HP Data Protector 7.00
トラブルシューティングガイド

HP 部品番号: N/A
2012 年 8 月
第 2 版

目次

出版履歴

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

表 1 出版履歴

製品番号	ガイド版	製品
B6960-96037	2008 年 11 月	Data Protector リリース A.06.10
B6960-90153	2009 年 9 月	Data Protector リリース A.06.11
N/A	2011 年 3 月	Data Protector リリース 6.20
N/A	2012 年 3 月	Data Protector リリース 7.00
N/A	2012 年 7 月	Data Protector リリース 7.00(次のいずれかのパッチバンドルを含む): DPWINBDL_00701、DPUXBDL_00701、DPLNXBDL_00701

本書について

本書では、Data Protector の使用時に発生する可能性がある問題をトラブルシューティングする方法について説明します。ここでは一般的な問題とそれらの解決方法を紹介しています。

注記: 本書では、Data Protector のインストール、統合ソフトウェア、ゼロダウンタイムバックアップ機能、ディザスタリカバリに固有のトラブルシューティング情報については説明していません。関連する情報は、各製品のガイドを参照してください。

対象読者

本書は、ネットワーク上のシステムの保守とバックアップに携わるバックアップ管理者を対象としています。

ドキュメントセット

その他のガイドおよびヘルプには、関連情報が記載されています。

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 ファイルは、Data Protector のセットアップ時に、Windows の場合は英語のドキュメント（ガイド、ヘルプ）コンポーネントを、UNIX の場合は `OB2-DOCS` コンポーネントを、それぞれ選択してインストールします。ガイドのインストール後の保存先ディレクトリは、*`Data_Protector_home`*`\docs`(Windows) または `/opt/omni/doc/C`(UNIX) です。

これらの資料は、HP サポート Web サイトの [Manuals] ページから入手できます。

http://support.openview.hp.com/selfsolve/manuals

[Storage] セクションの **[Storage Software]** をクリックし、ご使用の製品を選択してください。

- 『HP Data Protector コンセプトガイド』

  このガイドでは、Data Protector のコンセプトを解説するとともに、Data Protector の動作原理を詳細に説明しています。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計画、準備、テスト、および実行の方法について説明します。

- 『HP Data Protector インテグレーションガイド』

  このガイドでは、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。このガイドは、バックアップ管理者やオペレータを対象としています。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、HP Network Node Manager、および Network Data Management Protocol Server に対応する HP 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 - 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、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 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 Integration Guide for HP Operations Manager for UNIX』

  このガイドでは、UNIX 版の HP Operations Manager と HP Service Navigator を使用して、Data Protector 環境の健全性と性能を監視および管理する方法について説明します。

- 『HP Data Protector Integration Guide for HP Operations Manager for Windows』

  このガイドでは、Windows 版の HP Operations Manager を使用して、Data Protector 環境の健全性と性能を監視および管理する方法について説明します。

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

  このガイドでは、Data Protector ゼロダウンタイムバックアップとインスタントリカバリのコンセプトについて解説するとともに、ゼロダウンタイムバックアップ環境における Data Protector の動作原理を詳細に説明します。手順を中心に説明している『HP Data Protector 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 P10000 Storage Systems、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方法を説明します。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』

  このガイドでは、Microsoft Exchange Server 2010 環境用の Granular Recovery Extension を構成し使用する方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 Media Operations User Guide』

  このガイドは、システムの保守とバックアップを担当するネットワーク管理者を対象に、オフラインストレージメディアの追跡と管理に関する情報を提供します。アプリケーションのインストールと構成、日常のメディア操作、およびレポート作成のタスクについて説明します。

- 『HP Data Protector 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 7.00 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、制限事項、報告されている問題とその回避方法などの情報も記載されています。

- 『HP Data Protector Product Announcements, Software Notes, and References for Integrations to HP Operations Manager』

  このガイドは、HP Operations Manager 統合ソフトウェアに対して同様の機能を果たします。

- 『HP Data Protector Media Operations Product Announcements, Software Notes, and References』

  このマニュアルは、Media Operations に対して同様の機能を果たします。

- 『HP Data Protector Command Line Interface Reference』

  このガイドでは、Data Protector コマンド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。

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。

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` 経由でヘルプシステムにアクセスします。

ドキュメントマップ

略称

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
IG-IBM	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
IG-MS	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
IG-O/S	インテグレーションガイド - Oracle、SAP
IG-OMU	Integration Guide for HP Operations Manager for UNIX
IG-OMW	Integration Guide for HP Operations Manager for Windows
IG-Var	インテグレーションガイド - Sybase、Network Node Manager、Network Data Management Protocol Server
IG-VirtEnv	インテグレーションガイド - 仮想環境
IG-VSS	Integration Guide for Microsoft Volume Shadow Copy Service
Install	インストールおよびライセンスガイド
MO-GS	Media Operations Getting Started Guide
MO-PA	Media Operations Product Announcements, Software Notes, and References
MO-UG	Media Operations User Guide
PA	製品案内、ソフトウェアノートおよびリファレンス
Trouble	トラブルシューティングガイド
ZDB-Admin	ZDB 管理者ガイド

略称	ドキュメント項目
ZDB-Concept	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	PA	インテグレーションガイド: MS	O/S	IBM	Var	VSS	VirtEnv	OMU	OMW	ZDB: Concept	Admin	IG	GRE: Exchange	SPS	VMware	MO: GS	UG	PA	CLI
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	
新機能	X						X																	X	
プラニング方法	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	
必要条件				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				

統合ソフトウェア

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
HP Network Node Manager(NNM)	IG-Var
HP Operations Manager	IG-OMU、IG-OMW
IBM DB2 UDB	IG-IBM
Informix Server	IG-IBM
Lotus Notes/Domino Server	IG-IBM
Media Operations	MO-UG
Microsoft Exchange Server	IG-MS、ZDB IG、GRE-Exchange
Microsoft Hyper-V	IG-VirtEnv

ソフトウェアアプリケーション	ガイド
Microsoft SharePoint Server	IG-MS、ZDB-IG、GRE-SPS
Microsoft SQL Server	IG-MS、ZDB-IG
Microsoft ボリュームシャドウコピーサービス (VSS)	IG-VSS
ネットワークデータ管理プロトコル (NDMP) サーバー	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 vSphere	IG-VirtEnv、GRE-VMware
VMware vCloud Director	IG-VirtEnv

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-Concept、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 P10000 Storage Systems	ZDB-Concept、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」 (12 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
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。

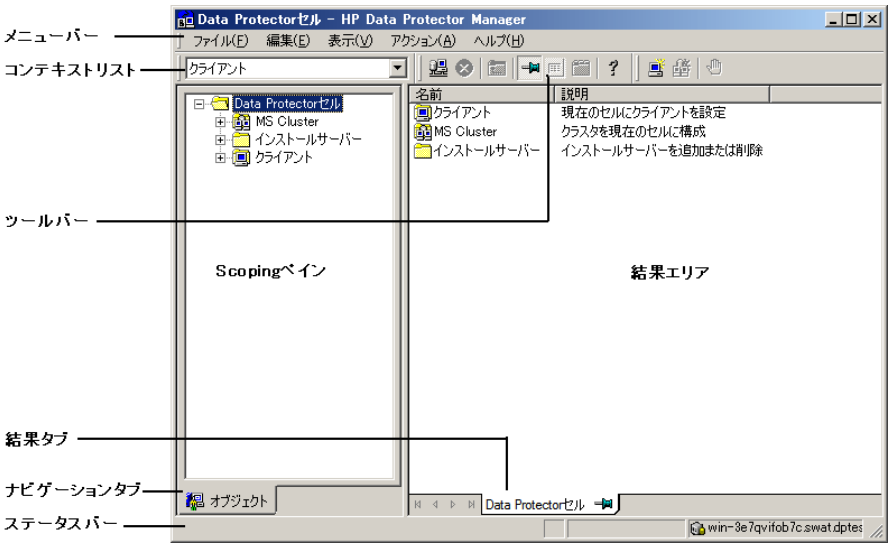
注記: 補足情報を示します。

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、クロスプラットフォーム (Windows と UNIX) のグラフィカルユーザーインタフェースを提供します。オリジナルの Data Protector GUI(Windows のみ) または Data Protector Java GUI を使用できます。Data Protector グラフィカルユーザーインタフェースに関する詳細は、『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

1 Data Protector のトラブルシューティングについて

概要

Data Protector の使用時に発生する問題の多くは、ユーザー自身で解決することができます。そのような場合には、このガイドを手引きとしてお役立てください。

このガイドの使い方

問題を短時間で効率的に解決するために、以下の事項に留意してください。

1. この章に記載されている全般的なトラブルシューティング情報を把握しておきます。
2. 発生している問題に関する情報がこのガイドに記載されているかどうかをチェックします。インストール、統合、ZDB、ディザスタリカバリに関する問題は、本書では扱いません。これらについては、それぞれのガイドを参照してください。
3. 問題の解決方法が見つからない場合は、その問題を HP カスタマサポートサービスにご連絡ください。サポートに必要なデータの準備方法については、「サポートへご連絡いただく前に」 (65 ページ) を参照してください。

ヒント: Data Protector のパフォーマンスに関する概要やヒントについては、『HP Data Protector ヘルプ』の索引「パフォーマンス」を参照してください。

全般的なチェック

最初に、以下の事項を確認してください。

- 現段階では回避できない既知の制限事項に関連していないこと。Data Protector の制限および推奨事項、Data Protector および Data Protector 以外の既知の問題の詳細については、『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』を参照してください。
- サードパーティ製のハードウェアやソフトウェアに関連した問題ではないこと。関連している場合は、各ベンダーにサポートの問い合わせを行ってください。
- Data Protector の最新のパッチがインストールされていること。パッチは http://www.itrc.hp.com から入手できます。

  どの Data Protector パッチがシステムにインストールされているかをチェックする方法については、『HP Data Protector ヘルプ』の索引キーワード「パッチ」で表示される内容を参照してください。
- 適切なオペレーティングシステムパッチがインストールされていること。

  必要なオペレーティングシステムパッチのリストについては、『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。
- アプリケーションバックアップの場合、バックアップ失敗の原因がアプリケーションのダウンではないこと。
- デバッグログまたは REDO ログを格納しているファイルシステムが満杯になっていないこと。
- アプリケーションデータを格納しているファイルシステムが満杯になっていないこと。
- システムのメモリーが不足していないこと。

Data Protector ログファイル

Data Protector の使用時に問題が発生した場合は、ログファイル内の情報が問題の特定に役立ちます。

ログファイルの保存場所

ほとんどの Data Protector ログファイルは、以下の場所にあります。

Windows Vista、Windows 7、および Windows Server 2008 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 および/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

Novell NetWare システムの場合: SYS: \USR\OMNI\LOG

ログファイルの形式

ほとんどの Data Protector ログファイルのエントリは以下の形式になっています。

time_stamp process.PID.Thread_ID source_file_info Data Protector_version log_entry_message

例

```
02/15/2012 1:44:50 PM  INET.3048.3036 ["inetnt/allow_deny.c
/main/dp61/6":467] A.07.00
A request 0 (BDF) came from host computer.company.com
(10.17.xx.xxx) which is not in AllowList: not proceeding with this request!
```

ログファイルの内容

Data Protector ログファイルに記録される情報は、下の表に示すとおりです。

表 3 Data Protector ログファイル

debug.log	予期されていなかった状況が記録されます。ユーザーにとって役立つ内容もありますが、主として当社サポートサービスが使用します。
inet.log	要求拒否など、クライアントのローカルセキュリティに関するイベントが記録されます。UNIX の場合は、Data Protector Inet サービスに対して発行されたすべての要求も記録されます。
enhincr.log	拡張増分バックアップの動作に関する情報が記録されます。たとえば、拡張増分バックアップレポジトリで起こった問題の詳細なエラー情報などがこれに含まれます。
Ob2EventLog.txt	Data Protector のイベントと通知が記録されます。イベントログには、Data Protector イベントが一括して保存されます。
media.log	バックアップ、初期化、インポートの各処理でメディアが使用されるたびに、このログファイルに新しいエントリが作成されます。IDB の復旧では、media.log を使って、IDB をバックアップしたメディアや、前回の IDB バックアップ以降に使用されたメディアを検索できます。
omnisv.log	Data Protector サービスが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。
security.log	Cell Manager 上のセキュリティ関連イベントが記録されます。イベントの中には、通常操作の結果として発生するものもあります。その場合は、許可されていない操作が特定のユーザーによって試行されたことを意味するだけですが、その一方で、故意に不正侵入が行われていることを示すイベントの場合もあります。
purge.log	IDB のバックグラウンドでの削除動作のトレース結果が記録されます。
RDS.log	IDB のログが記録されます。このファイルは Cell Manager 上の以下のディレクトリにあります。 **Windows Server 2008 の場合:** Data_Protector_program_data\db40\datafiles\catalog **その他の Windows システムの場合:** Data_Protector_home\db40\datafiles\catalog

表 3 Data Protector ログファイル (続き)

	UNIX システムの場合: `/var/opt/omni/server/db40/datafiles /catalog`
sanconf.log	`sanconf` コマンドにより生成されたセッションレポートが記録されます。
sm.log	バックアップセッションや復元セッションで発生した内部エラーの詳細 (バックアップ仕様の解析エラーなど) が記録されます。
upgrade.log	このログは、アップグレード処理中に作成されます。UCP(アップグレードコアパート) と UDP(アップグレード詳細パート) のメッセージが記録されます。
OB2_Upgrade.log (UNIX のみ)	このログは、アップグレード処理中に作成されます。アップグレード処理のトレース情報が記録されます。
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。
sap.log、oracle8.log、informix.log、sybase.log、db2.log	アプリケーション固有のログファイルです。アプリケーションと Data Protector 間の統合ソフトウェア呼び出しに関するトレース結果が記録されます。このファイルは、アプリケーションシステムに保存されます。

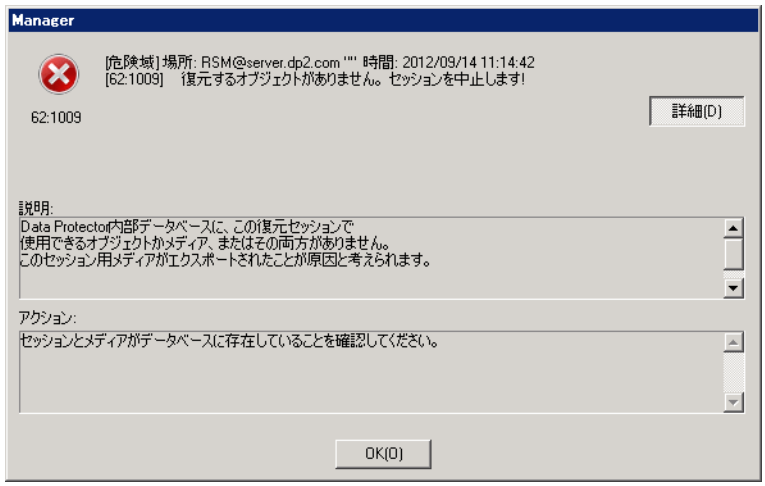
Data Protector エラーメッセージ

Data Protector の多くのエラーメッセージにはトラブルシューティング情報が関連付けられており、そのメッセージから、エラーの詳細情報や問題を解決するためのヒントを得ることができます。メッセージにはエラー番号が記述されており、関連情報にアクセスする際に使用することができます。

Data Protector GUI のエラーメッセージ

セッション出力内の一部のエラーメッセージには、クリッカブルリンクでエラー番号が示されています。そのリンクをクリックすると、エラーに関する詳細情報がエラーメッセージダイアログに表示されます。エラーの詳細な説明と解決のヒントを表示するには、[詳細] をクリックします。

図 2 エラーメッセージダイアログのサンプル



Data Protector CLI のエラーメッセージ

Data Protector CLI にエラー番号を含むエラーが返された場合は、トラブルシューティングファイルでエラーの詳細を探すことができます。このテキストファイルには、すべての Data Protector エラーメッセージが記述され、メッセージごとに説明と対処方法が示されています。

トラブルシューティングファイルは、Cell Manager 上の以下の場所にあります。

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

UNIX システムの場合: `/opt/omni/gui/help/C/Trouble.txt`

例

メッセージ:

[12:1051]クライアントのセキュリティ侵害。アクセスが拒否されました。

説明:

ターゲットホストはセキュリティ保護されており、Cell権限のリストに存在しないホストによってアクセスされました。

対処方法:

*クライアントのCell権限のリストを確認して更新してください。*クライアントがロックアウトされている場合は、allow_hostsファイルを手動で編集します。

Data Protector カスタマイズファイル

Data Protector 変数を設定することで、問題を解決できる場合があります。このガイドでは、ある特定の問題を解決しようとする際に、どの変数を設定すると有効かを示します。

グローバルオプション

グローバルオプションは Data Protector セル全体に影響を及ぼし、Data Protector のさまざまな側面(タイムアウトや制限値など)を制御します。すべてのグローバルオプションは、グローバルオプションファイルに記述されており、そのファイルを編集して Data Protector をカスタマイズできます。

グローバルオプションファイルは、Cell Manager 上の以下の場所にあります。

Windows Server 2008 の場合:

Data_Protector_program_data\Config\Server\Options\global

その他の Windows システムの場合:

Data_Protector_home\Config\Server\Options\global

UNIX システムの場合: /etc/opt/omni/server/options/global

グローバルオプションを設定するには、global ファイルを編集します。希望するオプション行の"#"記号を削除してコメント指定を解除し、適切な値を設定します。

注記: ほとんどの場合は、グローバルオプションを変更しなくても、Data Protector を操作できます。

最も頻繁に使用されるグローバル変数

最も頻繁に使用されるグローバル変数を以下に示します。詳細な説明については、グローバルオプションファイルを参照してください。

- MediaView: [メディア管理] コンテキストに表示されるフィールドとその順番を変更します。
- MaxBSessions: 同時処理バックアップ数のデフォルトの上限値 5 を変更します。
- InitOnLoosePolicy: メディアポリシーに [緩和] が使用された場合、空のメディアまたは認識されないメディアを Data Protector が自動的に初期化するようにします。
- MaxMAperSM: バックアップセッションごとのデバイス同時処理数のデフォルトの上限値を変更します (デバイス同時処理数の最大数は 32)。
- DCDirAllocation: 新しい詳細カタログのバイナリファイルの格納先に dcbf ディレクトリを選択する場合に使用するアルゴリズムを指定します。fill in sequence(デフォルト)、balance size、balance number の 3 種類のアルゴリズムが使用可能です。割り当てポリシーを [fill in sequence](デフォルト) から [balance size] に変更することをお勧めします。
- DailyMaintenanceTime: 日常の保守作業を開始可能な時刻を指定します。デフォルト値は 12:00(正午) です。日常の保守作業の一覧は、『HP Data Protector ヘルプ』の索引キーワード「Data Protector" が実行するチェック」で表示される内容を参照してください。

- DailyCheckTime: 日常のチェック作業の開始可能な時刻を指定します。デフォルト値は午後 12:30 です。日常のチェック作業を無効にすることもできます。日常のチェック作業の一覧は、『HP Data Protector ヘルプ』の索引キーワード「Data Protector" が実行するチェック」で表示される内容を参照してください。

Omnirc オプション

omnirc オプションは、トラブルシューティングを行う場合や、他の設定値を無効にしたい場合に非常に便利で、Data Protector クライアントの動作にのみ影響します。ただし、動作環境で本当に必要になった場合にのみ使用してください。このオプションの値は、Disk Agent や Media Agent によって使用されます。

omnirc 変数は、各クライアント上の以下のファイル内に設定します。

Windows Vista、Windows 7、および Windows Server 2008 の場合:
Data_Protector_program_data\omnirc

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

HP-UX、Solaris、および Linux システムの場合: /opt/omni/.omnirc

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

Novell NetWare システムの場合: sys:\usr\omni\omnirc

omnirc オプションの使用方法

omnirc オプションを設定するには、以下の手順を実行してください。

1. プラットフォームに応じて、omnirc.tmpl テンプレートか.omnirc.TMPL テンプレートを、それぞれ omnirc または.omnirc にコピーします。
2. omnirc ファイルまたは.omnirc ファイルを編集します。希望するオプション行の "#" 記号を削除してコメント指定を解除し、適切な値を設定します。
3. 変数の設定が終了したら、以下の操作を行います。
   - ファイルをコピーするかまたはエディタを使用して omnirc ファイルを作成したときは、ファイルの権限を確認してください。UNIX の場合、ファイルのパーミッションはユーザーの umask 設定値に応じて設定されるため、一部のプロセスでファイルを読み取れない設定になることがあります。ファイルのパーミッションを手動で 644 に設定してください。
   - omnirc ファイルを変更したときは、omnirc ファイルを変更した Data Protector クライアント上で、Data Protector のサービス/デーモンを再起動します。UNIX 上の crs デーモンについてはこの操作が必須です。必ず再起動してください。また、Windows 上の Data Protector CRS サービスと Inet サービスも再起動することをお勧めします。Windows の場合に限り、エントリを追加または変更した場合や、エントリを削除(またはファイル名を変更)しただけの場合は、再起動は必要ありません。

注記: omnirc ファイル内の変数名に特殊な文字を使用する場合は、環境変数の設定に使用できる文字に関するオペレーティングシステム固有の制限事項にも注意が必要です。たとえば UNIX システムの場合であれば、変数内にスペース タブ / : * " < > | を含めることはできません。

ディザスタリカバリ中に omnirc オプションを設定する方法については、『HP Data Protector ディザスタリカバリガイド』を参照してください。

最も頻繁に使用される omnirc 変数

最も頻繁に使用される omnirc 変数を以下に示します。各オプションの詳細については、omnirc ファイルを参照してください。

- **OB2_SSH_ENABLED:** セキュリティ保護されたシェル (SSH) を使用して保護されたリモートインストールを有効にするには、インストールサーバー上でこの変数を 1 に設定します。デフォルト値は 0(設定なし) です。
- **OB2_ENCRYPT_PVT_KEY:** セキュリティ保護されたリモートインストールのために暗号化された秘密キーを使用するには、インストールサーバーでこの変数を 1 に設定します。デフォルト値は 0(設定なし) です。
- **OB2_ENCRYPT_MEDIUM_STRICT:** バックアップ、オブジェクト集約、オブジェクトコピー、および自動メディアコピーの各セッションで、ドライブベースの暗号化を厳密な方針で実行するかどうかを制御できます。この変数は、現在のセッションに対して GUI オプションの [ドライブベースの暗号化] が選択されている場合にのみ考慮されます。

