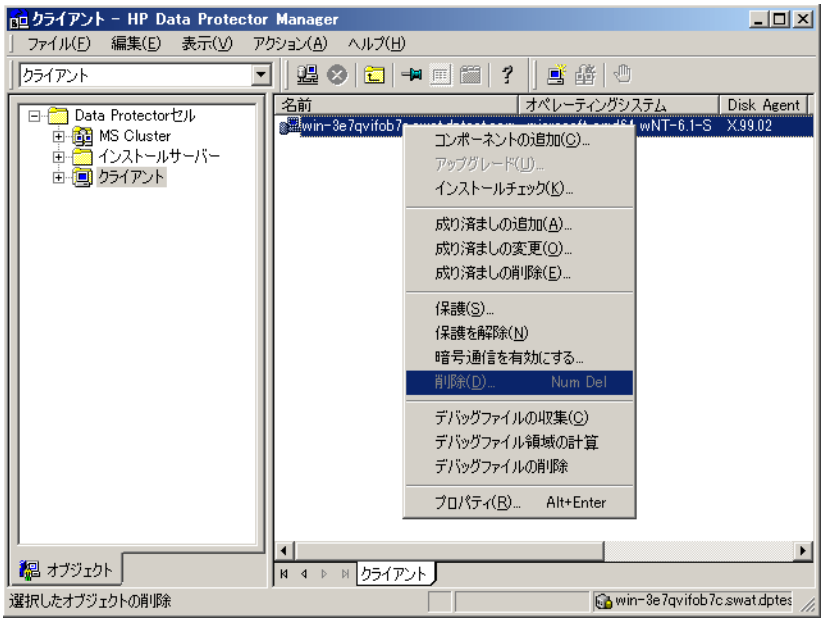
- 存在するすべてのクライアントがバックアップ仕様から削除されていること。削除されていない場合、Data Protector は不明なクライアントのバックアップを実行しようとするため、バックアップ仕様のこのシステムに対応する部分が正常に実行されません。バックアップ仕様の変更方法については、『HP Data Protector ヘルプ』の索引「バックアップ仕様の変更」の内容を参照してください。
- クライアントに接続済みおよび構成済みのバックアップデバイスやディスクアレイが存在しないこと。システムのエクスポートが完了すると、Data Protector は元のセル内のバックアップデバイスやディスクアレイを使用できなくなります。

エクスポート方法

Data Protector GUI を使用し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。「クライアントシステムのエクスポート 」 (134 ページ) を参照してください。

図 37 クライアントシステムのエクスポート



3. Data Protector ソフトウェアをアンインストールするかどうかを尋ねるメッセージが表示されます。クライアントをエクスポートする場合は、[いいえ] をクリックし、[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 Cell Manager がインストールされている場合は、Data Protector クライアントのエクスポートまたは削除はできません。ただし、クライアントとインストールサーバーのみがインストールされているシステムからクライアントをエクスポートすることはできます。この場合は、インストールサーバーはセルからも削除されます。

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 ソフトウェアをアンインストールするかどうかを尋ねるメッセージが表示されます。[いいえ] をクリックして、クラスタークライアントのみエクスポートします。

選択したクラスタークライアントが [結果エリア] のリストから削除されます。

ヒント: 特定のクラスターノードまたは仮想サーバーをエクスポートするには、Scoping ペインでクラスターノードまたは仮想サーバーを右クリックし、[削除] をクリックします。

セキュリティについて

ここでは、Data Protector のセキュリティについて説明します。Data Protector の保護を強化するために使用できる高度な設定、およびその前提条件や留意事項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。

この章で説明する内容は、保護設定を変更する場合だけではなく、新しいユーザーを構成する場合、クライアントを追加する場合、Application Agent を構成する場合、または留意事項の対象となるその他の変更を加える場合にも従う必要があります。保護設定の変更は、セル全体に影響を及ぼす可能性があるため、慎重に計画する必要があります。

セキュリティ層

Data Protector を安全に運用するためには、セキュリティが重要な以下の層に対して、セキュリティ対策を計画、テスト、および実現する必要があります。セキュリティ対策が必要な層は、Data Protector クライアント、Cell Manager、およびユーザーです。ここでは、これらの各層の保護の構成方法について説明します。

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ている Data Protector エージェントは、システム上のすべてのデータへのアクセスなど、多数の強力な機能を備えています。これらの機能は、**セル権限** (Cell Manager およびインストールサーバー) で実行されるプロセスにのみ使用できるようにし、それ以外の要求はすべて拒否することが重要です。

クライアントを保護する前に、信頼されるホストのリストを確認することが重要です。このリストには、以下が含まれます。

- Cell Manager
- 対応するインストールサーバー
- クライアントによっては、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、接続元になる可能性のあるすべてのホスト名 (または IP アドレス) が含まれている必要があります。上記のホストのいずれかがマルチホーム (複数のネットワークアダプターや複数の IP アドレスを持つ) またはクラスターの場合は、複数のクライアント名が必要になることがあります。

セル内の DNS 構成が一律でない場合は、他にも考慮すべき事項が存在することがあります。詳細は、「クライアントの保護設定」 (137 ページ) 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ーについては、保護設定が重要です。

- Cell Manager / Manager-of-Managers
- インストールサーバー
- Media Agent 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を信頼できるクライアントのリストに追加する必要はありません。ユーザー権限によっては、GUI を使用して Data Protector の全機能、または一部のコンテキストのみにアクセスできます。

Data Protector ユーザー

Data Protector ユーザーの構成時には、以下の点について十分に考慮してください。

- 一部のユーザー権限は非常に強力です。たとえば、`User configuration` および `Clients configuration` ユーザー権限を持つユーザーは保護設定を変更できます。`Restore to other clients` ユーザー権限も非常に強力です。`Back up as root` ま

たは Restore as root ユーザー権限のいずれかと組み合わせた場合は、特に強力です。

- それほど強力ではないユーザー権限にも、常にリスクは伴います。Data Protector を構成して一定のユーザー権限を制限し、これらのリスクを削減できます。これらの設定については、本章で後述します。「[バックアップ仕様を開始] ユーザー権限」(145 ページ) も参照してください。
- Data Protector では、少数のユーザーグループが事前に定義されています。Data Protector 環境内のユーザーの種類ごとに特定のグループを定義し、最小限の権限だけをユーザーに割り当てることをお勧めします。
- ユーザーグループのメンバーシップによるユーザー権限の割り当てに加えて、さらに特定のユーザーグループの操作を Data Protector セルの特定のシステムのみに制限することもできます。このポリシーは、user_restrictions ファイルを構成することによって実装できます。詳細は、『HP Data Protector ヘルプ』を参照してください。
- ユーザーの構成とユーザーのチェックは、密接な関係にあります (「厳密なホスト名チェック」(142 ページ) を参照)。ユーザーのチェックを強化しても注意してユーザーを構成しないと意味がなく、逆に、細心の注意を払ってユーザーを構成してもユーザーのチェックを強化しないと機能しない可能性があります。
- Data Protector のユーザーリストに「脆弱な」ユーザーが存在しないようにすることが重要です。

注記: ユーザー仕様の**ホスト**部分は、(特にチェックを強化した場合) 強度がある部分ですが、**ユーザー**部分と**グループ**部分は、確実にチェックすることができません。強力なユーザー権限を持つユーザーは、そのユーザーが Data Protector を管理する際に使用する特定のクライアントに対して構成する必要があります。複数のクライアントを使用する場合は、そのユーザーを**ユーザー**、**グループ**、<**任意**> として指定するのではなく、クライアントごとにエントリを追加するようにします。信頼されていないユーザーにはこれらのシステムへのログインを許可しないようにする必要があります。

ユーザーを構成する方法の詳細については、『HP Data Protector ヘルプ』の索引「構成、ユーザー」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、厳密なホスト名チェック機能によって強化できます。ただし、Cell Manager がクライアントとしても保護され、Data Protector ユーザーが十分に検討された上構成されていることが重要です。

必ずしもセル内のすべてのクライアントのセキュリティを強化する必要はありませんが、ほかのクライアントから信頼されるコンピューターについては、セキュリティの強化が重要です。この点は、Cell Manager だけではなく、インストールサーバーや Media Agent のクライアントについても同様です。

Cell Manager および Data Protector セル内のすべてのクライアントのセキュリティは、暗号制御通信を有効化することにより、さらに強化することができます。

詳細は、「厳密なホスト名チェック」(142 ページ)、「クライアントの保護設定」(137 ページ)、および「セキュアな通信の有効化」(143 ページ) 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。

- ユーザーが信頼されるクライアント (Cell Manager、インストールサーバー、MA、ロボティクスクライアント) にアクセスできないようにする必要があります。匿名ログオンや FTP アクセスも、全体的なセキュリティに重大なリスクをもたらす可能性があります。

- メディアおよびテープライブラリ (および接続先クライアント) を、許可されていないユーザーや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、オブジェクトまたはメディアのコピー、オブジェクト集約、またはオブジェクト検証の最中に、データがネットワーク経由で転送されます。ネットワークのセグメント化によって信頼されていないネットワークから完全に分離されていない場合は、ローカルに割り当てられたデバイス、Data Protector 暗号化テクニック、またはカスタム暗号化ライブラリを使用します。暗号化ライブラリを変更した後は、フルバックアップを実行する必要があります。
- さらに、Data Protector セル内で暗号制御通信を有効にすると、システムへの不正なアクセスを防止し、セキュリティを強化できます。

その他セキュリティ関連の内容については、『HP Data Protector ヘルプ』と『HP 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設定

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、クライアントがどのセル権限 (Cell Manager、MoM、インストールサーバー、およびインストールサーバー) から Data Protector ポート 5555 で要求を受け付けるかを指定できます。その結果、他のコンピューターからそのクライアントにアクセスできなくなります。「クライアントの保護」 (135 ページ) を参照してください。

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、実行前または実行後スクリプトの起動、クライアントのインポートやエクスポートなどの作業について、クライアントは、Data Protector ポート (デフォルト 5555) を介してこれらの作業を開始するコンピューターが、その作業を許可されているかどうかをチェックします。この保護メカニズムによって、クライアントは、指定されたセル権限からのみアクションを受け付けるよう指示されます。

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、問題を引き起こす可能性がある以下の状況について 考慮してください。

- 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。
- クラスター対応の 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、クライアントに接続するためのセル権限が明示的に認められたシステムを、1 つだけではなく、リストで指定することができます。障害を回避するために、事前にすべての適したクライアント名のリストを代わりのセル権限として用意しておきます。

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ーノードのクライアント名およびクラスター仮想サーバーのホスト名。
- セル権限の全ハードウェアがダウンした場合に、セル権限の移動先とな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、ディザスタリカバリ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。

アクセスの許可および拒否は、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、Cell Manager から Cell Manager、インストールサーバーからクライアント、またはクライアントからクライアントへのアクセスを許可または拒否できます。

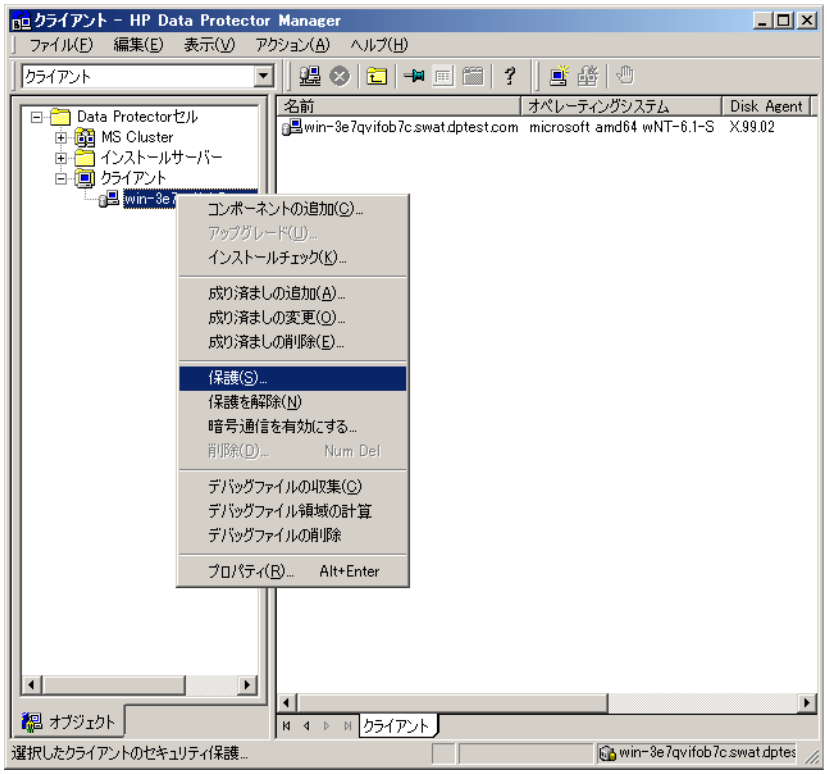
注記: Cell Manager 以外のシステムにあるインストールサーバーが許可されたクライアントのリストに追加されていない場合は、保護されたクライアントにアクセスできません。この場合は、インストールサーバーに依存している操作 (インストールのチェック、コンポーネントの追加、クライアントの削除など) は失敗します。保護されているクライアント上でこれらの操作を実行できるようにするには、インストールサーバーを許可されているクライアントのリストに追加してください。

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。

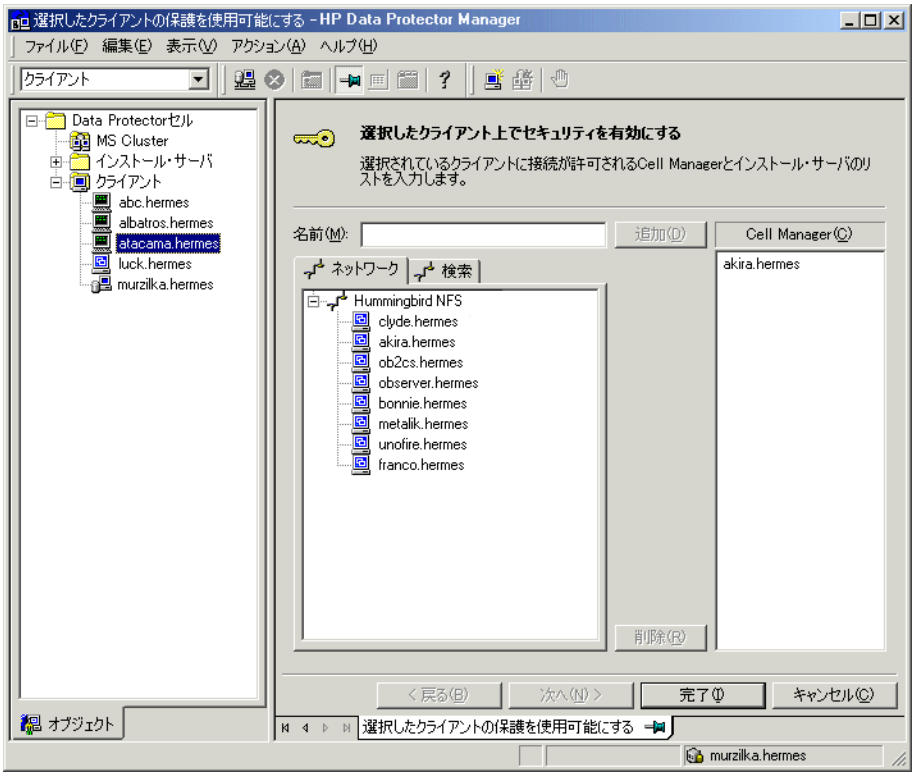
1. コンテキストリストで **[**クライアント**]** をクリックします。
2. Scoping ペインで [クライアント] を展開し、保護対象のクライアントを右クリックした後、**[**保護**]** をクリックします。「クライアントの保護設定」 (138 ページ) を参照してください。

図 38 クライアントの保護設定



3. 選択され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入力するか、[ネットワーク] タブ (Windows GUI の場合) または [検索] タブを使用してシステムを検索します。**[**追加**]** をクリックして、リストに各システムを追加します。「選択したクライアントの保護を使用可能にする」 (139 ページ) を参照してください。

図 39 選択したクライアントの保護を使用可能にする



Cell Manager は、自動的にアクセスが許可され、信頼できるクライアントのリストに追加されます。リストから Cell Manager を削除することはできません。

4. [完了] 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、各要求に対してソースを確認し、[選択したクライアント上でセキュリティを有効にする] ウィンドウで選択されているクライアントからの要求だけを受信します。これらのクライアントは、`allow_hosts`ファイルにリストされています。 要求が拒否されると、イベントは、以下のディレクトリの `inet.log` に記録されます。

Windows Vista、Windows 7、Windows 8、Windows Server 2008、および Windows Server 2012 の場合: *Data_Protector_program_data*`\log`

その他の Windows システムの場合: *Data_Protector_home*`\log`

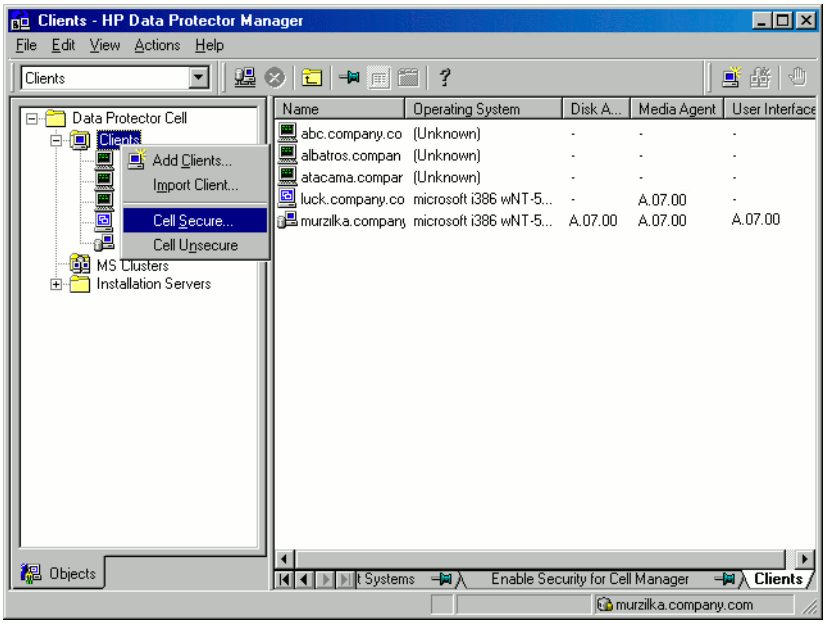
HP-UX、Solaris、および Linux システムの場合: `/var/opt/omni/log`

その他の UNIX システムおよび Mac OS X 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。

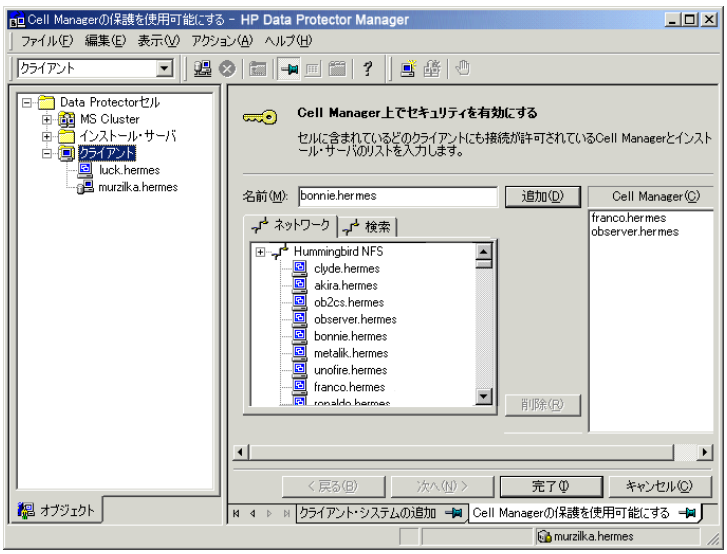
1. コンテキストリストで [クライアント] をクリックします。
2. Scoping ペインで [クライアント] を右クリックし、[セルの保護] をクリックします。「セルの保護設定」 (140 ページ) を参照してください。

図 40 セルの保護設定



3. セル内のすべての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入力するか、[ネットワーク] タブ (Windows GUI の場合) または [検索] タブで検索します。**[**追加**]** をクリックして、リストに各システムを追加します。「セル内のすべてのクライアントに対する保護の設定」 (140 ページ) を参照してください。

図 41 セル内のすべてのクライアントに対する保護の設定



4. **[**完了**]** 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、各要求に対してソースを確認し、[Cell Manager 上でセキュリティを有効にする] ウィンドウで選択されているクライアントからの要求だけを受信します。これらのクライアントは、`allow_hosts`ファイルにリストされています。要求が拒否されると、イベントは、以下のディレクトリの `inet.log` に記録されます。

Windows Vista、Windows 7、Windows 8、Windows Server 2008、および Windows Server 2012 の場合: *`Data_Protector_program_data`*`\log`

その他の Windows システムの場合: *`Data_Protector_home`*`\log`

HP-UX、Solaris、および Linux システムの場合: `/var/opt/omni/log`

その他の UNIX システムおよび Mac OS X システムの場合: `/usr/omni/log`

セル全体を保護すると、そのセル内に存在するすべてのクライアントが同時に保護されます。セルに新しいクライアントを追加する場合は、追加したクライアントも保護する必要があります。

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、保護を解除するクライアント (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、セル内のすべてのクライアントへのアクセスを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、クライアントへの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。特定のコンピューターからのクライアントへのアクセスを明示的に拒否することもできます。拒否するには、拒否するホスト名を `deny_hosts` ファイルに追加します。この 2 つのファイルは以下のディレクトリにあります。

Windows Vista、Windows 7、Windows 8、Windows Server 2008、および Windows Server 2012 の場合: *`Data_Protector_program_data`*`\Config\client`

その他の Windows システムの場合: *`Data_Protector_home`*`\Config\client`

HP-UX、Solaris、および Linux システムの場合: `/etc/opt/omni/client`

その他の UNIX システムおよび Mac OS X 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 手動で編集 (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 バイト形式 (Unicode) ですが、HP-UX、Solaris、Linux システムでは 1 バイト形式またはマルチバイト形式 (シフト JIS など) です。

inet.log ファイルに大量のログが記録される

クライアントに保護が設定されず、Cell Manager が MC/ServiceGuard 環境に構成されるか、複数の名前または IP 番号が割り当てられている場合に、`inet.log` ファイルに以下のようなエントリが多数含まれていることがあります。

`A request 0 came from host` *`name.company.com`* `which is not a Cell Manager of this client`

これは、保護されていないクライアントが Cell Manager のプライマリホスト名しか認識しないために発生します。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。

クライアントの保護は、`inet.log` ファイルへの不要なエントリを回避する方法として使用できます。ただし、Cell Manager のすべてのクライアント名は、各クライアントの `allow_hosts` ファイルにリストされている必要があります。これにより、フェイルオーバーの発生時にもクライアントへのアクセスが可能になります。

何らかの理由でユーザー環境でこの回避策を使用できない場合は、クライアントを保護し、アクセスを許可するシステムの IP アドレスの範囲として `*` を指定します。これによって、クライアントは、すべてのシステム (任意の IP アドレス) からの要求を受け付け、事実上保護されていない状態となりますが、大量のログが記録される問題は解決します。

厳密なホスト名チェック

デフォルトでは、Cell Manager によって、比較的簡単な方法を使ってユーザーのチェックが行われます。この方法では、ユーザーインタフェースまたは Application Agent を起動しているクライアントが認識できるホスト名が使用されます。この方法は、セキュリティが " 推奨 " される (たとえば、悪意のある攻撃の可能性があまり高くない) 環境で、中レベルのセキュリティをより簡単に構成および実現する場合に適しています。

一方、厳密なホスト名チェックの設定を使用すると、ユーザーのチェックが強化されます。このチェックでは、Cell Manager で接続から取得した IP を基に DNS 逆引きを行ってホスト名を解決し、そのホスト名を使用します。この方法には、以下の制限事項および留意事項があります。

制限事項

- IP ベースのユーザーチェックは、ネットワークのスプーフィング対策程度の強度しかありません。セキュリティ設計者は、特定のセキュリティ要件を満たすレベルのスプーフィング対策が既存のネットワークに施されているかどうかを確認する必要があります。スプーフィング対策は、ファイアウォール、ルーター、VPN などを使ってネットワークをセグメント化することによって追加できます。
- 特定のクライアント内でユーザーを分離しても、クライアント間で分離した場合ほど強度はありません。高レベルのセキュリティ環境では、標準ユーザーと強力な権限を持つユーザーが同じクライアント上で混在しないようにしてください。
- ユーザー仕様に含まれるホストは、DHCP を使用するように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)。

厳密なホスト名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厳密なホスト名チェックを行う場合で異なることがあります。

- DNS 逆引きで別のホスト名が返される。これは、意図的に行うこともありますが、クライアントまたは DNS 逆引き参照用テーブルの不正な設定を示していることもあります。
- クライアントがマルチホーム構成である (複数のネットワークアダプターや複数の IP アドレスを持つ)。マルチホームクライアントにこの留意事項が該当するかどうかは、そのクライアントのネットワーク内での役割や DNS での構成方法によって異なります。
- クライアントがクラスターの場合。

この設定で有効になるチェックの特性によっては、Data Protector ユーザーを再構成する必要があります。既存の Data Protector ユーザーの仕様をチェックして、上記のいずれかの理由により影響されるかどうかを確認する必要があります。状況によっては、既存の仕様を変更する

か、新しい仕様を追加して、接続元になる可能性のあるすべてのIPを含める必要があることがあります。

なお、厳密なホスト名チェックを有効にするときにユーザー仕様を変更する必要があった場合は、デフォルトのユーザーチェックに戻すときにユーザーを再構成する必要があります。そのため、継続的に使用するユーザーチェックを事前に決定することをお勧めします。

信頼性の高いDNS逆引きを行うための前提条件は、保護されたDNSサーバーを使用することです。許可されていないユーザーからの物理アクセスやログオンを防ぐ必要があります。

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

チェックを強化した場合、一部の内部接続へのアクセス権が自動的に付与されません。そのため、このチェックを使用する場合は、以下のそれぞれについて、新しいユーザーを追加する必要があります。

- Windowsクライアント上のApplication Agent (OB2BAR)。Windowsクライアントの場合、Application Agentがインストールされている各クライアントに、ユーザー `SYSTEM`、`NT AUTHORITY`、*`client`*を追加する必要があります。特定のアカウントを使用するようにクライアントの `Inet` を構成する場合は、そのアカウントが既に構成されている必要があります。詳細は、『HP Data Protectorヘルプ』の索引「厳密なホスト名チェック」を参照してください。
- Webレポートを使用する場合は、Webレポートの提供元になる各ホスト名について、`java`、`applet`、*`hostname`*を追加する必要があります。Webレポートの全機能を使用するためには、ユーザーが `admin` グループに属している必要があります。したがって、これらのクライアントは信頼済みクライアントである必要があります。また、(Webサーバー経由などで)Webレポートの機能を他のユーザーが使用できるようにする前に、全般的に使用可能にするデータのセキュリティについても検討してください。

ユーザーを構成する方法の詳細は、『HP Data Protectorヘルプ』の索引「構成、ユーザー」を参照してください。

機能を使用可能にする

厳密なホスト名チェックを有効に設定するには、`StrictSecurityFlags` グローバルオプションを `0x0001` に設定します。

グローバルオプションの詳細は、『HP Data Protectorトラブルシューティングガイド』を参照してください。

セキュアな通信の有効化

Data Protectorの暗号制御通信により、Data Protectorセル内の不正なアクセスを防止できます。Data Protector GUIまたはCLIを使用して、Data Protectorセル内のすべてのクライアントの暗号制御通信をリモートで有効化できます。

暗号制御通信を有効化する方法

CLIからセル内のすべてのクライアントの暗号制御通信を有効にするには、以下を実行します。

```
omnicc -encryption -enable -all
```

詳細は、`omnicc` のmanページまたは『HP Data Protector Command Line Interface Reference』を参照してください。

重要: 暗号制御通信は、Cell Managerまたはセル内で暗号制御通信がすでに有効になっているクライアントからのみ、有効にすることができます。

暗号制御通信を有効化するには、Data Protector GUI上以下の手順を実行してください。

注記: 最初に Cell Manager 上で暗号制御通信を有効化し、その後にセル内のクライアント上で有効化します。

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 ペインで **[Data Protector** セル] と [クライアント] を順に展開します。すべてのクライアントが表示されます。
3. 変更するクライアントをクリックします。
4. [接続] プロパティページで、[暗号制御通信] オプションを選択します。
5. [証明書チェーン] ドロップダウンリストで、証明書を選択します。
6. [秘密キー] ドロップダウンリストで、秘密キーを選択します。
7. [信頼済み証明書] ドロップダウンリストで、信頼済み証明書を選択します。
8. [適用] をクリックして変更内容を保存します。

複数のクライアントで暗号制御通信を有効化するには、Data Protector GUI で以下の手順を実行してください。

1. コンテキストリストで [クライアント] をクリックします。
2. Scoping ペインで **[Data Protector** セル] と [クライアント] を順に展開します。すべてのクライアントが表示されます。
3. 暗号制御通信の有効化の実行元となるクライアントを右クリックし、[暗号通信を有効にする] をクリックします。
4. 暗号制御通信を有効化するクライアントを 1 つ以上選択します。[次へ] をクリックします。
5. [証明書チェーン] ドロップダウンリストで、証明書を選択します。
6. [秘密キー] ドロップダウンリストで、秘密キーを選択します。
7. [信頼済み証明書] ドロップダウンリストで、信頼済み証明書を選択します。
8. [完了] をクリックして変更内容を保存します。

どのような処理が行われるか

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

セキュリティの例外リストにクライアントを追加する方法

何らかの理由により保護された通信がサポートされていないクライアントは、Cell Manager 例外リストに追加し、特定のクライアントの非暗号化モードによる通信を許可することができます。

セキュリティの例外リストにクライアントを追加するには、Data Protector GUI で以下の手順を実行してください。

1. コンテキストリストで [クライアント] をクリックします。
2. Scoping ペインで **[Data Protector** セル] と [クライアント] を順に展開します。すべてのクライアントが表示されます。
3. 変更する Cell Manager をクリックします。
4. セル内のセキュリティの例外リストに追加するシステムの名前を入力するか、[ネットワーク](Windows GUI のみ) または [検索] タブでシステムを検索します。
5. [追加] をクリックしてシステムをリストに追加し、[適用] をクリックして変更内容を保存します。

server configuration ファイル

プレーンテキストモードで許可されるクライアントは、Cell Manager 上の以下のディレクトリにある `server configuration` ファイルに書き込まれます。

Windows システムの場合: *`Data_Protector_program_data`*`\Config\server\config`

HP-UX システムおよび Linux システムの場合: `/etc/opt/omni/server/config`

システムをセキュリティの例外リストから削除するには、手順 1～4 を実行して [削除] をクリックし、[適用] をクリックして変更内容を保存します。

制限事項

- 非暗号化通信を使用するクライアントと暗号制御通信が有効化されたクライアントの間の通信はサポートされていません。つまり、Data Protector の操作は実行されません (たとえば、インストールサーバーからのリモートインストールは暗号制御通信が有効化されたクライアントに対して非暗号化通信を使用するため成功しません)。

  ただし、Cell Manager は Data Protector セル内の両方の種類のクライアントと通信できます。

[バックアップ仕様を開始] ユーザー権限

Data Protector のユーザーおよびユーザー権限の一般的な情報は、『HP Data Protector ヘルプ』の索引「ユーザー」を参照してください。

[バックアップ仕様を開始] ユーザー権限だけでは、GUI の [バックアップ] コンテキストを使用することができません。ユーザーは、omnib の-datalist オプションを使用してコマンドラインからバックアップ仕様を起動できます。

注記: [バックアップ仕様を開始] を [バックアップ開始] 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。

ユーザーには、必ずしも対話式バックアップの実行を許可する必要はありません。バックアップ仕様を保存する権限を持つユーザーのみに対話式バックアップを許可するには、`StrictSecurityFlags` グローバルオプションを `0x0200` に設定します。

グローバルオプションの詳細は、『HP Data Protector トラブルシューティングガイド』を参照してください。

バックアップ仕様の内容にアクセスできないようにする

高レベルのセキュリティ環境では、保存されたバックアップ仕様の内容が慎重に取り扱うべき情報、または秘密情報として認識される場合があります。Data Protector を構成して、`Save backup specification` ユーザー権限を持つユーザー以外のユーザーのバックアップ仕様を隠すことができます。これを行うには、`StrictSecurityFlags` グローバルオプションを `0x0400` に設定します。

グローバルオプションの詳細は、『HP Data Protector トラブルシューティングガイド』を参照してください。

ホストの信頼

ホスト信頼機能を使用すると、少数のクライアント間で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。ホスト信頼機能では、データを使用する信頼関係のあるホストのグループを定義します。

ホストの信頼は、通常、以下のような場合に使用します。

- クライアントがクラスター (ノードおよび仮想サーバー) 内に存在する場合。
- 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いて、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

トラストホストを構成するには、Cell Manager 上に *Data_Protector_program_data*\Config\Server\cell\host_trusts ファイル (Windows システム)、/etc/opt/omni/server/cell/host_trusts ファイル (UNIX システムの場合) 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 の使用時に問題が発生した場合は、ログファイルの情報を使用して問題を割り出すことができます。たとえば、ログに記録されたログが、誤って構成されたユーザーまたはクライアントの特定に役立つことがあります。

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、次のディレクトリにあるセル内の各クライアントの inet.log ファイルに記録されます。

Windows Vista、Windows 7、Windows 8、Windows Server 2008、および Windows Server 2012 の場合: *Data_Protector_program_data*\log

その他の Windows システムの場合: *Data_Protector_home*\log

HP-UX、Solaris、および Linux システムの場合: /var/opt/omni/log

その他の UNIX システムおよび Mac OS X システムの場合: /usr/omni/log

Cell Manager 保護イベント

Cell Manager のセキュリティイベントは、Cell Manager 上の次のディレクトリにある security.log ファイルに記録されます。

Windows システムの場合: *Data_Protector_program_data*\log\server

UNIX システムの場合: /var/opt/omni/server/log

Data Protector パッチの管理

Data Protector パッチは HP サポートによって提供され、HP サポート Web サイトからダウンロードできます。Data Protector パッチは、個別またはバンドルで提供されます。

パッチのインストール

Cell Manager パッチはローカルにインストールできます。ただし、クライアントにパッチを適用するには、インストールサーバーが必要です。インストールサーバーにパッチを適用した後、リモートでクライアントにパッチを適用できます。

重要: HP-UX システムでは、Cell Manager (CS) のパッチを Cell Manager に適用する前に、Data Protector `omnisv` コマンドを使用して Data Protector のサービスを停止し、パッチの適用が完了した後に再度 Data Protector を開始してください。

1 つのパッチバンドルに個々のパッチを含める場合、インストールできるのはバンドル全体のみです。詳細は、パッチで指定される手順を参照してください。

システム上にインストールされているパッチは、Data Protector GUI または CLI で確認できます。「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」 (148 ページ) を参照してください。

Data Protector パッチバンドルのインストールと削除

Data Protector がすでにインストールされている場合、Data Protector パッチバンドル (Data Protector パッチ群) を同じシステムにインストールすることが可能です。

Data Protector パッチバンドルを UNIX システムにインストールする操作には、`omnisetup.sh` スクリプトを使用できます。Windows システムでは、パッチバンドルは実行可能ファイルで提供されます。

パッチバンドルは、削除することもできます。パッチバンドルを削除すると、Data Protector は直前のリリースバージョンに戻ります。詳細は、パッチバンドルで指定される手順を参照してください。

UNIX システムでの Data Protector パッチバンドルのインストールと削除

Data Protector パッチバンドルをインストールするには、パッチバンドルファイルに付属する tar アーカイブの `omnisetup.sh` コマンドを実行します。コマンド実行では、`-bundleadd` オプションを指定します。たとえば、次のように入力します。

```
omnisetup.sh -bundleadd b701
```

Data Protector パッチバンドルをインストール可能なのは、インストールサーバーと Cell Manager のみです。インストールが失敗した場合や途中で停止した場合、インストールを続行して残りのパッチのインストールをインストールする操作 (Linux システムのみでサポートされている機能)、インストールしたパッチをロールバックして直前のパッチレベルに戻す操作、すべてのパッチのインストールをキャンセルして終了する操作が可能です。

Data Protector パッチバンドルを削除するには、`omnisetup.sh -bundlerem` コマンドを実行します。たとえば、次のように入力します。

```
omnisetup.sh -bundlerem b701
```

詳細は、パッチまたはパッチバンドルで指定される手順を参照してください。

Windows システムでの Data Protector パッチバンドルのインストールと削除

Windows 用の Data Protector パッチバンドルは、実行可能ファイル (`DPWINBDL_00701.exe` など) で提供されます。Data Protector パッチバンドルは、インストールサーバー、Cell Manager、またはクライアントシステムにインストールできます。

Windows システムにパッチバンドルをインストールするには、次の例のように、*`BundleName`*`.exe` コマンドを実行します。

```
DPWINBDL_00701.exe
```

このコマンドは、システム上にインストールされているコンポーネントを識別し、最新のパッチにアップグレードします。

Data Protector パッチバンドルを削除するには、*`Data_Protector_home`*`\bin\utilns` にある `remove_patch.bat` コマンドを実行します。

`remove_patch` *`BundleName DPInstallationDepot`*(*`DPInstallationDepot`* は、Data Protector のインストール元となった場所を示します。パッチバンドルのインストール元ではあ

りません)。たとえば、パッチバンドル `b701` を削除する場合は次のようになります。Data Protector は、`D:\WINDOWS_OTHER` からインストールされたとします。

```
remove_patch.bat b701 D:\WINDOWS_OTHER
```

Data Protector パッチバンドルは、インストールサーバー、Cell Manager、またはクライアントシステムから削除できます。

注記: Windows システムでは、`remove_patch.bat` コマンドにより、パッチを個々に削除することも可能です。ただし、システム上にパッチが残っている状態で CORE パッチを削除しないでください。削除してしまうと、残っている他のパッチを削除できなくなります。

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

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。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。

注記: サイト専用パッチまたはパッチバンドルをインストールすると、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。

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をインストールしておく必要があります。

制限事項

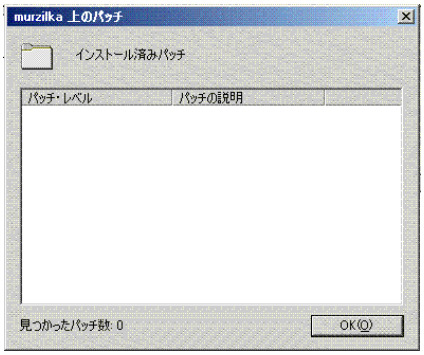
- パッチの確認は、同じセル内にあるシステムにインストールされているパッチのみが対象です。

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された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。
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 42 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してあるパッチを確認するには、`omnicheck` コマンドを実行します。 `-patches -host` *`hostname`* コマンド。ここで、*`hostname`* は確認対象システムの名前を表します。

このコマンドの詳細については、`omnicheck`man ページ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。

アンインストールすると、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、Cell Manager 上の IDB からそのシステムへの**すべての**参照が削除されます。ただし、デフォルトでは、以降の Data Protector のアップグレードに必要になることがあるため、Data Protector 構成データ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 がインストールされていたディレクトリを削除してください。

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含まれる場合は、Data Protector をアンインストールする前にそのデータを別の場所にコピーしてください。この作業を行わなければ、アンインストール処理中にデータが削除されます。

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。「Data Protector クライアントのアンインストール」 (150 ページ) を参照してください。
2. Data Protector Cell Manager およびインストールサーバーをアンインストールします。「Cell Manager とインストールサーバーのアンインストール」 (150 ページ) 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。「Data Protector ソフトウェアコンポーネントの変更」 (156 ページ) 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。「UNIX での Data Protector ソフトウェアの手動による削除」 (155 ページ) 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ー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。

- コンピューターへの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を確認します。削除されていない場合、Data Protector は不明なシステム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システムに対応する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については、『HP Data Protector ヘルプ』の索引「バックアップ仕様の変更」の内容を参照してください。
- アンインストールを行うシステムで、バックアップデバイスやディスクアレイが接続および構成されていないことを確認します。システムのエクスポートが完了すると、Data Protector は元のセル内のバックアップデバイスやディスクアレイを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ー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] コンテキストに切り替えます。
2. Scoping ペインで [クライアント] を展開し、アンインストール対象のクライアントを右クリックした後、[削除] をクリックします。Data Protector ソフトウェアをアンインストールするかどうかを尋ね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 構成データはクライアントシステムに残ります。構成データを削除するには、Data Protector がインストールされていたディレクトリを削除してください。

クラスタークライアント

Data Protector 環境内にクラスター対応クライアントがあり、それらをアンインストールする場合は、アンインストールをローカルに実行する必要があります。アンインストール手順は、Cell Manager およびインストールサーバーのアンインストール手順と同じです。「Cell Manager とインストールサーバーのアンインストール」 (150 ページ) を参照してください。

選択したクラスタークライアントが [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。エクスポート後に Data Protector クライアントをノードからアンインストールします。

HP 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ーを使用してリモートで削除することはできません。ローカルにアンインストールする必要があります。

OpenVMS システムから Data Protector クライアント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. まず、「セルからのクライアントのエクスポート」 (133 ページ) の手順に従って、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どう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. 実際の Data Protector クライアントソフトウェアを削除するには、OpenVMS クライアントの `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.` プロンプトに対して `YES` を選択します。

重要: これで Data Protector サービスが停止され、OpenVMS システムの Data Protector に関連付けられたすべてのディレクトリ、ファイル、およびアカウントが削除されます。

Cell Manager とインストールサーバーのアンインストール

ここでは Data Protector Cell Manager とインストールサーバーソフトウェアを Windows、HP-UX、Linux 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

Microsoft サーバークラスターからのアンインストール

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 セッションが終了され、GUI が閉じていることを確認します。
2. Windows の [コントロールパネル] で **[プログラムの追加と削除]** をクリックします。
3. 構成データをシステム上に残しておくかどうかによって、実行する作業が異なります。

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、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。

- Data Protector をアンインストールして、Data Protector の構成データをシステム上に残しておく場合は、**[HP Data Protector 8.00]** 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 構成データを削除するには、**[HP Data Protector 8.00]** を選択して、**[変更]**、**[次へ]** の順にクリックします。[プログラムの保守] ダイアログボックスで、**[削除]** を選択します。**[環境設定を削除]** を選択し、**[次へ]** 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。

HP-UX システムからのアンインストール

HP-UX 用の Cell Manager は、`omnisetup.sh` コマンドを使用して、常にローカルにインストールされます。したがって、`swremove` ユーティリティを使用して、ローカルでアンインストールする必要があります。

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。

前提条件

- インストール済みの Data Protector パッチバンドルがある場合、`omnisetup.sh -bundlerem` コマンドで削除します。「UNIX システムでの Data Protector パッチバンドルのインストールと削除」 (147 ページ) を参照してください。

手順

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ー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、`omnisv -stop` 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チェックします。`ps -ef | grep omni` の実行後、Data Protector プロセスはリストされなくなります。

   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` *`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` コマンドを実行して、Data Protector ソフトウェアを削除します。

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、「UNIX での Data Protector ソフトウェアの手動による削除」 (155 ページ) 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ーのアンインストール

MC/ServiceGuard クラスター上に Cell Manager やインストールサーバー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` *`PackageName`*

   `PackageName` には、クラスターパッケージの名前を指定します。

   たとえば、次のように入力します。

   `cmhaltpkg ob2cl`
2. ボリュームグループのクラスター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. 共有ディスクのマウントを解除します。

   `umount` *`shared_disk`*

たとえば、次のように入力します。

```
umount /omni_shared
```

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
```

たとえば、次のように入力します。

```
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。

```
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
```

たとえば、次のように入力します。

```
rm -rf /omni_shared/etc_opt_omni
rm -rf /omni_shared/etc_opt_omni
```

8. 共有ディスクのマウントを解除します。

```
umount shared_disk
```

9. 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。

Linux システムからのアンインストール

前提条件

- インストール済みの Data Protector パッチバンドルがある場合、`omnisetup.sh -bundlerem` コマンドで削除します。「UNIX システムでの Data Protector パッチバンドルのインストールと削除」 (147 ページ) を参照してください。

Cell Manager

Linux 用の Cell Manager は、`omnisetup.sh` コマンドを使用して、常にローカルでインストールされています。. したがって、`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する必要があります。

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 コンポーネントを一覧表示します。

   Cell Manager に関連するコンポーネントは以下のとおりです。

OB2-CORE	Data Protector のコアソフトウェア
OB2-TS-CORE	Data Protector コアテクノロジスタックライブラリ
OB2-CC	Cell Console ソフトウェア。これには、コマンドラインインタフェースが含まれます。
OB2-TS-CS	Cell Manager テクノロジスタックライブラリ
OB2-TS-JRE	Data Protector で使用する Java ランタイム環境。
OB2-TS-AS	Data Protector アプリケーションサーバー
OB2-WS	Data Protector Web サービス
OB2-JCE-DISPATCHER	ジョブコントロールエンジンのディスパッチャー
OB2-JCE-SERVICEREGISTRY	ジョブコントロールエンジンサービスのレジストリ
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。
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 ドキュメントサブプロダクト (PDF 形式との Data Protector ガイドと WebHelp 形式の『HP Data Protector ヘルプ』を収録)

   システム上に Data Protector クライアントやインストールサーバーが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表示されます。

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 コンポーネントを削除しないでください。これは、他のコンポーネント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コンポーネントを削除します。`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ー

UNIX 用のインストールサーバーは Linux で、`omnisetup.sh` コマンドを使用して、常にローカルにインストールされています。. したがって、`rpm` ユーティリティを使用して、ローカルでアンインストールする必要があります。

Data Protector インストールサーバー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 セッションが終了され、GUI が閉じていることを確認します。
2. `rpm -qa | grep OB2` コマンドを入力すると、インストールサーバーシステム上の Data Protector コンポーネントとリモートインストールパッケージがすべて一覧表示されます。

   インストールサーバーに関連するコンポーネントとリモートインストール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。インストールサーバーを Cell Manager システムに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-TS-CORE	Data Protector コアテクノロジスタックライブラリ
OB2-CORE-IS	インストールサーバーのコアソフトウェア
OB2-CFP	すべての UNIX プラットフォームに共通のインストールサーバーコアソフトウェア
OB2-TS-CFP	すべての UNIX プラットフォームに共通のインストールサーバーテクノロジスタックソフトウェア
OB2-DAP	すべての UNIX プラットフォーム用の Disk Agent リモートインストールパッケージ
OB2-MAP	すべての UNIX システム用の Media Agent リモートインストールパッケージ
OB2-NDMPP	NDMP Media Agent コンポーネント
OB2-CCP	すべての UNIX プラットフォーム用の Cell Console リモートインストールパッケージ

   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。

   全コンポーネントのリストおよびそれぞれの依存関係については、「Linux 上の Data Protector ソフトウェアコンポーネントの依存関係」 (157 ページ) を参照してください。

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 コンポーネントを削除しないでください。これは、他のコンポーネント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コンポーネントを削除します。`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 での Data Protector ソフトウェアの手動による削除

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。手順は、「セルからのクライアントのエクスポート」 (133 ページ) 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。

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
```

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
```

その他の UNIX システムおよび Mac OS X システム

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 ソフトウェアコンポーネントを Windows、HP-UX、Solaris、Linux システムで削除および追加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 Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。

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で追加できます。インストールサーバー機能を使用して、選択されたコンポーネントをリモートでインストールします。詳細な手順については、「リモートインストール」 (70 ページ) を参照してください。

Data Protector コンポーネントは、Cell Manager、インストールサーバー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、**[**プログラムの追加と削除**]** を開きます。
2. **[HP Data Protector 8.00]** を選択し、**[**変更**]**をクリックします。
3. **[**次へ**]** をクリックします。

4. [プログラムの保守] ウィンドウで [変更] をクリックして [次へ] をクリックします。
5. [カスタムセットアップ] 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、または削除するコンポーネントを選択解除します。[次へ] をクリックします。
6. [インストール] 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、[完了] をクリックします。

