HP Data Protector A.06.10
ディザスタ リカバリ ガイド

B6960-96060

製品番号： B6960-96060
初版： 2008年11月

invent

ご注意

本書で取り扱っているコンピュータ ソフトウェアは秘密情報であり、 その保有、使用、または複製には、Hewlett-Packard Companyから使用許諾を得る必要があります。 米国政府の連邦調達規則であるFAR 12.211および12.212の規定に従って、コマーシャル コンピュータ ソフトウェア、コンピュータ ソフトウェア ドキュメンテーションおよびコマーシャル アイテムのテクニカル データ（Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items）は、ベンダが提供する標準使用許諾規定に基づいて米国政府に使用許諾が付与されます。

本書に記載されている内容は事前の通知なしに変更されることがあります。 HP製品およびサービスに対する保証は、当該製品およびサービスに付属の明示的保証規定に記載されているものに限られます。 ここでの記載で追加保証を意図するものは一切ありません。 本書の内容につきましては万全を期しておりますが、本書の技術的あるいは校正上の誤り、省略に対しては責任を負いかねますのでご了承ください。

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

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

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

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

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

UNIXは、The Open Groupの登録商標です。

Printed in the US

目次

図目次

表目次

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	出版年月	製品
B6960-96029	2006 年 7 月	Data Protector リリース A.06.00
B6960-96060	2008 年 11 月	Data Protector リリース A.06.10

本書について

本書では、以下について説明します。

- ディザスタ リカバリのプランニングと準備
- ディザスタ リカバリ手順のテスト
- ディザスタ リカバリの正しい実行方法

対象読者

このマニュアルは、ディザスタ リカバリの計画、準備、テスト、および実行を担当するバックアップ管理者を対象としており、以下に関する知識があることを前提としています。

- Data Protector概念
- Data Protector のバックアップおよび復元手順

ドキュメント セット

その他のドキュメントおよびオンライン ヘルプでは、関連情報が提供されます。

ガイド

Data Protectorのガイドは、印刷された形式あるいはPDF形式で利用できます。PDFファイルは、Data Protectorのセットアップ時に、Windowsの場合はEnglish documentation and Helpコンポーネントを、UNIXの場合はOB2-DOCSコンポーネントを、それぞれ選択してインストールします。 インストールすると、このガイドはWindowsの場合は*Data_Protector_home*\docsディレクトリ、UNIXの場合は/opt/omni/doc/C/ディレクトリに保存されます。

これらの資料は、HP Business Support CenterのWebサイトの[Manuals]ページから入手できます。

http://www.hp.com/support/manuals

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

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

- 『HP Data Protector インストールおよびライセンスガイド』
  このガイドでは、Data Protectorソフトウェアのインストール方法をオペレーティング システムおよび環境のアーキテクチャごとに説明しています。また、Data Protectorのアップグレード方法や、環境に適したライセンスの取得方法についても説明しています。
- 『HP Data Protector トラブルシューティングガイド』
  このガイドでは、Data Protectorの使用中に起こりうる問題に対するトラブルシューティングの方法について説明します。
- 『HP Data Protector ディザスタリカバリガイド』
  このガイドでは、ディザスタ リカバリのプランニング、準備、テスト、および実行の方法について説明します。
- 『HP Data Protector インテグレーションガイド』
  このマニュアルでは、さまざまなデータベースやアプリケーションをバックアップおよび復元するための、Data Protectorの構成方法および使用法を説明します。 このマニュアルは、バックアップ管理者やオペレータを対象としています。4種類のガイドがあります。
  - 『HP Data Protector Microsoft アプリケーション用インテグレーションガイド： SQL Server、SharePoint Portal Server、Exchange Server、および Volume Shadow Copy Service』
    このガイドでは、Microsoft Exchange Server、Microsoft SQL Server、Volume Shadow Copy ServiceといったMicrosoftアプリケーションに対応するData Protectorの統合ソフトウェアについて 説明します。
  - 『HP Data Protector インテグレーションガイド – Oracle、SAP』
    このガイドでは、Oracle、SAP R3、SAP DB/MaxDB に対応するData Protectorの統合ソフトウェアについて説明します。
  - 『HP Data Protector integration guide for IBM applications： Informix, DB2, and Lotus Notes/Domino』
    このガイドでは、Informix Server、IBM DB2、Lotus Notes/Domino ServerといったIBMアプリケーションに対応するData Protectorの統合ソフトウェアについて 説明します。
  - 『HP Data Protector integration guide for VMware Virtual Infrastructure, Sybase, Network Node Manager, and Network Data Management Protocol Server』
    このガイドでは、VMware Virtual Infrastructure、Sybase、Network Node Manager、および Network Data Management Protocol Serverに対応するData Protector の統合ソフトウェアについて説明します。
- 『HP Data Protector integration guide for HP Service Information Portal』
  このガイドでは、HP Service Information Portalに対応するData Protector統合ソフトウェアのインストール、構成、使用方法について説明します。 これはバックアップ管理者用です。 ここでは、アプリケーションを使用して Data Protector サービスを管理する方法について説明しています。
- 『HP Data Protector integration guide for HP Reporter』
  このマニュアルでは、HP Reporter に対応する Data Protector 統合ソフトウェアのインストール、構成、使用方法について説明します。これはバック

アップ管理者用です。 Data Protector のサービス管理にアプリケーションを使用する方法について説明します。

- 『HP Data Protector integration guide for HP Operations Manager for UNIX』
  このガイドでは、UNIX 版の HP Operations Manager software 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 software と HP Service Navigator を使用して、Data Protector 環境の健全性と性能を監視および管理する方法について説明します。
- 『HP Data Protector integration guide for HP Performance Manager and HP Performance Agent』
  このマニュアルでは、Windows 版、HP-UX 版、Solaris 版、Linux 版のHP Performance Manager (PM) および HP Performance Agent (PA) を使用して Data Protector 環境の健全性と性能を監視および管理する方法について説明します。
- 『HP Data Protector ゼロダウンタイムバックアップ コンセプトガイド』
  このガイドでは、Data Protectorゼロ ダウンタイム バックアップとインスタント リカバリのコンセプトについて解説するとともに、ゼロ ダウンタイム バックアップ環境におけるData Protectorの動作原理を詳細に説明します。手順を中心に説明している『HP Data Protector zero downtime backup administrator's guide』および『HP Data Protector zero downtime backup integration guide』とあわせてお読みください。
- 『HP Data Protector zero downtime backup administrator's guide』
  このガイドでは、HP StorageWorks Virtual Array、HP StorageWorks Enterprise Virtual Array、EMC Symmetrix Remote Data FacilityおよびTimeFinder、HP StorageWorks Disk Array XPに対応するData Protector統合ソフトウェアのインストール、構成、使用方法について説明します。 このマニュアルは、バックアップ管理者やオペレータを対象としています。ファイルシステムやディスク イメージのゼロ ダウンタイム バックアップ、インスタント リカバリ、および復元についても説明します。
- 『HP Data Protector zero downtime backup integration guide』
  このガイドでは、Oracle、SAP R/3、Microsoft Exchange Server 2000/2003、およびMicrosoft SQL Server 2000データベースのゼロ ダウンタイム バックアップ、インスタント リカバリ、および標準復元を行うための、Data Protectorの構成方法および使用法について説明します。また、Microsoft Volume Shadow Copy Serviceを使用してバックアップ、および復元を実行するためのData Protectorの構成方法および使用方法についても説明します。
- HP Data Protector MPE/iX system user guide
  このマニュアルでは、MPE/iXクライアントの構成方法、およびMPE/iXデータのバックアップおよび復元方法を説明します。
- HP Data Protector『Media Operations user guide』

このガイドでは、オフライン ストレージ メディアのトラッキングと管理について説明します。アプリケーションのインストールと構成、日常のメディア操作、およびレポート作成のタスクについて説明します。

- 『HP Data Protector product announcements ソフトウェアノートおよびリファレンス』
  このガイドでは、HP Data Protector A.06.10の新機能について説明しています。また、サポートされている構成(デバイス、プラットフォームおよびオンライン データベースの統合ソフトウェア、SAN、ZDB)、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。 サポートされている構成の更新バージョンは、http://www.hp.com/support/manuals にあります。
- 『HP Data Protector product announcements ソフトウェアノートおよびリファレンス for integrations to HP Operations Manager, HP Reporter, HP Performance Manager, HP Performance Agent, and HP Service Information Portal』
  このガイドは、記載されている統合ソフトウェアに対して同様の役割を果たします。
- 『HP Data Protector Media Operations Product Announcements, Software Notes, and references』
  このガイドは、Media Operationsに対して同様の役割を果たします。

オンライン ヘルプ

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

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

- ***Windows の場合***:ZipファイルDP_help.zipを解凍し、DP_help.chmを開きます。
- ***UNIX の場合***:圧縮されたtarファイルDP_help.tar.gzをアンパックし、DP_help.htmでオンライン ヘルプ システムにアクセスします。

ドキュメントマップ

略称

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

略称	ガイド
CLI	コマンド行インタフェース リファレンス
Concepts	コンセプトガイド
DR	ディザスタ リカバリ ガイド
GS	スタート･ガイド
Help	オンライン ヘルプ
IG-IBM	IBMアプリケーション用インテグレーションガイド
IG-MS	Microsoftアプリケーション用インテグレーションガイド
IG-O/S	インテグレーション ガイド — Oracle、SAP R/3、SAP DB/MaxDB
IG-OMU	インテグレーション ガイド — HP Operations Manager software、UNIX
IG-OMW	インテグレーション ガイド — HP Operations Manager software、Windows
IG-PM/PA	インテグレーション ガイド — Performance ManagerおよびHP Performance Agent
IG-Report	インテグレーションガイド — HP Reporter
IG-SIP	インテグレーションガイド — HP Service Information Portal
IG-Var	インテグレーションガイド — VMware、Sybase、Network Node Manager、およびNDMP Server
Install	インストールおよびライセンスガイド
MO GS	Media Operations Getting Started Guide
MO RN	Media Operations Product Announcements, Software Notes, and References
MO UG	Media Operations User Guide
MPE/iX	MPE/iX System User Guide
PA	製品に関するお知らせ、ソフトウェア使用上の注意およびリファレンス
Trouble	トラブルシューティング ガイド
ZDB Admin	ZDB Administrator's Guide
ZDB Concept	ゼロダウンタイム バックアップ コンセプトガイド
ZDB IG	ZDB Integration Guide

対応表

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

	Help	GS	Concepts	Install	Trouble	DR	PA	インテグレーションガイド								ZDB			MO			MPE/iX	CLI
								MS	O/S	IBM	Var	SIP	Report	OMU	OMW	Concept	Admin	IG	GS	User	PA		
バックアップ	X	X	X					X	X	X	X					X	X	X				X	
CLI																							X
概念 / 手法	X		X					X	X	X	X	X		X	X	X	X	X				X	
障害復旧	X		X			X																	
インストール / アップグレード	X	X		X			X					X		X	X				X	X		X	
インスタントリカバリ	X		X													X	X	X					
ライセンス	X			X			X													X			
制限事項	X				X		X	X	X	X	X				X			X			X		
新機能	X						X																
プランニング方法	X		X									X				X							
手順 / 作業	X			X	X	X		X	X	X	X	X		X	X		X	X		X			
推奨事項			X				X									X					X		
必要条件				X			X	X	X	X	X				X				X	X	X		
復元	X	X	X					X	X	X	X						X	X				X	
サポート一覧							X																
サポートされる構成																X							
トラブルシューティング	X			X	X			X	X	X	X	X					X	X					

統合

以下の統合に関する詳細については、該当するガイドを参照してください。

統合	ガイド
HP Operations Manager software for UNIX/for Windows	IG-OMU、IG-OMW
HP Performance Manager	IG-PM/PA
HP Performance Agent	IG-PM/PA
HP Reporter	IG-R
HP Service Information Portal	IG-SIP
HP StorageWorks Disk Array XP	すべてのZDB
HP StorageWorks Enterprise Virtual Array (EVA)	すべてのZDB
HP StorageWorks Virtual Array (VA)	すべてのZDB
IBM DB2 UDB	IG-IBM
Informix	IG-IBM
Lotus Notes/Domino	IG-IBM
Media Operations	MO User
MPE/iX System	MPE/iX
Microsoft Exchange Server	IG-MS、ZDB IG
Microsoft Exchange Single Mailbox	IG-MS
Microsoft SQL Server	IG-MS、ZDB IG
Microsoft Volume Shadow Copy Service (VSS)	IG-MS、ZDB IG
NDMP Server	IG-Var
Network Node Manager (NNM)	IG-Var
Oracle	IG-O/S
Oracle ZDB	ZDB IG
SAP DB	IG-O/S
SAP R/3	IG-O/S、ZDB IG
Sybase	IG-Var
Symmetrix (EMC)	すべてのZDB
VMware	IG-Var

表記上の規則および記号

表 2 表記上の規則

表記	要素
ミディアム ブルーのテキスト：表 2 (18 ページ)	クロスリファレンス リンクおよびEメール アドレス
青色の下線付き語句： http://www.hp.com	Webサイト アドレス
斜体 テキスト	テキストの強調
固定スペース テキスト	▪ ファイルおよびディレクトリの名前 ▪ システム出力 ▪ コード ▪ コマンド、その引数、および引数の値
固定スペース、斜体 テキスト	▪ コード変数 ▪ コマンド変数
テキスト	強調された固定スペースのテキスト

△ **注意：**

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

重要：

詳細情報または特定の手順を示します。

注記：

補足情報を示します。

ヒント：

役に立つ情報やショートカットを示します。

Data Protectorグラフィカル ユーザー インタフェース

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

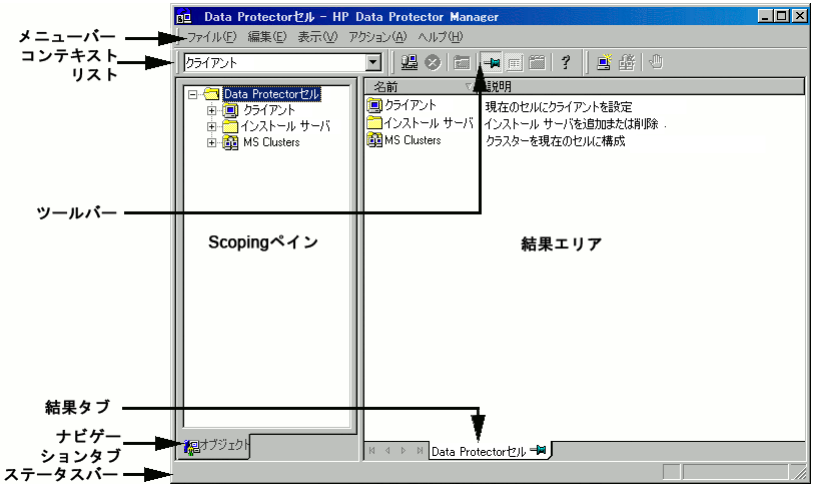


図 1 Data Protectorグラフィカル ユーザー インタフェース

一般情報

Data Protectorの概要については、以下のWebサイトでご覧いただけます。
http://www.hp.com/go/dataprotector.

HPテクニカル サポート

この製品のテクニカルサポートについては、次のHPサポートのWebサイトに記載されています。

http://www.hp.com/support

HPにお問い合わせになる前に、次の情報を収集してください。

- 製品のモデル名とモデル番号
- テクニカル サポートの登録番号（該当する場合）
- 製品シリアル番号
- エラー メッセージ

- オペレーティング システムの種類とリビジョン レベル
- 質問の詳細

製品サービスへの登録

下記のSubscriber's Choice for BusinessのWebサイトに製品を登録することをお勧めします。

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

登録を済ませると、製品のアップグレード、ドライバの新しいバージョン、ファームウェア アップデートなどの製品リソースに関する通知を電子メールで受け取ることができます。

HP Webサイト

その他の情報については、次のHP Webサイトを参照してください。

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

ご意見、ご感想

HPでは、お客様からのフィードバックを歓迎いたします。

製品ドキュメントについてのご意見、ご感想は、次のアドレスに電子メールでご送信ください。 DP.DocFeedback@hp.com.ご送信いただいた内容は、HPに帰属します。

1 概要

概要

この章では、ディザスタ リカバリ プロセス全体の概要を示すとともに、『ディザスタ リカバリ ガイド』で使用されている基本用語について説明し、基本的なディザスタ リカバリの方法に関する概要を示します。

コンピュータ障害とは、 とは、人的ミス、ハードウェア障害、ウィルス、自然災害などにより、コンピュータ システムがブート不可能な状態になるイベントを指します。このような場合には、システムのブート パーティションまたはシステム パーティションが使用できなくなり、標準的な復元操作を行う前に環境の復旧が必要となります。 このためには、ブート パーティションの再作成や再フォーマット、環境を定義するすべての構成情報を含めたオペレーティング システムの再構築などを実行する必要があります。*最初にこの作業を完了しておかなければ、その他のユーザ データを復旧できません。*

オリジナル システムとは、システムでコンピュータ障害が発生する前に Data Protector によってバックアップされたシステム構成を指します。

ターゲット システムとは、コンピュータ障害発生後のシステムを指します。 ターゲット システムは通常、ブート不可能な状態になっているため、Data Protector のディザスタ リカバリは、このシステムをオリジナル システムの構成に復元することを目的としています。 クラッシュしたシステムとは異なり、ターゲット システムの場合は、障害が発生したハードウェアはすべて交換されています。

ブート ディスク/パーティション/ボリュームとは、ブート プロセスの初期段階に必要なファイルを含むディスク/パーティション/ボリュームを指します。一方、 **システム ディスク/パーティション/ボリューム**とは、オペレーティング システム ファイルを含むディスク/パーティション/ボリュームを指します。

注記：

Microsoft 社の定義は上記とは逆で、ブート パーティションはオペレーティング システム ファイルを含むパーティション、システム パーティションはブート プロセスの初期段階で必要なファイルを含むパーティションを示します。

ホスティング システムとは、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、Disk Agent がインストールされた動作中の Data Protector クライアントです。

補助ディスクとは、ネットワーク機能を備えた最低限の OS と、Data Protector Disk Agent がインストールされたブート可能ディスクです。 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。

ディザスタ リカバリ オペレーティング システム(DR OS)とは、ディザスタ リカバリ プロセスが実行されているオペレーティング システム環境です。 Data Protector に基本的ランタイム環境（ディスク、ネットワーク、テープ、ファイルシステムへのアクセス）を提供します。 Data Protectorディザスタ リカバリを実行する前に、インストールおよび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、別のオペレーティング システムをターゲット オペレーティング システム構成データとともに復元するホスト環境としてだけ使用され、 ターゲットシステム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 リカバリ処理に使用されるだけでなく、自身の構成データをオリジナル システムの構成データと置き換えて、復元されたシステムの一部となります。

重要なボリュームとは、システム ファイルおよびData Protectorファイルのブートに必要なボリュームです。 オペレーティング システムの種類に関係なく、以下のボリュームがクリティカル ボリュームとなります。

- ブート ボリューム
- システム ボリューム
- Data Protector実行可能ファイル
- IDB（Cell Managerのみ）

注記：

IDB が上記のいずれとも違うボリュームにある場合は、IDB のあるボリュームもクリティカル ボリュームとなります。

Windowsシステムでは、上記の重要なボリューム以外にも、CONFIGURATIONデータが格納されているボリュームも重要なボリュームとなります。 サービスは、CONFIGURATIONバックアップの一部としてバックアップされます。

CONFIGURATION に含まれる一部の項目は、システム、ブート、Data Protector、IDB ボリュームとは異なるボリュームにある場合があります。 この場合、以下のボリュームもクリティカル ボリュームの一部となります。

- ユーザー プロファイル ボリューム
- Windows Server 上の Certificate Server データベース ボリューム
- Windows Server のドメイン コントローラ上のアクティブ ディレクトリ サービス ボリューム
- Microsoft Cluster Server の定数ボリューム

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

オフライン復旧は、Cell Manager がアクセスできない場合に行います（ネットワークや Cell Manager の障害、オンライン復旧が失敗した場合など）。 オフライン復旧では、

スタンドアロン デバイスおよび SCSI ライブラリ デバイスのみが使用可能です。 Cell Manager の復旧は常にオフラインで行うことに注意してください。

リモート復旧 は、SRD ファイルで指定された Media Agent システムがすべて使用可能な場合に行います。 1 台でも使用できない場合は、ディザスタ リカバリ プロセスは**ローカル**モードに切り替わります。 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。 デバイスが 2 台以上見つかった場合、Data Protector は使用するデバイスを画面に表示してユーザーに選択させます。 オフライン OBDR は常にローカルで行うことに注意してください。

障害は常に重大な問題ですが、以下の要因により状況はさらに悪化するおそれがあります。

- システムをできる限り迅速かつ効率的にオンライン状態に戻す必要がある。
- ディザスタ リカバリを実行するために必要な手順に管理者が十分精通していない。
- ディザスタ リカバリを実行すべき担当者が、基本的なシステム知識しか持っていない。

ディザスタ リカバリは複雑な作業であり、事前に広範囲にわたる計画と準備を行っておく必要があります。 したがって、障害に備えたり、障害から回復するためには、十分に整備された段階的な復旧プロセスを完備しておくことが必要です。

ディザスタ リカバリ プロセス

ディザスタ リカバリ プロセスは4つのフェーズに分けられます。

- **フェーズ 0** は、ディザスタ リカバリを成功させるために必要な準備作業です。 障害が*発生する前に*プランニングと準備を実施しておく必要があります。
- まず **フェーズ 1** で、DR OS のインストールと構成を行います。通常はブートパーティションの再作成と再フォーマットも行います。これは、システムのブートもしくはシステム パーティションは常に使用可能とは限らず、通常の復元操作を行う前に環境の復旧が必要な場合があるためです。
- さらに、Data Protector を含むオペレーティング システム環境を定義するすべての構成情報を以前と同じように復旧します (**フェーズ 2**)。
- このステップが完了した場合にのみ、アプリケーションとユーザー データの復元が可能となります (**フェーズ 3**)。

迅速で効率的な復元のためには、明確なプロセスを確実に実行することが必要です。

ディザスタ リカバリの方法

この項では、基本的なディザスタ リカバリの方法に関する全般的な概要を示します。個々のオペレーティング システムでサポートされるディザスタ リカバリの手法のリストについては、『HP Data Protector product announcements ソフトウェアノートおよびリファレンス』のサポート一覧か以下のWebサイトを参照してください。

http://www.hp.com/support/manuals

注記：

いずれかの方法を選択する前に、それぞれの方法の制限事項についても、あらかじめ確認してください。

表 3 (24ページ) は、Data Protector のディザスタ リカバリの方法に関する概要を示しています。

表 3 ディザスタ リカバリの方法に関する概要

フェーズ0	フェーズ1	フェーズ2	フェーズ3
手動によるディザスタ リカバリ			
フル クライアント バックアップ、IDB バックアップ (Cell Manager のみ)。 SRD ファイルを更新します (Windows の場合のみ)。 DR OS をインストールならびに構成できるようにするため、オリジナル システムに関する情報を収集します。	ネットワーク サポート付きの DR OS をインストールします。 ディスク パーティションを再作成し、オリジナルの記憶データ構造を再確立します。	drstart コマンドを実行して、クリティカル ボリュームを自動復旧します。 高度な復旧作業を実行するには、追加の手順が必要になります。	Data Protector 標準復元手順を使用して、ユーザー データとアプリケーション データを復元します。
「Windows システムの半自動ディザスタ リカバリ」 (39ページ) または「UNIX Cell Manager の手動によるディザスタ リカバリ 」 (112ページ) を参照してください。			
ディスク デリバリーによるディザスタ リカバリ (DDDR)			

フェーズ0	フェーズ1	フェーズ2	フェーズ3
フル クライアント バックアップ、IDB バックアップ (Cell Manager のみ)。補助ディスクを作成します (UNIX のみ)。	*Windows の場合*: 交換ディスクをホスティング システムに接続します。 *UNIX の場合*: 補助ディスクをホスティング システムに接続します。 すべてのシステム: 交換ディスク上にパーティションを再作成し、オリジナルの記憶データ構造を再確立します。	*Windows の場合*: DDDR ウィザードを使ってクリティカル ボリュームを復元した後、交換ディスクをホスティング システムから取り外してターゲット システムに接続します。 *UNIX の場合*: オリジナル システムのブート ディスクを交換ディスク上に復元し、補助ブート ディスクを取り外します。 すべてのシステム: システムをリブートします。 高度な復旧作業を実行するには、追加の手順が必要になります。	Data Protector 標準復元手順を使用して、ユーザー データとアプリケーション データを復元します。
「Windows クライアントのディスク デリバリーによる障害復旧」 (46ページ) または「UNIX Cell Manager の手動によるディザスタ リカバリ」 (112ページ) を参照してください。			
拡張自動ディザスタ リカバリ (EADR)			
フル クライアント バックアップ、IDB バックアップ (Cell Manager のみ)。 SRD を準備して更新します。 DR CD を準備します。	DR CD からシステムをブートし、復旧範囲を選択します。	クリティカル ボリュームの自動復元。 高度な復旧作業を実行するには、追加の手順が必要になります。	Data Protector 標準復元手順を使用して、ユーザー データとアプリケーション データを復元します。
「Windows システムの拡張自動ディザスタ リカバリ」 (50ページ) を参照。			
ワンボタン ディザスタ リカバリ (OBDR)			

フェーズ0	フェーズ1	フェーズ2	フェーズ3
ODBR ウィザードによるフル クライアント バックアップ。SRD を準備して更新します。	OBDR テープからターゲット システムをブートし、復旧範囲を選択します。	クリティカル ボリュームの自動復元。	Data Protector 標準復元手順を使用して、ユーザー データとアプリケーション データを復元します。
「Windows システムのワンボタン ディザスタ リカバリ」 (63ページ) を参照。			
自動システム復旧 (ASR)			
フル クライアント バックアップ。更新済みの SRD ファイルと DP バイナリが書き込まれた ASR フロッピー ディスクを準備します。	Windows インストール メディアからシステムをブートし、ASR モードに切り替えます。ASR フロッピー ディスクを使用します。	クリティカル ボリュームが復元されます。 高度な復旧作業を実行するには、追加の手順が必要になります。	Data Protector 標準復元手順を使用して、ユーザー データとアプリケーション データを復元します。
「自動システム復旧」 (75ページ) を参照。			

次のフェーズに進む前に、以下の作業を完了する必要があります。

- *フェーズ 0*:
  フル クライアント バックアップおよび IDB バックアップ (Cell Manager のみ) を実行するとともに、DR OS のインストールと構成に必要な情報を管理者がオリジナル システムから収集する必要があります。 UNIX 上のディスク デリバリーによるディザスタ リカバリに使用する補助ブート ディスクを作成する必要があります。
- *フェーズ 1*:
  DR OS をインストールおよび構成するとともに、オリジナルの記憶データ構造を再確立する必要があります (すべてのボリュームを復元できるようにします)。 UNIX 上のディスク デリバリーによるディザスタ リカバリに使用する交換ディスクをブート可能にする必要があります。
- *フェーズ 2*:
  クリティカル ボリュームが復元されます。高度な復旧作業を実行するには、追加の手順が必要になります。 詳細は、「高度な復旧作業」 (84ページ) を参照してください。
- *フェーズ 3*:
  アプリケーション データが正しく復元されたかどうかをチェックします (データベースの整合性など)。

手動によるディザスタ リカバリの方法

手動によるディザスタ リカバリは、基本的かつ柔軟性に優れたディザスタ リカバリの方法です。ターゲット システムをオリジナル システムの構成に復旧します。

最初に、DR OS をインストールして構成する必要があります。 次に、Data Protector を使ってデータを復元し(オペレーティング システム ファイルを含む)、現在のオペレーティング システム ファイルを、復元したオペレーティング システム ファイルで置き換えます。

手動復旧では、フラットファイルに維持されない記憶域構造に関する情報(パーティション情報、ディスクミラー化、ストライプ化など)を収集しておくことが重要なポイントになります。

ディスク デリバリーによるディザスタ リカバリ

この方法は、Windows クライアントおよび UNIX クライアント上でサポートされています。

Windowsクライアントの場合は、クラッシュしたシステム上のディスク(またはディスクが物理的に損傷している場合は交換用のディスク)を、ホスティング システムに一時的に接続します。 復元後、新しいディスクを障害が発生したシステムに接続し、ブートします。

UNIXシステムの場合は、最小限のオペレーティング システム、ネットワーク機能、およびData Protectorエージェントがインストールされた補助ディスクを使用して、ディスク デリバリーによるディザスタ リカバリを実行します。

この方法を使うと、クライアントを短時間で簡単に復旧できます。 Windows システムでは、オペレーティング システムの状態も自動的に復元されます。

ヒント：

この方法では、電源を切らずにシステムを稼動させたまま、システムからハードディスクドライブを取り外して新しいディスクドライブを接続することができます。ホットスワップ式のハードディスクドライブを使用している場合は、この方法が特に役立ちます。

「Windows クライアントのディスク デリバリーによる障害復旧 」 (46ページ)を参照。

ワンボタン ディザスタ リカバリ (OBDR)

ワンボタン ディザスタ リカバリ (OBDR) とは、Windows クライアントと Cell Manager 用に自動化された Data Protector 復旧方法で、ユーザーが介在する手間は最小限に抑えられています。

OBDR では、環境に関連するすべてのデータがバックアップ時に自動収集されます。バックアップの際に、一時 DR OS のセットアップと構成に必要なデータが、1 つの大きな OBDR イメージ ファイルにパックされ、バックアップ テープに保存されます。障害が発生した場合には、OBDR デバイス (CD-ROM をエミュレートできるバックアップ デバイス) を使用して、OBDR イメージ ファイルとディザスタ リカバリ情報を含むテープからターゲット システムを直接ブートします。

Data Protector は次に、ディザスタ リカバリ オペレーティング システム (DR OS) のインストールと構成、ディスクのフォーマットとパーティション作成を自動的に行い、最後に元のオペレーティング システムをバックアップ時と同じ状態に復元します。

重要：

ハードウェア、ソフトウェア、構成などに変更があった場合には、その都度、新しい OBDR ブート テープを準備する必要があります。 これは、IP アドレスや DNS サーバーの変更など、ネットワーク構成が変更された場合も同じです。

自動システム復旧

自動システム復旧(ASR)はWindowsシステム上の自動システムで、障害発生時にディスクをオリジナルの状態に再構成(または、新しいディスクがオリジナルのものより大きい場合、パーティションをサイズ変更)します。 この処理には、ディスクのパーティション化と論理ボリュームの構成(ファイル形式、ドライブ文字の割り当て、ボリュームマウントポイント、およびボリューム特性)が含まれます。 このように ASR は Data Protector の drstart.exe コマンドにより、Data Protector ディスク、ネットワーク、テープ、ファイルシステムへのアクセスを提供するアクティブな DR OS をインストールすることができます。

Data Protector は次に、ターゲット システムを元のシステム構成に復旧し、最後にユーザー データを復元します。

拡張自動ディザスタ リカバリ (EADR)

拡張自動ディザスタ リカバリ (EADR) では、Windows クライアント用とCell Manager用の自動化されたData Protector 復旧手法により、ユーザーの操作が最小限に抑えられます。

Windows プラットフォーム用の EADR 手順では、環境に関連するすべてのデータがバックアップ時に自動収集されます。 CONFIGURATION バックアップの際に、一時 DR OS のセットアップと構成に必要なデータが、セル内のバックアップ対象の各クライアントごとに 1 つの大きな **DR OS イメージ ファイル**にパックされ、バックアップ テープに (オプションで Cell Manager にも) 保存されます。

イメージ ファイルに加え、ディスクの適切なフォーマットとパーティション作成に必要なフェーズ 1 開始情報 (**P1S** ファイルに保存) が Cell Manager に保存されます。 障害が発生した場合、EADR ウィザードで、DR OS イメージをバックアップ メディア (フルバックアップ時に Cell Manager に保存されていない場合) から復元し、それを **ディザ**

スタ リカバリ CD ISO イメージに変換します。 CD ISO イメージは、CD 書き込みツールで CD に保存して、ターゲット システムのブートに使用します。

次に Data Protector は、DR OS のインストールと構成、ディスクのフォーマットとパーティション作成を自動的に行い、最後にオリジナル システムをバックアップ時と同じ状態に復旧します。

重要：

ハードウェア、ソフトウェア、構成などに変更があった場合には、その都度バックアップを実行して新しい DR CD を作成します。 これは、IP アドレスや DNS サーバーの変更など、ネットワーク構成が変更された場合も同じです。

復旧対象となるパーティションを以下に示します。

- ブート パーティション
- システム パーティション
- Data Protector を含むパーティション

その他のパーティションは、通常の Data Protector 復旧手順を使って復旧できます。

Data Protector 統合ソフトウェアとディザスタ リカバリ

ディザスタ リカバリは、複数のメーカーの製品に関係する非常に複雑なプロセスです。 したがって、ディザスタ リカバリを成功させるには、すべてのベンダーの製品に対して適切な処置をとる必要があります。 ここに記載されている情報は、あくまで目安として使用してください。

ディザスタ リカバリにどのように備えるべきかについては、データベースやアプリケーションのベンダーの指示をチェックしてください。

ここでは、アプリケーションを復旧する際の全般的な手順を示します。

1. ディザスタ リカバリを実行します。
2. Data Protector メディア上のデータをシステムに再ロードできるように、データベースやアプリケーションをインストール、構成、および初期設定します。 データベースを準備するために必要な手順の詳細は、データベースやアプリケーションのベンダーから提供されているマニュアルを参照してください。
3. 必要な Data Protector クライアント ソフトウェアがデータベースやアプリケーションのサーバーにインストールされており、正しく構成されていることを確認します。 HP Data Protector インテグレーションガイド の該当する部分の手順に従ってください。
4. 復元を開始します。 復元が完了したら、データベースやアプリケーションのベンダーの指示に従い、データベースをオンラインにするための手順を、必要に応じて実施します。

2 ディザスタ リカバリのプランニングと準備

この章の内容

迅速かつ効率的に復元が実行できるよう、この章で説明する手順に従って、ディザスタ リカバリに対する準備作業を行ってください。 準備作業はどのディザスタ リカバリの方法でも大きな違いはありませんが、詳細なディザスタ リカバリ プランの作成、整合性と関連性を兼ね備えたバックアップの実行、SRD ファイルの更新（Windows の場合）は、必ず行うようにしてください。

この章では、すべてのディザスタ リカバリの方法に共通する一般的な準備手順を説明します。 それぞれのディザスタ リカバリの方法について、個別に追加手順が必要です。 追加手順については対応する項を参照してください。

計画

綿密なディザスタ リカバリ プランの作成は、ディザスタ リカバリの手順が円滑に実行されるかどうかに大きく影響します。 さまざまなシステムが混在する大規模な環境でディザスタ リカバリを行うには、以下の手順で行います。

1. **プラン**

   計画は、IT管理者が作成する必要があります。計画には、以下のことを含めてください。

   - 復旧が必要なシステム、復旧の時間および度合いの決定。 重要なシステムは、ネットワークが正しく機能するために必要なすべてのシステム（DNS サーバー、ドメイン コントローラ、ゲートウェイなど）、Cell Manager および Media Agent クライアントです。
   - 復旧方法の決定（必要な準備に影響します）。
   - 復旧に必要な情報の取得方法の決定。この情報には、IDB が含まれているメディア、更新された SRD ファイルの位置、Cell Manager バックアップ メディアの位置とラベルなどがあります。
   - 復旧プロセスの指針となる、段階を追った詳細なチェックリストの作成。
   - 復旧が実際にうまくいくことを確認するテストプランの作成と実行 。

2. **復旧の準備**

   使用する復旧方法により、準備には以下のような作業が含まれます。

   UNIX の場合:

   - 補助ディスクなどのツールの作成。補助ディスクには、最低限のオペレーティング システム、ネットワーク機能、Data Protector Disk Agent をインストールします。
   - データ記憶構造などクライアント固有の準備データ収集を行う、実行前スクリプトの作成。

   Windows の場合:

   - **システム復旧データ (SRD)** の更新と安全な場所への保存。 セキュリティ上の理由から、SRD ファイルへのアクセスは制限する必要があります。

   すべてのシステム:

   - 定期的で整合性のとれたバックアップの実行。

3. **復旧手順の実行**

   テスト済みの手順とチェックリストに従い、クラッシュしたシステムを復旧します。

整合性と関連性を兼ね備えたバックアップ

障害が発生した場合、ターゲット システムを最新の有効なバックアップ時点の状態に戻さなければなりません。 また、システムが最新の有効なバックアップ直前と同様に機能するようにする必要もあります。

注記：

UNIX システムでは、さまざまな理由から、デーモンやプロセスの一部はシステムのブート直後に開始します (HP-UX の実行レベル 2 におけるライセンス サーバーなど)。 このような初期プロセスは、実行時にデータをメモリに読み込み、「ダーティ フラグ」をファイルに書き込むこともあります。 また、標準的な動作段階 (標準実行レベル 4) で行われたバックアップでは、適切なアプリケーションが正常に起動しません。 この例で言えば、ライセンス サーバーがこのような疑似復旧後に起動された場合、ライセンス サーバーはデータが不整合であると認識し、サービスを予定どおりに実行できません。

Windows では、システムの実行中は多くのシステム ファイルがシステムによりロックされているため、これらを置き換えることはできません。 たとえば、現在使用中のユーザープロファイルは復元できません。 ログイン アカウントを変更するか、関連するサービスを停止する必要があります。

バックアップ実行時にシステム上でどのプロセスが起動しているかによって異なりますが、アプリケーションに対するデータの整合性は維持されない可能性があります。したがって、復旧後、再起動や実行に関する問題が発生します。

整合性と関連性を兼ね備えたバックアップの作成

- 最も適切な方法として、関連するパーティションをオフラインに設定してバックアップする方法がありますが、通常はこの方法は実行できません。
- バックアップ時のシステム上の動作状況を調べます。 バックアップ実行中に稼動できるのは、オペレーティング システム関連のプロセスと、オンラインでバックアップされるデータベース サービスのみです。
- UNIX の低水準アプリケーションや Windows のバックグラウンドレベル アプリケーションに固有のサービスは実行できません。

整合性と関連性を兼ね備えたバックアップに何を含めるべきかは、使用する予定のディザスタ リカバリの方法や他のシステム仕様（Microsoft Cluster のディザスタ リカバリなど）に依存します。 特定のディザスタ リカバリの方法に関連する項を参照してください。

暗号化されたバックアップ

バックアップが暗号化されている場合、暗号化キーが安全に保存されており、ディザスタ リカバリを開始するときに使用可能であることを確認する必要があります。 適切な暗号化キーにアクセスできないと、ディザスタ リカバリの手順が中断してしまいます。

Data Protector A.06.10 では、Data Protector A.06.00 から暗号化モデルが変更されています。 暗号化キーは Cell Manager に保存されます。したがってディザスタ リカバリ クライアントを Cell Manager に接続して暗号化キーを取得するか、リムーバブル メディアの暗号化キーを使用する必要があります。 暗号化の詳細については、オンライン ヘルプの索引キーワード「暗号化」で表示される内容を参照してください。

2 つのディザスタ リカバリのシナリオが考えられます。

- Cell Manager への接続を確立可能なクライアントの復旧。 Data Protector では自動的に暗号化キーが取得されるため、このようなシナリオには、追加の暗号化に関連する準備は必要ありません。
- Cell Managerまたは、Cell Managerへの接続を確立できないスタンドアロン クライアントのディザスタ リカバリ。 プロンプトが表示されたら、暗号化キーを入力する必要があります。
  暗号化キーは、ディザスタ リカバリ ISO イメージの一部ではなく、キー ファイルにエクスポートされます。 このキーは、別のリムーバブル メディアに手動で保存する必要があります。 ディザスタ リカバリの準備のための各バックアップについて、暗号化キーが正しくコピーされていることを常に確認するようにしてください。 暗号化キーが使用できないと、ディザスタ リカバリは実行できなくなります。