  値を 1 に設定すると、以下のようになります。

  - 選択したテープドライブで暗号化がサポートされていない場合、デフォルトでセッションが中止されます。
  - 選択したテープドライブで暗号化がサポートされていても、そのドライブ内のメディアが暗号化をサポートしていない場合は、マウント要求が発行されます (スタンドアロンのテープドライブの場合)。または、まず次に利用可能なメディアが暗号化をサポートしているかどうかがチェックされ、暗号化をサポートしているメディアが見つからない場合に最終的にマウント要求が発行されます（テープライブラリの場合）。
  - 選択したテープドライブとドライブ内のメディアの両方が暗号化をサポートしている場合、暗号化モードでデータの書き込み操作が実行されます。

  値を 0 に設定すると、以下のようになります。

  - 選択したテープドライブで暗号化がサポートされていない場合、非暗号化モードでデータ書き込み操作が実行されます。
  - 選択したテープドライブで暗号化がサポートされていても、そのドライブ内のメディアが暗号化をサポートしていない場合は、非暗号化モードでデータ書き込み操作が実行されます。
  - 選択したテープドライブとドライブ内のメディアの両方が暗号化をサポートしている場合、暗号化モードでデータの書き込み操作が実行されます。
- **OB2_ENCRYPT_FORCE_FORMAT:** Data Protector ドライブベースの暗号化を使用するときに、フォーマットの動作を制御できます。

  設定する値に応じて、以下のようになります。

  - 0 (デフォルト値)。フォーマット操作は中止されます。
  - 1。フォーマット操作は強制されます。
- **OB2BLKPADDING_n:** 初期化時にメディアに書き込まれる空のブロック数を指定します。これにより、メディアのコピー時に、すべてのデータのコピーが完了する前にターゲットメディアがスペース不足になるのを防ぎます。
- **OB2DEVSLEEP:** デバイスのロード中、再試行後に次の再試行が行われるまでのスリープ時間を変更します。
- **OB2ENCODE:** バックアップ仕様でバックアップオプションがどのように設定されているかに関係なく、ユーザーがデータエンコーディングを常に使用できるようにします。
- **SESSIONSTATUSWHENNOOBJECTTOCOPY** および **SESSIONSTATUSWHENNOOBJECTTOCONSOLIDATE:** オブジェクトコピーおよびオブジェク

ト集約セッションで、コピーまたは集約するオブジェクトがない場合のセッションステータスを制御できます。

設定する値に応じて、以下のようになります。

- 0(デフォルト)の場合、セッションは失敗とみなされ、重大なエラーが表示されます。
- 1 の場合、セッションは成功とみなされますが、警告が表示されます。
- 2 の場合、セッションは成功とみなされ、通常のメッセージが表示されます。

- **OB2OEXECOFF:** 特定のクライアントに対するバックアップ仕様で定義されているオブジェクトの実行前/実行後スクリプトを、ユーザーが制限または無効化できるようにします。
- **OB2REXECOFF:** 特定のクライアントに対するリモートセッションの実行前/実行後スクリプトをユーザーが無効化できるようにします。
- **OB2CHECKCHANGETIME**(UNIX のみ): 増分バックアップで「前回 inode 変更日時」をいつ使用するかを制御します。
- **OB2INCRDIFFTIME**(UNIX のみ): 増分バックアップに対する「前回 inode 変更日時」のチェック時に適用される「増分待ち」時間を指定します。この変数は、**OB2CHECKCHANGETIME** 変数が 2 に設定されている場合にのみ有効です。
- **OB2RECONNECT_ACK:** Data Protector が Ack メッセージを待つ時間を定義します (デフォルト値は 1200 秒)。この時間内にエージェントが Ack メッセージを受け取らなければ、それ以降、ソケット接続は無効とみなされます。
- **OB2RECONNECT_RETRY:** 接続が切断した場合に、Data Protector Disk Agent または Media Agent が再接続を試みる時間を定義します。デフォルト値は 600 秒です。
- **OB2SHMEM_IPCGLOBAL:** Disk Agent と MediaAgent の両方がインストールされている HP-UX クライアントでは、バックアップ中に以下のエラーが発生した場合に備えて、このオプションを 1 に設定しておく必要があります。

  共有メモリーを割り当て/関連付けできません(IPC は共有メモリーセグメントを割り当てることができません。)システムエラー: [13] パーミッションが拒否されました。) => 中止しています。

- **OB2VXDIRECT:** 拡張 VxFS ファイルシステムの直接読み取り (キャッシュなし) を可能にして、パフォーマンスを向上させます。
- **OB2_CLP_MAX_ENTRIES**(Windows のみ): Change Log Provider がメモリー内に保持できるエントリ数を設定します。Change Log Provider で使用されるメモリー量は、すべてのエントリのファイル名を合わせた長さに依存します。最小構成は 15,000 エントリ (約 25MB の RAM) です。デフォルト値は 100,000 エントリーです (約 120MB の RAM)。この数値が小さな値に変更され、すべてのエントリをメモリー内に保持できなくなると、バックアップ時間が長くなることがあります。
- **OB2_CLP_CREATE_EI_REPOSITORY**(Windows のみ): Change Log Provider を初めて実行する際に、拡張増分リポジトリを作成するかどうかを指定します。拡張増分リポジトリを作成する場合は 1 に設定します。デフォルト値は 0 です (作成しません)。この変数を設定すると、拡張増分リポジトリが常に更新されるため、バックアップ時間が長くなります。ただし、その設定によって、従来の拡張増分バックアップに対するフォールバックが有効になります。
- **OB2_ENHINC_SQLITE_MAX_ROWS:** 内部メモリキャッシュに格納できる拡張増分バックアップデータベース (Windows、HP-UX、および Linux システムの SQLite) で、行の最大数を指定します。バックアップが膨大な数 (数百万) のディレクトリで構成されている場合、この変数を使用すると、キャッシュに格納できる行の最大数を増やすことができるため、Disk Agent のパフォーマンスが向上します。
- **OB2SANCONFSCSITIMEOUT=s**(Windows のみ): sanconf 関連操作のタイムアウト値を設定します。sanconf コマンドを実行するには、コマンドが影響するすべてのクライアントにこの変数を設定しておく必要があります。デフォルト値は 20 秒です。

- **OB2PORTRANGE:** Data Protector がリスンポートを動的に割り当てる際に使用するポート番号の範囲を限定します。通常このオプションは、ファイアウォール越しのセル管理を可能にする場合に設定します。ファイアウォールは別途構成する必要があり、また、このオプションで指定したポート範囲は `Inet` リスンポートには影響しない点に注意してください。
- **OB2PORTRANGESPEC:** 指定した Data Protector プロセスで使用するポート番号の範囲を限定します。ファイアウォールは別途構成する必要があり、また、このオプションで指定したポート範囲は `Inet` リスンポートには影響しない点に注意してください。

  ポート範囲の構成例については、『HP Data Protector ヘルプ』の索引キーワード「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。
- **AMS_ACQUIRE_RELEASE_TIMEOUT=s** スマートコピーのターゲットテープのロードおよびアンロード時のタイムアウトを設定します。指定時間を超えると、操作が中止されます。デフォルト値は 900 秒です。
- **AMS_POSITION_TIMEOUT=s** スマートコピーのターゲットテープの位置決め時のタイムアウトを設定します。この値は、ヘッダーの読み書き時の位置決め時間（短時間で完了）に加え、書き込み後にテープを巻き戻す時間 (かなりの時間が必要となる可能性あり) も含みます。指定時間を超えると、操作が中止されます。デフォルト値は 900 秒です。
- **AMS_SCAN_FORMAT_TIMEOUT=s** スマートコピーのターゲットテープに対するヘッダーの読み書き時のタイムアウトを設定します。指定時間を超えると、操作が中止されます。デフォルト値は 60 秒です。
- **AMS_COPY_TIMEOUT=s** スマートコピー操作のタイムアウトを設定します。指定時間を超えると、操作が中止されます。デフォルト値は 8400 秒です。
- **AMS_ENUM_SLOTS_TIMEOUT=s** スマートコピーのプールおよびスロットのリストを VLS から取得する際のタイムアウトを設定します。指定時間を超えると、操作が中止されます。デフォルト値は 600 秒です。

  このタイムアウトは、VLS がリスト要求を受け取ってから応答を送信するまでの時間を問題にしていることに注意してください。VLS への接続時間は含まれていません。

2 ネットワーキングと通信のトラブルシューティング

ホスト名の解決に関する問題

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。

通信を成功させるには、ホスト B の完全修復ドメイン名 (FQDN) が、ホスト A で解決される必要があります。ホストの解決とは、ホスト A がホスト B の FQDN を解釈し、その IP アドレスを特定することを意味します。

ホスト名の解決では、少なくとも以下の要件を満たす必要があります。

- 各クライアントで、Cell Manager のアドレスおよび Media Agent がインストールされているクライアントのアドレスを解決できること。
- Cell Manager がセル内のすべてのクライアントの名前を解決できること。
- MoM サーバーを使用する場合は、さらに MoM サーバーが MoM 環境内のすべての Cell Manager の名前を解決できること。

TCP/IP 設定をチェックする

TCP/IP プロトコルのインストールが完了したら、`ping` および `ipconfig` ユーティリティを使用するか (Windows)、`ifconfig` ユーティリティを使用して (UNIX)、TCP/IP 構成を検証できます。

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。

DNS の名前解決のテスト

次のコマンドを実行して、ホスト間の DNS の名前解決をテストします。

```
omnicheck -dns
```

このコマンドは、通常の Data Protector 操作に必要なすべての DNS 接続を確認します。

このコマンドの詳細については、『HP Data Protector ヘルプ』の索引キーワード、「DNS 設定のチェック」と、`omnicheck` の man ページを参照してください。

問題

接続したシステムがそれ自体の名前としてクライアント X を返す

`omnicheck` コマンドを実行した結果、以下の応答がありました。

`client_1` 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。

このメッセージは、*`client_1`* の `hosts` ファイルが正しく構成されていないか、*`client_2`* のホスト名が DNS 名と一致していない場合に出力されます。

対処方法

ネットワーク管理者に問い合わせてください。ユーザーの環境が名称解決の実行に対してどのように構成されているかによって異なりますが、この問題は、お使いの DNS 構成の中で解決するか、または以下のディレクトリにある影響を受けるクライアント上の `hosts` ファイルを編集するか、どちらかの方法で解決する必要があります。

Windows システムの場合: *`%SystemRoot%`*`\System32\drivers\etc`

UNIX システムの場合: `/etc`

問題

クライアント A がクライアント B への接続に失敗する

omnicheck コマンドを実行した結果、以下の応答がありました。

client_1 から *client_2* に接続できません。

このメッセージは、*client_1* の hosts ファイルが正しく構成されていないか、*client_2* にアクセスできない (接続されていないなど) 場合に出力されます。

対処方法

hosts ファイルを正しく構成するか、または切断されたシステムを接続します。

問題

クライアント X に接続できない

omnicheck コマンドを実行した結果、以下の応答がありました。

client_1 が *client_2* に接続できません。

これは、パケットは送信されたがタイムアウトのため受信されていないことを示します。

対処方法

リモートホスト上でネットワークの問題が発生していないかをチェックして解決します。

セル内の時刻設定のチェック

Data Protector では、さまざまなセルコンポーネント (Cell Manager、クライアント) 間の通信に、タイムスタンプが広範に使用されます。Cell Manager とクライアント上のシステムクロックが数週間や数ヶ月単位で大幅に異なる場合 (テスト用に設定を変更した場合や、仮想マシンの復元後にシステムクロックを更新しなかった場合など)、通信エラー、バックアップの検索や復元の失敗などの予期しない結果が発生する場合があります。

システム時刻設定をチェックして、システムクロックが大幅に異ならないようにしてください。

Novell Open Enterprise Server (OES) の問題

問題

Target Service Agent (TSA) がロードされていない

NSS ボリュームや NSS クラスターボリュームのバックアップまたは復元のセッションに失敗し、以下のメッセージが表示されます。

```
From:VRDA@computer.company.com
"/media/nss/NSS_VOLUME_5"
SMDR: The TSA must be loaded.
```

TSA がロードされていない場合、バックアップセッションまたは復元セッションは実行できません。

対処方法

現在の作業ディレクトリを/opt/novell/sms/bin に変更し、以下のコマンドを実行します。

```
./smdrd.
```

ファイルシステムコンポーネント tsafs 用の以下の TSA がロードされていることを確認します。

```
./smsconfig -t
```

問題

TSA ログインが拒否される

以下のメッセージが表示されます。

```
From:VRDA@computer.company.com
"/media/nss/NSS_VOLUME_5"
TSA: Cannot connect to Target Service (login denied).
```

対処方法

正しいユーザーの証明書で HPLOGIN ユーティリティ `/usr/omni/bin/hplogin` を実行します。

問題

圧縮された NetWare Traditional File System ボリュームから非圧縮 Novell Storage Services (NSS) ボリュームへの復元に失敗する

NetWare システム上の圧縮された NetWare Traditional File System から、OES Linus システム上の非圧縮 NSS ボリュームへのデータの復元は行えません。このようなセッションを実行しようとすると、以下のメッセージが表示されます。

```
From:VRDA@computer.company.com
"/media/nss/NSS_COMPRESSED"
TSA: Attempted to put compressed data on a non-compressed volume.
```

対処方法

圧縮された NetWare Traditional ボリュームにデータを復元し、GUI で **[Uncompress NetWare compressed files]** オプションを選択するか、`omnirc` 変数の `OB2NWUNCOMPRESS` を `1` に設定して、再度バックアップします。非圧縮の状態でファイルがバックアップされたら、OES Linux システムの NSS ボリュームでこれらを復元します。

その他の問題

問題

「接続はピアによってリセットされました」というメッセージを伴うクライアントの障害

Windows システムで TCP/IP プロトコルの構成パラメータがデフォルトの場合、接続に問題が発生することがあります。このような状態の原因としては、ネットワークまたはコンピュータの負荷が高いこと、ネットワークの信頼性が低いことが考えられ、特に異なるオペレーティングシステムに接続する場合に発生しがちです。以下のエラーが報告されます。

```
[10054] 接続はピアによってリセットされました。
```

対処方法

TCP/IP プロトコルを構成して、再送数をデフォルトの 5 から 8 に変更します。1 増加するごとにタイムアウトが 2 倍になるため、これ以上高い値を使用することはお勧めできません。この設定は、Data Protector が使用する接続だけでなく、すべてのネットワーク接続に適用されることに注意してください。

Windows の場合、この変更をまず Cell Manager システムに適用します。

Cell Manager を Windows システムで実行している場合は、この変更をまず Cell Manager システムに適用します。上記の手順を行っても問題が解決しないか、Cell Manager を UNIX システムで実行している場合は、問題が発生しているすべての Windows クライアントに変更を適用します。

1. 以下のレジストリキーで、DWORD パラメータ TcpMaxDataRetransmissions を追加して、値を 0x00000008(8) に設定します。

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

2. システムを再起動します。

△ **注意:** レジストリを誤って編集すると、システムが不安定になったり、使用できなくなったりする場合があります。

問題

「このクライアントは、どのセルのメンバでもありません。」というメッセージが表示されて、クライアントが異常終了する

クライアントに対して Data Protector の操作を実行したが、そのクライアント上で Cell Manager 情報が見つからない。次のエラーが表示されて、操作が失敗する。

このクライアントは、どのセルのメンバーでもありません。

対処方法

- 問題のクライアントが Data Protector GUI の [クライアント] コンテキストに一覧表示されている場合は、以下の操作を実行します。
  1. [クライアント] コンテキスト内で [クライアント] を展開して問題のクライアントを右クリックし、[削除] を選択します。
  2. クライアントから Data Protector もアンインストールするかどうかをたずねるダイアログが表示されます。[いいえ] をクリックします。
  3. [クライアント] を右クリックし、[クライアントのインポート] を選択します。
  4. クライアントを指定して [完了] をクリックします。
- 問題のクライアントが Data Protector GUI の [クライアント] コンテキストに一覧表示されていない場合は、以下の操作を実行します。
  1. [クライアント] コンテキスト内で [クライアント] を右クリックし、[クライアントのインポート] を選択します。
  2. クライアントを指定して [完了] をクリックします。

問題

inet.log ファイルに過剰なログが記録される

クライアントが保護されていない場合に、Cell Manager が MC/ServiceGuard 環境に構成されているか、複数の名前または IP アドレスを持っていると、inet.log ファイルに次の種類のエントリが大量に記録される可能性があります。

```
A request 3 (vbda.exe) came from host computer.company.com which is not a cell manager of this client.
```

これは、保護されていないクライアントでは、Cell Manager のプライマリホスト名しか認識できないことが原因です。他のホストからの要求も受け付けられますが、要求は inet.log ファイルに記録されます。

対処方法

クライアントに保護を設定してください。その手順については、『HP Data Protector ヘルプ』の索引キーワード「クライアントシステムの保護」で表示される内容を参照してください。

allow_hosts ファイルのリストにあるクライアントからの要求は、inet.log に記録されなくなります。他のクライアントからの要求は拒否されます。

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。この場合、クライア

ントはすべてのシステム (すべての IP アドレス) からの要求を受け付けるため、実際には保護されていないことになりますが、大量のログが記録される状況は回避できます。

重要: セキュリティ保護された各クライアント上の `allow_hosts` ファイルには、Cell Manager ノードが使用する可能性があるすべてのホスト名を記述しておく必要があります。これにより、フェイルオーバーの発生時にもクライアントへのアクセスが可能になります。クライアントを誤ってロックアウトしてしまった場合は、そのクライアント上の `allow_hosts` ファイルを手動で編集できます。詳細については、『HP Data Protector ヘルプ』の索引キーワード「クライアントシステム、セキュリティ」で表示される内容を参照してください。

3 Data Protector のサービスおよびデーモンのトラブルシューティング

概要

Data Protector のサービス (Windows) およびデーモン (UNIX) は Cell Manager 上で動作します。サービス/デーモンが実行されているかどうかを確認するには、`omnisv -status` コマンドを実行します。

Data Protector サービス/デーモンが停止していると思われる場合や、Data Protector ターゲットクライアント上にインストールされていない場合は、名前解決に関する問題が発生していないかをまず確認します。詳細は、「ネットワーキングと通信のトラブルシューティング」(23 ページ) を参照してください。

Data Protector のプロセス

「各種処理中に実行される Data Protector プロセス」(28 ページ) は、Data Protector の待機中や、バックアップ、復元、メディア管理セッションなどの基本処理が行われるときに、どのプロセスが実行されるかを示しています。

表 4 各種処理中に実行される Data Protector プロセス

		常時	バックアップ	復元	メディア管理

Cell Manager	Windows	`OmniInet.exe`
		`rds.exe`
		`mmd.exe`
		`crs.exe`
		`uiproxy.exe`
		`kms.exe`
			`bsm.exe`	`rsm.exe`	`msm.exe`

	UNIX	`rds`
		`mmd`
		`crs`
		`uiproxyd`
		`kms`
			`bsm`	`rsm`	`msm`

Disk Agent クライアント	Windows	`OmniInet.exe`	`vbda.exe`	`vrda.exe`	
	UNIX		`vbda`	`vrda`	
Media Agent クライアント	Windows	`OmniInet.exe`	`bma.exe`	`rma.exe`	`mma.exe`
	UNIX		`bma`	`rma`	`mma`

Data Protector のサービスを Windows で起動する際の問題

問題

サービスを起動するためのパーミッションがない

以下のエラーが表示されます。

`System_Name` で *`Service_Name`* を開始できませんでした。

アクセスが拒否されました。

対処方法

システム管理者が、管理対象のシステム上で、このユーザーに対してサービスを起動、終了、変更するパーミッションを設定する必要があります。

問題

変更されたサービスアカウントのプロパティ

サービスアカウントにサービスを起動するためのパーミッションがない場合、またはサービスアカウントのプロパティ (パスワードなど) が変更されている場合、以下のエラーが表示されます。

以下のエラーのため、Data Protector Inet サービスを開始できませんでした。

ログインに失敗したため、サービスを起動できませんでした。

対処方法

1. Windows の [コントロールパネル] → [管理ツール] → [サービス] の順にクリックし、サービスのパラメータを変更します。
2. 上記を行っても問題が解決しない場合は、システム管理者に連絡して、適切なパーミッションを持つアカウントを設定するよう依頼してください。Admin グループのメンバーで、[サービスとしてログオン] というユーザー権限を持つアカウントを作成する必要があります。

問題

指定したサービスが見つからない

サービスの場所は、ImagePath レジストリキーに登録されています。このキーで指定された場所に実行可能ファイルが存在しない場合は、次のエラーが表示されます。

System_Name で *Service_Name* を開始できませんでした。指定されたファイルが見つかりません。

対処方法

IDB を保持したまま、Cell Manager に Data Protector を再インストールします。その手順については、「問題」 (61 ページ) を参照してください。

問題

CRS サービスを起動すると MMD が異常終了する

Data Protector CRS サービスが起動に失敗し、mmd.exe により診断ツール **[ワトソン博士]** が起動された場合は、データベースログファイルが破損していることが考えられます。

対処方法

1. Data_Protector_home\tmp ディレクトリ内の mmd.ctx ファイルを削除します。
2. omnisv -start コマンドを使ってサービスを再起動します。

問題

Windows TSE Cell Manager 上で RDS が動作しない

対処方法

Data_Protector_home\db40\datafiles\catalog\rdmserver.ini ファイルを変更して、ローカル転送の代わりに TCP 転送を使用します。TCP Configuration という部分で、Enabled を yes に設定します。

Data Protector のデーモンを UNIX で起動する際の問題

UNIX Cell Manager では以下のデーモンが実行されます。

- ディレクトリ /opt/omni/lbin:
  - Data Protector CRS デーモン: crs
  - Data Protector IDB デーモン: rds