クラスター対応クライアント

クラスター対応クライアントで Data Protector ソフトウェアコンポーネントを変更する場合は、各クラスターノードで DVD-ROM を使用してローカルに変更する必要があります。変更後、GUI を使用して、Data Protector セルに仮想サーバーホスト名を手動でインポートする必要があります。

HP-UX システムの場合

インストールサーバー機能を使用して新しいコンポーネントを追加できます。

コンポーネントを削除するには、`swremove` コマンドを使用します。

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` ユーザーとしてログインし、`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。
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他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 Server 固有の問題

Oracle サーバー上の Data ProtectorOracle 用統合ソフトウェアをアンインストールしても、Oracle サーバーソフトウェアの Data Protector データベースライブラリへのリンクはそのまま残ります。このリンクを削除しなければ、Oracle 用統合ソフトウェアを削除した後に Oracle サーバーを起動できません。詳細は、『HP Data Protector インテグレーションガイド - Oracle、SAP』を参照してください。

Linux システムの場合

インストールサーバー機能を使用して新しいコンポーネントを追加できます。Linux システムでは、一部の Data Protector コンポーネントが相互に依存しているため、コンポーネントを削除すると他のコンポーネントが正常に動作しなくなる可能性があります。コンポーネントとその依存関係を、次の表に示します。

表 8 Linux 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
Cell Manager	
OB2-CC, OB2-DA, OB2-MA, OB2-DOCS	OB2-CORE, OB2-TS-CORE
OB2-CS	OB2-CORE, OB2-TS-CORE, OB2-CC

表 8 Linux 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-TS-CS, OB2-TS-JRE, OB2-TS-AS, OB2-WS, OB2-JCE-DISPATCHER, OB2-JCE-SERVICEREGISTRY	OB2-CORE, OB2-TS-CORE, OB2-CC
インストールサーバー	
OB2-CORE-IS	OB2-CORE
OB2-CF-P, OB2-TS-CFP	OB2-CORE-IS
OB2-CCP, OB2-DAP, OB2-MAP, OB2-NDMPP, OB2-AUTODRP, OB2-DOCSP, OB2-CHSP, OB2-FRAP, OB2-JPNP, OB2-INTEGP, OB2-VMWP, OB2-VMWAREGRE-AGENTP, OB2-SODAP, OB2-TS-PEGP	OB2-CORE-IS, OB2-CF-P, OB2-TS-CFP
OB2-DB2P OB2-EMCP OB2-INFP OB2-LOTP OB2-OR8P OB2-SAPDP OB2-SAPP OB2-SSEAP OB2-SYBP	OB2-INTEGP, OB2-CORE-IS, OB2-CF-P, OB2-TS-CFP
OB2-SMISP	OB2-CORE-IS, OB2-CF-P, OB2-TS-CFP, OB2-TS-PEG-P

手順

Linux システムから Data Protector コンポーネントを削除するには、以下の手順を実行します。

1. すべての Data Protector セッションが終了され、GUI が閉じていることを確認します。
2. `rpm | 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 コンポーネントを一覧表示します。
3. ステップ 2で挙げたコンポーネントを、インストールとは逆の順序で削除します。`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。

その他の UNIX システムの場合

HP-UX または Linux 以外の UNIX システムで Data Protector クライアントからコンポーネントを手動で削除する場合は、 `/usr/omni/bin/install` の `omni_info` ファイルを更新します。

削除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。

コンポーネントを Data Protector クライアントから削除し、クライアントがセルからエクスポートされていない場合は、`cell_info`ファイル (Cell Manager 上) のセル構成を更新する必要があります。セル構成を更新するには、セル内の Cell Console がインストールされているシステムで以下のコマンドを実行します。

```
omnicc -update_host HostName
```

4 Data Protector 8.00 へのアップグレード

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 8.00 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外のプラットフォームとバージョンについては、http://support.openview.hp.com/selfsolve/manuals および『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』にある最新のサポート一覧を参照してください。

  Cell Manager のサポート対象外になったプラットフォームについては、まずサポート対象プラットフォームに Cell Manager を移行してから Data Protector 8.00 にアップグレードします。詳細については、「Cell Manager の異なるプラットフォームへの移行」を参照してください。

  Data Protector 8.00 では、Data ProtectorJava グラフィカルユーザーインタフェースはサポート対象外の機能領域として提供されなくなりました。Data Protector Java グラフィカルユーザーインタフェースがインストールされている Data Protector セル内に UNIX システムが存在する場合、Data Protector セルのアップグレード中に Data Protector グラフィカルユーザーインタフェースクライアントの役割を果たすように、UNIX システム以外のシステムを選択する必要があります。これらのクライアントは、元の (ネイティブ)Data Protector グラフィカルユーザーインタフェースによってサポートされているオペレーティングシステム上で実行する必要があります。

- Data Protector 8.00 では、エンタープライズ環境における拡張性のニーズに対応した新しい内部データベース (IDB) が導入されました。その結果、IDB 構造、システム要件 (ディスクスペース、ユーザー権限など)、およびプラットフォームサポートに変更が加えられました。『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』および「UNIX 用 Cell Manager のインストール」 (27 ページ) に記載されている要件を確認してください。
- アップグレード後は、Cell Manager、およびインストールサーバー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 の Disk Agent および Media Agent の古いバージョンは同一セル内ではサポートされていますが、Data Protector コンポーネントのバージョンが同じクライアントをインストールすることを強くお勧めします。

  アップグレード後の古いバージョンの Disk Agent および Media Agent による制限事項については、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。

- 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.06.00、Data Protector A.06.10、または Data Protector A.06.11 の恒久ライセンスを取得している場合は、 その恒久ライセンスを Data Protector 8.00 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。

  Data Protector 8.00 からは、新しく生成されるすべてのパスワードは新しいライセンス技術に基づいており、暗号化が強化され、パスワードキーが長くなっています。新しいライセンスは、Data Protector の前のバージョンでは使用できません。既存のライセンスパスワードは新しい形式に移行されません。

ライセンスの詳細は、「Data Protector ライセンス」 (183 ページ) 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。
- フォーマットの変更により、新しい IDB にはより多くのディスクスペースが必要になりました。アップグレード場合は事前に、ディスクに十分な空き容量があることを確認してください。（「IDB 変換期間および IDB サイズと構造の変更」 (169 ページ) を参照）。
- アップグレードプロセス中に IDB をエクスポートできるようにするために、既存の Data Protector のインストールを使用できるようにし、IDB サービスまたは少なくとも Raima Database Server (RDS) サービスを稼働させる必要があります。

制限事項

- Data Protector 8.00 へのアップグレードは、Data Protector A.06.11、Data Protector 6.20、および Data Protector 7.00 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 8.00 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。
- アップグレード中の Cell Manager プラットフォームの変更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、Linux から Linux、Windows から Windows のアップグレード)。

  お使いのプラットフォームがサポート対象外のプラットフォームである場合、まずサポートされているプラットフォームに移行してから、新しいバージョンにアップグレードします。（「Cell Manager の異なるプラットフォームへの移行」 (175 ページ) を参照）。

アップグレード手順

旧バージョンから Data Protector 8.00 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 およびインストールサーバーを Data Protector 8.00 にアップグレードします。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ー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ります。
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. Data Protector 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 と同一のプラットフォームを使用するすべての MA クライアントで MA がアップグレードされると、バックアップを実行できるようになります。
5. HP では、Data Protector 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することをお勧めします。
6. 必要に応じて、詳細カタログバイナリファイル (DCBF) を移行します。

注記: Data Protector 8.00 では Data Protector 内部データベースが変更されており、アップグレード中に自動的に移行されます。ただし、詳細カタログバイナリファイル (DCBF) はこの移行から除外されます。DC バイナリファイルの移行は時間がかかるため、セル全体をアップグレードした後に DCBF の移行を実施することをお勧めします。詳細については、「詳細カタログバイナリファイル (DCBF) の移行」 (168 ページ) 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 8.00 にアップグレードするには、まず MoM Manager システムをアップグレードする必要があります。アップグレード完了後は、アップグレードされていないすべての以前のバージョンの Cell Manager で、Central MMDB およびライセンスの集中管理にアクセスして、バックアップを実行できるようになります。ただし、その他の MoM 機能は使用できません。Data Protector 8.00 MoM セルと製品の旧バージョンがインストールされたセル間のデバイスの共有はサポートされていません。MoM 環境でのアップグレード処理中は、MoM 環境の Cell Manager がすべて非稼動状態になっている必要があります。

Data Protector A.06.11、6.20、および 7.00 からのアップグレード

Data Protector A.06.11、6.20、および 7.00 の各リリースバージョンは、UNIX および Windows プラットフォームの Data Protector に直接アップグレードできます。

ライセンス

既存の Data Protector A.06.11、6.20、7.00 ライセンスは、Data Protector 8.00 との互換性を完全に確保し、Data Protector 8.00 の使用に有効です。ライセンスの詳細は、「Data Protector ライセンス」 (183 ページ) 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、「アップグレードの概要」 (159 ページ) を参照してください。

UNIX 用 Cell Manager とインストールサーバーのアップグレード

前提条件

- インストールには、POSIX シェル (`sh`) が必要です。
- 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 または Linux インストールサーバーが 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。

HP-UX または Linux インストールサーバーが 別のシステムにインストールされている場合は、「インストールサーバーのアップグレード」 (163 ページ) を参照してください。

Cell Manager のアップグレード

HP-UX または Linux Cell Manager は、 `omnisetup.sh` コマンドの実行時に自動的にアップグレード コマンドが実行されます。

HP-UX では、このコマンドを実行すると既存のコンポーネントが `swinstall` ユーティリティを使用して直接アップグレードされます。Linux では、このコマンドを実行すると既存のコンポーネントが `rpm` ユーティリティを使用して直接アップグレードされます。

インストールサーバー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は、`omnisetup.sh` コマンドによって削除されます。この場合は、`omnisetup.sh -IS` コマンドを使用して新しいインストールサーバーデポをインストールしてから、アップグレードしたインストールサーバーを再度インポートします。詳細については、「セルへのインストールサーバーのインポート 」 (130 ページ) を参照してください。

MC/ServiceGuard

MC/SG で構成されている Cell Manager のアップグレード手順は、MC/SG 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。手順の詳細は、「MC/ServiceGuard 上で構成されている Cell Manager のアップグレード」 (177 ページ) を参照してください。

環境の準備

HP-UX システムの場合:

- カーネルパラメーター `shmmax`(共有メモリーセグメントの最大サイズ) は、2.5GB 以上に設定します。構成をチェックするには、以下のコマンドを実行します。

  ```
  kcusage shmmax
  ```

- HP は、カーネルパラメーター `maxdsiz_64`(最大データセグメントサイズ) を 134217728 バイト (128MB) 以上に設定し、カーネルパラメーター `semmnu`(セマフォのアンドゥ構造の数) を 256 以上に設定することをお勧めします。これらの変更が完了したら、カーネルを再コンパイルしシステムを再起動してください。

Linux システムの場合:

- カーネルパラメーター `shmmax`(共有メモリーセグメントの最大サイズ) は、2.5GB 以上に設定します。構成をチェックするには、以下のコマンドを実行します。

  ```
  cat /proc/sys/kernel/shmmax
  ```

アップグレード手順

HP-UX または Linux 用の Cell Manager を Data Protector 8.00 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 UNIX インストール DVD-ROM(HP-UX または Linux 用) をマウントポイントに挿入してマウントします。

   DVD-ROM ファイルシステムは Rock Ridge 拡張を使用します。

   - 必要に応じて、DVD-ROM からローカルディスクに次のディレクトリをコピーします。

     `LOCAL_INSTALL`

     `platform_dir``/DP_DEPOT`

     ここで、*`platform_dir`* には、以下のいずれかの値を指定します。

`hpux`	HP-UX システムの場合
`linux_x86_64`	Linux システムの場合

2. DVD-ROM の `LOCAL_INSTALL` ディレクトリ、またはローカルディレクトリに移動して、以下のコマンドを実行します。

   ```
   ./omnisetup.sh
   ```

Data Protector の A.06.11、6.20、または 7.00 バージョンの検出後に、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 (以前のバージョンのデータベースは削除されます) を実行するには、旧バージョンをアンインストールし、インストールを初めからやり直します。

インストールの詳細は、「UNIX 用 Cell Manager のインストール」 (27 ページ) および「UNIX システム用のインストールサーバーのインストール」 (38 ページ) 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 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ー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。「構成の変更のチェック」 (166 ページ) を参照してください。
- 以前のバージョンの Data Protector で作成され、Data Protector 8.00 へのアップグレード後にデフォルトで 1TB に設定されている仮想テープライブラリのライブラリ容量

(VTLCAPACITY) を、手動で調整する必要があります。「構成の変更のチェック」(166 ページ) を参照してください。

インストールサーバーのアップグレード

HP-UX または Linux インストールサーバーは、 omnisetup.sh コマンドの実行時に自動的にアップグレード コマンドが実行されます。

HP-UX では、このコマンドを実行すると既存のコンポーネントとリモートインストールパッケージが swinstall ユーティリティを使用して直接アップグレードされます。Linux では、このコマンドを実行すると既存のコンポーネントとリモートインストールパッケージが rpm ユーティリティを使用して直接アップグレードされます。

インストールサーバー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は、omnisetup.sh コマンドによって削除されます。この場合は、omnisetup.sh -IS コマンドを使用して新しいインストールサーバーデポをインストールしてから、アップグレードしたインストールサーバーを再度インポートします。詳細については、「セルへのインストールサーバーのインポート 」(130 ページ) 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ー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 または Linux 用のインストールサーバーを Data Protector 8.00 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 UNIX インストール DVD-ROM(HP-UX または Linux 用) をマウントポイントに挿入してマウントします。

   DVD-ROM ファイルシステムは Rock Ridge 拡張を使用します。

   - 必要に応じて、DVD-ROM からローカルディスクに次のディレクトリをコピーします。

     LOCAL_INSTALL

     platform_dir/DP_DEPOT

     ここで、*platform_dir* には、以下のいずれかの値を指定します。

hpux	HP-UX システムの場合
linux_x86_64	Linux システムの場合

2. DVD-ROM の LOCAL_INSTALL ディレクトリ、またはローカルディレクトリに移動して、以下のコマンドを実行します。

   ./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 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 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ー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。「構成の変更のチェック」(166 ページ) を参照してください。

Windows Cell Manager とインストールサーバーのアップグレード

Data Protector の以前のバージョンが検出されると、オペレーティングシステムでは、インストール済みのものと同じコンポーネントセットが想定されます (削除されるコンポーネントなし)。インストール済みのコンポーネントが削除され、新しいコンポーネントが新しい (クリーン) インストールとしてインストールされます。

Windows インストールサーバーが Cell Manager と同じシステム上にインストールされている場合は、Windows インストールサーバーはアップグレード手順によって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ーデポは削除され、インストール時にインストールサーバーコンポーネントが選択されている場合は、新しいインストールサーバーデポがその場所にコピーされます。

インストールサーバーが 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ーも同時にアップグレードされます。

重要: インストール手順の終了後にアップグレード済みのインストールサーバーを再度インポートします。詳細については、「セルへのインストールサーバーのインポート」 (130 ページ) を参照してください。

留意事項

- **Microsoft Cluster Server**

  Microsoft 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、Microsoft Cluster Server での使用向け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。手順の詳細は、「Microsoft Cluster Server 上で構成されている Cell Manager のアップグレード」 (180 ページ) を参照してください。

- インストールパスに以下の文字が含まれている場合は、Data Protector を直接アップグレードできません。

  - 非 ASCII 文字
  - "@ "または"# "
  - ディレクトリの末尾にある"!"
  - 80 文字を超える文字

  問題の解決策については、「長いパスが原因でアップグレードが失敗する」 (211 ページ) および 「サポートされていない文字がパスに含まれているためにアップグレードが失敗する」 (212 ページ) 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ーを Data Protector 8.00 にアップグレードするには、以下の手順に従います。

1. Windows インストール DVD-ROM をドライブに挿入し、`\Windows\x8664\setup.exe` コマンドを実行します。以前行った Data Protector インストールが検出されます。**[Next]** をクリックして、アップグレードを開始します。
2. **[Component Selection]** ページで、以前にシステムにインストールされたコンポーネントが選択されています。コンポーネントは、追加のコンポーネントを選択または選択解除することによって変更できます。選択済みのコンポーネントの説明については、ウィザードの次の手順を参照してください。**[Next]** をクリックします。
3. また、Data Protector サービスの内部データベースサービスおよびアプリケーションサーバーで使用するユーザーカウントやポートも変更できます。

   [Next] をクリックします。これらのサービスの詳細については、「インストール後の状態」 (36 ページ) を参照してください。
4. Data Protector がシステムで Windows ファイアウォールを検出した場合、[Windows Firewall configuration] ページが表示されます。Data Protector セットアップにより、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、

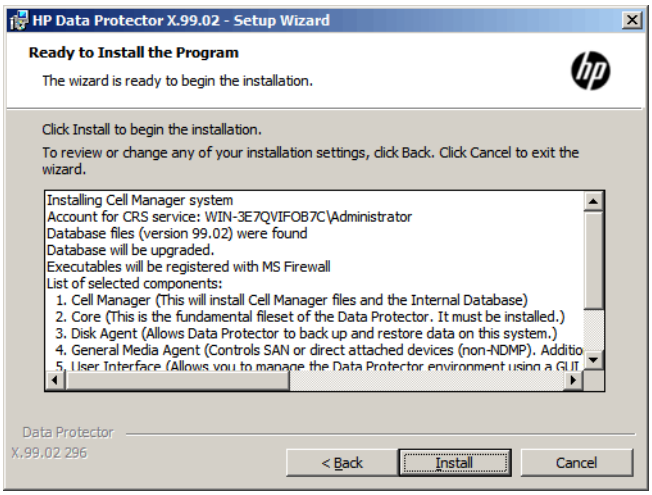
オプションを選択解除します。ただし、Data Protector を適切に機能させるには、実行可能ファイルを有効にする必要があります。

自動生成されるのはインバウンドファイアウォールルールのみであり、アウトバウンドファイアウォールルールは手動で作成する必要があるので注意してください。必要なポート範囲については、『HP Data Protector ヘルプ』の索引「ファイアウォールのサポート」で表示される内容を参照してください。

[Next] をクリックします。

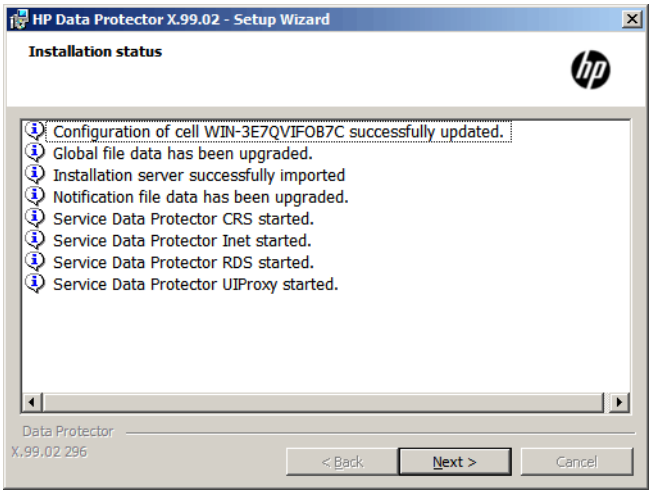
5. コンポーネントのサマリーリストが表示されます。**[Install]** をクリックして、アップグレードを開始します。

図 43 コンポーネント選択サマリーページ



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

図 44 [Installation status] ページ



7. この手順は Cell Manager のアップグレード時にのみ実行されます。Cell Manager 以外のクライアントにインストールされているインストールサーバーをアップグレードする場合は、この手順は発生しません。

ユーザーインターフェースコンポーネントをアップグレードしたか、新しくインストールした場合に、セットアップ直後に Data Protector GUI を使用して操作を開始するには **[Launch Data Protector GUI]** を選択します。

英語版ドキュメント（ガイド、ヘルプ）コンポーネントをアップグレードしたか、または新しくインストールした場合に、セットアップ直後に『HP Data Protector 製品案内、ソフ

トウェアノートおよびリファレンス』を表示するには、**[Open the Product Announcements, Software Notes, and References]** を選択します。

8. **[Finish]** をクリックします。
9. `omnisv -start` コマンドを実行してサービスを再起動します。

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ー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。「構成の変更のチェック」(166 ページ) を参照してください。
- 以前のバージョンの Data Protector で作成され、Data Protector 8.00 へのアップグレード後にデフォルトで 1TB に設定されている仮想テープライブラリのライブラリ容量 (VTLCAPACITY) を、手動で調整する必要があります。「構成の変更のチェック」(166 ページ) 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

アップグレード時には、UNIX Cell Manager では `/etc/opt/omni/server/options` ディレクトリまたは Windows Cell Manager では *`Data_Protector_home`*`\Config\server\Options` ディレクトリに存在する**古い**グローバルオプションファイルのコンテンツが Cell Manager 上の**新しい (デフォルト)** グローバルオプションファイルのコンテンツとマージされます。

Windows システムの場合: *`Data_Protector_program_data`*`\NewConfig\Server\Options`

UNIX システムの場合: `/opt/omni/newconfig/etc/opt/omni/server/options`

`global` という名前が付いた**マージ後の**ファイルは、古いファイルと同じ場所にある *`Data_Protector_program_data`*`\Config\server\Options` ディレクトリ (Windows システムの場合)、または `/etc/opt/omni/server/options` ディレクトリ (UNIX システムの場合) に置かれ、アップグレードされたバージョンの製品によって使用されます。**古い**グローバルオプションファイルの名前は、実行されたアップグレード数に応じて `global.1`、`global.2`...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。

- 古いファイルでアクティブ (コメント解除) だったグローバルオプションファイルは、マージ後のファイルでもアクティブなままとなります。古いファイルからオプションの値がコピーされたことを示す以下のコメントがマージファイルに付加されます。

  ```
  Option=Value
  # Data Protector 8.00
  # This value was automatically copied from previous
  ```

- 使用されなくなったグローバルオプションは、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、そのオプション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。

  ```
  #Option=Value # Data Protector 8.00
  # This value is no longer in use.
  ```

- サポート対象外となった値を持つグローバルオプションについては、マージファイルにコメント (非アクティブ化) が付加されます。テンプレート行 (*`DefaultValue`*) を含み、このオプションの以前の値を示す以下のコメントが付加されます。

  ```
  # Option=DefaultValue # # Data Protector 8.00
  # This variable cannot be transferred automatically.
  # The previous setting was:
  # Option=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。

新しいオプションについての説明は、マージ後のグローバルオプションファイルに含まれています。グローバルオプションの詳細は、『HP Data Protector トラブルシューティングガイド』を参照してください。

手動で行う作業

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動で行う必要がある作業をまとめたものです。

- Omnirc オプション

  Cell Manager およびインストールサーバーシステムのアップグレード後は、`omnirc` ファイルを編集することもできます。詳細な手順については、『HP Data Protector トラブルシューティングガイド』および『HP Data Protector ヘルプ』の「『omnirc オプションの使用方法』」を参照してください。

- コマンドライン

  Data Protector コマンドを呼び出すスクリプトについては、調整が必要になる場合があります。

  - Data Protector 8.00 で新たに導入されたコマンド、変更されたまたは機能が拡張されたコマンド、使用できなくなったコマンドの一覧については、「Data Protector 8.00 へのアップグレード後のコマンドラインの変更」(255 ページ) を参照してください。コマンドの使用法については、『HP Data Protector Command Line Interface Reference』または該当する man ページを参照してください。

  - Data Protector 8.00 では、`omnidbrestore` コマンドは、同じ機能を提供する、拡張された `omnioffl r` コマンドに置き換えられています。`omnidbrestore` コマンドラインを `omnioffl r` コマンドラインで置き換えるまでは、便宜のために提供されている `omnidbrestore.pl` スクリプトを使用できます。このスクリプトは、`omnioffl r` と同じオプションセットを認識します。スクリプトを実行する場合、次の形式で指定する必要があります。*`OMNIOFFLR_OPTIONS`* は、`omnioffl r` コマンドのオプションです。ただし、`-idb` オプションはありません。

    Windows システムの場合:

    `perl omnidbrestore.pl` *`OMNIOFFLR_OPTIONS`*

    UNIX システムの場合:

    `omnidbrestore.pl` *`OMNIOFFLR_OPTIONS`*

- `hosts` ファイルに、`computer.company.com` 形式の完全修飾ドメイン名 (FQDN) が含まれていることを確認します。必要に応じて、適切にファイルを更新します。ファイルは次の場所に配置されます。

  Windows システムの場合: *`%SystemRoot%`*`\system32\drivers\etc\`

  UNIX システムの場合: `/etc/hosts`

- 変更されたバックアップデバイスのデフォルトブロックサイズ

  Data Protector 8.00 のデバイス構成ウィザードでは、物理バックアップデバイスおよびその他のデバイスの種類のデフォルトブロックサイズが大きくなっていることに留意してください。オブジェクトのコピーやオブジェクトのミラーリング、オブジェクト集約などの特定の用途では、バックアップデバイスブロックサイズを慎重に選択する必要があります。Data Protector 8.00 のデフォルトブロックサイズで構成されたデバイスは、製品の旧バージョンのデフォルトブロックサイズで構成されたデバイスと併用したときに、このような用途の要件を満たさない場合があります。

内部データベースの変換されない部分

アップグレードを効率的に実行するために、Data Protector 8.00 のアップグレード処理では、内部データベースの特定の部分が新しい形式に自動的にアップグレード(変換)されません。変

換されない部分は新しい製品バージョンでも頻繁に使用されます。IDB のこれらの部分を構成するファイルは以下のディレクトリにあります。

Windows システムの場合: *Data_Protector_program_data*\db40

UNIX システムの場合: /var/opt/omni/server/db40

上記のディレクトリは、以下のいずれかの状態になるまで Data Protector 8.00 で引き続き使用されます。

- アップグレード時に、製品の旧バージョンの DCBF で参照されていたすべてのバックアップデータのカタログ保護が期限切れになる。
- omnimigrate.pl コマンドを使用してレガシー DCBF の新しい形式への移行を開始する。

  詳細は、「詳細カタログバイナリファイル (DCBF) の移行」 (168 ページ) を参照してください。

△ **注意:** 上記で説明したディレクトリは手動で削除しないでください。手動で削除すると、データが消失する場合があります。

この次に行う作業

Cell Manager およびインストールサーバーをインストールし、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することをお勧めします。「クライアントのアップグレード」 (170 ページ) を参照してください。

Data Protector 8.00 へのアップグレード後の内部データベースの変更

Data Protector 8.00 では、Data Protector 7.00 以前のバージョンとは大幅に異なる新しい内部データベース (IDB) が導入されています。新しい IDB には、IDB 構造、サイズ、操作の面でさまざまな変更が加えられました。これにより、IDB の変換後に IDB の一部を移行しなければならない場合があります。

詳細カタログバイナリファイル (DCBF) の移行

アップグレード後、Data Protector は完全に稼働状態となります。ただし、保存期限内のカタログを持つすべてのオブジェクトや、アップグレード前にバックアップされたカタログを持つすべてのオブジェクトのカタログは、古い形式で保存されています。カタログの期限が切れると、古い DC バイナリファイルは (日常の保守作業により) 自動的に削除されます。ただし、古いデータベースファイルは、保護されている古いカタログファイルのファイル名があるかぎり維持され、ディスクスペースを占有し続けます。

Data Protector は、古い DC バイナリファイルと IDB ファイルを必要とする保護されたメディア、オブジェクト、セッション、およびその占有スペース量を特定するのに役立ち、またイベントログにレポート (警告) を書き込みます。CLI から以下のコマンドを実行して、手動でレポートを実行することもできます。

```
omnimigrate.pl -report_old_catalog [media | sessions | objects]
```

永続的に保護されたオブジェクト、メディア、セッションのカタログは期限切れとならないので、手動で移行する必要があります。

ヒント: 移行にはかなりの時間がかかる可能性があります。したがって、ほとんどの古いメディアの期限が切れるまで待ち、永続的に保護されたメディアのみを移行することをお勧めします。

カタログファイルを移行するには、以下のコマンドを実行します。

```
omnimigrate.pl -start_catalog_migration
```

変換期間とスペース要件の見積もりについては「IDB 変換期間および IDB サイズと構造の変更」 (169 ページ) を参照してください。

重要: アップグレードが完了したら、IDB をバックアップします。古い IDB バックアップは Data Protector 8.00 では使用できません。

IDB 変換期間および IDB サイズと構造の変更

アップグレードプロセス中に、IDB は新しい形式に変換されます。変換期間は、既存のデータベースのサイズと複雑さ、ご使用のハードウェアの性能によって異なります。以下の例は、ご使用の環境では異なることがあるので注意してください。

IDB 移行後の IDB のサイズ

新しい IDB のサイズは、元の IDB のサイズと構造によって異なるため、新しい IDB のサイズを正確に予測することは不可能です。中規模データベースの場合、テスト中では十分なスペースとして考えられるのは 1 GB です。インストール時に、使用可能なスペースとしてさらに 1 GB があるかどうかがチェックされ、このスペースがない場合は警告が表示されます。大規模データベースを移行する場合、これより多くの空きスペースが必要になるでしょう。

詳細カタログバイナリファイルの移行

Data Protector 8.00 では DCBF のフォーマットが変更され、DCBF にファイルのバージョン情報が含まれるようになりました。さらに、新しい DCBF のスペースの要件も変更されました。

ファイル名が DCBF 内に格納されるようになったため、DCBF のサイズは大きくなっています。したがって、新しいサイズを正確に予測することはできません。しかし、おおよその目安として、約 4 倍のサイズになります。以下の表に、いくつかの変換例を示します。

古い DCBF サイズ	24 MB	48.4 MB	97.3 MB
アップグレード期間 (分:秒)	1:51	3:33	6:13
新しい DCBF サイズ	90.6 MB	181 MB	417 MB

サーバーレス統合バイナリファイルの移行

アップグレード処理中に、サーバーレス統合バイナリファイル (SIBF) 内のデータは IDB のカタログデータベース (CDB) 部分に移動し、一体化されます。したがって、IDB の SIBF 部分は不要となり、Data Protector 8.00 では以下の IDB インストールディレクトリがなくなりました。

Windows システムの場合: *Data_Protector_program_data*\server\db80\meta

UNIX システムの場合: /var/opt/omni/server/db80/meta

レガシー NDMP メディアのインポート

UNIX ファイルシステムからバックアップされ、NDMP メディアに格納されたオブジェクトの所有権は、8.00 より前の Data Protector バージョンでは正しく処理されませんでした。レガシー NDMP メディアを Data Protector 8.00 にインポートすると、元の所有権情報がないため、このようなオブジェクトの所有権フラグは 0 0(オーナー、グループ) に設定されます。

セッション ID の序数

Data Protector 8.00 では、特定のバックアップセッションの同時処理数メトリックの制限が増えたことによって、セッション ID に 5 桁の序数が使用される場合があります。また、Data Protector デバッグメッセージでは、10 000 未満の序数にはゼロが挿入されます。たとえば、2013 年 1 月 1 日に実行された最初のバックアップセッションは、デバッグファイル内に ID 2013/01/01-0001 で記録されます。

上記の変更を考慮するために、Data Protector と連携して使用していたスクリプトを変更し、適合させる必要がある場合もあります。

クライアントのアップグレード

アップグレード手順

クライアントのアップグレード手順は「アップグレードの概要」(159 ページ)を参照してください。

リモートアップグレードまたはローカルアップグレード

リモートインストールをサポートしているプラットフォームの場合、クライアントをリモートでアップグレードすることをお勧めします。

- インストールサーバーを使用してクライアントをアップグレードする手順は、「リモートインストール」(70 ページ)を参照してください。UNIX システムでは、新しい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。新しいコンポーネントを追加すると、以前のバージョンのコンポーネントは Data Protector に表示されません。この場合は、再度インストールする必要があります。
- ネットワーク上にインストールサーバーがない場合、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 クライアントのローカルアップグレード方法は、「Windows 用クライアントのインストール」(47 ページ)を参照してください。

  UNIX クライアントのローカルアップグレード方法は、「UNIX および Mac OS X システムのローカルインストール」(76 ページ)を参照してください。

制限事項

Windows、HP-UX、および Linux システムで Data Protector A.06.11 からアップグレードする場合、拡張増分バックアップデータベースは新しいバージョンに移行されません。古い拡張増分バックアップレポジトリが、*Data_Protector_home*\enhincrdb*MountPoint* ディレクトリから削除されます。クライアントアップグレード後の最初のフルバックアップ時に、同じ場所に新しいレポジトリが作成されます。アップグレード後の最初のバックアップは、フルバックアップを実行する必要があります。

Linux クライアント

`inetd` サービスではなく `xinetd` サービスを使用している場合は、`/etc/xinetd.d/omni` ファイルは**置き換えられない**ため、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
```

設定をデフォルト設定に戻す、または破損したファイルを置き換えるには、ファイルを削除し、任意の Data Protector ソフトウェアコンポーネントを Data Protector GUI からリモートでアップグレードします。`/etc/xinetd.d/omni` ファイルがデフォルトの設定で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、変更内容は失われます。変更内容を保持するには、バックアップコピーを事前に作成しておき、アップグレードの完了後に、新しくインストールしたファイルに設定を手動で移動します。

Solaris 8 システムから Solaris 9 システムへのアップグレード

Data Protector 7.00 以降、Data Protector Disk Agent クライアントのオペレーティングシステムを Solaris 8 から Solaris 9 にアップグレードする作業はサポートされなくなりました。

Solaris 8 に旧バージョンの Data ProtectorDisk Agent (DA) がインストールされていて、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には、旧バージョンの『HP Data Protector インストールおよびライセンスガイド』の該当部分を参照してください。

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. 次のコマンドを実行して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、Microsoft ボリュームシャドウコピーサービス、または HP P6000 EVA ディスクアレイファミリ 用統合ソフトウェア、自動ディザスタリカバリモジュール、Microsoft Exchange Server、Microsoft SQL Server、HP P9000 XP ディスクアレイファミリ、または EMC Symmetrix 用統合ソフトウェアなど) 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、「Oracle 用統合ソフトウェアのアップグレード」 (171 ページ) 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、「SAP R/3 用統合ソフトウェアのアップグレード」 (172 ページ) を参照してください。
- Microsoft ボリュームシャドウコピーサービス用統合ソフトウェアのアップグレード方法の詳細は、「Microsoft ボリュームシャドウコピーサービス用統合ソフトウェアのアップグレード」 (173 ページ) を参照してください。
- HP P6000 EVA ディスクアレイファミリ 用統合ソフトウェアのアップグレード方法の詳細は、「HP P6000 EVA ディスクアレイファミリ 用統合ソフトウェアのアップグレード」 (173 ページ) を参照してください。
- Microsoft Exchange Server、Microsoft SQL Server、HP P9000 XP ディスクアレイファミリ、EMC Symmetrix 用統合ソフトウェア、またはその他の統合ソフトウェエアのアップグレード方法の詳細は、「他の統合ソフトウェアのアップグレード」 (173 ページ) 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) を実行して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 Oracle 用統合ソフトウェアエージェントをリモートでインストールしてアップグレードします。UNIX では、Cell Manager にないクライアントをアップグレードする場合に `-install oracle8` 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。

ユーザールートは不要

UNIX クライアントの場合、ユーザールートの下に Data Protector Oracle Server 用統合ソフトウェアを構成し、その構成を確認し、Oracle データベースをブラウズする必要はありません。これらの操作は、バックアップ仕様で指定したオペレーティングシステムのユーザーアカウントの下で実行されます。したがって、ユーザールートを Data Protector ユーザーグループから安全に削除できます。

注記: ZDB およびインスタントリカバリセッションの場合、ユーザールートはこれまでどおり必要です。

アップグレードした場合は、Data Protector がオペレーティングシステムのユーザー アカウント (バックアップオーナー) を、バックアップ仕様から対応する Data Protector Oracle データベース構成ファイルへとコピー中に、各 Oracle データベースの構成チェックを実行することもお勧めします。

構成チェックを実行しないと、構成ファイルは更新されません。このような場合、復元処理の実行中、Data Protector は Oracle データベースを、直前のバックアップセッションのバックアップオーナーでブラウズします。過去 3 か月間にこのようなバック アップセッションが作成されなかった場合、最後のオプションとしてルートユーザーが使用されます。

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 オプションを設定する必要があります。『HP Data Protector ゼロダウンタイムバックアップインテグレーションガイド』を参照してください。

データストレージ用に HP P6000 EVA ディスクアレイファミリ を使用した Oracle ASM の構成

自動ストレージ管理 (ASM) を使用する構成の P6000 EVA アレイ 上で、Oracle Server データの整合性のある複製の作成をサポートするためには、Oracle 用統合ソフトウェアおよび HP P6000/HP 3PAR SMI-S Agent の両方の 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でアップグレードする必要があります。

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) を実行して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 SAP R/3 用統合ソフトウェアエージェントをリモートでインストールしてアップグレードします。UNIX では、Cell Manager にない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。

SAP 対応 ZDB セッション

SAP 標準では、ZDB セッション (SAP 対応 ZDB セッション) 処理中に、BRBACKUP をバックアップシステムで開始することをお勧めします。Data Protector 8.00 を使用すると、これらの標準に対応できます。まず、バックアップシステムを Oracle 用の SAP ガイドの説明に従って構成し (スプリットミラーバックアップ、ソフトウェア構成)、Data Protector `SAP R/3 Integration` コンポーネントをバックアップシステムにインストールします。それから、『HP Data Protector ゼロダウンタイムバックアップインテグレーションガイド』の説明に従って SAP 対応 ZDB セッション用に Data Protector を構成します。

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、以下の 3 つのオプションがあります。

- Oracle インスタンスを再構成します。
- `ZDB_ORA_INCLUDE_CF_OLF`、`ZDB_ORA_INCLUDE_SPF`、および `ZDB_ORA_NO_CHECKCONF_IR` omnirc オプションを設定します。
- BRBACKUP をバックアップシステム (SAP 対応 ZDB セッション) で開始するよう Data Protector を構成します。

詳細は、『HP Data Protector ゼロダウンタイムバックアップインテグレーションガイド』を参照してください。

Microsoft ボリュームシャドウコピーサービス用統合ソフトウェアのアップグレード

HP Data Protector HP A.06.11、HP Data Protector 6.20、または Data Protector 7.00 からのアップグレード後のインスタントリカバリが有効なバックアップセッション

VSS 用統合ソフトウェアを Data Protector の古いバージョンからアップグレードした後、ディスクへの ZDB セッションおよびディスク/テープへの ZDB セッションを実行する場合は、アプリケーションシステム上のソースボリュームを解決する必要があります。この処理を実行しないと、ディスクへの ZDB セッションは失敗し、ディスク/テープへの ZDB セッションはディスクアレイに複製を維持しないテープへのバックアップでのみ完了します。セルの VSS クライアントからの解決操作は、以下のように実行します。

```
omnidbvss -resolve {-apphost ApplicationSystem | -all}
```

詳細は、『HP Data Protector ゼロダウンタイムバックアップインテグレーションガイド』を参照してください。

HP P6000 EVA ディスクアレイファミリ 用統合ソフトウェアのアップグレード

留意事項

- 6.20 より古いバージョンの Data Protector を Data Protector 8.00 にアップグレードする場合、P6000 EVA アレイ での複製作成に適用する**緩和**スナップショットポリシーは、Data Protector バージョン 6.20 からサポートの対象外になっているので注意してください。このディスクアレイに関するすべての ZDB セッションは、暗黙的に**厳格**スナップショットポリシーを使用します。アップグレード後に**緩和**スナップショットポリシーを使用する ZDB セッションが実行された場合は、警告が報告され、**厳格**スナップショットポリシーが代わりに使用されますが、ZDB バックアップ仕様自体は更新されません。このような警告を回避するためには、上記のような ZDB バックアップ仕様を手動で更新する必要があります。

  ZDB バックアップ仕様を手動で更新して暗黙的に**厳格**スナップショットポリシーを使用するには、Data Protector GUI でバックアップ仕様を開き、そのオプションのいずれかを変更してから元に戻し、最後に [適用] をクリックしてバックアップ仕様を保存します。

  P6000 EVA アレイ 上での複製作成のスナップショットポリシーについては、『HP Data Protector ゼロダウンタイムバックアップ管理者ガイド』と『HP Data Protector ヘルプ』を参照してください。

仮想環境統合ソフトウェアのアップグレード

Data Protector 仮想環境統合ソフトウェアコンポーネントを Data Protector 6.20 以前のバージョンからアップグレードする場合、新しいコンポーネントを対応するクライアントにインストールした後で次のコマンドを実行します。

```
vepa_util.exe --upgrade-cell_info
```

これは、`cell_info` ファイルのパスワードエンコーディングの変更のために必要です。これにより、まず `cell_info.bak` ファイルが作成され、仮想環境統合ソフトウェアが使用するパスワードが再エンコードされます。

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 Microsoft Exchange Server、Microsoft SQL Server、HP P9000 XP ディスクアレイファミリ 、EMC Symmetrix、またはその他の統合ソフトウェアがインストールされている場合は、`omnisetup.sh -install` *`component_list`* コマンド (UNIX システム)、または `setup.exe` コマンド (Windows システム) を実行してローカルにクライアントをアップグレードするか、リモートから Data Protector GUI を使用してクライアントを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、「UNIX および Mac OS X システム

のローカルインストール」(76 ページ) を参照してください。Cell Manager にない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。

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。ただし、以下の制限事項に注意してください。

制限事項

- すべての Cell Manager が Data Protector 8.00 にアップグレードされるまで、**分散ファイルメディア形式**をファイルライブラリで使用することはできません。

MoM 環境を Data Protector 8.00 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 8.00 にアップグレードします。

   アップグレード処理中は、MoM 環境内の Cell Manager が非稼動状態になければなりません。アップグレード後も、MoM Manager は古い Cell Manager と連携可能です。
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、「UNIX 用 Cell Manager とインストールサーバーのアップグレード」(161 ページ) および「Windows Cell Manager とインストールサーバーのアップグレード」(163 ページ) 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 8.00 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。

シングルサーバー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ー版 (SSE) から Data Protector 8.00 シングルサーバー版へ。詳細については、「旧バージョンの SSE から Data Protector 8.00 SSE へのアップグレード」(174 ページ) を参照してください。
- Data Protector 8.00 シングルサーバー版から Data Protector 8.00 へ。詳細については、「Data Protector 8.00 SSE から Data Protector 8.00 へのアップグレード」(174 ページ) を参照してください。

旧バージョンの SSE から Data Protector 8.00 SSE へのアップグレード

旧バージョンの SSE から Data Protector 8.00 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 8.00 へのアップグレード手順と同じです。詳細は、「Data Protector A.06.11、6.20、および 7.00 からのアップグレード」(161 ページ) を参照してください。

Data Protector 8.00 SSE から Data Protector 8.00 へのアップグレード

ライセンス

Data Protector 8.00 シングルサーバー版から Data Protector 8.00 にアップグレードするには、ライセンスが必要です。ライセンスの詳細は、「Data Protector ライセンス」(183 ページ) を参照してください。

Data Protector 8.00 シングルサーバー版から Data Protector 8.00 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 シングルサーバー版を 1 つのシステム (Cell Manager) にのみインストールしている場合。「Cell Manager のアップグレード」(175 ページ) を参照してください。

- Data Protector シングルサーバー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する場合。「複数のシステムからのアップグレード」(175 ページ)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ー版を Data Protector のフルインストール版にアップグレードするには、最初にシングルサーバー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 8.00 にアップグレードする方法は、「Data Protector A.06.11、6.20、および 7.00 からのアップグレード」(161 ページ)を参照してください。

Cell Manager のアップグレード

シングルサーバー版の 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. 次のコマンドを実行して、シングルサーバー版のライセンスを削除します。

   Windows システムの場合:

   ```
   del Data_Protector_program_data\Config\server\Cell\lic.dat
   ```

   UNIX システムの場合:

   ```
   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 シングルサーバー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ー版システムのうち、新しい Cell Manager となるシステムを 1 つ選択します。「Cell Manager システムの選択」(23 ページ)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. 次のコマンドを実行して、シングルサーバー版のライセンスを削除します。

      `del Data_Protector_program_data\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ー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 シングルサーバー版をアンインストールします。「Data Protector ソフトウェアのアンインストール」(149 ページ)を参照してください。
5. 新しい Cell Manager にメディアをインポートします。

   メディアのインポートの詳細については、『HP Data Protector ヘルプ』の検索キーワード「インポート、メディア」を参照してください。

Cell Manager の異なるプラットフォームへの移行

PA-RISC HP-UX システムから Intel Itanium HP-UX システムへの移行

Data Protector 8.00 では、PA-RISC アーキテクチャーベースの HP-UX 11.11/11.23 システムは、Cell Manager プラットフォームとしてサポートされなくなりました。したがって、アップグレードの**前に**、Cell Manager を PA-RISC アーキテクチャーベースの HP-UX 11.11/11.23 システムから Intel Itanium 2 アーキテクチャーの HP-UX 11.23/11.31 システムに移行する必要があります。

移行の手順については、適切な製品バージョンの『HP Data Protector インストールおよびライセンスガイド』を参照してください。

32 ビット/64 ビット Windows から 64 ビット Windows/Windows Server 2008 への移行

Data Protector 8.00 では、32 ビット Windows システムを Cell Manager プラットフォームとしてサポートしなくなりました。したがって、Data Protector 8.00 へのアップグレード手順を開始する**前に** 64 ビット Windows システムに Cell Manager を移行する必要があります。移行の手順については、適切な製品バージョンの『HP Data Protector インストールおよびライセンスガイド』を参照してください。

Solaris から Linux への移行

この項では、Solaris システムから Linux システムに既存の Cell Manager を移行する手順を説明します。

重要: Data Protector 8.00 では、Cell Manager プラットフォームとして Solaris をサポートしなくなりました。したがって、Data Protector 8.00 へのアップグレード手順を開始する**前に**、インストールされた Data Protector バージョンを使用して新しいプラットフォームに Cell Manager を移行する必要があります。

手順

1. 既存の Data Protector インストールを使用して、以下の手順を実行して現在の Cell Manager 上のすべてのメディアカタログをエクスポートします。
   a. コンテキストリストで [デバイス/メディア] をクリックします。
   b. Scoping ペインで [メディア] を展開してから、[プール] を展開します。
   c. カタログをコピー対象にするメディアのメディア プールを展開します。
   d. メディアを選択して右クリックして、[カタログをファイルにコピー] をクリックします。
   e. MCF ファイルの出力ディレクトリを指定します。MCF ファイルにメディア関連カタログ データが含まれます。
   f. [完了] をクリックして、ウィザードを終了します。これにより、コピー処理が開始します。詳細については、『HP Data Protector ヘルプ』トピックの「『MCF ファイルにカタログメディアデータをコピーする』」を参照してください。
2. 新しい Cell Manager になる Linux システム上に、Data Protector をインストールします。詳細については、「UNIX 用 Cell Manager のインストール」 (27 ページ) を参照してください。
3. 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。「デフォルトの Data Protector Inet ポートの変更」 (227 ページ) を参照してください。
4. 新しい Cell Manager に MCF ファイルをインポートするには、以下の手順に従ってください。
   a. コンテキストリストで [デバイス/メディア] をクリックします。
   b. Scoping ペインで [メディア] を展開して [プール] を右クリックし、[カタログを **MCF** ファイルからインポート] をクリックして、ウィザードを起動します。
   c. インポート対象の MCF ファイルを指定します。
   d. セッションに適用するその他のオプションを指定します。デフォルトで、[可能ならば元のプールにインポート] オプションが選択されます。[コピーをオリジナルとしてインポート] オプションを選択します。
   e. [完了] をクリックして、ウィザードを終了します。これによって、インポート処理が開始されます。

   詳細については、『HP Data Protector ヘルプ』のトピック「『MCF ファイルからカタログメディアデータをインポートする』」を参照してください。
5. 新しい Cell Manager 上でライセンスを構成します。「Data Protector 8.00 の製品構成とライセンス」 (199 ページ) を参照してください。

6. 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。「MoM 固有の手順」 (177 ページ) 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 上にファイアウォールに関連するすべての設定を再構成します。『HP Data Protector ヘルプ』の索引「ファイアウォール環境」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ーを配置する場合。「インストールサーバー 固有の手順」 (177 ページ) を参照してください。

移行が完了したら、Data Protector をアップグレードできます。

MoM 固有の手順

新しい Cell Manager を MoM 構成にする場合、基本的な移行手順が完了した後、さらに手順を実行する必要があります。必要な手順は、環境における新旧の 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ています。

- 古い Cell Manager は MoM クライアントでした。新しい Cell Manager は同じ MoM Manager の MoM クライアントになります。

  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。『HP Data Protector ヘルプ』の索引「クライアントシステムのエクスポート」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。『HP Data Protector ヘルプ』の索引「MoM 管理者、追加」を参照してください。

- 古い Cell Manager は MoM Manager でした。新しい Cell Manager は MoM Manager になります。

  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。それ以外の場合は、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ー 固有の手順

インストールサーバーの移行は Cell Manager の移行の一部として行われません。古い Cell Manager 上にインストールサーバーをインストールしている場合は、インストールサーバーが新しい Cell Manager に移行されずにセルに残ります。

新しい Cell Manager もインストールサーバーとしても使用する場合は、移行後に新しい Cell Manager 上にインストールサーバー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。『HP Data Protector ヘルプ』の索引「" インストールサーバー "」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、以前のバージョンの製品は削除されます。Data Protector 8.00 は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する場合は、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。

前提条件

- MC/ServiceGuard の二次ノード上の Data Protector サービスは実行しないでください。
  これにより、アップグレードは一次ノードのアップグレード中にエクスポートされた IDB を使用し、他の IDB エクスポートを回避できるようになります。

Data Protector A.06.11、6.20、または 7.00 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。以下の項で示される順序で手順を実行します。

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。

1. `cmhaltpkg` *`PackageName`* コマンドを実行して (*`PackageName`* にはクラスターパッケージの名前を指定)、古い Data Protector パッケージを停止します。例:

   ```
   cmhaltpkg ob2cl
   ```

2. 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 VGName
   ```