システム復旧データ (SRD) の更新と編集

システム復旧データ (SRD) とは、Windows ターゲット システムの構成と復元に必要な情報が収められた、UNICODE 形式のテキスト ファイルです。 SRD ファイル

は、Windows クライアント上で CONFIGURATION バックアップを実行したときに生成され、以下の場所に保存されます。

- Windows Cell Manager の場合：*Data_Protector_home*\Config\server\dr\srd
- UNIX Cell Manager の場合：/etc/opt/omni/server/dr/srd/

重要：

IDB が使用できない場合、オブジェクトとメディアの情報は SRD ファイルだけに保存されます。

Cell Manager 上の SRD ファイルの名前は、このファイルが作成されたコンピュータのホスト名と同じです（computer.company.com など）。

CONFIGURATION バックアップの後、SRD には、DR OS のインストールに必要なシステム情報だけが保存されます。 ディザスタ リカバリを実行するには、バックアップ オブジェクトとそのオブジェクトが格納されたメディアに関する情報を SRD に追加する必要があります。 SRD は Windows クライアントでしか更新できません。 更新された SRD ファイルの名前は、recovery.srd です。

SRD ファイルの更新には、以下の 3 種類の方法を使用できます。

- [SRD ファイルの更新] ウィザード
- omnisrdupdate コマンド（スタンドアロン ユーティリティとして使用）
- omnisrdupdate コマンド（バックアップ セッションの実行後スクリプトとして使用）

[SRD ファイルの更新] ウィザードによる更新

[SRD ファイルの更新] ウィザードを使って SRD ファイルを更新するには、以下の手順を行います。

1. [Data Protector Manager] で［復元］コンテキストを選択し、**[タスク]** ナビゲーション タブをクリックします。
2. [タスク] ナビゲーション タブの Scoping ペインで、**[ディザスタ リカバリ]** を選択します。
3. 結果エリアで **[SRD ファイルの更新]** オプション ボタンを選択し、クライアントを選択した後、**[次へ]** をクリックします。
4. 各クリティカル オブジェクトごとにオブジェクトのバージョンを選択して、**[次へ]** をクリックします。
5. 更新した SRD ファイルの保存先ディレクトリを入力して、**[完了]** をクリックします。

重要：

SRD ファイルは Cell Manager システムに保存されるため、Cell Manager に障害が発生した場合は、このファイルにアクセスできなくなります。 したがって、Cell Manager の SRD ファイルのコピーを別途作成しておくことが必要です。 ディザスタ リカバリに備えた準備の一環として、更新された SRD ファイルは、Cell Manager だけでなく、セキュリティが確保されている複数の保管先に置いてください。「準備」 (48 ページ) を参照。

omnisrdupdate による更新

SRD ファイルは、omnisrdupdate コマンドをスタンドアロン コマンドとして使用して更新することもできます。 omnisrdupdate コマンドは *Data_Protector_home*\bin ディレクトリにあります。

あるセッションに所属するバックアップ オブジェクト情報が保存されている既存の SRD ファイルを更新するには、omnisrdupdate で session_ID を指定する必要があります。 omnisrdupdate は、渡された session_ID の値に対応するバックアップ オブジェクトの情報が格納されている SRD ファイルを更新します。 更新された SRD ファイルは、Cell Manager上に保存されます。

この手順は、(SRD ファイルで指定されている) すべての重要なバックアップ オブジェクトが、指定されたセッション内で実際にバックアップされた場合に限り、正常に実行されます。 どのオブジェクトが SRD 更新対象のクリティカル オブジェクトとされているかを調べるには、テキスト エディタを使って SRD ファイルを開き、オブジェクトに関する部分 (section objects) を参照します。 この部分に、SRD 更新対象のクリティカル オブジェクトがすべてリストされています。 データベースは “/” で示されています。

SRD ファイルのオブジェクトに関する部分は以下のようになります。

```
-section objects
-objcount 3
-object /C -objtype 6 -objpurpose 283
-endobject /C
-object / -objtype 3 -objpurpose 32
-endobject /
-object /CONFIGURATION -objtype 6 -objpurpose 4
-endobject /CONFIGURATION
-endsection objects
```

この場合、/C、/ (データベース)、/CONFIGURATION の 3 つの重要なオブジェクトがあります。

ヒント：

セッション ID を取得するには、omnidb コマンドを -session オプションを付けて実行します。 最新のセッション ID を取得する場合は、コマンド プロンプトから「omnidb -session -latest」と入力してください。

更新済みの SRD ファイルは、障害に備えて安全な場所に保存しておくことが必要です。 更新済み SRD ファイルの保存場所を指定するには、omnisrdupdate コマンドに -location オプションを付けて実行します。 -location パラメータは複数指定できます（書き込み権限を持っているネットワーク共有を含む）。 パラメータで指定した各保存場所に、更新済み SRD ファイルのコピーが保存されます。「準備」（48ページ）を参照。

Cell Manager 上の SRD ファイルをどのホスト名で更新するかを指定するには、omnisrdupdate コマンドで -host オプションを使用します。 ホスト名を指定しなかった場合は、ローカル ホストとみなされます。 Cell Manager 上の SRD ファイルは更新されません。

例

ホスト名が computer.company.com というクライアントの 2002/05/02-5 セッションに属するバックアップ オブジェクト情報で SRD ファイルを更新して、更新済みの SRD ファイルのコピーをフロッピー ディスクとホスト名が computer2 というコンピュータの SRDfiles 共有ディスクに保存するには、次のコマンドを実行してください。

```
omnisrdupdate -session 2002/05/02-5 -host computer.company.com -location
a: -location

\\computer2\SRDfiles
```

共有ディスクに対して書き込み権限があることを確認してください。

実行後スクリプトによる更新

SRD を更新するもう 1 つの方法は、バックアップの実行後スクリプトとして omnisrdupdate コマンドを使用します。 この方法を使用するには、既存のバックアップ仕様を変更するか、新しいバックアップ仕様を作成することが必要です。 以下の手順に従ってバックアップ仕様を変更することにより、バックアップ セッション終了時に、バックアップされたオブジェクトに関する情報を使って SRD ファイルが更新されます。

1. [バックアップ] コンテキストで [バックアップ仕様] → [ファイルシステム] の順に展開します。
2. 変更したいバックアップ仕様を選択します（選択するバックアップ仕様には、SRD ファイルでクリティカルとマークされているバックアップ オブジェクトがすべて含まれていることが必要です。 そうでない場合は、更新は正常に実行されません。このため、ディスク ディスカバリを使ったクライアント バックアップを実行することをお勧めします）。 選択後、結果エリアで **[オプション]** をクリックします。

3. ［バックアップ仕様オプション］の下の **［拡張］** ボタンをクリックします。
4. ［実行後］テキスト ボックスに「omnisrdupdate.exe」と入力します。
5. この実行後スクリプトを実行するクライアントを［実行対象］ドロップダウン リストで選択し、**[OK]** を選択して確認します。 選択するクライアントは、［ソース］ページでバックアップ対象としてマークされているクライアントでなければなりません。

omnisrdupdate コマンドを実行後ユーティリティとして実行すると、セッション ID が環境から自動的に取得されるので、ユーザーがセッション ID を指定する必要はありません。

その他すべてのオプションは、スタンドアロン ユーティリティ (-location *path*, -host *name*) の場合と同様に指定できます。

SRD ファイルの編集

ディザスタ リカバリを実行する時点で、SRD ファイルに保存されているバックアップ デバイスまたはメディアに関する情報が古くなっている場合もあります。 その場合は、ディザスタ リカバリを実行する前に SRD ファイルを編集して、関連する情報を正しい情報に置き換えてください。「編集後の SRD ファイルを使用した復旧」（94ページ）を参照。

重要：

セキュリティ上の理由から、SRD ファイルへのアクセスは制限する必要があります。

3 Windows 上でのディザスタ リカバリ

Windows システムの半自動ディザスタ リカバリ

この項では、Windows システム上での半自動ディザスタ リカバリの準備と実行方法について説明します。 サポート対象のオペレーティング システムは、『HP Data Protector product announcements ソフトウェアノートおよびリファレンス』を参照してください。

概要

Windows クライアントのディザスタ リカバリを半自動的に実行する手順の概要は、以下のとおりです。

1. **フェーズ 0**
   a. フル クライアント バックアップおよび IDB バックアップ（Cell Manager のみ）を実行します。
   b. SRD ファイルを更新します。 DR OS をインストールならびに構成できるようにするため、オリジナル システムに関する情報を収集します。
2. **フェーズ 1**
   a. 障害が発生したハードウェアを交換します。
   b. オペレーティングシステムを再インストールします。（必要なパーティションを作成およびフォーマットします）。
   c. サービス パックを再インストールします。
   d. 手動でディスク上にパーティションを再作成し、オリジナルのドライブ文字を割り当てて、オリジナルの記憶データ構造を再確立します。

ヒント：

手動ディザスタ リカバリのフェーズ 1 は、自動展開ツールと組み合わせて使用できます。

3. **フェーズ 2**
   a. Data Protector drstart.exe コマンドを実行します。このコマンドは、DR OS をインストールし、システムのクリティカル ボリュームの復元を開始します。

b. drstart コマンドの実行が終了したら、構成を再ブートする必要があります。
c. Cell Manager の復旧作業か高度な復旧作業を行う場合は、特別な手順が必要となります。 詳細については、「高度な復旧作業」（84ページ）を参照してください。

4. **フェーズ3**
   a. ユーザー データおよびアプリケーション データを復元する場合は、Data Protector 標準復元手順を使用します。

要件

- パーティションのサイズは、障害が発生したディスクのパーティション サイズと同じかそれより大きくなければなりません。 これにより、障害が発生したディスクに保存されていた情報を新しいディスクに復元できます。 また、ファイルシステムの形式（FAT、NTFS）と、ボリュームの圧縮属性も一致していることが必要です。
- ターゲット システムのハードウェア構成は、障害発生前の状態と同じでなければなりません。 これには、SCSI の BIOS 設定（セクタの再マッピング）も含まれます。
- ボリューム マウント ポイントは自動では復元されません。このため、障害が発生する前にボリューム マウント ポイントが作成されていた場合は、それらのマウント ポイントを最初に再作成してから、ディザスタ リカバリの手順を開始する必要があります。 マウント ポイントを再作成しないと、データの復元先が不正確になる可能性があります。

制限事項

- Internet Information Server (IIS) データベース、ターミナル サービス データベース、Certificate Server データベースは、フェーズ 2 で自動的には復元されません。これらをターゲット システムに復元するには、Data Protector 標準復元手順を実行してください。

準備

ディザスタ リカバリが正しく実行されるよう準備するには、一般的な準備に関する手順と、特定のディザスタ リカバリの方法を使用するための要件に関連する手順を実行することが必要です。 迅速かつ効率的にディザスタ リカバリを実行するには、事前の準備が必要です。 Cell Manager と Microsoft Cluster Server のディザスタ リカバリの準備にも十分な注意が必要です。

△ **注意：**

障害が発生してからディザスタ リカバリの準備をしても遅すぎます。

この項で挙げられている手順を完了する前に、すべてのディザスタ リカバリの方法に共通する一般的な準備手順として「計画」 (31ページ) も参照してください。 障害から迅速かつ効率的に復旧するため、以下の項目を考慮した上で適切な環境を準備してください。

1. システムを CD-ROM から起動するには、ブート可能な Windows インストール用 CD-ROM が必要です。 ブート可能な CD-ROM がない場合は、ディスクからコンピュータを起動する標準的手順を実行してください。
2. 復旧対象のシステムに適したドライバがあることを確認します。 Windows のセットアップ中、ネットワーク、HBA、SCSI ドライバなど、いくつかのドライバをインストールする必要があります。
3. クラッシュしたシステムを復旧するには、障害発生前のシステムに関する以下の情報が必要です (SRD ファイルにも保存されています)。
   - 障害発生前に DHCP が使用されていなかった場合 – TCP/IP のプロパティ (IP アドレス、デフォルト ゲートウェイ、サブネット マスク、DNS の順序)
   - クライアントのプロパティ (ホスト名)
4. 以下の条件が当てはまることを確認します。
   - 正常に実行されたクライアントのフル バックアップがあること。 ~ を参照してください。
     詳細は、オンライン ヘルプの索引キーワード「バックアップ、Windows 固有」および「バックアップ、構成」で表示される内容を参照してください。
   - 正常に実行されたバックアップ セッションに含まれるバックアップ オブジェクトに関する情報を使って更新された SRD ファイルが必要です。 「システム復旧データ (SRD) の更新と編集」 (33ページ) を参照。
   - Cell Manager を復旧する場合は、正常に実行された Cell Manager の IDB バックアップが必要です。 IDB バックアップの設定方法および実行方法の詳細は、オンライン ヘルプの索引キーワード「IDB、設定」で表示される内容を参照してください。
   - Microsoft Cluster Server のための整合性のあるバックアップには、(同じバックアップ セッションに) 以下のものが含まれている必要があります。
     - すべてのノード
     - 管理仮想サーバー (管理者が定義)
     - Cell Manager 仮想サーバーと IDB (Data Protector がクラスター対応アプリケーションとして構成されている場合)

     詳細については、「Microsoft Cluster Server の復元に固有の手順」 (84ページ) を参照してください。
   - ブート パーティションのあるディスクには、Data Protector ディザスタ リカバリ ユーティリティのインストール (15MB) とアクティブ DR OS インストールに必要な空きディスク スペースが必要です。 また、元のシステムの復元に必要な空きディスク スペースも別途必要です。

5. 32 ビット版 Windows クライアントまたは Cell Manager の場合は、*Data_Protector_home*\Depot\DRSetup または Data Protector インストール用メディア内の \i386\tools\DRSetup の内容を、3 枚のフロッピーディスク (**drsetup ディスク**) にコピーし、64 ビット版 Windows システムの場合は、*Data_Protector_home*\Depot\DRSetup64 または Data Protector インストール用メディア内の \i386\tools\DRSetup64 の内容を 4 枚のフロッピー ディスクにコピーします。 障害が発生した場合、クラッシュしたクライアントの更新済み SRD ファイルを 1 枚目のフロッピー ディスク (ディスク 1) に保存します。どの Windows システムの場合でも、1 つのサイトにつき必要な drsetup ディスクは 1 セットだけです。 ただし、1 枚目のフロッピー ディスク上にある、クラッシュしたクライアントの更新された SRD ファイルは必ずコピーしておいてください。 SRD ファイルが複数ある場合は、適切なバージョンを選ぶように Data Protector が尋ねてきます。
6. ディスク パーティションを障害発生前の初期状態に再構成するため、各パーティションごとに以下の情報を記録しておきます (この情報は復旧プロセスで必要になります)。
   - パーティションの長さと順序
   - パーティションに割り当てられるドライブ文字
   - パーティションのファイルシステムの種類

   この情報は、SRD ファイルに保存されています。 SRD ファイルの diskinfo セクションで -type オプションを使用すると、特定のパーティションのファイルシステムの種類が分かります。

   表 4 SRD ファイルからファイルシステムの種類を知る方法

種類を示す番号	[ファイルシステム]
1	Fat12
4および6	Fat32
5および15	拡張パーティション
7	NTFS
11および12	Fat32
18	EISA
66	LDM パーティション

次ページの表に、ディザスタ リカバリの準備例を示します。 表のデータは特定のシステムのものであり、それ以外のシステムでは使用できないことに注意してください。 半自動ディザスタ リカバリの準備に使用できる空のテンプレートについては、「Windows での手動によるディザスタ リカバリ準備用テンプレート」 (131 ページ) を参照してください。

表 5 半自動ディザスタ リカバリ準備用テンプレートの例

クライアント プロパティ	コンピュータ名	ANDES
	ホスト名	andes.company.com
ドライバ		hpn.sys、hpncin.dll
Windows Service Pack		Windows SP3
TCP/IP のプロパティ	IPアドレス	3.55.61.61
	デフォルトゲートウェイ	10.17.250.250
	サブネット マスク	255.255.0.0
	DNS の順序	11.17.3.108, 11.17.100.100
メディア ラベル / バーコード番号		“andes – disaster recovery” / [000577]
パーティション情報と順序	最初のディスクラベル	
	第 1 パーティションの長さ	31 MB
	第 1 ドライブの文字	
	第 1 ファイルシステム	EISA
	2番目のディスクラベル	BOOT
	第 2 パーティションの長さ	1419 MB
	第 2 ドライブの文字	C:
	第 2 ファイルシステム	NTFS/HPFS
	3番目のディスクラベル	
	第 3 パーティションの長さ	
	第 3 ドライブの文字	
	第 3 ファイルシステム	

Recovery

以下の手順に従って、半自動ディザスタ リカバリを使って Windows システムを復旧します。 高度な復旧作業（Cell Manager または IIS の復旧など）を行おうとしている場合は、「高度な復旧作業」 (84ページ) も参照してください。

1. CD-ROM から Windows システムをインストールし、必要に応じてドライバをインストールします。 Windows オペレーティング システムは、障害前と同じパーティションにインストールする必要があります。 システムのインストール中に Internet Information Server (IIS) をインストールしないでください。 詳細は、「Internet Information Server (IIS) の復元に固有の手順」 (92ページ) を参照してください。

重要：

Windows の無人セットアップを使用して Windows がインストールされている場合、復旧時に Windows のインストールに使用したスクリプトと同じものを使用して、*$SystemRoot$* フォルダと \Documents and Settings フォルダが同じ場所にインストールされるようにします。

2. [Windowsパーティションセットアップ]画面が表示されたら、次の操作を行います。
   - クラッシュ前のシステム上にベンダー固有のパーティション (EISA Utility Partition など) があった場合は、SRD ファイルから収集した EISA 情報に基づいて、“ダミー” の FAT パーティションを作成し (クラッシュにより失われた場合)、フォーマットします。 EUP はあとから、“ダミー” パーティションによって保持されているスペースに復旧されます。 “ダミー” パーティションの作成後すぐに、ブート パーティションを作成およびフォーマットしてください。 この方法については、「準備」 (48ページ) を参照してください。
   - クラッシュ前のシステム上に EUP がなかった場合は、クラッシュ前の状態になるようブート パーティションを作成し (クラッシュにより失われた場合)、フォーマットします。 この方法については、「準備」 (48ページ) を参照してください。

   Windows を元の位置 (つまり、障害発生前の元のシステムとドライブ文字およびディレクトリが同じ位置) にインストールします。 この情報は、SRD ファイルに保存されています。

注記：

インストール時には、障害発生前に Windows ドメインが置かれていた場所にシステムを追加せずに、ワークグループに追加してください。

3. TCP/IP プロトコルをインストールします。 障害の発生前に DHCP を使用していなかった場合は、クラッシュしたクライアントのホスト名、その IP アドレス、デフォルト ゲートウェイ、サブネット マスク、DNS サーバーに関する情報を設定し、障害発生前と同様に TCP/IP プロトコルを構成します。 [このコンピュータのプライマリDNSサフィックス] フィールドに、適切なドメイン名が指定されていることを確認してください。

注記：

Windowsのデフォルト設定では、WindowsのセットアップDHCP(Dynamic Host Configuration Protocol)がインストールされます。

4. Windows の Administrators グループ内にディザスタ リカバリ用の一時的なアカウントを作成し、Cell Manager 上で Data Protector の Admin グループに追加します。 詳細は、オンライン ヘルプの索引キーワード「追加, Data Protector ユーザー」で表示される内容を参照してください。

   障害発生前にシステム上に存在していなかったアカウントを使用する必要があります。 この一時的な *Windows* アカウントは、この手順の後半で削除します。

5. ログオフした後、新規作成したアカウントを使用してシステムにログインします。
6. 障害発生後にバックアップ デバイスを変更したなどの理由で SRD ファイルの情報が最新のものでなく、オフライン復旧を実行しようとしている場合は、この手順を続行する前に SRD ファイルを変更してください。「編集後の SRD ファイルを使用した復旧」 (94ページ) を参照。
7. *Data_Protector_home*\Depot\drsetup\Disk1 (Windows Cell Manager) または \i386\tools\drsetup\Disk1 (Data Protector インストール用メディア) のいずれかのディレクトリから drstart.exe コマンドを実行します。 drsetup ディスクが用意されている場合は「準備」 (40ページ) を参照、drstart.exe コマンドを実行することもできます。
8. drstart.exe は、まず現在の作業ディレクトリ、フロッピー ディスク、CD ドライブをスキャンして、ディザスタ リカバリ用セットアップ ファイル (Dr1.cab と omnicab.ini) の位置を調べます。 必要なファイルが見つかった場合、drstart ユーティリティはディザスタ リカバリ用ファイルを *%SystemRoot%*\system32\OB2DR ディレクトリにインストールします。 drstart.exe がファイルを見つけられない場合は、[DR Installation Source] テキストボックスにパスを入力するか、ブラウズしてファイルを選択します。
9. recovery.srd ファイルが dr1.cab および omnicab.ini ファイルと同じディレクトリに保存されている場合は、drstart.exe により recovery.srd ファイルが *%SystemRoot%*\system32\OB2DR\bin ディレクトリにコピーされ、omnidr ユーティリティが自動的に起動されます。 そうでない場合は、SRD ファイル (recovery.srd) の場所を [SRD Path] フィールドに入力するかブラウズして選択し、 [次へ] をクリックします。

   フロッピー ディスクに SRD ファイルが複数ある場合は、適切なバージョンを選ぶように Data Protector が尋ねてきます。

   omnidr が正常終了した後、システムを正しくブートするのに必要なすべてのクリティカル オブジェクトが復元されます。
10. ステップステップ 4 (45ページ) で追加した一時ユーザー アカウント *Data Protector* を Cell Manager 上の Data Protector Admin グループから削除します (このアカウントがディザスタ リカバリ前にも Cell Manager 上に存在していなかった場合)。
11. コンピュータを再起動し、ログオンして、復元されたアプリケーションが実行されているか検証します。

12. Cell Manager の復旧、または高度な復旧作業（MSCS または IIS の復旧、kb.cfg および SRD ファイルの編集など）を行おうとしている場合は、特別な手順が必要となります。 詳細については、「Data Protector Cell Manager 固有の復元手順」（90ページ）と「高度な復旧作業」（84ページ）を参照してください。
13. Data Protector を使って、ユーザー データとアプリケーション データを復元します。

一時 DR OS は、以下の場合を除いて、最初のログイン後に削除されます。

- 障害復旧ウィザードが DR のインストールとバックアップ メディア上の SRD ファイルを発見した後の 10 秒間のポーズの間に、ユーザーがウィザードを中断して **[デバッグを使用] (Use Debugs)** オプションを選択した場合。
- omnidr コマンドを、 no_reset または debug オプションを付けて手動で起動した場合。
- ディザスタリカバリが失敗した場合。

Windows クライアントのディスク デリバリーによる障害復旧

ディスク デリバリーによるディザスタ リカバリを実行するには、現在稼働中の Data Protector クライアント（Data Protector ディザスタ リカバリ ホスト）を使って、新しいディスクをこのクライアントに接続した状態で作成します。 管理者は、ディスクのフォーマットおよびパーティションの構成が正しく行われるよう、障害発生前に十分なデータを収集する必要があります。 ただし、Data Protector により CONFIGURATION バックアップの対象として関連情報が自動的に保存されます。

復旧対象となるパーティションを以下に示します。

- ブート パーティション
- システム パーティション
- Data Protector を含むパーティション

その他のパーティションは、通常の Data Protector 復旧手順を使って復旧できます。

サポート対象のオペレーティング システムは、『HP Data Protector product announcements ソフトウェアノートおよびリファレンス』を参照してください。

ヒント：

この方法は、ホットスワップ ハードディスク ドライブとともに使用すると非常に便利です。システムの電源を切らずに稼動させたまま、ハードディスク ドライブをシステムから外して、新しいハードディスク ドライブを接続できるためです。

概要

Windows クライアントのディザスタ リカバリにディスク デリバリーを使用する手順の概要は、以下のとおりです。

1. **フェーズ 0**
   a. フル クライアント バックアップおよび IDB バックアップ（Cell Manager のみ）を実行します。
   b. 各パーティションに関して必要な情報を収集します。
2. **フェーズ 1**
   a. ホスティング システムに交換ディスクを接続します。
   b. 交換ディスク上に手動でパーティションを作成して、記憶データ構造を再確立します。 Windows マウント ポイントの詳細については、オンライン ヘルプを参照してください。
3. **フェーズ 2**
   a. Data Protector ディスク デリバリー ウィザードを使用して、オリジナル システムのクリティカル ディスクを交換ディスクに復元します。
   b. ホスティング システムをシャットダウンした後、交換ディスクを取り外してターゲット システムに接続します。 なお、ホットスワップが可能なハードディスク ドライブを使用している場合は、システムをシャットダウンする必要はありません。
   c. 交換したディスクからターゲット システムを再ブートします。
4. **フェーズ3**
   a. ユーザー データおよびアプリケーション データを復元する場合は、Data Protector 標準復元手順を使用します。

要件

- パーティションのサイズは、障害が発生したディスクのパーティション サイズと同じかそれより大きくなければなりません。 これにより、障害が発生したディスクに保存されていた情報を新しいディスクに復元できます。 また、ファイルシステムの形式（FAT、NTFS）が一致していることが必要です。
- ディスクが作成されたシステムおよびディスクが使用されているシステムでは、同じセクタのマッピング/アドレッシングを使用する必要があります（有効化/無効化されたSCSI BIOS、EIDE：両システムでは同じアドレッシング モードを使用する必要があります：LBA、ECHS、CHS）。

制限事項

- ディスク デリバリーによるディザスタ リカバリは、Microsoft Cluster Server ではサポートされていません。
- RAID はサポートされていません。 これには、ソフトウェア RAID（フォールト トレラント ボリュームおよびダイナミック ディスク）も含まれます。

- Internet Information Server (IIS) データベース、ターミナル サービス データベース、Certificate Server データベースは、フェーズ 2 で自動的には復元されません。これらをターゲット システムに復元するには、Data Protector 標準復元手順を実行してください。

準備

ディザスタ リカバリの準備としていくつかの手順を実行します。 この項で挙げられている手順を完了する前に、すべてのディザスタ リカバリの方法に共通する一般的な準備手順として「計画」 (31ページ)も参照してください。

重要：

ディザスタ リカバリの準備は、障害が発生する*前に*行っておく必要があります。

障害から迅速かつ効率的に復旧するには、以下が必要です。

- 最新かつ有効な、復旧対象のクライアントのフル バックアップ
- クラッシュしたディスクと交換するための新しいハードディスク。
- Data Protector ホスト システムは、クラッシュしたクライアントとオペレーティング システムが同じで、新しいディスクの接続に必要なハードウェア I/O パスも一致していることが必要です。

ディスクパーティションをクラッシュ前の初期状態で再作成できるように、パーティションごとに以下の情報を記録しておきます。これらの情報は復旧時に必要になります。

- パーティションの長さと順序
- パーティションに割り当てられるドライブ文字
- パーティションのファイルシステムの種類

表 5 (43ページ) に、ディスク デリバリーによるディザスタ リカバリの準備の例を示します。 ディザスタ リカバリの準備に使用できる空のテンプレートについては、「Windows での手動によるディザスタ リカバリ準備用テンプレート」 (131ページ) を参照してください。

Recovery

この項では、ディスク デリバリーによるディザスタ リカバリを使って Windows クライアントを復旧する手順を説明します。「高度な復旧作業」 (84ページ)も参照してください。

Windows 上でのディスク デリバリーによるディザスタ リカバリでは、Data Protector ディザスタ リカバリ ホスト (DR ホスト) を使って、クラッシュしたディスクの最新の有効なフル バックアップを、クライアントに接続されている新しいハードディスクに復元します。 次に、障害が発生したシステムのクラッシュしたディスクを新しいハードディスクと交換します。

実際のディスク デリバリーによるディザスタ リカバリは以下の手順で構成されています。

1. DR ホストに新しいディスクを接続します。
2. DR ホストを再起動して、新しいディスクを認識させます。
3. ディザスタ リカバリ ホストの Data Protector GUI を使って、[復元] コンテキストに切り替え、[タスク] タブをクリックします。 Scoping ペインで**[ディザスタ リカバリ]** を選択して、ドロップダウン リストからクライアントを選択し、結果エリアで **[ディスクのデリバリーによるディザスタ リカバリ]** を選択します。
4. 各クリティカル オブジェクトごとに、復元対象のオブジェクト バージョンを選択して、**[次へ]** をクリックします。
5. パーティションをまだ作成していない場合は、ディスク アドミニストレータを使って新しいディスクのパーティションを作成します。 このとき、ディスク デリバリーによるディザスタ リカバリの準備作業の一環として収集したパーティション情報を使用します。
6. パーティションを作成する際には、フル バックアップが実行される前と同じ順序でパーティションを割り当てる必要があります。 これにより、復元後のドライブ文字の再割り当てが円滑に行われるので、boot.ini ファイルに設定されているシステム パーティションへのパスが不適切になることによって起こるシステム再起動時の障害を防止できます。

重要：

Windows のマウント ポイントにドライブ文字を割り当てます。 この場合、各マウント ポイントごとにドライブ文字を割り当てることができるよう、十分な未使用のドライブ文字が必要となります。

7. 元のドライブ文字を右クリックして、必要なドライブ文字の割り当てをすべて行います。 ホスト システムと元のシステムのドライブ文字が異なる可能性があるために、この作業が必要となります。
8. **[完了]** を選択します。
9. 新しいディスクを DR ホストから取り外して、ターゲット システムに接続します。
10. ターゲット システムの電源を入れます。
11. ユーザー データおよびアプリケーション データを復元する場合は、Data Protector 標準復元手順を使用します。 これでクライアントの復旧は完了です。

ディスク デリバリーは、マルチ ブート システムのディスクのうち 1 つがクラッシュした場合にも有効なディザスタ リカバリの方法です。この場合、ユーザーは少なくとも 1 つの構成をブートできるためです。

注記：

Data Protector はボリューム圧縮フラグを復元しません。 バックアップ時に圧縮されていたファイルはすべて圧縮されて復元されますが、新規ファイルを圧縮ファイルとして作成したい場合は、手動でボリューム圧縮フラグをセットする必要があります。

Windows システムの拡張自動ディザスタ リカバリ

Data Protector には、Windows Cell Manager 用やクライアント用に拡張されたディザスタ リカバリの手順が用意されています。 サポート対象のオペレーティング システムは、『HP Data Protector product announcements ソフトウェアノートおよびリファレンス』を参照してください。

EADR では、環境に関連するすべてのデータがバックアップ時に自動収集されます。 フル バックアップの際に、一時 DR OS のセットアップと構成に必要なデータが、セル内のバックアップ対象の各クライアントごとに 1 つの大きな **DR OS イメージ ファイル**にパックされ、バックアップ テープに（オプションで Cell Manager にも）保存されます。

イメージ ファイルに加え、ディスクの適切なフォーマットとパーティション作成に必要な**フェーズ 1 開始ファイル**（P1Sファイル）がバックアップ メディア上および Cell Manager 上に保存されます。 障害が発生した場合、拡張自動障害復旧ウィザードで、DR OS イメージをバックアップ メディア（フル バックアップ時に Cell Manager に保存されていない場合）から復元し、それを **ディザスタ リカバリ CD ISO イメージ**に変換します。 CD ISO イメージは、CD 書き込みツールで CD に保存して、ターゲット システムのブートに使用します。

次に Data Protector は、DR OS のインストールと構成、ディスクのフォーマットとパーティション作成を自動的に行い、最後にオリジナル システムをバックアップ時と同じ状態に復旧します。

重要：

バックアップ メディア、DR イメージ、SRD ファイル、ディザスタ リカバリ CD へのアクセスを制限しておくことをお勧めします。

概要

Windows クライアントに対して拡張自動ディザスタ リカバリを行う手順の概要は、以下のとおりです。

1. **フェーズ 0**
   a. フル クライアント バックアップを実行します。
   b. 拡張自動障害復旧ウィザードを使用して、クラッシュしたシステムの DR OS イメージ ファイルから DR CD ISO イメージを作成し、CD に書き込

みます。 DR OS イメージがフル バックアップ中に Cell Manager に保存されなかった場合、拡張自動障害復旧ウィザードでは、バックアップ メディアからイメージが復元されます。

重要：

ハードウェア、ソフトウェア、構成などに変更があった場合には、その都度バックアップを実行して新しい DR CD を作成する必要があります。 これは、IP アドレスや DNS サーバーの変更など、ネットワーク構成が変更された場合も同じです。

c. フル クライアント バックアップが暗号化されている場合は、暗号化キーをリムーバブル メディアに保存して、ディザスタ リカバリの際に使用できるようにします。 Cell Manager の復旧時、または Cell Manager への接続を確立できない場合には、このキーが必要になります。

2. **フェーズ 1**
   a. 障害が発生したハードウェアを交換します。
   b. ディザスタ リカバリ CD からターゲット システムをブートし、復旧範囲を選択します。 完全に無人状態での復旧が可能です。
3. **フェーズ 2**
   a. クリティカル ボリューム（ブート パーティション、オペレーティング システム、および Data Protector が格納されているパーティション）は自動的に復元されます。
4. **フェーズ3**
   a. ユーザー データおよびアプリケーション データを復元する場合は、Data Protector 標準復元手順を使用します。

重要：

最初に復元する必要のあるクリティカルなシステム（特に DNS サーバー、Cell Manager、Media Agent クライアント、ファイル サーバーなど）のそれぞれについて、ディザスタ リカバリ CD を準備します。

Cell Manager の復旧の場合は、暗号化キーを保存したリムーバブル メディアを事前に準備します。

以降の項では、Windows クライアントの拡張自動ディザスタ リカバリに関する制限事項、準備、および、復旧方法を説明します。「高度な復旧作業」 (84ページ) も参照してください。

要件

ディザスタ リカバリの方法を選択する前に、以下の必要条件と制限事項をよくお読みください。

- Data Protector 自動ディザスタ リカバリ コンポーネントが、この方法で復旧したいクライアントと、DR CD ISO イメージを作成するシステムにインストールされている必要があります。『HP Data Protector インストールおよびライセンスガイド』を参照してください。
- ターゲット システムのハードウェア構成は、障害発生前の状態と同じでなければなりません。 これには、SCSI の BIOS 設定（セクタの再マッピング）も含まれます。
- 同じバスの同じホストバスアダプタに交換用ディスクが接続されていること。
- DR OS をインストールするブート パーティションは少なくとも 200MB 以上のサイズにする必要があります。これを下回ると、ディザスタ リカバリが失敗します。 オリジナル パーティションで［ドライブを圧縮してディスク領域を空ける］オプションを有効に設定していた場合は、少なくとも 400MB の領域が必要になります。
- EADR バックアップの準備中は、Data Protector がインストールされているパーティションに少なくとも 200MB の一時的な空きスペースが必要です。 このスペースは、一時イメージの作成に使用されます。
- ブートに必要なドライバは、すべて *%SystemRoot%* フォルダにインストールされている必要があります。 インストールされていない場合は、kb.cfg ファイルで指定されている必要があります。「kb.cfg ファイルの編集」 (93ページ) を参照。
- ネットワーク機能が付いたセーフ モード、またはディレクトリ サービス復元モード（ドメイン コントローラのみ）でシステムをブートする場合は、ネットワークが使用可能でなければなりません。ただし、システムのバックアップは通常のブート プロセスの後に実行する必要があります。
- システムの BIOS は、El-Torito 標準で定義されているブート可能 CD をサポートしている必要があります。また、INT13h 機能の XXh により、LBA アドレッシングを使用しているハードディスク ドライブへの読み書きが可能である必要があります。 BIOS のオプションは、システムのユーザー マニュアル、またはブート前にシステム設定を調査することでチェックできます。
- オフライン復元を計画している場合は、クライアント バックアップ時のデバイスへの書き込みにはデフォルトのブロック サイズ 64KB を使用してください。 ディザスタ リカバリを実行する際に Windows で使用できるブロック サイズはこのデフォルトのサイズだけです。 デフォルトのブロック サイズ 64KB が設定されているかどうかを確かめるには、［プロパティ］ボックスの **［拡張...］** を選択します。図 2 (53ページ) を参照してください。

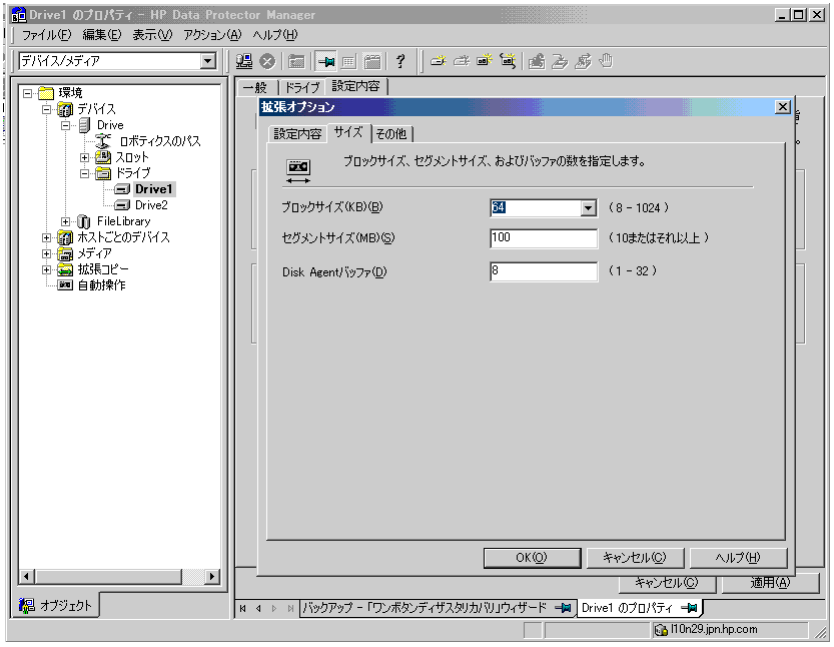


図 2 デフォルトのブロック サイズの確認

- ディザスタ リカバリに必要なすべてのデータをバックアップすると、大量の空き容量が必要になる場合があります。 通常は 500 MB で十分ですが、オペレーティング システムによっては 1 GB が必要になることもあります。.
- クラスタ環境では、各クラスタ ノードのバス アドレス一覧が同じであれば、クラスタ ノードは正常にバックアップできます。 これには、以下のものが必要です。
  - 同等のクラスタ ノードのマザーボード ハードウェア
  - 両方のノードで同じ OS のバージョン（サービス パックおよびアップデート）
  - バス コントローラの数とタイプが同一
  - バス コントローラが同じ PCI マザー ボードのスロットに挿入されている。
- Windows XP の場合は、オペレーティング システムがバックアップの時点で起動されておらず、起動期間が終了すると、ディザスタ リカバリは失敗します。
- AES 暗号化バックアップから ISO CD イメージを作成する際には、kms_allow_hosts ファイルが存在し(Cell Manager でイメージが準備された場合を除く) 、イメージが準備されたクライアントの完全修飾ドメイン名が含められている必要があります「kms_allow_hosts ファイルがない場合の、AES 暗号化バックアップのための ISO イメージの作成の失敗」 (126ページ) を参照。
- Windows Vista 用の ISO CD イメージを作成するには、イメージを作成するシステムに Windows Automated Installation Kit (WAIK) 1.1 がインストールされている必要があります。 WAIK の古いバージョンはサポートされていません。