    - Data Protector メディア管理デーモン: `mmd`
- ディレクトリ`/opt/omni/java/server/bin`:
    - Data Protector ユーザーインタフェースプロキシーデーモン: `uiproxyd`

通常、これらのデーモンはシステムの起動時に自動的に起動します。

Data Protector `Inet` プロセス (`/opt/omni/lbin/inet`) は、アプリケーションが Data Protector ポート (デフォルトのポートは 5555) へ接続しようとした場合にシステムの inet デーモンによって起動されます。

Data Protector の各デーモンに対して、手動による開始と停止およびステータスのチェックを行うには、`root` として Cell Manager にログインし、`/opt/omni/sbin` ディレクトリから次のコマンドを実行します。

- `omnisv -stop`
- `omnisv -start`
- `omnisv -status`

問題

Raima Velocis サーバーデーモンを起動できなかった

`omnisv -start` コマンドによって、次のようなメッセージが出力されます。

`Raima Velocis` サーバーのデーモンを起動できませんでした。

対処方法

`/var/opt/omni/server/db40/datafiles/catalog/RDS.log` で詳細を確認します。

すべての IDB ファイルが`/var/opt/omni/server/db40` ディレクトリにあるかどうかを確認します。ファイルのリストを`/opt/omni/newconfig/var/opt/omni/server/db40` 内のファイルのリストと比較します。これらのディレクトリがマウントされていることを確認します。

問題

Raima Velocis サーバーデーモンが実行されていないように見える

Data Protector コマンドが、以下のエラーで強制終了します。

`[12:1166] Velocis` デーモンのエラー - このデーモンは実行されていない可能性があります。

対処方法

`omnisv -status` コマンドを使って、データベースサーバーが実際に動作を停止しているかどうかをチェックします。

- データベースサーバーが実際に動作を停止している場合は、`omnisv -start` コマンドを使ってデータベースサーバーを起動します。
- データベースサーバーが実行されている場合は、`/var/opt/omni/server/db40` ディレクトリが存在しないか、一部のファイルが不足しています。これは、ディレクトリまたはファイルが誤って削除されたことが原因です。IDB を回復します。詳細は、『HP Data Protector ヘルプ』の索引キーワード「IDB の復旧」を参照してください。

問題

Data Protector Cell Manager デーモンを起動できなかった

`omnisv -start` コマンドによって、次のようなメッセージが出力されます。

`Cell Manager` デーモンを起動できませんでした。

対処方法

詳細については、/var/opt/omni/tmp/omni_start.log を参照してください。

以下の構成ファイルが存在することを確認します。

- /etc/opt/omni/server/options/global
- /etc/opt/omni/server/options/users/UserList
- /etc/opt/omni/server/options/ClassSpec

Data Protector プロセスの他の問題

問題

マルチプロセッサ HP-UX システムで RDS デーモンの CPU 使用率が高すぎる

Itanium(IA-64) マルチプロセッサアーキテクチャで実行されている HP-UX Cell Manager において、Data Protector 内部データベース (IDB) でアクティビティがない場合でも RDS デーモンの CPU 使用率が非常に高いままになります。

対処方法

1. 問題が発生した Cell Manager に、以下のオペレーティングシステムパッチをインストールします。
   - PHCO_37477(HP-UX 11.31 システム)
2. 同じシステムで、omnirc 変数を次のように構成します。

   ```
   PTHREAD_MUTEX_SPINVAL=old
   PTHREAD_COMPAT_MODE=1
   ```
3. omnisv -stop コマンドおよび omnisv -start コマンドを使用して、Data Protector デーモンを再起動します。

問題

Data Protector のパフォーマンスが、Red Hat Enterprise Linux 環境では、他のオペレーティングシステム環境に比べて低下する

Name Server Caching(nscd) デーモンが無効になると、Red Hat Enterprise Linux (RHEL) 上の Data Protector のパフォーマンスに悪影響を及ぼすことがあります。

対処方法

RHEL 上で Name Server Caching を有効にするか、ローカル DNS に切り替えてから、omnisv -start コマンドを実行します。

問題

バックアップの実行中、一定時間経過後にバックアップセッションが停止し、BSM が応答しなくなる

この問題は、ファイアウォールがアクティブではない接続を閉じたことにより発生する場合があります。

対処方法

接続をアクティブに保ち、ファイアウォールがその接続を閉じないようにします。以下の omnirc 変数をエクスポート/設定します。

```
OB2IPCKEEPALIVE=1
OB2IPCKEEPALIVETIME=number_of_seconds
OB2IPCKEEPALIVEINTERVAL=number_of_seconds
```

OB2IPCKEEPALIVETIME には、非アクティブな接続の猶予時間を指定します。この時間を超過すると、最初の keep-alive パケットが送信されます。OB2IPCKEEPALIVEINTERVAL には、ACK を受信しない場合に次の keep-alive パケットを送信するまでの間隔を指定します。

この変数は Cell Manager システムで設定する必要があります。

4 ユーザーインタフェースに関するトラブルシューティング

ユーザーインタフェースの起動に関する問題

Data Protector ユーザーインタフェースの起動に関する問題が発生する原因は、通常、サービスが実行されていない、サービスがインストールされていない、または、ネットワーク通信の問題が発生しているの、いずれかです。

問題

Cell Manager 上で Inet が応答しない

以下のメッセージが表示されます。

`Cell Manager システムにアクセスできません（inet が応答しません）。Cell Manager ホストと通信できない、Cell Manager が動作していない、または Cell Manager に Data Protector ソフトウェアがインストールまたは構成されていません。`

対処方法

システム間の通信に問題がない場合は、`telnet` を使ってソフトウェアがインストールされているかチェックしてください。

一部のコンポーネントが正しくインストールされていないことが考えられます。『HP Data Protector インストールおよびライセンスガイド』を参照し、インストール手順を確認してください。

インストールに問題がない場合は、`omnisv -status` コマンドを実行して、Cell Manager 上でサービスが正常に実行されているかチェックしてください。

Java GUI を使用している場合は、Java GUI サーバーが動作しているかどうかをチェックしてください。Java GUIサーバーが応答しなくなったを参照してください。

問題

Java GUI サーバーが応答しなくなった

対処方法

- Data Protector `UIProxy` サービスがシステム上で実行されていない場合は、`omnisv -start` コマンドを実行して、サービスを起動します。
- サービスが Cell Manager 上で正常に稼動しているかどうかを確認するには、`omnisv -status` コマンドを実行します。

問題

Cell Manager にアクセスする権限がない

以下のメッセージが表示されます。

`Data Protector 管理者によって、ユーザー権限が Data Protector の機能にアクセスできないように設定されています。`

`詳細は Data Protector 管理者に問い合わせてください。`

対処方法

Data Protector 管理者に、ユーザーとして追加することと、セル内での適切なユーザー権限の付与を要請します。ユーザーグループの構成方法については、『HP Data Protector ヘルプ』の索引キーワード「ユーザーグループ」で表示される内容を参照してください。

問題

リモートシステムへの接続が拒否される

Windows または Novell NetWare で `telnet hostname 5555` コマンドを実行すると、「接続が拒否されました」というメッセージが返されます。

対処方法

- Data Protector `Inet` サービスがリモートシステム上で実行されていない場合は、`omnisv -start` コマンドを実行して、サービスを起動します。
- Data Protector がリモートシステム上にインストールされていない場合は、インストールします。

問題

Java GUI がデフォルトの Cell Manager に自動的に接続されない

64 ビット版の Windows システムで 32 ビット版の Windows の Java が使用されている場合、Java GUI はデフォルトの Cell Manager に自動的に接続されません。**[Cell Manager** へ接続**]** ダイアログボックスで Cell Manager の名前を指定する必要があります。

対処方法

サポートされているバージョンの Java ランタイムクライアントをインストールして使用してください。『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』、または http://support.openview.hp.com/selfsolve/manuals にある最新のサポート一覧を参照してください。

問題

[スタート] メニューのショートカットをクリックしても、Java GUI が起動しない

Data Protector をインストールし、[スタート] メニューのショートカットを使用して Java GUI を起動すると、以下のメッセージが表示されます。

ファイル `javaw` が見つかりません。

これは、Java Runtime Environment(JRE) がシステムにインストールされていないか、システム環境変数 Path が JRE がインストールされているディレクトリに正しく設定されていない場合に発生します。

対処方法

1. サポートされているバージョンの Java ランタイムクライアントをインストールしてください。『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』、または http://support.openview.hp.com/selfsolve/manuals にある最新のサポート一覧を参照してください。
2. 環境変数 `DP_JAVA_DIR` を JRE がインストールされているディレクトリに設定するか、`java.exe` があるディレクトリがシステム環境変数 Path に含まれるようにします。たとえば、`DP_JAVA_DIR` を `C:\Program Files\Java\jre1.5.0_07\bin` に設定します。

表示に関する問題

問題

UNIX 上の Data Protector GUI で GUI オブジェクトの名前が正常に表示されない

UNIX 上の Data Protector GUI で、GUI オブジェクト（バックアップデバイスやバックアップ仕様など）の名前が正常に表示されないことがあります。

これらの GUI オブジェクトが特定のロケールで作成されている場合、他のロケールで表示すると正しく表示されないことがあります。GUI オブジェクト名が正しく表示されていなくても、その GUI オブジェクトは使用可能です。

たとえば、バックアップデバイスを構成し、非 ASCII 文字を含んだ名前を付けたとします。この場合、GUI が ASCII のみを使用するロケールで稼動していると、その名前は正しく表示されないことがあります。GUI に名前が正しく表示されなくても、このデバイスを使用してバックアップや復元を実行できます。

対処方法

それらのオブジェクトを、UTF-8 エンコードを使用するロケールで作成し直すか、Data Protector GUI が実行されているシステムの従来のロケールをそのまま使用してください。ただし、後者の場合は、GUI でエンコードを切り替えることはできず、従って Data Protector の国際化機能も使用できません。

5 デバイスとメディアのトラブルシューティング

デバイスおよびメディアに関する全般的な問題

バックアップデバイスには、専用の Data Protector ライセンスが必要です。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』を参照してください。

デバイスの SCSI アドレスに関する問題の詳細については、『HP Data Protector インストールおよびライセンスガイド』の付録 B を参照してください。

問題

Windows 上でエクスチェンジャ制御デバイスにアクセスできない

Data Protector は SCSI ミニポートドライバを使って、バックアップドライブとライブラリを制御します。他のデバイスのドライバが同じシステムにロードされている場合、Data Protector はこれらのデバイスを管理できない場合があります。この場合、デバイスの操作 (メディアのフォーマット、またはスキャンなど) を開始した時点で、以下のエラーメッセージが表示されます。

```
Cannot access exchanger control device
```

対処方法

デバイスが置かれているシステム上で次のコマンドを実行して、システム上で構成されているすべての物理デバイスのリストを表示します。

```
Data_Protector_home\bin\devbra -dev
```

SCSI アドレスのいずれかのステータスが CLAIMED の場合、その SCSI アドレスは別のデバイスドライバが使用中です。

Windows のロボティクスドライバを無効にします。その手順については、『HP Data Protector ヘルプ』の索引キーワード「ロボティクスドライバ」で表示される内容を参照してください。

問題

SCSI デバイスがロックされたままで、セッションが失敗

SCSI の予約操作または予約解除操作が不完全なため、SCSI ドライブまたはロボティクス制御がロックされたままです。以下のメッセージが表示されます。

デバイスをオープンできません。

Media Agent で障害が発生した場合、予約されたデバイスを再び解放することはできません。Data Protector は SCSI ドライブまたはロボティクス制御のロックの解除に失敗している可能性があります。以降のセッションでそれを使用することはできません。

対処方法

このデバイスを使用している他のアプリケーションがないことを確認してください。SCSI ドライブまたは SCSI ロボティクス制御をアンロックするには、デバイスの電源を切り、入れ直す必要があります。

問題

デバイスのオープンに関する問題

DDS デバイスを使おうとすると、次のエラーメッセージが表示されます。

デバイスを開くことができません。(オーナーではありません)

対処方法

Media Recognition System(メディア認識システム) と互換性のないメディアを使用していないかチェックしてください。DDS ドライブで使用するメディアは Media Recognition System と互換性がなければなりません。

問題

Windows 上でサポートされていない SCSI HBA/FC HBA の使用

バックアップデバイスで、サポートされていない SCSI HBA/FC HBA を使用すると、システムエラーが発生します。

問題が発生するのは、主に複数の Media Agent が同時に SCSI デバイスにアクセスした場合、またはデバイスのブロックサイズによって定義されている転送データの長さが SCSI HBA/FC HBA のサポートするデータ長を上回った場合です。

対処方法

デバイスのブロックサイズは、変更可能です。その手順については、『HP Data Protector ヘルプ』の索引キーワード「デバイスとメディアの拡張オプションの設定」で表示される内容を参照してください。

サポート対象の SCSI HBA/FC HBA 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。

問題

ライブラリ再構成の失敗

デバイスリストの変更後、`sanconf` コマンドで既存のライブラリ構成を変更しようとすると、構成エラーが報告されます。ライブラリ構成は一部しか作成されません。

対処方法

SAN 環境内のホストのリストを再利用し、`sanconf` コマンドで再度ホストをスキャンすることで、従来のライブラリ構成を復旧できます。 復旧後、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、セル内のホストをスキャンします。

   ```
   sanconf -list_devices mySAN.txt -hostsfile hosts.txt
   ```

2. 保存した構成ファイルを使用してライブラリを構成します。次のコマンドを実行してください。

   ```
   sanconf -configure mySAN.txt -library LibrarySerialNumber LibraryName
   [RoboticControlHostName] [DeviceTypeNumber] -hostsfile hosts.txt
   ```

   正常動作していた従来のライブラリ構成が自動的に復旧されます。

後でライブラリを追加、削除、変更する際に `sanconf` コマンドによるライブラリ構成に失敗した場合は、上記の手順を実行すれば正常な構成に戻すことができます。

問題

読み込み操作後または書き込み操作後に、暗号化されたメディアに不良 (Poor) マークが付加される

ドライブベースの暗号化を使用して書き込まれたメディアで読み取りまたは書き込み操作を行っているとき、セッションが失敗してメディアが自動的に不良とマークされます。以下のエラーが表示されます。

```
Cannot read from device ([5] I/O error)
```

このエラーは、ドライブベースの暗号化をサポートしていないプラットフォームで読み込み操作または書き込み操作が実行された場合に発生します。メディア品質には影響しません。サポートされるプラットフォームの最新リストについては、http://support.openview.hp.com/selfsolve/manuals にある最新サポート一覧を参照してください。

対処方法

メディア状態のステータスを修正するには、`omnimm -reset_poor_medium` オプションを使用してメディア状態をリセットします。詳細については、`omnimm` の man ページまたは『HP Data Protector Command Line Interface Reference』を参照してください。

問題

メディアに関するさまざまな問題

対処方法

メディア品質統計機能を使うと、メディアに関する問題を早期の段階で検出できます。

各メディアがドライブから取り出される前に、Data Protector は `SCSI log sense` コマンドを発行して、メディアの読み込み/書き込みに関する統計情報を照会します。この情報は `media.log` ファイルに書き込まれます。

メディア品質統計機能はデフォルトでは無効になっています。有効にするには、グローバルオプション `Ob2TapeStatistics` を `1` に設定します。その手順については、「グローバルオプション」 (18 ページ) を参照してください。

書込み操作中にメディア関連のエラーが表示された場合、またはメディアが「不良」とマークされた場合は、`media.log` ファイルでメディアのエラー統計を確認できます。

`Media.log` ファイルには以下のエラー統計が書き込まれます。 ここでは、*n* はエラー数です。

表 5 メディアエラー統計

エラー統計	説明
`errsubdel=`*n*	大幅な遅延後に修正されたエラーの数
`errposdel=`*n*	ある程度の遅延をもって修正されたエラーの数
`total=`*n*	再書き込みの合計回数
`toterrcorr=`*n*	書き込み中に修正および回復されたエラーの合計数
`totcorralgproc=`*n*	修正アルゴリズムの処理時間の合計
`totb=`*n*	書き込み処理したバイト数の合計
`totuncorrerr=`*n*	未修正のエラー (書き込み) の合計数

パラメータの値が`-1` の場合は、デバイスがその統計パラメータをサポートしていないことを表します。すべてのパラメータの値が`-1` の場合は、テープ品質統計の処理中にエラーが発生したか、デバイスがメディア品質統計をサポートしていないかのどちらかです。

テープの統計結果は、[処理したバイト数の合計] にバイト数でレポートされます。しかし、LTO デバイスについては、バイト単位ではなくデータセット単位で、DDS デバイスについてはグループ単位で、それぞれレポートされます。

例

以下に、`media.log` ファイルの内容の例をいくつか示します。

- DLT/SDLT デバイスに関する Log sense 書き込みレポート – 処理されたバイト数の合計

  ```
  Media ID from tape= 0fa003bd:3e00dbb4:2310:0001; Medium Label= DLT10;
  Logical drive= dlt1; Errors corrected no delay= 0; Errors corrected
  delay= 0; Total= 13639; Total errors corrected= 13639; Total correction
  algorithm processed= 0; Total bytes processed= 46774780560; Total
  uncorrected errors= 0
  ```

  46774780560 バイト (圧縮後) のネイティブデータが処理されました (DLT8000 テープ全体)。

- LTO デバイスに関する Log sense 書き込みレポート – 処理されたデータセット数の合計

```
Media ID from tape=0fa003bd:3e0057e6:05b7:0001; Medium Label= ULT2;
Logical drive=ultrium1; Errors corrected no delay= 0; Errors corrected
delay= 0; Total= 0;Total errors corrected= 0; Total correction algorithm
processed= 0; Total bytes processed= 47246; Total uncorrected errors= 0
```

1 つのデータセットのサイズは 404352 バイトです。処理されたバイト数の合計を計算するには、以下の公式を使用します。

47246データセット * 404352バイト = 19104014592バイト(テープ全体を圧縮後)

- DDS デバイスに関する Log sense 書き込みレポート − 処理されたグループ数の合計

```
Media ID from tape= 0fa0049f:3df881e9:41f3:0001;
Medium Label= Default DDS_5; Logical drive= DDS;
Errors corrected no delay= -1; Errors corrected delay= -1;
Total= -1; Total errors corrected= 0; Total correction algorithm
processed= 154; Total bytes processed= 2244; Total uncorrected errors= 0
```

DDS1/2: 1 グループは 126632 バイトです。

DDS3/4: 1 グループは 384296 バイトです。

処理されたバイト数の合計を計算するには、以下の公式を使用します。

2244グループ* 126632バイト = 284162208バイト(圧縮後)(DDS2上での359 MBのバックアップ)

359MB のデータがバックアップされ、テープ上に 271MB のネイティブデータが書き込まれました。

問題

メディアヘッダーのサニティチェックエラー

Data Protector のデフォルト動作では、メディアがドライブから取り出される前にメディアヘッダーのサニティチェックが実行されます。

メディアヘッダーのサニティーチェックでメディアヘッダーの整合性エラーが検出された場合は、エラーメッセージが表示され、メディア上のすべてのオブジェクトに失敗のマークが付けられます。

メディアヘッダーが破損していた場合、そのメディア上のすべてのオブジェクトに失敗のマークが付けられ、メディアには不良のマークが付けられます。

対処方法

IDB からメディアをエクスポートし、別のメディアを使用して失敗したセッションを再起動します。

問題

Data Protector 7.00 へのアップグレード後にデバイスを使用できない

Data Protector 7.00 にアップグレードした後、従来のリリースでは別の種類のデバイスとして構成されていたデバイスが使用できない。たとえば、9840 デバイスとして構成されていた 9940 デバイスを使用できない、3590 デバイスとして構成されていた 3592 デバイスを使用できない、DLT デバイスとして構成されていた SuperDLT デバイスを使用できない、などです。以下のエラーが表示されます。

```
[危険域] 場所: BMA@computer.company.com "SDLT" Time:
5/22/2006 5:12:34 PM
[90:43] /dev/rmt/1m
```

指定された物理デバイスの種類は無効です => 中止しています

対処方法

Cell Manager の以下のディレクトリにある `mchange` コマンドを使用して、手作業でこれらのデバイスを再構成します。

Windows システムの場合: `Data_Protector_home\bin\utilns\NT`

HP-UX システムの場合: `/opt/omni/sbin/utilns/HPUX`

Solaris システムの場合: `/opt/omni/sbin/utilns/SOL`

`mchange -pool` *`PoolName`* `-newtype` *`NewMediaClass`*

内容は以下のとおりです。

`PoolName` は、現在構成されているデバイスが使用していて再構成が必要なメディアプールの名前です (Default DLT、Default T3590、Default T9840 など)。

`NewMediaClass` は、デバイスに対する新しいメディアの種類です。例えば、9940 デバイスの場合は T9940、3590 デバイスの場合は T3592 、SuperDLT デバイスの場合は SuperDLT と表記します。

例

```
mchange -pool "Default DLT" -newtype "SuperDLT"
```

このコマンドは、指定したメディアプールを使用するすべてのメディア、ドライブ、ライブラリに対するメディアの種類を変更します。

変更すべき各デバイスに対してこのコマンドを実行し終えたら、再構成したデバイスに関連付けられているメディアを現在のメディアプールから、それらのメディアに対応するメディアプールに移動する必要があります。たとえば、再構成した 9940 デバイスに関連付けられているメディアは Default T9940 メディアプールに移動します。その手順については、『HP Data Protector ヘルプ』の索引キーワード「メディアの移動」で表示される内容を参照してください。

問題

デバイスのシリアル番号に関する問題

問題があるバックアップデバイスやロボティクスに対して何らかの操作 (バックアップ、復元、フォーマット、スキャンなど) を実行すると、以下のエラーが表示されます。

デバイス *`DeviceName`* を開くことができませんでした（シリアル番号が変更されています）。

このエラーは、デバイスパスで指定しているデバイスのシリアル番号が IDB に格納されている番号とは異なる場合に報告されます。この状況は、以下の場合に発生します。

- デバイスを正しく構成していない場合 (たとえば `omniupload` コマンドの使用時など、またはデバイスファイルの構成が正しくない)。
- 物理デバイスを交換したときに、対応する論理デバイスの更新 (新しいシリアル番号の再ロード) をしなかった場合。
- SCSI ライブラリにある SCSI テープドライブを物理的に置き換えました。[変更された **SCSI** アドレスの自動検出] オプションが有効ではないか、omnirc 変数 `OB2MADETECTDRIVESWAP` が `0` に設定されています。
- マルチパスデバイス内のパスを正しく構成していない場合。