   例:

   ```
   vgchange -a e -q y /dev/vg_ob2cm
   ```

3. 論理ボリュームを共有ディスクにマウントします。

   ```
   mount LVPath SharedDisk
   ```

   `LVPath` パラメーターには論理ボリュームのパス名を、*`SharedDisk`* パラメーター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
   ```

4. Data Protector サービスを開始します。

   ```
   omnisv -start
   ```

5. 「UNIX 用 Cell Manager とインストールサーバーのアップグレード」(161 ページ) で説明されている手順に従って Cell Manager をアップグレードします。アップグレードする製品のバージョンによって、手順が異なります。
6. Data Protector サービスを停止します。

   ```
   omnisv -stop
   ```

7. 共有ディスクのマウントを解除します。

   ```
   umount SharedDisk
   ```

   入力例:

   ```
   umount /omni_shared
   ```

8. ボリュームグループを非アクティブ化します。

   ```
   vgchange -a n VGName
   ```

   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. 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 VGName
   ```

2. 論理ボリュームを共有ディスクにマウントします。

   ```
   mount LVPath SharedDisk
   ```

3. 「UNIX 用 Cell Manager とインストールサーバーのアップグレード」 (161 ページ) で説明されている手順に従って Cell Manager をアップグレードします。アップグレードする製品のバージョンによって、手順が異なります。
4. `/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_DP70.sh` や `mafailover_DP70.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。
5. Data Protector サービスを停止します。

   ```
   omnisv -stop
   ```
6. 共有ディスクのマウントを解除します。

   ```
   umount SharedDisk
   ```
7. ボリュームグループを非アクティブ化します。

   ```
   vgchange -a n VGName
   ```

一次ノード

一次ノードに再度ログオンし、以下の手順に従ってください。

1. Data Protector パッケージを起動します。

   ```
   cmrunpkg PackageName
   ```
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` にサブディレクトリがマウントされていないことも確認してください。以下を実行します。

   ```
   /opt/omni/sbin/install/omniforsg.ksh -primary -upgrade
   ```
3. Data Protector パッケージを停止します。

   ```
   cmhaltpkg PackageName
   ```

二次ノード

二次ノードに再度ログオンし、以下の手順に従ってください。

1. Data Protector パッケージを起動します。

   ```
   cmrunpkg PackageName
   ```
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` ディレクトリにサブディレクトリがマウントされていないことを確認してください。以下を実行します。

   ```
   /opt/omni/sbin/install/omniforsg.ksh -secondary /share -upgrade
   ```
3. Data Protector パッケージを停止します。

   ```
   cmhaltpkg PackageName
   ```

一次ノード

一次ノードに再度ログオンし、以下の手順に従ってください。

1. Data Protector パッケージを起動します。

   ```
   cmrunpkg PackageName
   ```

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. 仮想ホストを再度インポートします。

   ```
   omnicc -import_host VirtualHostname -virtual
   ```

3. IDB 内の Cell Manager の名前を変更します。

   ```
   omnidbutil -change_cell_name
   ```

4. インストールサーバーが 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ー 仮想ホスト名をインポートします。

   ```
   omnicc -import_is VirtualHostname
   ```

注記: Cell Manager からのすべての要求は、Data Protector 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については、「セキュリティについて」 (135 ページ) 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.06.11、6.20、または 7.00 Cell Manager を Data Protector 8.00 にアップグレードするには、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。

前提条件

- アップグレードオプションがサポートされるのは、以前にインストールされた Data Protector ソフトウェアがクラスター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。クラスター内のシステムに Data Protector ソフトウェアがクラスター非対応でインストールされている場合、セットアップを開始する前にこのソフトウェアをアンインストールする必要があります。

アップグレード手順

アップグレードは、以下の手順で行ってください。

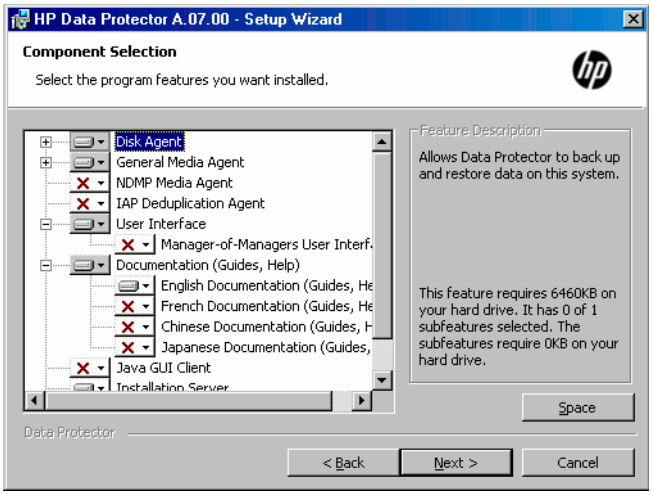
1. Windows インストール DVD-ROM をドライブに挿入し、`\Windows_Other\x8664\setup.exe` コマンドを実行します。現在アクティブ化されている仮想サーバーノードでセットアップを開始することをお勧めします。

   自動的に旧バージョンの製品が検出され、Data Protector 8.00 にアップグレードするよう促すメッセージが表示されます。

   [Next] をクリックし、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 45 コンポーネントの選択



[Next] をクリックします。

3. Data Protector がシステムで Windows ファイアウォールを検出した場合、[Windows Firewall configuration] ページが表示されます。Data Protector セットアップにより、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。

   自動生成されるのはインバウンドファイアウォールルールのみであり、アウトバウンドファイアウォールルールは手動で作成する必要があるので注意してください。必要なポート範囲については、『HP Data Protector ヘルプ』の索引「ファイアウォールのサポート」で表示される内容を参照してください。

   [Next] をクリックします。

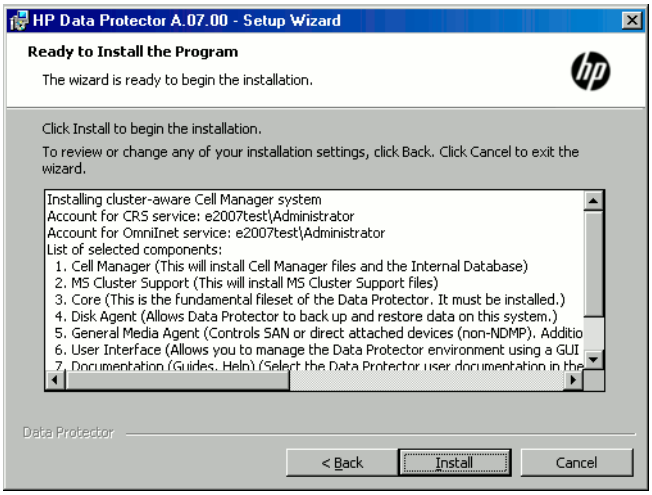
4. 必要に応じて、Data Protector IDB および HTTPS アプリケーションサーバーで使用するユーザーアカウントと、これらのサービスで使用するポートを変更します。

   [Next] をクリックします。

5. コンポーネント選択サマリーリストが表示されます。**[Install]** をクリックして、アップグレードを開始します。

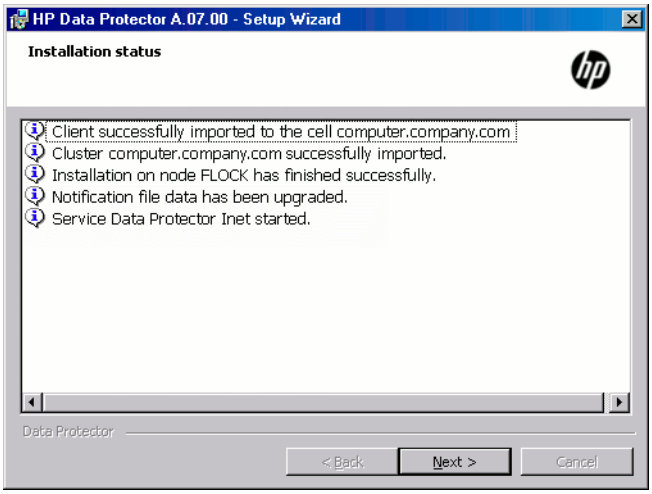
   アップグレード後には、すべてのノードに同じコンポーネントセットがインストールされます。

図 46 コンポーネント選択サマリーページ



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

図 47 [Installation status] ページ



7. ユーザーインターフェースコンポーネントをアップグレードしたか、新しくインストールした場合に、セットアップ直後に Data Protector GUI を使用して操作を開始するには **[Launch Data Protector GUI]** を選択します。

   英語版ドキュメント（ガイド、ヘルプ）コンポーネントをアップグレードしたか、または新しくインストールした場合に、セットアップ直後に『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を表示するには、**[Open the Product Announcements, Software Notes, and References]** を選択します。

   [Finish] をクリックします。

注記: クラスター対応クライアントをアップグレードする場合は、まずすべてのクラスターノードを個別にアップグレードしてから、仮想サーバーを再度インポートします。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 ライセンス

この章は、次の項目で構成されています。

- Data Protector ライセンスチェック機能とレポート機能
- Data Protector パスワードの取得とインストール
- Data Protector の製品構成とライセンス

概要

Data Protector 8.00 製品構成およびライセンスには、 次の 2 つのモデルがあります。

- 容量ベースのライセンス
- 従来のライセンス

従来のライセンスモデルには、主に次の 3 つのカテゴリがあります。

1. スターターパック
2. ドライブとライブラリの使用権
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、および Linux プラットフォーム上でしか使用できません。

スターターパックと**ドライブ拡張およびライブラリ拡張**の各カテゴリのライセンスとパスワードは Cell Manager にバインドされており、セッションの Data Protector クライアント数に関係なく Data Protector セル全体をカバーします。**機能拡張**カテゴリのライセンスは、ライセンスタイプに応じて、各対象クライアントのみ、またはセル全体に適用されます。

たとえば、ファイルシステムとディスクイメージのバックアップは**スターターパック**のライセンスでカバーされます。したがって、1 つのライセンスで、同じセル内の任意の数のクライアントからファイルシステムとディスクイメージをバックアップできます。

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。

- たとえば、Data Protector のチェックおよび保守メカニズムの一環としてライセンスがチェックされ、ライセンスが見つからない場合は、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_program_data*\log\server\Ob2EventLog.txt(Windows システムの場合)、または/var/opt/omni/server/log/Ob2EventLog.txt(UNIX システムの場合) に置かれています。Data Protector チェックおよび保守機構の詳細については、『HP Data Protector ヘルプ』の索引「イベントログ、Data Protector」を参照してください。
- ライセンスが見つからないというレポートが Data Protector イベントログに記録されている場合、Data Protector GUI の起動時にイベントログの通知が表示されます。Data Protector のイベントログの詳細は、『HP Data Protector ヘルプ』の索引「イベントログ、Data Protector」を参照してください。
- Data Protector セッションの開始時にライセンスがチェックされ、見つからない場合は、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

- エンティティーベースのライセンス
- 容量ベースのライセンス

Cell Manager 関連ライセンス

Data Protector Cell Manager には、以下の関連ライセンスがあります。

- スターターパック
- Manager-of-Managers 使用権
- シングルサーバー版

Cell Manager (スターターパックに含まれる) や Manager-of-Managers (MoM) など一部の Data Protector コンポーネントがセル内に存在する場合は、必要とされる基本ライセンスまたは特別ライセンスの有無のみがチェックされます。

エンティティーベースのライセンス

Data Protector には、以下のエンティティベースのライセンスがあります。

- 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)
- SAN、すべてのプラットフォーム用追加ドライブ使用権、および Windows、Linux 用追加ドライブ使用権
- UNIX 用オンラインバックアップ使用権 (システム 1 台)、および Windows、Linux 用オンラインバックアップ使用権 (システム 1 台)
- Data Protector クライアントシステム暗号化使用権 (1 台)
- 1 台のデータベースサーバーの Granular Recovery Extension

前述のいずれかのエンティティー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ーベース使用権の存在とその数がチェックされます。

Data Protector では、構成されているエンティティーベース項目の数とエンティティーベースのライセンスの数を比較します。ライセンスの数が構成されている項目の数より少ない場合は、通知が発生します。

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。

バックアップデバイスが SAN 環境内の複数の Data Protector クライアントに対して構成されている場合は、Multipath 機能を使って、Data Protector で 1 台のバックアップデバイスとして認識されるようにする必要があります。

容量ベースのライセンス

Data Protector の容量ベースのライセンスは、以下のとおりです。

- UNIX ゼロダウンタイムバックアップ使用権 (1TB、10TB)
- UNIX インスタントリカバリ使用権 (1TB、10TB)
- Linux ゼロダウンタイムバックアップ使用権 (1TB、10TB)
- Linux インスタントリカバリ使用権 (1TB、10TB)
- Windows ゼロダウンタイムバックアップ使用権 (1TB、10TB)
- Windows インスタントリカバリ使用権 (1TB、10TB)
- NDMP ダイレクトバックアップ使用権 (1TB、10TB)
- アドバンストバックアップ使用権 (1TB、10TB、100TB)

容量ベースのライセンス(アドバンスト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の容量と比較されます。

ライセンスのチェックは、ライセンスを受けている容量を使い果たした場合でも、インスタントリカバリまたはバックアップの実施の妨げにならないよう行われます。容量がなくなると、バックアップセッション中に、ライセンスを受けた容量を越えたことを示す警告メッセージが表示されます。

使用されたディスクの容量は、各 ZDB バックアップセッションから集めた履歴情報を基に計算されます。考慮される期間は 24 時間です。Data Protector では、過去 24 時間以内に発生したすべてのセッションで使用されたディスクを基に使用ディスク容量が計算され、算出された容量をライセンスを受けた容量と比較します。

ライセンス違反が起こると、バックアップ処理中に警告メッセージが表示されます。さらに、ライセンスレポートツールは毎日実行され、ライセンスを受けた容量を越えると Data Protector イベントログに通知が書き込まれます。

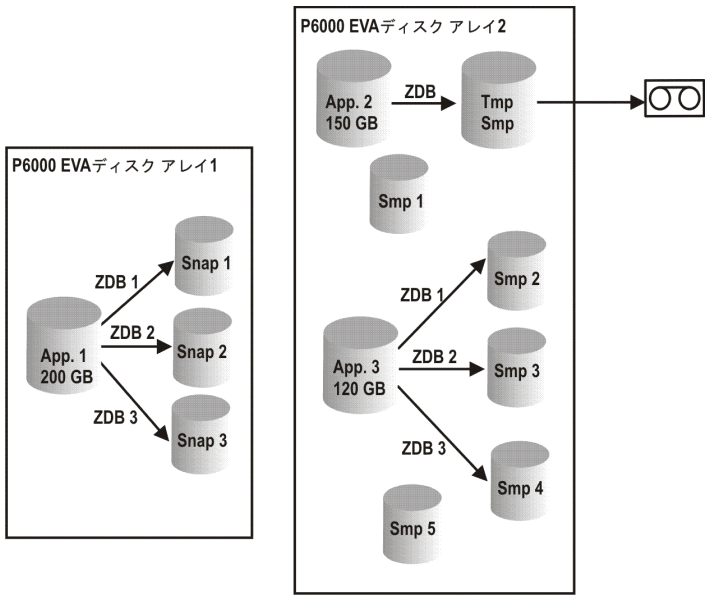
使用容量の計算

使用される容量の計算では、過去 24 時間以内に使用されたディスクアレイごとに、ライセンスを受けている容量を算出します。指定した期間内に複数回使用されたディスクは、1 回だけカウントされます。ディスクアレイユニットは、各アレイに使用されている識別番号によって識別されます。アレイの識別番号を使用すると、既にカウント済みのアレイの認識が可能です。

インスタントリカバリが含まれた ZDB バックアップを実行している場合は、ZDB に使用された各ディスクアレイの容量に加え、インスタントリカバリに使用された各ディスクアレイの容量が、元の単位の総容量の計算対象になります。

たとえば、2 台の P6000 EVA ディスクアレイがあるとします。1 台のアレイには、データ保護のために使用される 200GB の容量のディスク (App.1) が 1 台あります。バックアップセッションは 1 日に 3 回実行され、それぞれのセッションにインスタントリカバリオプションが設定されています。一度に 3 つの複製が保存され、これらがインスタントリカバリ用にローテーションされます。もう 1 台のディスクアレイには、150GB と 120GB の容量の 2 台のディスク (App.2 と App.3) があります。ディスク App.2 では 1 日に 1 回バックアップが実行され、データがテープに移動された後、スナップショットは削除されます。App.3 では、1 日に 3 回バックアップが実行され、インスタントリカバリ用に 5 つの複製がローテーションされます。「使用容量の計算シナリオ」 (185 ページ) を参照してください。

図 48 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、200GB (App.1) + 150GB (App.2) + 120GB (App.3) = 470GB。

インスタントリカバリ使用容量の計算では、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計算します。同じディスクは 1 回しかカウントしないので、200GB (App.1) + 120GB (App.3) = 320GB となります。

アドバンストバックアップ使用権

Data Protector ファイルライブラリと Data Protector StoreOnce 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です。また、仮想テープライブラリ (VTL) には、ドライブおよびライブラリライセンスの代わりに、このアドバンストバックアップ使用権を使用できます。

- Data Protector ファイルライブラリの使用可能なネイティブ容量は、そのファイルライブラリで使用可能なディスクサイズです。このサイズは、ファイルシステムにより報告されます。
  - 合成フルまたは仮想フルバックアップに統合される仮想フルバックアップおよび増分バックアップは、このライセンスを必要とする Data Protector ファイルライブラリに保存する必要があります。
- Data Protector で VTL のみを使用している場合は、VTL の物理容量と同量のライセンスが必要です。これは使用可能なネイティブ容量とも呼ばれます。
  - 仮想テープライブラリ (VTL) の使用可能なネイティブ容量は、すべての HP の保護バックアップにより使用される仮想テープライブラリのディスクのサイズです。このサイズは、VTL により報告されます。
  - VTL ごとに、ディスクへのバックアップまたはテープドライブへのバックアップのどちらのライセンスモデルを使用するかを選択できます。1 つの VTL で、この両方の方法を合わせて使用することはできません。
  - バックアップデータをディスクキャッシュから別のディスクまたはテープに移行するための組み込み容量が VTL にある場合は、移行されるストレージ容量を完全にライセンスする必要があります。VTL により排他的に制御されるテープライブラリにはドライブおよびライブラリライセンスは必要ありませんが、**物理テープライブラリのすべてのテープで使用される容量はライセンスする必要があります。**ただし、バックアップデータを別のディスクまたはテープに移行するために Data Protector のオブジェクトコピー機能が使用されている場合は、この方法は使用できません。
  - デフォルトでは、Data Protector は、VTL デバイスを SCSI II ライブラリなどの通常のライブラリとして扱い、容量ベースのライセンスは適用されません。容量ベースのライセンスを利用するには、デバイスの構成時にデバイスに VTL のマークを付ける必要があります。

    VTL をグラフィックユーザーインタフェース (GUI) を使用して構成する方法は、『HP Data Protector ヘルプ』の索引「仮想テープライブラリ」を参照してください。VTL をコマンドラインインタフェース (CLI) を使用して構成する方法は、後述の「例」(187 ページ) を参照してください。
- Manager-of-Managers (MoM) でライセンスを集中管理している場合は、ディスクへのアドバンストバックアップ機能を使用して、最低でも 1TB を各セルに割り当てる必要があります。

注記: Data Protector は、最新の仮想テープライブラリおよびファイルライブラリをホストしている一部のファイルサーバーの装備およびインタフェースが欠けているために、必要なライセンスの容量をレポートできません。ライセンス定義と一致するようにライセンスを容量に割り当てるのは、ユーザーの責任です。

例

omniupload コマンドを使用してコマンドラインインタフェース (CLI) で「VTL_2011」という名前の仮想テープライブラリを構成する場合は、構成ファイルの VTLCAPACITY 文字列に対してライブラリの推定容量を指定する必要があります。この推定値は、結果的にライセンスチェッカーレポートのアドバンストバックアップ使用権に使用される容量に追加されます。

注記: 推定仮想ライブラリ容量消費量の値 (VTLCAPACITY) は、「指定した VTL 容量は無効です」というエラーメッセージを避けるために、テラバイト (TB) 単位で整数で指定する必要があります。

「C:\Temp」ディレクトリにある「libVTL.txt」という名前の構成ファイル内で、ライブラリ容量の推定消費量として、たとえば 11 と入力し、次のコマンドを実行します。

```
omniupload -create_library VTL_2011 -file C:\Temp\libVTL.txt
```

構成を確認するには、次のコマンドを実行します。

```
omnidownload -library VTL_2011
```

```
#omnidownload -library VTL_2011
NAME "VTL2011"
DESCRIPTION ""
HOST computer.company.com
POLICY SCSI-II
TYPE DDS
LIBVIRTUAL
VTLCAPACITY 11
IOCTLSERIAL ""
CONTROL "SCSI address"
REPOSITORY
        "SCSI repository"
MGMTCONSOLEURL ""
```

ライセンス確認では、使用されているライセンス容量がレポートされます。これは、ファイルライブラリ (FL) に使用されているディスク上のスペースで、仮想テープライブラリ上のディスクスペースの推定サイズです。たとえば、バックアップにより FL で 2TB のディスクスペースを使用していて、VTL 上に 10TB のディスク容量を使用しているものとします。使用中の合計容量は 12TB です。5TB のライセンス容量しかインストールされていない場合には、アドバンストバックアップ使用権 (1TB) がさらに 7 つ必要であるという通知が表示されます。

```
#omnicc -check_licenses -detail
----------------------------------------------------------------------
ライセンスカテゴリ                    :アドバンストバックアップ使用権(1TB)
インストールされたライセンス容量      :5TB
使用されているライセンス容量          :12.0TB
必要な追加のライセンス容量:7TB

サマリー
-------
説明                                                    必要なライセンス
アドバンストバックアップ使用権(1TB)                                    7
```

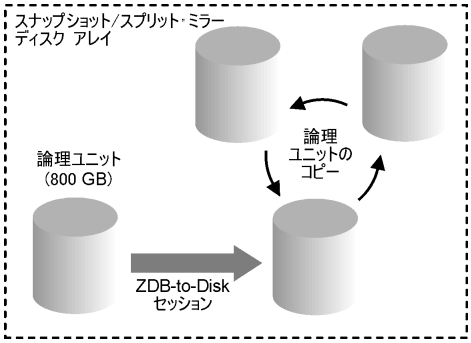
容量ベースのライセンスの例

ここでは、容量ベースのライセンスの計算方法の例を示します。

例 1

図 49「ディスクへの ZDB セッション」では、800GB 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+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。

図 49 ディスクへの ZDB セッション



インスタントリカバリに備えて、3 つのスプリットミラーコピーまたはスナップショットコピー (複製) がローテーションおよび保管されます。この場合、容量ベースのライセンスは、以下のように計算します。

800GB の論理ユニット 1 つを使用するディスクへの ZDB (ZDB-to-Disk) セッション:

1 x 800GB = 0.8TB 用として「ゼロダウンタイムバックアップ使用権 (1TB)」ライセンス

インスタントリカバリに備えて、同じ 800GB の論理ユニットの 3 つの複製が保管されます。なお、ライセンスの対象となるのは、複製の容量ではなく、ソースボリュームの容量です。

1 x 800GB = 0.8TB 用として「インスタントリカバリ使用権 (1TB)」ライセンス

この場合は、「ゼロダウンタイムバックアップ使用権 (1TB)」ライセンスが 1 つ、および「インスタントリカバリ使用権 (1TB)」ライセンスが 1 つ必要です。

例 2

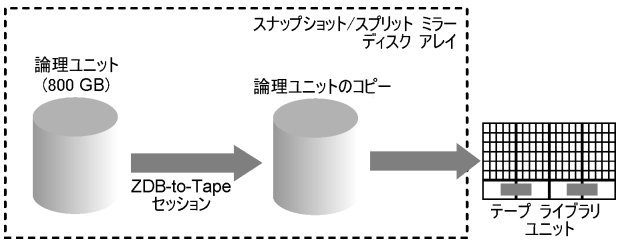
「テープへの ZDB セッション」 (188 ページ) では、800GB の論理ユニット 1 つからのデータが、テープへの ZDB (ZDB-to-Tape) セッションで 1 日に 2 度バックアップされる状況が例として示されています。したがって、インスタントリカバリ用のスプリットミラーコピーまたはスナップショットコピー (複製) は保管されません。この場合、容量ベースのライセンスは、以下のように計算します。

800GB の論理ユニット 1 つを使用するディスクへの ZDB (ZDB-to-Disk) セッション:

1 x 800GB = 0.8TB 用として「ゼロダウンタイムバックアップ使用権 (1TB)」ライセンス

この場合は、「ゼロダウンタイムバックアップ使用権 (1TB)」ライセンスが 1 つ必要です。

図 50 テープへの ZDB セッション



例 3

「ディスク + テープへの ZDB セッション」 (189 ページ) では、800GB 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。インスタントリカバリに備えて、5 つのスプリットミラーコピーまたはスナップショットコピー (複製) がローテーションおよび保管されます。この場合、容量ベースのライセンスは、以下のように計算します。

ディスク/テープへの ZDB (ZDB-to-Disk+Tape) セッションに 800GB の論理ユニットを 1 つ使用するため、以下のライセンスが必要です。

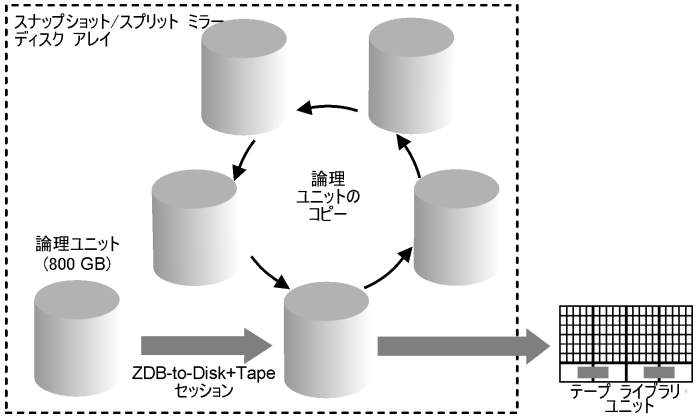
1 x 800GB = 0.8TB 用として「ゼロダウンタイムバックアップ使用権 (1TB)」ライセンス

インスタントリカバリに備えて、同じ 800GB の論理ユニットの 5 つの複製が保管されます。なお、ライセンスの対象となるのは、複製の容量ではなく、ソースボリュームの容量です。

1 x 800GB = 0.8TB 用として「インスタントリカバリ使用権 (1TB)」ライセンス

この場合は、「ゼロダウンタイムバックアップ使用権 (1TB)」ライセンスが 1 つ、および「インスタントリカバリ使用権 (1TB)」ライセンスが 1 つ必要です。

図 51 ディスク + テープへの ZDB セッション



例 4

ZDB セッションで、200GB の論理ユニットが 1 つ、500GB の論理ユニットが 1 つ、120GB の論理ユニットが 1 つ、および 300GB の論理ユニットが 1 つ使用されるため、以下のライセンスが必要です。

1 x 200GB + 1 x 500GB + 1 x 120GB + 1 x 300GB = 1.12TB は、「ゼロダウンタイムバックアップ使用権 (1TB)」ライセンス。

インスタントリカバリに備えて、1 つの 200GB の論理ユニット、1 つの 120GB の論理ユニット、および 1 つの 300GB の論理ユニットのスプリットミラーコピーまたはスナップショットコピーが保管されるため、以下のライセンスが必要です。

1 x 200GB+ 1 x120GB + 1 x 300GB = 0.62TB 用として「インスタントリカバリ使用権 (1TB)」ライセンス

「ディスクへの ZDB セッション」 (188 ページ) から「ディスク + テープへの ZDB セッション」 (189 ページ) で示した 3 つの例を 1 つのセルで構成する場合、「ゼロダウンタイムバックアップ使用権 (1TB)」ライセンス 1 つと、「インスタントリカバリ使用権 (1TB)」ライセンス 1 つで十分対応できます。

必要に応じたライセンスレポートの作成

セルからの関連情報のライセンスについてレポートを生成するには、以下を実行します。

```
omnicc -check_licenses [-detail]
```

`-detail` オプションが指定されなかった場合は、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。以下の情報が返されます。レポートが生成された時刻、ライセンスモード、およびライセンスサーバーの情報が返されます。

`-detail` オプションを指定すると、詳細なレポートが作成されます。ライセンス確認処理から、セル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、および必要な追加ライセンス (容量) の情報が返されます。

ドライブ使用権 LTU の場合、ライセンス確認では構成されたドライブと推奨された追加ライセンスに関する情報が返されます。いずれかの時点で使用するドライブの台数と同じ数のライセンスが必要です。これは、すべてのドライブを同時に使用できるようにするため、通常は構成されたドライブの総数になります。

なお、ライセンスの有効期限は表示されません。環境とインストールされているライセンスによっては、レポートの作成に若干時間がかかることがあります。ライセンスの有効期限に関する情報を取得するには、次のコマンドを実行します。

```
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。

詳細は、omnicc の man ページまたは『HP Data Protector Command Line Interface Reference』を参照してください。

Data Protector 8.00 以前のライセンスのチェックとレポート

Data Protector 8.00 のライセンス確認では、特定のライセンスが以前の Data Protector リリースから新しい Data Protector 製品構造にマッピングされ、新しいライセンスとしてレポートされます。ライセンスの適用時に制限事項が発生する場合があります。詳細は、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』の制限事項を参照してください。

この章は、次の項目で構成されています。

- 「マルチドライブサーバー使用権のレポート」 (190 ページ)
- 「以前のオンラインライセンスのレポート」 (192 ページ)
- 「NDMP ダイレクトバックアップ使用権のレポート」 (192 ページ)
- 「スロットライブラリ使用権のレポート」 (193 ページ)
- 「以前の ZDB および IR のライセンスのレポート」 (193 ページ)

マルチドライブサーバー使用権のレポート

UNIX 用マルチドライブサーバー使用権は、6 つの SAN、すべてのプラットフォーム用追加ドライブ使用権としてレポートされます。

マルチドライブ使用権は、GUI でクライアントを選択する際に [詳細設定] タブの下の [クライアント] コンテキストで [クライアントをデバイスサーバーとして設定する] オプションを設定した場合に、デバイスサーバーのみで使用されます。このオプションが設定されていない場合は、マルチドライブ使用権はインストールされていても使用されません。

インストールされている SAN、すべてのプラットフォーム用追加ドライブ使用権の数は、6 つ単位で増加します。たとえば、UNIX 用マルチドライブサーバー使用権 1 ライセンスと SAN、すべてのプラットフォーム用追加ドライブ使用権 1 ライセンスがデバイスサーバーにインストールされているとします。ライセンス確認では、SAN、すべてのプラットフォーム用追加ドライブ使用権が 7 ライセンス (1 シングルドライブ、および 1 マルチドライブから 6 つ) インストールされていることが示されます。

システム上に 10 台のドライブが構成されている場合、ライセンス確認では、すべてのドライブを同時に使用するために、SAN、すべてのプラットフォーム用追加ドライブ使用権 3 ライセンスの追加が推奨されることがレポートされます。

```
#omnicc -check_licenses -detail
ライセンスカテゴリ                    : SAN、すべてのプラットフォーム用追加ドライブ使用権
インストールされているライセンス: 7
構成されているドライブ                : 10
推奨する追加ライセンス                : 3

サマリー
説明                                                推奨する追加のドライブライセンス
SAN、すべてのプラットフォーム用追加ドライブ使用権                3
警告:いかなるときも、操作(フォーマット、バックアップ、復元、メディアとオブジェクトのコピー、メディアとオブジェクトの検証、オブジェクトのミラーリング、スキャン、ディザスタリカバリなど)に使用しているドライブと同数のライセンスが必要になります。すべてのドライブを同時に使用できるようにするには、構成されているドライブと同数のライセンスが必要です。

ライセンスがカバーされています。
```

Windows システムのライセンスについても同様です。Windows 用マルチドライブサーバー使用権もライセンス確認のレポートから削除され、Windows、Linux 用追加ドライブ使用権 4 ライセンス分としてレポートされます。Windows、Linux 用追加ドライブ使用権の数は、4 つ単位で増加します。10 台のドライブが構成されている環境で、マルチドライブ使用権 1 ライセンスとシングルドライブ使用権 1 ライセンスがインストールされている場合、ライセンス確認では、すべてのドライブを同時に使用するために、Windows、Linux 用追加ドライブ使用権 5 ライセンス (10 必要で、うち 5 つは 1 マルチドライブからの 4 つと 1 シングルドライブからの 1 つでカバー済み) の追加が推奨されることがレポートされます。

```
#omnicc -check_licenses -detail
ライセンスカテゴリ                              : Windows、Linux用追加ドライブ使用権
インストールされているライセンス    : 5
構成されているドライブ                  : 10
推奨する追加ライセンス                  : 5

サマリー
説明                                                                    推奨する追加のドライブライセンス
SAN、すべてのプラットフォーム用追加ドライブ使用権                      5

警告:いかなるときも、操作(フォーマット、バックアップ、復元、メディアとオブジェクトのコピー、メディアとオブジェクトの検証、オブジェクトのミラーリング、スキャン、ディザスタリカバリなど)に使用しているドライブと同数のライセンスが必要になります。すべてのドライブを同時に使用できるようにするには、構成されているドライブと同数のライセンスが必要です。

ライセンスがカバーされています。
```

また、以前の組み合わせライセンスとして、UNIX 用 Cell Manager およびマルチドライブサーバーと、Windows 用 Cell Manager およびマルチドライブサーバーがあります。

UNIX 用 Cell Manager およびマルチドライブサーバー使用権 1 ライセンスがインストールされている場合、omnicc コマンドでは、すべてのプラットフォーム用 Cell Manager 使用権 1 ライセンスと、UNIX 用マルチドライブサーバー使用権 1 ライセンスがインストールされていることがレポートされます。

```
#omnicc
ライセンスモード          :ローカル
ライセンスサーバー        :computer.company.com

カテゴリ                                                ライセンスの数
すべてのプラットフォーム用Cell Manager                  1
Windows/Linux用Cell Manager                             0
SAN、すべてのプラットフォーム用追加ドライブ             0
Windows、Linux用追加ドライブ                            0
UNIX用マルチドライブサーバー                            1
Windows用マルチドライブサーバー                         0
```

この組み合わせの使用権は、UNIX 用 Cell Manager およびシングルドライブサーバー 1 ライセンス、および SAN、すべてのプラットフォーム用追加ドライブ使用権 5 ライセンス分としてレポートされます。つまり、ライセンス確認では、すべてのプラットフォーム用 Cell Manager 使用権 1 ライセンスと、SAN、すべてのプラットフォーム用追加ドライブ使用権 6 ライセンスがレポートされます。

システム上に 10 台のドライブが構成されていて、UNIX 用 Cell Manager およびマルチドライブサーバー使用権 1 ライセンスがインストールされている場合、ライセンス確認では、すべてのドライブを同時に使用するために、SAN、すべてのプラットフォーム用追加ドライブ使用権 4 ライセンス (10 必要で、うち 6 つはマルチドライブ使用権でカバー済み) の追加が推奨されることがレポートされます。

```
#omnicc -check_licenses -detail
ライセンスカテゴリ          :インストールされているすべてのプラットフォーム用Cell Manager使用権          :1
使用されているライセンス                :1
必要な追加ライセンス                    :0

ライセンスカテゴリ:インストールされているWindows、Linux用追加ドライブ使用権          :6
構成されているドライブ          :10
推奨する追加のライセンス        : 4

サマリー
説明                                                    推奨する追加のライセンス
SAN、すべてのプラットフォーム用ドライブ使用権                                  4

警告:いかなるときも、操作(フォーマット、バックアップ、復元、メディアとオブジェクトのコピー、メディアとオブジェクトの検証、オブジェクトのミラーリング、スキャン、ディザスタリカバリなど)に使用しているドライブと同数のライセンスが必要になります。すべてのドライブを同時に使用できるようにするには、構成されているドライブと同数のライセンスが必要です。

ライセンスがカバーされています。
```

Windows システムの組み合わせライセンスについても同様です。Windows 用 Cell Manager およびマルチドライブサーバー使用権は、Windows 用 Cell Manager およびシングルドライブサーバー使用権 1 ライセンスと、Windows、Linux 用追加ドライブ使用権 4 ライセンス分としてレポートされます。ライセンス確認では、Windows/Linux 用 Cell Manager 使用権 1 ライセンスと、Windows、Linux 用追加ドライブ使用権 5 ライセンスがインストールされていることがレポートされます。

ライセンス確認では足りないライセンスの数がレポートされますが、バックアップ中、インストールされているライセンスのチェックは変更されません。ドライブサーバーにインストールされたマルチドライブ使用権では、構成済みドライブの数は無制限に同時に使用することは可能です。しかし、構成済みドライブサーバーがないにも関わらずマルチドライブ使用権がインストールされている場合は、ライセンス確認で十分なシングルドライブ使用権がインストールされているとレポートされていても、バックアップができない場合があります。

以前のオンラインライセンスのレポート

UNIX 用オンラインバックアップ使用権および Windows/Linux 用オンラインバックアップ使用権は、セル内のすべてのクライアントに有効です。以前の Data Protector リリースのオンラインバックアップ使用権は、インストールされている現在のライセンスの数が 1 ずつ増加します。

ライセンス確認では、セル内のシステムが多数ある場合に、追加のオンラインバックアップ使用権が必要であるとレポートされる場合があります。たとえば、セル内にオンラインバックアップを使用する 5 つの Windows システムがあり、Windows 用オンラインバックアップ使用権 1 ライセンスがインストールされているものとします。インストールされているライセンスでは 1 つのシステムがカバーされるため、他の 4 つのシステム用に、4 ライセンスの追加が必要となります。ライセンス確認では、Windows/Linux 用オンラインバックアップ使用権 (システム 1 台)4 ライセンスが必要であることがレポートされます。

```
#omnicc -check_licenses -detail
ライセンスカテゴリ          :インストールされているWindows/Linux用オンラインバックアップ
使用権(システム1台)1
使用されているライセンス  :5
必要な追加ライセンス      :4

サマリー
説明                                                    必要なライセンス
Windows/Linux用オンラインバックアップ使用権(システム1台)                  4

ライセンスがカバーされていません。
```

さらに 3 つの Windows/Linux 用オンラインバックアップ使用権 (システム 1 台) がインストールされている場合は、Windows/Linux 用オンラインバックアップ使用権 (システム 1 台) がもう 1 ライセンス (5 つ必要で、うち 4 つは以前のもの 1 つとシステム 1 台用 3 つでカバー済み) 必要であるという通知が表示されます。

```
#omnicc -check_licenses -detail
ライセンスカテゴリ          :インストールされているWindows/Linux用オンラインバックアップ
使用権(システム1台)4
使用されているライセンス  :5
必要な追加ライセンス      :1

サマリー
説明                                                    必要なライセンス
Windows/Linux用オンラインバックアップ使用権(システム1台)                  1

ライセンスがカバーされていません。
```

NDMP ダイレクトバックアップ使用権のレポート

NDMP サーバー使用権 (1 台) は、NDMP ダイレクトバックアップ使用権 (1TB)1 ライセンス分としてレポートされます。1 つ目はエンティティーベースのライセンスで、つまり、1 つの NDMP サーバーごとに 1 つのライセンスが必要になります。一方、NDMP ダイレクトバック

アップ使用権 (1TB) は容量ベースのライセンスで、1 つの NDMP サーバーで 1TB のバックアップをするために必要となります。

インストールされている NDMP ダイレクトバックアップ使用権 (1TB) のライセンス容量は、インストールされている NDMP サーバー使用権 (1 台) の数ごとに増加します。たとえば、NDMP ダイレクトバックアップ使用権 (1TB) 1 ライセンスと、NDMP ダイレクトバックアップ使用権 (1TB) 1 ライセンスがインストールされている場合は、インストールされているライセンス容量は合計で 2TB となります。結果として、ライセンス確認で追加のライセンスが必要であるとレポートされる場合があります。たとえば、NDMP を使用して 5TB のバックアップを行う際に、NDMP サーバー使用権 (1 台) 1 ライセンスと 1 つの NDMP ダイレクトバックアップ使用権 (1TB) 1 ライセンスがインストールされているものとします。ライセンス確認では、NDMP ダイレクトバックアップ使用権 (1TB) 3 ライセンス (5 つ必要、2 つは以前の 1 つと新しいライセンス 1 つでカバー済み) が必要であるとレポートされます。

```
#omnicc -check_licenses -detail
ライセンスカテゴリ                                  : NDMPダイレクトバックアップ使用権(1TB)
インストールされているライセンス容量: 2 TB
使用されているライセンス容量       : 5.0 TB
必要な追加のライセンス容量       : 3 TB

サマリー
説明                                                必要なライセンス
NDMPダイレクトバックアップ使用権(1TB)                 3
```

スロットライブラリ使用権のレポート

プラットフォーム固有のライブラリ使用権 (1 つは Windows システム用、1 つは UNIX システム用) は、プラットフォームに依存しないライセンスとしてレポートされます。

インストールされている 61-250 スロットライブラリ使用権 (1 台) の数は、インストールされているプラットフォーム固有の 61-250 スロットライブラリ使用権の数ごとに増加します。また、プラットフォーム固有の無制限ライセンスがインストールされているスロット数無制限ライブラリ使用権 (1 台) の数に追加されます。

UNIX 用スロット数無制限ライブラリ使用権 1 ライセンスと Windows 用スロット数無制限ライブラリ使用権 1 ライセンスがインストールされている場合、ライセンス確認では、スロット数無制限ライブラリ使用権 (1 台) 2 ライセンス分がインストールされていることがレポートされます。

```
#omnicc -check_licenses -detail
ライセンスカテゴリ                          : 61-250スロットライブラリ使用権(1台)
インストールされているライセンス: 2
使用されているライセンス              : 0
必要なライセンス                            : 0
ライセンスカテゴリ                          : スロット数無制限ライブラリ使用権(1台)
インストールされているライセンス: 2
使用されているライセンス              : 0
```

スロットライブラリのライセンスはプラットフォームに依存しないため、ライセンスの適用がライセンスのチェックよりも優先されます。バックアップ中に、Data Protector は異なるプラットフォームのライセンスをチェックします。ライセンス確認で十分かつ適切なライセンスがシステムにインストールされているとレポートされていても、特定のプラットフォームでライセンスが足りないためにバックアップが実行できない場合があります。

以前の ZDB および IR のライセンスのレポート

- ゼロダウンタイムバックアップ使用権 (1TB) (B7025CA) は、以前の Data Protector リリースのディスクアレイ固有のゼロダウンタイムバックアップ使用権を置き換えます。
  - HP Modular SAN Array 1000 用 ZDB 使用権 (1TB) (HP Modular SAN Array 1000 用ゼロダウンタイムバックアップ使用権 (1TB) (B7036AA))
  - HP P6000 EVA ディスクアレイファミリ 用 ZDB 使用権 (1TB) (汎用ゼロダウンタイムバックアップ使用権 (1TB) (B7025CA))

- HP P9000 XP ディスクアレイファミリ 用 ZDB 使用権 (1TB) (HP P9000 XP ゼロダウンタイムバックアップ使用権 (1TB) (B7023CA))
- EMC Symmetrix/DMX 用 ZDB 使用権 (1TB) (EMC Symmetrix/DMX 用ゼロダウンタイムバックアップ使用権 (1TB) (B6959CA))

すべてのディスクアレイ固有のライセンスは、ライセンスチェッカーによって、汎用ゼロダウンタイムバックアップ使用権 (1TB) (B7025CA) 1 ライセンス分としてレポートされます。インストールされている汎用ライセンスの容量は、すべての特定のアレイの種類のライセンスごとに増加します。使用中のライセンス容量は、すべてのアレイ上で使用されているデータの合計です。たとえば、各ディスクアレイに固有のライセンスカテゴリが 1 つずつ、合計 4 つの ZDB ライセンスがインストールされていて、EMC Symmetrix に 2TB、P9000 XP アレイ に 2TB、P6000 EVA アレイ に 6TB のバックアップを行うものとします。この場合、10 ライセンスが必要となりますが、4 ライセンスしかないため、ライセンス確認では、ゼロダウンタイムバックアップ使用権 (1TB) 6 ライセンス (10 必要で、4 つインストール済み) の追加が必要であるとレポートされます。

```
#omnicc -check_licenses -detail
------------------------------------------------------------
ライセンスカテゴリ                    :ゼロダウンタイムバックアップ使用権(1TB)
インストールされたライセンス容量:4TB
使用されているライセンス容量      :10.0TB
必要な追加のライセンス容量        :6TB

サマリー
-------
説明                                                必要なライセンス
ゼロダウンタイムバックアップ使用権(1TB)                    6

ライセンスがカバーされていません。
```

以前の EMC Symmetrix および P9000 XP アレイ 用の無制限 ZDB ライセンスは、以下のようにレポートされます。

- EMC Split Mirror 使用権 (B6959AA) は、EMC Symmetrix/DMX 用 ZDB (1TB) (B6959CA) 3 ライセンス分としてレポートされます。
- HP XP Split Mirror 使用権 (B7023AA) は、HP P9000 XP ディスクアレイファミリ ZDB (1TB) (B7023CA) 3 ライセンス分としてレポートされます。
- EMC Symmetrix 用ゼロダウンタイムバックアップ使用権 (1 台) (B6959BA) は、EMC Symmetrix/DMX 用 ZDB (1TB) (B6959CA) 3 ライセンス分としてレポートされます。
- HP StorageWorks XP 用ゼロダウンタイムバックアップ使用権 (1 台) (B7023BA) は、HP P9000 XP ディスクアレイファミリ ZDB (1TB) (B7023CA) 3 ライセンス分としてレポートされます。

これは、以前の EMC Symmetrix および P9000 XP アレイ 用のライセンスも同様に、ゼロダウンタイムバックアップ使用権 (1TB) 3 ライセンス分としてレポートされることを意味します。

たとえば、システム上に各ライセンスカテゴリから 1 つの ZDB ライセンスがインストールされていて、ライセンス確認でゼロダウンタイムバックアップ使用権 (1TB) が 16 (1+1+1+1+3+3+3+3) ライセンス分インストールされているものとします。

- インスタントリカバリ使用権 (1TB) (B7028AA) は、以前の Data Protector リリースのディスクアレイ固有のインスタントリカバリ使用権を置き換えます。
  - HP Modular SAN Array 1000 用 IR 使用権 (1TB) (HP Modular SAN Array 1000 用インスタントリカバリ使用権 (1TB) (B7037AA))
  - HP P6000 EVA ディスクアレイファミリ 用 IR 使用権 (1TB) (汎用インスタントリカバリ使用権 (1TB) (B7028AA))

- HP P9000 XP ディスクアレイファミリ 用 IR 使用権 (1TB) (HP P9000 XP インスタントリカバリ使用権 (1TB) (B7026CA))

すべてのディスクアレイ固有のライセンスは、ライセンスチェッカーによって、汎用インスタントリカバリ使用権 (1TB) 1 ライセンス分としてレポートされます。インストールされている汎用ライセンスの容量は、すべてのディスクアレイ固有のライセンスごとに増加します。ライセンス容量は、すべてのアレイ上で使用されているデータの合計です。