制限事項

- ダイナミック ディスクはサポートされていません（Windows NT からのミラー セットのアップグレードも含む）。
- 新しいディスクのサイズは、クラッシュしたディスクのサイズ以上である必要があります。 元のディスクのサイズよりも大きい場合、余った分に対しては割り当てが行われません。
- 拡張自動ディザスタ リカバリでサポートされているベンダー固有のパーティションは、0x12 タイプ（EISA を含む）と 0xFE タイプのみです。
- Microsoftのブートローダーを使用しないマルチブートシステムはサポートされていません。
- Internet Information Server（IIS）、ターミナル サービス データベース、Certificate Server データベースは、フェーズ 2 で自動的には復元されません。これらをターゲット システムに復元するには、 Data Protector 標準復元手順を実行してください。
- ディザスタ リカバリの ISO イメージは、Data Protector が FAT/FAT32 パーティションにインストールされているシステムには作成できません。 ディザスタ リカバリのイメージを作成するには、Data Protector が NTFS ボリュームにインストールされているクライアントがセル内に少なくとも1つ必要です。

準備

この項で挙げられている手順を完了する前に、すべてのディザスタ リカバリの方法に共通する一般的な準備手順として「計画」 (31ページ) も参照してください。「高度な復旧作業」 (84ページ) も参照してください。

重要：

ディザスタ リカバリの準備は、障害が発生する*前に*行っておく必要があります。

前提

- フル クライアント バックアップを実行します（CONFIGURATION も含む）。詳細は、オンライン ヘルプの索引キーワード「バックアップ、Windows 固有」および「バックアップ、構成」で表示される内容を参照してください。
- ***Microsoft Cluster Server の場合：*** Microsoft Cluster Server のための整合性のあるバックアップには、（同じバックアップ セッションに）以下のものが含まれている必要があります。
  - すべてのノード
  - 管理仮想サーバー（管理者が定義）
  - Cell Manager 仮想サーバーと IDB（Data Protector がクラスター対応アプリケーションとして構成されている場合）

詳細については、「Microsoft Cluster Server の復元に固有の手順」 (84ページ) を参照してください。

バックアップ実行後に、MSCS 内の全ノードの P1S ファイルをマージします。 これにより、各ノードの P1S ファイルには共有クラスター ボリューム構成の情報が格納されます。 詳しくは、「EADR 用に全ノードの P1S ファイルをマージ」 (87ページ) を参照してください。

DR イメージ ファイル

一時 DR OS のインストールと構成に必要なデータ (DR イメージ) は、フル クライアント バックアップ時に 1 つの大きなファイルにパックされ、バックアップ メディア、さらにオプションで Cell Manager にも保存されます。 Cell Manager にも、バックアップ仕様にあるクライアントすべてのディザスタ リカバリ イメージを保存したい場合は、以下の手順を実行してください。

1. コンテキスト リストで **[バックアップ]** を選択します。
2. Scoping ペインで［バックアップ仕様］→［ファイルシステム］の順に展開します。
3. フル クライアント バックアップに使用するバックアップ仕様を選択します (まだ作成していない場合は作成します)。
4. 結果エリアで **[オプション]** をクリックします。
5. ［ファイルシステム オプション］で **[拡張]** をクリックします。
6. **[WinFSオプション]**をクリックし、**[ディザスタリカバリイメージ全体をディスクにコピー]**を選択します。

   Windows Vista システムの場合は、**[Detect NTFS hardlinks]** および **[Use Shadow Copy]** も選択してください。

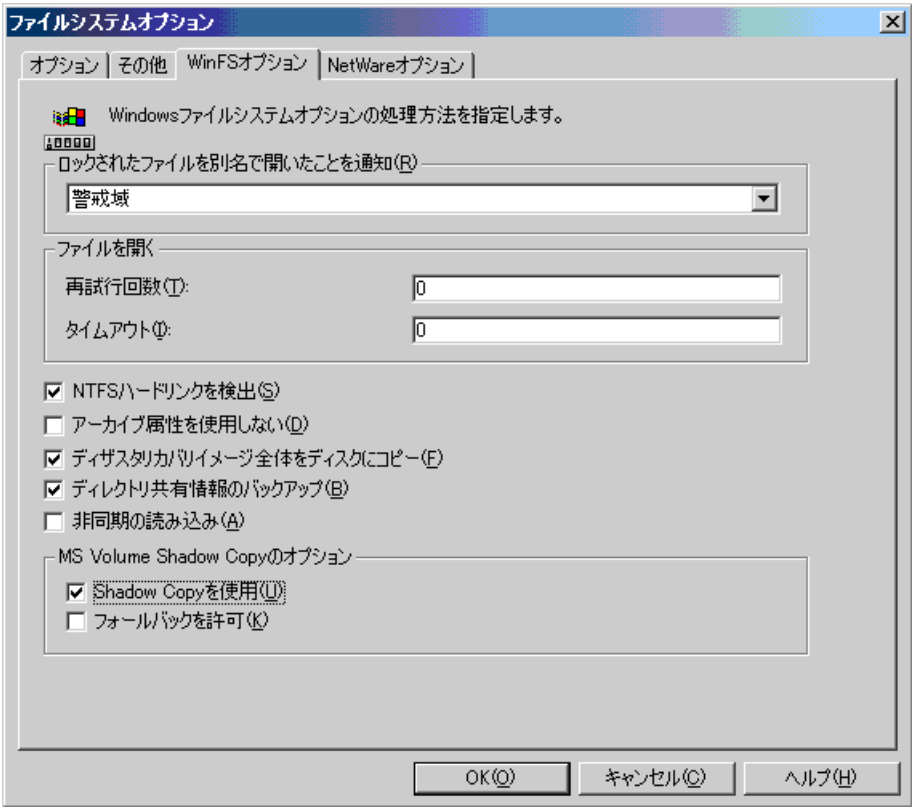


図 3 [WinFS オプション] タブ

バックアップ仕様内の特定クライアントの DR イメージ ファイルだけをコピーする場合は、以下の手順を実行します。

1. コンテキスト リストで **[バックアップ]** を選択します。
2. Scoping ペインで［バックアップ仕様］→［ファイルシステム］の順に展開します。
3. フル クライアント バックアップに使用するバックアップ仕様を選択します。 まだ作成していない場合は作成します。 詳細は、オンライン ヘルプの索引キーワード「バックアップ仕様の作成」で表示される内容を参照してください。
4. 結果エリアで **[バックアップ オブジェクトのサマリー]** をクリックします。
5. Cell Manager に DR イメージ ファイルを保存したいクライアントを選択して、**[プロパティ]** をクリックします。
6. **[WinFS オプション]** をクリックし、**[ディザスタ リカバリ イメージ全体をディスクにコピー]** を選択します。

ディザスタ リカバリ CD を Cell Manager 上で作成する場合、ディザスタ リカバリ イメージ全体を Cell Manager に保存するのが便利です。 そうすれば

DR イメージはハードディスクから読み込まれ、バックアップ メディアから読み込む場合よりもはるかに速く作業が進みます。 DR イメージはデフォルトでは、*Data_Protector_home*\Config\server\dr\p1s (Windows Cell Manager の場合)、または /etc/opt/omni/server/dr/p1s (UNIX Cell Manager の場合) に *client name*.img という名前で保存されます。 デフォルトのディレクトリを変更するには、グローバル オプション ファイルで新たなグローバル変数 EADRImagePath = *valid_path* (EADRImagePath = /home/images または EADRImagePath = c:\temp など) を指定します。 オンラインヘルプの索引キーワード「グローバル オプション ファイル、変更」で表示される内容を参照してください。

ヒント：

宛先ディレクトリに十分な空きディスク スペースがない場合には、他のボリュームへのリンクを作成するか (UNIX の場合)、マウント ポイントを作成します (Windows の場合)。

kb.cfg ファイル

このファイルの目的は、特定のブート関連ハードウェアまたはアプリケーション構成を持つシステム用に、ドライバ (および他の必要ファイル) を DR OS に含めるための柔軟な方法を提供することです。 デフォルトの kb.cfg ファイルには、あらかじめ業界標準のハードウェア構成に必要なすべてのファイルが含まれています。

デフォルトの kb.cfg ファイルを使用したテスト プランを作成し実行します。 DR OS が正常にブートしない、またはネットワークにアクセスできない場合は、ファイルを変更する必要があります。 詳細については、「kb.cfg ファイルの編集」 (93 ページ) を参照してください。

暗号化キーの準備

Cell Manager の復旧またはオフライン クライアントの復旧に対しては、暗号化キーをリムーバブル メディアに保存して、ディザスタ リカバリの際に使用できるようにする必要があります。 Cell Manager の復旧に対しては、事前に (障害が発生する前に) リムーバブル メディアを準備してください。

暗号化キーは、DR OS イメージ ファイルの一部ではありません。 このキーは、ディザスタ リカバリ イメージの作成時に、*Data_Protector_home*\Config\Server\export\keys\DR-*ClientName*-keys.csv に自動的にエクスポートされます。ここで、*ClientName* はイメージを作成するクライアントの名前です。

ディザスタ リカバリの準備のための各バックアップについて、正しい暗号化キーがあることを確認してください。

フェーズ 1 開始ファイル (P1S)

フル バックアップ中は、DR イメージ ファイル以外に、フェーズ 1 開始ファイル (P1S) が作成されます。 このファイルは、バックアップ メディア、および Cell Manager の *Data_Protector_home*\Config\server\dr\p1s ディレクトリ (Windows Cell Manager)、または /etc/opt/omni/server/dr/p1sディレクトリ (UNIX Cell Manager) に保存されます。 ファイル名はホスト名と同じです (たとえば computer.company.com など)。 これは Unicode UTF-8 でエンコードされたファイルで、システムにインストールされているすべてのディスクのフォーマット/パーティション作成方法に関する情報が含まれています。 これに対して更新済みの SRD ファイルには、システム情報、およびバックアップ オブジェクトと対応するメディアに関するデータのみが含まれています。

障害が発生した場合、障害復旧インストールの際に EADR ウィザードを使用して、DR イメージ、SRD ファイル、P1S ファイルを **ディザスタ リカバリ CD ISO イメージ** としてマージできます。 このイメージは ISO9660 フォーマットをサポートしている CD 書き込みツールで CD に保存できます。 この **ディザスタ リカバリ CD**は、自動ディザスタ リカバリを実行する際に使用します。

重要：

Cell Manager 用のディザスタ リカバリ CD を事前に用意しておく必要があります。

Microsoft Cluster のノード用のディザスタ リカバリ CD を作成する場合には、特別な手順が必要になります。「Microsoft Cluster Server の復元に固有の手順」 (84 ページ) を参照。

重要：

セキュリティ上の理由から、バックアップ メディア、DR イメージ、SRD ファイル、ディザスタ リカバリ CD へのアクセスを制限しておくことをお勧めします。

DR CD ISO イメージの作成

DR CD ISO イメージを作成するには、以下の手順を行います。

1. コンテキスト リストで **[復元]** を選択します。
2. **[タスク]** ナビゲーション タブをクリックし、[ディザスタ リカバリ] を選択します。
3. ドロップダウン リストから、ISO イメージを準備するクライアントを選択します。
4. **[拡張自動ディザスタ リカバリ]**、**[次へ]** の順にクリックします。
5. 各クリティカル オブジェクトごとに、適切なオブジェクト バージョンを選択して、**[次へ]** をクリックします。

6. Cell Manager に DR イメージ ファイルが保存されている場合は保存ディレクトリを指定するか、ブラウズします。それ以外の場合は、**[Restore image file from a backup]** をクリックします。**[次へ]** をクリックします。
7. ISO CD イメージ (recovery.iso) の保存先ディレクトリを選択して **[完了]** をクリックすると、ISO CD イメージが作成されます。

△ **注意：**

新しい ISO CD イメージを、すでに ISO イメージ (recovery.iso) があるディレクトリへ保存すると、既存の ISO CD イメージは新しいイメージで上書きされます。このとき警告メッセージは表示されません。

Windows Vista システム：WAIKオプションの指定：

- Windows 自動インストールキット (WAIK) ディレクトリを指定します。場所を入力すると、Data Protector で保存され、ISO CD イメージが次回作成されるときに、GUI でデフォルト選択として使用されます。
- ISO CD イメージに挿入するドライバも指定できます。 このオプションを使用して、見つからないドライバを DR OS に追加することができます。Windows Vista クライアント リカバリ セットの一部であるドライバを挿入するには、**[Inject]** をクリックします。 リカバリ セットの *%Drivers%* の部分からドライバが自動的に [Insert drivers] ダイアログ ウィンドウに挿入されます。 .inf という拡張子を持つドライバが一覧されます。

注記：

バックアップ手順で収集されてリカバリ セットの *%Drivers%* ディレクトリに保存されたドライバは、DR OS 内での使用に適しているとは限りません。 場合によっては、Windows PE 固有のドライバを挿入して、復旧中のハードウェアの適切な動作を確保する必要があります。

8. ディザスタ リカバリ ISO CD イメージを、ISO9660 フォーマットをサポートしている CD 書き込みツールを使用して CD に保存します。

重要：

ハードウェア、ソフトウェア、構成などに変更があった場合には、その都度バックアップを実行して新しい DR CD を作成します。 これは、IP アドレスや DNS サーバーの変更など、ネットワーク構成が変更された場合も同じです。

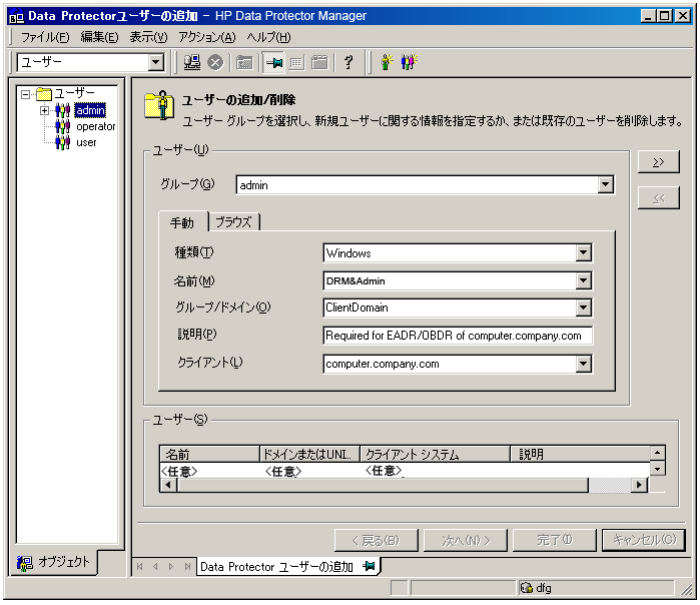
Recovery

クラッシュしたシステム上でシステムのディザスタ リカバリを正しく実行するには、以下が必要です。

- クラッシュしたディスクと交換するための新しいハードディスク。
- 復旧対象のクライアントの正常なフル バックアップ
- Data Protector ディザスタ リカバリ CD

Windows クライアントの拡張自動ディザスタ リカバリを実行する手順を以下に示します。

1. オフライン障害復旧を行う場合以外は、Cell Manager 上の Data Protector の Admin ユーザー グループに SYSTEM/NT Authority (Windows Vista の場合)またはDRM$Admin (その他の Windows システムの場合) というアカウントを追加します。 詳細は、オンライン ヘルプの索引キーワード「追加, Data Protector ユーザー」で表示される内容を参照してください。



2. 元のシステムのディザスタ リカバリ CD からクライアント システムをブートします。 復旧手順を開始する前に、システムに外付けの USB ディスク (USB キーを含む) が接続されていないことを確認してください。
3. 以下のメッセージが表示されたら、**F12** を押します。 To start recovery of the machine *HOSTNAME* press F12.
4. Windows Vista では、先に DR OS がメモリにロードされてから、範囲メニューが表示されます。 その他のWindowsシステムの場合は、ブートプロセスの最初に範囲選択メニューが表示されます。

   復旧範囲を選択して、**Enter** キーを押します。 復旧範囲は 5 種類あります。

   - **[再起動]**: ディザスタ リカバリは実行されず、コンピュータが再起動されます。

- **[デフォルト復旧]**：クリティカル ボリュームが復旧されます。 他のすべてのディスクはパーティション作成やフォーマットが行われず、フェーズ 3 に備えた状態になります。
- **[最小復旧]**：システム ディスクとブート ディスクのみが復旧されます (EADR と OBDR のみで使用可能)。
- **[Full Recovery]**：重要なものだけでなく、すべてのボリュームが復旧されます。
- **[共有ボリュームを含む完全復旧]**：Microsoft Cluster Server (MSCS) の場合にのみ選択できるオプションです。 このオプションは、MSCS 内のすべてのノードがクラッシュして、最初のノードに対する EADR を実行する場合に使用します。 復元セット内のすべてのボリューム (バックアップ時にバックアップ対象のノードによりロックされていたクラスター共有ボリュームを含む) が復元されます。
  1 つでも稼動中のノードがあって MSCS が実行されている場合、共有ボリュームは復元されません。これは、稼動中のノードにより共有ボリュームがロックされるためです。 この場合は [デフォルト復旧] を選択してください。

プラットフォームやオペレーティング システムによってはその他にもオプションがあり、主にディザスタ リカバリが完全に終了せず、追加の手順が必要な場合に使用します。

- **[Restore BCD]**：Windows Vista でのみ使用可能です。 デフォルトでは、Data Protector はディザスタ リカバリの際に Boot Configuration Data (BCD) ストアを復元します。 BCD ストアが復元されないと、マシンがブートできなくなる場合があります。
- **[Restore DAT]**：Windows Vista でのみ使用可能です。 Data Protector による復元前または復元後に、DR OS の一部として DAT ファイルに保存されているライターのデータを復元できます。
- **[Remove Boot Descriptor]**：Intel Itanium システムでのみ使用可能です。ディザスタ リカバリのプロセスによって残された起動記述子をすべて削除します。「Intel Itanium 固有の問題」 (128ページ) を参照してください。
- **[Manual disk selection]**：Intel Itanium システムでのみ使用可能です。ディスクの設定が大幅に変更された場合は、ディザスタ リカバリ モジュールがブート ディスクを見つけることができません。 このオプションを使用して正しいブート ディスクを選択します。「Intel Itanium 固有の問題」 (128ページ) を参照してください。

Windows Vista のみ：BitLocker ドライブ暗号化を使用してボリュームが暗号化されている場合、メニューが表示されて、暗号化されたドライバのロックを解除できます。「Windows VistaのBitLocker ドライブ暗号化」 (98ページ) を参照してください。

5. 復旧範囲を選択すると、Data Protector は、ハードディスクに対して直接 DR OS のセットアップを設定します。 この処理の進行状況はモニター可能です。 DR OS のセットアップが完了するとシステムは再起動します。 Windows Vista システムの場合は、この手順は省略され、再起動は行われません。

   "To start recovery of the machine *HOSTNAME* press F12（マシン HOSTNAME の復旧を開始するには、F12 キーを押してください。）" というプロンプトの表示で 10 秒間待つと、システムは CD ではなくハードディスクから起動します。

   ディザスタ リカバリ ウィザードが表示されます。 ディザスタ リカバリ オプションを変更するには、カウントダウン中に任意のキーを押してウィザードを停止した後、オプションを変更します。 **[完了]** をクリックして、ディザスタ リカバリを続行します。

6. ディザスタ リカバリのバックアップが Data Protector によって暗号化されているときに、Cell Manager を復旧または Cell Manager がアクセスできないクライアントを復旧しようとすると、次のプロンプトが表示されます。

   Do you want to use AES key file for decryption [y/n]?

   [y] キーを押してください。

   キー ストア (DR-*ClientName*-keys.csv) が (キーが保存されたメディアを挿入することにより) クライアントからアクセスできることを確認し、キー ストア ファイルのフル パスを入力します。 キー ストア ファイルが DR OS のデフォルトの場所にコピーされ、Disk Agent によって使用されます。 以降は何の操作も必要なく、ディザスタ リカバリが続行されます。

7. 障害発生後にバックアップ デバイスを変更したなどの理由で SRD ファイルの情報が最新のものでなく、オフライン復旧を実行しようとしている場合は、この手順を続行する前に SRD ファイルを変更してください。 詳細については、「編集後の SRD ファイルを使用した復旧」 (94ページ) を参照してください。

8. Data Protector は次に、選択された復旧範囲内で障害発生前の記憶データ構造を再構築し、すべてのクリティカル ボリュームを復元します。 一時 DR OS は、以下の場合を除いて、最初のログイン後に削除されます。

   - **[最小復旧]** が選択された場合。
   - 障害復旧ウィザードが DR のインストールとバックアップ メディア上の SRD ファイルを発見した後の 10 秒間のポーズの間に、ユーザーがウィザードを中断して **[デバッグを使用] (Use Debugs)** オプションを選択した場合。
   - omnidr コマンドを、 no_reset または debug オプションを付けて手動で起動した場合。
   - ディザスタリカバリが失敗した場合。

   Windows Vista システムの場合は、一時 DR OS が残されることはありません。

9. ステップステップ 1 (60ページ) で追加したクライアントのローカル管理者アカウントが、ディザスタ リカバリ前に Cell Manager 上に存在していなかった場合は、Cell Manager 上の Data Protector Admin ユーザー グループから削除します。

10. Cell Manager の復旧、または高度な復旧作業（MSCS または IIS の復旧、kb.cfg および SRD ファイルの編集など）を行おうとしている場合は、特別な手順が必要となります。 詳細については、「Data Protector Cell Manager 固有の復元手順」（90ページ）と「高度な復旧作業」（84ページ）を参照してください。
11. Data Protector 標準復元手順を使用して、ユーザー データとアプリケーション データを復元します。

注記：

Data Protector はボリューム圧縮フラグを復元しません。 バックアップ時に圧縮されていたファイルはすべて圧縮されて復元されますが、新規ファイルを圧縮ファイルとして作成したい場合は、手動でボリューム圧縮フラグをセットする必要があります。

Windows システムのワンボタン ディザスタ リカバリ

ワンボタン ディザスタ リカバリ（OBDR）とは、Windows クライアントと Cell Manager 用の自動化された Data Protector の復旧方法で、ユーザーが介在する手間は最小限に抑えられています。 サポート対象のオペレーティング システムは、『HP Data Protector product announcements ソフトウェアノートおよびリファレンス』を参照してください。

OBDR では、環境に関連するすべてのデータがバックアップ時に自動収集されます。バックアップの際に、一時 DR OS のセットアップと構成に必要なデータが、1 つの大きな OBDR イメージ ファイルにパックされ、バックアップ テープに保存されます。障害が発生した場合には、OBDR デバイス（CD-ROM をエミュレートできるバックアップ デバイス）を使用して、OBDR イメージ ファイルとディザスタ リカバリ情報を含むテープからターゲット システムを直接ブートします。

Data Protector は次に、ディザスタ リカバリ オペレーティング システム（DR OS）のインストールと構成、ディスクのフォーマットとパーティション作成を自動的に行い、最後に元のオペレーティング システムをバックアップ時と同じ状態に復元します。

重要：

ハードウェア、ソフトウェア、構成などに変更があった場合には、その都度バックアップを実行します。 これは、IP アドレスや DNS サーバーの変更など、ネットワーク構成が変更された場合も同じです。

復旧対象となるパーティションを以下に示します。

- ブート パーティション
- システム パーティション
- Data Protector を含むパーティション

その他のパーティションは、通常の Data Protector 復旧手順を使って復旧できます。

概要

Windows クライアントに対してワンボタン ディザスタ リカバリを行う手順の概要は、以下のとおりです。

1. **フェーズ 0**
   a. OBDR バックアップが必要です (Data Protector ワンボタン障害復旧ウィザードを使用してバックアップ仕様を作成します)。
   b. 暗号化されたバックアップを使用している場合は、暗号化キーをリムーバブル メディアに保存して、ディザスタ リカバリの際に使用できるようにします。Cell Manager の復旧時、または Cell Manager への接続を確立できない場合には、このキーが必要になります。
2. **フェーズ 1**

   復旧用テープからブートし、復旧範囲を選択します。
3. **フェーズ 2**

   クリティカル ボリューム（ブート パーティション、オペレーティング システム、および Data Protector が格納されているパーティション）はデフォルトで復元されます。
4. **フェーズ3**

   Data Protector 標準復元手順を使用して、残りのパーティションを復元します。

重要：

OBDR ブート テープへのアクセスを制限することをお勧めします。

以下の項で、Windows システム上でのワンボタン ディザスタ リカバリに関する必要条件、制限事項、準備、および、復旧について説明します。「高度な復旧作業」 (84ページ) も参照してください。

要件

- Data Protector 自動ディザスタ リカバリ コンポーネントとユーザー インターフェース コンポーネントが、この方法で復旧するシステムにインストールされている必要があります。 （『HP Data Protector インストールおよびライセンスガイド』 を参照）。
- OBDR を実行できるコンピュータ構成にしておく必要があります。 システムの BIOS は、El-Torito 標準で定義されているブート可能 CD をサポートしている必要があります。また、INT13h 機能の XXh により、LBA アドレッシングを使用しているハードディスク ドライブへの読み書きが可能である必要があります。 OBDR デバイスが CD-ROM をエミュレートする場合には、同じ標準に準拠していなければなり

ません。 BIOS のオプションは、システムのユーザー マニュアル、またはブート前にシステム設定を調査することでチェックできます。
サポートされているシステム、デバイスおよびメディアに関する詳細は、以下の Web ページにある HP StorageWorks のテープとハードウェアの互換性一覧表を参照してください。
http://www.hp.com/support/manuals 『HP Data Protector product announcements ソフトウェアノートおよびリファレンス』も参照してください。

- ターゲット システムのハードウェア構成は、障害発生前の状態と同じでなければなりません。 これには、SCSI の BIOS 設定（セクタの再マッピング）も含まれます。
- 同じバスの同じホストバスアダプタに交換用ディスクが接続されていること。
- 最小限のオペレーティング システムをインストールするブート パーティションは少なくとも 200MB 以上のサイズにする必要があります。 これを下回ると、ディザスタ リカバリが失敗します。 オリジナル パーティションで［ドライブを圧縮してディスク領域を空ける］オプションを有効に設定していた場合は、少なくとも 400MB の領域が必要になります。
- OBDR バックアップを実行するには、 Data Protector がインストールされているパーティションに少なくとも 200MB の一時的な空きスペースが必要です。 このスペースは、一時イメージの作成に使用されます。
- ブートに必要なドライバは、すべて *%SystemRoot%* フォルダにインストールされている必要があります。
- ネットワーク機能が付いたセーフ モード、またはディレクトリ サービス復元モード（ドメイン コントローラのみ）でシステムをブートする場合は、ネットワークが使用可能でなければなりません。ただし、システムのバックアップは通常のブート プロセスの後に実行する必要があります。
- メディアの使用ポリシーが［追加不可能］でメディア割り当てポリシーが［緩和］のメディア プールを OBDR 対応のデバイスに対して作成する必要があります。 ディザスタ リカバリには、このようなプールのメディアしか使用できません。
- オフライン復元を計画している場合は、クライアント バックアップ時のデバイスへの書き込みにはデフォルトのブロック サイズ 64KB を使用してください。 ディザスタ リカバリを実行する際に Windows で使用できるブロック サイズはこのデフォルトのサイズだけです。 デフォルトのブロック サイズ 64KB が設定されているかどうかを確かめるには、［プロパティ］ボックスの **［拡張...］** を選択します。図 4 （66ページ） を参照してください。

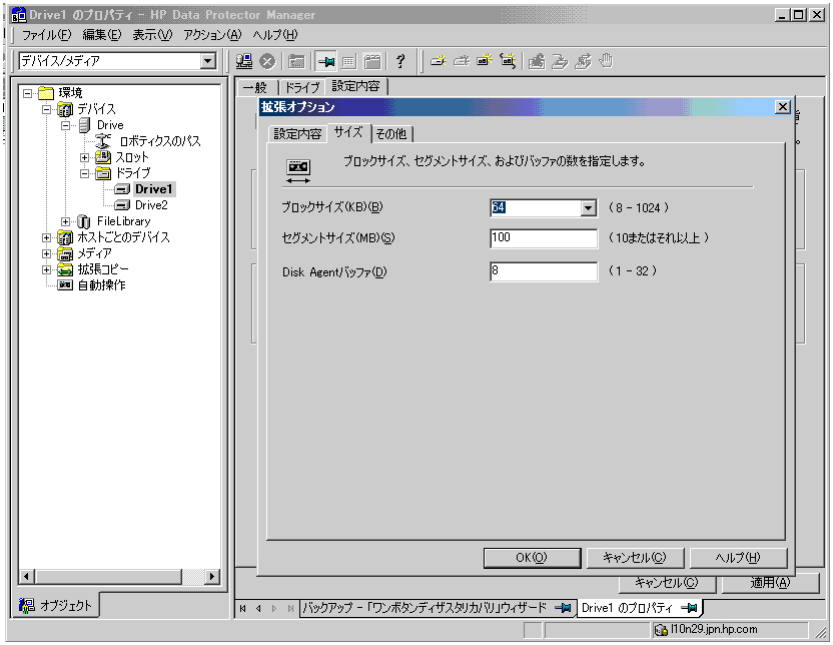


図 4 デフォルトのブロック サイズの確認

- AES 暗号化 OBDR バックアップを開始する前に、kms_allow_hosts ファイルが存在し、イメージが準備されたクライアントの完全修飾ドメイン名が含められている必要があります「kms_allow_hosts ファイルがない場合の、AES 暗号化バックアップのための ISO イメージの作成の失敗」 (126ページ) を参照)。
- Windows Automated Installation Kit (WAIK) 1.1 がバックアップするクライアントにインストールされている必要があります。 WAIK の古いバージョンはサポートされていません。

制限事項

- Microsoftのブートローダーを使用しないマルチブートシステムはサポートされていません。
- Internet Information Server (IIS) データベース、ターミナル サービス データベース、Certificate Server データベースは、フェーズ 2 で自動的には復元されません。これらをターゲット システムに復元するには、Data Protector 標準復元手順を実行してください。
- ワンボタン ディザスタ リカバリのバックアップ セッションは、同じ OBDR デバイス上では 1 度に 1 つのクライアントまたは Cell Manager に対してしか実行できません。 バックアップ セッションは、ローカルに接続された 1 台の OBDR 対応デバイス上で行う必要があります。
- ダイナミック ディスクはサポートされていません (Windows NT からのミラー セットのアップグレードも含む)。

- 新しいディスクのサイズは、クラッシュしたディスクのサイズ以上である必要があります。 元のディスクのサイズよりも大きい場合、余った分に対しては割り当てが行われません。
- OBDR でサポートされているベンダー固有のパーティションは、0x12 タイプ (EISA を含む) と 0xFE タイプのみです。
- OBDR は Data Protector が NTFS ボリュームにインストールされているシステムでのみサポートされています。
- LDM ディスクは Windows Vista ではサポートされていません。
- Intel Itanium システムでは、ブート ディスクの復旧はローカルの SCSI ディスク向けにのみサポートされています。

準備

この項で挙げられている手順を完了する前に、すべてのディザスタ リカバリの方法に共通する一般的な準備手順として「計画」 (31ページ) も参照してください。「高度な復旧作業」 (84ページ) も参照してください。

重要：

ディザスタ リカバリの準備は、障害が発生する*前に*行っておく必要があります。

DDS または LTO メディア用のメディア プールを作成します。 使用ポリシーは [追加不可能] (テープ上のバックアップであることを確実にするため)、メディア割り当てポリシーは [緩和] (テープは OBDR バックアップ時にフォーマットされるため) です。 また、このメディア プールを OBDR デバイス用のデフォルト メディア プールとして選択する必要があります。 オンラインヘルプの索引「メディア プールの作成」を参照してください。 このプールのメディアのみが、OBDR で使用できます。

Microsoft Cluster Server の場合： Microsoft Cluster Server のための整合性のあるバックアップには、(同じバックアップ セッションに) 以下のものが含まれている必要があります。

- すべてのノード
- 管理仮想サーバー (管理者が定義)
- Cell Manager 仮想サーバーと IDB (Data Protector がクラスター対応アプリケーションとして構成されている場合)

詳細については、「Microsoft Cluster Server の復元に固有の手順」 (84ページ) を参照してください。

OBDR で MSCS 内の全共有ディスク ボリュームの自動復元を可能にするには、ボリュームをすべて OBDR ブート テープの準備作業に使用するノードに一時的に移動します。 そうすることで、OBDR バックアップ中に共有ディスク ボリュームが他のノードによりロックされることはなくなります。 バックアップ時に他のノードによりロックされている共有ディスク ボリュームのディスクをフェーズ 1 で構成するために必要な情報を収集するのは不可能です。

OBDR バックアップ

OBDR を使用して復旧を実行したいシステム上で OBDR バックアップをローカルに実行するには、以下の手順を実行します。

1. コンテキスト リストで **[バックアップ]** を選択します。
2. Scoping ペインで **[タスク]** ナビゲーション タブをクリックし、**[ワンボタン ディザスタ リカバリ ウィザード]** を選択します。
3. **[次へ]** をクリックします。
4. クリティカル オブジェクトはすでにすべて選択された状態になっていて (Cell Manager OBDR バックアップの場合は IDB も含む)、選択を解除することはできません。 復旧手順の中で、 Data Protector はシステムからパーティションをすべて削除してしまうため、他のパーティションを復旧後も使用する場合、手動で選択します。 **[次へ]** をクリックします。
5. バックアップに使用するローカル接続の OBDR ドライブを選択して **[次へ]** をクリックします。
6. バックアップ オプションを選択します。 使用可能なオプションの詳細については、オンラインヘルプの索引「バックアップ オプション」を参照してください。

   Windows Vista システム: WAIKオプションの指定:

   - Windows 自動インストールキット (WAIK) ディレクトリを指定します。 場所を入力すると、Data Protector で保存され、ISO CD イメージが次回作成されるときに、GUI でデフォルト選択として使用されます。 ディレクトリが指定されていない場合は、Data Protector では WAIK のデフォルトのパスを使用します。
   - ISO CD イメージに挿入するドライバも指定できます。 このオプションを使用して、見つからないドライバを DR OS に追加することができます。 Windows Vista クライアント リカバリ セットの一部であるドライバを挿入するには、**[Autoinject drivers from Recovery Set]** を選択します。 リカバリ セットの *%Drivers%* の部分からドライバが自動的にDR OSイメージに挿入されます。

   注記:

   バックアップ手順で収集されてリカバリ セットの *%Drivers%*ディレクトリに保存されたドライバは、DR OS内での使用に適しているとは限りません。 場合によっては、Windows Preinstall Environment 固有のドライバを挿入して、復旧中のハードウェアの適切な動作を確保する必要があります。

   ドライバを手動で追加するには、**[Add]** をクリックして、不足しているドライバの名前を入力します。

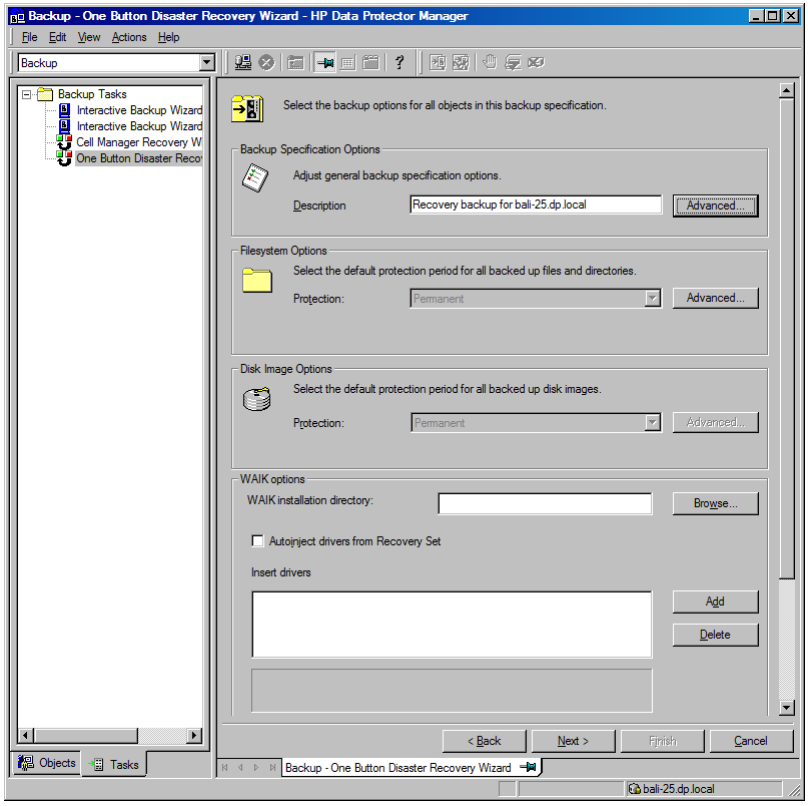


図 5 Windows Vista クライアントのバックアップ オプション

7. [次へ] をクリックして、[スケジューラ] ページを表示します。ここでは、バックアップの実行スケジュールを設定できます。 詳細は、オンライン ヘルプの索引キーワード「特定の日時にバックアップの実行をスケジュールする」で表示される内容を参照してください。
8. [次へ] をクリックして、[バックアップ オブジェクトのサマリー] ページを表示します。 このページには、バックアップ オプションが表示されます。

注記：

[サマリー] ページでは、それまでに選択したバックアップ デバイスやバックアップ仕様の順序を変更することができません (順序を入れ替える機能はありません)。 OBDR に必要ではないバックアップ オブジェクトのみ削除可能であり、一般的なオブジェクトのプロパティのみ表示できます。

ただし、バックアップ オブジェクトの説明は変更できます。

9. ［バックアップ］ウィザードの最終ページでは、バックアップ仕様の保存、対話型バックアップの開始、またはバックアップのプレビューを行うことができます。

   バックアップ仕様を保存して、後でスケジュールを設定したり仕様を変更できるようにしておくことをお勧めします。

   バックアップ仕様を一度保存すると、編集が可能になります。 バックアップ仕様を右クリックして、**［プロパティ］**を選択します。 変更されたバックアップ仕様を、Data Protector の標準バックアップ仕様または OBDR バックアップ仕様として扱うことができます。 修正したバックアップ仕様は、ワンボタン ディザスタ リカバリ固有の形式が保持されるように、OBDR バックアップ仕様として保存してください。 標準バックアップ仕様として保存した場合は、OBDR には使用できません。

10. **［バックアップ開始］**をクリックして、バックアップを対話形式で実行します。［バックアップ開始］ダイアログ ボックスが表示されます。 **［OK］**をクリックしてバックアップを開始します。

一時 DR OS のインストールと構成に必要な情報がすべて含まれているシステム用ブート可能イメージはテープの先頭に書き込まれ、これによりテープからのブートが可能となります。

重要：

ハードウェア、ソフトウェア、構成などに変更があった場合には、その都度バックアップを実行してブート可能なバックアップ メディアを作成します。 これは、IP アドレスや DNS サーバーの変更など、ネットワーク構成が変更された場合も同じです。

kb.cfg ファイル

このファイルの目的は、特定のブート関連ハードウェアまたはアプリケーション構成を持つシステム用に、ドライバ（および他の必要ファイル）を DR OS に含めるための柔軟な方法を提供することです。 デフォルトの kb.cfg ファイルには、あらかじめ業界標準のハードウェア構成に必要なすべてのファイルが含まれています。

デフォルトの kb.cfg ファイルを使用したテスト プランを作成し実行します。 DR OS が正常にブートしない、またはネットワークにアクセスできない場合は、ファイルを変更する必要があります。 詳細については、「kb.cfg ファイルの編集」（93 ページ）を参照してください。

△ **注意：**

バックアップメディアへのアクセスは、セキュリティ維持のため制限しておくことをお勧めします。

暗号化キーの準備

Cell Manager の復旧またはオフライン クライアントの復旧に対しては、暗号化キーをリムーバブル メディアに保存して、ディザスタ リカバリの際に使用できるようにする必要があります。 Cell Manager の復旧に対しては、事前に（障害が発生する前に）リムーバブル メディアを準備してください。

暗号化キーは、DR OS イメージ ファイルの一部ではありません。このキーは、ディザスタ リカバリ イメージの作成時に、*Data_Protector_home*\Config\Server\export\keys\DR-*ClientName*-keys.csv に自動的にエクスポートされます。ここで、*ClientName* はイメージを作成するクライアントの名前です。