対処方法

1. Data Protector GUI で、[デバイス/メディア] コンテキストを選択します。
2. Scoping ペインで [デバイス] を展開して問題のデバイスを右クリックし、[プロパティ] をクリックします。
3. [コントロール] タブをクリックし、[変更された **SCSI** アドレスの自動検出] オプションを有効にします。
4. [再読み込み] をクリックして IDB 内のデバイスシリアル番号を更新します。

   SCSI ライブラリ内にある SCSI テープ ドライブを物理的に交換する場合は、omnirc 変数 `OB2MADETECTDRIVESWAP` が `1`(デフォルト値) に設定されていることを確認します。デバイスシリアル番号を再ロードする必要はありません。

問題

破損データを復元またはコピーできない

デフォルトでは、テープ上で利用可能であれば CRC 値は常にチェックされますが、CRC の不一致により破損していることがわかったデータについては、復元もコピーも行われません。ただし、状況によっては該当データを復元またはコピーすることも可能です。

対処方法

Media Agent ホストで omnirc 変数 `OB2CRCCHECK` を一時的に 0 に設定します。破損したオブジェクト (データ) を復元したら、設定をデフォルト値 (`1`) に戻します。

問題

よく発生するハードウェア関連の問題

対処方法

システムとデバイス間の SCSI 通信 (アダプタ、または SCSI ケーブルとケーブル長など) をチェックします。OS で提供されている `tar` などのコマンドを実行して、システムとドライブが通信していることを検証してください。

ADIC/GRAU DAS ライブラリと STK ACS ライブラリに関する問題

問題

ADIC/GRAU DAS ライブラリのインストール失敗

対処方法

1. GRAU ロボティクス (PC/ロボット) を制御するクライアントに Media Agent をインストールします。
2. ドライブが接続されているクライアント (PC/ドライブ) に Media Agent をインストールします。
3. `aci.dll`、`winrpc.dll`、`ezrpcw32.dll` をディレクトリ `winnt\system32` と *`Data_Protector_home`*`\bin` にコピーします。
4. PC/ロボット上にディレクトリ `aci` を作成します。
5. `dasadmin.exe`、`portmapper`、および `portinst` を `aci` ディレクトリにコピーします。
6. `portinst` を起動して、`portmapper` をインストールします (PC/ロボット上のみ)。
7. Cell Manager に`mmd` パッチをインストールします。
8. システムを再起動します。
9. [コントロールパネル] ウィンドウで [管理ツール] をクリックし、[サービス] をダブルクリックして、`portmapper` サービスと `rpc` サービスが共に稼動しているかどうかをチェックします。
10. GRAU ライブラリ内の OS/2 システムで、`/das/etc/config` ファイルを編集します。PC/ロボットの IP アドレスを含む OMNIBACK という名前のクライアントを追加します。

問題

ドライブが 1 つも表示されない

対処方法

PC/ロボットから以下のコマンドを実行します。

1. `dasadmin listd`
2. `dasadmin all DLT7000 UP` *`AMUCLIENT`*
3. `dasadmin mount` *`VOLSER`*(このコマンドの実行後、ドライブの `UNLOAD` (取出し) ボタンを押す必要があります)。

4. `dasadmin dismount` *`VOLSER`* または `dasadmin dismount -d` *`DRIVENAME`*)

ここで、

- *`AMUCLIENT`* = `OMNIBACK`
- *`VOLSER`*(例: `001565`)
- *`DRIVENAME`*(例: `DLT7001`)
- `"all"`は"allocate"を意味します。

上記のコマンド (DAS Server (OS/2) への通信) が正しく実行されなかった場合は、OS/2 システム上で`/das/bin/`ディレクトリからコマンドをもう一度実行してみてください。

OS/2 システムから上記のコマンドを実行する場合は、*`AMUCLIENT`* `= AMUCLIENT` を使用してください。

1. AMU クライアントにログインします。一般的なログイン名は、以下のとおりです。

   `user: Administrator pwd: administrator`

   `user: Supervisor pwd: supervisor`
2. 必要に応じて、`ACI_MEDIA_TYPE` でメディアの種類を設定します (set `ACI_MEDIA_TYPE=DECDLT`)。
3. ライブラリを再起動します。
   a. OS/2 をシャットダウンして、ロボティクスの電源をオフにします。
   b. OS/2 を再起動します。 OS/2 が起動すると、ロボティクスの使用準備ができていないことを示す AMU ログが表示されます。ロボティクスの電源をオンにします。

問題

GRAU CAP が正しく構成されていない

対処方法

メディアを移動するには、CAP からスロットへ移動した後、デバイスのロボティクスを使ってドライブへ移動する方法しかありません。このとき `import` および `export` コマンドを使用します。例を下に示します。

```
import CAP: I01
import CAP range: I01-I03
export CAP:  E01
export CAP range: E01-E03
```

問題

ライブラリ操作が失敗する

対処方法

Data Protector の `uma` ユーティリティを使って GRAU および STK ライブラリデバイスを管理するには、以下の構文を使用します。

`uma -pol` *`POLNUMBER`* `-ioctl` *`LIBRARYNAME`* `-type` *`MEDIATYPE`*

ここで、*`POLNUMBER`* には、GRAU の場合は `8`、STK の場合は `9` を指定します。

たとえば、次のように入力してください。`uma -pol 8 -ioctl grauamu`

デフォルトのメディアの種類は DLT です。

6 バックアップセッションと復元セッションのトラブルシューティング

増分バックアップの代わりにフルバックアップが実行される

増分バックアップを指定したにもかかわらず、フルバックアップが実行されます。これには 2 つの理由が考えられます。

理由:

前回のフルバックアップがない

オブジェクトの増分バックアップを実行する前に、フルバックアップを実行することが必要です。Data Protector は、どのファイルが変更され、増分バックアップに含める必要があるかを比較するベースとしてフルバックアップを使用します。保護されたフルバックアップがない場合は、フルバックアップが実行されます。

対処方法

そのオブジェクトのフルバックアップが存在し、保護設定されているかどうかを確認します。

理由:

説明を変更した

バックアップオブジェクトは、クライアント、マウントポイント、および説明によって定義されます。これらの値のいずれかが変更された場合、Data Protector はそのオブジェクトを新しいバックアップオブジェクトとみなし、増分バックアップの代わりにフルバックアップを実行します。

対処方法

フルバックアップと増分バックアップの両方に同じ説明を使用します。

理由:

ツリーを変更した

保護されたフルバックアップがすでに存在しますが、増分バックアップとは異なるツリーが含まれています。これには 2 つの理由が考えられます。

- 保護設定されたフルバックアップに関するバックアップ仕様のツリーを変更した。
- 同じバックアップオブジェクトを含んでいるが、バックアップオブジェクトに異なるツリーが指定されている複数のバックアップ仕様を作成した。

対処方法

同一のバックアップオブジェクトに対して複数のバックアップ仕様を作成している場合は、そのバックアップオブジェクトの (自動生成された) 共通説明を変更します。Data Protector はそれらを新しいオブジェクトとみなし、フルバックアップを実行します。フルバックアップの実行後は、増分バックアップが可能になります。

理由:

バックアップオーナーが違う

バックアップをプライベートバックアップとして実行するよう構成されている場合、バックアップを開始したユーザーがデータのオーナーとなります。たとえば、ユーザー A がフルバックアップを実行し、ユーザー B が増分バックアップを開始しようとすると、増分バックアップはフルバックアップとして実行されます。これは、ユーザー A のデータがプライベートバックアップによるデータであり、ユーザー B が増分バックアップを実行する際のベースとしてこのデータを使用できないためです。

ユーザー A がフルバックアップを実行し、次にユーザー B がオブジェクトコピーセッションを実行してオリジナルをエクスポートまたは上書きした場合にも、同じ問題が発生します。この場合、フルバックアップ (コピー) のオーナーはユーザー B に変わるため、ユーザー A は増分バックアップを実行できなくなります。

対処方法

[バックアップ仕様オプション] の [拡張] でバックアップセッションの [所有権] を構成します。バックアップオーナーは `Admin` ユーザーグループに所属している必要があります。これにより、バックアップセッションを開始したユーザーが誰であっても、このユーザーがすべてのバックアップのオーナーとなります。その手順については、『HP Data Protector ヘルプ』の索引キーワード「バックアップオプションの設定」で表示される内容を参照してください。

理由

アップグレード後に拡張増分が実行されない

この問題は、Windows、HP-UX、および Linux システムで発生する場合があります。A.06.11 以前のバージョンから Data Protector にアップグレードした場合 、古い拡張増分バックアップのレポジトリを新バージョンの製品で使用できなくなります。そのため、フルバックアップを実行します。フルバックアップ中、拡張増分バックアップのレポジトリが以下の場所に新規作成されます。

- **Windows システムの場合:** *`Data_Protector_home`*`\enhincrdb`
- **UNIX システムの場合:** `/var/opt/omni/enhincrdb`

対処方法

フルバックアップを実行します。拡張増分バックアップのレポジトリが新規作成され、拡張増分バックアップを実行できます。

Data Protector がセッションを開始できない

問題

対話型セッションを開始できない

バックアップが開始されるたびに、バックアップセッションを開始するための権限が必要となり、Data Protector を現在実行しているユーザーについて権限の有無がチェックされます。ユーザーがこのパーミッションを持っていない場合は、セッションを開始できません。

対処方法

ユーザーが適切な権限のあるユーザーグループに所属していることを確認してください。ユーザーグループの構成方法については、『HP Data Protector ヘルプ』の索引キーワード「ユーザーグループ」で表示される内容を参照してください。

問題

スケジュール設定されたセッションが実行されない

スケジュール設定されたセッションを開始するはずの Data Protector システムアカウントが Cell Manager 上の `Admin` ユーザーグループにないため、スケジュール設定されたセッションは実行されません。

このアカウントは、インストール時に Cell Manager 上の Data Protector `Admin` グループに追加されます。このアカウントを変更してそのパーミッションが削除された場合、またはサービスアカウントが変更された場合は、スケジューリングされていたセッションは実行されません。

対処方法

Data Protector アカウントを Cell Manager の `Admin` ユーザーグループに追加します。

問題

セッションが正常に行われず、「使用可能なライセンスがありません」というステータスメッセージが表示される

バックアップセッションは、Data Protector が使用可能なライセンスをチェックした後に限り開始されます。ライセンスが使用可能でない場合は、バックアップセッションは正常に行われず、Data Protector からセッションステータスを示すメッセージ「使用可能なライセンスがありません」が表示されます。

対処方法

使用可能なライセンスの情報を取得するには、次のコマンドを実行します。

```
omnicc -check_licenses -detail
```

新しいライセンスを請求してください。ライセンスの詳細については、『HP Data Protector インストールおよびライセンスガイド』を参照してください。

問題

スケジュール設定したバックアップが開始されない (UNIX の場合のみ)

対処方法

`crontab -l` コマンドを実行して、`omnitrig` プログラムが `crontab` ファイルに含まれているかどうかチェックします。以下の行が表示されない場合、Data Protector によって `omnitrig` エントリが自動的に追加されます。

```
0,15,30,45 * * * * /opt/omni/sbin/omnitrig
```

`omnisv -stop` コマンドと `omnisv -start` コマンドを実行して、Data Protector デーモンの終了と再起動を行います。

マウント要求が発行される

デバイスにメディアが入っているのにマウント要求が発行される

バックアップセッション中に、バックアップデバイス内に使用可能なメディアがあるにもかかわらず、Data Protector からマウントが要求される場合があります。この場合は、以下のような理由が考えられます。

理由:

デバイス内のメディアが所属するメディアプールのポリシーが [追加不可能] である

メディアに使用可能なスペースが残っていても、メディアプールのポリシーが［追加不可能］に設定されていると、そのメディアは使用されません。

対処方法

メディアプールのポリシーを［追加可能］に変更して、メディアがいっぱいになるまでバックアップを追加できるようにしてください。

理由:

デバイス内のメディアがまだフォーマットされていない

デフォルトでは、メディアの自動フォーマットは行われません。フォーマット済みのメディアがない場合は、マウント要求が要求されます。

対処方法

メディアをフォーマットします。その手順については、『HP Data Protector ヘルプ』の索引キーワード「フォーマット、メディア」で表示される内容を参照してください。

理由:

デバイス内のメディアが事前割り当てリストで指定されているメディアと違っている

デバイス内のメディアはフォーマットされていますが、バックアップ仕様の事前割り当てリストで指定されたメディアと違っています。また、指定されたメディアプールのポリシーが［厳格］になっています。

メディアの事前割り当てリストと［厳格］ポリシーを併用している場合は、事前割り当てリストで指定されているメディアがバックアップの開始時にデバイス内で使用可能になっている必要があります。

対処方法

- 事前割り当てリストを併用しながら、デバイス内にある使用可能なメディアを使用するには、メディアプールポリシーを [緩和] に変更します。
- デバイス内の使用可能な任意のメディアを使用するには、バックアップ仕様から事前割り当てリストを削除します。削除するには、バックアップ仕様でバックアップデバイスのオプションを変更します。

ファイルライブラリに対してマウント要求が発行される

問題

ファイルライブラリデバイスのディスクに空き領域がない

ファイルライブラリデバイスの使用中に、以下のメッセージとともにマウント要求が発行されることがあります。

ファイルライブラリ *"File Library Device"* に使用できるディスクスペースがありません。新しいディスクスペースをこのライブラリに追加してください。

対処方法

ファイルライブラリが置かれているディスクの空き領域を増やす。

- ファイルのバックアップ先となるディスク上の空き領域を増やす。
- ファイルライブラリデバイスが存在するシステムにディスクを追加する。

ファイル名に関する問題

問題

ファイル名またはセッションメッセージが Data Protector GUI 上に正常に表示されない

非 ASCII 文字を含むファイル名やセッションメッセージは正しく表示されないことがあります。これは、Data Protector GUI でファイル名やセッションメッセージを表示するのに、不正な文字エンコードが使用されているためです。

対処方法

適切なエンコードを指定します。**View** メニューから **Encoding** を選択し、適切な符号化文字セットを選択します。

UNIX で GUI のエンコード切替を有効にするには、GUI を起動する前に、ロケールを UTF-8 文字エンコードを使用するロケールに設定してください。

国際化に関する制限事項については、『HP Data Protector ヘルプ』の索引キーワード「国際化」で表示される内容を参照してください。

問題

ファイル名に非 ASCII 文字が使用されている場合の問題

プラットフォームが混在した環境では、IDB が新しい内部文字エンコードにまだ変換されていない場合、Data Protector GUI における非 ASCII 文字を含んだファイル名の処理について、いくつかの制限があります。詳細は、『HP Data Protector インストールおよびライセンスガイド』を参照してください。

対処方法

IDB を新しい内部文字エンコードに変換した後、クライアント上の Disk Agent をアップグレードします。

IDB の変換を実施しない場合、バックアップまたは復元できないツリーに関する回避方法は、その上位のツリーを選択することです。この場合、この親ツリーが正常に指定されていることが必要です (その名前が ASCII 文字だけで構成されているなど)。

バックアップに関して、これはより多くのデータがバックアップされることを意味します。しかし、通常はディスク全体または少なくとも大きなツリーがバックアップされることが多いため、これは問題になりません (`/home` または `\My Documents` など) 復元に関しては、[復元先を指定して別名で復元] または [新しいディレクトリに復元] オプションを使用して、親ツリーを新しいディレクトリに復元することができます。これにより、目的のファイルやディレクトリ以外のオブジェクトを復元することで発生し得る問題を回避できます。

復元に関して自信が持てない場合は、1 つの復元セッションごとに 1 つのツリー/ファイルを復元することをお勧めします。「何も復元されませんでした」というメッセージが表示されれば、そのツリーが復元されなかったことがはっきりします。デフォルトのファイル重複処理 (最新ファイルを保存) を使用している場合、このメッセージは、そのファイルがディスク上に既に存在し、上書きされなかったことを示します。

一方、[復元先を指定] オプションを使用した場合は、指定したパスにファイルが復元されます。数ファイルだけしか復元しない場合は、[復元されたデータをリスト] オプションも使用できます。

国際化に関する制限事項については、『HP Data Protector ヘルプ』の索引キーワード「国際化」で表示される内容を参照してください。

クラスターに関する問題

問題

サーバーのフルバックアップ中に Novell NetWare の共有クラスターボリュームがバックアップされない

サーバーのフルバックアップ中に Novell NetWare クラスター上の共有ボリュームがバックアップされません。この理由として、SMS クラスターリソースの処理が不適切で、クラスターサポートを有効にした状態で TSA モジュールがロードされるためクラスターボリュームがスキップされていることが理由として考えられます。

対処方法

アクティブノード上で `TSAFS /NoCluster` コマンドを実行し、クラスターサポートを無効にします。

問題

TruCluster Server 上のバックアップまたは復元が中止される

次のエラーメッセージが表示されて、バックアップセッションまたは復元セッションが中止されます。

`("ma/xma/bma.c)` 内で内部エラー`=>` プロセスが中止されました。

これは予期しない状況であり、おもにメディアの破損か、この製品とオペレーティングシステムの両方に関係する環境の組み合わせによって発生したと予想されます。

このエラーは、以下のいずれかの状況で発生します。

- バックアップに使用されたバックアップデバイスが、クラスターの仮想サーバー上に構成されている。
- バックアップ対象のファイルシステムがクラスター仮想サーバー上に存在する。

対処方法

TruCluster Server 上に以下の `omnirc` 変数を設定してください。

- `OB2BMANET=1`
- `OB2RMANET=1`
- `OB2RDANET=1`
- `OB2BDANET=1`

その手順については、「Omnirc オプション」 (19 ページ) を参照してください。

問題

Cell Manager がクラスター内に構成されている場合に、復元に関する問題が発生する

[すべてのオブジェクトのバックアップを再開] バックアップオプションを有効にした状態で、クラスター対応の Data Protector Cell Manager によるバックアップが実行されました。バックアップ中にフェイルオーバーが発生し、他のクラスターノードでバックアップセッションが再開され、正常に終了しました。最新のバックアップから復元しようとすると、セッションが正常に終了したにもかかわらず以下のエラーが報告されます。

正常に完了していないバージョンが選択されています。このようなバックアップを復元すると、一部またはすべてのファイルが正しく復元されない可能性があります。

Cell Manager クラスターノード間でシステム時刻の同期がとられていないと、失敗したバックアップのタイムスタンプが、再開されたバックアップのタイムスタンプよりも新しい可能性があります。復元用のデータを選択したときに、最後のバックアップバージョンがデフォルトで選択され、失敗したバックアップからの復元が行われます。

対処方法

最後の正常なバックアップから復元を行うには、正しいバックアップバージョンを復元対象として選択します。

このようなエラーを防止するには、ネットワーク上にタイムサーバーを構成することをお勧めします。これにより、Cell Manager クラスターノード間でシステム時刻の同期が自動的にとられます。

問題

Microsoft Cluster Server ノードの CONFIGURATION オブジェクトのバックアップが失敗する

Windows Server 2008 システムでは、クラスターノード上の CONFIGURATION オブジェクトのバックアップが次のエラーで失敗します。

`[警戒域] 場所: VBDA@computer.company.com "CONFIGURATION:"時間: Date Time[81:141] \Registry\0.クラスターは構成オブジェクトをエクスポートできません: (詳細は不明) => バックアップは不完全です`

対処方法

Cluster Service の実行に使用されるユーザーアカウントで Data Protector Inet サービスを再開して、バックアップを再開始します。

その他の問題

問題

バックアップの保護期限が終了した

バックアップのスケジュール設定時にフルバックアップと増分バックアップの両方に対して同じ保護期間を設定すると、増分バックアップがその基準となるフルバックアップと同じ期間保護されることになります。つまり、フルバックアップの期限が切れた時点で、増分バックアップの期限も切れることになります。この場合、保護期限が終了したフルバックアップに基づいて実行された増分バックアップを復元することはできません。

対処方法

増分バックアップよりもフルバックアップの方が保護期間が長くなるように構成します。

フルバックアップと増分バックアップの保護期間の差が、フルバックアップから次のフルバックアップ前の最後の増分バックアップまでの期間になるように設定する必要があります。

たとえば、増分バックアップを月曜日から金曜日まで実行し、フルバックアップを土曜日に実行する場合は、フルバックアップの保護期間を増分バックアップよりも 6 日以上長く設定する必要があります。これにより、最後の増分バックアップの期限が切れるまで、フルバックアップが保護されて使用可能になります。

問題

エラーメッセージ「接続が拒否されました」が断続的に表示される

次の致命的エラーが表示されて、バックアップセッションが中止されます。

システム computer.company.com、ポート 40005 の Media Agent に接続できません (IPC は接続できません。システムエラー: [10061] 接続が拒否されました。)

これは、Media Agent が Windows の非サーバー版で実行されている場合で、Disk Agent の同時処理数が 5 より多く設定されている場合に、発生する可能性がある問題です。Windows の非サーバー版での TCP/IP の実装のため、オペレーティングシステムでは、同時に受け付けることができる着信接続は 5 つまでに限られます。

対処方法

Disk Agent の同時処理数に 5 以下の値を設定してください。

バックアップ処理に頻繁に使用されるシステムバック (Cell Manager、Media Agent クライアント、Application Agent クライアント、ファイルサーバーなど) には、サーバー版の Windows を使用することをお勧めします。

問題

ファイルが大量であるために拡張増分バックアップが失敗する

HP-UX では、大量のファイルをバックアップしようとすると拡張増分バックアップは失敗します。

対処方法

Disk Agent が HP-UX でより多くの拡張増分バックアップ用メモリにアクセスできるようにするには、調整可能カーネルパラメータ maxdsiz を次のように設定します。

- **HPUX 11.11 システムの場合:**

```
kmtune set maxdsiz=2147483648

kmtune set maxdsiz_64bit=2147483648
```

