

# HP Data Protector 7.00 ディザスタリカバリガイド

HP 部品番号: N/A  
2012 年 8 月  
第 3 版



© Copyright 2006, 2012 Hewlett-Packard Development Company, L.P.

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。本書のいかなる内容も当該保証に新たに保証を追加するものではありません。HP は、本書中の技術的あるいは校正上の誤り、省略に対して責任を負いかねます。

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、Oracle および/またはその関連会社の登録商標です。

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

UNIX® は、The Open Group の登録商標です。

LiveVault® は、Autonomy Corporation plc の登録商標です。

# 目次

出版履歴.....	7
本書について.....	8
対象読者.....	8
ドキュメントセット.....	8
ガイド.....	8
ヘルプ.....	11
ドキュメントマップ.....	11
略称.....	11
対応表.....	12
統合ソフトウェア.....	12
表記上の規則および記号.....	13
Data Protector グラフィカルユーザーインターフェース.....	14
一般情報.....	14
HP テクニカルサポート.....	14
メールニュース配信サービス.....	15
HP Web サイト.....	15
<b>1 概要.....</b>	<b>16</b>
概要.....	16
ディザスタリカバリプロセス.....	17
ディザスタリカバリの方法.....	18
手動によるディザスタリカバリの方法.....	19
ディスクデリバリーによるディザスタリカバリ.....	20
ワンボタンディザスタリカバリ (OBDR).....	20
自動システム復旧 (ASR).....	20
拡張自動ディザスタリカバリ (EADR).....	21
Data Protector 統合ソフトウェアとディザスタリカバリ.....	21
<b>2 ディザスタリカバリの計画と準備.....</b>	<b>22</b>
この章の内容.....	22
計画.....	22
整合性と関連性を兼ね備えたバックアップ.....	23
整合性と関連性を兼ね備えたバックアップの作成.....	23
暗号化されたバックアップ.....	23
システム復旧データ (SRD) の更新と編集.....	24
SRD ファイルの更新ウィザードによる更新.....	24
omnisrupdate による更新.....	24
実行後スクリプトによる更新.....	25
SRD ファイルの編集.....	26
<b>3 Windows 上でのディザスタリカバリ.....</b>	<b>27</b>
Windows システムの半自動ディザスタリカバリ.....	27
概要.....	27
要件.....	27
制限事項.....	28
準備.....	28
復旧.....	30
Windows 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.....	32
概要.....	33
要件.....	33
制限事項.....	33
準備.....	33

復旧.....	34
Windows システムの拡張自動ディザスタリカバリ.....	35
概要.....	35
前提条件.....	36
制限事項.....	38
準備.....	38
DR OS イメージファイル.....	39
kb.cfg ファイル.....	41
暗号化キーの準備.....	41
フェーズ 1 開始ファイル (P1S).....	41
ディザスタリカバリ用の DR OS イメージを準備する.....	42
ディザスタリカバリイメージを準備する.....	42
復旧.....	43
Windows システムのワンボタンディザスタリカバリ.....	48
概要.....	48
前提条件.....	49
制限事項.....	50
準備.....	50
OBDR 用のバックアップ仕様を作成する.....	51
ディスクイメージバックアップを使用するために OBDR バックアップ仕様を変更する.....	53
kb.cfg ファイル.....	54
暗号化キーの準備.....	54
復旧.....	55
自動システム復旧.....	60
概要.....	60
要件.....	61
ハードウェア構成.....	61
ハードディスクドライブ.....	61
制限事項.....	61
準備.....	62
ローカルデバイス.....	64
復旧.....	64
高度な復旧作業.....	66
Microsoft Cluster Server の復元に固有の手順.....	66
考えられる状況.....	66
二次ノードのディザスタリカバリ.....	66
一次ノードのディザスタリカバリ.....	67
EADR 用に全ノードの P1S ファイルをマージ.....	68
Windows でのハードディスク署名の復元.....	69
クラスター共有ボリュームと VHD ファイルを復元する.....	70
マジョリティノードセットクラスターでの自動システム復旧.....	70
Data Protector Cell Manager 固有の復元手順.....	70
IDB の整合性をとる (すべての方法).....	70
拡張自動ディザスタリカバリに固有の手順.....	71
ワンボタンディザスタリカバリに固有の手順.....	71
自動システム復旧に固有の手順.....	72
Internet Information Server (IIS) の復元に固有の手順.....	72
トラブルシューティング.....	72
kb.cfg ファイルの編集.....	73
編集後の SRD ファイルを使用した復旧.....	73
AMDR/ASR.....	75
EADR/OBDR.....	75
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.....	76
Windows の BitLocker ドライブ暗号化でロックされたボリュームのロック解除.....	76