```
#omnicc -check_licenses -detail
----------------------------------------------------
ライセンスカテゴリ                          :インスタントリカバリ使用権(1TB)
インストールされているライセンス容量: 3TB
使用されているライセンス容量          : 5.0TB
必要な追加のライセンス容量            : 2TB

サマリー
-------
説明                                                必要なライセンス
インスタントリカバリ使用権(1TB)                                2

ライセンスがカバーされていません。
```

ライセンスの履行はライセンスのチェックよりも強力になります。ZDB バックアップ中は、ライセンス確認で十分な数の ZDB および IR 使用権がレポートされていても、特定のストレージアレイのライセンスが足りないためにバックアップが実行できない場合があります。

Data Protector パスワード

Data Protector 製品のインストール後は、60 日間製品を利用できます。この期間が過ぎると、Cell Manager に恒久パスワードをインストールしてソフトウェアを有効にする必要があります。恒久パスワードがなくても Data Protector Cell Manager でソフトウェアを起動することはできますが、特定の Data Protector 機能に必要なライセンスにはパスワードが必要なため、構成作業を行うことはできません。

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、インストール時に製品に組み込まれています。インストール後は、Data Protector によってサポートされている任意のシステム上で、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 (PDC)** に恒久パスワードを請求し、インストールする必要があります。

- 恒久パスワード

  Data Protector 製品は、購入者が恒久パスワードを取得する権利を与える**権利保証書 (Entitlement Certificate)** とともに出荷されます。必要なライセンスをすべて購入して恒久パスワードを取得すると、ユーザーのバックアップ方針に合った Data Protector セルを構成できます。恒久パスワードを請求する前に、Cell Manager システムを決定し、セル構成条件を理解しておくことが重要です。

- 緊急用パスワード

  緊急事態が発生して、インストールされているパスワードが現行のシステム構成と一致しなくなった場合に、緊急用または予備パスワードを使用することができます。これらのパスワードを使用すると、任意のシステムを 120 日間操作できます。

  緊急用パスワードは、サポートサービスによって発行されます。緊急用パスワードは、HP サポート担当者によって請求され、HP サポート担当者に対して発行されます。サポートに問い合わせるか、HP のライセンスサイト (http://www.webware.hp.com) を参照してください。 http://www.webware.hp.com .

  緊急用パスワードの目的は、元のシステムを再構成する間、または新しい恒久的なインストール先に移るまでの間、バックアップ操作を可能にすることです。ライセンスを移動す

る場合は、License Move Form に必要事項を入力し、**HP Password Delivery Center (PDC)** に送るか、パスワードの生成や移動が可能な Web サイト (http://www.webware.hp.com) を利用します。

パスワードの取得およびインストール方法の詳細は、「恒久パスワードの取得とインストール」 (196 ページ) 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

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ます。このフォームの場所とフォームの入力方法は、「Data Protector ライセンスフォーム」 (203 ページ) を参照してください。
2. 製品構成の詳細は、「Data Protector 8.00 の製品構成とライセンス」 (199 ページ) を参照してください。請求フォームを送るときと同じ方法で、**HP Password Delivery Center** から恒久パスワードが届きます。たとえば、請求フォームを電子メールで送信した場合は、恒久パスワードは電子メールで送信されます。
3. 次のいずれかの作業を行います。
   - 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、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** に電子メールで送信します。

       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。ファイルは、Cell Manager またはインストールメディアに含まれています。

       Windows Cell Manager の場合:
       Data_Protector_home\Docs\license_forms.txt

       UNIX Cell Manager の場合:/opt/omni/doc/C/license_forms_UNIX

       Windows 用のインストール DVDCD-ROM の場合:
       Disk_Label:\Docs\license_forms.txt

       上記のフォームを使用して、 **Password Delivery Center (HP PDC)** へのメッセージをコピーして貼り付けることもできます。

       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

この項では、**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手順を説明します。

前提条件

HP Password Delivery Center から恒久パスワードが届き、Cell Manager に Data Protector ユーザーインタフェースがインストールされている必要があります。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。

GUI を使用する場合

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 ペインで **[Data Protector** セル**]** を右クリックし、**[**ライセンスの追加**]** をクリックします。
3. パスワードは、『パスワード証明書』に記載されているとおりに入力します。

   パスワードは、4 文字ごとの可変長グループをスペースで区切ったグループと、それに続く文字列で構成されます。パスワードの中に行送り文字や改行文字を含めることはできません。パスワードの例を次に示します。

   ```
   QB9A AQEA H9PQ KHU2 UZD4 H8S5 Y9JL 2MPL B89H MZVU EUJV KCS9 KHU4
   9AC2 CRYP DXMR KLLK XVSS GHU6 D2RJ N6KJ 2KG8 PVRJ 37LX DJ2J EWMB
   A3PG 96QY E2AW WF8E NMXC LNCK ZVWM 9AKS PU3U WCZ8 PSJ5 PQKM 5KCC
   FYDE 4MPM 9GUB C647 WEQX 4NMU BGN5 L8SM 23TX ANTR VFPJ PSJL KTQW
   U8NK H4H4 TB4K L4XQ "Product; Cell Manager for UNIX"
   ```

   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。

Cell Manager 上の以下のファイルにパスワードが書き込まれます。

Windows システムの場合:

Data_Protector_program_data\Config\server\Cell\lic.dat

UNIX システムの場合: /etc/opt/omni/server/cell/lic.dat

CLI を使用する場合

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. 次のコマンドを実行します。

   ```
   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。パスワードは 1 行で、埋め込みの改行が含まれないようにしてください。パスワードは引用符で囲まれている必要があります。パスワードに引用符に囲まれた説明が含まれる場合は、説明を示す引用符の直前にバックスラッシュが必要です。例および詳細は、omnicc の man ページまたは『HP Data Protector Command Line Interface Reference』を参照してください。

パスワードを Cell Manager 上の以下のファイルに追加することもできます。

Windows システムの場合:

Data_Protector_program_data\config\server\cell\lic.dat

UNIX システムの場合: /etc/opt/omni/server/cell/lic.dat

ファイルが存在しない場合は、vi や メモ帳などのエディターを使用して作成します。パスワードの例は、グラフィカルユーザーインタフェース用の手順ステップ 3を参照してください。

パスワードの検証

GUI を使用する場合

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 GUI で以下の手順に従います。

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。インストールされている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間違っている場合は、「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。

CLI を使用する場合

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、以下の手順に従います。

```
omnicc -password_info
```

このコマンドを実行すると、インストールされている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間違っている場合は、「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 を使用する場合

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確認できます。

1. Data Protector Manager を起動します。
2. メニューバーで、**[**ヘルプ**]**、**[**情報**]** の順にクリックします。[Manager について] ウィンドウが開き、インストールされているライセンスが表示されます。

CLI を使用する場合

コマンドラインを使用する場合は、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. 次のコマンドを実行します。

   ```
   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する場合。
- 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 セルに移動する場合。

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、以下の手順に従います。

1. 新しい Cell Manager ごとに**ライセンス移動フォーム (License Move Form)** を 1 つ作成し、**HP Password Delivery Center** に送付します。現在は購入できない製品のライセンスを移動

する場合は、以前のバージョンに付属している **License Move Forms** を使用してください。「Data Protector ライセンスフォーム」 (203 ページ) を参照してください。

フォームでは、既存の Cell Manager から移動するライセンスの数を明記する必要があります。

2. 以下のファイルを削除します。

   Windows システムの場合:

   Data_Protector_program_data\config\server\cell\lic.dat

   UNIX システムの場合:

   /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 (PDC)** 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。パスワードは、新しい Cell Manager ごとに配布されます。ライセンスが現在の Cell Manager に残される場合は、現在の Cell Manager にも新しいパスワードが配布されます。現在の Cell Manager のパスワードエントリは、新しいパスワードによって置き換えられます。

集中型ライセンス

Data Protector では、マルチセル環境全体を対象とする集中型ライセンスを構成できます。これにより、ライセンスを簡単に管理できるようになります。すべてのライセンスは、Manager-of-Managers (MoM) Manager システムに保管されます。ライセンスは、MoM Manager 上で構成された状態で、特定のセルに割り当てられます。

ライセンスの構成方法の詳細は、『HP Data Protector 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 (再割り当て) することができます。詳細は、『HP Data Protector ヘルプ』の索引「MoM 環境」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、ライセンスを請求する前に MoM 機能を確認してください。集中型ライセンスを後から適用する場合は、適用時に移動の手順を実行する必要があります。

注記: MoM 機能によって、集中型ライセンスが実現されます。これは、すべてのライセンスを MoM Manager にインストールしてから、MoM セルに属する Cell Manager にライセンスを配布できることを意味します。後から MoM セル間でライセンスを移動 (再配布) することもできます。詳細は、『HP Data Protector ヘルプ』の索引「MoM 環境」を参照してください。

Data Protector 8.00 の製品構成とライセンス

この項では、Data Protector 製品構成の使用方法について説明しており、購入する必要がある製品番号を簡単に特定できます。

Data Protector 8.00 製品構成およびライセンスには、 次の 2 つのモデルがあります。

- 容量ベースのライセンス設定例は、「HP Data Protector 製品構成」 (201 ページ) を参照してください。
- 従来のライセンス設定例は、「HP Data Protector の製品構成: 従来のライセンス」 (202 ページ) を参照してください。

製品構成は、製品構成例に示すように、いくつかのセクションに分かれています。

従来のライセンス方法を使用する Data Protector ソリューションは、これら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 52 HP Data Protector 製品構成

HP Data Protector software SKU Reference Sheet

CAPACITY BASED LICENSE METHOD

HP SKU	Description	9X5 Support	24X7 Support	Band
Capacity License Products per TB				
TF521AA/E	1-9 TB LTU	HM611A1/3/4/5	HM610A1/3/4/5	96Z
TF542AA/E	10-49TB LTU	HM611A1/3/4/5	HM610A1/3/4/5	7RZ
TF543AA/E	50-99 TB LTU	HM611A1/3/4/5	HM610A1/3/4/5	7RY
TF544AA/E	100-249 TB LTU	HM611A1/3/4/5	HM610A1/3/4/5	R1J
TF558AA/E	250-499 TB LTU	HM611A1/3/4/5	HM610A1/3/4/5	7RV
TF561AA/E	500-1000 TB LTU	HM611A1/3/4/5	HM610A1/3/4/5	1KB
TF582AA/E	>1000TB	HM611A1/3/4/5	HM610A1/3/4/5	7UF

TRADITIONAL LICENSE METHOD

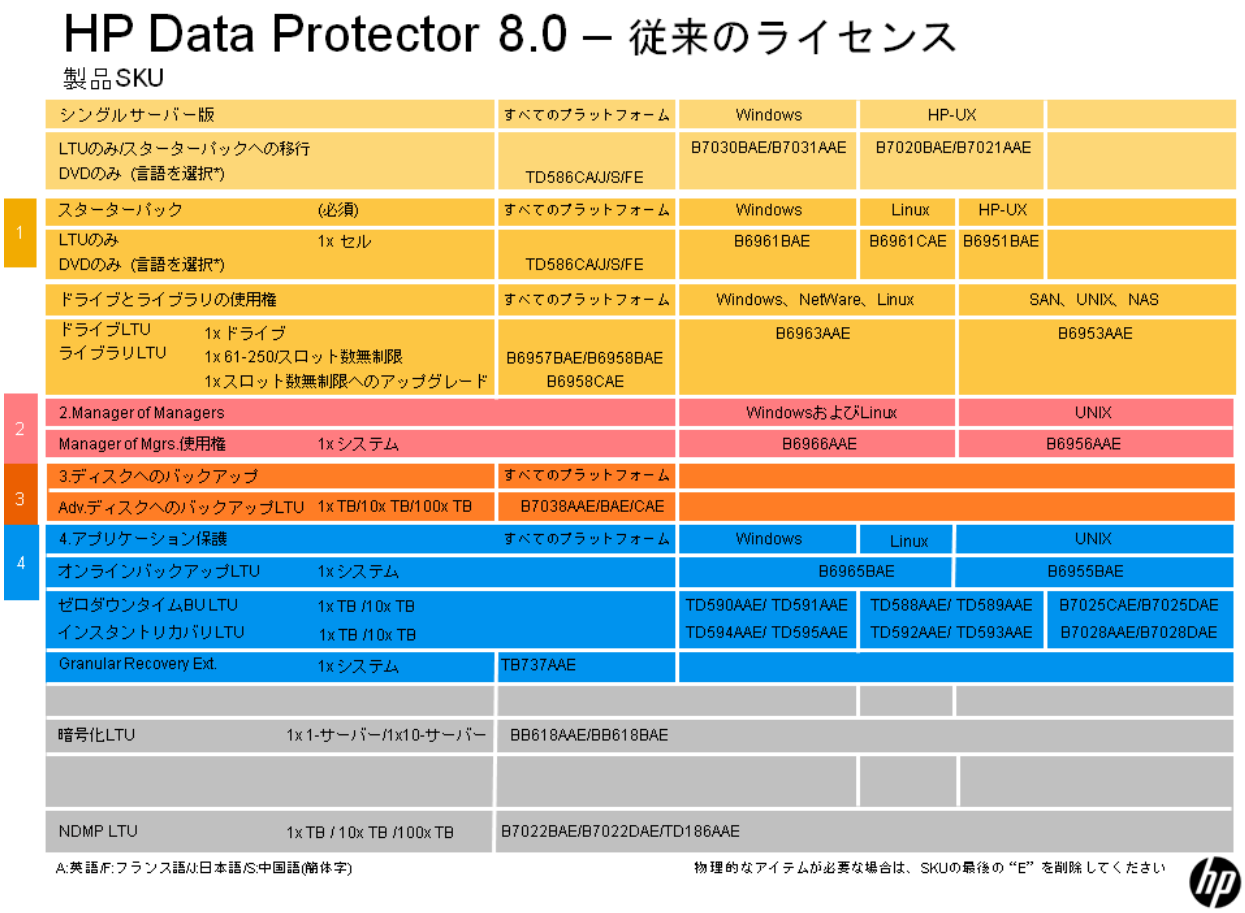
HP SKU	Description	9X5 Support	24X7 Support	Band
Starter Packs				
B6961BA/E	LTU Only – Windows	HM611A1/3/4/5	HM610A1/3/4/5	43B
B6951BA/E	LTU Only – HP-UX	HM611A1/3/4/5	HM610A1/3/4/5	7RW
B6961CA/E	LTU Only – Linux	HM611A1/3/4/5	HM610A1/3/4/5	43B
Drive and Library Extension				
B6963AA/E	Drive LTU – Windows / Linux / NetWare (1 x tape drive)	HM611A1/3/4/5	HM610A1/3/4/5	1QK
B6953AA/E	Drive LTU – UNIX / SAN / NAS (1 x tape drive)	HM611A1/3/4/5	HM610A1/3/4/5	7RV
B6957BA/E	Library LTU – ALL platforms (1x 61-250 slots)	HM611A1/3/4/5	HM610A1/3/4/5	7S4
B6958BA/E	Library LTU – ALL platforms (Unlimited slots)	HM611A1/3/4/5	HM610A1/3/4/5	7S8
B6958CA/E	Library LTU – Upgrade to unlimited (ALL platforms)	HM611A1/3/4/5	HM610A1/3/4/5	7S5
Backup To Disk				
B7038AA/E	Advanced Backup to Disk LTU – (1 x 1TB)	HM611A1/3/4/5	HM610A1/3/4/5	7TU
B7038BA/E	Advanced Backup to Disk LTU – (1 x 10TB)	HM611A1/3/4/5	HM610A1/3/4/5	7S5
B7038CA/E	Advanced Backup to Disk LTU – (1 x 100TB)	HM611A1/3/4/5	HM610A1/3/4/5	7SH
Application Protection				
B6965BA/E	Online Backup LTU – Windows / Linux (1 x system)	HM611A1/3/4/5	HM610A1/3/4/5	1QL
B6955BA/E	Online Backup LTU – UNIX (1 x system)	HM611A1/3/4/5	HM610A1/3/4/5	7S0
TB737AA/E	Granular Recovery LTU – Windows / Linux (1 x system)	HM611A1/3/4/5	HM610A1/3/4/5	43S
TD590AA/E	Zero Downtime Backup LTU – Windows (1 x 1TB)	HM611A1/3/4/5	HM610A1/3/4/5	WXE
TD591AA/E	Zero Downtime Backup LTU – Windows (1 x 10TB)	HM611A1/3/4/5	HM610A1/3/4/5	WXD
TD588AA/E	Zero Downtime Backup LTU – Linux (1 x 1TB)	HM611A1/3/4/5	HM610A1/3/4/5	7RQ
TD589AA/E	Zero Downtime Backup LTU – Linux (1 x 10TB)	HM611A1/3/4/5	HM610A1/3/4/5	7S8
B7025CA/E	Zero Downtime Backup LTU – UNIX (1 x 1TB)	HM611A1/3/4/5	HM610A1/3/4/5	7RT
B7025DA/E	Zero Downtime Backup LTU – UNIX (1 x 10TB)	HM611A1/3/4/5	HM610A1/3/4/5	7SC
TD594AA/E	Instant Recovery LTU – Windows (1 x 1TB)	HM611A1/3/4/5	HM610A1/3/4/5	7RE
TD595AA/E	Instant Recovery LTU – Windows (1 x 10TB)	HM611A1/3/4/5	HM610A1/3/4/5	7RV
TD592AA/E	Instant Recovery LTU – Linux (1 x 1TB)	HM611A1/3/4/5	HM610A1/3/4/5	43B
TD593AA/E	Instant Recovery LTU – Linux (1 x 10TB)	HM611A1/3/4/5	HM610A1/3/4/5	7S0
B7028AA/E	Instant Recovery LTU – UNIX (1 x 1TB)	HM611A1/3/4/5	HM610A1/3/4/5	7RL
B7028DA/E	Instant Recovery LTU – UNIX (1 x 10TB)	HM611A1/3/4/5	HM610A1/3/4/5	7S5
NDMP Backup				
B7022BA/E	Direct Backup LTU – NDMP (1 x 1TB)	HM611A1/3/4/5	HM610A1/3/4/5	4TF
B7022DA/E	Direct Backup LTU – NDMP (1 x 10TB)	HM611A1/3/4/5	HM610A1/3/4/5	4U7
TD186AA/E	Direct Backup LTU – NDMP (1 x 100TB)	HM611A1/3/4/5	HM610A1/3/4/5	7SH
Manager of Managers				
B6966AA/E	Manager of Managers LTU – Windows/Linux (1system)	HM611A1/3/4/5	HM610A1/3/4/5	1Ql
B6956AA/E	Manager of Managers LTU – UNIX (1system)	HM611A1/3/4/5	HM610A1/3/4/5	7RV

ADD-ON PRODUCTS

HP SKU	Description	9X5 Support	24X7 Support	Band
TD586CA/E	Media SKUs (For All Platforms) – English	-	-	-
BB618AA/E	Encryption LTU – (1 Server)	HM611A1/3/4/5	HM610A1/3/4/5	7RA
BB618BA/E	Encryption LTU – (10 Server pack)	HM611A1/3/4/5	HM610A1/3/4/5	7RP
B7100AA/E	Media Operations LTU – (1 x 2,000 tape cartridges)	HM611A1/3/4/5	HM610A1/3/4/5	7S5
B7101AA/E	Media Operations LTU – (1 x 10,000 tape cartridges)	HM611A1/3/4/5	HM610A1/3/4/5	1QN
B7102AA/E	Media Operations LTU – (Unlimited media)	HM611A1/3/4/5	HM610A1/3/4/5	3Z1
TD587BA/E	Media Operations – CD Only	HM611A1/3/4/5	HM610A1/3/4/5	97D
TD729AA/E	HP Data Protector Reporter 5 MAL SW LTU (Perpetual)	HM611A1/3/4/5	HM610A1/3/4/5	WVW
TD720AA/E	HP Data Protector Reporter 5 MAL SW LTU (1 Year Term)	-	-	-
TD726AA/E	Backup Manager MAL/server	HM611A1/3/4/5	HM610A1/3/4/5	WVW
TD723AA/E	Reporter Optimizer for custom report (Perpetual)	HM611A1/3/4/5	HM610A1/3/4/5	9X8
TD714AA/E	Reporter Optimizer for custom report (Term)	-	-	-
T4283EA/E	HP Data Protector Reporter – CD Only	-	-	-

May 2013

図 53 HP Data Protector の製品構成: 従来のライセンス



重要: このガイドの製品構成は、**例示のみを目的として**記載されています。最新の製品構成は、次の Web サイト http://h18006.www1.hp.com/products/quickspecs/Division/Division.html#12647 で入手可能です。

Data Protector では、以前の Data Protector バージョンの製品番号が利用されます。そのために、既存の Data Protector ライセンスは移行後も有効です。

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。

- 一時パスワードは任意の Cell Manager 候補で使用できます。ただし、その他のすべてのパスワードには、関連するプラットフォームを指定する必要があります。この場合は、中心的な Data Protector 管理システムとなる Cell Manager も指定する必要があります。恒久パスワードを取得する前に、一時パスワードを使用してセル構成条件を完全に理解しておくことが重要です。
- 恒久パスワードは、別の Cell Manager に移動できます。ただし、ライセンス移動フォーム (License Move Form) を **HP Password Delivery Center (PDC)** に送る必要があります。
- 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) 機能の一部として集中型ライセンスが提供されます。複数のセル用に複数のライセンスを購入した場合は、MoM システムにすべてのライセンスをインストールしておくことができます。
- 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。

注記: Cell Manager の IP アドレスを変更する場合、Cell Manager を別のシステムに移動する場合、またはセル間でライセンスを移動する場合 (この場合、MoM 機能を使用しない) は、**HP Password Delivery Center (PDC)** に連絡し、ライセンスを更新する必要があります。HP Password Delivery Center への連絡については、「恒久パスワードの取得とインストール」(196 ページ) を参照してください。

Data Protector 8.00 へのライセンス移行

Data Protector 8.00 に直接移行します。Data Protector の以前のリリースのライセンスは、自動的に移行されます。

Data Protector A.06.11、6.20、または 7.00 のサポート契約を結んでいるお客様は、Data Protector 8.00 を無料で受け取ることができます。環境を Data Protector 8.00 にアップグレードすると、A.06.11、6.20、または 7.00 で使用していた機能は追加費用なしで Data Protector 8.00 で使用できるようになります。新しい機能拡張が必要な場合は、新しいライセンスを購入するだけで入手できます。

Data Protector ライセンスフォーム

この章では、Data Protector ライセンスフォームについて説明します。以下のいずれかの方法で恒久パスワードを注文するには、これらのフォームに記入してください。

- オンラインの **Password Delivery Center** サイト (http://www.webware.hp.com) にアクセスし、恒久パスワードを請求します。
- 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 システムまたはインストールメディアに含まれています。

  HP-UX システムおよび Linux システムの場合: `/opt/omni/doc/C/license_forms_UNIX`

  Windows 用のインストール DVD-ROM の場合: *`DriveLetter`*`:Docs\license_forms.txt`

  または、電子的なファイルを使用して、メッセージを **Password Delivery Center (PDC)** に「コピー」して「貼り付け」ます。

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	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	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。
IP アドレス (IP Address)	このフィールドでは、**Password Delivery Center** がパスワードを生成するシステムが定義されます。集中ライセンスを使用する場合

	(MoM 環境のみ)、このシステムは MoM Manager システムにする必要があります。 Cell Manager に複数の LAN カードがある場合、どの IP アドレスでも入力できますが、HP ではプライマリ IP アドレスを入力することをお勧めしています。 MC/ServiceGuard 環境または Microsoft Cluster 環境で Data Protector をお使いの場合、仮想サーバーの IP アドレスを入力します。セキュリティの詳細については、『HP Data Protector 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** の横のフィールドに、この Cell Manager にインストールするライセンスの数量を入力します。この数量は、**Order Number** で購入する全ライセンスでも一部でもかまいません。

6 インストールのトラブルシューティングとアップグレード

この章では、インストール関連の問題に関する情報を提供します。Data Protector の一般的なトラブルシューティング情報については、『HP Data Protector トラブルシューティングガイド』を参照してください。

Windows 用 Cell Manager インストール時の名前解決に関する問題

Windows での Data Protector Cell Manager のインストール時に、必要とされる DNS または LMHOSTS ファイルがセットアップされていないことが検出され、警告メッセージが表示されます。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にも通知されます。

問題

DNS または LMHOSTS の使用時に名前解決に失敗する

名前の解決に失敗すると、"error expanding hostname" というメッセージが表示され、インストールが中止されます。

- DNS の使用時に名前解決の問題が発生した場合は、現在の DNS 構成についての警告メッセージが表示されます。
- LMHOSTS ファイルの使用時に名前解決の問題が発生した場合は、LMHOSTS ファイルの構成をチェックするように指示する警告メッセージが表示されます。
- DNS と LMHOSTS のどちらも構成していない場合は、DNS または LMHOSTS による名前解決を TCP/IP のプロパティダイアログで有効にするように指示する警告メッセージが表示されます。

操作

DNS または LMHOSTS ファイルの構成をチェックするか、構成を有効にします。「Data Protector セル内の DNS 接続の確認」 (205 ページ) 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。そうでない場合、インストールは中止されます。

操作

TCP/IP の設定を確認します。詳細は、「デフォルトの Data Protector Inet ポートの変更」 (227 ページ) を参照してください。

Data Protector セル内の DNS 接続の確認

DNS(ドメインネームシステム) は、TCP/IP ホスト用のネームサービスです。DNS は、ホスト名および IP アドレスのリストで構成されます。これにより、ユーザーは、IP アドレスではなくホスト名でリモートシステムを指定できます。DNS は、Data Protector セルのメンバー間で適切な通信が行われることを保証します。

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 では、Data Protector セルのメンバー間の DNS 接続を確認するための`omnicheck`が提供されています。このコマンドでは、セル内のあらゆる接続のチェックが可能ですが、Data Protector セルで重要な次の接続を検証すれば十分です。

- Cell Manager からその他すべてのセルメンバーへの接続、およびその逆。
- Media Agent からその他すべて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

- コマンドは、セルのメンバー間の接続のみを検証します。通常、DNS の接続は検証されません。

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]` オプションが指定されると、すべてのメッセージが返されます。このオプションを設定しなければ (デフォルト)、チェック失敗に関するメッセージだけが返されます。

詳細は、`omnicheck`man ページを参照してください。

`omnicheck` コマンドの出力メッセージの一覧は、「出力メッセージ」(206 ページ)を参照してください。DNS の名前解決で問題が発生したことを示すメッセージが表示された場合は、『HP Data Protector トラブルシューティングガイド』の「ネットワークおよび通信のトラブルシューティング」の章を参照してください。

表 9 出力メッセージ

出力メッセージ	意味
client_1 が *client_2* に接続できません。	*client_2* への接続がタイムアウトしました。
client_1 は *client_2* に接続していますが接続先のシステムは *client_3* として存在しています。	*client_1* の *%SystemRoot%*\System32\drivers\etc\hosts/etc/hosts (UNIX システム) ファイルが正しく構成されていないか、*client_2* のホスト名が DNS 名に一致しません。
client_1 から *client_2* に接続できません。	*client_2* がアクセス不能 (接続されていないなど) か、*client_1* 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ません。
client_1 と *client_2* の接続をチェック中	

表 9 出力メッセージ (続き)

出力メッセージ	意味
すべてのチェックが正常に完了しました。	
number_of_failed_checks のチェックが失敗しました。	
client はこのセルのメンバーではありません。	
client に接続しましたが、旧バージョンのようです。Hostname は検証されません。	

共通の問題のトラブルシューティング

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。
- システムが、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。

Data Protector 8.00 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 のアップグレード手順における エラーです。Microsoft Installer バージョン 1.x のデータ情報が Data Protector によってコンピューターにインストールされる Microsoft Installer バージョン 2.x に移行されないために発生します。

操作

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

Cell Manager 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。)

対処方法

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。

msvcr90.dll file is not found (msvcr90 ファイルが見つかりません)

ネットワーク共有では msvcr90.dll (小文字) のみが使用可能になっているため、MSVCR90.dll ライブラリ (大文字) が見つかりません。MSVCR90.dll と msvcr90.dll が同じファイルとして取り扱われていないため、setup.exe が適切な dll を見つけることができません。

操作

ファイル名を `msvcr90.dll`(小文字) から `MSCVCR90.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。

問題

インストールをキャンセルしても、すでにインストールされたコンポーネントがアンインストールされない

コンポーネントの一部がすでにインストールされている状態で Data Protector のインストールをキャンセルすると、それらのコンポーネントはアンインストールされません。インストールは終了し、エラーメッセージが表示されます。

操作

インストールのキャンセル後に、すでにインストールされているコンポーネントを手動でアンインストールします。

UNIX システムでのインストール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に失敗する

UNIX クライアントのインストールまたはアップグレードが失敗し、次のエラーメッセージが表示されることがあります。

```
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ときは、インストールするパッケージのうち、最大のパッケージを十分格納できるだけの空き領域がクライアントシステムの `/tmp` フォルダー内に存在しなければなりません。Solaris クライアントシステムでは、`/var/tmp` フォルダー内にも同じ量の空き領域が必要です。

操作

上記のディレクトリに十分な空き領域があることを確認した上で、インストール/アップグレード手順を再開します。

ディスクスペース要件は、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。

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.
```

操作

`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

Mac OS X クライアントのインストールに関する問題

Mac OS X クライアントを Data Protector セルに追加するときに、com.hp.omni プロセスが開始されません。

操作

Mac OS X では、com.hp.omni プロセスを開始するために launchd が使用されます。

サービスを開始するには、次のディレクトリに移動します。

```
cd /usr/omni/newconfig/System/Library/LaunchDaemons
```

以下を実行します。

```
launchctl load com.hp.omni
```

問題

UNIX 用のインストール後に Inet プロセスを開始できない Cell Manager

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。

エラー: 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。

操作

以下のコマンドにより、inetd または xinetd サービスが動作しているかどうかチェックします。

HP-UX システムの場合: `ps -ef | grep inetd`

Linux システムの場合: `ps -ef | grep xinetd`

サービスを開始するには、次のコマンドを実行します。

HP-UX システムの場合: `/usr/sbin/inetd`

Linux システムの場合: `rcxinetd start`

Windows システムでのインストールのトラブルシューティング

問題

Windows クライアントのリモートインストールに失敗する

Data Protector クライアントの Windows システムへのリモートインストールが失敗し、以下のエラーメッセージが報告されました。

[正常域] クライアント computer.company.com に接続中...

[正常域] 実行されました。

[正常域] クライアント computer.company.com に Data Protector ブートストラップサービスをインストール中...

[危険域] クライアント computer.company.com の SCM (Service Control Manager) に接続できません:[5] アクセスが拒否されました。

操作

1. インストールサーバーシステムの場合、次のコマンドを実行して、リモートインストール中にインストールサーバーで使用するローカルオペレーティングシステムの管理者ユーザーグループからユーザーアカウントをマークします。

   ```
   omniinetpasswd -inst_srv_user User@Domain
   ```

このユーザーアカウントは、ローカル Inet 構成にあらかじめ追加されている必要があります。詳細は、『HP Data Protector Command Line Interface Reference』の `omniinetpasswd` コマンドの説明を参照してください。

2. Data Protector クライアントのリモートインストールを再度開始します。

問題

Windows クライアントのリモートインストールが失敗する (Windows XP)

Windows XP システムがワークグループのメンバーで、簡易ファイルの共有セキュリティポリシーが有効になっていると、ネットワーク経由でこのシステムにアクセスするユーザーは、Guest アカウントしか使用できません。リモートインストールには管理者権限が必要なため、Data Protector は、Data Protector クライアントのリモートインストール中に有効なユーザー名とパスワードを繰り返し要求します。

操作

簡易ファイルの共有を無効にします。Windows XP で **[Windows** エクスプローラ**]** または **[**マイコンピュータ**]** を開き、**[**ツール**]** メニューをクリックして **[**フォルダオプション**]** をクリックします。**[**表示**]** タブを開いて、**[**簡易ファイルの共有を使用する **(**推奨**)]** チェックボックスをオフにします。

以下の場合は、簡易ファイルの共有ポリシーは無視されます。

- コンピューターがドメインのメンバーである場合
- ネットワークアクセス：ローカルアカウントの共有とセキュリティモデルのセキュリティポリシー設定がクラシック：ローカルユーザーがローカルユーザーとして認証するに設定されている場合

問題

Cell Manager をインストールすると、アプリケーションサーバーサービスが起動しない

アプリケーションサーバーサービスが以下のメッセージを表示して起動しない

`Data Protector` アプリケーションサーバーが起動する前にタイムアウトします。

以下のエラーが、インストールサマリーログファイルにログ記録されます。

```
Caused by: org.jboss.as.cli.
CommandLineException:The controller is not available at localhost:9999
```

PATH システム環境変数にディレクトリ `%SystemRoot%\system32` が含まれないため、インストールプロセスがさまざまなユーティリティにアクセスできません。

操作

PATH 変数に `%SystemRoot%\system32` ディレクトリを追加します。

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 `omnicheck -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ーが必要です。

制限事項

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 システムを右クリックします。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、セル内のシステムのインストール結果を確認します。[インストールの検証] ウィンドウが開き、インストールの結果が表示されます。

   詳細は、『HP Data Protector 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、「ログファイルの使用」 (215 ページ) 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 man 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

製品の旧バージョンを長いパスでインストールすると、Data Protector 8.00 へのアップグレードが失敗する

Data Protector 8.00 では、80 文字より長いパスへの Cell Manager のインストールはサポートされていません。この結果、アップグレードが失敗します。

操作

1. Data Protector 8.00 インストール DVD の `x8664\tools\Upgrade` ディレクトリから一時ディレクトリ (`c:\temp` など) に `omnimigrate.pl` スクリプトをコピーします。
2. 次のように `omnimigrate` コマンドを使用して IDB をエクスポートします。

   ```
   perl c:\temp\omnimigrate.pl -export -shared_dir c:\output
   ```

   Data Protector インストールの *`Data_Protector_home`*`\bin` ディレクトリに含まれている Perl バージョンを使用します。
3. Data Protector の旧バージョンを削除しますが、構成とデータベースデータは残します。*`Data_Protector_program_data`*`\db40` ディレクトリは削除しないでください。
4. Data Protector 8.00 をインストールします。インストール先のパスが 80 文字以下であることを確認します。
5. 以下を実行して、すべての Data Protector サービスを停止します。

   ```
   omnisv -stop
   ```

6. 古い *`Data_Protector_program_data`*`\db40` ディレクトリ (このディレクトリは旧バージョンの Data Protector の削除後も残っています) から新しい *`Data_Protector_program_data`*`\db40` フォルダーにファイルをコピーします。DCBF ディレクトリが移動していないことを確認してください。
7. 古い *`Data_Protector_program_data`*`\Config\Server` フォルダーから新しいフォルダーに構成をコピーします。
   a. 古い構成ディレクトリを新しい構成ディレクトリにコピーします。ただし古いファイルはそのまま残します。ファイルは *`Data_Protector_program_data`*`\Config\Server\install` ディレクトリからコピーしないでください。

b. セル構成 (クライアント、インストールサーバー) をす場合は、*Data_Protector_program_data*\Config\Server\cell\cell_info および *Data_Protector_program_data*\Config\Server\cell\installation_servers ファイルをコピーして上書きします。

8. 新しい通知とグローバルオプションファイルをマージします。
   a. 通知をマージするには、次の omninotifupg.exe ツールを実行します。

      ```
      omninotifupg.exe -quiet
      ```

   b. グローバルオプションファイルをマージするには、以下を実行します。

      ```
      mrgcfg.exe -global -except BackupDeviceIdle -rename
      DbFVerLimit=DbFnamesDatLimit,SessSucessfulWhenNoObjectsBackedUp
      =SessSuccessfulWhenNoObjectsBackedUp
      ```

      別の方法として、以前のインストールから手動でグローバルオプションファイルをマージすることもできます。

9. 以下を実行して、Data Protector サービスを開始します。

   ```
   omnisv -start
   ```

10. IDB を新しいインストールにインポートします。そのためには、以下を実行します。

    ```
    omnimigrate.pl -import -shared_dir c:\output -force
    ```

問題

製品の旧バージョンのインストールパスにサポートされていない文字が含まれていると、Data Protector 8.00 へのアップグレードが失敗する

Data Protector 8.00 では、以下の文字を含むパスへの Cell Manager のインストールはサポートされていません。

- 非 ASCII 文字
- "@ "または"# "
- ディレクトリの末尾にある"!"

この結果、アップグレードが失敗します。

操作

1. Data Protector 8.00 インストール DVD の x8664\tools\Upgrade ディレクトリから一時ディレクトリ (c:\temp など) に omnimigrate.pl スクリプトをコピーします。
2. ASCII 名を使用して次のような 2 つのディレクトリを作成します。

   ```
   c:\output\cdb
   ```

   ```
   c:\output\mmdb
   ```

3. MMDB と CDB をエクスポートします。

   ```
   omnidbutil -writedb -cdb c:\output\cdb -mmdb c:\output\mmdb
   ```

   この処理には時間がかかる場合があります。アップグレードにはこのデータは必要ないので、ファイル名のエクスポートが開始されたら、**Ctrl+C** を使用して omnidbutil プロセスを停止できます。

4. 次の omnimigrate コマンドを使用して IDB をエクスポートします。

   ```
   perl c:\temp\omnimigrate.pl -exportNonASCII -shared_dir c:\output
   ```

   Data Protector インストールの *Data_Protector_home*\bin ディレクトリに含まれている Perl バージョンを使用します。

5. ANSI 文字セットファイル `c:\output\old_cm` を作成します。このファイルには以下の 2 つの行を含めます。

   ```
   OLDCM_SHORTNAME=OldCmName OLDCM_ENDIANNESS=LITTLE_ENDIAN
   ```

   OldCmName を、Cell Manager の省略名に置き換えます。
6. Data Protector の旧バージョンを削除しますが、構成とデータベースデータは残します。*Data_Protector_program_data*\db40 ディレクトリは削除しないでください。
7. Data Protector 8.00 をインストールします。インストール先のパスに非 ASCII 文字が含まれていないことを確認します。
8. 以下を実行して、すべて Data Protector サービスを停止します。

   ```
   omnisv -stop
   ```
9. 古い *Data_Protector_program_data*\db40 ディレクトリ (このディレクトリは旧バージョンの Data Protector の削除後も残っています) から新しい *Data_Protector_program_data*\db40 フォルダーにファイルをコピーします。DCBF ディレクトリが移動していないことを確認してください。
10. 古い *Data_Protector_program_data*\Config\Server フォルダーから新しいフォルダーに構成をコピーします。
    a. 古い構成ディレクトリを新しい構成ディレクトリにコピーします。ただし古いファイルはそのまま残します。ファイルは *Data_Protector_program_data*\Config\Server\install ディレクトリからコピーしないでください。
    b. セル構成 (クライアント、インストールサーバー) を残す場合は、*Data_Protector_program_data*\Config\Server\cell\cell_info および *Data_Protector_program_data*\Config\Server\cell\installation_servers ファイルをコピーして上書きします。
11. 次の手順を実行して、新しい通知とグローバルオプションファイルをマージします。
    a. 通知をマージするには、次の `omninotifupg.exe` ツールを実行します。

       ```
       omninotifupg.exe -quiet
       ```
    b. グローバルオプションファイルをマージするには、以下を実行します。

       ```
       mrgcfg.exe -global -except BackupDeviceIdle -rename
       DbFVerLimit=DbFnamesDatLimit,SessSucessfulWhenNoObjectsBackedUp
       =SessSuccessfulWhenNoObjectsBackedUp
       ```

       上記の手順を実行する代わりに、以前行ったインストールから手動でグローバルオプションファイルをマージすることもできます。
12. 以下を実行して、Data Protector サービスを開始します。

    ```
    omnisv -start
    ```
13. IDB を新しいインストールにインポートします。そのためには、以下を実行します。

    ```
    omnimigrate.pl -import -shared_dir c:\output -force
    ```

問題

古い (Raima DB ベースの)IDB が破損していると、アップグレードプロセスが中止される

アップグレード中に、IDB 内の次の破損フィールドが検出され、修正されます。

- メディア `blocks_used` が `0` に設定される
- メディア `blocks_total` が `blocks_used` に設定される
- プール `media_age_limit` がデフォルト値 (同じメディアクラスを持つデフォルトプールの `media_age_limit`) に設定される
- プール `media_overwrite_limit` がデフォルト値 (同じメディアクラスを持つデフォルトプールの `media_overwrite_limit`) に設定される

ただし、IDB 内のその他のフィールドが破損していると、アップグレードは中止されます。

操作

次の手順を実行して、Data Protector のインストールを古いバージョンに戻します。

1. Data Protector 8.00 を削除します。
2. 旧バージョンの Data Protector を再インストールします。
3. 古い IDB を復元します。

もう一度アップグレードを試みる前に、古い IDB を修復する必要があります。詳細については、HP サポートに問い合わせてください。

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 を以前のリリースバージョンからアップグレードすると、IDB およびすべての構成ファイルが使用できなくなります。この問題は、アップグレード手順が何らかの理由で中断された場合に発生します。

操作

アップグレード前に作成しておいたバックアップから 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開してください。

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 のアップグレード終了後に `swlist` コマンドを実行すると、古い Data Protector パッチがインストールされたプログラムとともにリストされます。パッチは、アップグレード中にシステムから削除されますが、sw データベースには残ります。

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、「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」 (148 ページ) を参照してください。

操作

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、"PHSS_30143" パッチを sw データベースから削除するには、以下のコマンドを実行します。

```
swmodify -u PHSS_30143.\* PHSS_30143
```

問題

StorageTek ライブラリを使用する Media Agent クライアントをアップグレードすると、接続に問題が発生する

StorageTek ライブラリを使用するシステム上で Data Protector Media Agent コンポーネントをアップグレードすると、ライブラリに接続できなくなり、ライブラリを使用する Data Protector セッションの応答停止または異常終了が発生します。

操作

StorageTek ライブラリをサポートするサービスやデーモンを再起動すると、問題が解消することがあります。

Windows システムの場合: [管理ツール] の [サービス] を選択し、`LibAttach` サービスを再起動します。

HP-UX および Solaris システムの場合: `/opt/omni/acs/ssi.sh stop` コマンドと `/opt/omni/acs/ssi.sh start ACSLS_hostname` コマンドを実行します。

ACSLS_hostname には、Automated Cartridge System ライブラリソフトウェアがインストールされているシステムの名前を指定します。

AIX システムの場合: `/usr/omni/acs/ssi.sh stop` と `/usr/omni/acs/ssi.sh start` *ACSLS_hostname* コマンドを実行します。*ACSLS_hostname* には、Automated Cartridge System ライブラリソフトウェアがインストールされているシステムの名前を指定します。

Windows システムでのリモートアップグレードのトラブルシューティング

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。

セットアッププロセスの起動時にエラーが発生しました。エラー `=[1326]` ログオン失敗: ユーザー名を認識できないか、またはパスワードが間違っています。

この問題は、インストールサーバーコンピューター上の OmniBack 共有へのアクセス権を持たないユーザーアカウントでリモートコンピューター上の `Data ProtectorInet` サービスが実行されている場合に発生します。多くの場合は、ローカルユーザーを使用したときに発生します。

操作

`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。

UNIX システムでのローカルアップグレードの手動処理

通常、UNIX インストールサーバーおよびインストールサーバー上の Data Protector A.06.11、6.20、7.00 は、自動アップグレード手順を実行する `omnisetup.sh` コマンドを実行してアップグレードします。ただし、手動でアップグレードすることもできます。「ネイティブツールを使用した、HP-UX および Linux システムでのアップグレード」 (223 ページ) 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)
- システムログファイル (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で問題が発生した場合、次のログファイルを確認します。

HP-UX Cell Manager:

- `/var/adm/sw/swinstall.log`
- `/var/adm/sw/swagent.log`(詳細情報)

Linux 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*`\SetupLog.log`

- *Temp*\OB2DBG_*did*__setup_*HostName_DebugNo*_setup.txt(詳細情報)
  ここで、
  - *did*(デバッグ ID) は、デバッグパラメーターを受け付ける最初のプロセスのプロセス ID です。この ID は、デバッグセッションの ID として使用されます。この ID は、以降のすべてのプロセスで使用されます。
  - *HostName* は、トレースファイルが作成されたホストの名前です。
  - *DebugNo* は、Data Protector によって生成された番号です。
- *Temp*\CLUS_DBG_*DebugNo*.TXT(クラスター環境)

Temp ディレクトリの場所は、TEMP 環境変数で指定されます。この変数の値を確認するには、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で問題が発生した場合、次のログファイルを確認します。

UNIX インストールサーバーの場合:

/var/opt/omni/log/IS_install.log

Windows クライアント (コンポーネントのインストール先のリモートシステム):

- *SystemRoot*\TEMP\OB2DBG_*did*_INSTALL_SERVICE_*DebugNo*_debug.txt
- *SystemRoot*\TEMP\CLUS_DBG_*DebugNo*.TXT

Temp ディレクトリの場所は、TEMP 環境変数で指定されます。また、*SystemRoot* は、SystemRoot 環境変数で指定されたパスです。

セッ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。「インストール実行トレースの作成」(217 ページ) 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 Vista、Windows 7、Windows 8、Windows Server 2008、および Windows Server 2012 の場合: *Data_Protector_program_data*\log

その他の Windows システムの場合:*Data_Protector_home*\log

HP-UX、Solaris、Linux の場合: /var/opt/omni/log and /var/opt/omni/server/log

その他の UNIX システムおよび Mac OS X システムの場合: /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	予期しない状況が記録されます。ユーザーにとって役立つものもありますが、主に当社サポートサービスが使用します。
inet.log	Data Protector inet サービスに対する要求が含まれます。クライアント上での Data Protector の最近のアクティビティを確認するために役立ちます。
IS_install.log	リモートインストールのトレース結果が記録されます。インストールサーバーに保存されます。
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	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 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 カスタマーサポートサービスに要求された場合は、debug オプションを使用して、インストールを実行します。以下の debug オプションなどのデバッグの詳細および HP カスタマーサポートサービスに送信するデータの準備に関する詳細は、『HP Data Protector トラブルシューティングガイド』を参照してください。

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 1-200 DebugPostfix
```

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ーシステムの場合:

  Data_Protector_program_data\tmp\OB2DBG_*did*__BM_*Hostname_DebugNo_DebugPostfix*

- リモートシステムの場合:

  SystemRoot:\Temp\OB2DBG_*did*__INSTALL_SERVICE_*Hostname_DebugNo_DebugPostfix*

A UNIX システムネイティブツールを使用した Data Protector のインストールとアップグレード

この付録では、HP-UX システムの `swinstall` と Linux システムの `rpm` など、ネイティブインストールツールを使用して UNIX システム上で Data Protector をインストールおよびアップグレードする方法について説明します。

注記: Data Protector のインストールまたはアップグレードには、`omnisetup.sh` スクリプトを使用することをお勧めします。「UNIX 用 Cell Manager のインストール」(27 ページ) および「UNIX 用 Cell Manager とインストールサーバーのアップグレード」(161 ページ) を参照してください。

ネイティブツールを使用した、HP-UX および Linux システムへのインストール

注記: リモートインストールパッケージの限定セットを使用してインストールサーバーをインストールする場合、HP-UX および Linux へのネイティブインストール手順のみが示されています。Data Protector は、`omnisetup.sh` を使用して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

UNIX Cell Manager を HP-UX 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. HP-UX 用インストール 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]** に*Mountpoint*`/hpux/DP_DEPOT` と入力します。**[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。
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。