ディザスタ リカバリの準備のための各バックアップについて、正しい暗号化キーがあることを確認してください。

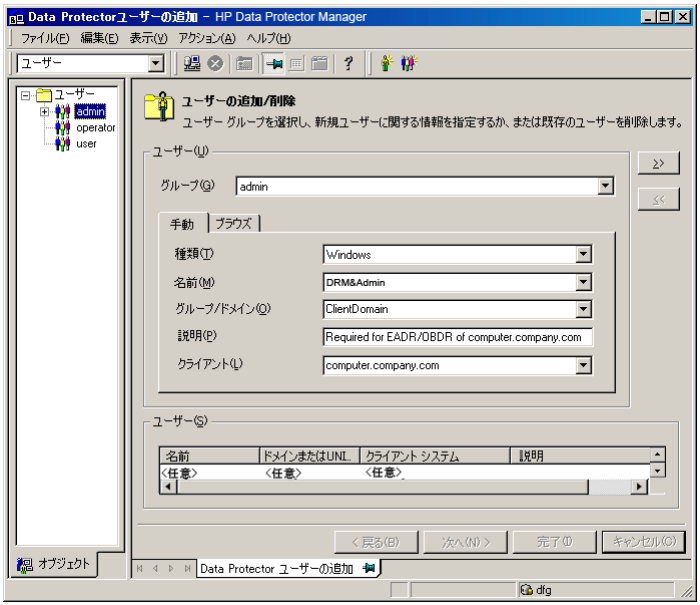
Recovery

クラッシュしたシステム上でシステムのディザスタ リカバリを正しく実行するには、以下が必要です。

- クラッシュしたディスクと交換する新しいハードディスク（必要な場合）。
- 復旧対象クライアントのクリティカル オブジェクトがすべて含まれたブート可能なバックアップ メディア。
- ターゲット システムにローカル接続された OBDR デバイス。

Windows システムのワンボタン ディザスタ リカバリの詳細な手順を以下に示します。

1. オフライン障害復旧を行う場合以外は、Cell Manager 上の Data Protector の Admin ユーザー グループに SYSTEM/NT Authority (Windows Vista の場合)またはDRM$Admin（その他の Windows システムの場合）というアカウントを追加します。 詳細は、オンライン ヘルプの索引キーワード「追加, Data Protector ユーザー」で表示される内容を参照してください。



2. イメージファイルとバックアップデータが格納されたテープをOBDRデバイスに挿入します。
3. ターゲットシステムをシャットダウンし、テープデバイスの電源を切ります。 復旧手順を開始する前に、システムに外付けの USB ディスク (USB キーを含む) が接続されていないことを確認してください。
4. ターゲット システムの電源を入れ、初期化中にテープ デバイスの取出しボタンを押して、テープ デバイスの電源を入れます。 詳しくはデバイス付属のドキュメントを参照してください。
5. Windows Vista では、先に DR OS がメモリにロードされてから、範囲メニューが表示されます。 その他のWindowsシステムの場合は、ブートプロセスの最初に範囲選択メニューが表示されます。

   復旧範囲を選択して、**Enter** キーを押します。復旧範囲は 5 種類あります。

   - **[再起動]**: ディザスタ リカバリは実行されず、コンピュータが再起動されます。
   - **[デフォルト復旧]**: クリティカル ボリュームが復旧されます。 他のすべてのディスクはパーティション作成やフォーマットが行われず空のまま残され、フェーズ 3 に備えた状態になります。
   - **[最小復旧]**:システム ディスクとブート ディスクのみが復旧されます (EADR と OBDR のみで使用可能)。
   - **[Full Recovery]**: 重要なものだけでなく、すべてのボリュームが復旧されます。
   - **[共有ボリュームを含む完全復旧]**: Microsoft Cluster Server (MSCS)の場合にのみ選択できるオプションです。 このオプションは、MSCS 内のすべ

てのノードがクラッシュして、最初のノードに対するワンボタン ディザスタ リカバリを実行する場合に使用します。 復元セット内のすべてのボリューム（バックアップ時にバックアップ対象のノードによりロックされていたクラスター共有ボリュームを含む）が復元されます。

ヒント：

MSCS 内の全共有ディスク ボリュームの自動復元を可能にするには、ボリュームをすべて OBDR ブート テープの準備作業に使用するノードに一時的に移動します。 バックアップ時に他のノードによりロックされている共有ディスク ボリュームのディスクをフェーズ 1 で構成するために必要な情報を収集するのは不可能なことです。

1 つでも稼動中のノードがあって MSCS サービスが実行されている場合、共有ボリュームは復元されません。稼動中のノードが共有ボリュームをロックしているためです。 この場合は[デフォルト復旧]を使用してください。

ハードウェアのプラットフォームやオペレーティング システムによってはその他にもオプションがあり、主にディザスタ リカバリが完全に終了せず、追加の手順が必要な場合に使用します。

- **[Restore BCD]**：Windows Vista でのみ使用可能です。 デフォルトでは、Data Protector はディザスタ リカバリの際に Boot Configuration Data (BCD) ストアを復元します。BCD ストアが復元されないと、マシンがブートできなくなる場合があります。
- **[Restore DAT]**：Windows Vista でのみ使用可能です。 Data Protector による復元前または復元後に、DR OS の一部として DAT ファイルに保存されているライターのデータを復元できます。
- **[Remove Boot Descriptor]**：Intel Itanium システムでのみ使用可能です。ディザスタ リカバリのプロセスによって残された起動記述子をすべて削除します。「Intel Itanium 固有の問題」（128ページ）を参照してください。
- **[Manual disk selection]**：Intel Itanium システムでのみ使用可能です。ディスクの設定が大幅に変更された場合は、ディザスタ リカバリ モジュールがブート ディスクを見つけることができません。 このオプションを使用して正しいブート ディスクを選択します。「Intel Itanium 固有の問題」（128ページ）を参照してください。

Windows Vista のみ：BitLocker ドライブ暗号化を使用してボリュームが暗号化されている場合、メニューが表示されて、暗号化されたドライバのロックを解除できます。「Windows VistaのBitLocker ドライブ暗号化」（98ページ）を参照してください。

6. 復旧範囲を選択すると、Data Protector は、ハードディスクに対して直接 DR OS のセットアップを開始します。 この処理の進行状況はモニター可能です。 DR OS のセットアップが完了するとシステムは再起動します。 Windows Vista の場合は、DR OS はインストールされず、再起動は行われません。

   ディザスタ リカバリ オプションを変更するには、カウントダウン中に任意のキーを押してウィザードを停止した後、オプションを変更します。 **[完了]** をクリックして、ディザスタ リカバリを続行します。

7. ディザスタ リカバリのバックアップが暗号化されているときに、Cell Manager を復旧または Cell Manager がアクセスできないクライアントを復旧しようとすると、次のプロンプトが表示されます。

   Do you want to use AES key file for decryption [y/n]?

   [y] キーを押してください。

   キー ストア (DR-*ClientName*-keys.csv) がクライアントからアクセスできること (たとえば、CD-ROM、フロッピー ディスク、または USB フラッシュ キーなどにある) を確認し、キー ストア ファイルのフル パスを入力します。 キー ストア ファイルが DR OS のデフォルトの場所にコピーされ、Disk Agent によって使用されます。 以降は何の操作も必要なく、ディザスタ リカバリが続行されます。

8. 障害発生後にバックアップ デバイスを変更したなどの理由で SRD ファイルの情報が最新のものでなく、オフライン復旧を実行しようとしている場合は、この手順を続行する前に SRD ファイルを変更してください。 詳細については、「編集後の SRD ファイルを使用した復旧」 (94ページ) を参照してください。

9. 次に Data Protector は、従来の記憶データ構造を再構築し、すべてのクリティカル ボリュームを復元します。

   一時 DR OS は、以下の場合を除いて、最初のログイン時に削除されます。

   - [最小復旧] が選択された場合。
   - ディザスタ リカバリ ウィザードが DR のインストールとバックアップ メディア上の SRD ファイルを発見した後の 10 秒間のポーズの間に、ユーザーがウィザードを中断して **[Debugs]** オプションを選択した場合。
   - omnidr コマンドを、-no_reset または -debug オプションを付けて手動で起動した場合。
   - ディザスタリカバリが失敗した場合。

   Windows Vista の場合は、一時 DR OS が残されることはありません。

10. ステップステップ 1 (71ページ) で追加したクライアントのローカル管理者アカウントが、障害復旧前に Cell Manager 上に存在していなかった場合は、Cell Manager 上の Data Protector Admin ユーザー グループから削除します。

11. Cell Manager の復旧、または高度な復旧作業 (MSCS または IIS の復旧、kb.cfg および SRD ファイルの編集など) を行おうとしている場合は、特別な手順が必要となります。 詳細については、「Data Protector Cell Manager 固有の復元手順」 (90ページ) と「高度な復旧作業」 (84ページ) を参照してください。

12. Data Protector 標準復元手順を使用して、ユーザー データとアプリケーション データを復元します。

注記：

Data Protector はボリューム圧縮フラグを復元しません。 バックアップ時に圧縮されていたファイルはすべて圧縮されて復元されますが、新しく作成するファイルも圧縮ファイルとして作成したい場合は、手動でボリューム圧縮フラグをセットする必要があります。

自動システム復旧

自動システム復旧(ASR)はWindowsシステム上の自動システムで、障害発生時にディスクをオリジナルの状態に再構成(または、新しいディスクがオリジナルのものより大きい場合、パーティションをサイズ変更)します。 この処理には、ディスクのパーティション化と論理ボリュームの構成(ファイル形式、ドライブ文字の割り当て、ボリュームマウントポイント、およびボリューム特性)が含まれます。 このように ASR は Data Protector の drstart.exe コマンドにより、Data Protector ディスク、ネットワーク、テープ、ファイルシステムへのアクセスを提供するアクティブな DR OS をインストールすることができます。

Data Protector は次に、ターゲット システムを元のシステム構成に復旧し、最後にユーザー データを復元します。

サポート対象のオペレーティング システムは、『HP Data Protector product announcements ソフトウェアノートおよびリファレンス』を参照してください。

重要：

ハードウェアやソフトウェア、または構成が変更された場合や、ASR ディスクをアップデートする場合には、その都度クライアントのフル バックアップを行う必要があります。 これは、IP アドレスや DNS サーバーの変更など、ネットワーク構成が変更された場合も同じです。

重要：

Cell Manager 用の ASR セットは、前もって作成しておく必要があります。これは、障害後には ASR アーカイブ ファイルを取得できないためです。 他のシステム用の ASR セットは障害発生時に Cell Manager を使用して作成できます。

復旧対象となるパーティションを以下に示します。

- ブート パーティション
- システム パーティション
- Data Protector を含むパーティション

その他のパーティションは、通常の Data Protector 復旧手順を使って復旧できます。

概要

Windows クライアントに対して自動システム復旧（ASR）を行う手順の概要は、以下のとおりです。

1. **フェーズ 0**
   a. フル クライアント バックアップを実行します。
   b. Data Protector バイナリをコピーした ASR フロッピー ディスクを作成し、構成を変更するたびに 1 枚目のフロッピー ディスクを更新します。
   c. 暗号化されたバックアップを使用している場合は、暗号化キーをリムーバブル メディアに保存して、ディザスタ リカバリの際に使用できるようにします。Cell Manager の復旧時、または Cell Manager への接続を確立できない場合には、このキーが必要になります。
2. **フェーズ 1**
   a. Windows インストール メディアからブートし、**F2** キーを押して ASR モードに切り替えます。
   b. ASRセットの1枚目のフロッピーディスク(更新されたフロッピーディスク)を用意します。
   c. 再ブート後、DR のインストールおよび SRD ファイルの場所に関する情報を指定します（a:\）。
   d. プロンプトが表示されたらフロッピー ディスクを交換します。
3. **フェーズ 2**
   a. すべてのクリティカル オブジェクトが自動的に復元されます。 システムを再起動し、Windows インストール メディアと ASR フロッピー ディスクを取り出します。
4. **フェーズ3**
   a. Data Protector 標準復元手順を使用して、ユーザー データとアプリケーション データを復元します。

ASR は、障害への準備作業（の一部）を実行するとともに、ブート パーティションを再作成する目的で使用されます。Data Protector には、集中管理、高パフォーマンスバックアップ、高可用性サポート、復元、監視、レポート、通知など、その他の必要な機能がすべて用意されています。

以下の項で、Windows システム上での自動システム復旧に関する必要条件、制限事項、準備、および、復旧について説明します。「高度な復旧作業」（84ページ）も参照してください。

要件

- Data Protector 自動システム復旧コンポーネントが、ASR で復旧するシステム上にインストールされている必要があります。 『HP 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。

- ファイアウォールを使用している場合は、ポート 1071 と 1073 が開放されている必要があります。 ASR は変数OB2PORTRANGE と OB2PORTRANGESPEC をサポートしていません。

ハードウェア構成

- ターゲット システムのハードウェア構成は、元のシステムのハードウェア構成と同じでなければなりません。 ただし、ハードディスク ドライブ、ビデオ カード、ネットワーク インターフェース カードは除きます。 ネットワーク カードまたはビデオ カードを交換した場合は、それらを手動で構成する必要があります。
- フロッピーディスクのディスクドライブがインストールされていること。
- フロッピー ドライブと CD ドライブが、IDE または SCSI コントローラに接続されている必要があります。 USB や PCMCIA デバイスなどの外部デバイスはサポートされていません。
  ただし、USB のフロッピー ドライブを使用した ASR は HP Integrity サーバー (IA-64 プラットフォーム) 上でサポートされています。 詳細は、http://docs.hp.com/en/windows.html 上のホワイト ペーパー『Recovering Windows Server 2003 on HP Integrity servers』を参照してください。

ハードディスク ドライブ

- ターゲットシステムと元のシステムの間で、重要なボリュームを持つ物理ディスクの数が一致していること。
- 同じバスの同じホストバスアダプタに交換用ディスクが接続されていること。
- ターゲット システムの各交換ディスクの記憶容量は、元のシステムの対応するディスクの記憶容量以上である必要があります。 さらに、交換ディスクのジオメトリも交換前のディスクと同じである必要があります。
- ターゲットシステム上のどのディスクも、セクターあたりのバイト数が512バイトであること。
- ASR で使用されるすべてのディスクがシステムからアクセスできる必要があります (ハードウェア RAID が構成されている、SCSI ディスクが適切にターミネートされている、など)。
- オフライン復元を計画している場合は、クライアント バックアップ時のデバイスへの書き込みにはデフォルトのブロック サイズ 64KB を使用してください。 ディザスタ リカバリを実行する際に Windows で使用できるブロック サイズはこのデフォルトのサイズだけです。 デフォルトのブロック サイズ 64KB が設定されているかどうかを確かめるには、[プロパティ] ボックスの **[拡張...]** を選択します。図 6 (78ページ) を参照してください。

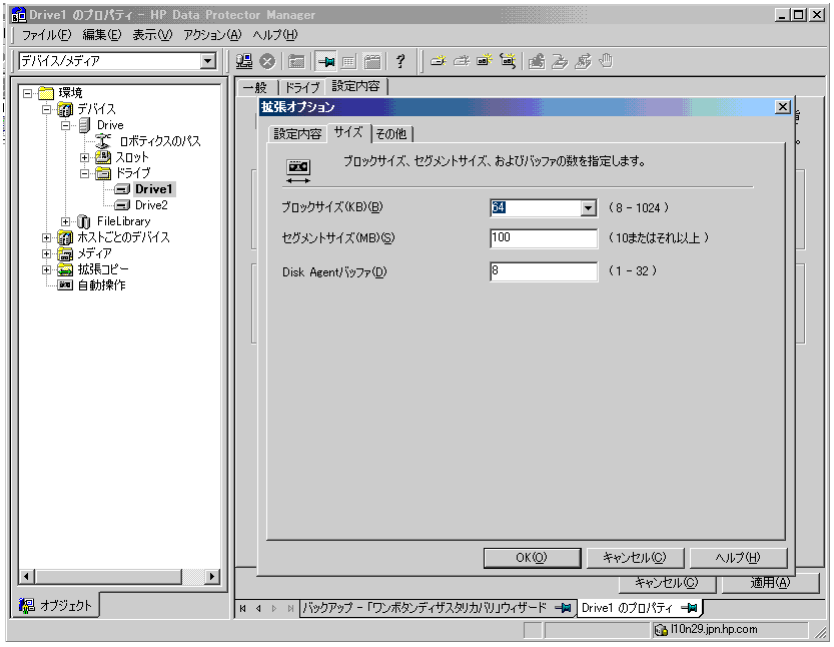


図 6 デフォルトのブロック サイズの確認

制限事項

- Windows XP Home Edition は ASR をサポートしていません。
- Microsoftのブートローダーを使用しないマルチブートシステムはサポートされていません。
- Internet Information Server (IIS) データベース、ターミナル サービス データベース、Certificate Server データベースは、フェーズ 2 で自動的には復元されません。これらをターゲット システムに復元するには、Data Protector 標準復元手順を実行してください。
- ベンダー固有のパーティションに格納されていたデータは、ASR では自動的に復元されません。 ASR 時にパーティションは再作成されますが、データはベンダー固有の手順で復元する必要があります。 ただし、EISA ユーティリティ パーティションに格納されていたデータは、Data Protector 標準復元手順で復元できます。
- サポートされているローカルバックアップデバイスは、Windowsのインストール中にインストール可能なデバイス(追加のドライバが必要とならないデバイス)だけです。

準備

この項で挙げられている手順を完了する前に、すべてのディザスタ リカバリの方法に共通する一般的な準備手順として「計画」（31ページ）も参照してください。 さらに、ディザスタ リカバリの準備に関して「高度な復旧作業」（84ページ）を参照してください。

重要：

ディザスタ リカバリの準備は、障害が発生する*前に*行っておく必要があります。

前提

- 自動システム復旧を正常に行うためには、フル クライアント バックアップ (CONFIGURATION も含む）が必要です。 オンライン ヘルプの索引キーワード「バックアップ、Windows 固有」および「バックアップ、構成」で表示される内容を参照してください。
  Microsoft Cluster Server のための整合性のあるバックアップには、(同じバックアップ セッションに）以下のものが含まれている必要があります。
  - すべてのノード
  - 管理仮想サーバー（管理者が定義）
  - Cell Manager 仮想サーバーと IDB (Data Protector がクラスター対応アプリケーションとして構成されている場合）

  詳細については、「Microsoft Cluster Server の復元に固有の手順」（84ページ） を参照してください。

フル クライアント バックアップの実行後、ASR セットを作成する必要があります。ASR セットは 3 枚または 4 枚のフロッピー ディスクに格納されたファイルの集まりで、交換ディスクの適切な再構成（ディスクのパーティションと論理ボリュームの構成)、および元のシステムの構成とフル クライアント バックアップでバックアップされたユーザー データの自動復旧に必要なものです。 これらのファイルは、ASR アーカイブ ファイルとして、バックアップ メディア上だけでなく Cell Manager 上の、*Data_Protector_home*\Config\server\dr\asr（Windows の場合）または /etc/opt/omni/server/dr/asr/（UNIX の場合）にも格納されます。 ASR アーカイブ ファイルは、障害発生後、32 ビット版 Windows システムでは 3 枚、64 ビット版 Windows システムでは 4 枚のフロッピー ディスクに取り出されます。 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。

注記：

Cell Manager 用の ASR セットは、前もって作成しておく必要があります。これは、障害後には ASR アーカイブ ファイルを取得できないためです。

ASR セットを作成するには、以下の手順を実行します。

1. フル クライアント バックアップを実行します。
2. フロッピー ディスクをフロッピー ディスク ドライブに挿入します。
3. [HP Data Protector Manager] で [復元] コンテキストを選択します。
4. Scoping ペインで **[タスク]** ナビゲーション タブをクリックし、**[ディザスタ リカバリ]** を選択します。
5. 結果エリアのドロップダウン リストから、ASR セットを作成するクライアントを選択します。
6. **[自動システム リカバリ セットの作成]** をクリックし、**[次へ]** をクリックします。

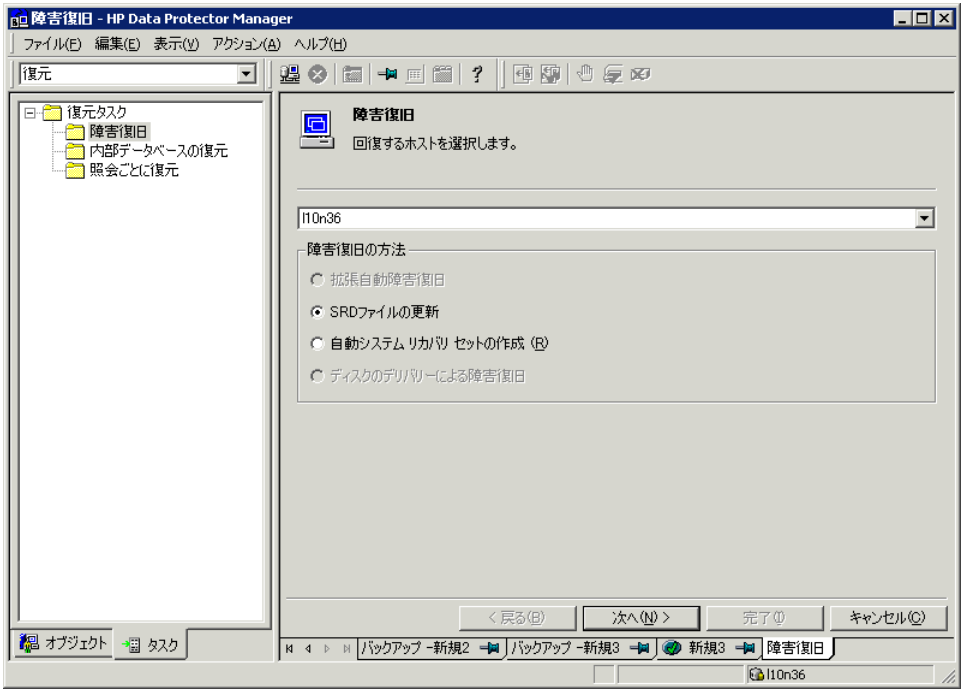


図 7 ASR セットの作成

Data Protector が Cell Manager から ASR アーカイブ ファイルを取得します。Cell Manager に保存されていない場合は、ディザスタ リカバリ ウィザードによりバックアップ メディアから復旧するようメッセージが表示されます。

7. 各クリティカル オブジェクトごとに、適切なオブジェクト バージョンを選択して、**[次へ]** をクリックします。

8. フル クライアント バックアップ時に作成された ASR アーカイブ ファイルが、Cell Manager からダウンロードされます。 取得された ASR アーカイブ ファイルの保存先を選択し、 **[DR インストールをコピー]** チェック ボックスをオンにして、DR インストール ファイルを同じ場所にコピーします。 ASR を実行するにはこれらのファイルをフロッピー ディスク（ASR セット）に保存する必要があるため、フロッピー ドライブを保存先に指定することをお勧めします。

   Data Protector は、32 ビット版 Windows システム用には 3 枚、64 ビット版 Windows システム用には 4 枚のディスクを作成します。 Cell Manager 用の ASR セットは事前に作成しておく必要がありますが、他のシステム用の ASR ディスクは障害発生時に Cell Manager を使用して作成できます。

ASR セットの作成後、ハードウェアやソフトウェア、構成の変更があった場合には、その都度 1 枚目のディスクのみをアップデートする必要があります。 これは、IP アドレスや DNS サーバーの変更など、ネットワーク構成が変更された場合も同じです。 ASR セットの 1 枚目のディスクをアップデートするには、最初からすべての手順を再度実行しますが、[DR インストールをコピー] チェック ボックスをオンにする必要はありません。 このオプションを選択すると、アップデートには不要な DR インストール ファイルが（選択した保存先に）コピーされます。

重要：

ASRフロッピーディスクへのアクセスは、セキュリティ維持のため制限しておくことをお勧めします。

ローカル デバイス

ローカル接続されたデバイスを ASR 用に使用する場合は、そのデバイスがサポートされているか確認してください。 以下の手順で確認します。

1. コマンド プロンプトから devbra -dev を実行します（ディレクトリは *Data_Protector_home*\bin）。
2. scsitab ファイル（ディレクトリは *Data_Protector_home*）の名前を変更して、コマンド プロンプトから devbra -dev を実行します。
3. devbra -dev コマンドの 2 つの出力を比較します。 2 つのファイルが同じであれば、ASR でそのデバイスを使用することができます。そうでない場合は、scsitab ファイルを ASR ディスクの 1枚目にコピーします。 scsitab ファイルをコピーする必要があるのは、最初に ASR セットを作成する時のみです。 ASR セットのアップデートだけを行う場合には、コピーする必要はありません。 オンラインヘルプの索引キーワード「新しいデバイスのサポート」で表示される内容を参照してください。
4. scsitab ファイル名前を元に戻します。

Recovery

クラッシュしたシステムのディザスタ リカバリを正常に実行するには、以下が必要です。

- クラッシュしたディスクと交換するための新しいハードディスク。
- 復旧対象のクライアントの正常なフル バックアップ
- アップデート済みの ASR セット
- Windowsインストールメディア

ASR を実行する手順を以下に示します。

1. Windowsのインストールメディアからシステムをブートします。
2. OS のセットアップ時に **F2** キーを押して、ASR モードに入ります。
3. ASRセットの1枚目のフロッピーディスク(更新されたフロッピーディスク)を用意します。
4. 再起動後、障害復旧ウィザードが起動され、[DR Installation Source] と [SRD Path] の入力を求めてきます。 DR インストール ファイルと SRD ファイルは、両方とも ASR セットの 1 枚目のディスクにあります (a:\)。

   ASR の設定を変更するには、カウントダウン中に任意のキーを押してウィザードを停止した後、オプションを選択します。 **[完了]** をクリックして、ディザスタ リカバリを続行します。

   障害発生後にバックアップ デバイスを変更したなどの理由で ASR ディスク上の SRD ファイルの情報が最新のものでなく、オフライン復旧を実行しようとしている場合は、この手順を続行する前に SRD ファイルを変更してください。「編集後の SRD ファイルを使用した復旧」 (94ページ) を参照。

注記：

オリジナルの OS メディアに適切なドライバが用意されていないと、ASR を実行できません。 [ハードウェアの追加] ウィザードを使用して、ネットワークをインストールすることができます。このウィザードは以下のコマンドで起動できます。 *%SystemRoot%*\System32\rundll32.exe shell32.dll,Control_RunDLL hdwwiz.cpl

5. オフライン ディザスタ リカバリを行う場合以外は、Cell Manager 上の Data Protector の Admin ユーザー グループにクライアントのローカル システム アカウントを追加します。 オンラインヘルプの索引「ユーザー、Data Protector"」を参照してください。

   図 8 (83ページ) に示されている情報を入力します。

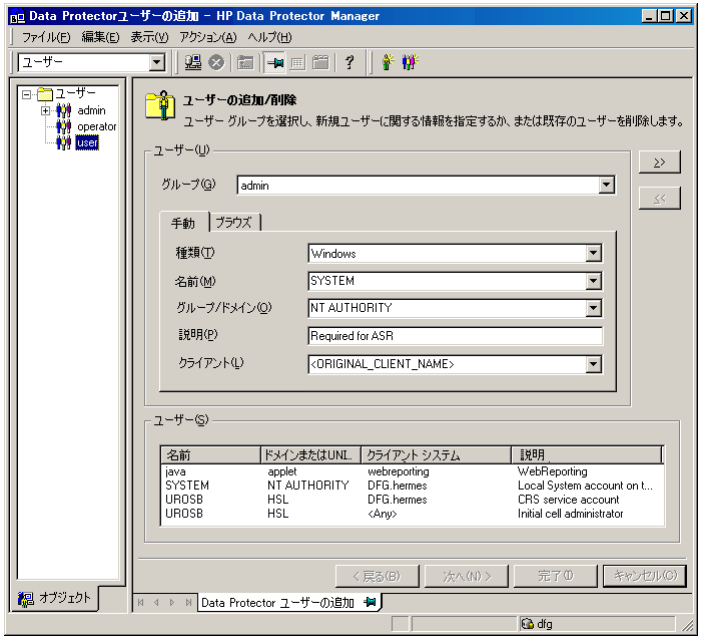


図 8 ASR のユーザー名

6. プロンプトが表示されたらフロッピー ディスクを交換します。
7. プロンプトが表示されたらシステムを再起動し、Windows インストール メディアと ASR ディスクを取り出します。
8. ディザスタ リカバリのバックアップが Data Protector によって暗号化されているときに、Cell Manager を復旧または Cell Manager がアクセスできないクライアントを復旧しようとすると、次のプロンプトが表示されます。

   Do you want to use AES key file for decryption [y/n]?

   [y] キーを押してください。 キー ストア (DR-ClientName-keys.csv) が (キーが保存されたメディアを挿入することにより) クライアントからアクセスできることを確認し、キー ストア ファイルのフル パスを入力します。キー ストア ファイルが DR OS のデフォルトの場所にコピーされ、Disk Agent によって使用されます。
9. ステップステップ 5 (82ページ) で追加したクライアントのローカル システム アカウントが、ディザスタ リカバリ前に Cell Manager 上に存在していなかった場合は、Cell Manager 上の Data Protector Admin ユーザー グループから削除します。
10. Data Protector 標準復元手順を使用して、ユーザー データとアプリケーション データを復元します。

高度な復旧作業

この項では、Microsoft Cluster Server や Internet Information Server の復元など、高度な復旧作業を行う場合に必要な手順について説明します。

Microsoft Cluster Server の復元に固有の手順

この項では、Microsoft Cluster Server (MSCS) のディザスタ リカバリを行う場合に必要な手順について説明します。 概念と一般的情報については、『HP Data Protector コンセプトガイド』のクラスター化関連の項を参照してください。 また、オンライン ヘルプの索引キーワード「クラスター」で表示される内容を参照してください。

ご使用のクラスター環境に適したディザスタ リカバリの方法を選択し、ディザスタ リカバリ プランに取り入れます。 どの方法を使用するかを決定する前に、それぞれのディザスタリカバリ方法の制限と必要条件を十分に検討し、 テスト計画に基づいてテストを実施してください。

考えられる状況

MSCS のディザスタ リカバリでは、考えられる状況が 2 つあります。

- 最低 1 台のノードが稼動している場合
- クラスタ内のすべてのノードに障害が発生した場合

重要：

MSCS の復旧は、「ディスク デリバリーによるディザスタ リカバリ」以外の方法で行えます。 使用するディザスタ リカバリの方法に関する固有の制限や必要条件は、MSCS のディザスタ リカバリにも当てはまります。 サポート対象のオペレーティング システムは、『HP Data Protector product announcements ソフトウェアノートおよびリファレンス』を参照してください。

MSCS を復旧するには、ディザスタ リカバリの必要条件（整合性のある最新のバックアップ、更新済みの SRD ファイル、不良ハードウェアの交換など）がすべて満たされていなければなりません。

MSCS のための整合性のあるバックアップには、(同じバックアップ セッションに）以下のものが含まれている必要があります。

- すべてのノード
- 管理仮想サーバー（管理者が定義）
- Cell Manager 仮想サーバーと IDB (Data Protector がクラスター対応アプリケーションとして構成されている場合）

二次ノードのディザスタ リカバリ

これは MSCS のディザスタ リカバリについての基本的な状況です。 ディザスタ リカバリに関する他の必要条件に加えて、以下の条件も満たされている必要があります。

- 最低 1 台のクラスター ノードが正常に機能していること
- そのノード上でクラスター サービスが実行されていること
- すべての物理ディスク資源がオンラインであること（つまり、クラスターによって所有されていること）
- 通常のクラスター機能がすべて使用可能であること（クラスター管理グループがオンラインであること）
- Cell Manager がオンラインであること

この場合、クラスター ノードのディザスタ リカバリは Data Protector クライアントのディザスタ リカバリと同じです。 二次ノードの復元に使用する特定のディザスタ リカバリの方法の手順に従ってください。

注記：

ローカル ディスクのみが復元されます。復旧作業中でも共有ディスクはすべてオンラインであり、稼動中のノードにより所有/ロックされているためです。

復旧が完了したセカンダリノードは、ブート後にクラスタに追加されます。

MSCS データベースの復元は、すべてのノードの復旧が完了し、それらがクラスターに参加したあとに実行できます。そうすることによって、すべてのノードが共同作用することを確実にします。 MSCS データベースは、Windows の CONFIGURATION に含まれています。 オンラインヘルプの索引キーワード「構成オブジェクトの復元」で表示される内容を参照してください。

一次ノードのディザスタ リカバリ

この場合、MSCS 内のすべてのノードが使用不能で、クラスター サービスは実行されていません。

ディザスタ リカバリに関する他の必要条件に加えて、以下の条件も満たされている必要があります。

- 一次ノードはクォーラム ディスクへの書き込みが可能である必要があります（クォーラム ディスクはロックされていてはいけません）。
- Cell Manager を復旧する場合、一次ノードはすべての IDB ボリュームへの書き込みが可能である必要があります。
- すべての物理ディスク資源がオンラインになるまで、他のノードはすべてシャットダウンしておく必要があります。

この場合、一次ノードの復元の際にはクォーラム ディスクを最初に復元します。 Cell Manager がクラスターにインストールされている場合には、IDB の復元も必要です。

必要に応じて、MSCS データベースを復元することもできます。 一次ノードの復元が完了したら、残りの全ノードの復元が可能となります。

注記：

MSCS サービスは、すべてのハードディスクの MBR に書き込まれているハードディスク署名を使用しています。 共有クラスター ディスクを交換した場合、ディザスタ リカバリのフェーズ 1 でこのディスク署名が変わることになります。 その結果、クラスター サービスは交換されたディスクを有効なクラスター資源として認識せず、その資源に依存するクラスター グループは正常に動作しません。 詳細は、「Windows でのハードディスク署名の復元」（88ページ）を参照してください。

一次ノードの復元は、以下の手順で行います。

1. クォーラムディスクを含めて、プライマリノードのディザスタリカバリを実行します。
   - 半自動ディザスタ リカバリの場合：クォーラム ディスク上のすべてのユーザー データとアプリケーション データが、drstart コマンド（-full_clus オプション）によって自動的に復元されます。
   - 拡張自動ディザスタ リカバリおよびワンボタン ディザスタ リカバリの場合：復旧範囲を尋ねられたときに、**[共有ボリュームを含む完全復旧]** を選択してクォーラム ディスクを復元します
   - 自動システム復旧の場合：クォーラム ディスク上のすべてのユーザー データとアプリケーション データは、自動的に復元されます。

   ヒント：

   OBDR で、MSCS 内の全共有ディスク ボリュームの自動復元を可能にするには、ボリュームをすべて OBDR ブート テープの準備作業に使用するノードに一時的に移動します。 他のノードによりロックされている共有ディスク ボリュームのディスクをフェーズ 1 で構成するために必要な情報を収集するのは不可能です。
2. コンピュータを再起動する。
3. クラスター データベースを復元します。 MSCS データベースは、Windows の CONFIGURATION に含まれています。 オンラインヘルプの索引キーワード「構成オブジェクトの復元」で表示される内容を参照してください。

注記：

MSCS データベースを復元するには、MSCS サービスが実行中である必要があります。 したがって、ディザスタ リカバリのフェーズ 2 では自動的に復元されません。 しかし、クラスター データベースはフェーズ 2 の最後に Data Protector 標準復元手順で復元できます。

4. Cell Manager を復元している場合は、IDB の整合性を取ります。「IDB の整合性をとる (すべての方法)」 (90ページ) を参照。
5. 定数ボリュームと IDB ボリュームが復元されます。 他のすべてのボリュームは影響を受けず、破損していなければ復元された一次ノードにより所有されます。

   他のボリュームが破損していた場合は、以下を行う必要があります。

   a. クラスター サービスとクラスター ディスク ドライバを使用不可にします (MSDN Q176970 に記述されているとおりに行う必要があります)。
   b. システムを再起動します。
   c. 従来の記憶データ構造を再構築します。
   d. クラスター サービスとクラスター ディスク ドライバを使用可能にします。
   e. システムを再起動します。
   f. ユーザー データとアプリケーション データを復元します。
6. 残りのノードを復元します。「二次ノードのディザスタ リカバリ」 (85ページ) を参照。

EADR 用に全ノードの P1S ファイルをマージ

EADR を行うには、バックアップ実行後に特別な手順が必要です。 バックアップ時に他のノードによりロックされている共有ディスク ボリュームのディスクをフェーズ 1 で構成するために必要な情報を収集するのは不可能です。 すべての共有ディスク ボリュームを復元するにはこの情報が必要です。 クラスター内の全ノードの P1S ファイルに共有クラスター ボリューム情報を含めるには、以下のいずれかを実行します。

- フル クライアント バックアップ実行後、クラスター内の全ノードの P1S ファイルに含まれる共有クラスター ボリューム情報をマージします。これにより、各ノードの P1S ファイルには共有クラスター ボリューム構成の情報が格納されます。
- すべての共有クラスター ボリュームを一時的にバックアップ対象のノードに移動します。 こうすれば、すべての共有クラスター ボリュームに関する必要情報が収集されます。 この場合、一次ノードにできるのはこのノードだけです。

全ノードの P1S ファイルをマージするには、以下のように *Data_Protector_home*\bin\drim\bin から mmerge.cmd コマンドを実行します。

```
mmerge p1sA_path ... p1sX_path
```

ここで、p1sA は MSCS 内の最初のノードの P1S ファイルへのフル パスであり、p1sX は最後のノードの P1S ファイルへのフル パスです。 マージ後の P1S ファイルは元の P1S ファイルと同じディレクトリに保存され、ファイル名には .merged が追加されます (例: computer.company.com.merged)。 元のファイルの他のディレクトリに移動した後、マージ後の P1S ファイルの名前を元の名前に変更します (.merged 拡張子を削除する)。

UNIX Cell Manager のみ： mmerge.cmd コマンドは、Data Protector 自動ディザスタ リカバリ モジュールがインストールされた Windows システムでのみ動作します。 UNIX Cell Manager を使用している場合は、P1S ファイルを自動ディザスタ リカバリ モジュールがインストールされた Windows クライアントにコピーして、ファイルをマージします。 マージ後の P1S ファイルの名前を元の名前に変更し、Cell Manager にコピーします。

例

MSCS 用の P1S ファイルの 2 つのノードでのマージ例： mmerge *Data_Protector_home*\Config\server\dr\p1s\node1.company.com *Data_Protector_home*\Config\server\dr\p1s\node2.company.com. パス名に空白が含まれている場合には、Windows ではパス名を引用符で囲む必要があります。 マージ後のファイルは、node1.company.com.merged と node2.company.com.merged です。これらのファイルの名前を元の名前 (node1.company.com と node2.company.com) に戻します。この場合、最初に元の P1S ファイルの名前を変更する必要があります。

Windows でのハードディスク署名の復元

MSCS サービスは、すべてのハードディスクの MBR に書き込まれているハードディスク署名を使用しています。 共有クラスター ディスクを交換した場合、ディザスタ リカバリのフェーズ 1 でこのディスク署名が変わることになります。 その結果、クラスター サービスは交換されたディスクを有効なクラスター資源として認識せず、その資源に依存するクラスター グループは正常に動作しません。 最低 1 台のノードが稼動中でその資源を所有している限り、共有クラスター資源は運用可能であるため、これはアクティブなノードを復元する場合のみ当てはまります。 また、EADR/OBDR ではクリティカル ディスクの元のディスク署名が自動的に復旧されるため、この問題は EADR と OBDR のクリティカル ディスクには当てはまりません。 クリティカル ディスク以外のディスクを交換した場合は、そのハードディスク署名を復元する必要があります。

最も重要な共有ディスクはクラスターのクォーラム リソースです。 これを交換した場合は元のディスク署名を復元する必要があり、そうしないとクラスター サービスは開始しません。