4 UNIX のディザスタリカバリ.....	78
HP-UX クライアントの手動によるディザスタリカバリ.....	78
概要.....	78
カスタムインストールメディアの使用.....	78
概要.....	78
準備.....	79
復旧.....	80
システム復旧ツールの使用.....	81
概要.....	81
準備.....	81
前提条件.....	81
make_tape_recovery を使用したアーカイブの作成.....	82
make_net_recovery を使用したアーカイブの作成.....	82
復旧.....	82
バックアップテープからの復旧.....	82
ネットワークからの復旧.....	83
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.....	83
概要.....	83
制限事項.....	84
準備.....	84
復旧.....	87
UNIX Cell Manager の手動でのディザスタリカバリ.....	88
概要.....	88
制限事項.....	89
準備.....	89
復旧.....	89
Linux システムの拡張自動ディザスタリカバリ.....	90
概要.....	90
要件.....	91
制限事項.....	91
準備.....	92
DR IOS イメージファイル.....	92
暗号化キーの準備.....	93
フェーズ 1 開始ファイル (P1S).....	93
DR ISO イメージの作成.....	94
復旧.....	94
Linux システムのワンボタンディザスタリカバリ.....	96
概要.....	96
要件.....	97
制限事項.....	98
準備.....	98
OBDR バックアップ.....	98
暗号化キーの準備.....	99
復旧.....	100
Linux システムでの高度な復旧作業.....	101
Data Protector Cell Manager 固有の復元手順.....	101
IDB の整合性をとる (すべての方法).....	102
拡張自動ディザスタリカバリに固有の手順.....	102
ワンボタンディザスタリカバリに固有の手順.....	103
編集後の SRD ファイルを使用した復旧.....	103
5 ディザスタリカバリのトラブルシューティング.....	106
この章の内容.....	106
作業を開始する前に.....	106
一般的なトラブルシューティング.....	106

AUTODR.log ファイル.....	106
ディザスタリカバリセッションのデバッグ.....	107
ディザスタリカバリ中の omnirc オプションの設定.....	109
Windows システムでの drm.cfg ファイル.....	109
共通の問題.....	110
Windows システム上の問題.....	110
半自動ディザスタリカバリ.....	112
ディスクデリバリーによるディザスタリカバリ.....	112
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.....	113
EADR および OBDR の共通の問題.....	113
Windows システム上の問題.....	115
Windows Itanium システム上の問題.....	116
Linux システム上の問題.....	117
自動システム復旧.....	117
<b>A 詳細情報.....</b>	<b>119</b>
抹消リンクの移動 (HP-UX 11.x).....	119
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.....	119
<b>B 異なるハードウェアへの復旧.....</b>	<b>121</b>
異なるハードウェアの復旧が必要になる場合.....	121
概要.....	121
要件.....	122
制限事項.....	122
ドライバ.....	123
準備.....	123
復旧.....	124
システムの復元.....	124
OS の復元と準備.....	124
ネットワークマッピングの修正.....	125
OS を正常に復元した後.....	125
ユーザーデータとアプリケーションデータの復元.....	125
<b>用語集.....</b>	<b>126</b>
<b>索引.....</b>	<b>160</b>

## 出版履歴

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

**表 1 出版履歴**

製品番号	ガイド版	製品
B6960-96038	2008 年 11 月	Data Protector リリース A.06.10
B6960-90154	2009 年 9 月	Data Protector リリース A.06.11
N/A	2011 年 3 月	Data Protector リリース 6.20
N/A	2012 年 3 月	Data Protector リリース 7.00
N/A	2012 年 4 月	Data Protector リリース 7.00
N/A	2012 年 7 月	Data Protector リリース 7.00(次のいずれかのパッチバンドルを含む):DPWINBDL_00701、DPUXBDL_00701、DPLNXBDL_00701