- **HPUX 11.23/11.31 システムの場合:**

```
kctune set maxdsiz=2147483648
```

```
kctune set maxdsiz_64bit=2147483648
```

問題

ディスクイメージ復元時に予想外のマウント済みファイルシステムが検出される

ディスクイメージの復元時に、復元対象のディスクイメージはマウントされたファイルシステムであるため復元されないというメッセージが表示されることがあります。

オブジェクトはマウントされたファイルシステムです => 復元されません。

これは、ディスクイメージ上のアプリケーションが特定のパターンをディスクイメージに保存しているためです。ディスクイメージ上のファイルシステムがマウント済みかどうかを確認するシステムコールでこのパターンが誤って解釈され、ディスクイメージ上にマウント済みのファイルシステムがあると表示されます。

対処方法

復元を開始する前に、復元対象のディスクイメージがある Data Protector クライアント上で、以下のコマンドを入力してディスクイメージを削除します。

```
prealloc null_file 65536
dd if=null_file of=device_file
```

上記で、*device_file* は、復元対象のディスクイメージ用のデバイスファイルです。

問題

アプリケーションデータベースの復元に関する問題

データベースを復元しようとすると、復元に失敗し、以下のいずれかのメッセージが表示されます。

- `Cannot connect to target database`
- `Cannot create restore set`

DNS 環境の構成に問題があると、データベースアプリケーションに問題が発生することがあります。問題は以下のようなものです。

データベースのバックアップ時には、データベースが置かれているクライアントで起動したエージェントがクライアント名を*computer.company.com* としてデータベースに記録します。

復元時には、復元セッションマネージャーが*computer.company.com* への復元を試行しますが、このクライアントを*computer* としてしか認識していないため復元に失敗します。これは、DNS が正しく構成されていないため、クライアント名をフルネームに展開できないことが原因です。

DNS が Cell Manager 上でのみ構成されていて、アプリケーションクライアント上で構成されていない場合にも、同じ問題が発生することがあります。

対処方法

TCP/IP プロトコルを設定し、DNS を適切に構成します。詳細については、『HP Data Protector インストールおよびライセンスガイド』の付録 B を参照してください。

問題

Novell NetWare Server 上でのバックアップパフォーマンスが低い

Novell NetWare Server 上でのバックアップパフォーマンスが低いバックアップは、連続的にではなく、断続的に実行されます。これは既知の問題で、システムの `TCPIP.NLM` に原因があります。

対処方法

以下のパラメータを設定します。

```
SET TCP DELAYED ACKNOWLEDGEMENT = OFF
```

これにより、他への影響なしにバックアップパフォーマンスが向上します。

問題

Data Protector が Novell NetWare クライアント上で並行復元 Media Agent の起動に失敗する

Novell NetWare クライアント上では、Data Protector UNIX セッションマネージャーが復元 Media Agent を並行して起動できずに、以下のいずれかのメッセージが表示されることがあります。

- `Could not connect to inet`
- `Connection reset by peer`

一部の並行復元セッションはエラーなしで完了しても、その他の復元セッションは起動さえしないことがあります。

対処方法

グローバルオプションの `SmMaxAgentStartupRetries` を 2 以上 (最大値 50) に設定して起動の最大再試行回数を増やします。その手順については、「グローバルオプション」(18 ページ) を参照してください。

問題

Novell OES から Novell NetWare への異種プラットフォーム間の復元が失敗する

Novell OES でファイルをバックアップし、そのバックアップファイルを NSS のボリュームに移動します。Data Protector を有効にする `OB2TRUSTEE_RESTORE` omnirc 変数を設定し、データではなくトラスティ情報だけを復元するようにします。Novell NetWare クライアントからこのファイルの復元セッションを開始します。以下のメッセージが表示されます。

```
From:HPVRDA@hostname.domain
"/media/nss/NSS_VOL1"
Nothing restored.
```

対処方法

Novell NetWare のボリュームを復元するときには、バックアップパスの場所についての **restore into** オプションを/で始めるようにします。デフォルト値は\に変更する必要があります。これを行わないと、復元処理が失敗します。

restore as オプションはデフォルト値のままにすることもできます。

restore to default destination オプションはデフォルト値のままにすることも、ボリューム内のフォルダ名を続けて指定することもできます。

問題

非同期読み込みを使用してもバックアップ性能が向上しない

バックアップ仕様で選択された [非同期の読み込み] (Windows 固有) オプションを使用しても、バックアップパフォーマンスが改善されないか、パフォーマンスが低下することさえあります。

対処方法

1. omnirc 変数 `OB2DAASYNC` が 0 に設定されていないかどうかを確認します。変数を 1 に設定して常に非同期の読み込みを使用するか、変数をコメントアウトしてバックアップ仕様で [非同期の読み込み] オプションを使用します。
2. 非同期読み込みがバックアップ環境に適しているかどうかを確認します。一般的に、非同期読み込みは 1 MB を超えるファイルには適していません。さらに、omnirc 変数 `OB2DAASYNC_SECTORS` の微調整を試みることもできます。原則として、ファイルのサイズ (バイト数) が変数の値の 2〜3 倍の大きさでなければなりません。

問題

Windows Vista、Windows 7、および Windows Server 2008 システムで、IIS 構成オブジェクトのバックアップが失敗した

Windows Vista、Windows 7、および Windows Server 2008 システムで、IIS 構成オブジェクトのバックアップ時に次のエラーが報告されました。

[警戒域] 場所: VBDA@computer.company.com "CONFIGURATION:"時間: Date & Time [81:141] \IIS データベース は構成オブジェクトをエクスポートできません:(詳細は不明) => バックアップは不完全です

対処方法

IIS 6 Management Compatibility の下に **IIS Metabase and IIS 6 configuration compatibility** コンポーネントをインストールし、バックアップを再起動します。

問題

ハードリンクがあるボリュームからのサブツリーの復元が失敗する

ハードリンクがあるボリュームからのサブツリーの復元が失敗し、次のメッセージが表示されます。

" " という名前のファイルシステム復元 DA への接続が切断されました

対処方法

ハードリンクがあるツリーを復元する場合は、グローバルオプションの RepositionWithinRestoredObject を 0 に設定します。

このオプションを 0 に設定すると、復元処理が若干遅くなる場合がありますが、ハードリンクを復元する場合は必要です。

このオプションは、デフォルトでは 1 に設定されています。

7 オブジェクト操作セッションのトラブルシューティング

オブジェクトコピーに関する問題

問題

コピーされたオブジェクトの数が想定された数より少ない

ポストバックアップのオブジェクトコピーまたはスケジュールされたオブジェクトコピーの実行時に、実際にコピーされるオブジェクトの数が、選択したフィルタに一致するオブジェクトの数よりも少ないことがあります。

以下のメッセージが表示されます。

指定したフィルタに一致するオブジェクトの数が多すぎます。

対処方法

- オブジェクトバージョンの選択条件を絞り込みます。
- グローバルオプション `CopyAutomatedMaxObjects` の値を大きくして、同一セッション内でコピーされるオブジェクトの最大数を増やします。その手順については、「グローバルオプション」 (18 ページ) を参照してください。

問題

選択したライブラリ内の一部のオブジェクトしかコピーされない

ポストバックアップのオブジェクトコピーまたはスケジュールされたオブジェクトコピーの実行時に、選択したライブラリ内のメディア上にあるオブジェクトの一部がコピーされないことがあります。この問題は、選択したライブラリにオブジェクトの完全なメディアセットが存在しない場合に発生します。

対処方法

選択したライブラリに不足しているメディアを挿入するか、問題のオブジェクトの完全なメディアセットが存在するライブラリを選択します。

問題

追加のメディアに対するマウント要求が発行される

メディアを始点とする対話型オブジェクトコピーセッションで、特定のメディアを選択したとします。このとき、追加メディアに対するマウント要求が発行されることがあります。この現象は、選択したメディア上に存在するオブジェクトが、他のメディアにまたがっている場合に発生します。

対処方法

要求されたメディアをデバイスに挿入して、マウント要求に確認してください。

問題

オブジェクトコピーを作成したときに、保護の終了時間が延長される

オブジェクトコピーを作成したときに、元のオブジェクトから保護の終了時間が継承されません。保護期間はコピーされますが、開始時間が、オブジェクトの作成時間ではなく、オブジェクトコピーの作成時間に設定されます。その結果、元のオブジェクトより保護期間が延長されます。元のバックアップが作成されてからオブジェクトコピーセッションを行うまでの時間が長いほど、保護終了時間の差は大きくなります。

たとえば、オブジェクトの作成日が 9 月 5 日で、保護期間が 14 日に設定されていた場合、保護は 9 月 19 日に終了します。仮に、オブジェクトコピーセッションを 9 月 10 日に開始したとすると、そのオブジェクトのコピー保護が終了するのは 9 月 24 日になります。

場合によっては、このような動作は望ましくなく、保護の終了時間を維持しなければならないこともあります。

対処方法

グローバルオプション `CopyDataProtectionEndtimeEqualToBackup` を `1` に設定すると、オブジェクトコピー保護の終了時間がバックアップのオブジェクト保護の終了時間に等しくなります。このオプションは、デフォルトでは 0 に設定されています。

オブジェクトの集約に関する問題

問題

多くのポイントインタイムのオブジェクト集約を実行するときに開かれるファイルが多すぎる

ポイントインタイムが多い場合にオブジェクトの集約操作を開始すると、Data Protector はその操作に必要なすべてのメディアを読み込みます。これにより、すべてのファイルが同時に開かれます。Data Protector で開くファイルの数が、オペレーティングシステムの許容数より多い場合、次のようなメッセージが表示されます。

```
|Major| From:RMA@computer.company.com
"AFL1_ConsolidateConc2_bs128"Time:time
/omni/temp/Cons_Media/AFL1/0a1109ab54417fab351d15500c6.fd Cannot open
device ([24] Too many open files)
```

対処方法

許容されるファイルの最大数を増やします。

HP-UX の場合

1. System Administration Manager(SAM) を使用して、開いているファイルの最大数を設定します。

   [**Kernel Configuration**]→[**Configurable parameters**] を選択します。次に、[**Actions**]→[**Modify Configurable Parameter**] を選択します。[**formula/value**] フィールドに、[**maxfiles_lim**] と [**maxfiles**] の新しい値を入力します。
2. 新しい値を適用した後で、コンピュータを再起動します。

Solaris の場合

1. `/etc/system` ファイルを編集して、開いているファイルの最大数を設定します。以下の行を追加します。

   ```
   set rlim_fd_cur=値
   set rlim_fd_max=値
   ```
2. 新しい値を適用した後で、コンピュータを再起動します。

8 Data Protector 内部データベース (IDB) のトラブルシューティング

ファイルやディレクトリが見つからないことによる問題

データファイル (ディレクトリ) が見つからない

Cell Manager には、以下の場所に以下の IDB データファイル (ディレクトリ) が存在する必要があります。

Windows Server 2008 の場合: *Data_Protector_program_data*\db40

その他の Windows システムの場合: *Data_Protector_home*\db40

UNIX システムの場合: /var/opt/omni/server/db40

- datafiles\catalog
- datafiles\cdb
- datafiles\mmdb
- dcbf
- logfiles\rlog
- logfiles\syslog
- meta
- msg
- keystore\catalog

問題

データベース/ファイルを開けない、またはデータベースのネットワーク通信エラーが発生する

Data Protector が IDB にアクセスしようとしたときに、1 つまたは複数の IDB データファイルまたはディレクトリが見つからない場合、以下のエラーが表示されます。

- データベース/ファイルを開くことができません。
- データベースのネットワーク通信エラー

対処方法

IDB データファイルおよびディレクトリを再インストールします。

1. Data Protector を再インストールします。その手順については、「問題」 (61 ページ) を参照してください。
2. Cell Manager を再起動します。

一時ディレクトリが見つからない

Cell Manager 上に、以下の一時ディレクトリが存在する必要があります。

Windows システムの場合: *Data_Protector_home*\tmp

UNIX システムの場合: /var/opt/omni/tmp

問題

Data Protector にアクセスできない

Data Protector GUI が Cell Manager に接続しようとしたときに、Data Protector の一時ディレクトリが見つからない場合、以下のエラーメッセージが表示されます。

Cell Manager システムにアクセスできません (inet が応答しません)。Cell Manager ホストと通信できない、Cell Manager ホストが動作していない、または Cell Manager ホストに Data Protector ソフトウェアがインストールまたは構成されていません。

対処方法

1. Data Protector GUI を閉じます。
2. Data Protector サービス/プロセスを停止します。Cell Manager 上で次のコマンドを実行します。

   Windows システムの場合: *Data_Protector_home*\bin\omnisv -stop

   UNIX システムの場合: /opt/omni/sbin/omnisv -stop
3. Cell Manager 上で、次の場所に tmp ディレクトリを手動で作成します。

   Windows システムの場合: *Data_Protector_home*

   UNIX システムの場合: /var/opt/omni
4. サービス/プロセスを起動します。

   Windows システムの場合: *Data_Protector_home*\bin\omnisv -start

   UNIX システムの場合: /opt/omni/sbin/omnisv -start
5. Data Protector GUI を再起動します。

バックアップ時およびインポート時の問題

問題

バックアップ中にファイル名が IDB に記録されない

以下に該当する場合は、Data Protector を使用してバックアップを実行したときにファイル名が IDB に記録されません。

- バックアップオプションとして [記録しない] を選択した場合。
- IDB の DCBF 部分のスペースが不足している場合、または IDB のあるディスクのディスクスペースが不足している場合。これは、セッション出力内のエラーにより通知されます。
- Windows Cell Manager 上で、クライアントのバックアップ中に IDB 内でファイル名変換が行われていた場合。この場合も、結果として [記録しない] オプションを使用してバックアップが行われるため、このクライアントに関して今回のセッションでは IDB にデータが書き込まれません。

対処方法

- バックアップオプションとして、[記録しない] を選択していないかどうかを確認してください。
- バックアップセッションのセッションメッセージに警告およびエラーが含まれていないかどうかをチェックします。

問題

IDB のバックアップまたはインポート中に、BSM または RSM が強制終了する

IDB のバックアップまたはインポートセッション中に、BSM または RSM が強制終了する場合、以下のエラーが表示されます。

IPC 読み込みエラーシステムエラー: [10054] ピアごとに接続がリセットされます。

Data Protector GUI の [内部データベース] コンテキストで、セッションが実際には実行中でないにもかかわらず、セッションステータスが [実行中] と表示されます。

対処方法

1. Data Protector GUI を閉じます。
2. `omnidbutil -clear` コマンドを実行し、実際には実行中でないが［実行中］と表示されているすべてのセッションのステータスを、［失敗］に設定します。
3. `omnidbutil -show_locked_devs` コマンドを実行して、Data Protector によってロックされているデバイスやメディアがないかどうか確認します。
4. ロックされているものがあった場合、`omnidbutil -free_locked_devs` を実行してロックを解除します。
5. Data Protector GUI を再起動します。

問題

IDB バックアップまたはインポート中に、MMD が強制終了する

IDB バックアップまたはインポートセッション中に、メディア管理デーモン (MMD) が強制終了する場合、以下のエラーが表示されます。

- `MMD` への接続が中断されました。
- `IPC` 読み込みエラーシステムエラー：［10054］ピアごとに接続がリセットされます。

MMD サービス/プロセスが稼動していない場合:

- `omnisv -status` コマンドを実行すると、MMD サービス/プロセスが動作していないことが通知されます。
- **Windows システムの場合:** Data Protector MMD プロセス (`mmd.exe`) は Windows タスクマネージャー内のプロセスとして表示されません。

  UNIX システムの場合: ps `-ef | grep omni` コマンドを使って Data Protector プロセスをリストすると、Data Protector MMD プロセス (`/opt/omni/lbin/mmd`) は表示されません。

対処方法

1. Data Protector GUI を閉じます。
2. `omnisv -stop` コマンドを実行して、Data Protector サービス/プロセスを停止します。
3. `omnisv -start` コマンドを実行して、Data Protector サービス/プロセスを起動します。
4. `omnisv -status` コマンドを実行して、サービス/プロセスがすべて実行中かどうかチェックします。

問題

DC バイナリファイルが破損または見つからない

Data Protector GUI の［復元］コンテキストでバックアップオブジェクトをブラウズすると、以下のエラーが表示されます。

詳細カタログバイナリファイルを開くことができませんでした。

- `omnidbcheck -bf` コマンドを実行すると、1 つまたは複数の DC バイナリファイルが見つからないか、サイズが不適切であることが通知されます。`omnidbcheck -dc` コマンドを実行すると、1 つまたは複数の DC バイナリファイルが破損していることが通知されます。
- Cell Manager 上の `debug.log` ファイルには、Data Protector が DC バイナリファイルを開くのに失敗したことを示すエントリが 1 つ以上含まれています。

対処方法

メディアからカタログをインポートして、DC バイナリファイルを再作成します。その手順については、『HP Data Protector ヘルプ』の索引キーワード「IDB の DCBF 部分の [警戒域] レベルの破損」を参照してください。

パフォーマンスに関する問題

問題

復元時のブラウズに時間がかかる

Data Protector GUI で復元対象のオブジェクトバージョンおよび個々のファイルをブラウズするとき、IDB から情報が読み込まれて表示されるまでに時間がかかります。この問題は、IDB 内のオブジェクト数とオブジェクトのサイズが大きすぎることが原因となって発生します。

対処方法

復元対象のオブジェクトバージョンをブラウズする際の時間間隔を設定します。

- 特定の復元に対して時間間隔を指定するには、[ソース] ページの［検索インターバル］オプションを設定します。
- これ以降ブラウズするすべての復元に対してグローバルに時間間隔を設定するには、以下の手順に従ってください。
  1. **[**ファイル**]** メニューの **[**選択値**]** をクリックします。
  2. **[**復元**]** タブをクリックします。
  3. **[**検索インターバル**]** オプションを設定し、**[OK]** をクリックします。

問題

IDB の削除処理が遅い

IDB でのファイルバージョン削除の速度が極端に低下します。

対処方法

現在の削除セッションに関して、次のメッセージが Data_Protector_home\log\server\purge.log ファイルに記録されていないか確認します。

```
Multiple passes needed.This will decrease the performance of the purge session.To improve performance increase the amount of memory a purge session is allowed to use.
```

ログファイルにこのメッセージが含まれている場合は、セッションを中止し、グローバルオプション PurgeBufferSize の値を増やします。その手順については、「グローバルオプション」 (18 ページ) を参照してください。この作業が終了したら、削除セッションを再開します。

その他の問題

問題

データベースセッションマネージャーが稼動していないことによるプロセス間通信エラー

Data Protector GUI が IDB にアクセスしているときに Cell Manager でデータベースセッションマネージャープロセスが動作を停止するか、または終了すると、以下のエラーが表示されます。

プロセス間通信エラー

Cell Manager 上では、以下の状態になります。

Windows システムの場合: Data Protector の dbsm.exe プロセスが Windows タスクマネージャーに表示されません。

UNIX システムの場合: ps -ef | grep omni コマンドを使って Data Protector プロセスをリストしたときに、/opt/omni/lbin/dbsm が表示されません。

対処方法

Data Protector GUI を再起動します。

問題

IDB のスペースが不足している

一部の IDB のスペースが不足しています。[IDB のスペース不足] 通知または [IDB テーブルスペースのスペース不足] 通知が発生します。

対処方法

IDB のサイズを拡大します。詳細は、『HP Data Protector ヘルプ』の索引キーワード「IDB サイズの増大」を参照してください。

問題

MMDB と CDB が同期しない

MMDB と CDB の非同期は、以下の場合に発生する可能性があります。

- MMDB と CDB に異なる時点で得られた情報が格納されている場合。これは、CDB と MMDB のインポート (`omnidbutil -readdb` コマンド) が、別々のエクスポートセッション (`omnidbutil -writedb` コマンド) で生成されたファイルから行われたことによって生じることがあります。
- MoM 環境において、ローカルの CDB および CMMDB が同期されていない場合。これは、CMMDB の復元によって生じることがあります。

Data Protector は、IDB 内のオブジェクトにメディアが割り当てられていない、またはメディアに対するデータ保護が正しく設定されていない場合に、それを通知します。

対処方法

MMDB と CDB を同期します。Cell Manager 上で、以下のディレクトリから、

Windows システムの場合: *Data_Protector_home*\bin

UNIX システムの場合: /opt/omni/sbin

次のコマンドを実行します。

```
omnidbutil -cdbsync Cell_Server_Hostname
```

MoM 環境の場合は、CMMDB がインストールされている MoM Manager から各 Cell Manager に対してコマンドを実行します。このとき、ホスト名を引数として指定します。

問題

HP-UX 上のメモリー割り当ての問題により IDB に障害が発生する

メモリー割り当て問題が原因で、IDB の保守または照会中に、HP-UX 上で RDS サービスが失敗します。

対処方法

1. Cell Manager 上で、`omnirc` 変数 `_M_ARENA_OPTS=1:32` を設定します。その手順については、「Omnirc オプション」 (19 ページ) を参照してください。
2. Data Protector サービスを再起動します。

   ```
   /opt/omni/sbin/omnisv -start
   ```

問題

IDB が破損している

以下のいずれかのメッセージが表示されることがあります。

- データベースが破損しています。
- プロセス間通信エラー
- データベース/ファイルを開くことができません。

- エラー – 詳細は不明

対処方法

IDB を回復します。詳細は、『HP Data Protector ヘルプ』の索引キーワード「IDB の復旧」を参照してください。

問題

拡張増分バックアップデータベースが壊れている

Windows、HP-UX、および Linux システムでのアップグレード後に、新しい拡張増分データベースが破損しています (拡張増分リポジトリを拡張増分バックアップで使用できません)。

対処方法

以下の場所の拡張増分バックアップリポジトリを削除します。

- **Windows システムの場合:** *Data_Protector_home*\enhincrdb
- **UNIX システムの場合:** /var/opt/omni/enhincrdb