フェーズ 2 において、MSDS データベースはシステム ボリュームの \TEMP\ClusterDatabase に復元されます。 フェーズ 1 でハードディスク署名が変わっているためクォーラム リソースが識別されず、システムを再起動してもクラスター サービスは実行されません。 これは、(*Data_Protector_home*\bin\utilns にある) clubar ユーティリティを実行することで解決できます。 これは元のハードディスク署名を復元するユーティリティです。 clubar が正常終了すると、クラスター サービスが自動的に開始されます。

例

コマンド プロンプトで clubar r c:\temp\ClusterDatabase force q: と入力し、c:\temp\ClusterDatabase から MSCS データベースを復元します。

clubar の使用法と構文の詳細は、*Data_Protector_home*\bin\utilns にある clubar.txt ファイルを参照してください。

Cell Manager 上の Data Protector 共有ディスクがクォーラム ディスクと異なる場合は、これも復元する必要があります。 Data Protector 共有ディスクと他のアプリケーション ディスクの署名を復元するには、Windows 2000 リソース キットに含まれている dumpcfg.exe ユーティリティを使用します。 dumpcfg.exe の使用法の詳細は、dumpcfg /? を実行するか、Windows 2000 リソース キットのマニュアルを参照してください。 Windows 2000 におけるハードディスク署名に関する問題については、MSDN Q280425 を参照してください。

元のハードディスク署名は SRD ファイルから取得できます。 SRD ファイル内の署名には、番号の後に volume というキーワードが付いています。

例

-volume 5666415943 -number 0 -letter C -offslow 32256 -offshigh 0 -lenlow 320430592 -lenhigh 2 -fttype 4 -ftgroup 0 -ftmember 0

-volume 3927615943 -number 0 -letter Q -offslow 320495104 -offshigh 2 -lenlow 1339236864 -lenhigh 0 -fttype 4 -ftgroup 0 -ftmember 0

-volume の後の数字がハードディスク署名です。 この例では、SRD ファイルにはローカル ハードディスク (ドライブ文字 C) とクォーラム ディスク (ドライブ文字 Q) に関する情報が保存されています。 クォーラム ディスクの署名は、バックアップ時にアクティブだったノードの SRD ファイルにだけ保存されています。 これは、アクティブなノードがクォーラム ディスクをロックしており、他のノードはクォーラム ディスクにアクセスできないためです。 したがって、常にクラスター全体のバックアップを取ることをお勧めします。 これは、フェーズ 1 で共有ディスク ボリュームのディスクを構成するのに十分な情報を得るにはすべての SRD ファイルを揃える必要があり、これにはクラスター内の全ノードの SRD ファイルが必要なためです。 SRD ファイルに保存されているハードディスク署名は 10 進数で表示されていることに注意してください。これに対して、dumpcfg コマンドでは 16 進数を指定する必要があります。

マジョリティ ノード セット クラスタでの自動システム復旧

マジョリティ ノード セット (MNS) クラスタで自動システム復旧 (ASR) を実行するには、次の手順を実行してください。

1. MNS クラスタを設定し、そのクラスタに Data Protector クライアントをインストールします。

   MNS クラスタに Cell Manager はインストールできないことに注意してください (サポートされていません)。

2. ファイルシステムのバックアップ、構成のバックアップ、IDB のバックアップを実行します。

3. ASR ディスク セットを作成します。

   ASR の準備方法、ASR セットを作成するための準備、ASR を使用する復旧の手順については、オンライン ヘルプの索引キーワード「自動システム復旧」で表示される内容を参照してください。

4. ノードでディザスタ リカバリを実行します。

   ディザスタ リカバリ準備方法など、詳細な手順については、オンライン ヘルプの索引キーワード「ディザスタ リカバリ」で表示される内容を参照してください。

ノードが復旧し、クラスタに参加できるようになります。

Data Protector Cell Manager 固有の復元手順

この項では、Windows Cell Manager の復元に必要な、特別な手順を説明します。

IDB の整合性をとる（すべての方法）

この項に記載の手順は、一般的なディザスタ リカバリ手順の実行後のみ使用します。

IDB の整合性をとるには、最新のバックアップがあるメディアをインポートして、バックアップされたオブジェクトの情報をデータベースにインポートします。 これを行うには以下の手順を実行してください。

1. 復元対象として残っているパーティションのバックアップが保存されたメディア（1 つ以上）を Data Protector GUI を使ってリサイクルして、IDB へメディアをインポートできるようにします。 詳細は、「メディアのリサイクル」を参照してください。 メディアが Data Protector によってロックされているためにリサイクルできない場合があります。 このような場合は、Data Protector プロセスを中止して、以下のコマンドを実行して \tmp ディレクトリを削除します。

   Data_Protector_home\bin\omnisv -stop

   del *Data_Protector_program_data*\tmp*.* (Windows Vista の場合)

   del *Data_Protector_home*\tmp*.* (その他の Windows システムの場合)

   Data_Protector_home\bin\omnisv -start

2. 復元対象として残っているパーティションのバックアップが保存されたメディア（1 つ以上）を Data Protector GUI を使ってエクスポートします。 この方法の詳細については、オンラインヘルプの索引「エクスポート、メディア」を参照してください。
3. 復元対象として残っているパーティションのバックアップが保存されたメディア（1 つ以上）を Data Protector GUI を使ってインポートします。 この方法の詳細については、オンラインヘルプの索引「インポート、メディア」を参照してください。

拡張自動ディザスタ リカバリに固有の手順

拡張自動ディザスタ リカバリを使用して、Windows Cell Manager を復元する場合には、フェーズ 0 で 2 つの特別な手順が必要です。

- Cell Manager 用のディザスタ リカバリ CD を事前に用意しておく必要があります。

重要：

ハードウェア、ソフトウェア、構成などに変更があった場合には、その都度バックアップを実行して新しい DR CD を作成します。 これは、IP アドレスや DNS サーバーの変更など、ネットワーク構成が変更された場合も同じです。

- ディザスタ リカバリの準備作業の一環として、Cell Manager の更新済みの SRD ファイルを、Cell Manager 以外の場所にも保存しておく必要があります。なぜなら、SRD ファイルは Data Protector で唯一、オブジェクトとメディアに関する情報が保存されているファイルだからです。 SRD ファイルを Cell Manager だけにしか保存していないと、Cell Manager に障害が発生した場合に利用できなくなります。「準備」 (40ページ) を参照。
- バックアップが暗号化されている場合は、障害が発生する前に暗号化キーをリムーバブル メディアに保存しておく必要があります。 暗号化キーを Cell Manager だけにしか保存していないと、Cell Manager に障害が発生した場合に利用できなくなります。 暗号化キーが使用できないと、ディザスタ リカバリは実行できなくなります。
「準備」 (40ページ) を参照してください。

重要：

バックアップ メディア、DR イメージ、SRD ファイル、暗号化キーの保存されたリムーバブル メディア、ディザスタ リカバリ CD へのアクセスを制限しておくことをお勧めします。

ワンボタン ディザスタ リカバリに固有の手順

Cell Manager がクラッシュした場合には IDB が使用できないため、OBDR のブート可能メディアの位置を知っている必要があります。

重要：

ハードウェア、ソフトウェア、構成などに変更があった場合には、その都度 OBDR バックアップを実行して新しいブート可能メディアを作成します。 これは、IP アドレスや DNS サーバーの変更など、ネットワーク構成が変更された場合も同じです。

バックアップが暗号化されている場合は、障害が発生する前に暗号化キーをリムーバブル メディアに保存しておく必要があります。 暗号化キーを Cell Manager だけにしか保存していないと、Cell Manager に障害が発生した場合に利用できなくなります。 暗号化キーが使用できないと、ディザスタ リカバリは実行できなくなります。

「準備」 (40ページ) を参照してください。

重要：

バックアップ メディアと暗号化キーが保存されたリムーバブル メディアへのアクセスを制限することをお勧めします。

自動システム復旧に固有の手順

自動システム復旧 (ASR) を使用して Windows Cell Manager を復旧する場合には、フェーズ 0 で別途手順が必要です。

- Cell Manager 用の ASR ディスクを事前に用意しておく必要があります。

重要：

ハードウェア、ソフトウェア、構成などに変更があった場合には、その都度バックアップを実行して ASR ディスクを更新します。 これは、IP アドレスや DNS サーバーの変更など、ネットワーク構成が変更された場合も同じです。

重要：

バックアップ メディアと ASR ディスクへのアクセスを制限することをお勧めします。

Internet Information Server (IIS) の復元に固有の手順

Internet Information Server (IIS) は、ディザスタ リカバリではサポートされていません。 IIS の半自動ディザスタ リカバリを行うには、(通常の半自動ディザスタ リカバリの手順に加えて) 以下の手順を実行してください。

1. システムのクリーン インストール中に IIS をインストールしないでください。
2. IIS Admin Service が実行されている場合は、それを停止またはアンインストールします。
3. drstart コマンドを実行します。
4. IIS データベースがプレーン ファイルとして、デフォルトの IIS ディレクトリ (*%SystemRoot%*\system32\inetsrv) に復元されます (ファイル名は DisasterRecovery)。
5. ブートが正常に終了したら、Data Protector 標準復元手順、または IIS バックアップ/復元スナップインを使用して、IIS データベースを復元します。この処理は長時間かかることに注意してください。

1. IIS に依存するサービス (SMTP、NNTP など) のいずれかが自動的に起動されない場合は、手動での起動を試みてください。
2. 手動でも起動できない場合は、IIS Admin Service を停止して、*%SystemRoot%*\system32\inetsrv\MetaBase.bin ファイルを overwrite オプションを使用して復元してください。

> **注記：**
>
> *%SystemRoot%*\system32\inetsrv は IIS サービスのデフォルトのディレクトリです。 IIS サービスを別のディレクトリにインストールした場合は、MetaBase.bin ファイルの復元先としてそのディレクトリを指定してください。

3. IIS Admin Service と、それに依存するサービスをすべて起動します。

kb.cfg ファイルの編集

ドライバの中には、正常に動作するために必要な機能が複数のファイルに分かれているものがあります。 それらが kb.cfg ファイルに逐次列挙されていなければ、Data Protector は DR イメージ ファイルの作成中にすべてのドライバ ファイルを特定できません。 この場合、それらのファイルはディザスタ リカバリ操作システムに含まれず、その結果、DR OS の起動後に一部のドライバやサービスが動作しなくなります。

kb.cfg ファイルは *Data_Protector_home*\bin\drim\config ディレクトリにあり、*%SystemRoot%* ディレクトリにあるドライバ ファイルの位置に関する情報を含んでいます。 テスト プランの実行時に、OS が起動した後、必要なサービスがすべて実行中で、必要なドライバがすべて動作することを確認してください。

これらのドライバをバックアップする場合は、依存ファイルに関する情報を kb.cfg ファイルに適切な形式で追加します。この形式についての指示は、kb.cfg ファイルの最初に記述されています。

このファイルを編集する最も簡単な方法は、既存の行をコピー、ペーストして適切な情報に書き換えることです。 パスの区切り文字が / (スラッシュ) であることに注意してください。 パス名が引用符で囲まれている場合以外、空白は無視されます。 したがって、エントリを複数行にまたがって記述することもできます。 また、# (シャープ) 記号で始まり行末で終わるコメント行も追加できます。

ファイルの編集が終了したら、元の場所に保存します。 次に、追加したファイルを DR イメージに含めるために、「準備」 (54ページ) の記述に従ってフル クライアント バックアップを再度実行します。

システムのハードウェアやアプリケーションの構成はさまざまであるため、すべての構成に対して「出来合い」の解決法を提供することはできません。 そのため、自らの責任でこのファイルを変更して、ドライバや他のファイルを含めてください。

このファイルへのあらゆる変更はユーザーの責任であり、Hewlett-Packard のサポート対象外となります。

⚠ 警告!

kb.cfg ファイルの編集後に復旧が正常動作するかを確認するため、テスト プランを作成して実行する必要があります。

編集後の SRD ファイルを使用した復旧

ディザスタ リカバリを実行する時点で、SRD ファイルに保存されているバックアップ デバイスまたはメディアに関する情報が古くなっている場合もあります。 オンライン復旧を実行する場合には、必要な情報が Cell Manager の IDB に保存されているため、これは問題となりません。 しかし、オフライン復旧を行う場合には、IDB の保存されている情報にアクセスできません。

たとえば、障害は、Cell Manager だけでなく、Cell Manager に接続されているバックアップ デバイスにも発生します。 障害発生後にバックアップ デバイスを別のバックアップ デバイスに交換した場合、更新されたSRDファイル (recovery.srd) に保存されているバックアップ デバイスに関する情報が正しくないため、復旧に失敗します。 この場合は、更新された SRD ファイルをディザスタ リカバリのフェーズ 2 を実行する前に編集して、復旧が正常終了するように不正な情報を更新します。

SRD ファイルを編集するには、テキスト エディタを使って SRD ファイルを開き、変更された情報を更新します。

ヒント：

デバイス構成に関する情報を表示するには、devbra -dev コマンドを使います。

たとえば、復旧しようとしているコンピュータのクライアント名が変更されている場合は、-host オプションの値を書き換えます。 以下に示す項目についても情報の修正が可能です。

- Cell Manager クライアント名 (-cm)
- Media Agent クライアント (-mahost)
- 論理デバイスまたはドライブ (ライブラリ) の名前 (-dev)
- デバイスの種類 (-devtype)
  -devtype オプションに指定可能な値については、sanconf マンページまたは『HP Data Protector command line interface reference』を参照してください。
- デバイスの SCSI アドレス (-devaddr)
- デバイスのポリシー (-devpolicy)
  ポリシーには、1 (スタンドアロン)、3 (スタッカー)、5 (ジュークボックス)、6 (外部制御)、8 (Grau DAS エクスチェンジャ ライブラリ)、9 (STK サイロ メディア ライブラリ)、10 (SCSI-II ライブラリ) のいずれかを定義します。

- ロボティクスの SCSI アドレス (-devioctl)
- ライブラリ スロット (-physloc)
- 論理ライブラリ名 (-storname)

ファイルを編集し終えたら、元の場所に Unicode 形式で保存してください。

例

MA クライアントの変更

old_mahost.company.com クライアントに接続されたバックアップ デバイスを使用して、ディザスタ リカバリ バックアップを実行した場合を考えてみましょう。 ディザスタ リカバリ時には、このバックアップ デバイスが new_mahost.company.com クライアントに同じ SCSI アドレスで接続されていたとします。 この場合、ディザスタ リカバリを適切に実行するには、ディザスタ リカバリのフェーズ 2 を開始する前に、(変更された) SRD ファイル内の -mahost old_mahost.company.com という文字列を -mahost new_mahost.company.com に変更する必要があります。

新しい MA クライアント上でバックアップ デバイスの SCSI アドレスが変更されている場合は、更新した SRD ファイル内の -devaddr オプションの値を適切に変更してください。

例

バックアップ デバイスと MA クライアントの変更

バックアップ時とは異なるデバイスを使用してディザスタ リカバリを実行するには (MA クライアントは同じものを使用)、更新された SRD ファイル内の次のオプションの値を変更します。 -dev, -devaddr, -devtype, -devpolicy, and -devioctl。 復元用にライブラリ デバイスを使用する場合は、SRD ファイル内の次のオプションの値も変更してください。 -physloc と -storname。

たとえば、ディザスタ リカバリの目的で、HP StorageWorks Ultrium スタンドアロン デバイスを使用してバックアップが実行した場合を考えてみましょう。 デバイス名は Ultrium_dagnja で、MA ホスト dagnja (Windows) に接続されています。 ただし、ディザスタ リカバリ時には、HP StorageWorks Ultrium ロボティクス ライブラリを使用するものとします。 このライブラリの論理ライブラリ名は Autoldr_kerala で、ドライブ Ultrium_kerala が MA クライアント kerala (Linux) に接続されています。

最初に kerala 上で devbra -dev コマンドを実行して、構成されているデバイスとその構成情報の一覧を確認しておきます。 この情報は、更新された SRD ファイル内の以下のオプション値を変更するために必要です。

-dev "Ultrium_dagnja" -devaddr Tape4:1:0:1C -devtype 13 -devpolicy 1 -mahost dagnja.company.com

これを次のように置き換えます。

-dev "Ultrium_kerala" -devaddr /dev/nst0 -devtype 13 -devpolicy 10 -devioctl /dev/sg1 -physloc " 2 -1" -storname "AutoLdr_kerala" -mahost kerala.company.com.

編集後の SRD ファイルをディザスタ リカバリに使用する手順は、それぞれのディザスタ リカバリの方法により異なります。 詳細は個々のディザスタ リカバリの方法に関する項を参照してください。

重要：

セキュリティ上の理由から、SRD ファイルへのアクセスは制限する必要があります。

AMDR/ASR

通常の AMDR/ASR 復旧手順を実行する前に、以下を実行します。

1. 最初の drsetup/ASR ディスクにある recovery.srd ファイルをテキスト エディタで開き、必要な変更を行います。
2. Unicode 形式で元の場所に保存します。

EADR/OBDR

通常の EADR/OBDR 復旧手順を実行する前に、以下を実行します。

1. 障害復旧ウィザードが表示されたら、カウントダウン中にいずれかのキーを押してウィザードを停止し、**[Install only]** オプションを選択して、**[完了]** をクリックします。 このオプションを選択すると、対象のシステムに一時オペレーティング システムのみがインストールされて、ディザスタ リカバリのフェーズ 1 を完了できます。 Install only を選択した場合、ディザスタ リカバリのフェーズ 2 が自動的には開始されません。

図 9 障害復旧ウィザードの Install only オプション

2. Windows タスク マネージャを実行します (**Alt+Ctrl+Del** キーを押し、**[タスク マネージャ]** を選択)。
3. **[ファイル]** をクリックし、**[新しいタスクの実行]** を選択します。 notepad c:\DRSYS\System32\OB2DR\bin\recovery.srdと入力して**Enter**キーを押します。 SRDファイルがメモ帳で開きます。
4. SRD ファイルを編集します。 編集方法の詳細は、『「システム復旧データ (SRD) の更新と編集」 (33ページ)』を参照してください。
5. SRD ファイルを編集して保存したら、c:\DRSYS\System32\OB2DR\bin ディレクトリから以下のコマンドを実行します。

   omnidr -drimini c:\$DRIM$.OB2\OBRecovery.ini
6. 通常の EADR/OBDR 復旧手順における次の手順に進みます。

CLI インターフェースを使用した ASR フロッピー ディスクの更新

Data Protector には ASR フロッピー ディスクを*自動的*に作成できる CLI コマンドはありません。 ただし、omnisrdupdate コマンドを使用すると、ASR セットの 1 枚目のフロッピー ディスクの内容を手動で更新できます。 ASR セットの 1 枚目のフロッピー ディスクをフロッピー ドライブに挿入し、次の例のように保存場所として a:\ を指定します。

omnisrdupdate -session 11/04/2005-1 -host computer1.com -location a:\ -asr

ASR フロッピー ディスクを*手動*で作成するには、さらに、*Data_Protector_home*\Depot\DRSetup\Disk*disk_number* フォルダから

DR*disk_number*.cab ファイルを適切な ASR フロッピー ディスクにコピーする必要があります。

Windows VistaのBitLocker ドライブ暗号化

BitLocker ドライブ暗号化を使用してボリュームが暗号化されている場合、ディザスタ リカバリ モジュールはそれを検出し、暗号化されたドライバのロックを解除するためのオプションを以下のプロンプトによって示します。

```
System storage inspection discovered n locked volume(s). Unlock? [y/n]
(システム ストレージの点検により n 個のロックされたボリュームが見つかりました。
ロックを解除しますか。 [y/n])
```

1. yを押してロック解除手順を開始します。
2. .2 ボタンを押して、選択メニューを開きます。
3. パスワードを含むボリューム (USBキーなど) が検索パスのリストに表示されているかどうか確認します。 以下のようなプロンプトが表示されます。

   ```
   Search dir(s): [a:\]
   [d:\]
   ```

   パスが表示されない場合:

   a. search と入力します。 新しいメニューが表示されます。
   b. 検索ディレクトリ (たとえばUSBキーがm:\にマウントされている場合はm:) を入力します。. 一度に複数のディレクトリを追加できます。.

      ディレクトリが検索パスに表示されます。

      ```
      Search dir(s): [a:\]
      [d:\]
      [m:\]
      ```

4. ロックを解除するボリュームを入力します (c:など)。 ドライブ文字を使用せず、ボリュームの GUID (\\?\Volume{*GUID*}など) でボリュームを指定したり、複数のボリュームを一度に指定することができます。

   全ボリュームのロックを解除するには、all と入力します。

   キー ファイルが USB キーやフロッピーから取得できない場合は、以下のプロンプトが表示されます。

   ```
   Type one of the following:
   * External key path
   * Numerical password (groups separated by hyphens)
   * Exit
   ```

   (以下のいずれかを入力します。* 外部のキーのパス * 数値のパスワード (グループをハイフンで区切る) * 終了)

   数値のパスワードを入力します。

4 UNIX のディザスタ リカバリ

HP-UX クライアントの手動によるディザスタ リカバリ

この項では、HP-UX クライアントのディザスタ リカバリの手順を説明します。

この手順は Ignite-UX 製品をベースにしています。これは主に HP-UX システムのインストールと構成作業用に開発されたアプリケーションで、(システム管理用の強力なインターフェースに加え) システム障害に対する準備と復旧のための機能を備えています。

Ignite-UX はターゲット クライアントのディザスタ リカバリに特化しているため (フェーズ 1 およびフェーズ 3)、ディザスタ リカバリのフェーズ 3 でユーザー データとアプリケーション データを復元するには Data Protector を使用する必要があります。

注記：

この項では、Ignite-UX の全機能を網羅しているわけではありません。 より詳細な情報については、『Ignite-UX 管理ガイド』を参照してください。

概要

Ignite-UX で、障害に対する準備と障害の復旧を行うには 2 つの方法があります。

- カスタム インストール メディアを使用する (ゴールド イメージ)
- システム復旧ツールを使用する (**make_tape_recovery**、**make_net_recovery**)

ゴールド イメージを使用する方法は、ハードウェア構成と OS リリースが基本的に同じシステムが多い IT 環境に適しています。一方、システム復旧ツールを使用する方法は、お使いの個々のシステムに合わせた復旧アーカイブの作成をサポートしています。

どちらの方法でも、DDS テープや CD などのブート可能インストール メディアの作成が可能です。これらのメディアを使用して、システム管理者は障害が発生したクライアントのシステム コンソールから直接、ローカルにディザスタ リカバリを行うことができます。 さらに、どちらの方法でも、故障したクライアントに適切なゴールド イメージまたは事前に作成した“復旧アーカイブ”を割り当てることにより、クライアントのネットワークを利用して復旧を実行できます。 この場合、クライアントは Ignite サーバーから直接ブートし、割り当てられたデポからインストールを実行します。このデポはネットワークの NFS 共有にある必要があります。

サポートされている場合は、Ignite-UX GUI を使用してください。

カスタム インストール メディアの使用

概要

大規模な IT 環境では、それを構成する多くのシステムが同じハードウェアやソフトウェアをベースにしている場合が多いものです。 あるインストール済みのシステムの完全なスナップショットを他のシステムのインストールに使用すれば、OS やアプリケーションのインストールやパッチ適用の手間が大幅に軽減されます。 Ignite-UX には、ゴールド イメージなどを別のシステムに割り当てる前に、ネットワークやファイルシステムの設定パラメータを変更したり、Data Protector などのソフトウェアをイメージに追加したりする機能（Ignite-UX の make_config コマンド）があります。 そこで、この機能を使用してシステムのディザスタ リカバリを行うことができます。

カスタム インストール メディアの使用手順の概要は、以下のとおりです。

1. **フェーズ0**
   a. クライアント システムのゴールド イメージを作成します。
2. **フェーズ 1 および 2**
   a. 問題のあるディスクを交換ディスクと交換します。
   b. HP-UX クライアントを Ignite-UX サーバーからブートし、ネットワークを構成します。
   c. ゴールド イメージを Ignite-UX サーバーからインストールします。
3. **フェーズ3**
   a. ユーザー データおよびアプリケーション データを復元する場合は、Data Protector 標準復元手順を使用します。

準備

以下に、ターゲット クライアント システムのゴールド イメージの作成手順を示します。クライアント システムは、ゴールド イメージをネットワークの NFS を介して共有します。 この例では、Data Protector クライアントはすでにクライアント システムにインストールされており、特別な構成手順を行わなくても“ゴールド イメージ”に含まれることになります。

1. /opt/ignite/data/scripts/make_sys_image ファイルを、Ignite-UX サーバからクライアント システム上の一時ディレクトリにコピーします。
2. クライアント ノード上で make_sys_image -ddirectory of the archive-n*name of the archive*.gz -s *IP address of the target system*コマンドを実行して、クライアントの圧縮イメージを他のシステム（ ターゲット システム）上に作成します。

   このコマンドにより、GZIP で圧縮されたファイル デポが -d オプションと -s オプションで指定したシステムの指定ディレクトリに作成されます。 HP-UX クライアントが、ターゲット システムへのパスワードなしのアクセス権を与えられていることを確認してください（ターゲット システムの .rhosts ファイルにクライアント システムのエントリがあること）。アクセス権がないと、コマンドは失敗します。

3. ターゲット ディレクトリをターゲット システムの /etc/exports ディレクトリに追加し、このディレクトリをターゲット サーバーにエクスポートします (exportfs -av)。
4. Ignite-UX サーバーの構成で、アーカイブ テンプレート ファイル core.cfg を archive_*name*.cfg にコピーします。 cp /opt/ignite/data/examples/core.cfg /var/opt/ignite/data/*OS_Release*/archive_*name*.cfg

例

cp /opt/ignite/data/examples/core.cfg /var/opt/ignite/data/Rel_B.11.11/archive_HPUX11_11_DP50_CL.cfg

5. コピーした構成ファイルの以下のパラメータを確認して変更します。
   - sw_source セクション:

     load_order = 0
     source_format = archive
     source_type="NET"
     # change_media=FALSE
     post_load_script = "/opt/ignite/data/scripts/os_arch_post_l"
     post_config_script =
     "/opt/ignite/data/scripts/os_arch_post_c"
     nfs_source = "*IP Target System*:*Full Path*"
   - 対応する OS archive セクション:

     archive_path = "*archive_name*.gz
6. archive_impact コマンドをイメージ ファイルに対して実行して impacts エントリの値を決定し、出力を以下の構成ファイルの同じ OS archive セクションにコピーします。

   /opt/ignite/lbin/archive_impact -t -g *archive_name*.gz

例

/opt/ignite/lbin/archive_impact -t -g
/image/archive_HPUX11_11_DP50_CL.gz
impacts = "/" 506Kb
impacts = "/.root" 32Kb
impacts = "/dev" 12Kb
impacts = "/etc" 26275Kb
impacts = "/opt" 827022Kb
impacts = "/sbin" 35124Kb
impacts = "/stand" 1116Kb
impacts = "/tcadm" 1Kb
impacts = "/usr" 729579Kb
impacts = "/var" 254639Kb

7. Ignite-UX に新しく作成したデポを認識させるには、cfg エントリを /var/opt/ignite/INDEX ファイルに以下のレイアウトで追加します。

   cfg "*This_configuration_name*" { description "*Description of this configuration*" "/opt/ignite/data/OS/config" "/var/opt/ignite/data/*OS*/archive_*name*.cfg }

例

```
cfg "HPUX11_11_DP50_Client" {
description "HPUX 11.i OS incl Patches and DP50 Client"
"/opt/ignite/data/Rel_B.11.11/config"
"/var/opt/ignite/data/Rel_B.11.11/archive_HPUX11_11_DP50_CL.cfg
"
}
```

8. ブートするクライアント用に予約してある 1 つ以上の IP アドレスが、/etc/opt/ignite/instl_boottab ファイルで構成されていることを確認してください。 IPアドレスの数は、並行ブートクライアントの数と同じになります。

上記の手順を完了すると、HP-UX クライアントのゴールド イメージ（固有のハードウェアおよびソフトウェア構成を含む）が作成されます。このイメージは、同様の構成のシステムを復旧するために使用することができます。

ハードウェアおよびソフトウェア構成が異なるシステムすべてに対して、ゴールド イメージの作成手順を繰り返します。

注記：

Ignite-UX を使用して、作成したゴールド イメージからブート可能なテープや CD を作成することができます。 詳しくは、『Ignite-UX 管理ガイド』を参照してください。 Ignite-UX を使用して、作成したゴールド イメージからブート可能なテープや CD を作成することができます。 詳しくは、『Ignite-UX 管理ガイド』を参照してください。

Recovery

ネットワークの NFS 共有上にあるゴールド イメージを適用して HP-UX クライアントを復旧するには、以下の手順を実行してください。

1. *クライアント システムでの手順*
   a. 障害が発生したハードウェアを交換します。
   b. Ignite-UXサーバーからHP-UXクライアントをブートします。 boot lan.*IP-address Ignite-UX server*install.
   c. [Welcome to Ignite-UX] 画面が表示されたら、**[Install HP-UX]** を選択します。

d. [UI Option] 画面で **[Remote graphical interface running on the Ignite-UX server]** を選択します。
e. ネットワーク構成ダイアログ ボックスに応答します。
f. 以上で、Ignite-UX サーバーによるリモート制御インストールに対するクライアント システムの準備は完了です。

2. *Ignite-UX サーバーでの作業*
a. Ignite-UX GUI の **[client]** アイコンを右クリックし、**[Install Client]** → **[New Install]** を選択します。
b. インストールするゴールド イメージを選択し、設定（ネットワーク、ファイルシステム、タイムゾーンなど）をチェックして、**[Go!]** ボタンをクリックします。
c. **[client]** アイコンを右クリックして **[Client Status...]** を選択すると、インストールの進行状況が確認できます。
d. インストールが完了したら、Data Protector標準復元手順でユーザー データとアプリケーション データの復元を行います。

システム復旧ツールの使用

概要

Ignite-UX にバンドルされているシステム復旧ツールにより、ディスク障害の復旧を迅速かつ容易に行うことができます。 デフォルトでシステム復旧ツールの復旧アーカイブに含まれるのは、HP-UXの運用に不可欠なディレクトリのみです。 しかし、復旧をより迅速に行うために、他のファイルやディレクトリ（追加のボリューム グループもしくは Data Protector のファイルおよびディレクトリなど）をアーカイブに含めることも可能です。

make_tape_recovery は、ブート可能な復旧（インストール）テープを作成するツールです。この復旧テープはご利用のシステムにカスタマイズされており、バックアップ デバイスをターゲット システムに直接接続して、ターゲット システムをこのブート可能な復旧テープからブートすることで、無人のディザスタ リカバリが可能となります。アーカイブ作成時とクライアント復旧時は、バックアップデバイスをクライアントにローカル接続しておく必要があります。

make_net_recovery は、ネットワーク上の Ignite-UX サーバーまたは他の指定システム上に、復旧アーカイブを作成するツールです。 ターゲット システムは、Ignite-UX の make_boot_tape コマンドで作成したブート可能なテープからブートするか、または Ignite-UX サーバ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。

システム復旧ツールの使用手順の概要は、以下のとおりです。

1. **フェーズ0**
a. Ignite-UX サーバー上の Ignite-UX GUI を使用して、HP-UX クライアントの復旧アーカイブを作成します。

2. **フェーズ 1 および 2**
   a. 問題のあるディスクを交換ディスクと交換します。
   b. ローカル復元の場合は、準備した復旧用テープからブートします。
   c. ローカル復元の場合は、復元プロセスが自動的に開始されます。
      ネットワーク復元の場合は、Ignite-UX クライアントからブートし、ネットワークと UI を構成します。
      ネットワーク復元の場合は、ゴールド イメージを Ignite-UX サーバーからインストールします。
3. **フェーズ3**
   a. ユーザー データおよびアプリケーション データを復元する場合は、Data Protector 標準復元手順を使用します。

準備

HP-UX 用の復旧アーカイブを作成する最も簡単な方法は、Ignite-UX サーバー上で Ignite-UX GUI を使用することです。 GUI コマンドはすべて、コマンド行からも実行できます。 詳しくは、『Ignite-UX 管理ガイド』を参照してください。

前提

システム障害に対する準備を行う前に、Ignite-UX ファイルセットをクライアントにインストールして、Ignite-UX サーバーとクライアントが通信できるようにする必要があります。 Ignite-UX のバージョンが、Ignite-UX サーバーとクライアントで同じになるようにします。 Ignite-UXファイルセットの整合性を確保するには、Ignite-UXサーバー上のデポからIgnite-UXをインストールするのが最も簡単な方法になります。 このデポを構築するには、Ignite-UX サーバーで以下のコマンドを実行します。

```
pkg_rec_depot -f
```

これにより、Ignite-UX のデポが /var/opt/ignite/depots/recovery_cmds ディレクトリに作成されます。クライアントで swinstall コマンドにより Ignite-UX をインストールする際に、このディレクトリをソース ディレクトリとして指定します。

クライアントに Ignite-UX をインストールしたら、Ignite-UX サーバーの GUI で、make_net_recovery または make_tape_recovery を使用して復旧アーカイブを作成します。

make_tape_recovery を使用したアーカイブの作成

make_tape_recovery を使用してアーカイブを作成するには、以下の手順を実行します。

1. HP-UXクライアントにバックアップデバイスが接続されていることを確認します。
2. 以下のコマンドを実行して、Ignite-UX GUIを起動します。 /opt/ignite/bin/ignite &
3. **[client]** アイコンを右クリックして、**[Create Tape Recovery Archive]** を選択します。

4. HP-UX クライアントに複数のデバイスが接続されている場合には、テープ デバイスを選択します。
5. アーカイブに含めたいボリュームグループを選択します。
6. テープ作成プロセスが開始されます。 [client] アイコンを右クリック後 [Client Status] を選択して、ステータスと Ignite-UX サーバー上のログ ファイルを確認します。

注記：

Ignite-UX では、すべての DDS がどの DDS ドライブでも確実に使用できるように、90m の DDS1 バックアップ テープの使用を推奨しています。

make_net_recovery を使用したアーカイブの作成

make_net_recovery を使用した復旧アーカイブの作成手順は、make_tape_recovery の場合とほとんど同じです。 この方法の利点は、復旧アーカイブがデフォルトで Ignite-UX サーバー上に保存されるため、ローカルに接続するデバイスが不要である点です。

1. 以下のコマンドを実行して、Ignite-UX GUIを起動します。 /opt/ignite/bin/ignite &
2. [client] アイコンを右クリックして、[Create Network Recovery Archive] を選択します。
3. 保存先のシステムとディレクトリを選択します。 圧縮されたアーカイブが保存できるだけの容量があることを確認してください。
4. アーカイブに含めたいボリュームグループを選択します。
5. アーカイブ作成プロセスが開始されます。 [client] アイコンを右クリック後 [Client Status] を選択して、ステータスと Ignite-UX サーバー上のログ ファイルを確認します。

注記：

Ignite-UX では、ブート可能なアーカイブ テープを圧縮アーカイブ ファイルから作成することができます。 『Ignite-UX 管理ガイド』の「ネットワーク経由でのリカバリ アーカイブの作成」を参照してください。

Recovery

バックアップ テープからの復旧

make_tape_recovery で作成したブート可能なテープを使用してシステムのディザスタ リカバリを行うには、以下の手順で行います。

1. 障害が発生したハードウェアを交換します。
2. クラッシュしたHP-UXクライアントにテープデバイスがローカルに接続されていることを確認した上で、復元するアーカイブが書き込まれているメディアを挿入します。
3. 用意した復旧テープからブートします。 そのためには、boot admin メニューで「SEARCH」と入力して、使用可能なすべてのブート デバイスのリストを出力します。 どのデバイスがテープ ドライブか特定し、次のように boot コマンドを入力します。boot *hardware path* または boot Pnumber
4. 復旧プロセスが自動的に開始されます。
5. インストールが正常に完了したら、Data Protector 標準復元手順でユーザー データとアプリケーション データの復元を行います。

ネットワークからの復旧

HP-UX クライアントのディザスタ リカバリをネットワーク経由で行うには、ゴールドイメージによる復旧手順に従います。 インストールしたいアーカイブが選択されていることを確認します。

- **クライアントでの手順**
  1. 障害が発生したハードウェアを交換します。
  2. Ignite-UXサーバーからHP-UXクライアントをブートします。
     boot lan.*IP-address Ignite-UX server*install
  3. [Welcome to Ignite-UX] 画面で **[Install HP-UX]** を選択します。
  4. [UI Option] 画面で **[Remote graphical interface running on the Ignite-UX server]** を選択します。
  5. ネットワーク構成ダイアログ ボックスに応答します。
  6. 以上で、Ignite-UX サーバーからのリモート制御インストールに対するクライアント システムの準備は完了です。
- **Ignite-UX サーバーでの作業**
  1. Ignite-UX GUI の **[client]** アイコンを右クリックし、**[Install Client]** → **[New Install]** を選択します。
  2. [Configurations] で、インストールする **[Recovery Archive]** を選択して設定（ネットワーク、ファイルシステム、タイムゾーンなど）を確認し、**[Go!]** ボタンをクリックします。
  3. **[client]** アイコンを右クリックして **[Client Status...]** を選択すると、インストールの進行状況が確認できます。

4. インストールが正常に完了したら、Data Protector 標準復元手順でユーザー データとアプリケーション データの復元を行います。

UNIX クライアントのディスク デリバリーによるディザスタ リカバリ

UNIX クライアントのディスク デリバリーによるディザスタ リカバリを実行するには、最低限の OS と Data Protector Disk Agent が含まれているブート可能なディスクを、クラッシュしたシステムに接続します。 管理者は、ディスクのフォーマットおよびパーティションの構成が正しく行われるよう、障害発生前に十分なデータを収集する必要があります。

サポート対象のオペレーティング システムは、『HP Data Protector product announcements ソフトウェアノートおよびリファレンス』を参照してください。

概要

UNIX クライアントのディスク デリバリーでは、持ち運び可能な補助ディスクを使用します。この補助ディスクには、最小限のオペレーティング システムとネットワークおよび Data Protector エージェントをインストールしておきます。

UNIX クライアントに対して補助ディスクを使用する手順の概要は、以下のとおりです。

1. **フェーズ0**
   a. フル クライアント バックアップおよび IDB バックアップ（Cell Manager のみ）を実行します。
   b. 補助ディスクを作成します。
2. **フェーズ1**
   a. 問題のあるディスクを交換し、 補助ディスクをターゲット システムに接続した後、補助ディスクにインストールされている最小限のオペレーティング システムでシステムをブートします。
   b. 交換したディスクに手動でパーティションを作成して、記憶データ構造を再確立し、交換ディスクをブート可能にします。
3. **フェーズ2**
   a. Data Protector 標準復元手順でオリジナル システムのブート ディスクを交換ディスクに復元します（Restore into オプションを使用します）。
   b. システムをシャットダウンして、補助ディスクを取り外します。 なお、ホットスワップが可能なハードディスク ドライブを使用している場合は、システムをシャットダウンする必要はありません。
   c. システムを再起動します。
4. **フェーズ3**
   a. ユーザー データおよびアプリケーション データを復元する場合は、Data Protector 標準復元手順を使用します。

制限事項

- ここでは、クラスター環境の復旧については説明しません。 クラスター環境の構成によっては、特別な手順や環境の変更が必要です。
- RAID はサポートされていません。
- ターゲット システムと同じハードウェア クラスのシステム上に、補助ディスクを用意する必要があります。

準備

このディザスタ リカバリの準備は、バックアップ仕様に関する情報の収集、ディスクの準備、バックアップ仕様の準備（実行前）、バックアップの実行など、数段階に分けて実行する必要があります。 クライアントのディザスタ リカバリを実行する前に、これらの準備手順をすべて行うことが必要です。