   サブプロダクトごとにインストールするかどうかを指定する場合には、**[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。インストールしないパッケージには **[Unmark for Install]** をクリックし、インストールするパッケージには **[Mark for Install]** をクリックして選択します。

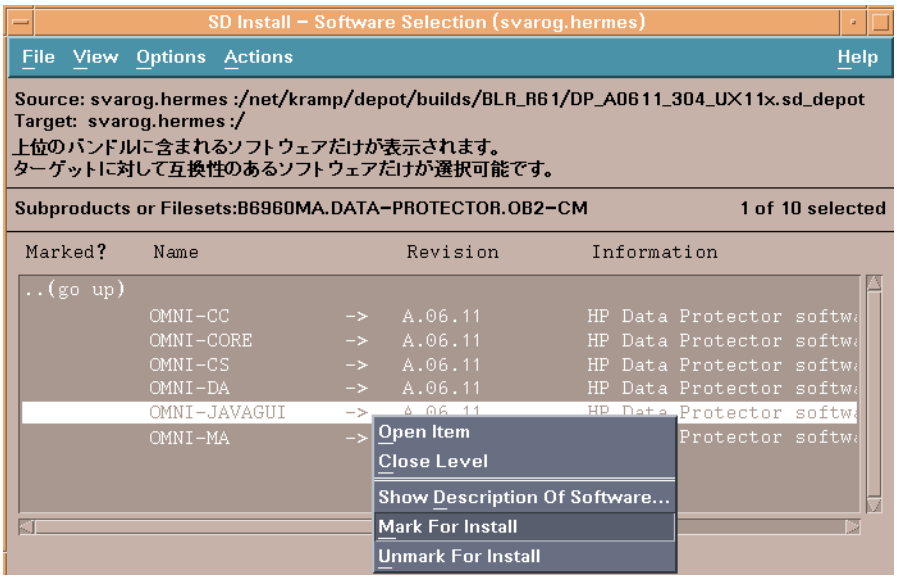
   以下のサブプロダクトが含まれています。

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 (PDF 形式との Data Protector ガイドと WebHelp 形式の『HP Data Protector ヘルプ』を収録)
OB2-IS	Data Protector インストールサーバーでは、以下の操作を行います。

   UNIX 用の Cell Manager をシステムにインストールしているときは、`[Marked?]` ステータスの値 (`OB2-CM` パッケージの横) が `[Yes]` になっていることを確認してください。「[SD install - software selection] ウィンドウ 」(219 ページ) 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。

図 54 [SD install - software selection] ウィンドウ



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。

注記: ネットワーク上のテープデバイスからソフトウェアをインストールするには、まずソースディレクトリをコンピューターにマウントする必要があります。

rpm を使用した Linux システムへの Cell Manager のインストール

Cell Manager 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. Linux 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. `linux_x86_64/DP_DEPOT` ディレクトリへ移動します。
3. 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.08.00-1.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。

   以下のコンポーネント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-TS-CORE	Data Protector コアテクノロジスタックライブラリ
OB2-CC	Cell Console ソフトウェア。これには、コマンドラインインタフェースが含まれます。
OB2-TS-CS	Cell Manager テクノロジスタックライブラリ
OB2-TS-JRE	Data Protector で使用する Java ランタイム環境。
OB2-TS-AS	Data Protector アプリケーションサーバー
OB2-WS	Data Protector Web サービス
OB2-JCE-DISPATCHER	ジョブコントロールエンジンのディスパッチャー
OB2-JCE-SERVICEREGISTRY	ジョブコントロールエンジンサービスのレジストリ
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。
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 ドキュメントサブプロダクト (PDF 形式との Data Protector ガイドと WebHelp 形式の『HP Data Protector ヘルプ』を収録)

重要: Linux のコンポーネントは相互に依存しています。これらのコンポーネントは、上記の順序でインストールする必要があります。

4. Data Protector サービスを再起動します。

```
omnisv stop
omnisv start
```

swinstall を使用した HP-UX システムへのインストールサーバーのインストール

1. HP-UX 用インストール 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]** に*Mountpoint*`/hpux/DP_DEPOT` と入力します。**[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コンポーネントのリスト内で、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 システム用の DATA-PROTECTOR 製品が表示されます。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。

   プロダクトには次のサブプロダクトコンポーネン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 (PDF 形式との Data Protector ガイドと WebHelp 形式の『HP Data Protector ヘルプ』を収録)
OB2-IS	Data Protector インストールサーバーでは、以下の操作を行います。

4. [SD Install - Software Selection] ウィンドウで、**[DATA-PROTECTOR]** をダブルクリックすると、インストール可能なソフトウェアが表示されます。**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]** をクリックして次に進みます。

インストールが完了すると、UNIX のソフトウェアデポは、`/opt/omni/databases/vendor` ディレクトリに置かれます。

重要: ネットワーク上に UNIX 用のインストールサーバーをインストールしない場合は、HP-UX 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する必要があります。さらに、Data Protector クライアント上のコンポーネントはパッチできなくなります。

rpm を使用した Linux システムへのインストールサーバーのインストール

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ーを 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. Linux 用インストール DVD-ROM をドライブに挿入します。
2. 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 (この場合は *Mount_point*/linux_x86_64/DP_DEPOT) に移動します。
3. 個々のコンポーネントについて、次のコマンドを実行します。

   ```
   rpm -i package_name-A.08.00-1.x86_64.rpm
   ```

   プロダクト内にはインストールサーバーのインストールに関連する以下のコンポーネント (*package_name*) が含まれています。

OB2-CORE	Data Protector のコアソフトウェア。インストールサーバーを Cell Manager システムに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-TS-CORE	Data Protector コアテクノロジスタックライブラリ
OB2-CORE-IS	インストールサーバーのコアソフトウェア
OB2-CFP	すべての UNIX プラットフォームに共通のインストールサーバーコアソフトウェア
OB2-TS-CFP	すべての UNIX プラットフォームに共通のインストールサーバーテクノロジスタックソフトウェア
OB2-DAP	すべての UNIX プラットフォーム用の Disk Agent リモートインストールパッケージ
OB2-MAP	すべての UNIX システム用の Media Agent リモートインストールパッケージ
OB2-NDMPP	NDMP Media Agent コンポーネント。
OB2-CCP	すべての UNIX プラットフォーム用の Cell Console リモートインストールパッケージ

   さらに、Cell Manager とは別のシステムの独立した環境でインストールサーバーをセットアップし、ユーザーインタフェースを使用する場合は、次のコンポーネントが必要です。

OB2-CC	Cell Console ソフトウェア。これには、コマンドラインインタフェースが含まれます。

4. これらのコンポーネントのインストールが完了したら、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コンポーネントで必要となるリモートインストール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 の統合コアソフトウェア。このコンポーネントは、統合ソフトウェアのインストールで必要になります。
OB2-TS-PEGP	PEGASUS テクノロジスタックコンポーネント。
OB2-SAPP	SAP 用統合ソフトウェアコンポーネント
OB2-VMWP	VMware 用統合ソフトウェア (レガシー) 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-SMISAP	HP P6000/HP 3PAR SMI-S Agent コンポーネント
OB2-SSEAP	HP P9000 XP Agent コンポーネント
OB2-VMWP	VMware 用統合ソフトウェア (レガシー) コンポーネント。
OB2-VEPAP	Virtual Environment Protection Agent コンポーネント
OB2-SODAP	StoreOnce ソフトウェア重複排除コンポーネント
OB2-AUTODRP	自動ディザスタリカバリコンポーネント
OB2-VMWAREGRE-AGENTP	VMware Granular Recovery Extension コンポーネント
OB2-DOCSP	英語版マニュアル (ガイド、ヘルプ) コンポーネント。
OB2-FRAP	フランス語版マニュアル (ガイド、ヘルプ) コンポーネント。
OB2-JPNP	日本語版マニュアル (ガイド、ヘルプ) コンポーネント。
OB2-CHSP	簡体字中国語版マニュアル (ガイド、ヘルプ) コンポーネント。

全コンポーネントのリストおよびインストールの依存関係については、「Linux 上の Data Protector ソフトウェアコンポーネントの依存関係」 (157 ページ) を参照してください。

インストールが完了すると、UNIX のソフトウェアデポは、`/opt/omni/databases/vendor` ディレクトリに置かれます。

重要: ネットワーク上に UNIX 用のインストールサーバーをインストールしない場合は、Linux 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 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。

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ー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、以下の作業を実施します。

1. 独立した形で (Cell Manager とは別のシステムに) インストールサーバーをセットアップした場合は、このシステムを Data Protector セルに手動で追加 (インポート) する必要があります。「セルへのインストールサーバーのインポート」 (130 ページ) を参照してください。

注記: インストールサーバー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、インストールされているリモートインストールパッケージがリストに表示されます。CLI からこのファイルを使用して、使用可能なリモートインストール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、リモートインストールパッケージをインストールまたは削除したときは必ずインストールサーバーのエクスポートと再インポートを実行してください。これは、インストールサーバーを 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ーをインストールする必要があります。「前提条件」 (39 ページ) 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。「Data Protector クライアントのインストール」 (42 ページ) 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ー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。`omnisetup.sh` を使用するか、Data Protector GUI からコンポーネントをリモートでインストールして、クライアントを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については、「Data Protector クライアントのインストール」 (42 ページ) を参照してください。

ネイティブツールを使用した、HP-UX および Linux 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、HP-UX 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ー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ー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ーからコンポーネントをリモートでインストールして、アップグレードする必要があります。詳細については、「UNIX および Mac OS X システムのローカルインストール」 (76 ページ) または「リモートインストール」 (70 ページ) を参照してください。

アップグレード手順

Data Protector A.06.11、6.20、または 7.00 を Data Protector 8.00 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. 既存の Data Protector A.06.11、6.20、または 7.00 IDB をエクスポートします。
   a. Data Protector 8.00 DVD-ROM をマウントし、`omnimigrate.pl` スクリプトを一時ディレクトリにコピーします。

      ```
      cp -p
      MountPoint/hpux/DP_DEPOT/DATA-PROTECTOR/OMNI-CS/opt/omni/sbin/omn
      imigrate.pl /tmp
      ```

   b. `omnimigrate.pl` コマンドを使用して IDB をエクスポートします。

      ```
      /opt/omni/bin/perl /tmp/omnimigrate.pl -shared_dir
      /var/opt/omni/server/exported -export
      ```

2. `root` でログインし、`omnisv -stop` コマンドを実行して Data Protector サービスを停止します。

   `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、Data Protector サービスは表示されないはずです。

3. Cell Manager またはインストールサーバーをアップグレードする場合には、「swinstall を使用した HP-UX システムへの Cell Manager のインストール」(218 ページ) または 「swinstall を使用した HP-UX システムへのインストールサーバーのインストール」(220 ページ) で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ー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**。

rpm を使用した Linux システムでの Data Protector のアップグレード

Linux 用 Cell Manager またはインストールサーバー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ーからコンポーネントをリモートでインストールして、アップグレードする必要があります。詳細については、「UNIX および Mac OS X システムのローカルインストール」(76 ページ) または 「リモートインストール」(70 ページ) を参照してください。

アップグレード手順

Data Protector A.06.11、6.20、または 7.00 を Data Protector 8.00 にアップグレードするには、`rpm` を使用し、以下の手順に従ってください。

1. 既存の Data Protector A.06.11、6.20、または 7.00 IDB をエクスポートします。
   a. Data Protector 8.00 DVD-ROM をマウントし、`omnimigrate.pl` スクリプトを一時ディレクトリにコピーします。

      ```
      cp -p
      MountPoint/hpux/DP_DEPOT/DATA-PROTECTOR/OMNI-CS/opt/omni/sbin/omn

      imigrate.pl /tmp
      ```

   b. `omnimigrate.pl` コマンドを使用して IDB をエクスポートします。

      ```
      /opt/omni/bin/perl /tmp/omnimigrate.pl -shared_dir
      /var/opt/omni/server/exported -export
      ```

2. `root` でログインし、`omnisv -stop` コマンドを実行して Data Protector サービスを停止します。

   `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、Data Protector サービスは表示されないはずです。

3. `rpm` 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。

4. `rpm -q` 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`

5. Cell Manager をアップグレードする場合は、Linux インストール DVD-ROM を挿入してマウントします。次に、`rpm` を使用して Cell Manager をインストールします。詳細な手順は、「rpm を使用した Linux 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ーをアップグレードする場合、Linux インストール DVD-ROM を挿入してマウントし、インストールサーバーをインストールします。詳細な手順は、「rpm を使用した Linux システムへのインストールサーバーのインストール」を参照してください。

B システムの準備と保守作業

この付録では、本来は本書の範囲外ながらも、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。これらの作業には、システムの準備と保守作業が含まれます。

UNIX システムでのネットワーク構成

UNIX システムに Data Protector をインストールする際、Data Protector `Inet` がネットワークサービスとして登録されます。これには通常、次の手順が含まれます。

- Data Protector `Inet` がリスンするポートを登録するための `/etc/services` ファイルの変更。
- システムの `inetd` デーモンまたはそれに相当するデーモン (`xinetd`、`launchd`) の Data Protector `Inet` の登録。

ネットワーク構成を変更すると、初期の Data Protector `Inet` 構成が不完全または無効になることがあります。これは、インターネットプロトコルバージョン 6 (IPv6) ネットワークインタフェースを追加または削除する場合に、IPv6 サポートをネットワークサービスに追加するためのシステム固有の設定が原因で発生します。また、これ以外の状況でも発生する可能性があります。

Data Protector `Inet` 構成を更新するために、`dpsvcsetup.sh` ユーティリティが使用できます。このユーティリティ (インストールでも使用され、必要な情報を収集し、それに応じてシステム構成を更新します) は、`/opt/omni/sbin` (HP-UX、Solaris、Linux システム) または `/usr/omni/bin` (その他 UNIX システム) にあります。

- Data Protector `Inet` の構成を更新するには、次のコマンドを実行します。

  ```
  dpsvcsetup.sh -update
  ```

- Data Protector `Inet` をネットワークサービスとして登録するには、次のコマンドを実行します。

  ```
  dpsvcsetup.sh -install
  ```

- Data Protector `Inet` のネットワークサービスとしての登録を解除するには、次のコマンドを実行します。

  ```
  dpsvcsetup.sh -uninstall
  ```

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。ネットワーク内の各システムは、Cell Manager のアドレス、および Media Agent と物理メディアデバイスが接続されたすべてのクライアントのアドレスを解決できなければなりません。Cell Manager は、セル内のすべてのクライアントの名前を解決できる必要があります。

TCP/IP プロトコルのインストール後、`ping` コマンドおよび `ipconfig/ifconfig` コマンドを使って TCP/IP 構成を確認できます。

一部のシステムでは、IPv6 のアドレスには `ping` コマンドを使用できないので、代わりに `ping6` コマンドを使用してください。

1. コマンドラインで、次のコマンドを実行します。

   Windows システムの場合: `ipconfig /all`

   UNIX システムの場合: `ifconfig` *`interface`*、`ifconfig -a`、`nestat -i` のいずれか (システムによって異なります)

   TCP/IP 構成に関する詳細情報、およびネットワークアダプターに設定されているアドレスが表示されます。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`* と入力して、ソフトウェアのインストールおよび構成を確認します。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。

   サブネット上ではゲートウェイが動作している必要があります。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 アドレスが正しいかどうか、およびゲートウェイが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。マシン名が `computer`、ドメイン名が `company.com` の場合は、次のように入力します。`ping computer.company.com`

   このコマンドが動作しない場合は、TCP/IP プロパティのウィンドウでドメイン名が正しいかどうかを確認します。hosts ファイルと DNS もチェックする必要があります。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。
   - クライアントでは、Cell Manager と、Media Agent がインストールされている各クライアントに対して ping コマンドを実行します。

   注記: 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してい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: 上記の名前解決が動作していない場合は、Data Protector を正しくインストールすることはできません。

   また、Windows のコンピューター名がホスト名と同じである必要があります。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。

5. Data Protector がインストールされ、Data Protector セルが作成された後で、DNS チェックツールを使って、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でセル内の他のクライアントに対する DNS 接続を解決できるかどうか、およびその逆をチェックします。これを行うには、`omnicheck -dns` コマンドを実行します。失敗したチェックとその合計数が表示されます。

   `omnicheck` コマンドの詳細については、『HP Data Protector Command Line Interface Reference』を参照してください。

デフォルトの Data Protector ポートの変更

デフォルトの Data Protector Inet ポートの変更

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、Data Protector 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。

デフォルトでは、`Inet` はポート番号 5555 を使用します。このポート番号が別のプログラムに使用されていないことを確認するには、ローカルの `/etc/services` ファイル (UNIX システム)、またはローカルで起動した `netstat -a` コマンド (Windows システムの場合) の出力を参照してください。ポートが別のプログラムによって使用されている場合、未使用ポートを使用するように `Inet` の構成を変更する必要があります。この変更はセルの**各**システムで行い、セル内の**すべての**システムが同じポートを使用するようにします。

インストールサーバーとしても機能する Cell Manager またはスタンドアロンのインストールサーバーでの変更が完了すると、このインストールサーバーを使用してリモートインストールされるすべてのクライアントが、新しいポートを自動的に使用します。したがって、セルの作成時に、`Inet` ポートの変更作業が非常に簡単になります。

注意: ディザスタリカバリ用に用意されたシステムで、デフォルトの `Inet` リッスンポートを変更しないでください。変更すると、システムに障害が発生した場合、ディザスタリカバリプロセスが失敗することがあります。

UNIX システム

Cell Manager、インストールサーバー、または Data Protector クライアントとして使用する予定の UNIX システムで `Inet` ポートを変更するには、次の手順を実行します。

- 目的のポート番号で、`/tmp/omni_tmp/socket.dat` ファイルを作成します。

Cell Manager、インストールサーバー、または Data Protector クライアントとしてすでに使用している UNIX システムで `Inet` ポートを変更するには、次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. `/etc/opt/omni/client/customize/socket` ファイルと `/opt/omni/newconfig/etc/opt/omni/client/customize/socket` ファイルがシステムに存在している場合は、目的のポート番号でファイルの内容を更新します。
3. `kill -HUP` *`inetd_pid`* コマンドを使用して関連プロセスを終了することによって、`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` コマンドを実行します。
4. Cell Manager の `Inet` の設定を変更するには、`Port` グローバルオプションに新しい値を設定します。
5. Cell Manager の `Inet` の設定を変更するには、Data Protector サービスを再開します。

   ```
   - omnisv stop
   - omnisv start
   ```

Windows システム

Cell Manager、インストールサーバー、または Data Protector クライアントとして使用する予定の Windows システムで `Inet` ポートを変更するには、次の手順を実行します。

1. コマンドラインから `regedit` を実行して、レジストリエディターを開きます。
2. `HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\ OpenView\OmniBackII\Common` キーの下に、`InetPort` というレジストリエントリを作成します。

   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` (文字列)

   レジストリエントリの値: *`PortNumber`*

Cell Manager、インストールサーバー、または Data Protector クライアントとしてすでに使用している Windows システムで `Inet` ポートを変更するには、次の手順を実行します。

1. コマンドラインから `regedit` を実行して、レジストリエディターを開きます。
2. **[HKEY_LOCAL_MACHINE]**、**[SOFTWARE]**、**[Hewlett-Packard]**、**[OpenView]**、**[OmniBack]** 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 フォルダーの Parameters サブフォルダーについても同様の手順を繰り返します。
4. Windows の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)。

UNIX システムでデフォルトの Data Protector IDB ポートおよびユーザーアカウントを変更する

UNIX システムの場合、インストールは `omnisetup.sh` スクリプトで実行され、対話形式ではありません。インストールを開始する前に、`/tmp/omni_tmp/DP.dat` ファイルのポート値を変更する必要があります。

次のポートエントリは次の IDB サービスに対応しています。

- HP Data Protector IDB (hpdp-idb) サービスポート: PGPORT

- HP Data Protector IDB 接続プーラー (hpdp-idb-cp) ポート: PGCPORT
- HP Data Protector アプリケーションサーバー (hpdp-as) サービスポート: APPSSPORT
- HP Data Protector アプリケーションサーバー (hpdp-as) 管理ポート: APPSNATIVEMGTPORT

PGOSUSER 変数を設定することで、IDB を実行するデフォルトのユーザーアカウントを変更できます。

DP.dat ファイルの例:

```
PGPORT=7112
PGCPPORT=7113
PGOSUSER=hpdp
APPSSPORT=7116
APPSNATIVEMGTPORT=7119
```

Data Protector インストールのための Windows Server 2008 または Windows Server 2012 上で実行する Microsoft サーバークラスターの準備

Windows Server 2008 上または Windows Server 2012 オペレーティングシステムで Microsoft Cluster Service (MSCS) が実行されているサーバークラスターに、クラスター対応の Data Protector Cell Manager または Data Protector クライアントをインストールできるようにするには、事前にクラスターを準備する必要があります。クラスターの準備をしていない場合、ディザスタリカバリの準備でバックアップが必要なローカルの CONFIGURATION オブジェクトのバックアップセッションに失敗し、データの損失が発生する可能性があります。

前提条件

- ドメインのユーザーアカウントでシステムにログオンしていることを確認します。このドメインユーザーアカウントは、ローカルの Administrators グループのメンバーでなければなりません。

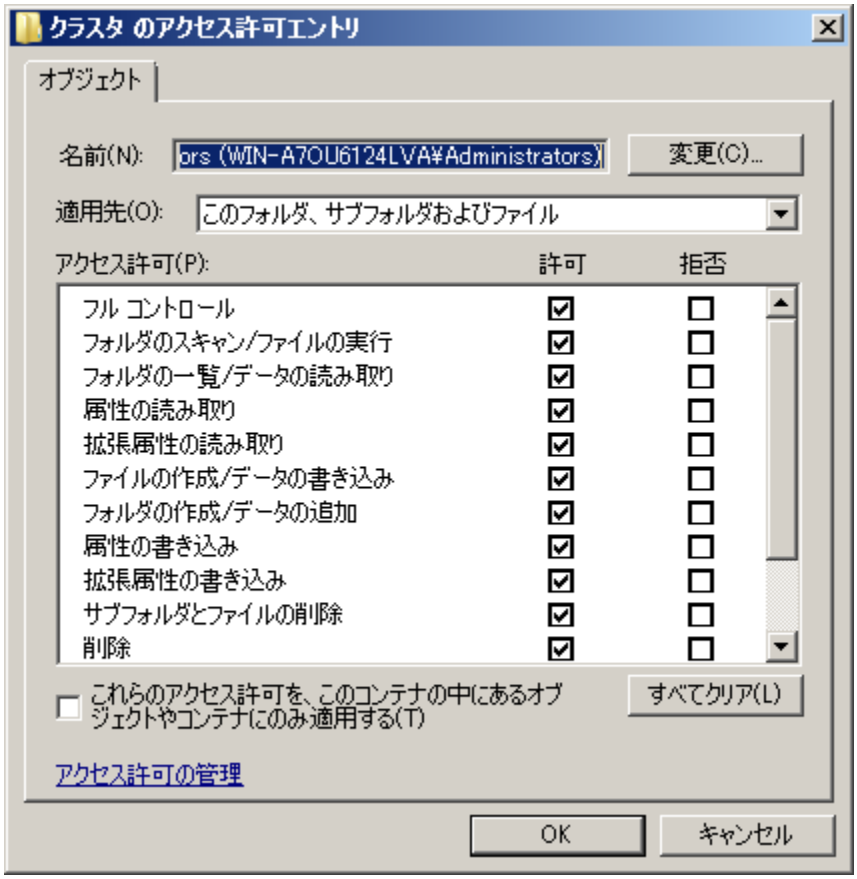
準備の手順

Data Protector インストールのためにクラスターを適切に準備するには、以下の手順を実行します。

1. 両方のクラスターノードで、Windows ファイアウォールを開始し、ファイルとプリンターの共有の例外を有効にします。
2. アクティブなクラスターノード上で、[フェールオーバークラスターの管理] を開始し、クォーラムリソース内の監視ディスクがオンラインになっていることを確認します。リソースがオフラインになっている場合はオンラインにします。

   以下の手順を、アクティブなクラスターノード上のみで実行します。
3. マジョリティノードセット (MNS) が構成されていないクラスターを準備する場合は、Windows エクスプローラーを起動して、*WitnessDiskLetter*:\Cluster フォルダーの所有者をローカルの Administrators グループに変更します。[Cluster のセキュリティの詳細設定] ウィンドウで所有者を変更する際は、必ず **[**サブコンテナーとオブジェクトの所有者を置き換える**]** オプションをオンにしてください。[Windows セキュリティ] ダイアログボックスで、操作を確認して **[**はい**]** をクリックし、その後に表示される通知を確認して **[**はい**]** をクリックします。
4. MNS が構成されていないクラスターを準備する場合は、Windows エクスプローラーで *WitnessDiskLetter*:\Cluster フォルダーのアクセス許可を変更して、SYSTEM およびローカルの Administrators グループのフルコントロールを許可します。両方のグループのアクセス許可設定が、「Cluster フォルダーおよび Administrators ローカルユーザーグループの適切なアクセス許可」(230 ページ) で示す設定と一致することを確認してください。

図 55 Cluster フォルダーおよび Administrators ローカルユーザーグループの適切なアクセス許可



5. Data Protector Cell Manager として使用するクラスターを準備する場合は、[フェールオーバークラスターの管理] で ［クラスターアクセスポイント］リソースを追加します。**[**リソースの追加**]** を選択し、**[1** クライアントアクセスポイント**]** をクリックして、新しいリソースウィザードを開始します。
   a. [クライアントアクセスポイント] ペインで、[名前] テキストボックスに仮想サーバーのネットワーク名を入力します。
   b. [アドレス] テキストボックスに仮想サーバーの IP アドレスを入力します。
6. Data Protector Cell Manager として使用するクラスターを準備する場合は、[フェールオーバークラスターの管理] でクラスターに共有フォルダーを追加します。**[**共有フォルダーの追加**]** をクリックして共有フォルダーの準備ウィザードを開始します。
   a. [共有フォルダーの場所] ペインで、[場所] テキストボックスにディレクトリパスを入力します。選択したディレクトリに、Data Protector インストールで作成されるデータを保存するための十分な空き領域があることを確認してください。**[**次へ**]** をクリックします。
   b. [NTFS アクセス許可]、[共有プロトコル]、[SMB 設定] の各ペインで、オプションの値をデフォルトのまま変更しないでおきます。**[**次へ**]** をクリックして次のペインに進みます。
   c. [SMB アクセス許可] ペインで、**[Administrators** がフルコントロールを持ち、他のすべてのユーザーとグループは読み取りと書き込みのみのアクセス権を持つ**]** オプションを選択します。**[**次へ**]** をクリックします。
   d. [DFS 名前空間への発行] で、オプションの値をデフォルトのままにします。**[**次へ**]** をクリックします。
   e. [設定の確認と共有の作成] ペインで、**[**作成**]** をクリックします。

Veritas Volume Manager がインストールされた Microsoft Cluster Server 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手順を実行します。「Microsoft Cluster Server への Data Protector のインストール」 (117 ページ) 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ーではなく専用のリソースドライバーを使用しているローカルおよびクラスター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 -maintenance` コマンドを実行して、保守モードを開始します。
2. 新しいシステム環境変数 `OB2CLUSTERDISKTYPES` の値を `Volume Manager Disk Group` として定義するか、両方のクラスターノード上で `omnirc` オプション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、単純に、リソースの種類の名前を `OB2CLUSTERDISKTYPES` 環境変数の値に追加します。

   ```
   OB2CLUSTERDISKTYPES=Volume Manager Disk Group;NETRaid4M Diskset
   ```

   `omnirc` ファイルオプション数の使用に関する詳細は、『HP Data Protector トラブルシューティングガイド』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 -maintenance –stop` コマンドを実行して、保守モードを終了します。

NIS サーバーの準備

ここでは、NIS サーバーに Data Protector Cell Manager を認識させるための手順を説明します。

NIS サーバーに 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` サーバーに `root` 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。「デフォルトの Data Protector Inet ポートの変更」 (227 ページ) 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/lbin/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` サーバー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 サーバーから使用するかを定義できます。また、名前の保持場所を 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、man 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 サーバーを準備し、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
  ```

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。詳しい手順は、「セルからのクライアントのエクスポート」(133 ページ)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。詳しい手順は、「セルへのクライアントのインポート」(129 ページ)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 システムの場合

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。

   ```
   omnidbutil -change_cell_name [OldHost]
   ```

Windows システムの場合

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_program_data\config\server\cell\cell_info
   Data_Protector_program_data\config\server\users\userlist
   ```

2. 次のレジストリキーで Cell Manager 名を変更します。HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\ OpenView\OmniBack\Site\CellServer

C デバイスとメディア関連タスク

この付録では、本来は本書の範囲外となる作業についての Data Protector 固有の情報を説明します。これらの作業には、デバイスドライバー構成、SCSI ロボティクスの管理、SCSI 環境類の保持が含まれます。

Windows システムでのテープドライバーおよびロボティクスドライバーの使用

Data Protector では、Windows システムに接続された有効な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ーをサポートしています。ただし、(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ーは、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ーデバイス用にロードされるネイティブドライバー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。

テープドライバー

Windows には、ハードウェア互換性リスト (HCL) に記載されているデバイスが、ドライバー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

コンピューターが起動すると、デバイスドライバー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。ネイティブのテープドライバーは、別途ロードする必要はなく、更新が可能です。ネイティブのテープドライバーを更新または置換するには、次の手順を実行します。

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 **[**コンピューターの管理**]** をダブルクリックします。**[**デバイスマネージャー**]** 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ーを確認するには、テープドライブ名をマウスの右ボタンでクリックし、**[**プロパティ**]** をクリックします。
4. **[**ドライバー**]** タブを選択し、**[**ドライバーの更新**]** をクリックします。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ーを更新するか、別のドライバーに置き換えるかを、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を適用します。

重要: ドライバーがネイティブテープドライバーを使用しないで 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。

詳細については、「Windows システム上でのデバイスファイル (SCSI アドレス) の作成」(234 ページ) を参照してください。

ロボティクスドライバー

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ー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、対応するドライバーを無効化する必要があります。

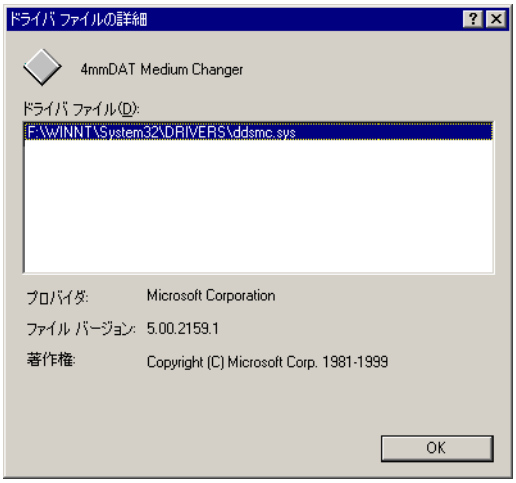
ここでは、4mm DDS テープを使用する HP 1557A テープライブラリを例に取り上げます。Windows システムで自動的にロードされるロボティクスドライバー (`ddsmc.sys`) を無効にするには、以下の手順に従ってください。

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 [コンピューターの管理] をダブルクリックします。[デバイスマネージャー] をクリックします。
3. [デバイスマネージャー] ウィンドウの結果エリアで、[メディアチェンジャー] を展開します。
4. 現在ロードされているドライバーを確認するには、**[4mm DDS Medium Changer]** をマウスの右ボタンでクリックし、[プロパティ] をクリックします。

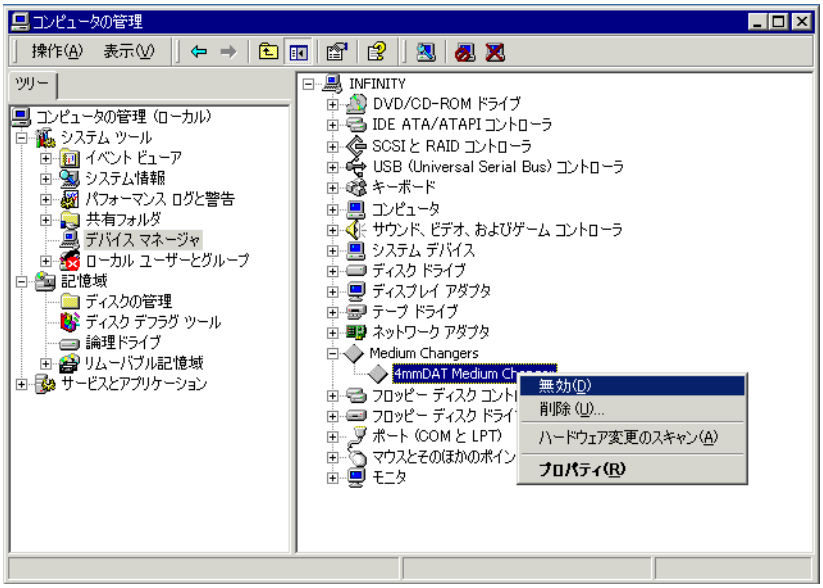
   [ドライバー] タブを選択し、[ドライバーの詳細] をクリックします。以下のウィンドウが表示されます。

図 56 メディアチェンジャーのプロパティ



ネイティブロボティクスドライバーを無効にするには、**[4mm DDS Medium Changer]** をマウスの右ボタンでクリックし、[無効] を選択してください。

図 57 ロボティクスドライバーの無効化



5. システムを再起動して変更を適用します。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 システム上でのデバイスファイル (SCSI アドレス) の作成

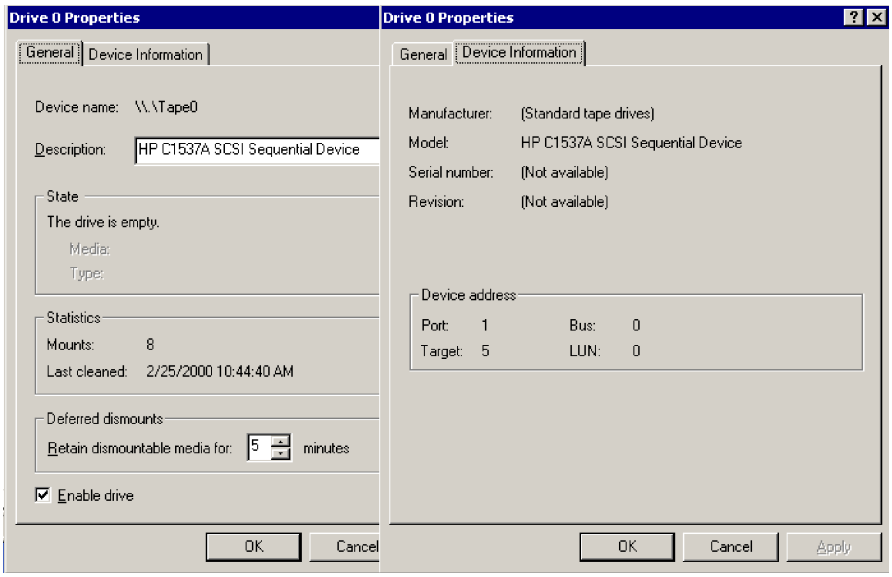
テープデバイスファイル名の構文は、ネイティブテープドライバーをテープドライブに対してロード (`tapeN:B:T:L`) またはアンロード (`scsiP:B:T:L`) するかによって異なります。

ネイティブテープドライバーを使用する Windows

Windows システムに接続され、ネイティブテープドライバー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。
2. [管理ツール] ウィンドウで **[**コンピューターの管理**]** をダブルクリックします。[リムーバブル記憶域] と [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バーがロードされていれば、[一般] プロパティページにデバイスファイル名が表示されます。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。「テープドライブプロパティ」 (235 ページ) を参照してください。

図 58 テープドライブプロパティ



「テープドライブプロパティ」 (235 ページ) 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バー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バーを使用していない場合 `scsii1:0:5:0`

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、システムを再起動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、`E:`は、ドライブ文字 `E` に割り当てられている磁気光デバイス用に作成されたデバイスファイルです。

HP-UX システム上の 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ーを使ってテープライブラリデバイス (HP 12000e など) の SCSI コントローラー**および**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 59 SCSI 制御デバイス

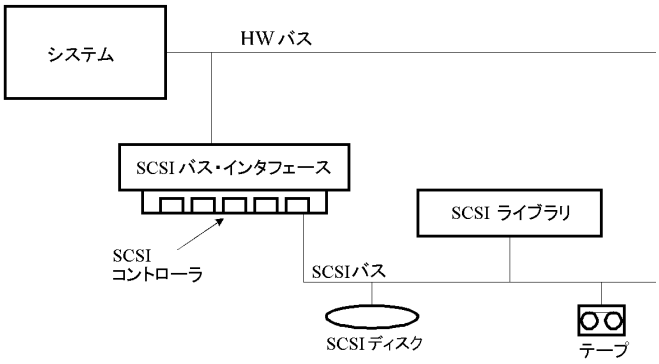
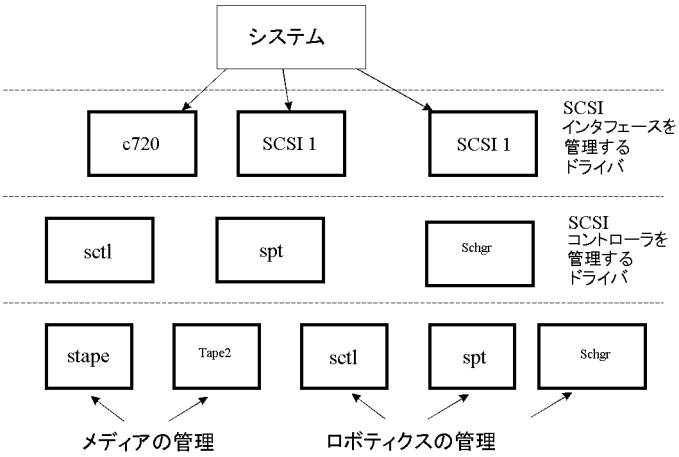


図 60 デバイスの管理



使用される SCSI ロボティクスドライバーの種類は、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 オートチェンジャードライバー schgr が、EISA 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ー 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 サーバーの場合は、spt という名前の SCSI パススルードライバーを使用します。このドライバーは、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ーが現在の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ーを**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 プラットフォームでは、**HP System Administration Manager (SAM)** ユーティリティを使用してカーネルをビルドすることもできます。「HP-UX クライアントのインストール」 (51 ページ) 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ー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 61 SCSI パススルードライバー (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                      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
```

「SCSI パススルードライバー (sctl) のステータス」 (237 ページ) では、SCSI パススルードライバー `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` です。(SCSI=2, LUN=0)

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ーは `stape` です。対応するハードウェアパス (H/W Path) は `8/12.1.0` です。(SCSI=0, LUN=0)

重要: SCSI アドレス 7 は SCSI コントローラー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 コントローラーは `sctl` によって管理されています。

図 62 SCSI パススルードライバー 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        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
# 
```

「SCSI パススルードライバー spt のステータス」 (237 ページ) 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ー `spt` によって制御されています。このデバイスは、HP 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ー `spt` が正しく割り当てられています。

`sctl`、`spt`、または `schgr` のドライバーがロボティクスに割り当てられていない場合は、ロボティクスの H/W Path を `system` ファイルのドライバー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ーを**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. 次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/lbin/sysadm/system_prep -s system
   ```

3. どの SCSI ロボティクスドライバーが、現在の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、以下のコマンドを実行してください。

   ```
   grep SCSIRoboticDriver system
   ```

   ここで、*SCSIRoboticDriver* には `spt`、`sctl`、または `schgr` を指定します。ドライバーが現在の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. エディターを使って、`/stand/build/system` ファイルに以下のドライバー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 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ー行を追加する必要があります。

   `schgr` ドライバーを構成する場合は、ドライバー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保存し、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保存し、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、システムを再起動します。

   ```
   shutdown -r 0
   ```

9. システムを再起動したら、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 システム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` コマンドの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がこれに該当します。

ここでは、HP-UX システムに接続された HP 12000e ライブラリデバイス (ライブラリロボティクス) 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後に自動作成されますが、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。

「SCSI パススルードライバー spt のステータス」(237 ページ)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 63 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 システムドライバー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ー spt を使用する必要があります。このドライバーはすでにインストールされており、HP 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 ドライバーではなく、sctl ドライバーが必要になります。

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ーの**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、どちらのドライバーの場合も共通です)。

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
```

「接続済みデバイスのリスト」(239 ページ)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
```

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ーの場合も、共通の**マイナー番号**は以下の形式をとります。

```
0xIITL00
```

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、リストの二番目の列 (I の列) に表示されます。この例では、インスタンス番号は 0 なので、2 桁の 16 進数 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 と入力します。

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 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
```

sctl 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 コントローラーのパラメーターの設定

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 コントローラー上で追加の構成が必要になる場合があります。

Windows システムで Adaptec SCSI コントローラーや Adaptec チップセット搭載の SCSI コントローラーのパラメーターを設定するには、そのコントローラー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 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 Protector GUI を使って設定する必要があります。

HP-UX システム上の未使用の 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のできる未使用の SCSI アドレス (ポート) を見つける必要があります。

HP-UX システムでは、/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みなすことができます。

「HP-UX システム上で実行した ioscan -f コマンドの出力」 (241 ページ) 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 64 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        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
# 
```

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。

「HP-UX システム上で実行した ioscan -f コマンドの出力」 (241 ページ) 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 コントローラー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 コントローラー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す。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 ドライバー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ー spt によって制御されています。説明を見ると、デバイスが HP 12000e ライブラリであることを確認できます。このライブラリはテープドライブとロボティックスと同じ SCSI アドレスを使用しますが、異なる LUN を使用するため、SCSI ライブラリで簡単に識別できます。

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スに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に指示さ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ー構成の更新

構成ファイルの更新

デバイスおよびドライバーの構成には、次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上で設定します。
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
   ```

   これにより、接続した SCSI デバイスに関する情報 (新たに接続したバックアップデバイスの正しいデバイス ID 文字列など) が取得されます。
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) ドライバーで使用されます。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 番目のパラメーターである 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 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 24x6 などの一部の例外もあります。

1. `sst` ドライバー (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.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. ドライバーを 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ー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. システムを再起動します。

   ```
   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、システム起動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、起動処理の`/devices` ディレクトリ構成段階で、デバイスが接続されたことを示すために、ユーザーが選択した *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. 再起動が完了したら、コマンド `ls -all` を使用して、作成されたデバイスファイルを確認できます。ライブラリデバイスの場合、このコマンドの出力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

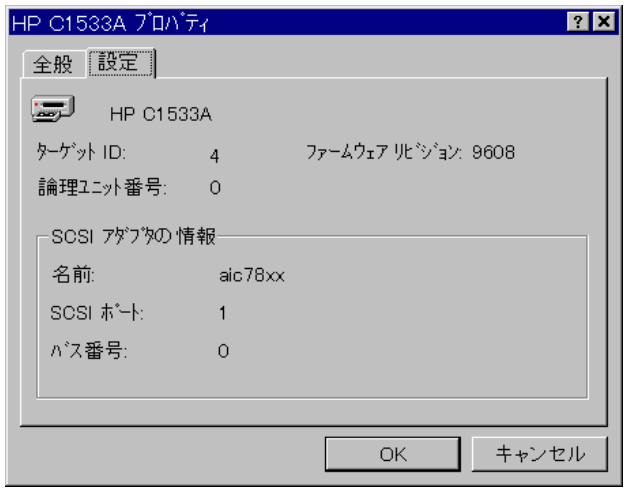
Windows システム上の未使用の SCSI ターゲット ID の取得

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** アダプター**]** をクリックします。
2. SCSI アダプター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。「デバイスの設定」 (245 ページ) 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 `LUN（論理ユニット番号）` 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 65 デバイスの設定



HP 330fx ライブラリでの 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 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、Linux 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。「リモートインストール」(70 ページ) 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、「HP-UX システム上の未使用の SCSI アドレスの取得」(240 ページ) を参照してください。Solaris システムについては、「Solaris システム上の未使用の SCSI ターゲット ID の取得」(241 ページ) を参照してください。Windows システムについては、「Windows システム上の未使用の SCSI ターゲット ID の取得」(245 ページ) 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、必要なドライバーがすでに**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。「HP-UX のカーネル構成のチェック」(52 ページ) を参照してください。

     SCSI パススルードライバーを構成する必要がある場合は、「HP-UX システム上の SCSI ロボティクス構成」(235 ページ) を参照してください。

   - Solaris システムに接続する場合は、必要なドライバー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。「Solaris システム上でのデバイスおよびドライバー構成の更新」(242 ページ) 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ーを構成する場合は、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ーをロードまたは無効化します。「Windows システムでのテープドライバーおよびロボティクスドライバーの使用」(233 ページ) 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ー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ー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、「Windows システム上でのデバイスファイル (SCSI アドレス) の作成」(234 ページ) を参照してください。

4. デバイスの SCSI アドレス (ID) 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、「HP 330fx ライブラリでの SCSI ID の設定」(245 ページ) を参照してください。

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

注記: AdaptecSCSI アダプター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 アダプターメニューを表示し、**[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、コンピューター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。

   Windows システムの場合: `devbra` ユーティリティを使用すると、新しいバックアップデバイスが正しく認識された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。

   ```
   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ー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ー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。

   HP-UX システムの場合: `/usr/sbin/ioscan -fn` 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、新しく接続されたデバイスに正しい 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システムの起動時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。「HP-UX システム上のデバイスファイルの作成」 (238 ページ) を参照してください。

   Solaris システムの場合: `/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、新しく接続されたデバイスに正しい 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。

   Linux システムの場合: `/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、新しく接続されたデバイスに正しい 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。

   AIX システムの場合: `lsdev -C` コマンドを実行すると、接続済みのデバイスを対応するデバイスファイルとともに示すリストが表示されます。

ハードウェア圧縮

最近のバックアップデバイスは、ハードウェア圧縮機能が組み込まれているものが大半です。ハードウェア圧縮は、デバイス構成手順でデバイスファイルまたは SCSI アドレスを作成するときに有効化できます。詳細な手順は、『HP Data Protector 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。ハードウェア圧縮を使うと、テープに書き込まれるデータのサイズが小さくなり、テープドライブがデータを受信する速度が向上します。

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軽減されます。

ハードウェア圧縮を Windows システム上で有効化するには、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 [テープドライバー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る場合は、ハードウェア圧縮が使用されます。サポートしていない場合、C オプションは無視されます。

ハードウェア圧縮を Windows システム上で無効化するには、デバイスやドライブの SCSI アドレスの末尾に "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 システム上で有効化/無効化するには、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。構成タスクの詳細は、『HP Data Protector ヘルプ』の索引「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。

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。「リモートインストール」 (70 ページ) を参照してください。

この後の項では、HP HP Standalone 24 テープデバイス、HP 12000e ライブラリ、および HP DLT ライブラリ 28/48 スロットを、HP-UX システムと Windows システムに接続する場合の手順を説明します。

HP 24 スタンドアロンデバイスの接続

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 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. 必要なドライバー (`stape` または `tape2`) 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。「HP-UX のカーネル構成のチェック」 (52 ページ) 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。「HP-UX システム上の未使用の SCSI アドレスの取得」 (240 ページ) 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、コンピューター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。`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

デバイスを正しく接続したら、『HP Data Protector ヘルプ』の索引「構成、バックアップデバイス」で表示される内容を参照し、新しく接続したデバイスの Data Protector バックアップデバイスを構成する手順を確認してください。

Windows システムに接続する場合

HP 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。「Windows システム上の未使用の SCSI ターゲット ID の取得」 (245 ページ) 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、コンピューター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、新しく接続した HP 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

デバイスを正しく接続したら、『HP Data Protector ヘルプ』の索引「構成、バックアップデバイス」で表示される内容を参照し、新しく接続したデバイスの Data Protector バックアップデバイスを構成する手順を確認してください。

HP DAT オートローダーの接続

HP 12000e と DAT24x6 のライブラリはいずれも、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。また、ダーティテープ検出機能も組み込まれています。

HP-UX システムに接続する場合

HP 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. 必要なドライバー (`stape` または `tape2`) 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。「HP-UX のカーネル構成のチェック」 (52 ページ) を参照してください。
3. 必要な SCSI パススルードライバー (`sctl` または `spt`) が**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**ことを確認します。「HP-UX システム上の SCSI ロボティクス構成」 (235 ページ) 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。「HP-UX システム上の未使用の SCSI アドレスの取得」 (240 ページ) を参照してください。