# 本書について

本書では、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

その他のガイドおよびヘルプには、関連情報が記載されています。

## ガイド

Data Protector のガイドは、電子的な PDF 形式で提供されます。PDF ファイルは、Data Protector のセットアップ時に、Windows の場合は英語のドキュメント（ガイド、ヘルプ）コンポーネントを、UNIX の場合は OB2-DOCS コンポーネントを、それぞれ選択してインストールします。ガイドのインストール後の保存先ディレクトリは、

`Data_Protector_home\docs(Windows)` または `/opt/omni/doc/C(UNIX)` です。

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

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

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

- 『HP Data Protector コンセプトガイド』  
このガイドでは、Data Protector のコンセプトを解説するとともに、Data Protector の動作原理を詳細に説明しています。これは、タスクごとのヘルプとともに使用するように作成されています。
- 『HP Data Protector インストールおよびライセンスガイド』  
このガイドでは、Data Protector ソフトウェアのインストール方法をオペレーティングシステムおよび環境のアーキテクチャごとに説明しています。また、Data Protector のアップグレード方法や、環境に適したライセンスの取得方法についても説明しています。
- 『HP Data Protector トラブルシューティングガイド』  
このガイドでは、Data Protector の使用中に起こりうる問題に対するトラブルシューティングの方法について説明します。
- 『HP Data Protector ディザスタリカバリガイド』  
このガイドでは、ディザスタリカバリの計画、準備、テスト、および実行の方法について説明します。

- 『HP Data Protector インテグレーションガイド』  
 このガイドでは、さまざまなデータベースやアプリケーションをバックアップおよび復元するための、Data Protector の構成方法および使用法を説明します。このガイドは、バックアップ管理者やオペレータを対象としています。6 種類のガイドがあります。
  - 『HP Data Protector インテグレーションガイド - Microsoft アプリケーション: SQL Server、SharePoint Server、Exchange Server』  
 このガイドでは、Microsoft SQL Server、Microsoft SharePoint Server、Microsoft Exchange Server といった Microsoft アプリケーションに対応する Data Protector の統合ソフトウェアについて説明します。
  - 『HP Data Protector インテグレーションガイド - Oracle、SAP』  
 このガイドでは、Oracle Server、SAP R/3、SAP MaxDB に対応する Data Protector の統合ソフトウェアについて説明します。
  - 『HP Data Protector インテグレーションガイド - IBM アプリケーション: Informix、DB2、Lotus Notes/Domino』  
 このガイドでは、Informix Server、IBM DB2 UDB、Lotus Notes/Domino Server といった IBM アプリケーションに対応する Data Protector の統合ソフトウェアについて説明します。
  - 『HP Data Protector インテグレーションガイド - Sybase、Network Node Manager、Network Data Management Protocol Server』  
 このガイドでは、Sybase Server、HP Network Node Manager、Network Data Management Protocol Server に対応する HP の統合ソフトウェアについて説明します。
  - 『HP Data Protector インテグレーションガイド - 仮想環境』  
 このガイドでは、Data Protector と仮想環境 (VMware 仮想インフラストラクチャ、VMware vSphere、VMware vCloud Director、Microsoft Hyper-V、および Citrix XenServer) との統合について説明します。
  - 『HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service』  
 このガイドでは、Data Protector と Microsoft ポリウムシャドウコピーサービスの統合について説明します。また、ドキュメントアプリケーションライターの詳細についても説明します。
- 『HP Data Protector Integration Guide for HP Operations Manager for UNIX』  
 このガイドでは、UNIX 版の HP Operations Manager と HP Service Navigator を使用して、Data Protector 環境の健全性と性能を監視および管理する方法について説明します。
- 『HP Data Protector Integration Guide for HP Operations Manager for Windows』  
 このガイドでは、Windows 版の HP Operations Manager を使用して、Data Protector 環境の健全性と性能を監視および管理する方法について説明します。
- 『HP Data Protector ゼロダウンタイムバックアップコンセプトガイド』  
 このガイドでは、Data Protector ゼロダウンタイムバックアップとインスタントリカバリのコンセプトについて解説するとともに、ゼロダウンタイムバックアップ環境における Data Protector の動作原理を詳細に説明します。手順を中心に説明している『HP Data Protector ゼロダウンタイムバックアップ管理者ガイド』および『HP Data Protector ゼロダウンタイムバックアップインテグレーションガイド』とあわせてお読みください。
- 『HP Data Protector ゼロダウンタイムバックアップ管理者ガイド』  
 このガイドでは、HP P4000 SAN ソリューション、HP P6000 EVA ディスクアレイファミリ、HP P9000 XP ディスクアレイファミリ、HP P10000 Storage Systems、EMC Symmetrix