この項では、復旧作業を正しく実行するため、バックアップ時に各ターゲット システムに対して実行する必要のある項目を示します。 これらの情報を実行前コマンドの一部として収集する場合は、これらのファイルのあるディレクトリをディザスタ リカバリ プランに明記して、障害発生時にこの情報を見つけやすくしておくことが必要です。 また、バージョン管理（バックアップごとの「補助情報」を集めたもの）についても考慮が必要です。

- バックアップ対象のシステムがアプリケーション プロセスを低実行レベルで実行している場合は、復旧後のエラーを避けるため、*最小限の動作*状態（修正 *init 1 実行レベル*）を確立して、シングル ユーザー モードに入ることが必要です「整合性と関連性を兼ね備えたバックアップ」 (32ページ) を参照してください。 詳細については、ご使用のオペレーティングシステムのマニュアルを参照してください。
  HP-UXの場合：

例

1. 抹消リンクを /sbin/rc1.d から /sbin/rc0.d に移動して、ブート セクションに対する変更内容を補足します。 抹消リンクには基本サービスが含まれており、上記の作業を行わなかった場合、実行レベル 1 に移行することによってこのサービスは中断されます。このサービスはバックアップに必要です。 例として、「抹消リンクの移動 (HP-UX 11.x)」 (131ページ) を参照してください。
2. システムで rpcd を構成します（ファイル /etc/rc.config.d/dce で変数 RPCD=1 を構成します）。

   これにより、システムが最小限の動作状態で実行する準備ができました。 この状態の特徴を以下に示します。

   - Init-1 の実行レベル (ファイルシステム：マウント済み、ホスト名：設定済み、日付および時刻：設定済み、syncer：実行中)
   - ネットワークが稼動している必要があります。
   - inetd、rpcd、swagentd の各プロセスも実行されます。

Solaris:

例

1. rpc 抹消リンクを /etc/rc1.d から /etc/rc0.d に移動して、ブート セクションに対する変更内容を補足します。 抹消リンクには基本サービスが含まれており、上記の作業を行わなかった場合、実行レベル 1 に移行することによってこのサービスは中断されます。このサービスはバックアップに必要です。
2. rpcbind がシステム上で構成されていることを確認します。

   これにより、システムが最小限の動作状態で実行する準備ができました。 この状態の特徴を以下に示します。

   - Init 1
   - ネットワークが稼動している必要があります。
   - inetd、rpcbind の各プロセスも実行されます。

Tru64:

例

1. システムの電源が落とされている場合は、システムをブートし、System Reference Manual (SRM)コンソール(ファームウェアコンソール)を起動します。
2. SRMコンソールから下記のコマンドを実行して、シングルユーザーモードに切り替えます。

   - boot -fl s で、生成済みの vmunix ファイルを使用して起動します。
   - boot -fi genvmunix -fl s で、一般的なカーネルを使用するシングル ユーザー モードに入ります。
3. システムの電源が既に投入されており、システムが既に稼動している場合は、init s コマンドを実行して現在の実行レベルからシングル ユーザー モードに切り替えます。

AIX:
操作は必要ありません。補助ディスクの作成に使用する alt_disk_install コマンドにより、システムの動作状態を最小限にしなくてもディスク イメージの整合性が保証されるためです。

- 補助ディスクを使用してディザスタ リカバリを行う場合は、補助ブート ディスクを準備する必要があります。 1 つのサイトとプラットフォームにつき、ブート可能な補助ディスクが 1 台だけ必要です。 このディスクには、オペレーティング システムとネットワーク構成が含まれており、ブート可能であることが必要です。
- 以下を実行する実行前スクリプトを作成します。
  - 保管場所の物理的および論理的保存構造
  - 現在の論理ボリュームの構造 (HP-UX の場合、vgcfgbackup と vgdisplay -v を使用)
  - MC/ServiceGuard の構成データ、ディスク ミラーリング、ストライピング

- ファイルシステムとマウント ポイントの概要 (HP-UX の場合、bdf、または /etc/fstab のコピーを使用)
- システムのページング スペース情報 (HP-UX の場合、 swapinfo コマンドの出力を使用)
- I/O 構造の概要 (HP-UX の場合、ioscan -fun と ioscan -fkn を使用)
- クライアントのネットワーク設定

環境に関して必要なすべての情報を収集して、収集した情報をディザスタ リカバリ時に使用可能な場所に保存するスクリプト。 このスクリプトは、容易にアクセスできる別のシステムに保存することをお勧めします。収集する情報を以下に示します。

- データの非常用コピーもバックアップに保存できます。 ただし、これを実行した場合は、実際の復旧を行う前にこの情報を取り出しておく必要があります。
- システムからすべてのユーザーをログアウトさせます。
- アプリケーション データを個別にバックアップする場合でない限り、データベースのオンライン バックアップなどを使ってすべてのアプリケーションを停止します。
- システムへのネットワーク アクセスを制限します。これにより、バックアップの実行中はシステムへのログオンが禁止されます (HP-UX の場合、inetd.sec を上書きして、inetd -c を使用する)。
- 必要に応じて、システムの動作状態を最小限にします (たとえば、HP-UX 上では、sbin/init 1 を使用し、60 秒待ち、run_level が 1 になっているかどうかをチェックします)。 これは、修正された “init 1" 状態であることに注意してください。

- システムの実行レベルを標準にする実行後スクリプトを実行して、アプリケーションの再起動などを行います。
- Data Protector Cell Manager 上のクライアントに対するバックアップ仕様を設定します。 バックアップ仕様には、すべてのディスクを指定し (ディスク ディスカバリを使用)、実行前/実行後スクリプトを指定することが必要です。
- バックアップ手順を実行します。この手順は、定期的に繰り返し実行するか、または少なくともシステム構成に主要な変更があった場合、特に論理ボリューム構造に何らかの変更があった場合 (HP-UX では、LVM) に実行します。

Recovery

この項では、バックアップ実行時の状態にシステムを復元する方法を説明します。 ディスク デリバリーによるディザスタ リカバリを正しく実行するには、以下が必要です。

- クラッシュしたディスクと交換するための新しいハードディスク。
- 適切なオペレーティング システムと Data Protector エージェントを含む補助ディスク
- 復旧対象のクライアントの正常なフル バックアップ

以下のステップを実行します。

1. 問題のあるディスクを新しいディスク（同等サイズ）と交換します。
2. 補助ディスク（適切なオペレーティング システムと Data Protector クライアントが含まれているディスク）をシステムに接続して、これをブート デバイスにします。
3. 補助のオペレーティングシステムからブートします。
4. 必要に応じて、論理ボリューム構造を再構築します（HP-UX の場合は、LVM）。ルート以外のボリューム グループについては、保存されているデータを使用します（HP-UX の場合は、vgcfgrestore または SAM を使用）。
5. さらに、復元対象のルート ボリューム グループを修復済みディスク上に作成します（HP-UX の場合は、vgimport を使用）。 このボリューム グループは、復元プロセス中はルート ボリューム グループとはみなされません。 これは、補助ディスクから OS を実行しているためです。 vgimport の詳細は、同コマンドの man ページを参照してください。
6. 新しいディスクをブート可能にします。
7. バックアップ時に二次記憶デバイスに保存したデータから、他のデータ記憶構造（ミラー、ストライピング、MC/ServiceGuard など）を再構築します。
8. バックアップ データからの要求に従って、ファイルシステムを作成してマウントします。 マウントポイントの名前には、元の名前そのものではなく、それに類似した名前を使用してください。たとえば、元の名前が/etcであれば、/etc_restore のようにします。
9. マウント ポイントにある復元対象のファイルをすべて削除して、マウント ポイントを空の状態にします。
10. Data Protector GUI を起動して、Cell Manager との接続を開始します。 補助ディスクを使って、システムをセルにインポートします。
11. 復元するバージョンを選択します。 まず復元に必要なメディアをすべてリストして、それらが使用可能であることを確認します。 **[Restore As** *新しいマウント ポイント名*] オプションを使って、（今後）システムに対してルート ボリュームとなるボリュームを含む必要なマウント ポイントをすべて復元します。 バックアップのルート ボリュームは修復ディスク上のルート ボリュームに復元されます。 補助ディスク上の現在実行中の補助オペレーティングシステムに対して、何らかの復元が行われることはありません。
12. 復元したシステムをシャットダウンします。
13. 補助ディスクをシステムから取り外します。
14. システムを新しい（または修復された）ディスクからリブートします。

注記：

補助ディスクの代わりに、新しいディスクを、Disk Agent がインストールされているクライアント システムに一時的に接続することもできます。 復元後、新しいディスクを障害が発生したシステムに接続し、ブートします。

UNIX Cell Manager の手動によるディザスタ リカバリ

手動によるディザスタ リカバリは、基本的なディザスタ リカバリの方法です。この方法には、最初にインストールした時と同様の方法でシステムを再インストールして復旧する他に、 Data Protector を使ってオペレーティング システムを含むすべてのファイルを復元する方法があります。

概要

UNIX Cell Manager のディザスタ リカバリを手動で実行する手順の概要は、以下のとおりです。

1. **フェーズ0**
   a. フル クライアント バックアップおよび IDB バックアップを実行します。
   b. DR OS をインストールならびに構成できるようにするため、オリジナル システムに関する情報を収集します。
2. **フェーズ 1:**
   a. 障害が発生したハードウェアを交換します。
   b. 手動でディスク上にパーティションを再作成し、オリジナルの記憶データ構造を再確立します。
   c. オペレーティングシステムを再インストールします。
   d. パッチを再インストールします。
3. **フェーズ2**
   a. Data Protector Cell Manager を再インストールします。
   b. その他のファイルをメディアから復元する作業を簡単にするため、IDB の最新のバックアップを復元します。
   c. Data Protector 構成情報 (/etc/opt/omni) をバックアップに含まれている最新の Data Protector 構成情報で置き換え、以前の構成を再作成します。
4. **フェーズ3**
   a. ユーザーおよびアプリケーション データを復元するには、Data Protector 標準復元手順を使用します。
   b. システムを再起動します。

制限事項

サポート対象のオペレーティング システムは、『HP Data Protector product announcements ソフトウェアノートおよびリファレンス』を参照してください。

ここでは、クラスター環境の復旧については説明しません。 クラスター環境の構成によっては、特別な手順や環境の変更が必要です。

準備

HP-UX または Solaris クライアントの手動によるディザスタ リカバリに対する準備と同じ手順を行います（ただし補助ディスクに関する手順を除く）。 詳しくは、「準備」（108ページ）を参照してください。 上記の手順とは別に、以下の手順も実行することが必要です。

1. IDB の通常バックアップを行います。このとき、別のバックアップ仕様を使って、Cell Manager 自体のバックアップ完了後にバックアップが実行されるようスケジュール設定することをお勧めします。
2. Cell Manager システム上の指定したデバイスに IDB と構成のバックアップを行います。これにより、管理者はそのデバイス内のメディアに IDB の最新バージョンが含まれていることが分かります。

Recovery

以下の手順に従って、UNIX Cell Manager を復元します。

前提

ディスク デリバリーによるディザスタ リカバリを正しく実行するには、以下が必要です。

- Cell Manager と IDB のルート パーティションの最新の有効なバックアップが含まれているメディア
- Cell Manager システムに接続されたデバイス

以下の手順に従って、Cell Manager の復旧を実行します。

1. クラッシュしたディスクを交換します。
2. お使いのオペレーティング システムのインストール用メディアからシステムをブートします。
3. オペレーティングシステムを再インストールします。 インストール方法については、お使いのシステムの管理者用マニュアルを参照してください。 インストール時に、復旧準備手順（実行前スクリプト）で収集したデータを使って、保管場所の物理的および論理的保存構造、論理ボリューム構造、ファイルシステムとマウント ポイント、ネットワーク設定などを再作成して構成します。
4. Cell Manager に Data Protector を再インストールします。

5. データベースの最新バックアップと /etc/opt/omni を一時ディレクトリに復元します。 これにより、メディアから他のすべてのファイルを容易に復元できます。

注記：

ただし、データベースを直接復元することはできません。 手順の詳細は、オンライン ヘルプを参照してください。 /opt/omni/sbin/omnisv -stop コマンドを使用してすべての Data Protector プロセスを終了します。 これにより、使用中のファイルがない状態になります。

6. /etc/opt/omni ディレクトリを削除して、一時ディレクトリの /etc/opt/omni と置き換えます。 これにより、前回の構成が再び作成されます。
7. /opt/omni/sbin/omnisv -start コマンドを使って Data Protector プロセスを起動します。
8. Data Protector ユーザー インターフェースを起動して、すべてのファイルをバックアップから復元します。
9. システムを再起動します。

以上で、Cell Manager が正しく復旧されます。

5 ディザスタ リカバリのトラブルシューティング

この章の内容

この章では、ディザスタ リカバリの実行中に発生する可能性がある問題について説明します。 問題の発生時には、まず、ある特定のディザスタ リカバリの方法に関連する問題かどうかを検討した後、ディザスタ リカバリ全般の問題かどうかを検討してください。 エラーメッセージの確認方法については、「autodr.log ファイル」 (115 ページ) を参照してください。

Data Protector の一般的なトラブルシューティング情報については、『HP Data Protector トラブルシューティングガイド』を参照してください。

作業を開始する前に

- 最新の Data Protector パッチがインストールされていることを確認します。確認する方法は、オンライン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。
- Data Protector の全般的な制限事項、既知の問題、および回避方法については、『HP Data Protector product announcements ソフトウェアノートおよびリファレンス』を参照してください。
- サポートされているバージョン、プラットフォーム、およびその他の情報の最新リストについては、 http://www.hp.com/support/manuals を参照してください。

一般的なトラブルシューティング

autodr.log ファイル

autodr.log は *Data_Protector_home*\tmp ディレクトリにあるログ ファイルで、自動ディザスタ リカバリ (EADR、OBDR、ASR) に関するメッセージが含まれています。 エラーが発生した場合は、このファイルを点検してください。 Autodr.logには、主に開発およびサポート用のさまざまなメッセージが記録されます。 実際に関係があり、エラーが発生したことを示しているメッセージは、そのうちの一部だけです。 そうしたエラーメッセージは通常、トレースバックとともにログ ファイルの最後に記録されています。

autodr.log に記録されるメッセージには 4 つのタイプ/レベルがあります（これらのタイプ/レベルは、Data Protector GUI のバックアップ セッションの最後に報告されるメッセージの報告レベルとは対応していないことに注意してください）。

- 致命的エラー：深刻なエラーで、オブジェクトのバックアップは続行不可能であり、中止されます。
- エラー：致命的である可能性もありますが、いくつかの要因に依存します。たとえば、autodr.log に、あるドライバがディザスタ リカバリ オペレーティング システムに含まれていないことが記録されていたとします。 そのドライバがないことで、復旧後のシステムが動作しない場合もありますが、OS のブート後に重要でないサービスが実行されないだけの場合もあります。 これは、どのドライバがバックアップされていなかったかに依存します。
- 警告および情報：これらはエラー メッセージではなく、通常は何らかの障害を意味するものではありません。

autodr.log ファイルに記録される最も一般的なメッセージには、次のようなものがあります。

- unsupported location：Data Protector は、ディザスタ リカバリ オペレーティング システム（DR OS）に含まれる予定のサービスやドライバに必要なファイルが、*%SystemRoot%* ディレクトリにないことを通知します。
  こうしたドライバは多くの場合、アンチウィルス ソフトウェアやリモート コントロール ソフトウェア（pcAnywhere など）で使用されます。 必要なファイルが不足しているサービスやドライバがブート後に動作しない可能性があるため、このメッセージは重要です。 ディザスタ リカバリが正常終了するか失敗するかは、影響を受けるサービスやドライバに左右されます。 この問題に対して考えられる解決方法は、不足しているファイルを *%SystemRoot%* ディレクトリにコピーし、Windows レジストリ内のそのパスを変更することです。 Windows レジストリを不正に編集すると、システムが深刻なダメージを受ける可能性があることに注意してください。

ディザスタ リカバリ セッションのデバッグ

Data Protector に対して、ディザスタ リカバリ セッションの際にデバッグ ログを作成し、保存するよう指定できます。 このオプションはEADRおよびOBDRでのみ使用可能です。

デバッグを設定するには：

1. [Disaster recovery] ウィザードの [Debugs] ボタンの左側にあるチェック マークを選択します。

図 10 ディザスタ リカバリ セッション中のデバッグを有効にします。

2. デバッグを保存する場所などのデバッグ オプションを指定するには、**[Debugs]** をクリックします。 デフォルトでは、 *%System32%*\ob2dr\tmp にデバッグが保存されます。

注記：

Windows Vistaシステムの場合、リストア セッションによる大量のデバッグの発生が予想されるときは、デバッグを保存する場所を指定する必要があります。 Windows Vista の RAM ディスクで使用可能な容量は大幅に制限されており (通常 32MB 未満)、この制限を超えると Data Protector が予期しない動作を起こす可能性があります。

3. [Debug Options] ウィンドウが表示されます。

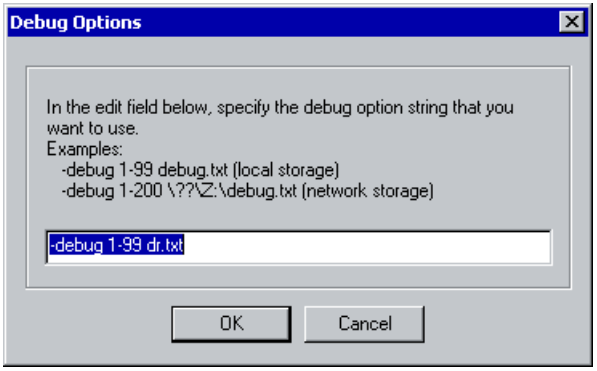


図 11 デバッグ ログの保存場所の変更

デバッグ ログを保存する場所を入力します。 ドライブ文字の前に \\? を付ける必要があります。たとえば、\\?\Z:\debug.txt のようになります。

デバッグをネットワーク上の共有領域に保存する場合は、 net use コマンドを使用して、デバッグ ログを書き込む共有領域をマウントします。 例：

NET USE X: "*client**debug_output_folder* /*user*:*username password*"

Windows 上でのディザスタ リカバリ中の omnirc オプションの設定

omnirc オプションに関する一般情報は、『HP Data Protector トラブルシューティング ガイド』を参照してください。

Windows 上でのディザスタ リカバリ中に omnirc オプションを設定する必要がある場合は (ディスク デリバリーによるディザスタ リカバリ時を除く)、以下の手順を実行してください。

1. [ディザスタ リカバリ ウィザード] が表示されたら、カウントダウン中に任意のキーを押してウィザードを停止します。

図 12 ディザスタ リカバリ ウィザード

2. **[Cmd]** をクリックして、コマンド プロンプトを開始します。
3. コマンド

   echo *variable* > *%systemroot%*\system32\OB2DR\omnirc

   variable には、omnirc ファイルに書き込む omnirc オプションを正確に指定します。

   たとえば、次のように入力してください。

   echo OB2RECONNECT_RETRY=1000 > *%systemroot%*\system32\OB2DR\omnirc

   このコマンド例では、ディザスタ リカバリ オペレーティング システム内に omnirc ファイルを作成し、OB2RECONNECT_RETRY 変数に値 1000 秒を設定しています。
4. コマンド プロンプトを閉じ、[ディザスタ リカバリ ウィザード] 内の **[次へ]** をクリックして、ディザスタ リカバリを続行します。

drm.cfg ファイル

Data Protector のディザスタ リカバリの構成は、広範なシステム構成を対象とするよう設定されています。 しかし、場合によっては、これらの設定が最適ではないことや、システム上の問題をトラブルシューティングするために設定の一部を変更しなければならないことがあります。

drm.cfg ファイルには、変更が可能で、ディザスタ リカバリの処理に影響を与えるパラメータが、その影響の説明と一緒に記述されています。 drm.cfg ファイルはEADRおよびOBDRでのみ使用可能です。

これらの変数を変更するには、以下の手順に従ってください。

1. 一時ファイルの drm.cfg.tmpl を drm.cfg にコピーします。

   この一時ファイルは、インストールやアップグレードの際に *Data_Protector_home*\bin\drim\config に作成されます。変数はすべてデフォルト値に設定されています。

2. drm.cfg ファイルを編集します。 変数に対して適切な値を設定します。 ファイルの指示に従ってください。

全般的な問題

問題

ディザスタ リカバリ終了後のシステムへのログオン時の問題

システム復旧後、以下のエラー メッセージが表示される場合があります。

The system cannot log you on to this domain, because the system's computer account in its primary domain is missing or the password on that account is incorrect.
(このドメインにログオンできません。
プライマリ ドメイン内にシステムのコンピュータ アカウントがないか、
このアカウントに対するパスワードが不適切なためです。)

この種類のメッセージは、通常以下のいずれかの理由により表示されます。

- ディザスタ リカバリ プロセス (フル バックアップを含む) を正常に実行するためのすべての情報を収集した後、Windows を再インストールして、要求を満たしていないドメインにシステムを (再度) 追加した。
- ディザスタ リカバリ プロセス (フル バックアップを含む) を正常に実行するためのすべての情報を収集した後、要求を満たしていないドメインからシステムを削除して、同じドメインまたはその他のドメインにシステムを (再度) 追加した。

対策

このような場合、Windows は、ディザスタ リカバリ時に復元される情報とは互換性のない新しいシステム保護情報を生成します。 この場合の解決方法を以下に示します。

1. 管理者アカウントを使って、ローカルでシステムにログオンします。
2. [コントロール パネル] ウィンドウで **[ネットワーク]** をクリックし、[識別] タブを使って、このシステムを現在のドメインから一時的なワークグループ (TEMP など) に移します。 この後、システムを削除したドメインにこのシステムを再度追加します。 この作業には、ドメイン管理者用パスワードが必要です。
3. コンピュータを再び適切なドメインに入れた後、[ネットワーク] ウィンドウで **[OK]** をクリックします。 この時点で Windows システムの再起動が必要となります。
4. ディザスタ リカバリ プロセスを使ってこの新しい状態を更新するには、もう一度必要な手順 (システム データの収集、バックアップ) をすべて実行することが必要です。 詳しくは、「ディザスタ リカバリの準備」の項を参照してください。

問題

コピーからのディザスタ リカバリ

メディアコピーまたはオブジェクトコピーからディザスタリカバリを実行できない。

Data Protector はデフォルトで、オリジナル メディア セットを使用してディザスタ リカバリを行います。 したがって、Data Protector GUI のディザスタ リカバリ ウィザードにはコピー オブジェクトのバージョンは表示されません。

対策

オリジナル メディア セットが使用できないまたは損傷した場合に、メディア コピーまたはオブジェクト コピーからディザスタ リカバリを実行するには、以下の手順を実行します。

- オブジェクトコピー： オリジナル メディア セット内のすべてのメディアを IDB からエクスポートした後、SRD ファイルを再生成します。その後、Data Protector のディザスタ リカバリ ウィザードでは、最初に使用可能なオリジナル メディア セットのコピーが表示されます。
  詳細は、オンライン ヘルプの索引キーワード「メディア, エクスポート」および「システム復旧データ (SRD) の更新と編集」 (33ページ) で表示される内容を参照してください。
- メディアコピー： SRD ファイル内のオリジナル メディアのメディア ID をメディア コピーのメディア ID に書き換えます。その後、 Data Protector のディザスタ リカバリ ウィザードでは、最初に使用可能なオリジナル メディア セットのコピーが表示されます。
  詳細は、「システム復旧データ (SRD) の更新と編集」 (33ページ) を参照してください。

問題

自動ディザスタ リカバリの各方法 (EADR、OBDR、ASR) でデータを収集する際に、構成のバックアップが失敗します。

フル クライアント バックアップを実行しているときは、特定のバックアップ方法に必要なデータの収集中に構成のバックアップが失敗する場合があります。これは、そのバックアップ方法がディザスタ リカバリ以外に使用されている場合でも発生します。デフォルトでは、Data Protector がすべての自動ディザスタ リカバリ方法のデータを収集するからです。 たとえば、ブートディスクがLDM ディスクの場合は、Data Protector が EADR のデータを収集する際にこれが発生します。

対策

失敗したディザスタ リカバリ方法でのデータの自動収集を使用不可にします。 これにより、Data Protector は必要なデータを他の方法で収集します。

変数 OB2_TURNOFF_COLLECTING を以下のいずれかの値に設定します。

0	デフォルト設定、すべての自動方法 (EADR, OBDR, ASR) でのデータ収集がオンになります。
1	EADR/OBDR データの収集をオフにします。 ASR データは収集されます。
2	ASR データの収集をオフにします。 EADR/OBDR データは収集されます。
3	すべての方法での収集をオフにします。

「Windows 上でのディザスタ リカバリ中の omnirc オプションの設定」 (118ページ) を参照してください。

半自動ディザスタ リカバリ

問題

Drstartレポート：“*filename*をコピーできません。”

このエラーは、drstart ユーティリティが指定されたファイルをコピーできなかった場合に出力されます。 1 つの原因として、ファイルがシステムによってロックされていたことが考えられます。 たとえば、drstart が omniinet.exe をコピーできない場合は、おそらく Inet サービスがすでに実行中であると思われます。 これは通常では考えられない状況で、クリーン インストールの後では起きないはずです。

対策

残りのファイルのコピーを続けるかを確認するダイアログ ボックスが表示されます。 [はい] をクリックすると、drstart はロックされたファイルをスキップして他のファイルのコピーを続行します。 ファイルがシステムによりロックされている場合には、ディザスタ リカバリに必要なプロセスがすでに実行中でありそのファイルはコピーする必要がないため、これで問題は解決されます。

[中止] ボタンをクリックして drstart ユーティリティをクローズすることもできます。

ディスク デリバリーによるディザスタ リカバリ

問題

Cannot find physical location of drives selected for disk delivery (ディスクのデリバリー用に選択されたドライブの物理的位置が見つかりません。)

ディスク デリバリーによるディザスタ リカバリを行う場合、以下のエラーが表示される可能性があります。

Cannot find physical location of drives selected for disk delivery（ディスクのデリバリー用に選択されたドライブの物理的位置が見つかりません。）

オブジェクトを復元するには、新しいディスク上にパーティションを作成する際、これまでに使用されていないドライブ文字を選択しておく方法もあります。 さらに優れた解決策を以下に示します。

対策

ディザスタ リカバリ プロセスは、オブジェクトの復元前にディスク情報をチェックします。 内部関数は、ディスク アドミニストレータによって作成されたレジストリ値 Information を読み取ります。 ディスク アドミニストレータを何度か起動すると、Information は破損し（更新中にフォーマットが変更されるため）、このような場合、解析プログラムは正常に動作しません。 このとき、HKEY_LOCAL_MACHINE\SYSTEM\DISK Information キーを削除してディスク アドミニストレータを再起動すると、この関数は正常に動作します。

問題

オペレーティング･システムが見つからない

ディザスタ リカバリ実行後、Windowsシステムの最終ブート時に、「No Operating System Found（オペレーティング システムが見つかりません。）」というメッセージが表示されます。

対策

boot.ini ファイルにパーティション情報の位置に関する情報があるかどうかを確認してください。 詳細は、「システム復旧データ（SRD）の更新と編集」（33ページ）の項の手順 4 を参照してください。

問題

Media Agent クライアントのディスク デリバリーによるディザスタ リカバリ

ディスク デリバリーによるディザスタ リカバリを実行する場合、Data Protector はまず、バックアップ デバイスが接続されていた元のクライアント（Media Agent クライアント）に接続し、同じデバイスを使って復元を実行しようとします。 ただし、バックアップを実行した Media Agent クライアントがクラッシュし、そのクライアントに対してディスク デリバリーによるディザスタ リカバリを実行した場合、Data Protector はこのクライアントに接続できず、オフラインによる復元を実行して、復元用のローカル デバイスを検索します。 ローカル デバイスが接続されていない場合は、その旨とディザスタ リカバリの中止を通知するメッセージが表示されます。

対策

これを回避する方法には以下の 2 通りがあります。

- メディアを別のメディア プールに移動します。 これにより、メディアを新しいデバイスに割り当てることができます。 その後、ディスク デリバリーによるディザスタ リカバリを続行します。
- 2 番目の方法では、障害発生前の準備段階の作業が必要です。 セル内に Media Agent クライアントが 2 つある場合、障害発生前に第一の Media Agent クライアントを第二の Media Agent クライアント（およびその逆）にバックアップして、Media Agent クライアントのディスク デリバリーによるディザスタ リカバリ実行時の問題を回避することができます。

拡張自動ディザスタ リカバリとワンボタン ディザスタ リカバリ

問題

自動ディザスタ リカバリ情報が収集できない

EADEまたはOBDRを実行中に、次のエラーが出力される場合があります。

自動ディザスタリカバリ情報が収集できません。 システム復旧情報の収集を中止しています

対策

- すべての記憶デバイスが正しく構成されているかどうか、確認してください。デバイス マネージャがデバイスを“不明なデバイス”と表示している場合は、EADR または OBDR を実行する前に、正しいデバイス ドライバをインストールする必要があります。
- 使用可能なレジストリ スペースが十分にある必要があります。 レジストリの最大サイズを、少なくとも現在のレジストリ サイズの 2 倍に設定することをお勧めします。 使用可能なレジストリ スペースが十分にない場合、autodr.log に次と同様のエントリが記録されます。
  ERROR registry 'Exception while saving registry'
  ...

この問題が継続する場合は、Data Protector 自動ディザスタ リカバリ モジュールをアンインストールして（手動およびディスク デリバリーによるディザスタ リカバリは可能）、当社サポート担当に連絡してください。

問題

致命的でないエラーが検出された

EADEまたはOBDRを実行中に、次のエラーが出力される場合があります。

自動ディザスタ リカバリ データの収集中に重要でないエラーが検出されました。 自動ディザスタ リカバリ ログ ファイルを確認してください。

自動ディザスタ リカバリ モジュール実行中に致命的でないエラーが検出された場合は、そのバックアップがまだディザスタ リカバリに使用できる可能性が高いことを示

します。 致命的でないエラーの原因は autodr.log に記録されています（ディレクトリは *Data_Protector_home*\tmp）。

対策

- *%SystemRoot%* フォルダにないサービスやドライバ（ウィルス スキャナなど）が検出されました。 Autodr.log には、次と同様のエラー メッセージが記録されます。

  ERROR safeboot 'unsupported location' 'intercheck support 06' 2 u'\\??\\D:\\Program Files\\Sophos SWEEP for NT\\icntst06.sys'.
  これはディザスタリカバリの成否に影響する問題ではないので、このエラーメッセージは無視してかまいません。

問題

復元中にネットワークが使用できなくなった

対策

スイッチ、ケーブルなどに問題がないか確認します。他に考えられるのは DNS サーバー（バックアップ時の構成と同じ）が復元時にオフラインになっていることです。 DR OS の構成はバックアップ時と同じであるため、ネットワークが使用できません。 この場合はオフライン復元を行い、復旧後に DNS の設定を変更します。 またフェーズ 2 の開始前にレジストリ (HKey_Local_Machine\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters) を変更することもできます。 この場合は変更を有効にするために、フェーズ 2 実行前に再起動が必要です。 フェーズ 2 完了後、フェーズ 3 を開始する前に設定を修正します。

△ **注意：**
レジストリを不適切に編集すると、ディザスタリカバリが失敗する原因になります。

問題

自動ログオンが正常動作しない

対策

自動ログオンが正常に動作せず、DRM$ADMIN アカウントを使って手動でログオンしなくてはならない場合があります。

問題

コンピュータが応答しなくなった

対策

CD/テープが読み込み可能か確認します。 CD-RW/テープを何回も再使用してはいけません。

問題

Microsoft Cluster ServerのEADR用のCD ISOイメージを作成できない

対策

CD ISO イメージを作成できるようにするためには、クォーラム ディスクのバックアップを行う必要があります。

問題

kms_allow_hosts ファイルが Cell Manager 上にない場合、AES 暗号化 OBDR 用または EADR 用のバックアップのための ISO イメージの作成に失敗する Cell Manager

ISO イメージがクライアント システムで作成された場合に、kms_allow_hosts ファイルがないか、または ISO イメージが準備されている EADR または OBDR クライアントの完全修飾名がファイルに含まれていません。

ISOイメージが Cell Manager で作成された場合は、この問題は発生しません。

対策

1. *Data_Protector_home*\config\server\cell\kms_allow_hosts ファイルがない場合、作成して、クライアントの名前をファイルに追加します。
2. Data Protector サービスを再起動します。

問題

フェーズ 1 でボリュームが再マウントされない

システムによっては (ディスク コントローラとその構成による)、別のボリュームのマウント ポイントに対応づけられたボリューム (ドライブ文字の割り当てなし) が、ディザスタ リカバリのフェーズ 1 で正しく再マウントされない場合があります。 この現象は、マウント ポイントが含まれるボリュームが再作成または再フォーマットされた場合に発生します (たとえば、MiniOS を搭載したシステム ボリュームなど)。この結果、オペレーティング システムが「セーフ モード」で起動して、元のマウント ポイントのターゲット ボリュームにあるファイル システムの検出が行われなくなります。そのため、ディザスタ リカバリのモジュールでこのボリュームを認識できなくなり、drecovery.ini ファイルに MISSING として報告されます。 このようなボリュームは認識されないだけで、内容は無傷です。

対策

- ドライブ文字を付けてボリュームをマウントし、chkdsk /v /f コマンドを実行して検証するか、システムで復旧が完了するまで待機した後に元のマウント ポイントを再作成します。
- システムを MiniOS に直接手動で再起動します (リカバリ CD から再起動しないようにします)。 以前にアンマウントされたボリュームが、ドライブ文字に対して自動的にマウントされます。

問題

Windows Vista で、ネットワーク ドライバがないために、ネットワークが使用できない

搭載されているネットワーク カードがDR OS でサポートされていないため、ディザスタ リカバリの際にネットワークが使用できなくなっています。

対策

見つからないドライバを DR OS イメージに挿入してください。「DR CD ISO イメージの作成」 (58ページ) (EADRの場合) または「OBDR バックアップ」 (68ページ) (OBDRの場合) を参照してください。

問題

ISO イメージの作成に失敗して、"Unsupported version of drecovery.ini" のメッセージが表示される

Windows Server 2003 または Windows XP で開始されたGUIからWindows 2000 Server のクライアントのイメージを作成する際に、旧バージョンの Data Protector クライアントで作成されたバックアップを選択すると以下のエラーが表示されます。

Unsupported version of drecovery.ini file. The drecovery.ini file of your client is created with old version of Disaster Recovery Module and is not supported by the Disaster Recovery Module on this client. Go to the client that has the old version of Disaster Recovery Module and create ISO image for your client there. (サポートされていないバージョンの drecovery.ini ファイルです。お使いのクライアントの drecovery.ini ファイルは古いバージョンのディザスタ リカバリ モジュールで作成されたので、このクライアントのディザスタ リカバリ モジュールではサポートされません。古いバージョンのディザスタ リカバリ モジュールのあるクライアントを使用して、そこから ISO イメージを作成してください。)

Data Protector のバージョン A.05.10、A.05.50、A.06.00 (パッチDPWIN_00270 不使用) からアップグレードしていない場合、ディザスタ リカバリ イメージは Windows 2000 システムで開始したGUIからしか作成できません。これは、旧バージョンのディザスタ リカバリが Windows 2000 システムにしかないためです。 アップグレード後は、任意のクライアントの GUI を使用して任意のクライアントのイメージを作成できます。

対策

このクライアントの ISO イメージを作成するには、古いバージョンのディザスタ リカバリ モジュールのあるクライアントを使用してください。

可能であれば、Windows 2000 のクライアントを新バージョンにアップグレードしてください。

Intel Itanium 固有の問題

問題

ディザスタ リカバリの失敗または中断後に、起動記述子が EFI に残る

Intel Itanium システムでは、ディザスタ リカバリ セッションの失敗または中断後に起動記述子 (DRM Temporary OS) が EFI 環境に残ります。 これにより、ディザスタ リカバリ プロセスを再起動した場合に、意図しない動作が発生する場合があります。

対策

範囲選択メニューから **[Remove Boot Descriptor]** オプションを使用して起動記述子を削除します。 起動記述子を削除した後に、範囲を選択することによってディザスタ リカバリを続行できます。

問題

Intel Itanium システムで間違ったブート ディスクが選択されるか、またはブート ディスクが選択されない

Intel Itanium システムで、間違ったブート ディスクが選択されます（またはブート ディスクが全く選択されません）。

対策

1. 範囲選択メニューから **[Manual Disk Selection]** を選択します。 使用可能なディスクのリストが新しいメニューに表示されます。
2. 正しいブート ディスクを指定します。 **o** を押すと元のディスクに関する情報が表示され、**d** を押すと選択したディスクに関する情報が表示されます。
3. カーソル キーを使用してリストからディスクを選択し、**b** を押します。 **c** を押すと選択が解除されます。

   ブート ディスクがシステムディスクと同じでない場合は（通常2つのディスクは同じ）、システム ディスクも選択する必要があります。

   [Back] を選択します。
4. 復旧範囲を選択すると、ディザスタ リカバリが続行されます。

自動システム復旧

問題

ASR 中のネットワーク障害

ASR 中にはネットワーク障害が原因となって、さまざまな問題が発生する可能性があります。

たとえば、ターゲット システムに2つのネットワーク アダプタがインストールされており、片方が無効化された状態でディザスタ リカバリ バックアップが実行されたとします。 しかし、ASR 中には、すべてのデバイスがデフォルトで有効化されます。 ASR 中に両方のネットワーク アダプタがターゲット システム上で有効になっていると、ネットワークを正しく構成できないことがあり、その結果、Cell Manager および Media Agent クライアントへの接続に問題が生じる可能性があります。 この場合、Data Protector はオフライン復旧またはローカル復旧に切り替わり、接続エラーが出力されます。あるいは、ASR が失敗します。

対策

この問題を解決するには、通常の ASR 復旧手順を実施します。次のメッセージがディザスタ リカバリ ウィザードに表示されたら **F8** を押します。

ネットワーク構成をスキップするには、この後5秒以内にF8を押します。

これにより、Data Protector ASR ネットワーク構成が、標準の Microsoft ASR ネットワーク構成に戻されます。

問題

ネットワーク カード ドライバが見つからない場合、ASRが中止される

この問題は、新しいモデルのマシン上で ASR を実行している場合に発生します。 このようなマシンの場合、Windows インストール CD には適切なネットワーク アダプタのドライバが見つからないためです。 ネットワーク アダプタが正しくインストールされていないため、omnidr で静的 IP アドレスを使用する設定を試みても、失敗します。

[重要]元のネットワーク(TCP/IP)構成を再作成できませんでした。 ネットワークアダプタが、正しく取り付けられ動作していることを確認してください。

対策

- 適切なネットワーク ドライバをインストールしてから、omnidr を起動します。
  または、可能であれば、必要なネットワーク ドライバが含まれた最新（後続）バージョンの Windows インストール CD を使用します。
  ディザスタ リカバリを開始する前にネットワーク ドライバをインストールするには、[ハードウェアの追加] ウィザードを使用します。このウィザードは以下のコマンドで起動できます。

%SystemRoot%\System32\rundll32.exe shell32.dll,Control_RunDLL hdwwiz.cpl

- デフォルトの ASR (DHCP) のネットワーク インストールも使用できます。通常のASR手順を行い、ディザスタ リカバリ ウィザードに次のテキストが表示されたら、**F8**を押します。 ネットワーク構成をスキップするには、この後5秒以内にF8を押します。
  これにより、Data Protector ASR ネットワーク構成が、標準の Microsoft ASR ネットワーク構成に戻されます。

A 詳細情報

抹消リンクの移動 (HP-UX 11.x)