フルバックアップを実行したときに、新しい拡張増分バックアップリポジトリが作成されます。

問題

Cell Manager への Data Protector の再インストールが必要となるその他の問題

何らかの理由で、IDB を保持したまま、Cell Manager に Data Protector を再インストールしなくてはなりません。

対処方法

以下の手順で、Cell Manager に Data Protector を再インストールします。

1. Data Protector サービスを停止します。
2. Data_Protector_home\db40 と Data_Protector_home\Config ディレクトリを安全な場所にコピーします。
3. Data Protector サービスを開始します。
4. Cell Manager から Data Protector をアンインストールした後、Data Protector を再インストールします。
5. Data Protector サービスを停止します。
6. 先ほど保存したデータを、Data_Protector_home\db40 と Data_Protector_home\Config ディレクトリにコピーして戻します。
7. Data Protector サービスを開始します。

9 レポートおよび通知のトラブルシューティング

レポートと通知に関する問題

問題

Data Protector Windows 上で送信方法として電子メールを使用したときに GUI が応答しなくなる

最新のセキュリティパッチをインストールした Microsoft Outlook XP を使用している場合、送信方法として電子メールを指定してレポートグループにレポートを追加した後、レポートグループを開始しようとすると、GUI がハングするという問題が発生します。通知を構成して電子メールを送信方法として選択した場合にも同じ問題が発生します。

Outlook では、電子メール通知を送信する前にユーザー操作を要求するようになっているため、この問題が発生します。この機能は、Outlook セキュリティポリシーの一部なので無効化できません。

対処方法

- ネットワーク上で SMTP サーバーを使用できる場合は、送信方法として [電子メール (SMTP)] を選択します。電子メールの送信方法としては、この方法が推奨されます。『HP Data Protector ヘルプ』の索引「送信方法」を参照してください。
- 以下の Data Protector CLI を使用してレポートを開始します。

  ```
  omnirpt -report licensing -email EmailAddress
  ```

  電子メールの自動送信を許可するかどうかを確認する警告メッセージが表示されたら、[はい] をクリックして、レポートを受信します。

  セキュリティ設定のカスタマイズ方法の詳細については、『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』を参照してください。

問題

SNMP による送信が失敗する

レポートを SNMP トラップとして送信する際、レポートがあて先に到達しません。

対処方法

SNMP トラップによる送信方法は、構成された SNMP トラップの最大サイズを超えないレポートにのみ使用します。

10 Data Protector オンラインヘルプのトラブルシューティング

概要

Data Protector のオンラインヘルプは、以下の 2 つのパートで構成されています。

- **ヘルプトピック**: 概念、手順、例などが含まれます。
- **状況依存型ヘルプ**とは、状況に応じて動的に表示されるオンラインヘルプで、Data Protector GUI の画面やオプションの説明を表示します。状況依存型ヘルプは、ヘルプナビゲータという Data Protector GUI コンポーネントによって表示されます。

ヘルプの形式は、Data Protector GUI を実行しているプラットフォームと、使用している GUI の種類に依存します。

- Windows システム用のオリジナルの Data Protector GUI を実行している場合は、Microsoft HTML ヘルプが使用されます。
- 任意のプラットフォーム上で Java GUI を実行している場合は、WebHelp が使用されます。

Windows のオンラインヘルプのトラブルシューティング

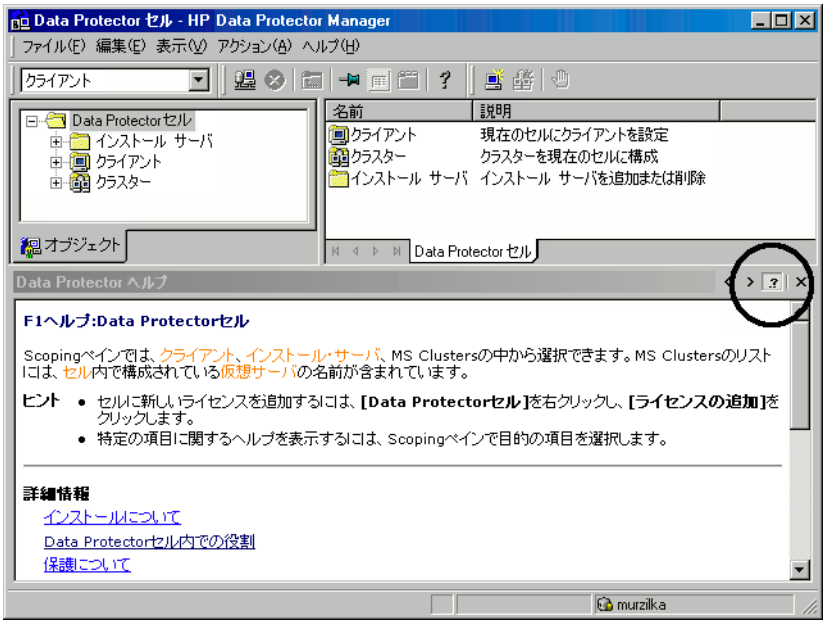
問題

Data Protector の画面を別の画面に切り替えても、その画面の説明がヘルプナビゲータに表示されない

対処方法

- Microsoft HTML ヘルプモード (デフォルト) を使用している場合、以下の図に示されているボタンが有効であることを確認してください。

図 3 トレース用のボタンが有効な場合



- [デフォルトの HTML ブラウザ] モード (外部 Web ブラウザでヘルプファイルを表示) を使用している場合、[ファイル] メニューから [選択値] をクリックし、[状況依存のヘルプナ

ビゲータを使用可能にする] オプションを選択します。その後、ヘルプナビゲータを再起動します。

UNIX のオンラインヘルプのトラブルシューティング

問題

オンラインヘルプの起動と表示に関する問題

Web ブラウザ (HTML ビューアー) が正しく設定されていないと、オンラインヘルプの起動と表示に関して問題が生じることがあります。

対処方法

Web ブラウザを以下のように設定します。

1. [ファイル] メニューの [選択値] をクリックし、[設定] をクリックして [設定] ダイアログを開きます。
2. [実行スクリプトまたはバイナリファイルの位置 (ディレクトリ)] テキストボックスに、Web ブラウザのパス (例: `/usr/bin`) を入力します。
3. [ビューアーの起動コマンド] テキストボックスに、ブラウザを起動するコマンドを入力します (例: `firefox $HTML$`)。

11 サポートへご連絡いただく前に

当社サポートサービスへご連絡いただく前に

問題を解決できない場合は、HP カスタマサポートサービスへご連絡ください。ただし、HP カスタマサポートサービスへご連絡いただく前に、以下のことを確認してください。

- 全般的なチェックをすでに済ませていること。「全般的なチェック」 (15 ページ) を参照してください。
- その問題に関する情報がこのガイドに記載されているかどうかを既にチェックし終えていること。インストール、統合ソフトウェア、ZDB、およびディザスタリカバリに関する問題については、各ガイドのトラブルシューティングの項を参照してください。
- HP カスタマサポートサービスに送付するデータとして、発生している問題の説明、セッションの出力 (問題の種類によっては同等の出力)、および実際の環境の説明などの情報をすでに収集し終えていること。

その後の手順については、HP カスタマサポートサービスよりご説明させていただきます。たとえば、以下のような作業をお願いすることがあります。

1. Data Protector をデバッグモードで実行する。
2. HP カスタマサポートサービスに送付するための生成データを準備する。

これらの手順について、以降の項で説明します。なお、これらの手順が必要になるのは、HP カスタマサポートサービスから依頼があった場合のみです。

デバッグ

当社サポート担当者が技術的な問題を解決するために情報が必要となった場合にのみ、デバッグ情報の収集をお願いいたします。Data Protector をデバッグモードで実行すると、デバッグ情報が作成され、大量のディスクスペースを消費します。デバッグの際に必要となる詳細レベルおよび環境条件については、当社サポートサービスにお問い合わせください。

デバッグの有効化

Data Protector をデバッグモードで起動するには、数通りの方法があります。デバッグオプションについては、「デバッグ構文」 (66 ページ) を参照してください。

重要: Data Protector がデバッグモードで実行されている場合、すべての動作についてデバッグ情報が生成されます。バックアップ仕様をデバッグモードで開始した場合、このバックアップ仕様でバックアップされた各クライアント上に Disk Agent から出力が送信されます。

注記: Windows Vista、Windows 7、および Windows Server 2008 システムの場合、ネットワーク共有によるバックアップや復元のデバッグを有効にするには、そのセッションが実行されているオペレーティングシステムのアカウントに対して、*Data_Protector_program_data*\tmp フォルダへの書き込みパーミッションが割り当てられている必要があります。

Data Protector GUI の使用

[ファイル] メニューで [選択値] をクリックし、続いて [デバッグ] タブをクリックします。デバッグオプションを指定し GUI を再起動します。GUI はデバッグモードで再起動されます。

トレース構成ファイルを使用する

トレース構成ファイルを編集します。このファイルは、以下の場所にあります。

Windows Server 2008 の場合:

Data_Protector_program_data\Config\server\Options\trace

その他の Windows システムの場合:
Data_Protector_home\Config\server\Options\trace

UNIX システムの場合: /etc/opt/omni/server/options/trace

OB2OPTS 変数を使用する

Data Protector 統合ソフトウェア用のデバッグパラメータは、OB2OPTS 環境変数を使用して設定します。この変数の設定方法については、当社サポート担当にお問い合わせください。

スケジューラを使用する

スケジュール設定されたセッションをデバッグするには、スケジュールファイルを編集します。スケジュールファイルは以下の場所にあります。

Windows Server 2008 の場合:
Data_Protector_program_data\Config\server\Schedules または
Data_Protector_program_data\Config\server\Barschedules

その他の Windows システムの場合: *Data_Protector_home*\Config\server\Schedules または*Data_Protector_home*\Config\server\Barschedules

UNIX システムの場合: /etc/opt/omni/server/schedules または/etc/opt/omni/server/barschedules

デバッグパラメータは、ファイルの先頭行に追加します。

注記: ファイルを編集する前にコピーを作成して、デバッグが不要になった場合に変更を元に戻せるようにしておく必要があります。

例

```
-debug 1-99 sch.txt -full -only 2010      -day 14 -month Dec      -at 22:00
```

デバッグ構文

ほぼすべての Data Protector コマンドは、以下の構文を持つパラメータ-debug を使って起動できます。

```
-debug 1-99[,C:n][,T:s][,U] XYZ [host]
```

ここで、

- 1-99 は、デバッグ範囲を示します。特に指示のない限り、1-99 と指定してください。省略可能なパラメータは、この範囲パラメータの一部として、カンマ区切りで指定してください。
  - C:*n* は、デバッグファイルのサイズを*n*KB に制限します。最小値は 4(4KB)、デフォルト値は 1024(1MB) です。
    詳細は、「デバッグの最大サイズの制限」 (67 ページ) を参照してください。
  - T:*s* は、タイムスタンプの分解能です。デフォルトは 1 で、1000 が分解能 1 ミリ秒、0 がタイムスタンプを使用しないことを意味します。
    Novell NetWare などの一部のプラットフォームでは、ミリ秒の分解能を使用できません。
  - U は、Unicode フラグです。指定すると、Windows 上のデバッグファイルが Unicode 形式で書き込まれます。
- *XYZ* は、デバッグの接尾辞です (DBG_01.txt など)。

- *host* は、デバッグモードが起動されているクライアントのリストです。

  このオプションを使うと、指定したクライアント上でのみデバッグを実行することができます。複数のクライアントを指定する場合は、スペースで区切ります。リストは引用符で囲みます。例: "computer1.company.com computer2.company.com"。

デバッグの最大サイズの制限

Data Protector を**循環デバッグ**と呼ばれる特殊なデバッグモードで実行することができます。このモードでは、デバッグファイルのサイズが事前設定されたサイズ (*n*) に達するまで、デバッグメッセージが追加されます。事前設定されたサイズに達すると、カウンターがリセットされ、最も古いデバッグメッセージが上書きされます。これにより、最新レコードに影響を与えることなく、トレースファイルのサイズを制限できます。

このモードは、セッションの終わり近くで問題が発生する場合、または問題発生後すぐに Data Protector が中止または終了する場合にのみ使用することをお勧めします。

循環デバッグを使用する場合、必要なディスクスペースの推定値は以下のようになります。

表 6 循環デバッグに必要となるディスクスペース

システム	必要となるディスクスペースの最大量
Media Agent クライアント	バックアップまたは復元で実行される Media Agent ごとに、2*n[kB]
Disk Agent クライアント	バックアップまたは復元のマウントポイントごとに、2*n[kB]
Cell Manager	2*n[kB]
統合クライアント	2*n[kB] * *parallelism*

Inet および CRS のデバッグでは、それぞれの動作に対して個別にデバッグファイルが作成されるため、正確な上限値を計算することはできません。

デバッグファイルの名前と保存場所

デバッグの接尾辞オプションを使って、デバッグファイルを以下のディレクトリに作成します。

Windows Vista、Windows 7、Windows Server 2008 の場合:
Data_Protector_program_data\tmp

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

UNIX システムの場合: /tmp

Novell NetWare システムの場合: SYS:\USR\OMNI\TMP

ファイル名は以下のようになります。

OB2DBG_*did*__*Program*_*Host*_*pid*_*XYZ*

ここで、

- *did*(デバッグ ID) は、デバッグパラメータを受け付ける最初のプロセスのプロセス ID です。この ID がデバッグセッションの ID として使用されます。後続のプロセスもこの ID を使用します。
- *Program* はトレース結果の書き込みを行う Data Protector プログラムのコード名です。
- *Host* はデバッグファイルが作成されるクライアントの名前です。
- *pid* はプロセス ID です。
- *XYZ* は-debug パラメータで指定された接尾辞です。

バックアップまたは復元セッションの ID(*sid*) が決まると、その ＩＤ がファイル名に付加されます。

OB2DBG_*did*_*sid*_*Program*_*Host*_*pid*_*XYZ*

sid を付加するプロセスは、BMA/RMA、xBDA/xRDA、およびセッションにより起動された他のプロセスであり、BSM/RSM 自体によっては付加されません。

注記: セッション ID は、デバッグファイルの識別に役立ちます。他のデバッグファイルも同じセッションに属している場合、それらにも付加する必要があります。

`ctrace.log` ファイルは Cell Manager 上に作成され、デバッグファイルがどこに (どのクライアントに) 作成されたか、どのようなデバッグ接頭辞が使われたかという情報が保存されます。このファイルには、生成されたすべてのファイルのリストが含まれているわけではないことに注意してください。

デバッグファイルのデフォルトの保存場所をシステムごとに変更するには、`omnirc` 変数の `OB2DBGDIR` を使います。その手順については、「Omnirc オプション」 (19 ページ) を参照してください。

Inet のデバッグ

注記: `Inet` デバッグを有効に設定した場合は、すべての統合ソフトウェアによってデバッグファイルが生成されます。

Windows システムの場合:

Windows Service Control Manager を起動し、`Data Protector Inet` サービスを次の起動パラメータで再起動します。

```
-debug 1-140 POSTFIX
```

UNIX システムの場合:

`/etc/inetd.conf` ファイルを編集します。

1. 次の行を探します。

   ```
   omni stream tcp nowait root /opt/omni/lbin/inet inet -log
   /var/opt/omni/log/inet.log
   ```

   この行を、以下のように変更します。

   ```
   omni stream tcp nowait root /opt/omni/lbin/inet inet -log
   /var/opt/omni/log/inet.log -debug 1-140 DBG_01.txt
   ```

2. ファイルを変更、保存した後、`/etc/inetd -c` コマンドを実行して変更を適用します。

CRS のデバッグ

注記: デバッグファイルのサイズは非常に大きくなる可能性があるため、`-debug` オプションを使用する際は注意が必要です。

Windows システムの場合:

Windows Service Control Manager を起動し、`Data Protector CRS` サービスを次の起動パラメータで再起動します。

```
-debug 1-140 POSTFIX Cell_Manager_name
```

UNIX システムの場合:

1. 次のコマンドを実行して、CRS を停止します。

   ```
   /opt/omni/lbin/crs -shutdown
   ```

2. 以下のように、CRS をデバッグオプション付きで再起動します。

   ```
   /opt/omni/lbin/crs -debug 1-140 POSTFIX
   ```

Microsoft Cluster Server 環境の場合:

Data Protector 共有ディレクトリ内で、次のファイルを編集します。

Windows Server 2008 の場合:
Data_Protector_program_data\Config\server\options\Trace
その他の Windows システムの場合:
Data_Protector_home\Config\server\options\Trace
以下の行を追加します。

```
ranges=1-99.110-500
postfix=DBG
select=obpkg.rc.aus.hp.com
```

クラスターアドミニストレータユーティリティを使用して、CRS サービスリソース (OBVS_MCRS) をオフラインにします。

△ **注意:** Data Protector クラスターグループがフェイルオーバーする原因となるため、Windows Service Control Manager から CRS を終了しないでください。

MC/ServiceGuard 環境の場合:

1. `/etc/opt/omni/server/options/trace` ファイル内で、コメントを解除して必要なデバッグオプションを設定します。ファイルを保存して閉じます。
2. デバッグを起動します。

   ```
   /opt/omni/lbin/crs -redebug
   ```

デバッグを停止するには、`trace` ファイルのすべてのデバッグオプションを空白文字列に設定してファイルを保存した後、`/opt/omni/lbin/crs -redebug` コマンドを実行します。

HP カスタマサポートサービスに送付するための生成データの準備

HP カスタマサポートサービスが技術上の問題を解決するために何らかのデータが必要な場合は、それらのデータを収集して送付するようにお客様にお願いすることがあります。

Data Protector は大規模なネットワーク環境で動作するため、データの収集が難しい場合があります。Data Protector の `omnidlc` コマンドは、に送付するログファイル、デバッグファイル、getinfo ファイルの収集やパッキングを行うためのツールとして用意されています。このコマンドは、HP カスタマサポートサービスから依頼があった場合に使用してください。

`omnidlc` コマンドは、Data Protector CLI または Data Protector GUI から実行できます。この項では、両方の方法を説明します。

注記: `omnidlc` コマンドでは、Data Protector インストール実行トレースの収集はできません。これらのトレースの作成と収集の方法については、『HP Data Protector インストールおよびライセンスガイド』を参照してください。

omnidlc コマンドについて

Data Protector デバッグデータの生成後、`omnidlc` コマンドを使用すると、Data Protector セル (デフォルトでは、すべてのクライアントから) から、Data Protector デバッグファイル、ログファイル、getinfo ファイルを収集できます。このコマンドでは、選択したクライアントから Cell Manager にデータが転送され、そこでデータがパックされます。

このコマンドでは、特定のデータを選別して収集することができます。たとえば、あるクライアントのログファイルのみを収集したり、ある特定の Data Protector セッション中に作成されたデバッグファイルのみを収集したりすることができます。

注記: オブジェクト集約がポストバックアップセッションの一部としてスケジュールされている場合、バックアップセッションと集約セッションのセッション ID は異なります。ただし、デバッグ ID はバックアップと集約の両方で同じになります。この場合、`-session` パラメータを使用して `omnidlc` コマンドを実行し、集約セッション ID を指定すると、デバッグがバックアップと集約の両方に対して収集されます。

制限事項

- このコマンドは Cell Manager でのみ実行できます。
- MoM 環境では、それぞれの Cell Manager からコマンドを実行することで、各 Data Protector セルのデータを別々に収集することしかできません。
- HP OpenVMS でデバッグおよびログファイルコレクタを使用する場合、以下の制限事項が適用されます。
  - OpenVMS ODS-2 ディスク構造のファイル名には、最大で 39 文字まで使用できます。
  - OpenVMS システムには `get_info` ユーティリティが存在しないので、`get_info.out` ファイルは空で、収集されません。
  - `-session` オプションを指定して `omnidlc` コマンドを実行すると、指定したセッションの途中で作成されたデバッグファイルは収集されません。セッション名が OpenVMS デバッグファイル名の一部ではないからです。代わりに、すべての利用可能なログが収集されます。

CLI から omnidlc コマンドを使用することによるデバッグログの処理

omnidlc コマンドの構文

```
omnidlc {-session sessionID | -did debugID | -postfix string |
-no_filter} [-hosts list] [-pack filename | -depot [directory] | -space
| -delete_dbg] [-no_logs] [-no_getinfo] [-no_compress] [-no_config]
[-no_debugs | -debug_loc dir1 [dir2]...][-verbose] [-add_info [-any |
host] path]
omnidlc -localpack [filename]
omnidlc -unpack [filename]
omnidlc -uncompress filename
omnidlc [-hosts list] -del_ctracelog
```

以下の各項では、これらのオプションについて説明します。

収集データの範囲限定

収集データの範囲を限定するには、`omnidlc` コマンドを以下のオプションと共に使用します。

```
{-session sessionID | -did debugID | -postfix string | -no_filter}
[-hosts list] [-no_logs] [-no_getinfo] [-no_config] [-no_debugs |
-debug_loc dir1 [dir2]...]
```

以下の機能は、組み合わせて使用することができます。

- 選択したクライアントからのみデータを収集するには、`-hosts list` オプションを使用します。クライアントの名前をスペース区切りで指定します。

  クラスター環境では、`-hosts` オプションを使用して、クラスターノードを指定します。このオプションが指定されていない場合、データはアクティブなノードからのみ収集されます。
- 収集データから getinfo ファイル、構成情報ファイル、ログファイル、デバッグファイルを除外するには、それぞれ`-no_getinfo`、`-no_config`、`-no_logs`、または`-no_debugs` オプションを使用します。`-no_getinfo` は、HP OpenVMS システムには適用できないことに留意してください。
- 特定のセッションだけからデバッグファイルを収集するには、`-session sessionID` オプションを使用します。OpenVMS では、利用可能なすべてのログが収集されます。

- 特定のデバッグ ID に一致するデバッグファイルだけを収集するには、`-did debugID` オプションを使用します。
- 指定した接尾辞に一致するデバッグファイルだけを収集するには、`-postfix string` オプションを使用します。
- すべてのデバッグファイルを収集するには、`-no_filter` オプションを使用します。
- デフォルトのデバッグファイルディレクトリだけではなく、他のディレクトリからもデバッグファイルを収集するには、`-debug_loc dir1 [dir2]...` オプションを使用します。サブディレクトリは検索対象に含まれません。指定したディレクトリがクライアントに存在しない場合、そのディレクトリは無視されます。