   注記: HP 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 番号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、コンピューター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。「HP-UX システム上のデバイスファイルの作成」 (238 ページ) 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。以下のコマンドで ioscan ユーティリティを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正しく接続したら、『HP Data Protector ヘルプ』の索引「構成、バックアップデバイス」で表示される内容を参照し、新しく接続したデバイスの Data Protector バックアップデバイスを構成する手順を確認してください。

Windows システムに接続する場合

HP 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。「Windows システム上の未使用の SCSI ターゲット ID の取得」 (245 ページ) 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 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 番号を割り当てるように設計されています。
4. デバイス、コンピューター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 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正しく接続したら、『HP Data Protector ヘルプ』の索引「構成、バックアップデバイス」で表示される内容を参照し、新しく接続したデバイスの Data Protector バックアップデバイスを構成する手順を確認してください。

HP DLT ライブラリ 28/48 スロットの接続

HP 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。80～600GB のバックアップ容量を提供します。複数のデータチャネル、1 つのメールスロット、1 つのバーコードリーダーを備えた DLT 4000 または DLT 7000 のドライブが 4 つあります。

HP-UX システムに接続する場合

HP-UX システムに HP 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. 必要なドライバー (`stape` または `tape2`) 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。「HP-UX のカーネル構成のチェック」 (52 ページ) を参照してください。
2. 必要な SCSI パススルードライバー (`sctl` または `spt`) が**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**ことを確認します。「HP-UX システム上の SCSI ロボティクス構成」 (235 ページ) 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。「HP-UX システム上の未使用の SCSI アドレスの取得」 (240 ページ) を参照してください。

   注記: HP DLT ライブラリ 28/48 スロットには、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、コンピューター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。「HP-UX システム上のデバイスファイルの作成」 (238 ページ) 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 DLT ライブラリ 28/48 スロットライブラリデバイスを正しく接続したら、『HP Data Protector ヘルプ』の索引「構成、バックアップデバイス」で表示される内容を参照し、新しく接続したデバイスの Data Protector バックアップデバイスを構成する手順を確認してください。

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` ドライバー (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. ドライバーを 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。

   ここでは、SCSI コントロールデバイスにポート 6、最初のドライブにポート 2、2 番目のドライブにポート 1 を使用します。LUN は 0 です。
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. ステップ 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;
   ```

   注記: 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なければなりません。（ステップ 8を参照）。
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と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。これらのファイルは、ls -all コマンドを使用して一覧表示できます。ここでは、以下のようになります。

/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

この次に行う作業

HP DLT ライブラリ 28/48 スロットライブラリデバイスを正しく接続したら、『HP Data Protector ヘルプ』の索引「構成、バックアップデバイス」で表示される内容を参照し、新しく接続したデバイスの Data Protector バックアップデバイスを構成する手順を確認してください。

Windows システムに接続する場合

Windows システムに HP 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。「Windows システム上の未使用の SCSI ターゲット ID の取得」(245 ページ)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 DLT ライブラリ 28/48 スロットには、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、コンピューター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 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 DLT ライブラリ 28/48 スロットライブラリデバイスを正しく接続したら、『HP Data Protector ヘルプ』の索引「構成、バックアップデバイス」で表示される内容を参照し、新しく接続したデバイスの Data Protector バックアップデバイスを構成する手順を確認してください。

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用のスタンドアロンデバイスです。100～200 GB のバックアップ容量を提供します。

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 コントローラー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ます。

   ```
   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 コントローラーを使用することをお勧めします。また、Ultra2 SCSI コントローラーまたは Ultra3 SCSI コントローラー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 テープドライブを正しく接続したら、『HP Data Protector ヘルプ』の索引「構成、バックアップデバイス」で表示される内容を参照し、新しく接続したデバイスの Data Protector バックアップデバイスを構成する手順を確認してください。

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。「Windows システム上の未使用の SCSI ターゲット ID の取得」 (245 ページ) 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。
1. デバイス、コンピューター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。
2. 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 テープドライブを正しく接続したら、『HP Data Protector ヘルプ』の索引「構成、バックアップデバイス」で表示される内容を参照し、新しく接続したデバイスの Data Protector バックアップデバイスを構成する手順を確認してください。

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` パラメーターを指定します。

```
scsi2:0:0:0C
```

D Data Protector 8.00 へのアップグレード後のコマンドラインの変更

ここでは、Data Protector 8.00 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。使用法については、『HP Data Protector Command Line Interface Reference』または該当する man 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.06.11 からアップグレードした場合は、「Data Protector A.06.11 からのアップグレード」 (255 ページ) を参照してください。
- Data Protector 6.20 からアップグレードした場合は、「Data Protector 6.20 からのアップグレード」 (260 ページ) を参照してください。
- Data Protector 7.00 からアップグレードした場合は、「Data Protector 7.00 からのアップグレード」 (265 ページ) を参照してください。

表 10 Data Protector A.06.11 からのアップグレード

コマンド	影響を受けるオプションまたは引数、注意事項	状態
NNMpost.ovpl		削除されるコマンド
NNMpre.ovpl		削除されるコマンド
NNMScript.exe		削除されるコマンド
ob2install	veagent chs_ls	新しいソフトウェアコンポーネント
	snapa javagui ov	削除されるソフトウェアコンポーネント
omnib	-storedrim -clp -veagent_list -e2010_list -mssharepoint_list -idb_list	新しいオプション
	-copy	オプションの更新 Microsoft SQL Server 用統合ソフトウェアを使用したバックアップでも指定できます。
	-netware -omnidb	削除されるオプション
omnib2dinfo	Media Agent コンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
omnicc	-encryption -enable -cert -key -trust	新しいオプション

表 10 Data Protector A.06.11 からのアップグレード (続き)

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-all -add_exception -remove_exception -list_exceptions -status -add_certificate -get_certificate -list_certificates -impersonation -create_userrestrictions_tmpl	
	-import_vcd	新しいオプション
omnicreatedl	-va -lun_security	削除されるオプション
omnidb	-veagent -e2010 -mssharepoint -idb	新しいオプション
	-netware -omnidb	削除されるオプション
omnidbcheck	-connection -database_consistency -media_consistency -schema_consistency -verify_db_files	新しいオプション
	-dc -extended -quick	オプションの更新
	-core -filenames	削除されるオプション
omnidbp4000	このコマンドは、Data Protector の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た Windows システムで使用できます。	新しいコマンド
omnidbrestore		削除されるコマンド
omnidbsmis	-ompasswd -delete	新しいオプションの組み合わせ
	-reference -sync_check -exclude -include	新しいオプション
	-namespace -sync	削除されるオプション

表 10 Data Protector A.06.11 からのアップグレード (続き)

コマンド	影響を受けるオプションまたは引数、注意事項	状態
omnidbupgrade		削除されるコマンド
omnidbutil	-all -autovacuum -cp -disabled -enabled -freeze_max_age -on_n_rows -on_percentage -param -set -set_passwd -sync_srv -table -to_default	新しいオプション
	-info -readdb -show_db_files -writedb	オプションの更新
	-cdb -check_overs -chktblspace -extendfnames -extendinfo -extendtblspace -filenames -force -list_large_directories -list_mpos_without_overs -maxsize -mmdb -modifytblspace -no_detail -purge_stop -top -upgrade_info	削除されるオプション
omnidbva		削除されるコマンド
omnidbxp	-user -add -username -password -user -check -host -user -update -username -password -user -list -user -remove	新しいオプションとオプションの組み合わせ

表 10 Data Protector A.06.11 からのアップグレード (続き)

コマンド	影響を受けるオプションまたは引数、注意事項	状態
omnidbzdb	このコマンドは、Data Protector の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た Windows、HP-UX (Itanium)、Linux システムで使用できます。	新しいコマンド
omniiso	-out -net -use_raw_object -host -remotehost -move_to -unique_name -exec_script -password	新しいオプション
	-session	変更されるオプション
	-iso	削除されるオプション -out で置き換えられました。下位互換性維持のために使用できます。
omnimm	-show_locked_devs -all	新しいオプション
omniobjcopy	-replication -replist -veagent -e2010 -mssharepoint -idb	新しいオプション
	-netware -omnidb	削除されるオプション
omniobjverify	-veagent -e2010 -mssharepoint -idb	新しいオプション
	-netware -omnidb	削除されるオプション
omniofflr	このコマンドは、ユーザーインタフェースコンポーネントからコアインストールコンポーネントに移動したため、Data Protector コンポーネントをインストールしたシステム上で使用できるようになりました。	移動されたコマンド
	-rawdisk -section -idb -autorecover -changedevhost -read	新しいオプション

表 10 Data Protector A.06.11 からのアップグレード (続き)

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-force -session -save -skiprestore -logview -opview	
	-omnidb	削除されるオプション
omnir	-veagent -e2010 -mssharepoint -idb	新しいオプション
	-copyback -switch -leave_source -no_leave_source -no_check_config	新しいオプション HP P6000 EVA ディスクアレイファミリの新しいオプション
	-tail_log	新しいオプション Microsoft SQL Server 復元の新しいオプション。
	-restoredb -restoreconf -restoredcbf -pre -post -targetdir -port -nodbrecover -nouseasnewidb -keeprecent -nooverwrite	新しいオプション Data Protector 内部データベースの復元の新しいオプション。
	-deletebefore -skip	オプションの更新 仮想環境統合ソフトウェアを使用する Microsoft Hyper-V の復元でも指定できます。
	-omnidb -netware -vsr_only -trustee	削除されるオプション
omnirpt	-db_purge -db_purge_preview -db_system	削除されるオプション

表 10 Data Protector A.06.11 からのアップグレード (続き)

コマンド	影響を受けるオプションまたは引数、注意事項	状態
omnirsh	-add -modify	新しいオプション
omnisetup.sh	veagent chs_ls	新しいソフトウェアコンポーネント
	snapa javagui ov	削除されるソフトウェアコンポーネント
	-bundleadd -bundlerem	新しいオプション
omnisrdupdate	-use_raw_object	新しいオプション
	-session	変更されるオプション
omnisv	-maintenance -mom -mom_stop	新しいオプション
omniusb	Data Protector Automatic Disaster Recovery コンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
SharePoint_VSS_backup.ps1	このコマンドは、Data Protector MS Volume Shadow Copy 用統合ソフトウェアコンポーネントがインストールされている Windows システムで使用できます。	新しいコマンド
util_cmd	veagent	新しいオプション
vepa_util.exe	Data Protector 仮想環境統合ソフトウェアコンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
winomnimigrate.pl		削除されるコマンド

表 11 Data Protector 6.20 からのアップグレード

コマンド	影響を受けるオプションまたは引数、注意事項	状態
NNMpost.ovpl		削除されるコマンド
NNMpre.ovpl		削除されるコマンド
NNMScript.exe		削除されるコマンド
ob2install	javagui ov	削除されるソフトウェアコンポーネント
omnib	-storedrim -idb_list	新しいオプション
	-copy	オプションの更新 Microsoft SQL Server 用統合ソフトウェアを使用したバックアップでも指定できます。
	-barmode	オプションの更新

表 11 Data Protector 6.20 からのアップグレード (続き)

コマンド	影響を受けるオプションまたは引数、注意事項	状態
		値 `incr` は、仮想環境統合ソフトウェアを使用した Microsoft Hyper-V 仮想マシンのバックアップにも指定できます。
	`-netware` `-omnidb`	削除されるオプション
`omnib2dinfo`	`Media Agent` コンポーネントがインストールされたシステム上で使用可能です。	新しいコマンド
`omnicc`	`-import_vcd`	新しいオプション
`omnidb`	`-idb`	新しいオプション
	`-netware` `-omnidb`	削除されるオプション

`omnidbcheck`	`-connection`
	`-database_consistency`
	`-media_consistency`
	`-schema_consistency`
	`-verify_db_files`
		新しいオプション

	`-dc`
	`-extended`
	`-quick`
		オプションの更新

	`-core` `-filenames`	削除されるオプション
`omnidbrestore`		削除されるコマンド
`omnidbupgrade`		削除されるコマンド

`omnidbutil`	`-all`
	`-autovacuum`
	`-cp`
	`-disabled`
	`-enabled`
	`-freeze_max_age`
	`-on_n_rows`
	`-on_percentage`
	`-param`
	`-set`
	`-set_passwd`
	`-sync_srv`
	`-table`
	`-to_default`
		新しいオプション

	`-info`
	`-readdb`
	`-show_db_files`
		オプションの更新

表 11 Data Protector 6.20 からのアップグレード (続き)

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-writedb	
	-cdb -check_overs -chktblspace -extendfnames -extendinfo -extendtblspace -filenames -force -list_large_directories -list_mpos_without_overs -maxsize -mmdb -modifytblspace -no_detail -purge_stop -top -upgrade_info	削除されるオプション
omnidbxp	-user -add -username -password -user -check -host -user -update -username -password -user -list -user -remove	新しいオプションとオプションの組み合わせ
omnidbzdb	このコマンドは、Data Protector の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た Windows、HP-UX (Itanium)、Linux システムで使用できます。	新しいコマンド
omnidownload	-dev_info -list_devices -list_libraries -detail	更新されたオプションとオプションの組み合わせ ディスクへのバックアップデバイスで指定するオプションとオプションの組み合わせの更新。
omniiso	-out -net -use_raw_object -host -remotehost -move_to -unique_name -exec_script -password	新しいオプション
	-session	変更されるオプション
	-iso	削除されるオプション

表 11 Data Protector 6.20 からのアップグレード (続き)

コマンド	影響を受けるオプションまたは引数、注意事項	状態
		-out で置き換えられました。下位互換性維持のために使用できます。
omnimm	-delete_unprotected_media	新しいオプション ディスクへのバックアップデバイスの新しいオプション。
	-all -recycle -remove_slots	オプションの更新 ディスクへのバックアップデバイスで指定するオプションの更新。
omniobjcopy	-replication -replist -idb	新しいオプション
	-netware -omnidb	削除されるオプション
omniobjverify	-idb	
	-netware -omnidb	削除されるオプション
omniofflr	このコマンドは、ユーザーインタフェースコンポーネントからコアインストールコンポーネントに移動したため、Data Protector コンポーネントをインストールしたシステム上で使用できるようになりました。	移動されたコマンド
	-rawdisk -section -idb -autorecover -changedevhost -read -force -session -save -skiprestore -logview -opview	新しいオプション
	-omnidb	削除されるオプション
omnir	-idb	新しいオプション
	-tail_log	新しいオプション Microsoft SQL Server 復元の新しいオプション。
	-host/cluster -resourcePool -specificHost	新しいオプション 仮想環境統合ソフトウェアを使用する VMware

表 11 Data Protector 6.20 からのアップグレード (続き)

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-fromSession -untilSession	vSphere の新しいオプション。
	-neworganization -virtual_datacenter_path -virtual_datacenter_uuid -vapp_path -vapp_uuid -vcenter_path -vcenter_uuid -network_name -network_uuid	新しいオプション 仮想環境統合ソフトウェアを使用する VMware vCloud Director の新しいオプション。
	-restoredb -restoreconf -restoredcbf -pre -post -targetdir -port -nodbrecover -nouseasnewidb -keeprecent -nooverwrite	新しいオプション Data Protector 内部データベースの復元の新しいオプション。
	-targetstoragepath	新しいオプション 仮想環境統合ソフトウェアを使用する Microsoft Hyper-V の新しいオプション。
	-deleteafter -keep_for_forensics -new_name	新しいオプション 仮想環境統合ソフトウェアを使用する VMware vSphere の新しいオプション。
	-deletebefore -skip	オプションの更新 仮想環境統合ソフトウェアを使用する Microsoft Hyper-V の復元でも指定できます。
	-virtual-environment -method	オプションの更新 仮想環境統合ソフトウェアを使用する VMware vCloud Director でも指定できます。
	-network_name	オプションの更新 このオプションは、仮想環境統合ソフトウェアを使用する VMware

表 11 Data Protector 6.20 からのアップグレード (続き)

コマンド	影響を受けるオプションまたは引数、注意事項	状態
		vSphere でも指定できます。
	-omnidb -netware -trustee -vsr_only	削除されるオプション
omnirpt	-db_purge -db_purge_preview -db_system	削除されるオプション
omnisetup.sh	javagui ov	削除されるソフトウェアコンポーネント
	-bundleadd -bundlerem	新しいオプション
omnisrdupdate	-use_raw_object	新しいオプション
	-session	変更されるオプション
omnisv	-maintenance -mom -mom_stop	新しいオプション
vepa_util.exe	--list-organizations	新しいオプション 仮想環境統合ソフトウェアを使用する VMware vCloud Director の新しいオプション。
	--check-config --config --configvm --virtual-environment	オプションの更新 仮想環境統合ソフトウェアを使用する VMware vCloud Director でも指定できます。
	--show-incremental-flag --enable-incremental --disable-incremental --list-vms	新しいオプション 仮想環境統合ソフトウェアを使用する Microsoft Hyper-V の新しいオプション。
winomnimigrate.pl		削除されるコマンド

表 12 Data Protector 7.00 からのアップグレード

コマンド	影響を受けるオプションまたは引数、注意事項	状態
NNMpost.ovpl		削除されるコマンド
NNMpre.ovpl		削除されるコマンド
NNMScript.exe		削除されるコマンド
ob2install	javagui ov	削除されるソフトウェアコンポーネント

表 12 Data Protector 7.00 からのアップグレード (続き)

コマンド	影響を受けるオプションまたは引数、注意事項	状態
omnib	-storedrim -idb_list	新しいオプション
	-netware -omnidb	削除されるオプション
omnidb	-idb	新しいオプション
	-netware -omnidb	削除されるオプション
omnidbcheck	-connection -database_consistency -media_consistency -schema_consistency -verify_db_files	新しいオプション
	-dc -extended -quick	オプションの更新
	-core -filenames	削除されるオプション
omnidbrestore		削除されるコマンド
omnidbupgrade		削除されるコマンド
omnidbutil	-all -autovacuum -cp -disabled -enabled -freeze_max_age -on_n_rows -on_percentage -param -set -set_passwd -sync_srv -table -to_default	新しいオプション
	-info -readdb -show_db_files -writedb	オプションの更新
	-cdb -check_overs -chktblspace -extendfnames	削除されるオプション

表 12 Data Protector 7.00 からのアップグレード (続き)

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-extendinfo -extendtblspace -filenames -force -list_large_directories -list_mpos_without_overs -maxsize -mmdb -modifytblspace -no_detail -purge_stop -top -upgrade_info	
omnidbzdb		更新されたコマンド コマンドは、HP-UX (Itanium) および Linux システムでも利用できるようになりました。
	--diskarray	変更されるオプション このオプションは、HP-UX システム上の Data Protector HP P6000/HP 3PAR SMI-S Agent に関連する新しいキーワード 3PAR も受け付けます。
omniiso	-host -remotehost -move_to -unique_name -exec_script -password	新しいオプション
	-session	変更されるオプション
omniobjcopy	-idb	
	-netware -omnidb	削除されるオプション
omniobjverify	-idb	
	-netware -omnidb	削除されるオプション
omnioffl r	このコマンドは、ユーザーインタフェースコンポーネントからコアインストールコンポーネントに移動したため、Data Protector コンポーネントをインストールしたシステム上で使用できるようになりました。	移動されたコマンド
	-idb -autorecover -changedevhost	新しいオプション

表 12 Data Protector 7.00 からのアップグレード (続き)

コマンド	影響を受けるオプションまたは引数、注意事項	状態
	-read -force -session -save -skiprestore -logview -opview	
	-omnidb	削除されるオプション
omnir	-idb	新しいオプション
	-restoredb -restoreconf -restoredcbf -pre -post -targetdir -port -nodbrecover -nouseasnewidb -keeprecent -nooverwrite	新しいオプション Data Protector 内部データベースの復元の新しいオプション。
	-omnidb -netware -trustee -vsr_only	削除されるオプション
omnirpt	-db_purge -db_purge_preview -db_system	削除されるオプション
omnisetup.sh	javagui ov	削除されるソフトウェアコンポーネント
omnisrdupdate	-session	変更されるオプション
omnisv	-maintenance -mom -mom_stop	新しいオプション
winomnimigrate.pl		削除されるコマンド

索引

A

ACS クライアント, 79
ADIC/GRAU ライブラリ
  Media Agent のインストール, 79
  Media Agent をクライアントにインストール, 80
  クライアントの準備, 79
  ドライブの接続, 79
ADIC ライブラリ 参照 ADIC/GRAU ライブラリ
AIX クライアント
  インストール, 64
  バックアップデバイスの接続, 65
allow_hosts ファイル, 139, 140, 141

C

cell_info ファイル, 158
Cell Manager
  Cell Request Server (CRS) サービス, 31, 36
  Data Protector A.06.11、6.20、および 7.00 からのアップグレード、HP-UX の場合, 161, 163
  Key Management Server (KMS), 31
  Key Management Server (KMS) サービス, 36
  Media Management Daemon (MMD) サービス, 31, 36
  SSE のアップグレード, 175
  Veritas Volume Manager の構成、Microsoft Cluster Server, 231
  アップグレード、MC/ServiceGuard の場合, 177
  アップグレード、Microsoft Cluster Server の場合, 180
  アンインストール、HP-UX の場合, 151
  アンインストール、Linux の場合, 154
  アンインストール、MC/ServiceGuard の場合, 152
  アンインストール、Windows の場合, 151
  インストール、HP-UX, 28
  インストール、HP-UX の場合、ネイティブツールの使用, 218
  インストール、Linux の場合, 28
  インストール、Linux の場合、ネイティブツールの使用, 219
  インストール、MC/ServiceGuard, 116
  インストール、Microsoft Cluster Server, 117
  インストール、Windows の場合, 32
  インストール手順, 26
  インストールの前提条件、UNIX の場合, 27
  インストールの前提条件、Windows の場合, 32
  概念, 19
  環境変数の設定、UNIX の場合, 31
  機能, 23
  構成の変更のチェック, 166
  システムの選択, 23
  自動構成されるファイル、UNIX の場合, 30
  手動でアップグレード、UNIX の場合, 215
  準備、NIS サーバー, 231
  セキュリティの概念, 135
  ソフトウェアコンポーネントの変更, 156
  ディレクトリ構造、UNIX の場合, 29
  トラブルシューティング, 207, 211, 215, 217
  名前の変更, 232
Cell Manager のインストール
  HP-UX システムの場合, 28
  HP-UX システムの場合、ネイティブツールの使用, 218
  Linux システムの場合, 28
  Linux システムの場合、ネイティブツールの使用, 219
  MC/ServiceGuard システム, 116
  Microsoft Cluster Server システム, 117
  Windows システムの場合, 32
  前提条件、UNIX の場合, 27
  前提条件、Windows の場合, 32
Cell Request Server (CRS) サービス, 31, 36
CLI 参照 コマンドラインインタフェース
CRS 参照 Cell Request Server (CRS) サービス

D

DAS クライアント, 79
Data Protector 8.00 へのアップグレード
  P6000 EVA アレイ 用統合ソフトウェア, 173
Data Protector A.06.11、6.20、7.00 からのアップグレード
  Oracle 用統合ソフトウェア, 171
  構成の変更のチェック, 166
Data Protector A.06.11、6.20、および 7.00 からのアップグレード
  Cell Manager、HP-UX の場合, 161, 163
  Cell Manager、MC/ServiceGuard の場合, 177
  Cell Manager、Microsoft Cluster Server の場合, 180
  Windows 用インストールサーバー, 164
  インストールサーバー、HP-UX の場合, 161
  概要, 161
  クライアント, 170
  クライアント、MC/ServiceGuard の場合, 171
  クライアント、Microsoft Cluster Server の場合, 182
  前提条件, 161
Data Protector のサービス
  hpdp-idb, 31, 36
  hpdp-idb-as, 31, 37
  hpdp-idb-cp, 31, 36
DB2 用統合ソフトウェア、インストール, 93
debug オプション
  概要, 217
deny_hosts ファイル, 141
Disk Agent
  概念, 19
  構成、HP OpenVMS, 68
DNS
  omnicheck コマンド, 206
  セル内の接続の確認, 205
DNS チェックツール, 227
DVD-ROM
  インストール DVD-ROM 一覧, 22

E

ESX Server クライアント
  インストール, 63

G

global ファイル, 166
GRAU ライブラリ 参照 ADIC/GRAU ライブラリ
GUI 参照 グラフィカルユーザーインタフェース

H

HP
  テクニカルサポート, 17
HP-UX Cell Manager
  Data Protector A.06.11、6.20、および 7.00 からのアップグレード, 161, 163
  PA-RISC から Itanium への移行, 175
  アンインストール, 151
  インストール, 28
  インストール、ネイティブツールの使用, 218
  インストールの前提条件, 27
  環境変数の設定, 31
  自動構成されるファイル, 30
  ディレクトリ構造, 29
  トラブルシューティング, 211, 215
HP-UX インストールサーバー
  インストール、ネイティブツールの使用, 220
HP-UX クライアント
  インストール, 51
  トラブルシューティング, 208
  バックアップデバイスの接続, 53
HP 12000e オートローダー、接続, 249
HP 330fx ライブラリ、SCSI ID の設定, 245
HP 3PAR StoreServ Storage 用統合ソフトウェア
  インストール, 107
HP DAT 24 テープドライブ、接続, 248
HP DLT ライブラリ 24/48 スロット、接続, 250
HP OpenVMS クライアント
  Disk Agent の構成, 68
  Media Agent の構成, 69
  アンインストール, 150
  インポート, 130
HP P4000 SAN ソリューション 用統合ソフトウェア
  インストール, 97
HP P6000 EVA ディスクアレイファミリ 用統合ソフトウェア
  インストール, 97
HP P9000 XP ディスクアレイファミリ 用統合ソフトウェア
  インストール, 102

I

IBM HACMP Cluster
  クライアントのインストール, 126
IDB
  アップグレードのトラブルシューティング, 214
  サイズの増加, 23
inet.conf
  ファイル, 232
inet.log ファイル, 139, 140, 141, 180
Inet サービス, 36
Informix 用統合ソフトウェア、インストール, 91
infs コマンド, 238
installation_servers ファイル, 39
ioscan コマンド, 236, 238, 240

K

Key Management Server (KMS), 31, 36
KMS 参照 Key Management Server (KMS) サービス

L

Linux Cell Manager
  アンインストール, 154
  インストール, 28
  インストール、ネイティブツールの使用, 219
  インストールの前提条件, 27
  環境変数の設定, 31
  自動構成されるファイル, 30
  ディレクトリ構造, 29
Linux インストールサーバー
  インストール、ネイティブツールの使用, 221
Linux クライアント
  インストール, 60
  バックアップデバイスの接続, 62
  リモートインストールのトラブルシューティング, 61
Lotus 用統合ソフトウェア、インストール, 93

M

Mac OS X クライアント
  インストール, 63
Manager-of-Managers
  アップグレード, 174
  アップグレードの概要, 161
MC/ServiceGuard
  Cell Manager のアップグレード, 177
  Cell Manager のアンインストール, 152
  Cell Manager のインストール, 116
  Data Protector A.06.11、6.20、および 7.00 からのクライアントアップグレード, 171
  inet.log ファイルに大量のログが記録される場合, 141
  インストールサーバーのアンインストール, 152
  インポート, 132
  クライアントのインストール, 116
Media Agent
  ADIC/GRAU ライブラリ用のインストール, 80
  StorageTek ACS ライブラリ用のインストール, 84
  概念, 19
  構成、HP OpenVMS, 69
  種類, 19
Media Management Daemon (MMD), 36
Media Management Daemon (MMD) サービス, 31
Microsoft Cluster Server
  Cell Manager と Veritas Volume Manager の構成, 231
  Cell Manager のアップグレード, 180
  Cell Manager のインストール, 117
  インポート, 131
  エクスポート, 134
  クライアントと Veritas Volume Manager の構成, 231
  クライアントのアップグレード, 182
  クライアントのインストール, 123
Microsoft Exchange Server 2007 用統合ソフトウェア
  インストール, 87
Microsoft Exchange Server 2010 用統合ソフトウェア

インストール, 88
Microsoft Exchange 用統合ソフトウェア
HP P6000 EVA ディスクアレイファミリ を備えたシステムへのインストール, 101
HP P9000 XP ディスクアレイファミリ を備えたシステムへのインストール, 106
Microsoft Installer, 207
Microsoft SharePoint Server 2007 用統合ソフトウェア
インストール, 89
Microsoft SQL 用統合ソフトウェア
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, 111
HP P6000 EVA ディスクアレイファミリ を備えたシステムへのインストール, 102
HP P9000 XP ディスクアレイファミリ を備えたシステムへのインストール, 107
インストール, 89
Microsoft サーバークラスター
インストールのための Windows Server 2008 または Windows Server 2012 システムの準備, 229
Microsoft ターミナルサービスクライアント, 33
Microsoft ボリュームシャドウコピーサービス用統合ソフトウェア、インストール, 91
MMD 参照 Media Management Daemon (MMD) サービス

N
NDMP Media Agent、概念, 19
NDMP クライアント、インポート, 130
NDMP 用統合ソフトウェア、インストール, 97
netstat, 227
NIS サーバー、準備, 231
nsswitch.conf
ファイル, 232
nsswitch.conf ファイル, 232

O
omni_info ファイル, 158
omnicc コマンド, 189
omnicheck コマンド, 149, 206
omniinet プロセス 参照 Inet サービス
omnirc ファイル, 167
omnisetup.sh, 154, 155
omnisetup.sh コマンド
アップグレード, 161, 163
インストール, 114
Oracle 用統合ソフトウェア
Data Protector A.06.11、6.20、7.00 からのアップグレード, 171
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, 108
HP P6000 EVA ディスクアレイファミリ を備えたシステムへのインストール, 98
HP P9000 XP ディスクアレイファミリ を備えたシステムへのインストール, 103
アンインストール固有の問題, 157
インストール, 92

P
P6000 EVA アレイ 用統合ソフトウェア
Data Protector 8.00 へのアップグレード, 173

R
rpm ユーティリティ, 154, 155

S
SAP DB 用統合ソフトウェア、インストール, 92
SAP R/3 用統合ソフトウェア
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, 109
HP P6000 EVA ディスクアレイファミリ を備えたシステムへのインストール, 99
HP P9000 XP ディスクアレイファミリ を備えたシステムへのインストール, 104
アップグレード, 172
インストール, 92
SCSI アドレス。 参照 SCSI インタフェース
SCSI インタフェース
ID の設定、HP 330fx ライブラリ, 245
カーネルにロボティクスドライバーを追加、HP-UX, 237
コントローラーパラメーターの設定、Windows の場合, 240
テープドライバーの使用、Windows の場合, 233
未使用の SCSI アドレス、Windows の場合, 245
未使用のアドレスの確認、HP-UX, 240
未使用のアドレスの確認、Solaris の場合, 241
ロボティクスドライバーの無効化、Windows の場合, 233
ロボティクスの構成、HP-UX, 235
SCSI コントローラー。 参照 SCSI インタフェース
SCSI テープドライバー 参照 SCSI インタフェース
SCSI ロボティクス。 参照 SCSI インタフェース
SCSI ロボディクスドライバーの無効化、Windows の場合, 233
Seagate Viper 200 LTO テープドライブ、接続, 253
services ファイル, 227
Solaris Cell Manager
インストールの前提条件, 27
環境変数の設定, 31
ディレクトリ構造, 29
トラブルシューティング, 211, 215
Solaris クライアント
インストール, 54
構成、インストール後, 55
トラブルシューティング, 208
バックアップデバイスの接続, 59
SSE, 174 参照 シングルサーバー版
sst.conf ファイル, 244
st.conf ファイル, 55, 242
STK ACS 参照 StorageTek ACS ライブラリ
StorageTek ACS ライブラリ
Media Agent のインストール, 79
Media Agent をクライアントにインストール, 84
クライアントの準備, 83
ドライブの接続, 79

StorageTek ライブラリ 参照 StorageTek ACS ライブラリ
swagent デーモン, 208
swremove ユーティリティ, 151
Sybase 用統合ソフトウェア、インストール, 91

T
TCP/IP
  設定のチェック、Windows の場合, 226

V
Veritas Cluster
  インポート, 132
  クライアントのインストール, 125
  制限、フェイルオーバー, 125
Veritas Volume Manager
  Cell Manager の構成、Microsoft Cluster Server, 231
  クライアントの構成、Microsoft Cluster Server, 231
VLS デバイス、インポート, 130
VMware(レガシー) 用統合ソフトウェア
  インストール, 94
VMware Granular Recovery Extension
  インストール, 94
VSS 用統合ソフトウェア
  アップグレード, 173

W
Web Reporting、インストール, 115
Web サイト
  HP, 17
  HP メールニュース配信登録, 17
  製品マニュアル, 10
Windows Cell Manager
  32 ビットから 64 ビットへの移行, 176
  アンインストール, 151
  インストール, 32
  インストールの前提条件, 32
  インストールのトラブルシューティング, 37
  トラブルシューティング, 207, 211
Windows Server 2008 および Windows Server 2012
  インストールのための Microsoft サーバークラスターの準備, 229
Windows クライアント
  アンインストール, 150
  インストール, 47
  トラブルシューティング, 207, 209, 215
  バックアップデバイスの接続, 50

Z
ZDB 統合クライアント, 85
  参照 統合

あ
アクセス確認を使用可能にする
  クライアントの場合, 138
  セルで, 139
アクセス権限
  root アカウントへの追加、Linux の場合, 61
アップグレード
  CLI の変更, 255
  global ファイル, 166
  IDB のトラブルシューティング, 214
  Manager-of-Managers, 174
  omnirc ファイル, 167
  omnisetup.sh, 161
  omnisetup.sh コマンド, 163
  SAP R/3 用統合ソフトウェア, 172
  SSE から Data Protector 8.00, 174
  VSS 用統合ソフトウェア, 173
  アップグレード前の注意点, 159
  概要, 159
  手順, 160
  手動、UNIX の場合, 215
  制限事項, 160
  トラブルシューティング、UNIX の場合, 211
  トラブルシューティング、Windows の場合, 207, 211
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, 207
  Data Protector パッチ, 214
  IDB が使用できない, 214
  Microsoft Installer に関する問題, 207
  構成ファイルが使用できない, 214
アンインストール
  Cell Manager、HP-UX の場合, 151
  Cell Manager、Linux の場合, 154
  Cell Manager、MC/ServiceGuard の場合, 152
  Cell Manager、Windows の場合, 151
  Oracle 用統合ソフトウェア固有の問題, 157
  rpm ユーティリティ, 154, 155
  swremove ユーティリティ, 151
  インストールサーバー、HP-UX の場合, 151
  インストールサーバー、Linux の場合, 155
  インストールサーバー、MC/ServiceGuard の場合, 152
  インストールサーバー、Windows の場合, 151
  概要, 149
  クライアント、HP OpenVMS から, 150
  クライアント、リモート, 150
  クラスタークライアント, 150
  前提条件, 149

い
移行
  HP-UX 上の Cell Manager、PA-RISC から Itanium へ, 175
  Windows 用 Cell Manager、32 ビットから 64 ビットへ, 176
  ライセンス, 203
インストール
  ADIC/GRAU ライブラリ用の Media Agent, 79, 80
  DB2 用統合ソフトウェア, 93
  HP 3PAR StoreServ Storage 用統合ソフトウェア, 107
  HP P4000 SAN ソリューション 用統合ソフトウェア, 97
  HP P6000 EVA ディスクアレイファミリ 用統合ソフトウェア, 97
  HP P9000 XP ディスクアレイファミリ 用統合ソフトウェア, 102

Informix 用統合ソフトウェア, 91
Lotus 用統合ソフトウェア, 93
Microsoft Exchange Server 2007 用統合ソフトウェア, 87
Microsoft Exchange Server 2010 用統合ソフトウェア, 88
Microsoft SharePoint Server 2007 用統合ソフトウェア, 89
Microsoft SQL 用統合ソフトウェア, 89
Microsoft ボリュームシャドウコピーサービス用統合ソフトウェア, 91
NDMP 用統合ソフトウェア, 97
omnisetup.sh, 154, 155
Oracle 用統合ソフトウェア, 92
SAP DB 用統合ソフトウェア, 92
SAP R/3 用統合ソフトウェア, 92
StorageTek ACS ライブラリ用の Media Agent, 79, 84
Sybase 用統合ソフトウェア, 91
VMware(レガシー) 用統合ソフトウェア, 94
VMware Granular Recovery Extension, 94
Web Reporting, 115
Windows Server 2008 または Windows Server 2012 での Microsoft サーバークラスターの準備, 229
一般的な手順, 20
概要, 19
各国語版ユーザーインタフェース, 112
仮想環境統合ソフトウェア, 94
クライアントのインストール、概要, 42
クライアントの確認, 210
クライアントのトラブルシューティング、UNIX の場合, 208
クラスター対応 Cell Manager, 116, 117
クラスター対応クライアント, 116, 123, 125, 126
クラスター対応統合ソフトウェア, 87
恒久ライセンスパスワード, 197
コンポーネント 参照 インストールコンポーネント
シングルサーバー版, 114
ソフトウェアコンポーネント, 44
ソフトウェアコンポーネントコード, 77
統合, 84
統合ソフトウェア、概要, 84
トラブルシューティング、Windows の場合, 207, 209
リモートインストール、概要, 70
リモート、概念, 21
ローカルクライアント, 47, 65, 76
ログファイル, 215
インストールコンポーネント
Disk Agent, 19
General Media Agent, 19
Media Agent, 19
NDMP Media Agent, 19
インストールサーバー, 19
ユーザーインタフェース, 19
インストールサーバー
Data Protector A.06.11、6.20、および 7.00 からのアップグレード、HP-UX の場合, 161
アンインストール、HP-UX の場合, 151
アンインストール、Linux の場合, 155
アンインストール、MC/ServiceGuard の場合, 152
アンインストール、Windows の場合, 151
インストール、HP-UX の場合、ネイティブツールの使用, 220
インストール、Linux の場合、ネイティブツールの使用, 221
インストール、UNIX の場合, 38
インストール、Windows の場合, 39
インストール概要, 37
インストール手順, 26
インストールの前提条件、UNIX の場合, 38
インストールの前提条件、Windows の場合, 39
概念, 19
手動でアップグレード、UNIX の場合, 215
セルへのインポート, 130
ディレクトリ構造、UNIX の場合, 29
インストールサーバー A.06.11、6.20、および 7.00、Windows の場合
Data Protector からのアップグレード, 164
インストールサーバーのインストール
HP-UX システムの場合、ネイティブツールの使用, 220
Linux システムの場合、ネイティブツールの使用, 221
UNIX システムの場合, 38
Windows システムの場合, 39
概要, 37
前提条件、UNIX の場合, 38
前提条件、Windows の場合, 39
インストールの準備
Windows Server 2008 または Windows Server 2012 で実行している Microsoft サーバークラスター, 229
インストールのトラブルシューティング
Cell Manager、Windows の場合, 37
Data Protector ソフトウェア、Windows の場合, 207
debug オプション, 217
Mac OS X クライアント, 209
Microsoft Installer に関する問題, 207
omnicheck コマンド, 206
swagent デーモン, 208
各国語版ユーザーインタフェース, 112
クライアント、HP-UX の場合, 208
実行トレースファイル, 217
リモートインストール、Linux の場合, 61
リモートインストール、UNIX の場合, 208
リモートインストール、Windows の場合, 209
ログファイル, 215
インポート
HP OpenVMS クライアント, 130
NDMP クライアント, 130
VLS デバイス, 130
インストールサーバー, 130
クライアント, 129
クラスター, 131
複数の LAN カードが構成されたクライアント, 130

え

エクスポート
Microsoft Cluster Server クライアント, 134
クライアント, 134

か

カーネル
  SCSI ロボティクスドライバーの追加、HP-UX, 237
  再ビルド、HP-UX, 237
カーネルの再ビルド、HP-UX, 237
概念
  Cell Manager, 19
  Disk Agent, 19
  Media Agent, 19
  NDMP Media Agent, 19
  インストールサーバー, 19
  インポート, 129
  エクスポート, 133
  クライアント, 19
  グラフィカルユーザーインタフェース (GUI), 24
  セル, 19
  バックアップ環境, 19
  ユーザーインタフェース, 19
  リモートインストール, 21
概要
  Data Protector、A.06.11、6.20、および 7.00 からのアップグレード, 161
  debug オプション, 217
  アップグレード, 159
  アプリケーションクラスターパッケージのインポート, 131
  アンインストール, 149
  インストールサーバーのインストール, 37
  クライアントのインストール, 42
  クライアントのリモートインストール, 70
  クラスター対応クライアントのインポート, 131
  クラスター対応統合ソフトウェアのインストール, 87
  実行トレースファイル, 217
  製品構成, 183
  ソフトウェアコンポーネント, 44
  ソフトウェアコンポーネントの変更, 156
  統合, 85
  統合ソフトウェアのインストール, 84
  バックアップデバイスの接続, 246
  ライセンス, 199
各国語版ユーザーインタフェース, 111
  参照 ユーザーインタフェース
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, 112
確認
  インストールされたライセンス, 198
  パッチ, 148
  必要なライセンスパスワード, 202
  未使用の SCSI アドレス、HP-UX, 240
  未使用の SCSI アドレス、Solaris の場合, 241
  未使用のアドレスの確認、Windows の場合, 245
仮想環境統合ソフトウェア
  インストール, 94
仮想サーバー、セルへのインポート, 131
環境変数、UNIX Cell Manager での設定, 31
関連ドキュメント, 10
関連ライセンス, 184

き

規則
  表記, 15
機能拡張、ライセンス, 183

く

クライアント, 226
  ADIC/GRAU ライブラリの準備, 79
  Data Protector A.06.11、6.20、および 7.00 からのアップグレード, 170
  Data Protector A.06.11、6.20、および 7.00 からのアップグレード、MC/ServiceGuard の場合, 171
  Microsoft Cluster Server、セルからエクスポート, 134
  root アクセス権限の追加、Linux の場合, 61
  StorageTek ACS ライブラリの準備, 83
  Veritas Volume Manager の構成、Microsoft Cluster Server, 231
  アクセス確認を解除する, 141
  アクセス確認を使用可能にする, 138
  アップグレード、Microsoft Cluster Server の場合, 182
  インストール、概要, 42
  インストール後の構成、Solaris の場合, 55
  インストールの確認, 210
  概念, 19
  クラスター対応、セルへのインポート, 131
  クラスター対応統合ソフトウェアのインストール、概要, 87
  セキュリティの概念, 135
  セルからのエクスポート, 133
  セルへのインポート, 129
  ソフトウェアコンポーネントの変更, 156
  デバイスファイルの作成、HP-UX, 238
  デバイスファイルの作成、Solaris の場合, 244
  統合ソフトウェアのインストール、概要, 84
  トラブルシューティング, 207, 208, 209, 215, 217
  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, 242
  保護, 138
  ホストからのアクセスの拒否, 141
  リモートアンインストール, 150
  リモートインストール、概要, 70
  ローカルインストール、HP OpenVMS, 65
クライアント、インストール
  ADIC/GRAU ライブラリ用の Media Agent, 80
  AIX システムの場合, 64
  DB2 用統合ソフトウェア, 93
  ESX Server システムの場合, 63
  HP-UX システムの場合, 51
  HP 3PAR StoreServ Storage 用統合ソフトウェア, 107
  HP OpenVMS システム, 65
  HP P4000 SAN ソリューション 用統合ソフトウェア, 97
  HP P6000 EVA ディスクアレイファミリ 用統合ソフトウェア, 97
  HP P9000 XP ディスクアレイファミリ 用統合ソフトウェア, 102
  IBM HACMP クラスターシステムの場合, 126
  Informix 用統合ソフトウェア, 91
  Linux システムの場合, 60

Lotus 用統合ソフトウェア, 93
Mac OS X システム, 63
MC/ServiceGuard システム, 116
Microsoft Cluster Server システム, 123
Microsoft Exchange Server 2007 用統合ソフトウェア, 87
Microsoft Exchange Server 2010 用統合ソフトウェア, 88
Microsoft SharePoint Server 2007 用統合ソフトウェア, 89
Microsoft SQL 用統合ソフトウェア, 89
Microsoft ボリュームシャドウコピーサービス用統合ソフトウェア, 91
NDMP 用統合ソフトウェア, 97
Oracle 用統合ソフトウェア, 92
SAP DB 用統合ソフトウェア, 92
SAP R/3 用統合ソフトウェア, 92
Solaris システムの場合, 54
StorageTek ACS ライブラリ用の Media Agent, 84
Sybase 用統合ソフトウェア, 91
UNIX システムの場合, 76
Veritas Cluster システム, 125
VMware(レガシー) 用統合ソフトウェア, 94
VMware Granular Recovery Extension, 94
Windows システムの場合, 47
仮想環境統合ソフトウェア, 94
シングルサーバー版, 114
クライアントのインストール
AIX システムの場合, 64
ESX Server システムの場合, 63
HP-UX システムの場合, 51
HP OpenVMS システム, 65
IBM HACMP クラスターシステムの場合, 126
Linux システムの場合, 60
Mac OS X システム, 63
MC/ServiceGuard システム, 116
Microsoft Cluster Server システム, 123
Solaris システムの場合, 54
UNIX システムの場合, 76
Veritas Cluster システム, 125
Windows システムの場合, 47
クライアントのセルへの追加
Data Protector GUI, 73
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, 79
AIX クライアント, 65
HP-UX クライアント, 53
Linux クライアント, 62
Solaris クライアント, 59
Windows クライアント, 50
クラスター
Cell Manager のインストール, 117
Microsoft Cluster Server、セルからエクスポート, 134
アンインストール, 150
クライアントのインストール, 123, 125
セルへのインポート, 131
ソフトウェアコンポーネントの変更, 157
統合ソフトウェアのインストール, 87
グラフィカルユーザーインタフェース (GUI)
概念, 24
ビュー, 24

け
権限を認められたシステムのリスト、保護, 137
検証
クライアントのインストール, 210
セル内の DNS 接続, 205
ライセンスパスワード, 198

こ
恒久ライセンスパスワードの取得, 197
構成
Cell Manager と Veritas Volume Manager、MSCS, 231
Disk Agent、HP OpenVMS, 68
Media Agent、HP OpenVMS, 69
SCSI ロボティクス、HP-UX, 235
Solaris クライアント、インストール後, 55
Solaris クライアント、バックアップデバイスの使用前, 242
sst.conf ファイル, 244
st.conf ファイル, 55, 242
クライアントと Veritas Volume Manager、Microsoft Cluster Server, 231
構成ファイル
cell_info, 158
Data Protector A.06.11、6.20、および 7.00 からのアップグレード後の変更のチェック, 166
inet.conf, 232
installation_servers, 39
nsswitch.conf, 232
omni_info, 158
omnirc, 167
sst.conf, 244
st.conf, 242
st.conf ファイル, 55
アップグレードに関する問題, 214
グローバル, 166
自動構成されるファイル、UNIX Cell Manager の場合, 30
変更、Solaris クライアントのインストール, 55
コマンド, 161, 227
CLI の変更、アップグレード後, 255
infs, 238
ioscan, 236, 238, 240
netstat, 227
omnicc, 189
omnicheck, 149, 206
omnisetup.sh, 114, 161, 163
コマンドラインインタフェース (CLI), 19, 24

さ
削除
Data Protector ソフトウェアを手動で、UNIX の場合, 156
クライアントのアクセス確認, 141
ソフトウェアコンポーネント、UNIX の場合, 157, 158

ソフトウェアコンポーネント、Windows の場合, 156
ソフトウェアコンポーネント、概要, 156
作成
実行トレースファイル、インストール, 217
デバイスファイル、HP-UX, 238
デバイスファイル、Solaris の場合, 244
デバイスファイル、Windows の場合, 234

し
実行トレースファイル
debug オプション, 217
準備、NIS サーバー, 231
使用
SCSI テープドライバー、Windows の場合, 233
ライセンス, 159, 161
ログファイル, 215
使用権, 199
シングルサーバー版
Data Protector 8.00 へのアップグレード, 174
インストール, 114
制限事項, 114
製品概要、ライセンス, 202
複数のシステムからのアップグレード, 175