リンクを移動するには、バックアップ対象のシステム上で以下の手順を行います。

```
# The system will go from "run-level" 4 to "run-level 1"
# retaining the inetd, networking, swagentd services up.
#The state is called "minimum activity" for backup
#purposes (need networking).
# IMPORTANT: ensure the links are present in /sbin/rc1.d before
# moving and they do have this exact name. You have to
#rename them for the rc0.d directory. Put them BELOW the
#lowest (original "/sbin/rc0.dKxx") "K...-link" in rc0.d
# Move K430dce K500inetd K660net K900swagentd into ../rc0.d BELOW
#the lowest kill link!!!
echo "may needto be modified for this system"
exit 1
#
cd /sbin/rc1.d
mv K430dce../rc0.d/K109dce
mv K500inetd../rc0.d/K110inetd
mv K660net../rc0.d/K116net
mv K900swagentd ../rc0.d/K120swagentd
```

Windows での手動によるディザスタ リカバリ準備用テンプレート

次ページに示すテンプレートは、第3章 (39ページ) で説明している Windowsでの半自動ディザスタ リカバリに備えてお使いください。

クライアント プロパティ	コンピュータ名	
	ホスト名	
ドライバ		
Windows Service Pack		
TCP/IP のプロパティ	IPアドレス	
	デフォルトゲートウェイ	
	サブネット マスク	
	DNS の順序	
メディア ラベル / バーコード番号		
パーティション情報と順序	最初のディスクラベル	
	第 1 パーティションの長さ	
	第 1 ドライブの文字	
	第 1 ファイルシステム	
	2番目のディスクラベル	
	第 2 パーティションの長さ	
	第 2 ドライブの文字	
	第 2 ファイルシステム	
	3番目のディスクラベル	
	第 3 パーティションの長さ	
	第 3 ドライブの文字	
	第 3 ファイルシステム	

用語集

ACSLS

(StorageTek固有の用語) Automated Cartridge System Library Server の略語。 ACS (Automated Cartridge System: 自動カートリッジ システム) を管理するソフトウェア。

Active Directory

(Windows固有の用語) Windowsネットワークで使用されるディレクトリ サービス。ネットワーク上のリソースに関する情報を格納し、ユーザーやアプリケーションからアクセスできるように維持します。このディレクトリ サービスでは、サービスが実際に稼動している物理システムの違いに関係なく、リソースに対する名前や説明の付加、検索、アクセス、および管理を一貫した方法で実行できます。

AES 256ビット暗号化

Data Protectorソフトウェアの暗号化方式で、256ビット長のランダムなキーを使用するAES-CTR (Advanced Encryption Standard in Counter Mode)の暗号化アルゴリズムを基盤にしています。暗号化にも復号化にも同じキーを使用します。データはネットワークを介して転送される前およびメディアに書き込まれる前に、AES 256ビット暗号化方式によって暗号化されます。

AML

*(EMASS/GRAU固有の用語)*Automated Mixed-Media library (自動混合メディア ライブラリ) の略。

ASRセット

フロッピー ディスク上に保存されたファイルのコレクション。交換用ディスクの適切な再構成(ディスク パーティション化と論理ボリュームの構成)およびフル クライアント バックアップでバックアップされた元のシステム構成とユーザー データの自動復旧に必要となります。これらのファイルは、バックアップ メディア上に保存されると共に、Cell Manager上の*Data_Protector_home*\Config\Server\dr\asr ディレクトリ (Windows用Cell Managerの場合) または /etc/opt/omni/server/dr/asr/ディレクトリ (UNIX用Cell Managerの場合) に保存されます。ASRアーカイブ ファイルは、障害発生後に複数のフロッピー ディスクに展開されます。32ビット版のWindows XP/.NETでは3枚のフロッピー ディスクに展開され、64ビット版のWindows XP/.NETの場合は4枚のフロッピー ディスクに展開されます。これらのフロッピー ディスクは、ASRの実行時に必要となります。

Automatic Storage Management

(Oracle固有の用語) 自動ストレージ管理は、Oracle 10g/11gによって統合された、Oracleデータベース ファイルを管理するファイルシステムおよびボリュームのマネージャ機能です。データとディスクの管理の複雑さを解消するとともに、ストライプ化とミラー化によってパフォーマンスの最適化も行います。

BACKINT

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

BC

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

BC

(HP StorageWorks Disk Array XP固有の用語) Business Copy XPの略。 BCを使うと、HP StorageWorks Disk Array XP LDEVの内部コピーをデータ バックアップやデータ複製などの目的で維持できます。これらのコピー（セカンダリ ボリュームまたはS-VOL）は、プライマリ ボリューム（P-VOL）から分離して、バックアップや開発などの用途に応じた別のシステムに接続することができます。バックアップ目的の場合、P-VOLをアプリケーション システムに接続し、S-VOLミラー セットのいずれかをバックアップ システムに接続する必要があります。
「HP StorageWorks Disk Array XP LDEV 、CA 、Main Control Unit 、アプリケーション システム 、およびバックアップ システム 。」を参照。

BC EVA

(HP StorageWorks EVA固有の用語) Business Copy EVAは、ローカル複製ソフトウェア ソリューションです。EVAファームウェアのスナップショット機能とクローン機能を使用して、ソース ボリュームのポイントインタイム コピー(複製)を作成できます。
「複製 、ソース ボリューム 、スナップショット 、およびCA+BC EVA 。」を参照。

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 。」を参照。

BC VA

(HP StorageWorks Virtual Array固有の用語) Business Copy VAを使用すると、同じ仮想アレイ内で、データ バックアップ用またはデータ複製用のHP StorageWorks Virtual Array LUNの内部コピーを管理することができます。コピー(子またはBusiness Copy LUN)は、バックアップやデータ解析、開発など様々な目的に使用できます。バックアップ目的で使用されるときは、元(親)のLUNはアプリケーション システムに接続され、Business Copy(子) LUNはバックアップ システムに接続されます。
「HP StorageWorks Virtual Array LUN 、アプリケーション システム 、およびバックアップ システム 」を参照。

BCV

*(EMC Symmetrix固有の用語)*Business Continuance Volumesの略。 BCVデバイスはICDA内であらかじめ構成された専用のSLDです。 ビジネスの継続運用を可能にするために使用されます。BCVデバイスには、これらのデバイスによりミラー化されるSLDのアドレスとは異なる、個別のSCSIアドレスが割り当てられます。BCVデバイスは、保護を必要とする一次EMC Symmetrix SLDの分割可能なミラーとして使用されます。
「BC およびBC Process 」を参照。

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 ファイルをアーカイブできます。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 。」を参照。

BRBACKUP

(SAP R/3固有の用語) SAP R/3 バックアップ ツールの1つ。制御ファイル、個々のデータ ファイル、またはすべてのテーブルスペースをオンラインでもオフラインでもバックアップできます。 また、必要に応じて、オンラインREDOログ ファイルをバックアップすることもできます。
「BRARCHIVE 、および BRRESTORE 。」を参照。

BRRESTORE

(SAP R/3固有の用語) SAP R/3のツール。以下の種類のファイルを復元するために使います。

- BRBACKUPで保存されたデータベース データ ファイル、制御ファイル、オンラインREDOログ ファイル
- BRARCHIVEでアーカイブされたREDOログ ファイル
- BRBACKUPで保存された非データベース ファイル

ファイル、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 。」を参照。

BSM

Data Protector Backup Session Managerの略。バックアップ セッションを制御します。このプロセスは、常にCell Manager システム上で稼動します。

CA

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

CA+BC EVA

(HP StorageWorks EVA固有の用語) Continuous Access (CA) EVAとBusiness Copy (BC) EVAを併用すると、リモートEVA上にソース ボリュームのコピー(複製)を作成して保持でき、その後、これらのコピーをそのリモート アレイ上でローカル複製のソースとして使用できます。
「BC EVA 、複製 、およびソース ボリューム 」を参照。

CAP

(StorageTek固有の用語) Cartridge Access Portの略。ライブラリのドア パネルに組み込まれたポートです。メディアの出し入れに使用されます。

CDB カタログ データベース (Catalog Database) の略。

カタログ データベース (Catalog Database) の略。CDBは、IDBのうち、バックアップ、オブジェクト コピー、復元、メディア管理セッションおよびバックアップしたデータに関する情報を格納する部分。選択したロギング レベルによっては、ファイル名とファイル バージョンも格納されます。CDBは、常にセルに対してローカルとなります。
「MMDB 」を参照。

CDFファイル

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

Change Journal

(Windows固有の用語) 各変更のレコードがローカルNTFSボリューム上のファイルおよびディレクトリに発生するたびに、それが記録されるWindowsのファイル システムの機能。

Change Log Provider

(Windows固有の用語) 作成、変更、または削除されたファイル システム上のオブジェクトを特定するために問い合わせることができるモジュール。

Cluster Continuous Replication

(Microsoft Exchange Server固有の用語) Cluster continuous replication (CCR)は、クラスタ管理およびフェイルオーバーの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）を作成および管理する、高可用ソリューションです。ストレージ グループは、別のサーバに複製されます。CCRでは、使用しているExchangeバックエンド サーバの単一障害ポイントが削除されます。CCRコピーの配置により、アクティブ ノード上の負荷が低減しているExchange Serverのパッシブ ノード上では、VSSを使用してバックアップを実行することができます。
数秒でCCRコピーに切り替えることができるため、CCRコピーはディザスタ リカバリに使用されます。複製ストレージ グループは、Exchange Replication Serviceと呼ばれるExchangeライタの新しいインスタンスとして表され、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。
「Exchange Replication Service およびLocal Continuous Replication 。」を参照。

CMMDB

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

CMMDB (Centralized Media Management Database：集中型メディア管理データベース)	「CMMDB 」を参照。
COM+登録データベース	*(Windows固有の用語)*COM+登録データベースとWindowsレジストリには、COM+アプリケーションの属性、クラスの属性、およびコンピュータ レベルの属性が格納されます。これにより、これらの属性間の整合性を確保でき、これらの属性を共通の方法で操作できます。
Command View (CV) EVA	*(HP StorageWorks EVA固有の用語)* HP StorageWorks EVA ストレージ システムを構成、管理、モニターするためのユーザー インタフェース。さまざまなストレージ管理作業を行うために使用されます。たとえば、仮想ディスクファミリの作成、ストレージ システム ハードウェアの管理、仮想ディスクのスナップクローンやスナップショットの作成などに使用されます。Command View EVA ソフトウェアは HP Storage マネジメント アプライアンス上で動作し、Web ブラウザからアクセスできます。 「HP StorageWorks EVA SMI-S Agent およびHP StorageWorks SMI-S EVAプロバイダ 。」を参照。
CRS	Data Protector Cell Manager上で実行される、Cell Request Serverのプロセス(サービス)。バックアップ セッションと復元セッションの開始および制御を行います。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。Windowsシステムでは、CRSは、インストール時に指定したユーザー アカウントで実行されます。UNIXシステムでは、rootアカウントで実行されます。
CSM	Data Protectorコピーおよび集約セッション マネージャ(Copy and Consolidation Session Manager)の略。このプロセスは、オブジェクト コピー セッションとオブジェクト集約セッションを制御し、Cell Managerシステム上で動作します。
Data Replication (DR)グループ	*(HP StorageWorks EVA固有の用語)* EVA仮想ディスクの論理グループ。共通の性質を持ち、同じCA EVAログを共有していれば、最大8組のコピー セットを含めることができます。 「コピー セット 」を参照。
Data_Protector_home	Data_Protector_home Windows Vista および Windows Server 2008 では、Data Protector のプログラム ファイルを含むディレクトリ。その他の Windows オペレーティング システムでは、Data Protector のData Protectorおよびデータ ファイルを含むディレクトリ。デフォルトのパス

は *%ProgramFiles%*\OmniBack ですが、インストール時に Data Protector セットアップ ウィザードでパスを変更できます。
「Data_Protector_program_data .」を参照。

Data_Protector_program_data

Data_Protector_program_data Windows Vista および Windows Server 2008 では、Data Protector のデータ ファイルを含むディレクトリ。デフォルトのパスは *%ProgramData%*\OmniBack ですが、インストール時に Data Protector セットアップ ウィザードでパスを変更できます。
「Data_Protector_home .」を参照。

Dbobject

(Informix Server固有の用語) Informix Serverの物理データベース 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

DCBF (Detail Catalog Binary Files: 詳細カタログ バイナリ ファイル) ディレクトリは、IDBの一部です。IDBの約80%を占有します。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) が含まれています。DCBFファイルの中には、ファイル バージョンについての情報が保管されています。これは、IDBのDCBF部分を表し、IDB全体の約80%の容量を占めます。デフォルトの DC ディレクトリは、dcbf ディレクトリと呼ばれ、Cell Manager の以下のディレクトリに配置されています。*Data_Protector_program_data*\db40 (Windows Server 2008 の場合)、*Data_Protector_home*\db40 (その他の Windows システムの場合)、または /var/opt/omni/server/db40 (UNIX システムの場合)。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10個までです。DCディレクトリのデフォルト最大サイズは16 GBです。

DHCPサーバ

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

Disk Agent

クライアントのバックアップと復元を実行するためにクライアント システム上にインストールする必要があるコンポーネントの1つ。Disk Agentは、ディスクに対するデータの読み書きを制御します。バックアップ セッション中には、Disk Agent がディスクからデータを読み取って、Media Agentに送信してデータをデバイスに移動させます。復元セッション中に

は、Disk AgentがMedia Agentからデータを受信して、ディスクに書き込みます。

Disk Agentの同時処理数

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

DMZ

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

DNSサーバ

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

DR OS

ディザスタ リカバリ オペレーティング システムとは、ディザスタ リカバリを実行するためのオペレーティング システム環境です。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 ProtectorData Protectorディザスタ リカバリを実行する前に、DR OSをインストールおよび構成しておく必要があります。DR OSは、Data Protector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。

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

「Symmetrix Agent (SYMA) 。」を参照。

Event Log (Data Protector Event Log)

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___BC_BRIEF_PRODUCT_NAME___イベント ログに送信されます。このイベント ログにアクセスできるData Protectorユーザーは、Adminユーザー グループに所属しているか、または「レポートと通知」のユーザー権限が付与されているData Protectorユーザーのみです。イベント ログ内のイベントは、すべてブラウズしたり削除することができます。

Exchange Replication Service

(Microsoft Exchange Server固有の用語) Local Continuous Replication (LCR) テクノロジまたはCluster Continuous Replication (CCR) テクノロジ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サービス。「Cluster Continuous Replication およびLocal Continuous Replication 。」を参照。

FCブリッジ

「Fibre Channelブリッジ 。」を参照。

Fibre Channelブリッジ

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

fnames.dat

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

GUI

Data Protectorには、グラフィカル ユーザー インタフェース (GUI) が用意されており、すべての構成タスク、管理タスク、および処理タスクに容易にアクセスできます。Windows 上で実行される Data Protector の GUI には、Data Protectorオリジナル以外にも、操作感の変わらない Java ベースの GUI があり、多数のプラットフォームで実行されます。

hard recovery

(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。

Holidaysファイル

休日に関する情報を格納するファイル。Cell Manager の以下のディレクトリにあるこのファイルを編集して、休日の設定を変更できます。*Data_Protector_program_data*\Config\Server\holidays (Windows Server 2008の場合)、 *Data_Protector_home*\Config\Server\holidays (その他の Windows システムの場合)、または /etc/opt/omni/server/Holidays (UNIX システムの場合)。

HP ITO

「OM 。」を参照。

HP OM

「OM 。」を参照。

HP OpC

「OM 。」を参照。

HP Operation Manager SMART Plug-In (SPI)

ドメイン管理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ソフトウェアに追加するだけですぐに使えます。 Through theHP OpenView SMART Plug-Inとして実装されるData Protector用統合ソフトウェアを使用して、ユーザーはHP Operations Managerソフトウェア (OM) の拡張機能として任意の数のData Protector Cell Managerを監視できます。

HP StorageWorks Disk Array XP LDEV

HP StorageWorks Disk Array XPの物理ディスクの論理パーティション。LDEVは、Continuous Access XP (CA)構成およびBusiness Copy XP (BC)構成で複製することができるエンティティで、スタンドアロンのエンティティとしても使用できます。「BC 、CA *(HP StorageWorks Disk Array XP固有の用語)*、および複製 。」を参照。

HP StorageWorks EVA SMI-S Agent

Data Protectorのソフトウェア モジュール。HP StorageWorks Enterprise Virtual Array用統合ソフトウェアに必要なタスクをすべて実行します。EVA SMI-S Agentを使用すると、受信した要求とCV EVA間のやり取りを制御するHP StorageWorks SMI-S EVA プロバイダを通じてアレイを制御できます。「Command View (CV) EVA およびHP StorageWorks SMI-S EVAプロバイダ 。」を参照。

HP StorageWorks SMI-S EVAプロバイダ

HP StorageWorks Enterprise Virtual Arrayを制御するために使用されるインタフェース。SMI-S EVAプロバイダはHP OpenView ストレージ マネジメント アプライアンス システム上で個別のサービスとして動作し、受信した要求とCommand View EVA間のゲートウェイとして機能します。Data Protector HP StorageWorks EVA用統合ソフトウェアでは、SMI-S EVAプロバイダはEVA SMI-S Agentから標準化された要求を受け入れ、Command View EVAとやり取りして情報または方法を呼び出し、標準化された応答を返します。「HP StorageWorks EVA SMI-S Agent およびCommand View (CV) EVA 。」を参照。

HP StorageWorks Virtual Array LUN

HP StorageWorks Virtual Array内の物理ディスクの論理パーティション。LUNはHP StorageWorks Business Copy VA 構成で複製することができるエンティティで、スタンドアロンのエンティティとしても使用できます。「BC VA および複製 。」を参照。

HP VPO

「OM 。」を参照。

IAPへのバックアップ

HP Integrated Archiving Platform (IAP) アプライアンスへのData Protectorベースのバックアップ。各データ チャンク固有のコンテンツ アドレスを作成することによって、IAPの機能の利点を生かし、ブロック (またはチャンク) レベルで保存された

	データの冗長性が低減されます。変更されたチャンクのみ、ネットワーク経由で転送され、保存場所に追加されます。
ICDA	*(EMC Symmetrix固有の用語)* MCのSymmetrixの統合キャッシュ ディスク アレイ (ICDA) は、複数の物理ディスク、複数のFWD SCSIチャネル、内部キャッシュ メモリ、および通常マイクロコードと呼ばれる制御/診断ソフトウェアを備えたディスク アレイ デバイスです。
IDB	Data Protector内部データベースは、Cell Manager上に維持される埋込み型データベースです。どのデータがどのメディアにバックアップされるか、バックアップ セッションと復元セッションがどのように実行されるか、さらに、どのデバイス上やライブラリ上に構成されているかについての情報が格納されます。
IDB回復ファイル	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) 。この情報を使うと、IDBの復旧を大幅に効率化できます。ファイルをIDBトランザクション ログとともに、ほかのIDBディレクトリから別の物理ディスク上に移し、さらに、そのファイルのコピーを作成します。
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。
IP アドレス	IP(インターネット プロトコル)アドレスは、ネットワーク上のシステムを一意に識別するアドレスで、数字で表されます。IPアドレスは、ピリオド(ドット)で区切られた4組の数字からなります。
ISQL	*(Sybase固有の用語)* Sybaseのユーティリティの1つ。Sybase SQL Serverに対してシステム管理作業を実行できます。
ITO	**「OM 。」を参照。**
Java GUI クライアント	Java GUI コンポーネントの1つ。ユーザー インタフェース関連の機能のみを含みます。動作するためは、Java GUI サーバに接続する必要があります。

Java GUI サーバ
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 クライアントからの要求を受け取ると、それを処理し、要求があったクライアントに応答を返します。通信は、HTTPプロトコル（ポート 5556）により行います。

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は、インストール サーバにインストールして構成する必要があります。

KMS
KMS キー マネジメント サービス (KMS) は、Cell Manager 上で稼動してData Protectorの暗号化機能のためのキー マネジメントを行う集中化されたサービスです。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。

LBO
(EMC Symmetrix固有の用語) Logical Backup Object（論理バックアップ オブジェクト）の略。LBOは、EMC Symmetrix/Fastrax環境内で保存/取得されるデータ オブジェクトです。LBOはEMC Symmetrixによって1つのエンティティとして保存/取得され、部分的には復元できません。

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

Local Continuous Replication
(Microsoft Exchange Server固有の用語) Local continuous replication (LCR) は、ストレージ グループの精密なコピー (LCRコピー）を作成および管理する単一サーバ ソリューションです。LCRコピーは、オリジナル ストレージ グループと同じサーバ上にあります。LCRコピーが作成される際、変更伝播（ログ リレー）テクノロジを介して最新の状態に保たれます。LCRの複製機能では、複製されていないログは削除されないことが保証されます。この動作は、ログのコピーよりかなり後に複製を行う場合、ログを削除するモードでバックアップを実行しても、実際には領域を解放しない可能性があることを意味します。
数秒でLCRコピーに切り替えることができるため、LCRコピーはディザスタ リカバリに使用されます。LCRコピーがバックアップに使用され、オリジナル データとは異なるディスク上にある場合、本稼働データベースへのI/O負荷は最小限に抑制されます。
複製ストレージ グループは、Exchange Replication Service と呼ばれるExchangeライタの新しいインスタンスとして表され、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。
「Cluster Continuous Replication およびExchange Replication Service 。」を参照。

log_fullシェル スクリプト

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

Lotus C API

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

LVM

LVM(Logical Volume Manager：論理ボリューム マネージャ)は、HP-UXシステム上で物理ディスク スペースを構造化し、論理ボリュームにマッピングするためのサブシステムです。LVMシステムは、複数のボリューム グループで構成されます。各ボリューム グループには、複数のボリュームが含まれます。

Main Control Unit (MCU)

(HP StorageWorks Disk Array XP固有の用語) CA構成およびBC構成用のプライマリ ボリュームを含み、マスター デバイスとしての役割を果たすHP StorageWorks XPディスク アレイ。「 BC (HP StorageWorks Disk Array XP固有の用語)、CA *(HP StorageWorks Disk Array XP固有の用語)*、およびHP StorageWorks Disk Array XP LDEV 。」を参照。

make_net_recovery

make_net_recoveryは Ignite-UX のコマンドで、Ignite-UX サーバまたは他の指定システム上に、ネットワークを経由して復旧アーカイブを作成するツールです。ターゲット システムは、Ignite-UX のmake_boot_tapeコマンドで作成したブート可能なテープからブートするか、または Ignite-UX サーバから直接ブートした後、サブネットを通じて復旧することができます。Ignite-UX サーバからの直接ブートは、Ignite-UX のbootsysコマンドで自動的に行うか、またはブート コンソールから対話的に指定して行うことができます。

make_tape_recovery

make_tape_recoveryは Ignite-UX のコマンドで、ブート可能な復旧（インストール）テープを作成するツールです。この復旧テープはご利用のシステムにカスタマイズされており、バックアップ デバイスをターゲット システムに直接接続して、ターゲット システムをこのブート可能な復旧テープからブートすることで、無人のディザスタ リカバリが可能となります。アーカイブ作成時とクライアント復旧時は、バックアップデバイスをクライアントにローカル接続しておく必要があります。

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	**「Main Control Unit (MCU) 。」を参照。**
Media Agent	デバイスに対する読み込み/書き込みを制御するプロセス。制御対象のデバイスはテープなどのメディアに対して読み込み/書き込みを行います。バックアップ セッション中、Media AgentはDisk Agentからデータを受信し、デバイスに送信します。データを受信したデバイスはメディアに書き込みます。Media Agentは、ライブラリのロボティクス制御も管理します。
Microsoft Exchange Server	多様な通信システムへの透過的接続を提供するクライアント/サーバ型のメッセージング/ワークグループ システム。電子メール システムの他、個人とグループのスケジュール、オンライン フォーム、ワークフロー自動化ツールなどをユーザーに提供します。また、開発者に対しては、情報共有およびメッセージング サービス用のカスタム アプリケーション開発プラットフォームを提供します。
Microsoft SQL Server	分散型クライアント サーバ コンピューティングのニーズを満たすように設計されたデータベース管理システム。
Microsoft Volume Shadow Copy Service (VSS)	VSS対応アプリケーションのバックアップと復元をそのアプリケーションの機能に関係なく統合管理する統一通信インタフェースを提供するソフトウェア サービスです。このサービスは、バックアップ アプリケーション、ライター、シャドウ コピー プロバイダ、およびオペレーティング システム カーネルと連携して、ボリューム シャドウ コピーおよびシャドウ コピー セットの管理を実現します。 「シャドウ コピー 、シャドウ コピー プロバイダ 、複製 、およびライタ 。」を参照。
Microsoft管理コンソール (MMC)	*(Windows固有の用語)* Windows環境における管理モデル。シンプルで一貫した統合型管理ユーザー インタフェースを提供します。同じGUIを通じて、さまざまなMMC対応アプリケーションを管理できます。
MMD	Media Management Daemon (メディア管理デーモン)の略。MMDプロセス (サービス) は、Data Protector Cell Manager上で稼動し、メディア管理操作およびデバイス操作を制御します。このプロセスは、Data ProtectorをCell Managerにインストールしたときに開始されます。

MMDB

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

MoM

複数のセルをグループ化して、1つのセルから集中管理することができます。集中管理用セルの管理システムがMoM (Manager-of-Managers)です。他のセルはMoMクライアントと呼ばれます。MoMを介して、複数のセルを一元的に構成および管理することができます。

MSM

Data Protector Media Session Manager（メディア セッション マネージャ）の略。MSMは、Cell Manager上で稼動し、メディア セッション（メディアのコピーなど）を制御します。

MU番号

(HP StorageWorks Disk Array XP固有の用語) ミラー ユニット番号。ファーストレベルミラーを示すために使う整数(0、1または2)です。
「ファースト レベル ミラー 。」を参照。

obdrindex.dat

「IDB復旧ファイル 。」を参照。

OBDR対応デバイス

ブート可能ディスクを装填したCD-ROMドライブをエミュレートできるデバイス。バックアップ デバイスとしてだけでなく、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。

OM

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、UNIX用HP Operations Managerソフトウェアの略称。Data Protectorには、この管理製品用の統合ソフトウェアが用意されています。この統合ソフトウェアは、HP-UX、Solaris、およびLinux上のOM管理サーバ用のSMART Plug-Inとして実装されています。以前のバージョンのOMは、IT/Operation、Operations Center、および Vantage Point Operationsと呼ばれていました。
「マージ 。」を参照。

ON-Bar

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

- onbarコマンド
- バックアップ ソリューションとしてのData Protector

- XBSAインタフェース
- ON-Barカタログ テーブル。これは、dbobjectをバックアップし、複数のバックアップを通してdbobjectのインスタンスをトラッキングするために使われます。

ONCONFIG

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

OpC

「OM 。」を参照。

OpenSSH

さまざまな認証方式と暗号化方式を採用することにより、リモート マシンへの安全なアクセスを提供するネットワーク接続ツールのセット。セキュア シェルを使用してリモート インストールを実行する場合、Installation Serverとクライアントにこれをインストールして構成する必要があります。

Oracle Data Guard

(Oracle固有の用語) Oracle Data Guardは、Oracleの主要なディザスタ 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) ログイン情報の書式は、*user_name*/*password*@*service*です。

- *user_name*は、Oracle Serverおよびその他のユーザーに対して公開されるユーザー名です。各ユーザーがOracleターゲット データベースに接続するには、ユーザー名とパスワードの両方を入力しなければなりません。ここでは、

OracleのSYSDBA権限またはSYSOPER権限が付与されているユーザーを指定する必要があります。

- *password*は、Oracle パスワード ファイル (orapwd) に指定されているパスワードに一致する必要があります。これは、データベース管理を行うユーザーの認証に使用されるファイルです。
- *service*は、ターゲット データベースのSQL*Net サーバ プロセスを識別する名前です。

P1Sファイル

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

RAID

Redundant Array of Inexpensive Disksの略。

RAID Manager XP

(HP StorageWorks Disk Array XP固有の用語) RAID Manager XPアプリケーションでは、CAおよびBC アプリケーションのステータスをレポートおよび制御する多数のコマンド リストが提供されます。これらのコマンドは、RAID Managerインスタンスを通じて、StorageWorks Disk Array XP Disk Control Unitと通信します。このインスタンスは、コマンドを一連の低レベルSCSIコマンドに変換します。

RAID Manager ライブラリ

(HP StorageWorks Disk Array XP固有の用語) Solarisシステム上のData Protectorでは、RAID Manager ライブラリを内部的に使用して、HP StorageWorks Disk Array XPの構成データ、ステータス データ、およびパフォーマンス データにアクセスします。さらに、一連の低レベル SCSI コマンドに変換される関数呼び出しを通じて、HP StorageWorks Disk Array XPの主要な機能にアクセスします。

rawディスク バックアップ

「ディスク イメージ バックアップ 。」を参照。

RCU

「Remote Control Unit (RCU) 。」を参照。

RDBMS

Relational Database Management System（リレーショナル データベース管理システム）の略。

RDF1/RDF2

*(EMC Symmetrix固有の用語)*SRDF デバイス グループの一種。RDF グループには RDF デバイスだけを割り当てることができます。RDF1 グループ タイプにはソース デバイス (R1)

が格納され、RDF2 グループ タイプにはターゲット デバイス（R2）が格納されます。

RDS

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

Recovery Manager（RMAN）

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

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 リカバリ実行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。

Remote Control Unit（RCU）

(HP StorageWorks Disk Array XP固有の用語) Remote Control Unit（RCU）は、CA構成の中でMCU（Main Contol Unit）のスレーブとしての役割を果たします。双方向の構成の中では、RCUはMCUとしての役割を果たします。

RMAN *(Oracle固有の用語)*

「Recovery Manager 。」を参照。

RSM

Data Protector Restore Session Managerの略。復元セッションを制御します。このプロセスは、常にCell Managerシステム上で稼動します。

RSM

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

SIBF

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

SMB

「スプリット ミラー バックアップ 。」を参照。

SMBF

セッション メッセージ バイナリ ファイル(SMBF)は、IDBのうち、バックアップ、復元、オブジェクト コピー、オブジェクト集約、およびメディア管理のセッション中に生成されたセッション メッセージが格納される部分です。セッションごとに1つのバイナリファイルが作成されます。バイナリ ファイルは、年と月に基づいて分類されます。

sqlhostsファイル

(Informix Server固有の用語) Informix Serverの接続情報ファイル (UNIX) またはレジストリ (Windows)。各データベース サーバの名前の他、ホスト コンピュータ上のクライアントが接続できるエイリアスが保存されています。

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SLDのリアルタイム データ複製を実現するBusiness Continuationプロセスです。同じルート コンピュータ環境内だけではなく、互いに遠距離にある環境も対象となります。

SRDファイル

SRD (System Recovery Data：システム復旧データ) ファイルには、障害発生時にオペレーティング システムをインストールおよび構成するために必要なシステム情報が含まれています。SRDファイルはASCIIファイルで、CONFIGURATIONバックアップがWindowsクライアント上で実行されCell Managerに保存される時に生成されます。

SSE Agent

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

sst.confファイル

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

st.confファイル

/kernel/drv/st.conf ファイルは、バックアップ デバイスが接続されているData Protector Solarisクライアントのそれぞれに

インストールされていなければならないファイルです。このファイルには、クライアントに接続されている各バックアップ ドライブのデバイス情報とSCSIアドレスが記述されていなければなりません。シングルドライブ デバイスについては単一のSCSIエントリが必要で、マルチドライブ ライブラリ デバイスについては複数のSCSIエントリが必要です。

StorageTek ACS ライブラリ *(StorageTek固有の用語)* ACS (Automated Cartridge System) は、1つのライブラリ管理ユニット (LMU) と、このユニットに接続された1 ~ 24個のライブラリ記憶域モジュール (LSM) からなるライブラリ システム (サイロ) です。

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

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

Symmetrix Agent (SYMA) *(EMC Symmetrix固有の用語)*EMC Symmetrix 環境でのバックアップ操作と復元操作を可能にするData Protectorソフトウェア モジュール。

System Backup to Tape *(Oracle固有の用語)*Oracleがバックアップ要求または復元要求を発行したときに正しいバックアップ デバイスをロード、ラベリング、およびアンロードするために必要なアクションを処理するOracle インタフェース。

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

TimeFinder *(EMC Symmetrix固有の用語)*単一または複数のEMC Symmetrix 論理デバイス (SLD) のインスタント コピーを作成するBusiness Continuationプロセス。インスタント コピーは、BCVと呼ばれる専用の事前構成SLD上に作成され、システムに対する別個のプロセスを経由してアクセスできます。

TLU Tape Library Unit (テープ ライブラリ ユニット) の略。

TNSNAMES.ORA *(OracleおよびSAP R/3固有の用語)* サービス名にマッピングされた接続記述子が保存されているネットワーク構成ファイル。このファイルは、1か所で集中的に管理してすべてのクライアントで使用することも、また、ローカルに管理して各クライアントで個別に使用することもできます。

TSANDS.CFG ファイル

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

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クライアントとCell Manager間の通信を行います。また、ビジネス ロジック処理を実行し、重要な情報のみをクライアントに送信します。このサービスは、Data ProtectorがCell Manager上にインストールされるとすぐに開始されます。

VMware 管理クライアント

(VMware用統合統合ソフトウェア固有の用語) Data Protectorを使用してVMware Virtual Infrastructureと通信するクライアント。VirtualCenter Server システム（VirtualCenter 環境）または ESX Server システム（スタンドアロンの ESX Server 環境）が考えられます。

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。

Volume Shadow Copy Service

「Microsoft Volume Shadow Copy Service 。」を参照。

VPO

「OM 。」を参照。

VSS

「Microsoft Volume Shadow Copy Service 。」を参照。

VSS準拠のモード

(HP StorageWorks Disk Array XP VSSプロバイダ固有の用語) 2つのXP VSSハードウェア プロバイダのうちの1つの操作モード。XPプロバイダがVSS準拠モードである場合、ソース ボリューム (P-VOL) および複製 (S-VOL) は、バックアップ後に単方向のペアリングされない状態になります。したがって、ローテーションされる複製（1つのP-VOLごとのS-VOL）の最大数には、制限がありません。このような構成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です。「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 。」を参照。

VxFS

Veritas Journal Filesystemの略。

VxVM (Veritas Volume Manager)

Veritas Volume Managerは、Solarisプラットフォーム上でディスク スペースを管理するためのシステムです。VxVMシステムは、論理ディスク グループに編成された1つまたは複数の物理ボリュームの任意のグループからなります。

Wake ONLAN 節電モードで動作しているシステムを同じLAN上の他のシステムからのリモート操作により電源投入するためのサポート。

Webレポート Data Protectorの機能の1つ。バックアップ ステータス、オブジェクト コピー ステータスおよびオブジェクト集約ステータスとData Protector構成に関するレポートをWebインタフェース経由で表示できます。

Windows CONFIGURATION バックアップ Data Protectorでは、Windows CONFIGURATION（構成データ）をバックアップできます。Windowsレジストリ、ユーザー プロファイル、イベント ログ、WINSサーバ データおよびDHCPサーバ データ（システム上で構成されている場合）を1回の操作でバックアップできます。

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

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

XBSAインタフェース *(Informix Server固有の用語)* ON-BarとData Protectorの間の相互通信には、X/Open Backup Services Application Programmer's Interface (XBSA)が使用されます。

XCopyエンジン *(ダイレクト バックアップ固有の用語)* SCSI-3のコピー コマンド。SCSIソース アドレスを持つストレージ デバイスからSCSIあて先アドレスを持つバックアップ デバイスにデータをコピーし、ダイレクト バックアップを可能にします。XCopyでは、ソース デバイスからデータをブロック（ディスクの場合）またはストリーム（テープの場合）としてあて先デバイスにコピーします。これにより、データをストレージ デバイスから読み込んであて先デバイスに書き込むまでの一連の処理が、制御サーバをバイパスして行われます。
「ダイレクト バックアップ 。」を参照。

ZDB **「ゼロ ダウンタイム バックアップ (ZDB) 。」を参照。**

ZDBデータベース *(ZDB固有の用語)*ソース ボリューム、複製およびセキュリティ情報などのZDB関連情報を格納するIDBの一部。ZDBデータベースはZDB、インスタント リカバリ、スプリット ミラー復元に使用されます。
「ゼロ ダウンタイム バックアップ (ZDB) 。」を参照。

アーカイブ ロギング *(Lotus Domino Server固有の用語)* Lotus Domino Serverのデータベース モードの1つ。トランザクション ログ ファイルがバックアップされて初めて上書きされるモードです。

アーカイブREDOログ

(Oracle固有の用語) オフラインREDOログとも呼ばれます。OracleデータベースがARCHIVELOGモードで動作している場合、各オンラインREDOログが最大サイズまで書き込まれると、アーカイブ先にコピーされます。このコピーをアーカイブ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 」を参照。

アクセス権限

「ユーザー権限 。」を参照。

アプリケーション エージェント

クライアント上でオンライン データベース統合ソフトウェアを復元およびバックアップするために必要なコンポーネント。「Disk Agent 。」を参照。

アプリケーション システム

(ZDB固有の用語) このシステム上でアプリケーションやデータベースが実行されます。 アプリケーションまたはデータベース データは、ソース ボリューム上に格納されています。「バックアップ システム およびソース ボリューム 。」を参照。

イベント ログ

(Windows固有の用語) イベント ログ (Windows固有の用語) サービスの開始および停止、ユーザーのログインおよびログオフなど、Windows のすべてのイベントが記録されるファイル。 Data Protector では、Windowsの構成バックアップの一部として、Windows Event Logをバックアップすることができます。

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 。」を参照。

Installation Server
特定のアーキテクチャ用のData Protectorソフトウェア パッケージのレポジトリを保持するコンピュータ システム。Installation ServerからData Protectorクライアントのリモート インストールが行われます。混在環境では、少なくとも2台のInstallation Serverが必要です。1台がUNIXシステム用、もう1台が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 ストアでは、メールボックス ストアとパブリック フォルダ ストアの2種類のストアが管理されます。メールボックス ストアは個々のユーザーに属するメールボックスから成ります。パブリック フォルダ ストアには、複数のユーザーで共有するパブリック フォルダおよびメッセージがあります。
「キー マネージメント サービス およびサイト複製サービス 。」を参照。

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 。」を参照。

エクスチェンジャ
SCSIエクスチェンジャとも呼ばれます。
「ライブラリ 。」を参照。

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 。」を参照。

オートチェンジャー
「ライブラリ 。」を参照。

オートローダ
「ライブラリ 。」を参照。

オブジェクト
「バックアップ オブジェクト 。」を参照。

オブジェクト コピー
特定のオブジェクト バージョンのコピー。オブジェクト コピー セッション中またはオブジェクト ミラーのバックアップ セッション中に作成されます。

オブジェクト コピー セッション

異なるメディア セット上にバックアップされたデータの追加のコピーを作成するプロセス。オブジェクト コピー セッション中に、選択されたバックアップ オブジェクトがソースからターゲット メディアへコピーされます。

オブジェクト ミラー

オブジェクトのミラーリングを使用して作成されるバックアップ オブジェクトのコピー。オブジェクトのミラーは通常オブジェクト コピーと呼ばれます。

オブジェクト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。

オブジェクトのコピー

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

オブジェクトのミラーリング

バックアップ セッション中に、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

フル バックアップと1回以上の増分バックアップから成るバックアップ オブジェクトの復元チェーンを、新しい集約バージョンのオブジェクトにマージするプロセス。

オフライン バックアップ

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

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

「ゼロ ダウンタイム バックアップ (ZDB) およびオンライン バックアップ 。」を参照。

オフラインREDOログ

「アーカイブREDOログ 。」を参照。

オフライン復旧

オフライン復旧は、ネットワーク障害などによりCell Managerにアクセスできない場合に行われます。オフライン復旧には、スタンドアロン デバイスとSCSIライブラリ デバイスだけを使用できます。Cell Managerの復旧は、常にオフラインで行われます。

オリジナル 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 バックアップ

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

- 単純なバックアップ方法の場合（ZDBではない）、バックアップ中（数分から数時間）は、常にバックアップ モードである必要があります。たとえばテープへのバックアップの場合、テープへのデータ ストリーミングが終わるまでの間となります。
- ZDBの方法を使うと、バックアップ モードである必要がある時間はデータ複製プロセス中のわずか数秒間です。残りのバックアップ プロセスでは、データベースは通常の稼動を再開できます。