データのセグメント化

Cell Manager に送信するファイルのサイズが 2 GB を超えている場合、そのファイルは 2 GB のチャンクに分割されます。各チャンクには、`s001`～`s999` の範囲内の拡張子が付加されます。ファイルが圧縮されている場合は、2 番目の拡張子として `.gz` が付加されます。

一方、Cell Manager 側では、圧縮済みまたは未圧縮の収集ファイルのサイズがすべて 2 GB を超えている場合、収集ファイルは 2GB のパッケージにパックされ、ファイル名には `s001`～`s999` の範囲内の拡張子が付加されます。

収集データの圧縮の無効化

デフォルトでは、収集データが Cell Manager への送信前に圧縮されます。圧縮を無効にするには、`-no_compress` オプションを使用します。

パックしたデータの保存

デフォルトでは、ネットワークを経由して Cell Manager にデータが送信され、そこでデータがパックされて、カレントディレクトリに `dlc.pck` ファイルとして保存されます。

パックされたファイルには、関連するクライアントのホスト名、パス、収集ファイルを含むディレクトリ構造が含まれています。

制限事項

- 最終的なパック済みファイルのサイズは 2 GB 以内に制限されます。この制限を超える場合はデータをパックしないでください。

データをパックして保存するには、`-pack filename` オプションを使用します。

- 異なるファイル名を使用する場合は、ファイル名として *filename* を指定します。
- 異なるディレクトリに異なるファイル名で保存する場合は、フルパス名として *filename* を指定します。

アンパックしたデータの保存

データをパックせずに保存するには、`-depot [directory]` オプションを使用します。*directory* を省略すると、Cell Manager 上の以下のディレクトリにファイルが保存されます。

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

UNIX システムの場合: `/tmp/dlc`

directory を指定した場合は、指定したディレクトリ内の `dlc` ディレクトリに収集ファイルが保存されます。

パックされた、またはパックされていないファイルのディレクトリは、以下のように生成されます。

```
./dlc/client_1/tmp/debug_files
./dlc/client_1/log/log_files
./dlc/client_1/getinfo/get_info.txt
```

```
./dlc/client_2/tmp/debug_files
./dlc/client_2/log/log_files
./dlc/client_2/getinfo/get_info.txt ...
```

必要なスペースの推定

データの収集に必要となる Cell Manager 上のディスクスペースを表示するには、`-space` オプションを使用します。

クライアント上のデバッグファイルの削除

収集データをクライアントから削除するには、`-delete_dbg` オプションを使用します。デバッグファイルだけが削除されることに注意してください。getinfo ファイルとログファイルは削除されません。HP Open VMS の場合、`-session` オプションも一緒に使用して `omnidlc` コマンドを実行すると、デバッグファイルディレクトリからデバッグファイルが削除されなくなります。

デバッグファイルについての情報の削除

デバッグログの生成場所 (どのクライアント上か)、および使用されるデバッグ接頭辞の情報を含む `ctrace.log` ファイルを削除するには、`-del_ctracelog` オプションを使用します。`-hosts` *`list`* オプションと一緒に使用すると、そのコマンドにより、特定のクライアント上だけで `ctrace.log` ファイルが削除されます。それ以外の場合は、セル内のすべてのクライアントで `ctrace.log` ファイルが削除されます。

注記: `ctrace.log` ファイルのクリーンアップには、このオプションを使用します。このファイルを削除すると、デバッグログコレクタでデフォルトのディレクトリ (UNIX の場合は `/tmp/dlc`、Windows の場合は Data_Protector_home`\tmp\dlc`) からのみデバッグが取得され、指定した他のデバッグディレクトリからは取得されなくなることに注意してください。

その他の操作

- 圧縮データか未圧縮データかにかかわらず、アンパックされたデータを Cell Manager に送信 (`-depot` オプションを使用) した後でパックするには、`-localpack [`*`filename`*`]` オプションを使用します。

  このオプションでは、カレントディレクトリのディレクトリ構造がパックされます (カレントディレクトリは、`-depot` オプションで生成された `dlc` ディレクトリが含まれるディレクトリでなければなりません)。*`filename`* 引数を省略すると、カレントディレクトリ内に `dlc.pck` ファイルが生成されます。

  このオプションの機能は-pack オプションの機能と同等ですが、`-depot` オプションを使用してデータを収集した場合のみ使用してください。

- クライアントの特定のディレクトリから追加情報 (スクリーンショットやピクチャーなど) を取得するには、`[-add_info [-any | `*`host`*`] `*`path`*`]` オプションを使用します。

  `-any` オプションは、すべてのクライアントでディレクトリパスが同じ場合に使用されます。

- データをアンパックするには、`-unpack [`*`filename`*`]` オプションを使用します。

  `filename` 引数を省略すると、カレントディレクトリ内の `dlc.pck` ファイルがアンパックされます。カレントディレクトリ内の `dlc` ディレクトリが常にデータのアンパック先となります。

  このオプションは、`-pack` オプションまたは`-localpack` オプションのいずれかを使用して収集データを Cell Manager 上でパックした場合に使用してください。

- 単一の圧縮ファイルを展開するには、`-uncompress` *`filename`* オプションを使用します。パックされているデータの場合は、先にアンパックしておく必要があります。
- 詳細出力を有効にするには、`-verbose` オプションを使用します。

問題と回避策

問題

デバッグログの収集に失敗する

デバッグログの収集処理の際に、omnidlc がクライアントに接続できなくなります。以下のエラーが表示されます。

```
client1.company.com からの収集が開始されました。
Error:Data retrieval from client1.company.com failed.
Warning: Collection from client1.company.com incomplete.
```

この問題は、クライアントの構成ファイルで指定されている Cell Manager の名前と、デバッグログの収集で必要とする Cell Manager の名前が一致しない場合に発生します。

対処方法

Cell Manager のホスト名を、`/etc/opt/omni/client` (UNIX クライアント) または *`Data_Protector_home`*`\config\client` (Windows クライアント) にある `omnidlc_hosts` ファイルに追加します。

omnidlc コマンドの使用例

1. 詳細出力を有効にして、セル内のすべてのデバッグファイル、ログファイル、getinfo ファイルを収集して圧縮し、それらを Cell Manager 上のカレントディレクトリに `dlc.pck` ファイルとしてパックするには、次のコマンドを実行します。

   ```
   omnidlc -no_filter -verbose
   ```

2. `client1.company.com` および `client2.company.com` というクライアントからログファイルとデバッグファイルのみを Cell Manager の `c:\depot` ディレクトリに収集し、圧縮もパックも行わないようにするには、次のコマンドを実行します。

   ```
   omnidlc -no_filter -hosts client1.company.com client2.company.com
   -depot c:\depot -no_getinfo -no_compress
   ```

3. `client1.company.com` というクライアントからログファイル、デバッグファイル、getinfo ファイルを収集し、それらを Cell Manager 上の `c:\pack\pack.pck` というファイルに圧縮パックするには、次のコマンドを実行します。

   ```
   omnidlc -hosts client1.company.com -pack c:\pack\pack.pck
   ```

4. クライアント `client1.company.com` および `client2.company.com` 上で、デフォルトの保存場所からログファイル、デバッグファイル、getinfo ファイルを収集するとともに、追加のディレクトリ `C:\tmp` および `/temp/debugs` からデバッグファイルを収集して、Cell Manager 上で圧縮およびパックするには、次のコマンドを実行します。

   ```
   omnidlc -hosts client1.company.com client2.company.com -debug_loc
   C:\tmp /tmp/debugs
   ```

5. ID`2006/05/27-9` に一致するセッションからすべてのデバッグファイルを削除するには、次のコマンドを実行します。

   ```
   omnidlc -session 27.05.06-9 -delete_dbg
   ```

6. クライアント `client.company.com` 上で、デバッグ ID `2351` に一致する未圧縮デバッグファイルに関して、Cell Manager 上で必要となるディスクスペースを表示させるには、次のコマンドを実行します。

   ```
   omnidlc -did 2351 -hosts client.company.com -space -no_getinfo
   -no_logs -no_compress
   ```

7. クライアント `client1.company.com` の `C:\debug` ディレクトリにある他のファイルを、ID `2007/11/17-24` のセッションのデバッグログファイルとともにパックするには、次のコマンドを実行します。

   ```
   omnidlc -session 2007/11/17-24 -add_info -host client1.company.com
   C:\debug
   ```

8. カレントディレクトリのディレクトリ構造を同じディレクトリ内の `dlc.pck` ファイルにパックするには、次のコマンドを実行します (カレントディレクトリは、`-depot` オプションで生成した `dlc` ディレクトリが格納されているディレクトリでなければなりません)。

   ```
   omnidlc -localpack
   ```

9. `dlc.pck` ファイルをカレントディレクトリの `dlc` ディレクトリにアンパックするには、次のコマンドを実行します。

   ```
   omnidlc -unpack
   ```

Data Protector GUI を使用することによるデバッグファイルの処理

Data Protector GUI では、以下のデバッグファイル操作を実行できます。

- デバッグファイルの収集。デバッグファイルがクライアントシステムから収集され、Cell Manager 上に格納されます。
- デバッグファイルスペースの計算。収集ファイル用として Cell Manager 上に必要なスペースが計算されます。
- デバッグファイルの削除。デバッグファイルがクライアントシステムから削除されます。

これらは、内部データベースまたはクライアントのコンテキストで実行できます。

GUI 操作では、`omnidlc` CLI コマンドのさまざまなオプションを使用します。コマンドラインインタフェースで `omnidlc` コマンドを直接使用すると、収集したファイルに対して他の操作も実行できます。詳細については、『HP Data Protector Command Line Interface Reference』を参照してください。

以下の項の操作を実行すると、使用された `omnidlc` 構文が [結果] ウィンドウに表示されます。

デバッグファイル操作の実行

クライアントのコンテキストからデバッグファイル操作にアクセスするには:

1. Scoping ペインで、[クライアント] フォルダを展開し、デバッグファイル操作が必要なクライアントを選択します。
2. 実行する操作を選択します。
   - 選択したアイテムを右クリックし、**[**デバッグファイルの収集**]**、**[**デバッグファイル領域の計算**]**、**[**デバッグファイルの削除**]** の中から必要な操作を選択します。

     または

   - メニューバーで **[**アクション**]** → **[**デバッグファイル**]** を選択してから、**[**収集**]**、**[**スペースのチェック**]**、または **[**削除**]** を選択します。

内部データベースのコンテキストからデバッグファイル操作にアクセスするには:

1. Scoping ペインで、[セッション] フォルダを展開し、デバッグファイル操作が必要なセッションを選択します。
2. 実行する操作を選択します。
   - 選択したアイテムを右クリックし、**[**デバッグファイルの収集**]**、**[**デバッグファイル領域の計算**]**、**[**デバッグファイルの削除**]** の中から必要な操作を選択します。

     または

- メニューバーで [アクション] → [デバッグファイル] を選択してから、[収集]、[スペースのチェック]、または [削除] を選択します。

どちらの場合も、操作を選択するとウィザードが開始され、必要な手順を画面に従って実行できます。

デバッグファイルの収集

デバッグファイルを収集するには:

1. 「デバッグファイル操作の実行」の説明に従って、「デバッグファイルコレクタ」ウィザードを起動します。

   セッションを選択して [内部データベース] コンテキストから開始した場合は、そのセッションがウィザードの [クライアント] ページの [フィルタ] セクションであらかじめ選択され、セッションに関係するクライアントが選択されます。

   [クライアント] コンテキストから開始した場合は、そこで選択したクライアントがウィザードの [クライアント] ページであらかじめ選択されます。

2. [クライアント] ページで、ログを収集するクライアントを限定するために、以下の手順を実行します。
   a. ログを収集するクライアントのみを選択します。クライアントがあらかじめ選択されていた場合、その選択は解除してもかまいません。
   b. [フィルタ] で、フィルタ条件 ([セッション ID]、[デバッグ ID]、[Postfix]、または [フィルタなし]) を選択し、必要な識別子を入力します。[フィルタなし] を選択すると、選択したクライアント上のすべてのデバッグログが収集されます。セッション ID があらかじめ選択されていた場合、それを変更することはできません。
   c. [次へ] をクリックします。
3. [ディレクトリ] ページで、以下の手順を実行します。
   a. デバッグログの有無をチェックするディレクトリが、デフォルトのデバッグファイルディレクトリの他にあればそのディレクトリを入力し、[追加] をクリックします。
   b. 内容を収集するディレクトリが他にある場合は、ディレクトリツリーでそのディレクトリを選択します (サブディレクトリの内容は選択されません)。
   c. [次へ] をクリックします。
4. [オプションと操作] ページで、以下の手順を実行します。
   a. 使用しないデバッグ収集オプションがあれば、選択を解除します。`omnirc` オプションに関する一般情報は、『HP Data Protector Command Line Interface Reference』を参照してください。
   b. デバッグログを Cell Manager に格納する際の操作を選択します。
      - [デポの作成] は、(パックされていない) ファイルを次の場所の `dlc` ディレクトリに保存します。

        `Data_Protector_program_data``\tmp\` (Windows Vista、Windows 7、および Windows Server 2008 の場合)、*`Data_Protector_home`*`\tmp\` (他の Windows システムの場合)、または`/tmp/dlc` (UNIX システムの場合)

        別の場所を指定するには、既存のディレクトリを [ターゲットパス] に入力します。デフォルトの場所を使用する場合は、テキストボックスを空白にしてください。

        このオプションを使用すると、サポート窓口に情報を送付する前に、収集したファイルを確認し任意のファイルを削除できます。続いて、CLI コマンドの `omnidlc -localpack [`*`filename`*`]` を使用して、パックファイルを作成できます (この詳細については、『HP Data Protector Command Line Interface Reference』を参照してください)。

- [パックファイルの作成] (デフォルト) は、パックファイルを現在のディレクトリに作成します。別のディレクトリやファイル名を指定するには、フルパスを [ターゲットパス] に入力します。

c. [完了] をクリックします。

デバッグファイルスペースの計算

実際に収集を行う前に、デバッグファイル収集用として Cell Manager 上に必要な合計スペースを計算できます。それには、必要なすべての収集情報を「デバッグファイル領域計算」ウィザードに入力します。計算が完了したら、指定条件に基づいて収集を開始することができます。

デバッグファイル収集用として Cell Manager に必要な合計スペースを計算するには:

1. 「デバッグファイル操作の実行」の説明に従って、「デバッグファイル領域計算」ウィザードを起動します。
2. [クライアント] ページで、対象とするクライアントを限定するために、以下の手順を実行します。
   a. ファイルを収集するクライアントのみを選択します。クライアントがあらかじめ選択されていた場合、その選択は解除してもかまいません。
   b. [フィルタ] で、フィルタ条件 ([セッション **ID**]、[デバッグ **ID**]、**[Postfix]**、または [フィルタなし]) を選択し、必要な識別子を入力します。[フィルタなし] を選択すると、選択したクライアント上のすべてのデバッグファイルが収集されます。セッション ID があらかじめ選択されていた場合、それを変更することはできません。
   c. [次へ] をクリックします。
3. [ディレクトリ] ページで、以下の手順を実行します。
   a. デバッグファイルの有無をチェックするディレクトリが、デフォルトのデバッグファイルディレクトリの他にあればそのディレクトリを入力し、[追加] をクリックします。
   b. 内容を考慮するディレクトリが他にあれば、そのディレクトリをディレクトリツリーで選択します。
   c. [次へ] をクリックします。
4. [オプション] ページで、以下の手順を実行します。
   a. 使用しないデバッグ収集オプションがあれば、選択を解除します。`omnirc` オプションに関する一般情報は、『HP Data Protector Command Line Interface Reference』を参照してください。
   b. [次へ] をクリックします。

   チェックの結果は [結果] タブに表示されます。

計算が終了すると、ダイアログボックスが表示され、デバッグファイルの収集を開始するかどうかが尋ねられます。

スペース計算に対して選択したオプションを使用して、デバッグファイルの収集を開始するには:

- [はい] をクリックします。

  デフォルトの操作動作 ([パックファイルの作成]) が Cell Manager で使用されます。「デバッグファイルの収集」を参照してください。

デバッグファイルの削除

デバッグファイルをクライアントから削除するには:

1. 「デバッグファイル操作の実行」の説明に従って、「デバッグファイルの削除」ウィザードを起動します。

2. [クライアント] ページで、デバッグファイルを削除するクライアントを限定するために、以下の手順を実行します。
   a. ファイルを削除するクライアントのみを選択します。
   b. **[**フィルタ**]** で、フィルタ条件 (**[**セッション **ID]**、**[**デバッグ **ID]**、**[Postfix]**、または **[**フィルタなし**]**) を選択し、必要な識別子を入力します。**[**フィルタなし**]** を選択すると、選択したクライアント上のすべてのデバッグファイルが削除されます。
   c. **[**次へ**]** をクリックします。
3. [ディレクトリ] ページで、以下の手順を実行します。
   a. デバッグファイルを削除するディレクトリが、デフォルトのデバッグファイルディレクトリの他にあればそのディレクトリを入力し、**[**追加**]** をクリックします。
   b. **[**完了**]** をクリックします。

HP カスタマサポートサービスに送付するデータ収集の例

あるクライアントと Cell Manager に関して、バックアップセッション中に発生した問題についてデバッグファイル、ログファイル、getinfo ファイルを収集するには、以下の手順に従います。

1. 以下のことを行って、エラー環境の規模をできる限り縮小します。
   - 1 つまたは少数のファイルやディレクトリだけを含むバックアップ仕様を作成します。
   - 障害が発生している 1 つのクライアントだけをデバッグの実行対象とします。
2. 情報用のテキストファイルを作成して、以下の情報を入力します。
   - Cell Manager、Media Agent、Disk Agent のクライアントのハードウェア識別名 (例: `HP 9000 シリーズ T-600、Vectra XA`)
   - Windows Media Agent クライアント用 SCSI コントローラ名 (例: `onboard_type/Adaptec xxx/...`)
   - トポロジーの情報 (`omnicellinfo -cell` コマンドの出力から入手可能)
   - `devbra -dev` コマンドの出力 (バックアップデバイスに問題がある場合)
3. 技術的な問題について当社サポート窓口にお問い合わせの上、以下の情報を照会します。
   - デバッグレベル (1-99 など。このコマンドオプションは後で必要になります)
   - デバッグ範囲 (クライアントのみ、Cell Manager のみ、すべてのシステムなど)
4. すべてのユーザーインタフェースを終了して、セル内の他のすべてのバックアップ動作を中止します。
5. CRS デバッグまたは Inet デバッグも同時に収集するには、Cell Manager 上で Inet サービスまたは CRS サービスをデバッグモードで再起動する必要があります。詳細については、「Inet のデバッグ」 (68 ページ) および 「CRS のデバッグ」 (68 ページ) を参照してください。
6. Cell Manager 上で以下のコマンドを実行すると、GUI がデバッグモードで起動します。

   Windows システムの場合: `manager -debug 1-140 error_run.txt`

   UNIX システムの場合: `xomni -debug 1-140 error_run.txt`

   作成されるデバッグファイルの名前の接尾辞には、`error_run.txt` の代わりに、ユーザーが希望する名前を定義できます。
7. Data Protector を使って問題を再現します。
8. すべてのユーザーインタフェースを終了して、デバッグモードを終了します。

   CRS または Inet デバッグも同時に収集した場合は、Cell Manager 上の Data Protector サービスをデバッグオプションなしで再起動する必要があります。

9. Cell Manager 上で次のコマンドを実行します。

   ```
   omnidlc -postfix error_run.txt
   ```

   このコマンドにより、クライアント上のログファイル、getinfo ファイル、デバッグファイルが圧縮され、`error_run.txt` という接尾辞がつけられます。 それらはネットワーク経由で Cell Manager に送信され、現在のディレクトリの `dlc.pck` というファイルにパック、保存されます。詳細は、「HP カスタマサポートサービスに送付するための生成データの準備」 (69 ページ) を参照してください。
10. パックされたファイル（`dlc.pck`）を当社サポートサービス宛に電子メールで送付してください。
11. Cell Manager 上で次のコマンドを実行し、クライアント上に作成されたデバッグファイル (`error_run.txt` という接尾辞が付いたファイル) を削除します。

    ```
    omnidlc -postfix error_run.txt -delete_dbg
    ```

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、AES256 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、バックアップメディア上に保存されると共に、Cell Manager 上の*Data_Protector_program_data*\Config\Server\dr\asr ディレクトリ (Windows Server 2008 の場合)、*Data_Protector_home*\Config\Server\dr\asr ディレクトリ (その他の Windows システムの場合)、または/etc/opt/omni/server/dr/asr ディレクトリ (UNIX システムの場合) に保存されます。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 Catalog Database(カタログデータベース) の略。CDB は 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。選択したロギングレベルによっては、ファイル名とファイルバージョンも格納されます。CDB は、常にセルに対してローカルとなります。
MMDB も参照。

CDF ファイル **(UNIX 固有の用語)**Context Dependent File(コンテキスト依存ファイル) の略。CDF ファイルは、同じパス名でグループ化された複数のファイルからなるファイルです。通常、プロセスのコンテキストに基づいて、これらのファイルのいずれかがシステムによって選択されます。このメカニズムにより、クラスタ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。

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レベルの属性が格納されます。これにより、これらの属性間の整合性を確保でき、これらの属性を共通の方法で操作できます。

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

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

CSM
Data Protector コピーおよび集約セッションマネージャー (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、および Windows Server 2008 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、および Windows Server 2008 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。

DCBF
IDB の詳細カタログバイナリファイル (DCBF) 部には、ファイルのバージョンと属性に関する情報が格納されます。IDB の約 80% を占めるファイルバージョンと属性に関する情報を格納します。バックアップに使用される Data Protector メディアごとに 1 つの DC バイナリファイルが作成されます。サイズの最大値は、ファイルシステムの設定による制限を受けます。

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

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 で記録され、*Data_Protector_program_data*\log\server\Ob2EventLog.txt (Windows Server 2008 の場合)、*Data_Protector_home*\log\server\Ob2EventLog.txt (その他の Windows システムの場合)、/var/opt/omni/server/log/Ob2EventLog.txt (UNIX システムの場合) に書き込まれます。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。

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

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。Windows 用のオリジナルの Data Protector GUI の他に、Data Protector には、さまざまなプラットフォームで実行できる、外観も操作も変わらない Java ベースの GUI も用意されています。