す
スターターパック、ライセンス, 183

せ
制限事項
Manager-of-Managers のアップグレード, 161
Windows システムの場合, 40, 48
アップグレード, 160
シングルサーバー版, 114
セキュリティ
allow_hosts ファイル, 139, 140, 141
deny_hosts ファイル, 141
inet.log ファイルに大量のログが記録される場合, 141
クライアントのアクセス確認を解除する, 141
クライアントの保護を使用可能にする, 138
権限を認められたシステムのリスト, 137
セルの保護を使用可能にする, 139
潜在的な問題点, 137
ホストからのアクセスの拒否, 141
設定
SCSI ID、HP 330fx ライブラリ, 245
SCSI コントローラーパラメーター、Windows の場合, 240
環境変数、UNIX Cell Manager の場合, 31
セル
DNS 接続の確認, 205
Microsoft Cluster Server クライアントのエクスポート, 134
アップグレード、概要, 160
インストールサーバーのインポート, 130
概念, 19
クライアントのインポート, 129
クライアントのエクスポート, 133
クライアントの保護設定, 138
クラスターのインポート, 131
セキュリティを有効にする, 139
ライセンス, 183
前提条件
Cell Manager のインストール、UNIX の場合, 27
Cell Manager のインストール、Windows の場合, 32
Data Protector A.06.11、6.20、および 7.00 からのアップグレード, 161
インストールサーバーのインストール、UNIX の場合, 38
インストールサーバーのインストール、Windows の場合, 39

そ
ソフトウェアコンポーネント
依存関係、Solaris の場合, 158
概要, 44
コンポーネントコード, 77
削除、UNIX の場合, 157, 158
削除、Windows の場合, 156
追加、HP-UX の場合, 157
追加、Linux への, 157
追加、Windows の場合, 156
変更、概要, 156
変更、クラスタークライアントの場合, 157
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, 157
Linux システムへの, 157
Windows システムの場合, 156
概要, 156

た
ターミナルサービスクライアント, 33
対象読者, 10
大量のログ, 141

ち
チェック
TCP/IP の設定、Windows の場合, 226
クライアントのインストール, 210
ライセンス, 183
ログファイル、インストール, 215

つ
追加
アクセス権限、Linux の場合, 61
カーネルの SCSI ロボティクスドライバー、HP-UX, 237

て
データベースのサイズの増加 参照 IDB
テープドライバー 参照 SCSI インタフェース
テクニカルサポート
HP, 17
サービスロケーター Web サイト, 17
デバイスファイル
作成、HP-UX, 238
作成、Solaris の場合, 244
作成、Windows の場合, 234
デフォルトポート、変更, 227

と
統合
Oracle、UNIX の場合, 171
Oracle のアップグレード、Windows の場合, 171
P6000 EVA アレイ , 173
P6000 EVA アレイ のアップグレード, 173
SAP R/3、UNIX システムの場合, 172
SAP R/3 のアップグレード、Windows システムの場合, 172
VSS のアップグレード , 173
概要, 85
クラスター対応、インストール, 87
リモートインストール, 86
ローカルインストール, 86
統合クライアント, 84
参照 統合
統合ソフトウェア、インストール
DB2 用統合ソフトウェア, 93
HP 3PAR StoreServ Storage 用統合ソフトウェア, 107
HP P4000 SAN ソリューション 用統合ソフトウェア, 97
HP P6000 EVA ディスクアレイファミリ 用統合ソフトウェア, 97
HP P9000 XP ディスクアレイファミリ 用統合ソフトウェア, 102
Informix 用統合ソフトウェア, 91
Lotus 用統合ソフトウェア, 93
Microsoft Exchange 2007 用統合ソフトウェア, 87
Microsoft Exchange Server 2010 用統合ソフトウェア, 88
Microsoft SharePoint Server 2007 用統合ソフトウェア, 89
Microsoft SQL 用統合ソフトウェア, 89
Microsoft ボリュームシャドウコピーサービス用統合ソフトウェア, 91
NDMP 用統合ソフトウェア, 97
Oracle 用統合ソフトウェア, 92
SAP DB 用統合ソフトウェア, 92
SAP R/3 用統合ソフトウェア, 92
Sybase 用統合ソフトウェア, 91
VMware(レガシー) 用統合ソフトウェア, 94
VMware 統合ソフトウェア, 94
仮想環境統合ソフトウェア, 94
ドキュメント
HP Web サイト, 10
意見の送付, 18
関連ドキュメント, 10
ドメインネームシステム 参照 DNS
ドライブライセンス, 183
トレースファイル 参照 実行トレースファイル

は
バックアップ環境の概念, 19
バックアップデバイス
SCSI ID の設定、HP 330fx ライブラリ, 245
バックアップデバイス、接続
ADIC/GRAU ライブラリドライブ, 79
AIX クライアント, 65
HP-UX クライアント, 53
HP 12000e オートローダー, 249
HP DAT 24 テープドライブ, 248
HP DLT ライブラリ 24/48 スロット, 250
Linux クライアント, 62
Seagate Viper 200 LTO テープドライブ, 253
Solaris クライアント, 59
Windows クライアント, 50
概要, 246
バックアップデバイスの接続
ADIC/GRAU ライブラリドライブ, 79
AIX クライアント, 65
HP-UX クライアント, 53
HP 12000e オートローダー, 249
HP DAT 24 テープドライブ, 248
HP DLT ライブラリ 24/48 スロット, 250
Linux クライアント, 62
Seagate Viper 200 LTO テープドライブ, 253
Solaris クライアント, 59
Windows クライアント, 50
概要, 246
パッチ
omnicheck コマンド, 149
確認, 148

ひ
ビュー、グラフィカルユーザーインタフェース, 24
表記
規則, 15

ふ
ファイル
allow_hosts, 139, 140, 141
deny_hosts, 141
services, 227
複数の LAN カードが構成されたクライアント、インポート, 130
プロセス
Cell Request Server (CRS) サービス, 31, 36
Inet サービス, 36
Key Management Server (KMS), 31, 36
Media Management Daemon (MMD), 36
Media Management Daemon (MMD) サービス, 31

へ
ヘルプ
取得, 17
変更
Cell Manager 名, 232
ソフトウェアコンポーネント, 156
デフォルトポート, 227

ほ
保護
クライアント, 138
セル, 139
保守モード, 127
ホストからのアクセスの拒否, 141

み
未使用の SCSI アドレス。 参照 SCSI インタフェース

め
メールニュース配信登録、HP, 17

ゆ
ユーザーインタフェース 参照 コマンドラインインタフェース (CLI)、グラフィカルユーザーインタフェース (GUI)
  概念, 19
  各国語版ユーザーインタフェースのインストール, 112
  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, 112
  システムの選択, 24

ら
ライセンス, 199
  Cell Manager, 184
  Data Protector A.06.11、6.20、および 7.00 からのアップグレード, 161
  SSE からのアップグレード, 174
  一時パスワード, 195
  インストールされたライセンスの確認, 198
  エンティティーベースのライセンス, 184
  概要, 199
  機能拡張, 183
  緊急用パスワード, 195
  恒久パスワード, 195
  恒久パスワード、取得とインストール, 197
  恒久パスワードの取得とインストール, 197
  集中型ライセンス、構成, 199
  スターターパック, 183
  製品概要, 201, 202
  製品構成, 183, 199
  ドライブライセンス, 183
  パスワードの検証, 198
  パスワードのタイプ, 195
  必要なパスワードの確認, 202
  容量ベースのライセンス, 184
  容量ベースのライセンス、例, 187, 189
  ライセンスの移行, 203
  ライセンスの移動, 198
  ライセンスの使用、アップグレード後, 161, 174
  ライセンスのチェックとレポート, 183
  ライセンスフォーム, 203
  ライセンスレポートの作成, 189
ライセンスの移動, 198
ライセンスのレポート, 183
ライセンスフォーム, 203

り
リモートインストール
  クライアント, 70
  統合, 86
  トラブルシューティング、Linux の場合, 61

ろ
ローカルインストール、クライアント, 47, 65, 76
ログファイル
  inet.log, 139, 140, 141, 180
  位置, 216
  説明, 216
  チェック、インストール, 215
ロボティクス。 参照 SCSI インタフェース

用語集

A

ACSLS
(StorageTek 固有の用語) Automated Cartridge System Library Server の略語。ACS(Automated Cartridge System: 自動カートリッジシステム) を管理するソフトウェア。

Active Directory
(Windows 固有の用語) Windows ネットワークで使用されるディレクトリサービス。ネットワーク上のリソースに関する情報を格納し、ユーザーやアプリケーションからアクセスできるように維持します。このディレクトリサービスでは、サービスが実際に稼動している物理システムの違いに関係なく、リソースに対する名前や説明の付加、検索、アクセス、および管理を一貫した方法で実行できます。

AES 256 ビット暗号化
256 ビット長のランダムキーを使用する AES-CTR(Advanced Encryption Standard in Counter Mode) 暗号化アルゴリズムを基にした Data Protector ソフトウェア暗号化。暗号化と復号化の両方で同じキーが使用されます。データはネットワークを介して転送される前およびメディアに書き込まれる前に、AES 256 ビット暗号化機能によって暗号化されます。

AML
(ADIC/GRAU 固有の用語) Automated Mixed-Media library(自動混合メディアライブラリ) の略。

AMU
(ADIC/GRAU 固有の用語) Archive Management Unit(アーカイブ管理単位) の略。

Application Agent
クライアント上でオンラインデータベース統合ソフトウェアを復元およびバックアップするために必要なコンポーネント。
Disk Agent も参照。

ASR セット
フロッピーディスク上に保存されたファイルのコレクション。交換用ディスクの適切な再構成 (ディスクパーティション化と論理ボリュームの構成) およびフルクライアントバックアップでバックアップされたオリジナルシステム構成とユーザーデータの自動復旧に必要となります。これらのファイルは、ASR アーカイブファイルとして、バックアップメディア上だけでなく Cell Manager 上の、*Data_Protector_program_data*\Config\server\dr\asr ディレクトリ (Windows の場合)、または/etc/opt/omni/server/dr/asr/ディレクトリ (UNIX の場合) にも格納されます。障害が発生すると、ASR アーカイブファイルは複数のフロッピーディスクに展開されます。これらのフロッピーディスクは、ASR の実行時に必要となります。

B

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

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

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

BCV
(EMC Symmetrix 固有の用語) Business Continuance Volumes の略。BCV デバイスは ICDA 内であらかじめ構成された専用の SLD です。ビジネスの継続運用を可能にするために使用されます。BCV デバイスには、これらのデバイスによりミラー化される SLD のアドレスとは異なる、個別の SCSI アドレスが割り当てられます。BCV デバイスは、保護を必要とする一次 EMC Symmetrix SLD の分割可能なミラーとして使用されます。
BC および BC Process も参照。

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

BRBACKUP **(SAP R/3 固有の用語)**SAP R/3 バックアップツールの 1 つ。制御ファイル、個々のデータファイル、またはすべての表領域をオンラインでもオフラインでもバックアップできます。また、必要に応じて、オンライン REDO ログファイルをバックアップすることもできます。BRARCHIVE および BRRESTORE も参照。

BRRESTORE **(SAP R/3 固有の用語)**SAP R/3 のツール。以下の種類のファイルを復元するために使います。

- BRBACKUP で保存されたデータベースデータファイル、制御ファイル、オンライン REDO ログファイル
- BRARCHIVE でアーカイブされた REDO ログファイル
- BRBACKUP で保存された非データベースファイル

ファイル、テーブルスペース、バックアップ全体、REDO ログファイルのログシーケンス番号、またはバックアップのセッション ID を指定することができます。BRBACKUP および BRARCHIVE も参照。

BSM Data Protector バックアップセッションマネージャー (Backup Session Manager) の略。バックアップセッションを制御します。このプロセスは、常に Cell Manager システム上で稼動します。

C

CAP **(StorageTek 固有の用語)**Cartridge Access Port の略。ライブラリのドアパネルに組み込まれたポートです。メディアの出し入れに使用されます。

CDB カタログデータベース (CDB) を参照。

CDF ファイル **(UNIX システム固有の用語)**Context Dependent File(コンテキスト依存ファイル) の略。CDF ファイルは、同じパス名でグループ化された複数のファイルからなるファイルです。通常、プロセスのコンテキストに基づいて、これらのファイルのいずれかがシステムによって選択されます。このメカニズムにより、クラスター内のすべてホストから同じパス名を使って、マシンに依存する実行可能ファイル、システムデータ、およびデバイスファイルを正しく動作させることができます。

Cell Manager セル内のメインシステム。Data Protector の運用に不可欠なソフトウェアがインストールされ、すべてのバックアップおよび復元作業がここから管理されます。管理タスク用の GUI は、異なるシステムにインストールできます。各セルには Cell Manager システムが 1 つあります。

Certificate Server Windows Certificate Server をインストールして構成すると、クライアントに証明書を提供することができます。証明書サーバーは、エンタープライズ用の証明書を発行および管理するためのカスタマイズ可能なサービスを提供します。これらのサービスでは、公開キーベースの暗号化技術で使用されている証明書の発行、取り消し、および管理が可能です。

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

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

CMMDB(Centralized Media Management Database: 集中型メディア管理データベース) CMMDB を参照。

COM+ クラス登録データベース **(Windows 固有の用語)**COM+ クラス登録データベースと Windows レジストリには、アプリケーションの属性、クラスの属性、およびコンピューター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。

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

CSM
Data Protector コピーおよび集約セッションマネージャー (Copy and Consolidation Session Manager) の略。このプロセスは、オブジェクトコピーセッションとオブジェクト集約セッションを制御し、Cell Manager システム上で動作します。

D

Data_Protector_home
Data Protector のプログラムファイルを含むディレクトリへの参照 (Windows Vista、Windows 7、Windows 8、Windows Server 2008、および Windows Server 2012 の場合)、または Data Protector のプログラムファイルおよびデータファイルを含むディレクトリへの参照 (他の Windows オペレーティングシステムの場合)。デフォルトのパスは、`%ProgramFiles%\OmniBack` ですが、パスはインストール時に Data Protector セットアップウィザードで変更できます。
Data_Protector_program_data も参照。

Data_Protector_program_data
Windows Vista、Windows 7、Windows 8、Windows Server 2008、および Windows Server 2012 上の Data Protector データファイルを含むディレクトリへの参照。デフォルトのパスは、`%ProgramData%\OmniBack` ですが、パスはインストール時に Data Protector セットアップウィザードで変更できます。
Data_Protector_home も参照。

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

DC ディレクトリ
DC バイナリファイルを格納するディレクトリ。構成済み Data Protector バックアップメディアごとに 1 つあります。DC ディレクトリは、Data Protector 内部データベースの詳細カタログバイナリファイル部分を構成します。
詳細カタログバイナリファイル (DBCF) および内部データベース (IDB) も参照。

DCBF
詳細カタログバイナリファイル (DCBF) を参照。

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

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

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

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

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

DR OS
ディザスタリカバリを実行するオペレーティングシステム環境。Data Protector に対して基本的な実行時環境 (ディスク、ネットワーク、テープ、およびファイルシステムへのアクセス) を提供します。Data Protector ディザスタリカバリを実行する前に、DR OS をディスクにインストールするかメモリにロードして、構成しておく必要があります。DR OS には、一時 DR OS とアクティブ DR OS があります。一時 DR OS は、他のオペレーティングシステムの復元用ホスト環境として排他的に使用されます。このホスト環境には、ターゲットとなるオペレーティングシステムの構成データも置かれます。ターゲットシステムを元のシステム構成

に復元し終えた後、一時 DR OS は削除されます。アクティブ DR OS は、Data Protector ディザスタリカバリプロセスのホストとして機能するだけでなく、復元後のシステムの一部にもなります。その場合、DR OS の構成データは元の構成データに置き換わります。

DR イメージ 一時ディザスタリカバリオペレーティングシステム (DR OS) のインストールおよび構成に必要なデータ。

E

EMC Symmetrix Agent EMC Symmetrix 環境でのバックアップ操作と復元操作を可能にする Data Protector ソフトウェアモジュール。

Event Log(Data Protector: イベントログ) イベントログには、Data Protector 関連のすべての通知が書き込まれます。デフォルトの送信方法では、すべての通知がイベントログに送信されます。イベントは、Cell Manager の *Data_Protector_program_data*\log\server\Ob2EventLog.txt ファイル (Windows システムの場合)、または/var/opt/omni/server/log/Ob2EventLog.txt ファイル (UNIX システムの場合) に記録されます。このイベントログにアクセスできるのは、Data Protector の Admin ユーザーグループに所属しているユーザーか、Data Protector の「レポートと通知」ユーザー権限が付与されているユーザーのみです。イベントログに書き込まれているイベントは、いずれも表示と削除が可能です。

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

F

FC ブリッジ ファイバーチャネルブリッジ を参照。

G

GUI Data Protector には、構成、管理、および操作に関するあらゆるタスクに簡単にアクセスできる、グラフィカルユーザーインタフェースが用意されています。Microsoft Windows オペレーティングシステムで使用できます。

H

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

HP Business Copy (BC) P6000 EVA **(HP P6000 EVA ディスクアレイファミリ 固有の用語)** ローカル複製ソフトウェアソリューションの 1 つで、P6000 EVA ファームウェアのスナップショット機能およびクローン機能を使用して、ソースボリュームの特定時点のコピー (複製) を作成できます。
複製、ソースボリューム、スナップショット、および HP Continuous Access + Business Copy (CA+BC) P6000 EVA も参照。

HP Business Copy (BC) P9000 XP **(HP P9000 XP ディスクアレイファミリ 固有の用語)** HP P9000 XP ディスクアレイファミリ 構成の 1 つで、データ複製やバックアップなどのさまざまな目的のために LDEV の内部コピーの作成および保守を可能にします。これらのコピー (セカンダリボリューム:S-VOL) は、プライマリボリューム (P-VOL) から分離して、別のシステムに接続することができます。Data Protector ゼロダウンタイムバックアップを目的とする場合、アプリケーションシステムで P-VOL を使用可能にし、S-VOL セットのいずれかをバックアップシステムで使用可能にする必要があります。
LDEV、HP Continuous Access (CA) P9000 XP、メインコントロールユニット、アプリケーションシステム、およびバックアップシステム も参照。

HP Command View (CV) EVA **(HP P6000 EVA ディスクアレイファミリ 固有の用語)** P6000 EVA ストレージシステムを構成、管理、モニターするためのユーザーインタフェース。さまざまなストレージ管理作業を行うために使用されます。たとえば、仮想ディスクファミリの作成、ストレージシステムハードウェアの管理、仮想ディスクのスナップショットやスナップクローン、ミラークローンの

作成などに使用されます。HP Command View EVA ソフトウェアは HP ストレージマネジメントアプライアンス上で動作し、Web ブラウザーからアクセスできます。
HP P6000/HP 3PAR SMI-S Agent および HP SMI-S P6000 EVA アレイ プロバイダー も参照。

HP Continuous Access (CA) P9000 XP
(HP P9000 XP ディスクアレイファミリ 固有の用語) HP P9000 XP ディスクアレイファミリ 構成の 1 つで、データ複製やバックアップ、ディザスタリカバリなどのために LDEV のリモートコピーの作成および保守を可能にします。HP CA P9000 XP を使用するには、メイン (プライマリ) ディスクアレイユニットとリモート (セカンダリ) ディスクアレイユニットが必要です。メインディスクアレイユニットはアプリケーションシステムに接続され、オリジナルのデータを格納しているプライマリボリューム (P-VOL) を格納します。リモートディスクアレイはバックアップシステムに接続され、セカンダリボリューム (S-VOL) を格納します。
HP Business Copy (BC) P9000 XP、メインコントロールユニット、および LDEV も参照。

HP Continuous Access + Business Copy (CA+BC) P6000 EVA
(HP P6000 EVA ディスクアレイファミリ 固有の用語) HP P6000 EVA ディスクアレイファミリ 構成の 1 つで、リモート P6000 EVA 上にソースボリュームのコピー (複製) を作成および保守し、このリモートアレイでローカル複製を行うときにソースとしてこのコピーを使用できます。
HP Business Copy (BC) P6000 EVA、複製、およびソースボリューム も参照。

HP P6000 / HP 3PAR SMI-S Agent
HP P6000 EVA ディスクアレイファミリ 統合に必要なすべてのタスクを実行する Data Protector のソフトウェアモジュール。HP P6000 / HP 3PAR SMI-S Agent を使用すると、受信した要求とストレージシステムのネイティブインタフェース間のやり取りを制御する適切な SMI-S プロバイダーを通じてアレイを制御できます。
HP Command View (CV) EVA および HP SMI-S P6000 EVA アレイ プロバイダー も参照。

HP P9000 XP Agent
Data Protector HP P9000 XP ディスクアレイファミリ 統合に必要なすべてのタスクを実行する Data Protector コンポーネント。P9000 XP アレイ ストレージシステムとの通信に RAID Manager ライブラリを使用します。
RAID Manager ライブラリ も参照。

HP SMI-S P6000 EVA アレイ プロバイダー
HP P6000 EVA ディスクアレイファミリ を制御するために使用するインタフェース。SMI-S P6000 EVA アレイ プロバイダーは HP ストレージマネジメントアプライアンスシステム上で個別のサービスとして動作し、受信した要求と HP Command View EVA 間のゲートウェイとして機能します。Data Protector HP P6000 EVA ディスクアレイファミリ 統合を使用すると、SMI-S P6000 EVA アレイ プロバイダーは HP P6000 / HP 3PAR SMI-S Agent からの標準化された要求を受け入れ、HP Command View EVA と通信して情報の取得またはメソッドの起動を行って、標準化された応答を返します。
HP P6000 / HP 3PAR SMI-S Agent および HP Command View (CV) EVA も参照。

I

ICDA
(EMC Symmetrix 固有の用語)EMC の Symmetrix の統合キャッシュディスクアレイ (ICDA) は、複数の物理ディスク、複数の FWD SCSI チャネル、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
内部データベース (IDB) を参照。

IDB 復旧ファイル
完了した IDB バックアップセッション、バックアップメディア、そのバックアップメディアで使用するバックアップデバイスに関する情報を保存するファイル。使用可能な場合、このファイルにより、Cell Manager の障害が発生した場合の内部データベースのオフラインリカバリが大幅に簡素化され、処理時間も短縮されます。ファイル名は `obdrindex.dat` です。.

Inet
Data Protector セル内の各 UNIX システムまたは Windows システム上で動作するプロセス。このプロセスは、セル内のシステム間の通信と、バックアップおよび復元に必要なその他のプロセスの起動を受け持ちます。システムに Data Protector をインストールすると、Inet サービスが即座に起動されます。Inet プロセスは、inetd デーモンにより開始されます。

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

Informix Server 用の CMD スクリプト
(Informix Server 固有の用語) Informix Server データベースの構成時に INFORMIXDIR 内に作成される Windows CMD スクリプト。環境変数を Informix Server にエクスポートするコマンド一式が含まれています。

ISQL
(Sybase 固有の用語) Sybase のユーティリティの 1 つ。Sybase SQL Server に対してシステム管理作業を実行できます。

K

keychain パスフレーズを手動で入力しなくても秘密キーを復号化できるようにするツールです。セキュアシェルを使用してリモートインストールを実行する場合、このツールをインストールサーバーにインストールして構成する必要があります。

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

L

LBO **(EMC Symmetrix 固有の用語)**Logical Backup Object(論理バックアップオブジェクト) の略。LBO は、EMC Symmetrix/Fastrax 環境内で保存/取得されるデータオブジェクトです。LBO は EMC Symmetrix によって 1 つのエンティティとして保存/取得され、部分的には復元できません。

LDEV **(HP P9000 XP ディスクアレイファミリ 固有の用語)** HP P9000 XP ディスクアレイファミリ のディスクアレイの物理ディスクの論理パーティション。LDEV は、このようなディスクアレイのスプリットミラー機能やスナップショット機能を使用して複製可能なエンティティです。HP Business Copy (BC) P9000 XP、HP Continuous Access (CA) P9000 XP、および複製 も参照。

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

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` 構成パラメーターは、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` 構成パラメーターを*`INFORMIXDIR`*`/etc/no_log.sh` に設定してください。

Lotus C API **(Lotus Domino Server 固有の用語)**Lotus Domino Server と Data Protector などのバックアップソリューションの間でバックアップ情報および復元情報を交換するためのインタフェース。

LVM LVM (Logical Volume Manager: 論理ボリュームマネージャー) は、HP-UX システム上で物理ディスクスペースを構造化し、論理ボリュームにマッピングするためのサブシステムです。LVM システムは、複数のボリュームグループで構成されます。各ボリュームグループには、複数のボリュームが含まれます。

M

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

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

Manager-of-Managers (MoM) MoM を参照。

MAPI **(Microsoft Exchange Server 固有の用語)**MAPI (Messaging Application Programming Interface) は、アプリケーションおよびメッセージングクライアントがメッセージングシステムおよび情報システムと対話するためのプログラミングインタフェースです。

MCU メインコントロールユニット (MCU) を参照。

Media Agent デバイスに対する読み込み/書き込みを制御するプロセス。制御対象のデバイスはテープなどのメディアに対して読み込み/書き込みを行います。復元またはオブジェクト検証セッション

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

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

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

Microsoft ボリュームシャドウコピーサービス (VSS) VSS 対応アプリケーションのバックアップと復元をそのアプリケーションの機能に関係なく統合管理する統一通信インタフェースを提供するソフトウェアサービスです。このサービスは、バックアップアプリケーション、ライター、シャドウコピープロバイダー、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ー、複製およびライター 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 およびカタログデータベース (CDB) も参照。

MoM 複数のセルをグループ化して、1 つのセルから集中管理することができます。集中管理用セルの管理システムが、MoM(Manager-of-Managers) です。他のセルは MoM クライアントと呼ばれます。MoM を介して、複数のセルを一元的に構成および管理することができます。

MSM Data Protector メディアセッションマネージャー (Media Session Manager) の略。MSM は、Cell Manager 上で稼動し、メディアセッション (メディアのコピーなど) を制御します。

○

OBDR 対応デバイス ブート可能ディスクを装填した CD-ROM ドライブをエミュレートできるデバイス。バックアップデバイスとしてだけでなく、ディザスタリカバリ用のブートデバイスとしても使用可能です。

obdrindex.dat IDB 復旧ファイル を参照。

ON-Bar **(Informix Server 固有の用語)**Informix Server のためのバックアップと復元のシステム。ON-Bar により、Informix Server データのコピーを作成し、後でそのデータを復元することが可能になります。ON-Bar のバックアップと復元のシステムには、以下のコンポーネントが含まれます。

- `onbar` コマンド
- バックアップソリューションとしての Data Protector
- XBSA インタフェース
- ON-Bar カタログテーブル。これは、dbobject をバックアップし、複数のバックアップを通して dbobject のインスタンスをトラッキングするために使われます。

ONCONFIG **(Informix Server 固有の用語)** アクティブな ONCONFIG 構成ファイルの名前を指定する環境変数。ONCONFIG 環境変数が存在しない場合、Informix Server によって、*`INFORMIXDIR`*`\etc`(Windows システムの場合)、または*`INFORMIXDIR`*`/etc/`(UNIX システムの場合) ディレクトリの `onconfig` ファイルにある構成値が使われます。

Oracle Data Guard **(Oracle 固有の用語)**Oracle Data Guard は Oracle の主要なディザスタリカバリソリューションです。プロダクション (一次) データベースのリアルタイムコピーであるスタンバイデータベースを最大 9 個まで保持することにより、破損、データ障害、人為ミス、および災害からの保護を提供します。プロダクション (一次) データベースに障害が発生すると、フェイルオーバーによりスタンバイデータベースの 1 つを新しい一次データベースにすることができます。また、プロダクション処理を現在の一次データベースからスタンバイデータベースに迅速に切り替えたり、元に戻したりできるため、保守作業のための計画ダウンタイムを縮小することができます。

Oracle 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 つのコンピューターシステム上で、複数のデータベースインスタンスを同時に稼動させることができます。

Oracle ターゲットデータベースへのログイン情報

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

- この場合、*user_name* は、Oracle Server およびその他のユーザーに対して公開されるユーザー名です。各ユーザー名はパスワードと関連付けられており、Oracle ターゲットデータベースに接続するにはユーザー名とパスワードの両方を入力する必要があります。ここでは、Oracle の SYSDBA 権限または SYSOPER 権限が付与されているユーザーを指定する必要があります。
- *password* には、Oracle パスワードファイル (orapwd) 内に指定したのと同じパスワードを指定しなければなりません。パスワードは、データベースを管理するユーザーの認証に使用されます。
- *service* には、ターゲットデータベースのための SQL*Net サーバープロセスの識別に使用される名前を指定します。

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 リスナーの定義に含まれています。

P

P1S ファイル P1S ファイルには、システムにインストールされているすべてのディスクを拡張自動ディザスタリカバリ (EADR) 中にどのようにフォーマットするかに関する情報が格納されます。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 の *Data_Protector_program_data*\Config\Server\dr\p1s ディレクトリ (Windows システム)、または/etc/opt/omni/server/dr/p1s ディレクトリ (UNIX システム) にファイル名 recovery.p1s で保存されます 。.

R

RAID Redundant Array of Independent Disks の略。

RAID Manager P9000 XP **(HP P9000 XP ディスクアレイファミリ 固有の用語)** HP P9000 XP ディスクアレイファミリ のディスクアレイに対するコマンドラインインタフェースを提供するソフトウェアアプリケーション。P9000 XP アレイ ストレージシステムのステータスのレポートと制御を行い、ディスクアレイに対する各種操作を実行するための広範なコマンドセットが用意されています。

RAID Manager ライブラリ **(HP P9000 XP ディスクアレイファミリ 固有の用語)**P9000 XP アレイ ストレージシステムの構成、ステータス、およびパフォーマンス測定のデータへのアクセスと、ディスクアレイの操作の開始に使用されるソフトウェアライブラリ。このライブラリにより、関数呼び出しが一連の低レベルの SCSI コマンドに変換されます。
HP P9000 XP Agent も参照。

raw ディスクバックアップ ディスクイメージバックアップ を参照。

RCU Remote Control Unit(RCU) を参照。

RCU Remote Control Unit (RCU) **(HP P9000 XP ディスクアレイファミリ 固有の用語)** HP CA P9000 XP または HP CA+BC P9000 XP 構成におけるメインコントロールユニット (MCU) に対するスレーブデバイスとして機能

する HP P9000 XP ディスクアレイファミリ ユニット。双方向の構成の中では、RCU は MCU としての役割も果たします。

RDBMS Relational Database Management System (リレーショナルデータベース管理システム) の略。

RDF1/RDF2 **(EMC Symmetrix 固有の用語)**SRDF デバイスグループの一種。RDF グループには RDF デバイスだけを割り当てることができます。RDF1 グループタイプにはソースデバイス (R1) が格納され、RDF2 グループタイプにはターゲットデバイス (R2) が格納されます。

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

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

REDO ログ **(Oracle 固有の用語)** 各 Oracle データベースには、複数の REDO ログファイルがあります。データベース用の REDO ログファイルのセットをデータベースの REDO ログと呼びます。Oracle では、REDO ログを使ってデータに対するすべての変更を記録します。

RMAN(Oracle 固有の用語) Recovery Manager を参照。

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

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

S

SAPDBA **(SAP R/3 固有の用語)** BRBACKUP ツール、BRARCHIVE ツール、BRRESTORE ツールを統合した SAP R/3 ユーザーインタフェース。

SMB スプリットミラーバックアップ を参照。

SMBF セッションメッセージバイナリファイル (SMBF) は、IDB のうち、バックアップ、復元、オブジェクトコピー、オブジェクト集約、オブジェクト検証、およびメディア管理のセッション中に生成されたセッションメッセージが格納される部分です。1 つのセッションにつき 1 つのバイナリファイルが作成されます。ファイルは年毎や月毎に分類されます。

SMI-S Agent (SMISA) HP P6000 / HP 3PAR SMI-S Agent を参照。

sqlhosts ファイルまたはレジストリ **(Informix Server 固有の用語)**Informix Server の接続情報ファイル (UNIX システムの場合) またはレジストリ (Windows システムの場合)。各データベースサーバーの名前の他、ホストコンピューター上のクライアントが接続できるエイリアスが格納されます。

SRD ファイル **(ディザスタリカバリ固有の用語)** Unicode (UTF-16) 形式のテキストファイルで、Windows システムの CONFIGURATION バックアップ中に生成され Cell Manager に格納されます。このファイルには、障害発生時にターゲットシステムにオペレーティングシステムをインストールおよび構成するために必要なシステム情報が含まれています。
ターゲットシステム も参照。

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ー環境内だけではなく、互いに遠距離にある環境も対象となります。

SSE Agent(SSEA) HP P9000 XP Agent を参照。

sst.conf ファイル `/usr/kernel/drv/sst.conf` ファイルは、マルチドライブライブラリデバイスが接続されている Data Protector Solaris クライアントのそれぞれにインストールされていなければなら

ないファイルです。このファイルには、クライアントに接続されている各ライブラリデバイスのロボット機構の SCSI アドレスエントリが記述されていなければなりません。

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

StorageTek ACS ライブラリ **(StorageTek 固有の用語)**ACS (Automated Cartridge System) は、1 つのライブラリ管理ユニット (LMU) と、このユニットに接続された 1～24 個のライブラリ記憶域モジュール (LSM) からなるライブラリシステム (サイロ) です。

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

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

SYMA EMC Symmetrix Agent を参照。

System Backup to Tape **(Oracle 固有の用語)**Oracle がバックアップ要求または復元要求を発行したときに正しいバックアップデバイスをロード、ラベリング、およびアンロードするために必要なアクションを処理する Oracle インタフェース。

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

T

TimeFinder **(EMC Symmetrix 固有の用語)** 単一または複数の EMC Symmetrix 論理デバイス (SLD) のインスタントコピーを作成する Business Continuation プロセス。インスタントコピーは、BCV と呼ばれる専用の事前構成 SLD 上に作成され、システムに対する別個のプロセスを経由してアクセスできます。

TLU Tape Library Unit (テープライブラリユニット) の略。

TNSNAMES.ORA **(Oracle および SAP R/3 固有の用語)** サービス名にマッピングされた接続記述子を格納するネットワーク構成ファイル。このファイルは、1 か所で集中的に管理してすべてのクライアントで使用することも、また、ローカルに管理して各クライアントで個別に使用することもできます。

U

user_restrictions ファイル 割り当てられているユーザー権限に応じて Data Protector のユーザーグループが使用できる特定のユーザーアクションを、Data Protector セルの特定のシステムでのみ実行されるように制限するファイル。このような制限は、**Admin** および **Operator** 以外の Data Protector のユーザーグループにのみ適用されます。

V

VMware 管理クライアント **(VMware(レガシー) 用統合ソフトウェア固有の用語)**Data Protector で、VMware 仮想インフラストラクチャーとの通信に使用されるクライアント。VirtualCenter Server システム (VirtualCenter 環境)、または ESX Server システム (スタンドアロン ESX Server 環境) のどちらかです。

VOLSER **(ADIC および STK 固有の用語)** ボリュームシリアル (VOLume SERial) 番号は、メディア上のラベルで、大容量ライブラリ内の物理テープの識別に使用されます。VOLSER は、ADIC/GRAU デバイスおよび StorageTek デバイス固有の命名規則です。

VSS Microsoft ボリュームシャドウコピーサービス (VSS) を参照。

VSS 準拠モード **(HP P9000 XP ディスクアレイファミリ VSS プロバイダー固有の用語)** 2 種類ある P9000 XP アレイ VSS ハードウェアプロバイダーの操作モードの 1 つ。P9000 XP アレイ プロバイダーが VSS 準拠モードであると、ソースボリューム (P-VOL) とその複製 (S-VOL) は、バックアップ後、単純非対状態になります。したがって、ローテーションされる複製数 (P-VOL 当たりの

S-VOL 数) に制限はありません。このような構成でのバックアップからの復元は、ディスクの切り替えによってのみ可能となります。
再同期モード、ソースボリューム、プライマリボリューム (P-VOL)、複製、セカンダリボリューム (S-VOL)、および複製セットローテーション も参照。

VxFS Veritas Journal Filesystem の略。

VxVM (Veritas Volume Manager) Veritas Volume Manager は、Solaris プラットフォーム上でディスクスペースを管理するためのシステムです。VxVM システムは、論理ディスクグループに編成された 1 つまたは複数の物理ボリュームの任意のグループからなります。

W

Wake ONLAN 節電モードで動作しているシステムを同じ LAN 上の他のシステムからのリモート操作により電源投入するためのサポート。

Web レポート Data Protector の機能の 1 つ。バックアップステータス、オブジェクトコピーステータスおよびオブジェクト集約ステータスと Data Protector 構成に関するレポートを Web インタフェース経由で表示できます。

Windows 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。

Windows 構成のバックアップ Data Protector では、Windows CONFIGURATION(構成データ) をバックアップできます。Windows レジストリ、ユーザープロファイル、イベントログ、WINS サーバーデータおよび DHCP サーバーデータ (システム上で構成されている場合) を 1 回の操作でバックアップできます。

WINS サーバー Windows ネットワークのコンピューター名を IP アドレスに解決する Windows インターネットネームサービスソフトウェアを実行しているシステム。Data Protector では、WINS サーバーデータを Windows の構成データの一部としてバックアップできます。

X

XBSA インタフェース **(Informix Server 固有の用語)**ON-Bar と Data Protector の間の相互通信には、X/Open Backup Services Application Programmer's Interface (XBSA) が使用されます。

Z

ZDB ゼロダウンタイムバックアップ (ZDB) を参照。

ZDB データベース **(ZDB 固有の用語)** ソースボリューム、複製、セキュリティ情報などの ZDB 関連情報を格納する IDB の一部。ZDB データベースは、ゼロダウンタイムバックアップ、インスタントリカバリ、スプリットミラー復元の各セッションで使用されます。
ゼロダウンタイムバックアップ (ZDB) も参照。

あ

アーカイブ REDO ログ **(Oracle 固有の用語)** オフライン REDO ログとも呼びます。Oracle データベースが ARCHIVELOG モードで動作している場合、各オンライン REDO ログが最大サイズまで書き込まれると、アーカイブ先にコピーされます。このコピーをアーカイブ REDO ログと呼びます。各データベースに対してアーカイブ REDO ログを作成するかどうかを指定するには、以下の 2 つのモードのいずれかを指定します。

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

オンライン REDO ログ も参照。

アーカイブロギング **(Lotus Domino Server 固有の用語)**Lotus Domino Server のデータベースモードの 1 つ。トランザクションログファイルがバックアップされて初めて上書きされるモードです。

アーカイブログファイル
(Data Protector 固有の用語) Data Protector の内部データベース (IDB) への変更を記録するファイル。アーカイブログファイルは、オンラインおよびオフラインの IDB の復元と復旧を行うために使用します。IDB の復元と復旧では、最新の状態、または最後の IDB バックアップセッション以降に、あるいは連続する 2 つの IDB バックアップセッション間の特定の状態のいずれかで、IDB を再作成する必要があります。

アクセス権限
ユーザー権限 を参照。

アプリケーションシステム
(ZDB 固有の用語) このシステム上でアプリケーションやデータベースが実行されます。アプリケーションまたはデータベースデータは、ソースボリューム上に格納されています。
バックアップシステムおよびソースボリューム も参照。

暗号化 KeyID-StoreID
Data Protector Key Management Server が、Data Protector で使用される暗号化キーの識別と管理に使用する複合識別子です。`KeyID` は、キーストア内のキーを識別します。`StoreID` は、Cell Manager 上のキーストアを識別します。Data Protector を暗号化機能付きの旧バージョンからアップグレードした場合、同じ Cell Manager 上で使用される `StoreID` が複数存在する可能性があります。

暗号化キー
256 ビットのランダムに生成された数値で、AES 256 ビットソフトウェア暗号化またはドライブベースの暗号化が指定されたバックアップの際に、Data Protector の暗号化アルゴリズムが情報を暗号化するために使用します。これに続く情報の復号化では、同じキーが使用されます。Data Protector セルの暗号化キーは、Cell Manager 上の中央キーストアに保存されます。

暗号制御通信
Data Protector セル内のクライアント間における Data Protector のセキュアな通信は、Secure Socket Layer (SSL) をベースにしており、SSLv3 アルゴリズムを使用して制御通信が暗号化されます。Data Protector セル内の制御通信は、Disk Agent(および統合用ソフトウェア) から Media Agent へのデータ転送とその逆方向のデータ転送を除く、Data Protector プロセス間のすべての通信です。

い

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

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

インストールサーバー
特定のアーキテクチャー用の Data Protector インストールパッケージのレポジトリを保持するコンピューターシステム。インストールサーバーから Data Protector クライアントのリモートインストールが行われます。混在環境では、少なくとも 2 台のインストールサーバーが必要です。1 台は UNIX システム用で、1 台は Windows システム用です。

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

インフォメーションストア
(Microsoft Exchange Server 固有の用語) ストレージ管理を行う Microsoft Exchange Server のサービス。Microsoft Exchange Server のインフォメーションストアは、メールボックスストアとパブリックフォルダーストアという 2 種類のストアを管理します。メールボックスストアは、個々のユーザーに属するメールボックスから成ります。パブリックフォルダーストアには、複数のユーザーで共有するパブリックフォルダーおよびメッセージがあります。
キーマネージメントサービスおよびサイト複製サービス も参照。

う

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

え

エクスチェンジャー
SCSI エクスチェンジャーとも呼ばれます。
ライブラリ も参照。

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

お

オートチェンジャー
ライブラリ を参照。

オートローダ
ライブラリ を参照。

オブジェクト
バックアップオブジェクト を参照。

オブジェクト ID
(Windows 固有の用語) オブジェクト ID(OID) を使用すると、システムのどこにファイルがあるかにかかわらず、NTFS 5 ファイルにアクセスできます。Data Protector では、ファイルの代替ストリームとして OID を扱います。

オブジェクトコピー
特定のオブジェクトバージョンのコピー。オブジェクトコピーセッション中またはオブジェクトミラーのバックアップセッション中に作成されます。

オブジェクトコピーセッション
異なるメディアセット上にバックアップデータの追加コピーを作成するプロセス。オブジェクトコピーセッション中に、選択されたバックアップオブジェクトがソースからターゲットメディアへコピーされます。

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

オブジェクトのミラーリング
バックアップセッション中に、いくつかのメディアセットに同じデータを書き込むプロセス。Data Protector を使用すると、1 つまたは複数のメディアセットに対し、すべてまたは一部のバックアップオブジェクトをミラーリングすることができます。

オブジェクトミラー
オブジェクトのミラーリングを使用して作成されるバックアップオブジェクトのコピー。オブジェクトのミラーは、通常、オブジェクトコピーと呼ばれます。

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

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

オブジェクト集約
1 つのフルバックアップと 1 つ以上の増分バックアップで構成されたバックアップオブジェクトの復元チェーンを、新たな集約されたバージョンのオブジェクトとしてマージするプロセス。このプロセスは、合成バックアップの一部です。このプロセスの結果、指定のバックアップオブジェクトの合成フルバックアップが出力されます。

オブジェクト集約セッション
1 つのフルバックアップと 1 つ以上の増分バックアップで構成されたバックアップオブジェクトの復元チェーンを、新たな統合されたバージョンのオブジェクトとしてマージするプロセス。

オフライン REDO ログ
アーカイブ REDO ログ を参照。

オフラインバックアップ 実行中はアプリケーションデータベースがアプリケーションから使用できなくなるバックアップ。オフラインバックアップセッションでは、一般にデータベースはデータ複製プロセス中に休止状態となり、バックアップシステムからは使用できますが、アプリケーションシステムからは使用できません。たとえばテープへのバックアップの場合、テープへのデータストリーミングが終わるまでの間となります。残りのバックアッププロセスでは、データベースは通常の稼動を再開できます。
ゼロダウンタイムバックアップ (ZDB) およびオンラインバックアップ も参照。

オフライン復旧 オフライン復旧は、ネットワーク障害などにより Cell Manager にアクセスできない場合に行われます。オフライン復旧では、スタンドアロンデバイスおよび SCSI ライブラリデバイスのみが使用可能です。Cell Manager はオフラインでのみ復旧できます。

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

オンライン REDO ログ **(Oracle 固有の用語)** まだアーカイブされていないが、インスタンスでデータベースアクティビティを記録するために利用できるか、または満杯になっており、アーカイブまたは再使用されるまで待機している REDO ログ。
アーカイブ REDO ログ も参照。

オンラインバックアップ データベースアプリケーションを利用可能な状態に維持したまま行われるバックアップ。データベースは、データ複製プロセスの間、特別なバックアップモードで稼動します。たとえばテープへのバックアップの場合、テープへのデータストリーミングが終わるまでの間となります。この期間中、データベースは完全に機能しますが、パフォーマンスに多少影響が出たり、ログファイルのサイズが急速に増大したりする場合もあります。残りのバックアッププロセスでは、データベースは通常の稼動を再開できます。

場合によっては、データベースを整合性を保って復元するために、トランザクションログもバックアップする必要があります。

ゼロダウンタイムバックアップ (ZDB) およびオフラインバックアップ も参照。

オンライン復旧 Cell Manager がアクセス可能な場合に使用できる内部データベースのリカバリの種類です。この場合、Cell Manager がセッションを実行し、そのセッションが IDB に記録され、そのセッションの進行状況を GUI を使用して監視できます。

か

カタログデータベース (CDB) Data Protector 内部データベース (IDB) の一部で、バックアップ、復元、オブジェクトコピー、オブジェクト集約、オブジェクト検証、メディア管理の各セッションに関する情報が格納されます。IDB のこの部分は、常にセルに対してローカルとなります。これは埋込み型データベースに格納されます。
MMDB も参照。

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属性など) を IDB に維持する期間を定義します。
データ保護 も参照。

仮想コントローラーソフトウェア (VCS) **(HP P6000 EVA ディスクアレイファミリ 固有の用語)**HSV コントローラーを介した HP Command View EVA との通信など、記憶システムの処理すべてを管理するファームウェア。
HP Command View (CV) EVA も参照。

仮想サーバー ネットワーク IP 名および IP アドレスでドメイン内に定義されるクラスター環境の仮想マシンです。アドレスはクラスターソフトウェアによりキャッシュされ、仮想サーバーリソースを現在実行しているクラスターノードにマップされます。こうして、特定の仮想サーバーに対するすべての要求が特定のクラスターノードにキャッシュされます。

仮想ディスク **(HP P6000 EVA ディスクアレイファミリ 固有の用語)** HP P6000 EVA ディスクアレイファミリ のディスクアレイのストレージプールから割り当てられるストレージユニット。仮想ディスクは、このようなディスクアレイのスナップショット機能を使用して複製可能なエンティティです。
ソースボリュームおよびターゲットボリューム も参照。

仮想テープ **(VLS 固有の用語)** テープに保存された場合と同様にディスクドライブにデータをバックアップするアーカイブ式ストレージテクノロジ。バックアップスピードおよびリカバリスピードの向上、運用コストの削減など仮想テープシステムとしての利点がある。
仮想ライブラリシステム (VLS) および仮想テープライブラリ (VTL) も参照。

仮想テープライブラリ (VTL) **(VLS 固有の用語)** 従来のテープベースのストレージ機能を提供する、エミュレートされるテープライブラリ。
仮想ライブラリシステム (VLS) も参照。

仮想デバイスインタフェース **(Microsoft SQL Server 固有の用語)**Microsoft SQL Server のプログラミングインタフェースの 1 つ。大容量のデータベースを高速でバックアップおよび復元できます。

仮想フルバックアップ コピーするのではなくポインターを使用してデータが統合される、効率の良い合成バックアップ。配布ファイルメディア形式を使用する 1 つのファイルライブラリにすべてのバックアップ (フルバックアップ、増分バックアップ、およびその結果である仮想フルバックアップ) が書き込まれる場合に実行されます。

仮想ライブラリシステム (VLS) 1 つまたは複数の仮想テープライブラリ (VTL) をホストする、ディスクベースのデータストレージデバイス。

階層ストレージ管理 (HSM) 使用頻度の低いデータを低コストの光磁気プラッタに移動することで、コストの高いハードディスク記憶域を有効利用するための仕組み。移動したデータが必要になった場合は、ハードディスク記憶域に自動的に戻されます。これにより、ハードディスクからの高速読み取りと光磁気プラッタの低コスト性のバランスが維持されます。

拡張可能ストレージエンジン (ESE) **(Microsoft Exchange Server 固有の用語)**Microsoft Exchange Server で情報交換用の記憶システムとして使用されているデータベーステクノロジ。