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

オンラインREDOログ

(Oracle固有の用語) まだアーカイブされていないが、インスタンスでデータベース アクティビティを記録するために利用できるか、または満杯になっており、アーカイブまたは再使用されるまで待機しているREDOログ。
「アーカイブREDOログ 。」を参照。

階層ストレージ管理(HSM)

使用頻度の低いデータを低コストの光磁気プラッタに移動することで、コストの高いハード ディスク記憶域を有効利用するための仕組み。移動したデータが必要になった場合は、ハード ディスク記憶域に自動的に戻されます。これにより、ハード ディスクからの高速読み取りと光磁気プラッタの低コスト性のバランスが維持されます。

拡張可能ストレージ エンジン (ESE)
(Microsoft Exchange Server固有の用語) Microsoft Exchange Serverで情報交換用の記憶システムとして使用されているデータベース テクノロジ。

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。

仮想コントローラ ソフトウェア (VCS)
(HP StorageWorks EVA固有の用語) HSVコントローラを介したCommand View EVAとの通信など、記憶システムの処理すべてを管理するファームウェア。
「Command View (CV) EVA 。」を参照。

仮想サーバ
仮想マシンとは、ネットワークIP名およびIPアドレスでドメイン内に定義されるクラスタ環境を意味します。このアドレスは、クラスタ ソフトウェアによってキャッシュされ、仮想サーバ リソースを現在実行しているクラスタ ノードにマッピングされます。こうして、特定の仮想サーバに対するすべての要求が特定のクラスタ ノードにキャッシュされます。

仮想ディスク
(HP StorageWorks EVA固有の用語) HP StorageWorks Enterprise Virtual Arrayストレージ プールから割り当てられたストレージのユニット。仮想ディスクは、HP StorageWorks Enterprise Virtual Arrayのスナップショット機能により複製されるエンティティです。
「ソース ボリューム およびターゲット ボリューム 。」を参照。

仮想テープ
(VLS固有の用語) テープに保存するのと同様に、データをディスク ドライブにバックアップするアーカイブ ストレージ テクノロジ。仮想テープ システムの利点には、バックアップおよび復元のスピードが向上すること、運用コストが低いことなどがあります。
「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 。」を参照。

仮想テープ ライブラリ (VTL)
(VLS固有の用語) 従来のテープ ベースのストレージ機能を提供する、エミュレートされるテープ ライブラリ。
「仮想ライブラリ システム (VLS) 。」を参照。

仮想デバイス インタフェース
(Microsoft SQL Server固有の用語) SQL Server のプログラミング インタフェースの1つ。大容量のデータベースを高速でバックアップおよび復元できます。

仮想フル バックアップ
効率の良い合成バックアップのタイプ。コピーされる代わりに、ポインタの使用によってデータが集約されます。すべての

バックアップ(フル バックアップ、増分バックアップ、およびその結果生成される仮想フル バックアップ)を、配布ファイル メディア形式を使用する単一のファイル ライブラリに書き込む場合に実行します。

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 。」を参照。

監査情報 Data Protectorセル全体でユーザーによって定義された拡張期間に実行された、各バックアップ 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ているデータから作成された、ユーザーが読み取り可能な形式の監査情報。

監査ログ 監査データが保存されているデータ ファイル。

キー ストア 暗号化キーはすべてCell Managerのキー ストアに集中して保存され、Key Management Server (KMS)によって管理されます。

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 。」を参照。

共有ディスク あるシステム上に置かれたWindowsのディスクをネットワーク上の他のシステムのユーザーが使用できるように構成したもの。共有ディスクを使用しているシステムは、Data Protector Disk Agentがインストールされていなくてもバックアップ可能です。

緊急ブート ファイル *(Informix Server固有の用語)* *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) にある、Informix Serverの構成ファイル ixbar.*server_id*。*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。

クライアント または**クライアント システム** セル内でData Protectorの機能を使用できるように構成された任意のシステム。

クライアント バックアップ
クライアント上にマウントされている状態のすべてのファイルシステムのバックアップ。ただし、バックアップ仕様の作成後にクライアントにマウントされたファイルシステムは、自動検出されません。

クラスタ対応アプリケーション
クラスタ アプリケーション プログラミング インタフェースをサポートしているアプリケーション。クラスタ対応アプリケーションごとに、クリティカル リソースが宣言されます。これらのリソースには、ディスク ボリューム(Microsoft Cluster Serverの場合)、ボリューム グループ(MC/ServiceGuardの場合)、アプリケーション サービス、IP名、およびIPアドレスなどがあります。

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

グローバル オプション ファイル
Data Protectorをカスタマイズするためのファイル。このファイルでは、Data Protectorのさまざまな設定（特に、タイムアウトや制限）を定義でき、その内容はData Protectorセル全体に適用されます。ファイルは、Cell Managerの*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Solarisシステムの場合)に配置されています。

検証
指定したメディア上のData Protectorデータが読み取り可能かどうかをチェックする機能。また、CRC（巡回冗長検査）オプションをオンにして実行したバックアップに対しては、各ブロック内の整合性もチェックできます。

合成バックアップ
合成フル バックアップを生成するバックアップ ソリューション。データに関しては従来のフル バックアップと同等ですが、プロダクション サーバまたはネットワークに負荷がかかりません。合成フル バックアップは、前回のフル バックアップと任意の回数の増分バックアップから作成されます。

合成フル バックアップ
バックアップ オブジェクトの復元チェーンを新しい合成フル バージョンのオブジェクトにマージする、オブジェクト集約処理の結果として生成されます。合成フル バックアップは、復元速度の点では、従来のフル バックアップと同等です。

コピー セット
(HP StorageWorks EVA固有の用語) ローカルEVA上にあるソース ボリュームとリモートEVA上にあるその複製とのペア。

「ソース ボリューム 、複製 、およびCA+BC EVA 」を参照。

コマンド ビュー VLS

(VLS固有の用語) LANを介してVLSを構成、管理、監視するために使用されるWebブラウザ ベースのGUI。
「仮想ライブラリ システム (VLS) 。」を参照。

コマンド行インタフェース (CLI)

CLIには、DOSコマンドやUNIXコマンドと同じようにシェル スクリプト内で使用でできるコマンドが用意されています。これらを使用して、Data Protectorの構成、バックアップ、復元、および管理の各タスクを実行することができます。

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 StorageWorks Disk Array XP VSSプロバイダ固有の用語) One of two XP VSS hardware provider operation modes.XPプロバイダが再同期モードである場合、ソース ボリューム (P-VOL) および複製(S-VOL) は、バックアップ後に一時停止されたミラー関係になります。ローテーションされる複製 (1つのP-VOLごとのS-VOL) の最大数は、MU範囲が0 ~ 2または0、1、2の場合、3つになります。このような構成のバックアップからの復元は、S-VOLのP-VOLとの再同期によってのみ可能です。
「VSS 準拠モード 、ソース ボリューム 、プライマリ ボリューム (P-VOL) 、複製 、セカンダリ ボリューム (S-VOL) 、MU番号 、および複製セット ローテーション 。」を参照。

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によって、Microsoft Exchange Server 5.5との互換性を持つMicrosoft Exchange Server 2000/2003のサービスです。
「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 。」を参照。

差分同期(再同期)

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

バイス(R2)が増分的に同期化され、EMC Symmetrixミラー化メディアとして機能します。EMC Symmetrixデバイスは、事前にペアにしておく必要があります。

差分バックアップ (delta backup)

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

差分リストア

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

システム データベース

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

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

システム ボリューム/ディスク/パーティション

オペレーティング システム ファイルが格納されているボリューム/ディスク/パーティション。ただし、Microsoftの用語では、ブート プロセスの開始に必要なファイルが入っているボリューム/ディスク/パーティションをシステム ボリューム/ディスク/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 (証明書サーバの場合) が含まれます。サーバがドメイン コントローラの場合は、Active Directoryサービスと SYSVOLディレクトリもシステム状態データに含まれます。サーバ上でクラスタ サービスが実行されている場合は、リソース レジストリ チェックポイントと、最新のクラスタ データベース情報を格納するクォーラム リソース回復ログもシステム状態データに含まれます。

事前割当てリスト メディア プール内のメディアのサブセットをバックアップに使用する順に指定したリスト。

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

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

実行前/実行後コマンド 実行前コマンドおよび実行後コマンドは、バックアップ セッションまたは復元セッションの前後に付加的な処理を実行する実行可能ファイルまたはスクリプトです。実行前コマンドおよび実行後コマンドは、Data Protectorで事前に用意されているものではありません。ユーザーは、コマンドを独自に作成する必要があります。Windows上で動作する実行可能ファイルまたはバッチファイル、UNIX上で動作するシェル スクリプトなどを使用できます。

自動移行 *(VLS固有の用語)* 最初にVLS仮想テープに対してデータ バックアップを行い、次にバックアップ アプリケーションを使用することなく物理テープ (1つの物理テープをエミュレートする1つの仮想テープ) に移行することができる機能。
「仮想ライブラリ システム (VLS) および仮想テープ 。」を参照。

シャドウ コピー *(Microsoft VSS固有の用語)* 特定の時点におけるオリジナル ボリューム (元のボリューム) の複製を表すボリューム。オリジナル ボリュームからではなく、シャドウ コピーからデータがバックアップされます。バックアップ中に元のボリュームに変更が加えられても、ボリュームのシャドウ コピーは整合性のある状態に保たれます。
「Microsoft Volume Shadow Copy Service および複製 。」を参照。

シャドウ コピーセット *(Microsoft VSS固有の用語)* 同じ時点で作成されたシャドウ コピーのコレクション。
「シャドウ コピー および複製セット 。」を参照。

シャドウ コピー プロバイダ

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

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 。」を参照。

循環ログ

(Microsoft Exchange ServerおよびLotus Domino Server固有の用語).循環ログは、Microsoft Exchange Serverデータベース モードおよびLotus Domino Serverデータベース モードで、該当するデータがデータベースにコミットされた後、トランザクション ログ ファイルの内容が定期的に上書きされる形式のログです。循環ログにより、ディスク記憶領域の消費が低減できます。

初期化

「フォーマット 。」を参照。

所有権

バックアップの所有権は、どのユーザーがバックアップからデータを復元できるかを決定します。あるユーザーが対話型バックアップを開始すると、そのユーザーはセッション オーナーになります。ユーザーが既存のバックアップ仕様を修正せずにそのまま起動した場合、そのバックアップ セッションは対話型とみなされません。この場合、バックアップ仕様内でバックアップ オーナーが指定されていれば、その指定が継承されます。バックアップ仕様内でバックアップ オーナーが指定されていなければ、バックアップを開始したユーザーがセッション オーナーになります。スケジュールされたバックアップについては、デフォルトで、UNIX Cell Managerのセッション所有者はroot.sys@*Cell Manager*、Windows Cell Managerのセッション所有者はCell Managerのインストール中に指定されたユーザーです。所有権は変更可能なので、特定のユーザーをセッション オーナーにすることができます。

シングル インスタンス機能

(IAP固有の用語) オブジェクト全体およびチャンク レベルの両方で、データの冗長性を認識するプロセス。各データ チャンクのストロング ハッシュ関数が計算され、作成中の複製の保存を試行するか決める際に必要となる、固有のコンテンツ アドレスとして使用されます。
「IAPへのバックアップ 。」を参照。

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。

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セカンダリ ボリューム (S-VOL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 プロセスで管理します。

ストレージ ボリューム

(ZDB固有の用語) ストレージ ボリュームは、オペレーティング システムまたはボリューム管理システム、ファイル システム、または他のオブジェクトが存在可能なその他のエンティティに提供可能なオブジェクトを表します（たとえば仮想化技法)。ボリューム管理システム、ファイル システムはこの記憶域に構築されます。これらは通常、ディスク アレイなどの記憶システム内に作成または存在します。

スナップショット

(HP StorageWorks VAおよびHP StorageWorks EVA固有の用語) スナップショット作成技法を使用して作成された複製の形式。使用するアレイ/技法に応じて、特徴の異なるさまざまな種類のスナップショットが使用できます。スナップショッ

トで作成された複製は動的なもので、スナップショットの種類や作成時間によって、ソース ボリュームの内容に依存する仮想コピーか、独立した正確な複製（クローン）かのいずれかになります。
「複製 およびスナップショット作成 。」を参照。

スナップショット バックアップ *(HP StorageWorks VA およびHP StorageWorks EVA固有の用語)*

「テープへのZDB 、ディスクへのZDB 、およびディスク+テープへのZDB 。」を参照。

スナップショット作成

(HP StorageWorks VAおよびHP StorageWorks EVA固有の用語) 複製を作成する技法で、ストレージ仮想化技法を使用して、ソース ボリュームのコピーが作成されます。 複製はある一時点で作成されたものとみなされ、事前構成することなく、即座に使用できます。ただし、通常は複製作成後もコピープロセスはバックグラウンドで継続されます。
「スナップショット 。」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。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その例です。スパースファイルの処理を復元中に有効にしておかないと、スパースファイルを復元できなくなる可能性があります。

スプリット ミラー

*(EMC SymmetrixおよびHP StorageWorks Disk Array XP固有の用語)*スプリット ミラー技法を使用して作成した複製。複製により、ソース ボリュームの内容について独立した正確な複製（クローン）が作成されます。
「複製 およびスプリット ミラー作成 。」を参照。

スプリット ミラー バックアップ *(EMC Symmetrix固有の用語)*

「テープへのZDB 。」を参照。

スプリット ミラー バックアップ *(HP StorageWorks Disk Array XP固有の用語)*

「テープへのZDB 、ディスクへのZDB 、およびディスク+テープへのZDB 。」を参照。

スプリット ミラーの作成

*(EMC SymmetrixおよびHP StorageWorks Disk Array XP固有の用語)*事前構成したターゲット ボリュームのセット（ミラー）を、ソース ボリュームの内容の複製が必要になるまでソース ボリュームのセットと同期化し続ける複製技法。その後、同期を停止（ミラーを分割）すると、分割時点での

ソース ボリュームのスプリット ミラー複製はターゲット ボリュームに残ります。
「スプリット ミラー 。」を参照。

スプリット ミラー復元

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

スマート コピー

(VLS固有の用語) 仮想テープから物理テープ ライブラリに作成されたバックアップ データのコピー。スマート コピーのプロセスのよって、Data Protectorでは、ソース メディアとターゲット メディアが区別され、メディア管理が可能になります。
「仮想ライブラリ システム (VLS) 。」を参照。

スマート コピープール

(VLS固有の用語) 指定したソース仮想ライブラリのスマート コピー ターゲットとして使用可能なコピー先ライブラリ スロットが定義されたプール。
「仮想ライブラリ システム (VLS) およびスマート コピー 。」を参照。

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1式のレジスタ値からなります。同じプロセス内で複数のスレッドを同時に実行できます。

スロット

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

制御ファイル

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

セカンダリ ボリューム (S-VOL)

(HP StorageWorks Disk Array XP固有の用語) セカンダリ ボリューム (S-VOL) は、他のLDEV (P-VOL)のセカンダリなCAミラーおよびBCミラーとして動作するXP LDEVです。CAの場合、S-VOLをMetroCluster構成内のフェイルオーバー デバイスとして使うことができます。S-VOLには、P-VOLによって使用されるアドレスとは異なる、個別のSCSIアドレスが割り当てられます。

「プライマリ ボリューム (P-VOL) およびMain Control Unit (MCU) 。」を参照。

セッション

「バックアップ セッション 、メディア管理セッション 、および復元セッション 。」を参照。

セッション キー

実行前スクリプトおよび実行後スクリプト用の環境変数。プレビュー セッションを含めたData Protectorセッションを一意に識別します。セッション キーはデータベースに記録されず、CLIコマンドのomnimnt、，omnistat、およびomniabortコマンド。

セッションID

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

セル

1台のCell Managerに管理されているシステムの集合。セルには、一般に、同じLANに接続されたサイトや組織エンティティ上のシステムが含まれます。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。

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 。」を参照。

増分1メールボックス バックアップ

増分1メールボックス バックアップでは、前回のフル バックアップ以降にメールボックスに対して行われた変更をすべてバックアップします。

増分ZDB

保護されている最後のフル バックアップまたは増分バックアップより後に変更された部分のみをバックアップする、ファイルシステムのテープへのZDBセッションまたはディスク+テープへのZDBセッション。
「フルZDB 。」を参照。

増分バックアップ

前回のバックアップ以降に変更があったファイルだけを選択するバックアップ。増分バックアップには複数のレベルがあり、復元チェーンの長さを細かく制御できます
「バックアップの種類 。」を参照。

増分バックアップ

(Microsoft Exchange Server固有の用語) 前回のフル バックアップまたは増分バックアップ以降の変更だけをバックアップするMicrosoft Exchange Serverデータのバックアップ。 増分

バックアップでは、バックアップ対象はトランザクション ログだけです。
「バックアップの種類 。」を参照。

増分メールボックス バックアップ

増分メールボックス バックアップでは、前回の各種バックアップ以降にメールボックスに対して行われた変更をすべてバックアップします。

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) 。」を参照。

ソース ボリューム

(ZDB固有の用語) 複製されたデータを含むストレージ ボリューム。

ターゲット システム

(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) ソース デバイス (R1) との SRDF操作に参加するEMC Symmetrixデバイス。リモート EMC Symmetrix ユニット内に置かれます。ローカル EMC Symmetrix ユニット内でソース デバイス (R1) とペアになり、ミラー化ペアから、すべての書き込みデータを受け取ります。このデバイスは、通常のI/O操作ではユーザー アプリケーションからアクセスされません。R2 デバイスは、RDF2 グループ タイプに割り当てる必要があります。
「ソース デバイス (R1) 。」を参照。

ターゲット ボリューム

(ZDB固有の用語) データの複製先のストレージ ボリューム。

ターミナル サービス

(Windows固有の用語) Windowsのターミナル サービスは、サーバ上で実行されている仮想Windowsデスクトップ セッションとWindowsベースのプログラムにクライアントからアクセスできるマルチセッション環境を提供します。

ダイレクト バックアップ

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

チャネル

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

- diskタイプ
- SBT_TAPEタイプ

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

チャンク化

(IAP固有の用語) データをブロック (チャンク) に分割するプロセスで、各チャンクでは固有のコンテンツ アドレスが取得されます。次に、このアドレスは、特定のチャンクがIAPアプライアンスにすでにバックアップされたかどうかを特定するために使用されます。重複データが特定された場合 (2つのアドレスが同じ、つまり、取得したアドレスがIAPにすでに保存されているデータ チャンクのアドレスと同じ場合)、バックアップされません。この方法では、データの冗長性が低減され最適なデータ保存が達成されます。
「IAPへのバックアップ 。」を参照。

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。

ディスク イメージ (rawディスク) のバックアップ

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

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

ディスク グループ *(Veritas Volume Manager固有の用語)* VxVMシステムにあるデータ 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 複数のフェーズでデータをバックアップするプロセス。これにより、バックアップと復元のパフォーマンスが改善し、バックアップ データの保存コストが低減し、復元に対するデータの可用性とアクセス性が向上します。バックアップ ステージは、最初に1種類のメディア(たとえば、ディスク)にデータをバックアップし、その後データを異なる種類のメディア(たとえば、テープ)にコピーすることから構成されます。

ディスク+テープへのZDB *(ZDB固有の用語)* ゼロ ダウンタイム バックアップの1つの形式。ディスクへのZDBと同様に、作成された複製が特定の時点でのソース ボリュームのバックアップとしてディスク アレイに保持されます。ただし、テープへのZDBと同様、複製データはバックアップ メディアにもストリーミングされます。このバックアップ方法を使用した場合、同じセッションでバックアップしたデータは、インスタント リカバリ、Data Protector標準のテープからの復元を使用して復元できます。スプリット ミラー アレイではスプリット ミラー復元が可能です。
「ゼロ ダウンタイム バックアップ (ZDB) 、ディスクへのZDB 、テープへのZDB 、インスタント リカバリ 、複製 、および複製セット ローテーション 。」を参照。

ディスクへのZDB *(ZDB固有の用語)* ゼロ ダウンタイム バックアップの1つの形式。作成された複製が、特定の時点でのソース ボリュームのバックアップとしてディスク アレイに保持されます。同じバックアップ仕様を使って別の時点で作成された複数の複製を、複製セットに保持することができます。テープにZDBした複製はインスタント リカバリ プロセスで復元できます。
「ゼロ ダウンタイム バックアップ (ZDB) 、テープへのZDB 、ディスク+テープへのZDB 、インスタント リカバリ 、および複製セット ローテーション 。」を参照。

ディスク検出 ディスク検出では、クライアントのバックアップ中にディスクを検出します。このときData Protectorが探索（検出）するのは、クライアント上に存在するディスクで、バックアップの構成時にシステム上に存在しなかったディスクも検出の対象に含まれます。検出されたディスクがバックアップされます。これにより、ディスクのマウントとマウント解除が頻繁に繰り返される動的な構成にも対応できます。ディスクが展開されると、それぞれのディスクがマスター クライアント オブジェクト

のオプションをすべて継承します。実行前コマンドと実行後コマンドは、1回しか指定されていなくても、オブジェクトごとに繰り返し起動されることになります。

ディスク検出によるクライアントのバックアップ
クライアントにマウントされているすべてのファイルシステムのバックアップ。バックアップの開始時に、Data Protectorがクライアント上のディスクを自動検出します。ディスク検出によるクライアント バックアップでは、バックアップ構成が単純化され、ディスクのマウント/アンマウントが頻繁に行われるシステムに対するバックアップ効率が向上されます。

ディファレンシャル バックアップ
前回のフル バックアップより後の変更をバックアップする増分バックアップ。このバックアップ タイプを実行するには、増分1バックアップ タイプを指定します。
「インクリメンタル バックアップ 。」を参照。

ディファレンシャル バックアップ
(Microsoft SQL Server固有の用語) 前回のフル データベース バックアップ以降にデータベースに対して加えられた変更のみ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 。」を参照。

ディレクトリ接合
(Windows固有の用語) ディレクトリ接合は、Windowsの再解析ポイントのコンセプトに基づいています。NTFS 5 ディレクトリ接合では、ディレクトリ/ファイル要求を他の場所にリダイレクトできます。

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が保存されます。データファイルは、1つのOracleデータベースにのみ所属できます。

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

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

データベースの並列処理(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 」を参照。

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。スプリット ミラー アレイでは、スプリット ミラー復元も使用することができます。
「ゼロ ダウンタイム バックアップ（ZDB）、ディスクへのZDB 、インスタント リカバリ 、ディスク+テープへのZDB 、および複製 。」を参照。

テーブルスペース（表領域、表スペース）

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

デバイス

ドライブまたはより複雑な装置（ライブラリなど）を格納する物理装置。

デバイス グループ

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

デバイス ストリーミング

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

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

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

同時処理数
「Disk Agentの同時処理数 」を参照。

動的（ダイナミック）クライアント
「ディスク検出によるクライアント バックアップ 。」を参照。

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

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

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

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方式では、ドライブの暗号化機能を使用します。バックアップの実行時に、メディアに書き込まれるデータとメタ データの両方がドライブによって暗号化されます。

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元できます。

トランザクション ログ ファイル
データベースを変更するトランザクションを記録するファイル。データベースが破損した場合にフォールト トレランスを提供します。

トランスポータブル スナップショット
(Microsoft VSS固有の用語) アプリケーション システム上に作成されるシャドウ コピー。このシャドウ コピーは、バックアップを実行するバックアップ システムに提供できます。
「Microsoft Volume Shadow Copy Service (VSS) 。」を参照。

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

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 タイ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 。」を参照。

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 システムのターゲット ボリュームに接続しているシステム。典型的なバックアップ システムは、バックアップ デバイスに接続され、複製内のデータのバックアップを実行します。
「アプリケーション システム 、ターゲット ボリューム 、および複製 。」を参照。

バックアップ 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（対話式セッション）こともできます。1つのバックアップ仕様の中で複数のクライアントが構成されている場合、すべてのクライアントが同じバックアップの種類（フルまたは増分）を使って、1回のバックアップ セッションで同時にバックアップされます。バックアップ セッションの結果、1式のメディア にバックアップ データが書き込まれます。これらのメディアは、バックアップ セットまたはメディア セットとも呼ばれます。
「および バックアップ仕様、 増分バックアップ、およびフルバックアップ 。」を参照。

バックアップ セット

バックアップに関連したすべての統合ソフトウェア オブジェクトのセットです。

バックアップ セット

(Oracle固有の用語) RMANバックアップ コマンドを使用して作成したバックアップファイルの論理グループ。バックアップ セットは、バックアップに関連したすべてのファイルのセットです。これらのファイルはパフォーマンスを向上するため多重化することができます。バックアップ セットにはデータファイルまたはアーカイブ ログのいずれかを含めることができますが、両方同時に使用できません。

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

バックアップAPI
Oracleのバックアップ/復元ユーティリティとバックアップ/復元メディア管理層の間にあるOracleインタフェース。このインタフェースによってルーチンのセットが定義され、バックアップ メディアのデータの読み書き、バックアップ ファイルの作成や検索、削除が行えるようになります。

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

バックアップの種類
「増分バックアップ 、差分バックアップ (differential backup) 、トランザクション バックアップ 、フル バックアップ 、および差分バックアップ 。」を参照。

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。

バックアップ仕様
バックアップ対象オブジェクトを、使用するデバイスまたはドライブのセット、仕様内のすべてのオブジェクトに対するバックアップ オプション、バックアップを行う日時とともに指定したリスト。オブジェクトとなるのは、ディスクやボリューム全体、またはその一部、たとえばファイル、ディレクトリ、Windowsレジストリなどです。インクルード リストおよびエクスクルード リストを使用して、ファイルを選択することもできます。

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

パブリック フォルダ ストア

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

パブリック/プライベート バックアップ データ

バックアップを構成する際は、バックアップ データをパブリックまたはプライベートのいずれにするかを選択できます。

- パブリック データ – すべてのData Protectorユーザーに対してアクセスと復元が許可されます。
- プライベート データ – バックアップの所有者および管理者に対してのみ表示と復元が許可されます。

未介在操作

「無人操作 。」を参照。

ファースト レベル ミラー

(HP StorageWorks Disk Array XP固有の用語) HP StorageWorks Disk Array XPでは、プライマリ ボリュームのミラー コピーを最大3つまで作成することができ、このコピー1つにつきさらに2つのコピーを作成できます。最初の3つのミラー コピーはファースト レベル ミラーと呼ばれます。「プライマリ ボリューム およびMU番号 。」を参照。

ファイバ チャネル

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

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) 作成、変更、または削除されたオブジェクトを特定するために、ファイルシステムをたどる処理。

ファイル デポ

バックアップからファイル ライブラリ デバイスまでのデータを含むファイル。

ファイル バージョン

フル バックアップや増分バックアップでは、ファイルが変更されている場合、同じファイルが複数回バックアップされます。バックアップのロギング レベルとして[すべてログに記録]を選択している場合は、ファイル名自体に対応する1つのエントリとファイルの各バージョンに対応する個別のエントリがIDB内に維持されます。

ファイル ライブラリ デバイス

複数のメディアからなるライブラリをエミュレートするディスク上に存在するデバイス。ファイル デポと呼ばれる複数のファイルが格納されます。

ファイルシステム
ハード ディスク上に一定の形式で保存されたファイルの集まり。 ファイルシステムは、ファイル属性とファイルの内容がバックアップ メディアに保存されるようにバックアップされます。

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

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

ブール演算子
オンライン ヘルプ システムの全文検索には、AND、OR、NOT、NEAR の各ブール演算子を使用できます。複数の検索条件をブール演算子で組み合わせて指定することで、検索対象をより正確に絞り込むことができます。複数単語の検索に演算子を指定しなければ、ANDを指定したものとみなされます。たとえば、「manual disaster recovery」という検索条件は、「manual AND disaster AND recovery」と同じ結果になります。

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

フェイルオーバー
(HP StorageWorks EVA固有の用語) CA+BC EVA構成におけるソースとあて先の役割を逆にする操作。
「CA+BC EVA 。」を参照。

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上（メディア ヘッダ）に保存されます。保護データがある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では、指定された順序でデバイスにアクセスします。

復元セッション
バックアップ メディアからクライアントシステムにデータをコピーするプロセス。

復元チェーン
バックアップ オブジェクトをある時点まで復元するのに必要なすべてのバックアップ。復元チェーンは、オブジェクトのフル バックアップと任意の数の関連する増分バックアップで構成されます。

複製
(ZDB固有の用語) ユーザー指定のバックアップ オブジェクトを含む、特定の時点におけるソース ボリュームのデータのイメージ。 イメージは、作成するハードウェア/ソフトウェアによって、物理ディスクレベルでの記憶ブロックの独立した正確な複製(クローン)になる（スプリットミラー、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。基本オペレーティング システムでは、バックアップ オブジェクトが含まれている完全な物理ディスクが複製されます。しかし、UNIXでボリュームマネージャを使用するときは、バックアップ オブジェクト（論理ボリューム）を含むボリュームまたはディスクグループ全体が複製されます。Windowsでパーティションが使用されている場合、選択されたパーティションが含まれている物理ボリュームが複製されます。
「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 。」を参照。

複製セット
(ZDB固有の用語) 同じバックアップ仕様を使って作成される複製のグループ。
「複製 および複製セット ローテーション 。」を参照。

複製セット ローテーション
(ZDB固有の用語) 通常のバックアップ作成のために継続的に複製セットを使用すること。複製セットの使用を必要とする同一のバックアップ仕様が実行されるたびに、新規の複製がセットの最大数になるまで作成され、セットに追加されます。その後、セット内の最も古い複製は置き換えられ、セット内の複製の最大数が維持されます。
「複製 および複製セット 。」を参照。

物理デバイス
ドライブまたはより複雑な装置（ライブラリなど）を格納する物理装置。

プライマリ ボリューム (P-VOL)
(HP StorageWorks Disk Array XP固有の用語) CA構成およびBC構成用のプライマリ ボリュームとしての役割を果たす標準のHP StorageWorks Disk Array XP LDEV。P-VOLはMCU内に配置されています。

「セカンダリ ボリューム (S-VOL) およびMain Control Unit (MCU) 。」を参照。

フラッシュ リカバリ領域

(Oracle固有の用語) フラッシュ リカバリ領域は、Oracle 10g/11gで管理されるディレクトリ、ファイル システム、または自動ストレージ管理のディスク グループです。バックアップと復旧に関するファイル(リカバリ ファイル)の中央格納領域として機能します。
「リカバリ ファイル 。」を参照。

フリー プール

フリー プールは、メディア プール内のすべてのメディアが使用中になっている場合にメディアのソースとして補助的に使用できるプールです。ただし、メディア プールでフリー プールを使用するには、明示的にフリー プールを使用するように構成する必要があります。

フル データベース バックアップ

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

フル バックアップ

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

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。

フルZDB

前回のバックアップから変更がない場合でも選択されたすべてのオブジェクトをテープにストリーミングする、テープへのZDBセッションまたはディスク+テープへのZDBセッション。
「インクリメンタルZDB 。」を参照。

分散ファイルシステム (DFS)

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

ペア ステータス

(HP StorageWorks Disk Array XP固有の用語) ミラー化されたディスクのペアは、そのペア上で実行されるアクションによって、さまざまなステータス値を持ちます。最も重要なステータス値は以下の3つです。

- コピー – ミラー化されたペアは、現在再同期中。データは一方のディスクからもう一方のディスクに転送されます。2つのディスクのデータは同じではありません。

- ペア – ミラー化されたペアは、完全に同期されており、両方のディスク（プライマリ ボリュームとミラー ボリューム）は全く同じデータを持ちます。
- 中断 – ミラー化されたディスク間のリンクは中断されています。両方のディスクが別々にアクセスされ、更新されています。ただし、ミラー関係はまだ保持されており、このペアはディスク全体を転送することなく、再同期することができます。

並行復元

1つの Media Agentからデータを受信するDisk Agentを複数実行して、バックアップ データを複数のディスクに同時に（並行して）復元すること。並行復元を行うには、複数のディスクまたは論理ボリュームに置かれているデータを選択し、同時処理数を2以上に設定してバックアップを開始し、異なるオブジェクトのデータを同じデバイスに送信する必要があります。並行復元中には、復元対象として選択した複数のオブジェクトがメディアから同時に読み取られるので、パフォーマンスが向上します。

並列処理

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。

保護

「データ保護 およびカタログ保護 。」を参照。

ホスティング 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。

ホスト バックアップ

「ディスク検出によるクライアント バックアップ 。」を参照。

ボリューム グループ

LVMシステムにおけるデータ ストレージ単位。ボリューム グループは、1つまたは複数の物理ボリュームから作成できます。同じシステム上に複数のボリューム グループを置くことができます。

ボリューム マウント ポイント

(Windows固有の用語) ボリューム上の空のディレクトリを他のボリュームのマウントに使用できるように構成したもの。ボリューム マウント ポイントは、ターゲット ボリュームへのゲートウェイとして機能します。ボリュームがマウントされていれば、ユーザーやアプリケーションがそのボリューム上のデータをフル（マージ）ファイルシステム パスで参照できます（両方のボリュームが一体化されている場合）。

マージ

復元中のファイル名競合を解決するモードの1つ。復元するファイルと同じ名前のファイルが復元先に存在する場合、変更日時の新しい方が維持されます。既存のファイルと名前が重複しないファイルは、常に復元されます。

「上書き 。」を参照。

マウント ポイント ディレクトリ構造内において、ディスクまたは論理ボリュームにアクセスするためのアクセス ポイント（/optやd:など）。UNIXでは、bdfコマンドまたはdfコマンドを使ってマウント ポイントを表示できます。

マウント要求 マウント要求時には、デバイスにメディアを挿入するように促す画面が表示されます。必要なメディアを挿入して確認することでマウント要求に応答すると、セッションが続行されます。

マジック パケット **「Wake ONLAN 。」を参照。**

マルチドライブ サーバ 単一システム上でMedia Agentを無制限に使用できるライセンス。このライセンスは、Cell ManagerのIP アドレスにバインドされており、新しいバージョンでは廃止されました。

ミラー ローテーション *(HP StorageWorks Disk Array XP固有の用語)* **「複製セット ローテーション 。」を参照。**

ミラー *(EMC SymmetrixおよびHP StorageWorks Disk Array XP固有の用語)* **「ターゲット ボリューム 。」を参照。**

無人操作 または**未介在操作** 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。

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 セット バックアップ セッションでは、メディア セットと呼ばれるメディアのグループにデータをバックアップします。メディ

アの使用法によっては、複数のセッションで同じメディアを共有できます。

メディア プール 同じ種類のメディア(DDS)などのセット。グループとして追跡されます。フォーマットしたメディアは、メディア プールに割り当てられます。

メディア ラベル メディアに割り当てられるユーザー定義の識別子。

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

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 。」を参照。

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

メディアのボールティング メディアを安全な別の場所に収納すること。メディアが復元に必要になった場合や、今後のバックアップにメディアを再使用する場合は、メディアをデータ センターに戻します。ボールティング手順は、会社のバックアップ戦略やデータ保護/信頼性ポリシーに依存します。

メディアの割り当て方針 メディアをバックアップに使用する順序を決定します。[Strict] メディア割り当てポリシーでは、特定のメディアに限定されます。[Loose] ポリシーでは、任意の適切なメディアを使用できます。[フォーマットされていないメディアを先に割り当てる] ポリシーでは、ライブラリ内に利用可能な非保護メディアがある場合でも、不明なメディアが優先されます。

メディアの使用法 ここでは、メディアの使用法として、以下のオプションのいずれかを選択します。メディアの使用法は、[追加可能]、[追加不可能]、[増分のみ追加可能]のいずれかに設定できます。

メディアの位置 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。

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

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

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 アカウントを持つユーザーのみ、Data Protectorを使用できなる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)
管理者が特権レベルの昇格を許可するまで、アプリケーション ソフトウェアの実行権限を標準ユーザーに限定するWindows Vista および Windows Server 2008 のセキュリティ コンポーネント。

ユーザー グループ
各Data Protectorユーザーは、ユーザー グループのメンバーです。各ユーザー グループには1式のユーザー権限があり、それらの権限がユーザー グループ内のすべてのユーザーに付与されます。ユーザー権限を関連付けるユーザー グループの数は、必要に応じて定義できます。ユーザー グループの例は、Admin、Operator、Userなどです。

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、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を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。

ユーザー権限
特定のData Protectorタスクの実行に必要なパーミッションをユーザー権限またはアクセス権限と呼びます。主なユーザー権限には、バックアップの構成、バックアップ セッションの開

始、復元セッションの開始などがあります。ユーザーには、そのユーザーの所属先ユーザー グループに関連付けられているアクセス権限が割り当てられます。

ライター

(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。

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archived logバックアップ セット
- データ ファイルのコピー
- アーカイブ REDO ログ
- ストアド スクリプト

リカバリ カタログ データベース

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

リカバリ カタログ データベースへのログイン情報

(Oracle固有の用語) リカバリ カタログ データベース (Oracle) へのログイン情報の形式は *<user_name>*/*<password>*@*<service>*で、ユーザー名、パスワード、サービス名の説明は、Oracleターゲット データベースへのOracle SQL*Net V2ログイン情報と同じです。ただし、この場合の*service*はOracleターゲット データベースではなく、リカバリ カタログ データベースに対するサービス名となります。
ここで指定するOracleユーザーは、Oracleのリカバリ カタログのオーナー(所有者)でなければなら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 リカバリ領域に置かれるOracle 10g/11g固有のファイルです。現在の

制御ファイル、オンライン REDO ログ、アーカイブ REDO ログ、フラッシュバック ログ、制御ファイル自動バックアップ、データファイル コピー、およびバックアップ ピースがこれにあたります。
「フラッシュ リカバリ領域 。」を参照。

リサイクル

メディア上のすべてのバックアップ データのデータ保護を解除して、以降のバックアップで上書きできるようにするプロセス。同じセッションに所属しているデータのうち、他のメディアに置かれているデータも保護解除されます。リサイクルを行っても、メディア上のデータ自体は変更されません。

リムーバブル記憶域の管理データベース

(Windows固有の用語) Windowsサービスの1つ。リムーバブル メディア (テープやディスクなど) と記憶デバイス (ライブラリ) の管理に使用されます。リムーバブル記憶域により、複数のアプリケーションが同じメディア リソースを共有できます。

ローカル復旧とリモート復旧

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

ロギング レベル

ロギング レベルは、バックアップ、オブジェクトのコピー、またはオブジェクトの集約時にファイルとディレクトリに関する情報をどの程度まで詳細にIDBに記録するかを示します。バックアップ時のロギング レベルに関係なく、データの復元は常に可能です。Data Protectorには、[すべてログに記録]、[ディレクトリ レベルまでログに記録]、[ファイル レベルまでログに記録]、および[ログなし]の4つのロギング レベルがあります。ロギング レベルの設定によって、IDBのサイズ増加、バックアップ速度、復元対象データのブラウズしやすさが影響を受けます。

ログイン ID

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

ロック名

別のデバイス名を使うことで同じ物理デバイスを違う特性で何度も構成することができます。そのようなデバイス(デバイス名)が複数同時に使用された場合に重複を防ぐ目的で、デバイス構成をロックするためにロック名が使用されます。ロック名

はユーザーが指定する文字列です。同一の物理デバイスを使用するデバイス定義には、すべて同じロック名を使用します。

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

ワイルドカード文字 1文字または複数文字を表すために使用できるキーボード文字。たとえば、通常、アスタリスク (*) は1文字以上の文字を表し、疑問符 (?) は1文字を示します。ワイルドカード文字は、名前により複数のファイルを指定するための手段としてオペレーティング システムで頻繁に使用されます。

索引

あ

お

か

く

さ

と

は

ひ

ふ