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

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 ブラウザからアクセスできます。
HP P6000 EVA SMI-S Agent および HP SMI-S P6000 EVA アレイプロバイダ 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 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 Operations Manager

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

HP Operations Manager SMART Plug-In(SPI)

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

HP P6000 EVA 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。P6000 EVA SMI-S Agent を使用すると、受信した要求と HP CV EVA 間のやり取りを制御する HP SMI-S P6000 EVA アレイプロバイダ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 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

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 アレイプロバイダは P6000 EVA 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 EVA 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 チャンネル、内部キャッシュメモリ、およびマイクロコードと呼ばれる制御/診断ソフトウェアを備えたディスクアレイデバイスです。

IDB Data Protector の内部データベース。IDB は、Cell Manager 上に維持される埋込み型データベースです。どのデータがどのメディアにバックアップされたか、バックアップ、復元などのセッションがどのように実行されたか、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が格納されます。

IDB 復旧ファイル IDB バックアップ、メディア、バックアップ用デバイスに関する情報を含む IDB ファイル (obrindex.dat)。この情報により、IDB の復旧を大幅に簡素化できます。IDB トランザクションログと共にこのファイルを他の IDB ディレクトリとは別の物理ディスクに移動し、さらにこのファイルのコピーを作成することをお勧めします。

Inet Data Protector セル内の各 UNIX システムまたは Windows システム上で動作するプロセス。このプロセスは、セル内のシステム間の通信と、バックアップおよび復元に必要なその他のプロセスの起動を受け持ちます。システムに Data Protector をインストールすると、Inet サービスが即座に起動されます。Inet プロセスは、inetd デーモンにより開始されます。

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

Informix Server 用の CMD スクリプト **(Informix Server 固有の用語)**Informix Server データベースの構成時に INFORMIXDIR 内に作成される Windows CMD スクリプト。環境変数を Informix Server にエクスポートするコマンド一式が含まれています。

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。

J

Java GUI クライアント Java GUI クライアントは Java GUI コンポーネントの 1 つで、ユーザーインタフェース関連の機能 (Cell Manager グラフィカルユーザーインタフェースおよび Manager-of-Managers(MoM) のグラフィカルユーザーインタフェース) のみで構成されており、機能するためには Java GUI サーバーと接続する必要があります。

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

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 リスナを定義します。

log_full シェルスクリプト **(Informix Server UNIX 固有の用語)**ON-Bar に用意されているスクリプトの 1 つで、Informix Server で logfull イベント警告が発行された際に、論理ログファイルのバックアップを開始するために使用できます。Informix Server の `ALARMPROGRAM` 構成パラメータは、デフォルトで、*`INFORMIXDIR`*`/etc/log_full.sh` に設定されます。ここで、*`INFORMIXDIR`* は、Informix Server ホームディレクトリです。論理ログファイルを継続的にバックアップしたくない場合は、`ALARMPROGRAM` 構成パラメータを*`INFORMIXDIR`*`/etc/no_log.sh` に設定してください。

Lotus C API **(Lotus Domino Server 固有の用語)**Lotus Domino Server と Data Protector などのバックアップソリューションの間でバックアップ情報および復元情報を交換するためのインタフェース。

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

Microsoft 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、およびオペレーティングシステムカーネルと連携して、ボリュームシャドウコピーおよびシャドウコピーセットの管理を実現します。
シャドウコピー、シャドウコピープロバイダ、複製およびライター も参照。

MMD Media Management Daemon (メディア管理デーモン) の略。MMD プロセス (サービス) は、Data Protector Cell Manager 上で稼動し、メディア管理操作およびデバイス操作を制御します。このプロセスは、Data Protector を Cell Manager にインストールしたときに開始されます。

MMDB Media Management Database(メディア管理データベース) の略。MMDB は、IDB の一部です。セル内で構成されているメディア、メディアプール、デバイス、ライブラリ、ライブラリデバイス、スロットに関する情報と、バックアップに使用されている Data Protector メディアに関する情報を格納します。エンタープライズバックアップ環境では、データベースをすべてのセル間で共有できます。
CMMDB および CDB も参照。

MoM 複数のセルをグループ化して、1 つのセルから集中管理することができます。集中管理用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。

O

obdrindex.dat IDB 復旧ファイル を参照。

OBDR 対応デバイス ブート可能ディスクを装填した CD-ROM ドライブをエミュレートできるデバイス。バックアップデバイスとしてだけでなく、ディザスタリカバリ用のブートデバイスとしても使用可能です。

ON-Bar **(Informix Server 固有の用語)**Informix Server のためのバックアップと復元のシステム。ON-Bar により、Informix Server データのコピーを作成し、後でそのデータを復元することが可能になります。ON-Bar のバックアップと復元のシステムには、以下のコンポーネントが含まれます。

- `onbar` コマンド
- バックアップソリューションとしての Data Protector
- XBSA インタフェース
- ON-Bar カタログテーブル。これは、dbobject をバックアップし、複数のバックアップを通して dbobject のインスタンスをトラッキングするために使われます。

ONCONFIG **(Informix Server 固有の用語)** アクティブな ONCONFIG 構成ファイルの名前を指定する環境変数。ONCONFIG 環境変数が存在しない場合、Informix Server が*INFORMIXDIR*`\etc`(Windows の場合)、または*INFORMIXDIR*`/etc/`(UNIX の場合) ディレクトリの `ONCONFIG` ファイルにある構成値を使います。

Oracle Data Guard **(Oracle 固有の用語)**Oracle Data Guard は Oracle の主要なディザスタリカバリソリューションです。プロダクション (一次) データベースのリアルタイムコピーであるスタンバイデータベースを最大 9 個まで保持することにより、破損、データ障害、人為ミス、および災害からの保護を提供します。プロダクション (一次) データベースに障害が発生すると、フェイルオーバーによりスタンバイデータベースの 1 つを新しい一次データベースにすることができます。また、プロダクション処理を現在の一次データベースからスタンバイデータベースに迅速に切り替えたり、元に戻したりできるため、保守作業のための計画ダウンタイムを縮小することができます。

ORACLE_SID **(Oracle 固有の用語)**Oracle Server インスタンスの一意な名前。別の Oracle Server に切り替えるには、目的の*ORACLE_SID* を指定します。*ORACLE_SID* は、`TNSNAMES.ORA` ファイル内の接続記述子の CONNECT DATA 部分と `LISTENER.ORA` ファイル内の TNS リスナの定義に含まれています。

Oracle インスタンス **(Oracle 固有の用語)**1 つまたは複数のシステムにインストールされた個々の Oracle データベース。1 つのコンピュータシステム上で、複数のデータベースインスタンスを同時に稼動させることができます。

Oracle ターゲットデータベースへのログイン情報

(Oracle および SAP R/3 固有の用語) ログイン情報の形式は、*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。

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。このファイルはフルバックアップ中に作成され、バックアップメディアと Cell Manager に保存されます。保存場所は、*Data_Protector_program_data*\Config\Server\dr\p1s ディレクトリ (Windows Server 2008 の場合)、*Data_Protector_home*\Config\Server\dr\p1s ディレクトリ (その他の Windows システムの場合)、/etc/opt/omni/server/dr/p1s ディレクトリ (UNIX システムの場合) です。ファイル名は以下のとおりです。recovery.p1s.

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。

RDS

Raima Database Server の略。RDS(サービス) は、Data Protector Cell Manager 上で稼動し、IDB を管理します。このプロセスは、Data Protector を Cell Manager にインストールしたときに開始されます。

Recovery Manager (RMAN)

(Oracle 固有の用語) Oracle コマンド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、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。

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

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 EVA 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) またはレジストリ (Windows)。各データベースサーバーの名前の他、ホストコンピュータ上のクライアントが接続できるエイリアスが格納されます。

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

SRD ファイル **(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。

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。

TSANDS.CFG ファイル **(Novell NetWare 固有の用語)** バックアップを開始するコンテナの名前を指定するファイル。このファイルはテキストファイルで、`TSANDS.NLM` がロードされるサーバーの `SYS:SYSTEM\TSA` ディレクトリにあります。

U

UIProxy Java GUI サーバー (`UIProxy` サービス) は Data Protector Cell Manager で実行されます。Java GUI サーバーでは、Java GUI クライアントと Cell Manager との間の通信を行います。また、ビジネスロジック操作を実行し、重要な情報のみをクライアントに送信する必要があります。このサービスは、Data Protector が Cell Manager 上にインストールされるとすぐに開始されます。

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の操作モードの 1 つ。P9000 XP アレイプロバイダが VSS 準拠モードであると、ソースボリューム (P-VOL) とその複製 (S-VOL) は、バックアップ後、単純非対状態になります。したがって、ローテーションされる複製数 (P-VOL 当たりの S-VOL

数) に制限はありません。このような構成でのバックアップからの復元は、ディスクの切り替えによってのみ可能となります。
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 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。

Windows レジストリ オペレーティングシステムやインストールされたアプリケーションの構成情報を保存するため、Windows により使用される集中化されたデータベース。

WINS サーバー Windows ネットワークのコンピュータ名を IP アドレスに解決する Windows インターネットネームサービスソフトウェアを実行しているシステム。Data Protector では、WINS サーバーデータを Windows の構成データの一部としてバックアップできます。

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ストアには、複数のユーザーで共有するパブリックフォルダおよびメッセージがあります。
キーマネージメントサービスおよびサイト複製サービス も参照。

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 SCSI エクスチェンジャとも呼ばれます。

ライブラリ も参照。

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

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 の復旧は、常にオフラインで行われます。

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

オンライン 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 オンライン復旧は、Cell Manager がアクセス可能な場合に行います。この場合、Data Protector のほとんどの機能 (Cell Manager によるセッションの実行、復元セッションの IDB への記録、GUI を使った復元作業の進行状況の監視など) が使用可能です。

か

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。

仮想コントローラソフトウェア (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。

カタログ保護 バックアップデータに関する情報 (ファイル名やファイルバージョンなど) を IDB に維持する期間を定義します。
データ保護 も参照。

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。

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。

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

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

こ

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。

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、DOS コマンドや UNIX コマンドと同じようにシェルスクリプト内で使用でできるコマンドが用意されています。これらを通じて、Data Protector の構成、管理、バックアップ/復元タスクを実行することができます。

コンテナ **(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。

さ

再解析ポイント **(Windows 固有の用語)** 任意のディレクトリまたはファイルに関連付けることができるシステム制御属性。再解析属性の値は、ユーザー制御データをとることができます。このデータの形式は、データを保存したアプリケーションによって認識され、データの解釈用にインストールされており、該当ファイルを処理するファイルシステムフィルタによっても認識されます。ファイルシステムは、再解析ポイント付きのファイルを検出すると、そのデータ形式に関連付けられているファイルシステムフィルタを検索します。

再同期モード **(HP P9000 XP ディスクアレイファミリ VSS プロバイダ固有の用語)** 2 種類ある P9000 XP アレイ VSS ハードウェアプロバイダの操作モードの 1 つ。P9000 XP アレイプロバイダが再同期モードであると、ソースボリューム (P-VOL) とその複製 (S-VOL) は、バックアップ後、中断ミラー関係になります。MU 範囲が 0-2(つまり、0、1、2) の場合、ローテーションされる最大複製数 (P-VOL 当たりの S-VOL 数) は 3 となります。このような構成でのバックアップからの復元は、S-VOL をその P-VOL と再同期することによってのみ可能となります。
VSS 準拠モード、ソースボリューム、プライマリボリューム (P-VOL)、複製、セカンダリボリューム (S-VOL)、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。

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 2003 のサービス。
インフォメーションストアおよびキーマネージメントサービス も参照。

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

差分バックアップ 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。

し

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。

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

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

システム復旧データファイル SRD ファイル を参照。

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。

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

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

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

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

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。

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 **(Microsoft VSS 固有の用語)** ボリュームシャドウコピーの作成と表現を行うエンティティ。プロバイダは、シャドウコピーデータを所有して、シャドウコピーを公開します。プロバイダは、ソフトウェア (システムプロバイダなど) で実装することも、ハードウェア (ローカルディスクやディスクアレイ) で実装することもできます。
シャドウコピー も参照。

ジュークボックス ライブラリ を参照。

ジュークボックスデバイス 光磁気メディアまたはファイルメディアを格納するために使用する、複数のスロットからなるデバイス。ファイルメディアの格納に使用する場合、ジュークボックスデバイスは「ファイルジュークボックスデバイス」と呼ばれます。

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

オブジェクトのコピーまたは統合を行う場合のオーナーは、コピー仕様や統合仕様で別のオーナーが指定されていない限り、デフォルトでは、その操作を開始するユーザーです。

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

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 P10000 Storage Systems 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 P10000 Storage Systems 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。

スマートコピー **(VLS 固有の用語)** 仮想テープから物理テープライブラリへ作成されたバックアップデータのコピー。スマートコピーのプロセスによって、Data Protector ではソースメディアとターゲットメディアを区別できるため、メディア管理が可能になります。
仮想ライブラリシステム (VLS) も参照。

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

スレッド **(Microsoft SQL Server 固有の用語)** 1 つのプロセスのみに属する実行可能なエンティティ。プログラムカウンタ、ユーザーモードスタック、カーネルモードスタック、およびレジスタ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

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。

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。

そ

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。

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。

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

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

- disk タイプ
- sbt_tape タイプ

Oracle が Data Protector と統合されており、指定されたチャンネルの種類が sbt_tape タイプの場合は、上記のサーバープロセスが Data Protector に対してバックアップの読み取りとデータファイルの書き込みを試行します。

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 (raw ディスク) のバックアップ ディスクイメージのバックアップでは、ファイルがビットマップイメージとしてバックアップされるので、高速バックアップが実現します。ディスクイメージ (raw ディスク) バックアップでは、ディスク上のファイルおよびディレクトリの構造はバックアップされませんが、ディスクイメージ構造がバイトレベルで保存されます。ディスクイメージバックアップは、ディスク全体か、またはディスク上の特定のセクションを対象にして実行できます。

ディスククォータ コンピュータシステム上のすべてのユーザーまたはユーザーのサブセットに対してディスクスペースの消費を管理するためのコンセプト。このコンセプトは、いくつかのオペレーティングシステムプラットフォームで採用されています。

ディスクグループ **(Veritas Volume Manager 固有の用語)**VxVM システム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 通信チャンネルを通じて転送されるデータのシーケンス。

データファイル **(Oracle および SAP R/3 固有の用語)**Oracle によって作成される物理ファイル。表や索引などのデータ構造を格納します。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。

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

データベースの差分バックアップ 前回のフルデータベースバックアップ以降にデータベースに対して加えられた変更だけを記録するデータベースバックアップ。

データベースの並列処理 (数) 十分な台数のデバイスが利用可能で、並列バックアップを実行できる場合には、複数のデータベースが同時にバックアップされます。

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

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

テープ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、テープへの書込みを再開します。言い換えると、テープにデータを書き込む速度が、コンピュータシステムがデバイスへデータを送信する速度以下の場合、

デバイスはストリーミングを行います。ストリーミングは、スペースの使用効率とデバイスのパフォーマンスを大幅に向上します。

デバイスチェーン デバイスチェーンは、シーケンシャルに使用するように構成された複数のスタンドアロンデバイスからなります。デバイスチェーンに含まれるデバイスのメディアで空き容量がなくなると、自動的に次のデバイスのメディアに切り替えて、バックアップを継続します。

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

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。

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

ドライブ コンピュータシステムからデータを受け取って、磁気メディア (テープなど) に書き込む物理装置。データをメディアから読み取って、コンピュータシステムに送信することもできます。

ドライブのインデックス ライブラリデバイス内のドライブの機械的な位置を識別するための数字。ロボット機構によるドライブアクセスは、この数に基づいて制御されます。

ドライブベースの暗号化 Data Protector のドライブベースの暗号化では、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 **(Data Protector 固有の用語)**IDB に対する変更を記録します。IDB 復旧に必要なトランザクションログファイル (前回の IDB バックアップ以降に作成されたトランザクションログ) が失われることがないように、トランザクションログのアーカイブを有効化しておく必要があります。

トランザクションログテーブル **(Sybase 固有の用語)** データベースに対するすべての変更が自動的に記録されるシステムテーブル。

トランザクションログバックアップ トランザクションログバックアップは、一般に、データベースのバックアップよりも必要とするリソースが少ないため、データベースのバックアップよりもより高い頻度で実行できます。トランザクションログバックアップを用いることにより、データベースを特定の時点の状態に復旧できます。

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。

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。

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。

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 (raw ディスク) の場合もあります。

バックアップオブジェクトは以下のように定義されます。

- クライアント名: バックアップオブジェクトが保存される Data Protector クライアントのホスト名
- マウントポイント: ファイルシステムオブジェクトを対象とする場合 — バックアップオブジェクトが存在するクライアント (Windows ではドライブ、UNIX ではマウントポイント) 上のディレクトリ構造におけるアクセスポイント。統合オブジェクトを対象とする場合 — バックアップストリーム ID。バックアップされたデータベース項目/アプリケーション項目を示します。
- 説明: ファイルシステムオブジェクトを対象とする場合 — 同一のクライアント名とマウントポイントを持つオブジェクトを一意に定義します。統合オブジェクトを対象とする場合 — 統合の種類を表示します (例: SAP または Lotus)。
- 種類: バックアップオブジェクトの種類。ファイルシステムオブジェクトを対象とする場合 — ファイルシステムの種類 (例: WinFS)。統合オブジェクトを対象とする場合 — 「Bar」

バックアップシステム **(ZDB 固有の用語)** 1 つ以上のアプリケーションシステム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。

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。

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

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。

ふ

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

ファイルシステム 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。

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

ファイル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。

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

フェイルオーバー **(HP 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) 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。

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

複製 **(ZDB 固有の用語)** ユーザー指定のバックアップオブジェクトを含む、特定の時点におけるソースボリュームのデータのイメージ。イメージは、作成するハードウェアまたはソフトウェアによって、物理ディスクレベルでの記憶ブロックの独立した正確な複製 (クローン) になる (スプリットミラーやスナップクローンなど) 場合もあれば、仮想コピーになる (スナップショットなど) 場合もあります。基本的なオペレーティングシステムの観点からすると、バックアッ

プオブジェクトを含む物理ディスク全体が複製されます。しかし、UNIX でボリュームマネージャーを使用するときは、バックアップオブジェクトを含むボリュームまたはディスクグループ全体が複製されます。Windows でパーティションを使用する場合、選択したパーティションを含む物理ボリューム全体が複製されます。
スナップショット、スナップショット作成、スプリットミラー、およびスプリットミラーの作成 も参照。

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。

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。

分散ファイルシステム (DFS) 複数のファイル共有を単一の名前空間に接続するサービス。対象となるファイル共有は、同じコンピュータに置かれていても、異なるコンピュータに置かれていてもかまいません。DFS は、リソースの保存場所の違いに関係なくクライアントがリソースにアクセスできるようにします。

ペアステータス **(HP 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

保護 データ保護およびカタログ保護 を参照。

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。

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)。

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 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が指定されている場合は、メールボックスから個人用フォルダに電子メールがルーティングされます。

メールボックスストア **(Microsoft Exchange Server 固有の用語)** インフォメーションストアのうち、ユーザーメールボックス内の情報を維持する部分。メールボックスストアは、バイナリデータを格納するリッチテキスト.edb ファイルと、ストリーミングネイティブインターネットコンテンツを格納する.stm ファイルからなります。

メディア ID Data Protector がメディアに割り当てる一意な識別子。

メディア管理セッション 初期化、内容のスキャン、メディア上のデータの確認、メディアのコピーなどのアクションをメディアに対して実行するセッション。

メディア集中管理データベース (CMMDB) CMMDB を参照。

メディア状態要素 使用回数のしきい値と上書きのしきい値。メディアの状態の判定基準となります。

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

メディアの位置 バックアップメディアが物理的に収納されている場所を示すユーザー定義の識別子。"building 4"や"off-site storage"のような文字列です。

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

メディアのエクスポート メディアに格納されているすべてのバックアップセッション情報 (システム、オブジェクト、ファイル名など) を IDB から削除するプロセス。メディア自体に関する情報やメディアとプールの関係に関する情報も IDB から削除されます。メディア上のデータは影響されません。メディアのインポート も参照。

メディアの種類 メディアの物理的な種類 (DDS や DLT など)。

メディアの状態 メディア状態要素から求められるメディアの品質。テープメディアの使用頻度が高く、使用時間が長ければ、読み書きエラーの発生率が高くなります。状態が [不良] になったメディアは交換する必要があります。

メディアの使用法 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。

や

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

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 および Windows Server 2008 のセキュリティコンポーネント。管理者が権限レベルを上げるまで、アプリケーションソフトウェアを標準のユーザー権限に限定します。

ユーザーグループ 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。

ユーザー権限 特定の Data Protector タスクの実行に必要なパーミッションをユーザー権限またはアクセス権限と呼びます。主なユーザー権限には、バックアップの構成、バックアップセッションの開始、復元セッションの開始などがあります。ユーザーには、そのユーザーの所属先ユーザーグループに関連付けられているアクセス権限が割り当てられます。

ユーザーディスク割り当て NTFS の容量管理サポートを使用すると、共有ストレージボリュームに対して、拡張された追跡メカニズムの使用およびディスク容量に対する制御が行えるようになります。Data Protector では、システム全体にわたるユーザーディスク割り当てが、すべてのユーザーに対して一度にバックアップされます。

ユーザープロファイル **(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。

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 ロギングレベルは、バックアップ、オブジェクトのコピー、またはオブジェクトの集約時にファイルとディレクトリに関する情報をどの程度まで詳細に IDB に記録するかを示します。バックアップ時のロギングレベルに関係なく、データの復元は常に可能です。Data Protector には、[すべてログに記録]、[ディレクトリレベルまでログに記録]、[ファイルレベルまでログに記録]、および [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、バックアップ速度、および復元データのブラウザのしやすさが影響を受けます。

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 の各ブール演算子を使用できます。複数の検索条件をブール演算子で組み合わせて指定することで、検索対象をより正確に絞り込むことができます。複数単語の検索に演算子を指定しなければ、AND を指定したものとみなされます。たとえば、「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。

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。

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。

索引