拡張増分バックアップ 従来の増分バックアップでは、前回のバックアップより後に変更されたファイルがバックアップされますが、変更検出機能に限界があります。これに対し、拡張増分バックアップでは、名前が変更されたファイルや移動されたファイルのほか、属性が変更されたファイルについても、信頼性のある検出とバックアップが行われます。

確認 指定したメディア上の Data Protector データが読み取り可能かどうかをチェックする機能。また、CRC(巡回冗長検査) オプションをオンにして実行したバックアップに対しては、各ブロック内の整合性もチェックできます。

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

監査ログ 監査情報が保存されるデータファイル。

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

き

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

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

共有ディスク あるシステム上に置かれた Windows のディスクをネットワーク上の他のシステムのユーザーが使用できるように構成したもの。共有ディスクを使用しているシステムは、Data Protector Disk Agent がインストールされていなくてもバックアップ可能です。

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

く

クライアントバックアップ Data Protector クライアントにマウントされているすべてのボリューム (ファイルシステム) のバックアップ。実際に何がバックアップされるかは、バックアップ仕様でどのようにオブジェクトを選択するかによって異なります。

- クライアントシステム名の隣のチェックボックスを選択した場合、[クライアントシステム] の種類の 1 つのバックアップオブジェクトが作成されます。その結果、バックアップ時に Data Protector は選択されたクライアントにマウントされているすべてのボ

リュームを最初に検出してから、それらをバックアップします。Windows クライアントの場合、CONFIGURATION もバックアップされます。

- クライアントシステムにマウントされているすべてのボリュームを別々に選択する場合、Filesystem タイプの個別バックアップオブジェクトがボリュームごとに作成されます。その結果、バックアップ時に、選択されたボリュームのみがバックアップされます。バックアップ仕様の作成後にクライアントにマウントされたボリュームは、バックアップされません。

クライアントまたはクライアントシステム

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

クラスター対応アプリケーション

クラスターアプリケーションプログラミングインタフェースをサポートしているアプリケーション。クラスター対応アプリケーションごとに、クリティカルリソースが宣言されます。これらのリソースには、ディスクボリューム (Microsoft Cluster Server の場合)、ボリュームグループ (MC/ServiceGuard の場合)、アプリケーションサービス、IP 名および IP アドレスなどがあります。

クラスター連続レプリケーション

(Microsoft Exchange Server 固有の用語) クラスター連続レプリケーション (CCR) はクラスター管理とフェイルオーバーオプションを使用して、ストレージグループの完全なコピー (CCR コピー) を作成および維持する高可用性ソリューションです。ストレージグループは個別のサーバーに複製されます。CCR は Exchange バックエンドサーバーで発生した単発箇所の障害を取り除きます。CCR コピーが存在するパッシブ Exchange Server ノードで VSS を使用してバックアップを実行すれば、アクティブノードの負荷が軽減されます。

CCR コピーへの切り替えは数秒で完了するため、CCR コピーはディザスタリカバリに使用されます。複製されたストレージグループは、Exchange ライターの新しいインスタンス (Exchange Replication Service) として表示され、元のストレージグループと同様に VSS を使用してバックアップできます。

Exchange Replication Service およびローカル連続レプリケーション も参照。

グループ

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

グローバルオプション

Data Protector セル全体の動作を定義するオプションのセット。これらのオプションは、Cell Manager 上のテキスト形式のファイルに保存されます。

こ

コピーセット

(HP P6000 EVA ディスクアレイファミリ 固有の用語) ローカル P6000 EVA 上にあるソースボリュームとリモート P6000 EVA 上にあるその複製とのペア。
ソースボリューム、複製、および HP Continuous Access + Business Copy(CA+BC)P6000 EVA も参照。

コマンドデバイス

(HP P9000 XP ディスクアレイファミリ 固有の用語) ディスクアレイ内の専用のボリュームで、管理アプリケーションとディスクアレイのストレージシステムとの間のインタフェースとして機能します。データストレージ用に使用することはできません。操作に対する要求のみを受け付け、ディスクアレイによってその操作が実行されます。

コマンドラインインタフェース (CLI)

CLI には、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。これらを通じて、Data Protector の構成、管理、バックアップ/復元タスクを実行することができます。

コンテナー

(HP P6000 EVA ディスクアレイファミリ 固有の用語) ディスクアレイ上のスペース。後で標準スナップショット、vsnap、またはスナップクローンとして使用するために事前に割り当てられます。

合成バックアップ

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

合成フルバックアップ

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

さ

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

差分バックアップ 前回のフルバックアップより後の変更をバックアップする増分バックアップ。このバックアップを実行するには、増分 1 バックアップを指定します。
増分バックアップ も参照。

差分バックアップ **(Microsoft SQL Server 固有の用語)** 前回のフルデータベースバックアップ以降にデータベースに対して加えられた変更だけを記録するデータベースバックアップ。
バックアップの種類 も参照。

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

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

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ー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ーを検索します。

再同期モード **(HP P9000 XP ディスクアレイファミリ VSS プロバイダー固有の用語)** 2 種類ある P9000 XP アレイ VSS ハードウェアプロバイダーの操作モードの 1 つ。P9000 XP アレイ プロバイダーが再同期モードであると、ソースボリューム (P-VOL) とその複製 (S-VOL) は、バックアップ後、中断ミラー関係になります。MU 範囲が 0-2(つまり、0、1、2) の場合、ローテーションされる最大複製数 (P-VOL 当たりの S-VOL 数) は 3 となります。このような構成でのバックアップからの復元は、S-VOL をその P-VOL と再同期することによってのみ可能となります。
VSS 準拠モード、ソースボリューム、プライマリボリューム (P-VOL)、複製、セカンダリボリューム (S-VOL)、ミラーユニット (MU) 番号、および複製セットローテーション も参照。

し

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

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

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

ム/ディスク/パーティションをシステムボリューム/システムディスク/システムパーティションと呼んでいます。

システム状態 **(Windows 固有の用語)** システム状態データには、レジストリ、COM+ クラス登録データベース、システム起動ファイル、および証明書サービスデータベース (Certificate Server の場合) が含まれます。サーバーがドメインコントローラーの場合は、Active Directory サービスと SYSVOL ディレクトリもシステム状態データに含まれます。サーバーがクラスターサービスを実行している場合、システム状態データにはリソースレジストリチェックポイントとクォーラムリソースリカバリログが含まれ、最新のクラスターデータ情報が格納されます。

システム復旧データファイル SRD ファイル を参照。

シャドウコピー **(Microsoft VSS 固有の用語)** 特定の時点におけるオリジナルボリューム (元のボリューム) の複製を表すボリューム。オリジナルボリュームからではなく、シャドウコピーからデータがバックアップされます。オリジナルボリュームはバックアップ処理中も更新が可能ですが、ボリュームのシャドウコピーは同じ内容に維持されます。
Microsoft ボリュームシャドウコピーサービスおよび複製 も参照。

シャドウコピーセット **(Microsoft VSS 固有の用語)** 同じ時点で作成されたシャドウコピーのコレクション。
シャドウコピーおよび複製セット も参照。

シャドウコピープロバイダー **(Microsoft VSS 固有の用語)** ボリュームシャドウコピーの作成と表現を行うエンティティ。プロバイダーは、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。プロバイダーは、ソフトウェア (システムプロバイダーなど) で実装することも、ハードウェア (ローカルディスクやディスクアレイ) で実装することもできます。
シャドウコピー も参照。

ジュークボックス ライブラリ を参照。

ジュークボックスデバイス 光磁気メディアまたはファイルメディアを格納するために使用する、複数のスロットからなるデバイス。ファイルメディアの格納に使用する場合、ジュークボックスデバイスは「ファイルジュークボックスデバイス」と呼ばれます。

事前割り当てリスト メディアプール内のメディアのサブセットをバックアップに使用する順に指定したリスト。

自動ストレージ管理 (ASM) **(Oracle 固有の用語)** Oracle に統合されるファイルシステムおよびボリュームマネージャーで、Oracle データベースファイルを管理します。データやディスクの管理が簡単になり、ストライピング機能やミラーリング機能によってパフォーマンスが最適化されます。

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 システム上では実行可能ファイルやバッチファイル、UNIX システム上ではシェルスクリプトとして記述できます。
実行前 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 システム上では実行可能ファイルやバッチファイル、UNIX システム上ではシェルスクリプトとして記述できます。
実行後 も参照。

実行前コマンドと実行後コマンド 実行前コマンドおよび実行後コマンドは、バックアップセッションまたは復元セッションの前後に付加的な処理を実行する実行可能ファイルまたはスクリプトです。実行前コマンドおよび実行後コマンドは、Data Protector で事前に用意されているものではありません。ユーザーは、コマンドを独自に作成する必要があります。Windows システム上では実行可能ファイルやバッチファイル、UNIX システム上ではシェルスクリプトとして記述できます。

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

循環ログ **(Microsoft Exchange Server および Lotus Domino Server 固有の用語)** 循環ログは、Microsoft Exchange Server データベースおよび Lotus Domino Server データベースモードの 1 つ。この

モードでは、トランザクションログファイルのコンテンツは、対応するデータがデータベースにコミットされると、定期的に上書きされます。循環ログにより、ディスク記憶領域の要件が軽減されます。

初期化
フォーマット を参照。

所有権
バックアップ所有権は、データを参照および復元するユーザーの能力に影響します。各バックアップセッションとその中でバックアップされたすべてのデータはオーナーに割り当てられます。所有者は、対話型バックアップを開始するユーザー、CRS プロセスを実行するときに使用するアカウント、またはバックアップ仕様オプションで所有者として指定されたユーザーです。

ユーザーが既存のバックアップ仕様を修正せずにそのまま起動した場合、そのバックアップセッションは対話型とみなされません。

ユーザーがバックアップ仕様を修正して起動すると、以下の条件が成立しない限り、そのユーザーがオーナーになります。

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

UNIXCell Manager 上でスケジュールしたバックアップの場合、上記の条件が成立しない限り、root: sys がセッションオーナーになります。

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

バックアップオブジェクトをコピーまたは集約すると、コピーまたは集約したオブジェクトのオーナーは、元のバックアップセッションを開始したユーザーになります。

詳細カタログバイナリファイル (DCBF)
バックアップされた項目の名前、バージョン、メタデータを格納する Data Protector の内部データベースの一部です。これは、DC バイナリファイルを格納した DC ディレクトリで構成されます。
DC ディレクトリおよび内部データベース (IDB) も参照。

す

スイッチオーバー
フェイルオーバー を参照。

スキャン
デバイス内のメディアを識別する機能。これにより、MMDB を、選択した位置 (たとえば、ライブラリ内のスロット) に実際に存在するメディアと同期させることができます。デバイスに含まれる実際のメディアをスキャンしてチェックすると、第三者が Data Protector を使用せずにメディアを操作 (挿入または取り出しなど) していないかどうかなどを確認できます。

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

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

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

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

ストレージボリューム
(ZDB 固有の用語) ボリューム管理システム、ファイルシステム、他のオブジェクトなどが存在可能なオペレーティングシステムや他のエンティティ (たとえば、仮想化機構など) に提示できるオブジェクト。ボリューム管理システム、ファイルシステムはこの記憶域に構築されます。これらは通常、ディスクアレイなどの記憶システム内に作成または存在します。

スナップショット
(HP P4000 SAN ソリューション 、HP P6000 EVA ディスクアレイファミリ 、HP P9000 XP ディスクアレイファミリ 、および HP 3PAR StoreServ Storage 固有の用語) 特定の複製方法で作成されたターゲットボリュームの種類の 1 つ。ディスクアレイモデルと選択した複製方法に応じて、特性の異なる、さまざまなスナップショットの種類が使用できます。基本的に、各スナップショットは仮想コピー (ソースボリュームの内容に引き続き依存します)、またはソースボリュームから独立した複製 (クローン) のどちらかです。

複製およびスナップショット作成 も参照。

スナップショットバックアップ テープへの ZDB、ディスクへの ZDB、およびディスク + テープへの ZDB を参照。

スナップショット作成 **(HP P4000 SAN ソリューション 、HP P6000 EVA ディスクアレイファミリ 、HP P9000 XP ディスクアレイファミリ 、および HP 3PAR StoreServ Storage 固有の用語)** 選択したソースボリュームのコピーをストレージ仮想化技術を使用して作成する複製作成プロセス。スナップショットは、ある特定の時点で作成されたとみなされる複製で、作成後すぐに使用できます。ただし、スナップショットの種類によっては、複製作成後にデータコピープロセスがバックグランドで継続して実行されるものもあります。
スナップショット も参照。

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

スプリットミラー **(EMC Symmetrix Disk Array および HP P9000 XP ディスクアレイファミリ 固有の用語)** 特定の複製方法で作成されたターゲットボリュームの種類の 1 つ。スプリットミラー複製により、ソースボリュームの独立した複製 (クローン) が作成されます。
複製およびスプリットミラーの作成 も参照。

スプリットミラーの作成 **(EMC Symmetrix および HP P9000 XP ディスクアレイファミリ 固有の用語)** 事前構成したターゲットボリュームのセット(ミラー)を、ソースボリュームの内容の複製が必要になるまでソースボリュームのセットと同期化し続ける複製技法。その後、同期を停止 (ミラーを分割) すると、分割時点でのソースボリュームのスプリットミラー複製はターゲットボリュームに残ります。
スプリットミラー も参照。

スプリットミラーバックアップ (EMC Symmetrix 固有の用語) テープへの ZDB を参照。

スプリットミラーバックアップ (HP P9000 XP ディスクアレイファミリ 固有の用語) テープへの ZDB、ディスクへの ZDB、およびディスク + テープへの ZDB を参照。

スプリットミラー復元 **(EMC Symmetrix および HP P9000 XP ディスクアレイファミリ 固有の用語)** テープへの ZDB セッションまたはディスク + テープへの ZDB セッションでバックアップされたデータを、最初にバックアップメディアから複製に、その後に複製からソースボリュームにコピーするプロセス。この方法では、完全なセッションを復元することも個々のバックアップオブジェクトを復元することも可能です。
テープへの ZDB、ディスク + テープへの ZDB および複製 も参照。

スレッド **(Microsoft SQL Server 固有の用語)**1 つのプロセスのみに属する実行可能なエンティティ。プログラムカウンター、ユーザーモードスタック、カーネルモードスタック、およびレジスター値のセットからなります。同じプロセス内で複数のスレッドを同時に実行できます。

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

せ

セカンダリボリューム (S-VOL) **(HP P9000 XP ディスクアレイファミリ 固有の用語)** HP P9000 XP ディスクアレイファミリ のディスクアレイの内部ディスク (LDEV) で、もう 1 つの LDEV であるプライマリボリューム (P-VOL) とペアとなっています。プライマリボリューム (P-VOL) セカンダリボリュームは、P-VOL のミラーとして、また P-VOL のスナップショットストレージに使用されるボリュームとして機能することが可能です。S-VOL は P-VOL に使用される SCSI アドレスとは異なるアドレスに割り当てられます。HP CA P9000 XP 構成では、ミラーとして機能する S-VOL を MetroCluster 構成のフェイルオーバーデバイスとして使用することができます。
プライマリボリューム (P-VOL) およびメインコントロールユニット (MCU) も参照。

セッション バックアップセッション、メディア管理セッション、および復元セッション を参照。

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

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

セル 1 台の Cell Manager に管理されているシステムの集合。セルは、通常、同じ LAN または SAN に接続されている、サイト上または組織エンティティ上のシステムを表します。集中管理によるバックアップおよび復元のポリシーやタスクの管理が可能です。

ゼロダウンタイムバックアップ (ZDB) ディスクアレイにより実現したデータ複製技術を用いて、アプリケーションシステムのバックアップ処理の影響を最小限に抑えるバックアップアプローチ。バックアップされるデータの複製がまず作成されます。その後のすべてのバックアップ処理は、元のデータではなく複製データを使って実行し、アプリケーションシステムは通常の処理に復帰します。
ディスクへの ZDB、テープへの ZDB、ディスク + テープへの ZDB、およびインスタントリカバリ も参照。

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

そ

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

ソースボリューム **(ZDB 固有の用語)** 複製されるデータを含むストレージボリューム。

増分 1 メールボックスバックアップ 増分 1 メールボックスバックアップでは、前回のフルバックアップ以降にメールボックスに対して行われた変更をすべてバックアップします。

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

増分バックアップ 前回のバックアップ以降に変更があったファイルだけを選択するバックアップ。増分バックアップには複数のレベルがあり、復元チェーンの長さを細かく制御できます。
バックアップの種類 も参照。

増分バックアップ **(Microsoft Exchange Server 固有の用語)** 前回のフルバックアップまたは増分バックアップ以降の変更だけをバックアップする Microsoft Exchange Server データのバックアップ。増分バックアップでは、バックアップ対象はトランザクションログだけです。
バックアップの種類 も参照。

増分メールボックスバックアップ 増分メールボックスバックアップでは、前回の各種バックアップ以降にメールボックスに対して行われた変更をすべてバックアップします。

た

ターゲットシステム **(ディザスタリカバリ固有の用語)** コンピューターの障害が発生した後のシステム。ターゲットシステムは、ブート不能な状態になっていることが多く、そのような状態のシステムを元のシステム構成に戻すことがディザスタリカバリの目標となります。クラッシュしたシステムがそのままターゲットシステムになるのではなく、正常に機能していないハードウェアをすべて交換することで、クラッシュしたシステムがターゲットシステムになります。

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

ターゲットデバイス (R2) **(EMC Symmetrix 固有の用語)** ターゲットデバイス (R1) との SRDF 操作に参加する EMC Symmetrix デバイス。リモート EMC Symmetrix ユニット内に置かれます。ローカル EMC Symmetrix ユニット内でソースデバイス (R1) とペアになり、ミラー化ペアから、すべての書

き込みデータを受け取ります。このデバイスは、通常の I/O 操作ではユーザーアプリケーションからアクセスされません。R2 デバイスは、RDF2 グループタイプに割り当てる必要があります。
ソースデバイス (R1) も参照。

ターゲットボリューム **(ZDB 固有の用語)** 複製されるデータを含むストレージボリューム。

ターミナルサービス **(Windows 固有の用語)**Windows のターミナルサービスは、サーバー上で実行されている仮想 Windows デスクトップセッションと Windows ベースのプログラムにクライアントからアクセスできるマルチセッション環境を提供します。

ち

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

- disk タイプ
- sbt_tape タイプ

Oracle が Data Protector と統合されており、指定されたチャネルの種類が sbt_tape タイプの場合は、上記のサーバープロセスが Data Protector に対してバックアップの読み取りとデータファイルの書き込みを試行します。

て

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

ディザスタリカバリオペレーティングシステム
DR OS を参照。

ディザスタリカバリの段階 0 ディザスタリカバリの準備 (ディザスタリカバリを成功させるための必須条件)。

ディザスタリカバリの段階 1 DR OS のインストールと構成 (以前の記憶領域構造の構築)。

ディザスタリカバリの段階 2 オペレーティングシステム (環境を定義する各種の構成情報を含む) と Data Protector の復元。

ディザスタリカバリの段階 3 ユーザーデータとアプリケーションデータの復元。

ディスク + テープへの ZDB **(ZDB 固有の用語)** ゼロダウンタイムバックアップの 1 つの形式。ディスクへの ZDB と同様に、作成された複製が特定の時点でのソースボリュームのバックアップとしてディスクアレイに保持されます。ただし、テープへの ZDB と同様、複製データはバックアップメディアにもストリーミングされます。このバックアップ方法を使用した場合、同じセッションでバックアップしたデータは、インスタントリカバリプロセス、Data Protector 標準のテープからの復元を使用して復元できます。特定のディスクアレイファミリではスプリットミラー復元が可能です。
ゼロダウンタイムバックアップ (ZDB)、ディスクへの ZDB、テープへの ZDB、インスタントリカバリ、複製、および複製セットローテーション も参照。

ディスクイメージバックアップ 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 コンピューターシステム上のすべてのユーザーまたはユーザーのサブセットに対してディスクスペースの消費を管理するためのコンセプト。このコンセプトは、いくつかのオペレーティングシステムプラットフォームで採用されています。

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

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

ディスクへの ZDB **(ZDB 固有の用語)** ゼロダウンタイムバックアップの 1 つの形式。作成された複製が、特定の時点でのソースボリュームのバックアップとしてディスクアレイに保持されます。同じバックアップ仕様を使って別の時点で作成された複数の複製を、複製セットに保持することができます。テープに ZDB した複製はインスタントリカバリプロセスで復元できます。
ゼロダウンタイムバックアップ (ZDB)、テープへの ZDB、ディスク + テープへの ZDB、インスタントリカバリ、および複製セットローテーション も参照。

ディレクトリ接合 **(Windows 固有の用語)** ディレクトリ接合は、Windows の再解析ポイントのコンセプトに基づいています。NTFS 5 ディレクトリ接合では、ディレクトリ/ファイル要求を他の場所にリダイレクトできます。

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

データベースの差分バックアップ 前回のフルデータベースバックアップ以降にデータベースに対して加えられた変更だけを記録するデータベースバックアップ。

データベースの並列処理 十分な台数のデバイスが利用可能で、並列バックアップを実行できる場合には、複数のデータベースが同時にバックアップされます。

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

データ複製 (DR) グループ **(HP P6000 EVA ディスクアレイファミリ 固有の用語)**HP P6000 EVA ディスクアレイファミリ仮想ディスクの論理グループ。共通の性質を持ち、同じ HP CA P6000 EVA ログを共有していれば、最大 8 組のコピーセットを含めることができます。
コピーセット も参照。

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

テープなしのバックアップ (ZDB 固有の用語) ディスクへの ZDB を参照。

テープへの ZDB **(ZDB 固有の用語)** ゼロダウンタイムバックアップの 1 つの形式。作成された複製が、バックアップメディア (通常はテープ) にストリーミングされます。このバックアップ形式ではインスタントリカバリはできませんが、バックアップ終了後にディスクアレイ上に複製を保持する必要がありません。バックアップデータは Data Protector 標準のテープからの復元を使用して復元できます。特定のディスクアレイファミリでは、スプリットミラー復元が可能です。
ゼロダウンタイムバックアップ (ZDB)、ディスクへの ZDB、ディスク + テープへの ZDB、インスタントリカバリ、および複製 も参照。

デバイス ドライブまたはより複雑な装置 (ライブラリなど) を格納する物理装置。

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

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

デバイスチェーン デバイスチェーンは、シーケンシャルに使用するように構成された複数のスタンドアロンデバイスからなります。デバイスチェーンに含まれるデバイスのメディアで空き容量がなくなると、自動的に次のデバイスのメディアに切り替えて、バックアップを継続します。

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

と

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

ドライブ コンピューター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、コンピューターシステムに送信することもできます。

ドライブのインデックス ライブラリデバイス内のドライブの機械的な位置を識別するための数字。ロボット機構によるドライブアクセスは、この数に基づいて制御されます。

ドライブベースの暗号化 Data Protector のドライブベースの暗号化では、ドライブの暗号化機能が使用されます。バックアップの実行中、ドライブではメディアに書き込まれるデータとメタデータの両方が暗号化されます。

トランザクション 一連のアクションを単一の作業単位として扱えるようにするためのメカニズム。データベースでは、トランザクションを通じて、データベースの変更を追跡します。

トランザクションバックアップ トランザクションバックアップは、一般に、データベースのバックアップよりも必要とするリソースが少ないため、データベースのバックアップよりもより高い頻度で実行できます。トランザクションバックアップを適用することで、データベースを問題発生以前の特定の時点の状態に復旧することができます。

トランザクションバックアップ **(Sybase および SQL 固有の用語)** トランザクションログをバックアップすること。トランザクションログには、前回のフルバックアップまたはトランザクションバックアップ以降に発生した変更が記録されます。

トランザクションログテーブル **(Sybase 固有の用語)** データベースに対するすべての変更が自動的に記録されるシステムテーブル。

トランザクションログバックアップ トランザクションログバックアップは、一般に、データベースのバックアップよりも必要とするリソースが少ないため、データベースのバックアップよりもより高い頻度で実行できます。トランザクションログバックアップを用いることにより、データベースを特定の時点の状態に復旧できます。

トランザクションログファイル データベースを変更するトランザクションを記録するファイル。データベースが破損した場合にフォールトトレランスを提供します。

トランスポータブルスナップショット **(Microsoft VSS 固有の用語)** アプリケーションシステム上に作成されるシャドウコピー。このシャドウコピーは、バックアップを実行するバックアップシステムに提供できます。
Microsoft ボリュームシャドウコピーサービス (VSS) も参照。

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。

な

内部データベース (IDB) どのデータがどのメディアにバックアップされたか、バックアップや復元などのセッションがいつどのように実行されたか、また、どのデバイス、ライブラリ、ディスクアレイが構成されているかなどに関する情報を格納する Data Protector のエンティティです。IDB は、Cell

Manager 上にある独自のデータファイルの集まりで、埋込み型データベース内にそのデータを格納します。
DC ディレクトリおよび詳細カタログバイナリファイル (DBCF) も参照。

は

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

ハードリカバリ **(Microsoft Exchange Server 固有の用語)** トランザクションログファイルを使用し、データベースエンジンによる復元後に実行される Microsoft Exchange Server のデータベース復旧。

バックアップ API Oracle のバックアップ/復元ユーティリティとバックアップ/復元メディア管理層の間にある Oracle インタフェース。このインタフェースによってルーチンのセットが定義され、バックアップメディアのデータの読み書き、バックアップファイルの作成や検索、削除が行えるようになります。

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

バックアップオーナー IDB の各バックアップオブジェクトにはオーナーが定義されています。デフォルトのオーナーは、バックアップセッションを開始したユーザーです。

バックアップオブジェクト 1 つのディスクボリューム (論理ディスクまたはマウントポイント) からバックアップされた項目すべてを含むバックアップ単位。バックアップ項目は、任意の数のファイル、ディレクトリ、ディスク全体またはマウントポイントの場合が考えられます。また、バックアップオブジェクトはデータベース/アプリケーションエンティティまたはディスクイメージの場合もあります。

バックアップオブジェクトは以下のように定義されます。

- クライアント名: バックアップオブジェクトが保存される Data Protector クライアントのホスト名
- マウントポイント: ファイルシステムオブジェクトを対象とする場合 — バックアップオブジェクトが存在するクライアント (Windows システムではドライブ、UNIX システムではマウントポイント) 上のディレクトリ構造におけるアクセスポイント。統合オブジェクトを対象とする場合 — バックアップストリーム ID。バックアップされたデータベース項目/アプリケーション項目を示します。
- 説明: ファイルシステムオブジェクトを対象とする場合 — 同一のクライアント名とマウントポイントを持つオブジェクトを一意に定義します。統合オブジェクトを対象とする場合 — 統合の種類を表示します (例: SAP または Lotus)。
- 種類: バックアップオブジェクトの種類。ファイルシステムオブジェクトを対象とする場合 — ファイルシステムの種類 (例: WinFS)。統合オブジェクトを対象とする場合 — 「Bar」

バックアップシステム **(ZDB 固有の用語)** 1 つ以上のアプリケーションシステムとともにディスクアレイに接続されているシステム。ほとんどの場合、バックアップシステムはターゲットボリューム (複製) を作成するためにディスクアレイに接続されるほか、ターゲットボリューム (複製) のマウント処理に使用されます。
アプリケーションシステム、ターゲットボリュームおよび複製 も参照。

バックアップセッション データのコピーを記憶メディア上に作成するプロセス。バックアップ仕様に処理内容を指定することも、対話式に操作を行うこともできます (対話式セッション)。1 つのバックアップ仕様の中で複数のクライアントが構成されている場合、すべてのクライアントが同じバックアップの種類を使って、1 回のバックアップセッションで同時にバックアップされます。バックアップセッションの結果、1 式のメディアにバックアップデータが書き込まれます。これらのメディアは、バックアップセットまたはメディアセットとも呼ばれます。
バックアップ仕様、フルバックアップ、および増分バックアップ も参照。

バックアップセット バックアップに関連したすべての統合ソフトウェアオブジェクトのセットです。

バックアップセット **(Oracle 固有の用語)**RMAN バックアップコマンドを使用して作成したバックアップファイルの論理グループ。バックアップセットは、バックアップに関連したすべてのファイルのセッ

トです。これらのファイルはパフォーマンスを向上するため多重化することができます。バックアップセットにはデータファイルまたはアーカイブログのいずれかを含めることができますが、両方同時に使用できません。

バックアップチェーン 復元チェーン を参照。

バックアップデバイス 記憶メディアに対するデータの読み書きが可能な物理デバイスを Data Protector で使用できるように構成したもの。たとえば、スタンドアロン DDS/DAT ドライブやライブラリなどをバックアップデバイスとして使用できます。

バックアップの種類 増分バックアップ、差分バックアップ、トランザクションバックアップ、フルバックアップおよびデルタバックアップ を参照。

バックアップビュー Data Protector では、バックアップ仕様のビューを切り替えることができます。

[種類別] を選択すると、バックアップ/テンプレートで利用できるデータの種類に基づいたビューが表示されます。(デフォルト)

[グループ別] を選択すると、バックアップ仕様/テンプレートの所属先のグループに基づいたビューが表示されます。

[名前別] を選択すると、バックアップ仕様/テンプレートの名前に基づいたビューが表示されます。

[Manager 別](MoM の実行時のみ有効) を選択すると、バックアップ仕様/テンプレートの所属先の Cell Manager に基づいたビューが表示されます。

バックアップ仕様 バックアップ対象のオブジェクトのリストに、使用するデバイスまたはドライブのセット、仕様に含まれているすべてのオブジェクトのバックアップオプション、およびバックアップを実行する曜日や時刻を加えたもの。オブジェクトとなるのは、ディスクやボリューム全体、またはその一部、たとえばファイル、ディレクトリ、Windows レジストリなどです。インクルードリストおよびエクスクルードリストを使用して、ファイルを選択することもできます。

バックアップ世代 1 つのフルバックアップとそれに続く増分バックアップを意味します。次のフルバックアップが行われると、世代が新しくなります。

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

パブリック/プライベートバックアップデータ

バックアップを構成する際は、バックアップデータをパブリックまたはプライベートのいずれにするかを選択できます。

- パブリックデータ − すべての Data Protector ユーザーに対してアクセスと復元が許可されます。
- プライベートデータ − バックアップの所有者および管理者に対してのみ表示と復元が許可されます。

パブリックフォルダーストア **(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ー内の情報を維持する部分。パブリックフォルダーストアは、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。

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

ひ

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

ファーストレベルミラー **(HP P9000 XP ディスクアレイファミリ 固有の用語)** HP P9000 XP ディスクアレイファミリ のディスクアレイの内部ディスク (LDEV) のミラーで、このミラーをさらにミラー化し、セカンドレベルのミラーを作成できます。Data Protector ゼロダウンタイムバックアップおよびインスタントリカバリ目的には、ファーストレベルミラーのみを使用できます。
プライマリボリュームおよびミラーユニット (MU) 番号 も参照。

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

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

ファイルシステム ハードディスク上に一定の形式で保存されたファイルの集まり。ファイルシステムは、ファイル属性とファイルの内容がバックアップメディアに保存されるようにバックアップされます。

ファイルジュークボックスデバイス ファイルメディアを格納するために使用する、複数のスロットからなるディスク上に存在するデバイス。

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

ファイルデポ バックアップからファイルライブラリデバイスまでのデータを含むファイル。

ファイルバージョン フルバックアップや増分バックアップでは、ファイルが変更されている場合、同じファイルが複数回バックアップされます。バックアップのロギングレベルとして [すべてログに記録] を選択している場合は、ファイル名自体に対応する 1 つのエントリとファイルの各バージョンに対応する個別のエントリが IDB 内に維持されます。

ファイルライブラリデバイス 複数のメディアからなるライブラリをエミュレートするディスク上に存在するデバイス。ファイルデポと呼ばれる複数のファイルが格納されます。

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

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

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

フェイルオーバー **(HP P6000 EVA ディスクアレイファミリ 固有の用語)**HP Continuous Access + Business Copy (CA+BC) P6000 EVA 構成でソースとあて先の役割を逆にする操作。
HP Continuous Access + Business Copy (CA+BC) P6000 EVA も参照。

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

プライマリボリューム (P-VOL) **(HP P9000 XP ディスクアレイファミリ 固有の用語)** HP P9000 XP ディスクアレイファミリ のディスクアレイの内部ディスク (LDEV) で、これに対して、そのミラー、またはスナップショットストレージに使用されるボリュームのいずれかのセカンダリボリューム (S-VOL) が存在し

ます。HP CA P9000 XP および HP CA+BC P9000 XP 構成では、プライマリボリュームはメインコントロールユニット (MCU) 内に配置されています。
セカンダリボリューム (S-VOL) およびメインコントロールユニット (MCU) も参照。

フラッシュリカバリ領域 **(Oracle 固有の用語)** Oracle によって管理されるディレクトリ、ファイルシステム、または自動ストレージ管理 (ASM) ディスクグループであり、バックアップ、復元、およびデータベース復旧に関係するファイル (リカバリファイル) 用の集中管理ストレージ領域として機能します。
リカバリファイル も参照。

フリープール フリープールは、メディアプール内のすべてのメディアが使用中になっている場合にメディアのソースとして補助的に使用できるプールです。ただし、メディアプールでフリープールを使用するには、明示的にフリープールを使用するように構成する必要があります。

フル ZDB テープへの ZDB セッションまたはディスク + テープへの ZDB セッション。前回のバックアップから変更がない場合でも、選択したすべてのオブジェクトがテープにストリーミングされます。
増分 ZDB も参照。

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

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

フルメールボックスバックアップ フルメールボックスバックアップでは、メールボックス全体の内容をバックアップします。

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

復元セッション バックアップメディアからクライアントシステムにデータをコピーするプロセス。

復元チェーン 選択した時点の状態までバックアップオブジェクトを復旧するために必要なバックアップイメージ。通常、オブジェクトの復元チェーンは、オブジェクトのフルバックアップイメージと、少なくとも 1 つの関連する増分バックアップイメージで構成されます。

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

複製セット **(ZDB 固有の用語)** 同じバックアップ仕様を使って作成される複製のグループ。
複製および複製セットローテーション も参照。

複製セットのローテーション **(ZDB 固有の用語)** 通常のバックアップ作成のために継続的に複製セットを使用すること。複製セットの使用を必要とする同一のバックアップ仕様が実行されるたびに、新規の複製がセットの最大数になるまで作成され、セットに追加されます。その後、セット内の最も古い複製は置き換えられ、セット内の複製の最大数が維持されます。
複製および複製セット も参照。

物理デバイス ドライブまたはより複雑な装置 (ライブラリなど) を格納する物理装置。

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、同じコンピューターに置かれていても、異なるコンピューター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。

へ

ペアステータス **(HP P9000 XP ディスクアレイファミリ 固有の用語)** HP P9000 XP ディスクアレイファミリ のディスクアレイのディスクペア (セカンダリボリュームとそれに対応するプライマリボリューム) の状態。状況によってペアのディスクはさまざまな状態になる可能性があります。Data Protector HP P9000 XP Agent の操作において特に以下の状態が重要となります。

- ペア – セカンダリボリュームがゼロダウンタイムバックアップ用に準備されています。セカンダリボリュームがミラーの場合、完全に同期化されます。セカンダリボリュームがスナップショットストレージ用に使用されるボリュームの場合、空の状態です。
- 中断 – ディスク間のリンクは中断されています。ただし、ペアの関係は維持されたままとなり、後で再度ゼロダウンタイムバックアップを行うためにセカンダリディスクを準備できます。
- コピー – ディスクペアは現在使用中であり、ペア状態に移行中です。セカンダリボリュームがミラーの場合、プライマリボリュームで再同期されています。セカンダリボリュームがスナップショットストレージに使用されるボリュームの場合、その内容はクリアされています。

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

並列処理 1 つのオンラインデータベースから複数のデータストリームを読み取ること。

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

ほ

ホストシステム Data Protector Disk Agent がインストールされており、ディスクデリバリーによるディザスタリカバリに使用される稼動中の Data Protector クライアント。

ボリュームグループ LVM システムにおけるデータストレージ単位。ボリュームグループは、1 つまたは複数の物理ボリュームから作成できます。同じシステム上に複数のボリュームグループを置くことができます。

ボリュームシャドウコピーサービス Microsoft ボリュームシャドウコピーサービス (VSS) を参照。

ボリュームマウントポイント **(Windows 固有の用語)** ボリューム上の空のディレクトリを他のボリュームのマウントに使用できるように構成したもの。ボリュームマウントポイントは、ターゲットボリュームへのゲートウェイとして機能します。ボリュームがマウントされていれば、ユーザーやアプリケーションがそのボリューム上のデータをフル (マージ) ファイルシステムパスで参照できます (両方のボリュームが一体化されている場合)。

保護 データ保護およびカタログ保護 を参照。

保守モード 内部データベースへの変更を防ぐために Cell Manager で開始できる操作モード。Data Protector インストールのアップグレードやパッチなど、さまざまな保守作業を実行できます。

補助ディスク 必要最小限のオペレーティングシステムファイル、ネットワークファイル、および Data Protector Disk Agent がインストールされたブート可能ディスク。ディスクデリバリーで UNIX クライアントを障害から復旧するときのフェーズ 1 では、補助ディスクをターゲットシステムのブートに使用することができます。

ま

マージ 復元中のファイル名競合を解決するモードの 1 つ。復元するファイルと同じ名前のファイルが復元先に存在する場合、変更日時の新しい方が維持されます。既存のファイルと名前が重複しないファイルは、常に復元されます。

上書き も参照。

マウントポイント ディレクトリ構造内において、ディスクまたは論理ボリュームにアクセスするためのアクセスポイント (`/opt` や `d:` など)。UNIX システムでは、`bdf` コマンドまたは `df` コマンドを使ってマウントポイントを表示できます。

マウント要求 マウント要求時には、デバイスにメディアを挿入するように促す画面が表示されます。必要なメディアを挿入して確認することでマウント要求に応答すると、セッションが続行されます。

マジックパケット Wake ONLAN を参照。

マルチスナップ **(HP P6000 EVA ディスクアレイファミリ 固有の用語)** 個々のターゲットボリュームだけでなく、スナップショットを構成するすべてのボリュームでバックアップデータの整合性が取れるように、複数のターゲットボリュームを同時に作成すること。
スナップショット も参照。

み

ミラー (EMC Symmetrix および HP P9000 XP ディスクアレイファミリ 固有の用語) ターゲットボリューム を参照。

ミラークローン **(HP P6000 EVA ディスクアレイファミリ 固有の用語)** ストレージボリュームの動的な複製です。元のストレージボリュームに加えられた変更は、ローカル複製リンクを介して、ミラークローンに反映されます。元のストレージボリュームとそのミラークローン間の複製は中断できます。各ストレージボリュームについてディスクアレイ上に 1 つのミラークローンを作成できます。

ミラーユニット (MU) 番号 **(HP P9000 XP ディスクアレイファミリ 固有の用語)** HP P9000 XP ディスクアレイファミリ のディスクアレイ上にある内部ディスク (LDEV) のセカンダリボリューム (S-VOL) を特定する 0 以上の整数。
ファーストレベルミラー も参照。

ミラーローテーション (HP P9000 XP ディスクアレイファミリ 固有の用語) 複製セットローテーション を参照。

む

無人操作 夜間処理 を参照。

め

メインコントロールユニット (MCU) **(HP P9000 XP ディスクアレイファミリ 固有の用語)** HP CA P9000 XP または HP CA+BC P9000 XP 構成のプライマリボリューム (P-VOL) を含み、マスターデバイスとして機能する HP P9000 XP ディスクアレイファミリ のユニット。
HP Business Copy (BC) P9000 XP、HP Continuous Access (CA) P9000 XP、および LDEV も参照。

メールボックス **(Microsoft Exchange Server 固有の用語)** 電子メールが配信される場所。管理者がユーザーごとに設定します。電子メールの配信場所として複数の個人用フォルダー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ー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。

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

メディアのエクスポート メディアに格納されているすべてのバックアップセッション情報 (システム、オブジェクト、ファイル名など) を IDB から削除するプロセス。メディア自体に関する情報やメディアとプールの関係に関する情報も IDB から削除されます。メディア上のデータは影響されません。
メディアのインポート も参照。

メディアのボールティング メディアを安全な別の場所に収納すること。メディアが復元に必要になった場合や、今後のバックアップにメディアを再使用する場合は、メディアをデータセンターに戻します。ボールティング手順は、会社のバックアップ戦略やデータ保護/信頼性ポリシーに依存します。

メディアの位置 バックアップメディアが物理的に収納されている場所を示すユーザー定義の識別子。"building 4"や"off-site storage"のような文字列です。

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

メディアの種類 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。

メディアプール 同じ種類のメディア (DDS など) のセット。グループとして追跡されます。フォーマットしたメディアは、メディアプールに割り当てられます。

メディアラベル メディアに割り当てられるユーザー定義の識別子。

メディア割り当てポリシー メディアをバックアップに使用する順序を決定します。[厳格] メディア割り当てポリシーでは、特定のメディアに限定されます。[緩和] ポリシーでは、任意の適切なメディアを使用できます。[フォーマットされていないメディアを先に割り当てる] ポリシーでは、ライブラリ内に利用可能な非保護メディアがある場合でも、不明なメディアが優先されます。

メディア管理セッション 初期化、内容のスキャン、メディア上のデータの確認、メディアのコピーなどのアクションをメディアに対して実行するセッション。

メディア状態要素 使用回数のしきい値と上書きのしきい値。メディアの状態の判定基準となります。

や

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

ゆ

ユーザーアカウント (Data Protector ユーザーアカウント) Data Protector およびバックアップデータに対する無許可のアクセスを制限するために、Data Protector ユーザーとして許可を受けたユーザーにしか Data Protector を使用できないようになっています。Data Protector 管理者がこのアカウントを作成するときには、ユーザーログオン名、ユーザーのログオン元として有効なシステム、および Data Protector ユーザーグループのメンバーシップを指定します。ユーザーが Data Protector のユーザーインタフェースを起動するか、または特定のタスクを実行するときには、このアカウントが必ずチェックされます。

ユーザーアカウント制御 (UAC) Windows Vista、Windows 7、Windows 8、Windows Server 2008、Windows Server 2012 のセキュリティコンポーネント。管理者が権限レベルを上げるまで、アプリケーションソフトウェアを標準のユーザー権限に限定します。

ユーザーグループ 各 Data Protector ユーザーは、ユーザーグループのメンバーです。各ユーザーグループにはユーザー権限のセットがあり、それらの権限がユーザーグループ内のすべてのユーザーに付与されます。ユーザー権限を関連付けるユーザーグループの数は、必要に応じて定義できま

す。Data Protector には、デフォルトで admin、operator、user という 3 つのユーザーグループが用意されています。

ユーザーディスククォータ NTFS のクォータ管理サポートを使用すると、共有ストレージボリュームに対して、拡張された追跡メカニズムの使用およびディスク容量に対する制御が行えるようになります。Data Protector では、システム全体にわたるユーザーディスククォータが、すべての構成されたユーザーに対して一度にバックアップされます。

ユーザープロファイル **(Windows 固有の用語)** ユーザー別に維持される構成情報。この情報には、デスクトップ設定、画面表示色、ネットワーク接続などが含まれます。ユーザーがログオンすると、そのユーザーのプロファイルがロードされ、Windows 環境がそれに応じて設定されます。

ユーザー権限 特定の Data Protector タスクの実行に必要なパーミッションをユーザー権限またはアクセス権限と呼びます。主なユーザー権限には、バックアップの構成、バックアップセッションの開始、復元セッションの開始などがあります。ユーザーには、そのユーザーの所属先ユーザーグループに関連付けられているアクセス権限が割り当てられます。

ら

ライター **(Microsoft VSS 固有の用語)** オリジナルボリューム上のデータの変更を開始するプロセス。主に、永続的なデータをボリューム上に書き込むアプリケーションまたはシステムサービスがライターとなります。ライターは、シャドウコピーの同期化プロセスにも参加し、データの整合性を保証します。

ライブラリ オートチェンジャー、ジュークボックス、オートローダ、またはエクスチェンジャーとも呼ばれます。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。

り

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

- Oracle ターゲットデータベースの物理スキーマ
- データファイルおよびアーカイブログのバックアップセット
- データファイルのコピー
- アーカイブ REDO ログ
- ストアドスクリプト

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

リカバリカタログデータベースへのログイン情報

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

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

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

リサイクルまたは保護解除 メディア上のすべてのバックアップデータのデータ保護を解除して、以降のバックアップで上書きできるようにするプロセス。同じセッションに所属しているデータのうち、他のメディ

アに置かれているデータも保護解除されます。リサイクルを行っても、メディア上のデータ自体は変更されません。

リムーバブル記憶域の管理データベース **(Windows 固有の用語)**Windows サービスの 1 つ。リムーバブルメディア (テープやディスクなど) と記憶デバイス (ライブラリ) の管理に使用されます。リムーバブル記憶域により、複数のアプリケーションが同じメディアリソースを共有できます。

ろ

ローカル復旧とリモート復旧 リモート復旧は、SRD ファイルで指定されている Media Agent ホストがすべてアクセス可能な場合にのみ実行されます。いずれかのホストがアクセス不能になっていると、ディザスタリカバリプロセスがローカルモードにフェイルオーバーされます。これは、ターゲットシステムにローカルに接続しているデバイスが検索されることを意味します。デバイスが 1 台しか見つからない場合は、そのデバイスが自動的に使用されます。複数のデバイスが見つかった場合は、デバイスが選択できるプロンプトが表示され、ユーザーが選択したデバイスが復元に使用されます。

ローカル連続レプリケーション **(Microsoft Exchange Server 固有の用語)** ローカル連続レプリケーション (LCR) はストレージグループの完全コピー (LCR コピー) を作成および維持するシングルサーバーソリューション。LCR コピーは元のストレージグループと同じサーバーに配置されます。LCR コピーが作成されると、変更伝播 (ログリプレイ) テクノロジで最新に保たれます。LCR の複製機能では未複製のログが削除されません。この動作の影響により、ログを削除するモードでバックアップを実行しても、コピー中のログと複製に十分な余裕がある場合、実際にはディスクの空き容量が解放されない場合があります。

LCR コピーへの切り替えは数秒で完了するため、LCR コピーはディザスタリカバリに使用されます。元のデータとは異なるディスクに存在する LCR コピーをバックアップに使用すると、プロダクションデータベースの入出力の負荷が最小になります。

複製されたストレージグループは、Exchange ライターの新しいインスタンス (Exchange Replication Service) として表示され、通常のストレージグループのように VSS を使用してバックアップできます。

クラスター連続レプリケーションおよび Exchange Replication Service も参照。

ロギングレベル バックアップ、オブジェクトコピー、またはオブジェクト集約中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 に記録するかを指定するオプションです。バックアップ時のロギングレベルに関係なく、データの復元は常に可能です。Data Protector には、[すべてログに記録]、[ディレクトリレベルまでログに記録]、[ファイルレベルまでログに記録]、および [記録しない] の 4 つのロギングレベルがあります。ロギングレベル設定によって、IDB のサイズ増加、および復元データのブラウズのしやすさが影響を受けます。

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

ロック名 別のデバイス名を使うことで同じ物理デバイスを違う特性で何度も構成することができます。そのようなデバイス (デバイス名) が複数同時に使用された場合に重複を防ぐ目的で、デバイス構成をロックするためにロック名が使用されます。ロック名はユーザーが指定する文字列です。同一の物理デバイスを使用するデバイス定義には、すべて同じロック名を使用します。

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

論理演算子 Data Protector ヘルプシステムの全文検索には、AND、OR、NOT、NEAR の各論理演算子を使用できます。複数の検索条件を論理演算子で組み合わせて指定することで、検索対象をより正確に絞り込むことができます。複数単語の検索に演算子を指定しなければ、AND を指定したものとみなされます。たとえば、「マニュアル ディザスタ リカバリ」という検索条件は、「マニュアル AND ディザスタ AND リカバリ」と同じ結果になります。

わ

ワイルドカード文字 1 文字または複数文字を表すために使用できるキーボード文字。たとえば、通常、アスタリスク (*) は 1 文字以上の文字を表し、疑問符 (?) は 1 文字を示します。ワイルドカード文字

は、名前により複数のファイルを指定するための手段としてオペレーティングシステムで頻繁に使用されます。