Remote Data Facility および TimeFinder に対応する Data Protector 統合ソフトウェアの構成方法および使用方法を説明します。このガイドは、バックアップ管理者やオペレータを対象としています。ファイルシステムとディスクイメージのゼロダウンタイムバックアップ、インスタントリカバリ、および復元についても説明します。

- 『HP Data Protector ゼロダウンタイムバックアップインテグレーションガイド』  
このガイドでは、Oracle Server、SAP R/3、Microsoft Exchange Server、Microsoft SQL Server の各データベースに対して、そのゼロダウンタイムバックアップ、インスタントリカバリ、標準復元を実行するための Data Protector の構成方法および使用方法について説明します。
- 『HP Data Protector Granular Recovery Extension User Guide for Microsoft Exchange Server』  
このガイドでは、Microsoft Exchange Server 2010 環境用の Granular Recovery Extension を構成し使用する方法について説明します。Microsoft Exchange Server 用の Data Protector Granular Recovery Extension のグラフィカルユーザーインターフェースは、Microsoft 管理コンソールに組み込まれます。このガイドは、Microsoft Exchange Server 管理者および Data Protector バックアップ管理者を対象としています。
- 『HP Data Protector Granular Recovery Extension ユーザーガイド - Microsoft SharePoint Server』  
このガイドでは、Microsoft SharePoint Server 用に Data Protector Granular Recovery Extension を構成し使用する方法について説明します。Data Protector Granular Recovery Extension は Microsoft SharePoint Server のサーバーの全体管理に組み込まれ、個々のアイテムをリカバリできるようになります。このガイドは、Microsoft SharePoint Server 管理者および Data Protector バックアップ管理者を対象としています。
- 『HP Data Protector Granular Recovery Extension User Guide for VMware vSphere』  
このガイドでは、VMware vSphere 用 Data Protector Granular Recovery Extension の構成方法および使用方法について説明します。Data Protector Granular Recovery Extension は VMware vCenter Server に組み込まれ、個々のアイテムをリカバリできるようになります。このガイドは、VMware vCenter Server ユーザーおよび Data Protector バックアップ管理者を対象としています。
- 『HP Data Protector Media Operations User Guide』  
このガイドは、システムの保守とバックアップを担当するネットワーク管理者を対象に、オフラインストレージメディアの追跡と管理に関する情報を提供します。アプリケーションのインストールと構成、日常のメディア操作、およびレポート作成のタスクについて説明します。
- 『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』  
このガイドでは、HP Data Protector 7.00 の新機能について説明しています。また、インストール要件、必要なパッチ、制限事項、報告されている問題とその回避方法などの情報も記載されています。
- 『HP Data Protector Product Announcements, Software Notes, and References for Integrations to HP Operations Manager』  
このガイドは、HP Operations Manager 統合ソフトウェアに対して同様の機能を果たします。
- 『HP Data Protector Media Operations Product Announcements, Software Notes, and References』  
このマニュアルは、Media Operations に対して同様の機能を果たします。
- 『HP Data Protector Command Line Interface Reference』  
このガイドでは、Data Protector コマンドラインインターフェース、コマンドオプション、使用方法を、基本コマンドラインの例とともに説明しています。

## ヘルプ

Data Protector は、Windows および UNIX の各プラットフォーム用にヘルプトピックとコンテキスト依存ヘルプ (F1 キー) を備えています。

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

**Windows システムの場合:** DP\_help.chm を開きます。

**UNIX システムの場合:** 圧縮された tar ファイル DP\_help.tar.gz をアンパックし、DP\_help.htm 経由でヘルプシステムにアクセスします。

## ドキュメントマップ

### 略称

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

略称	ドキュメント項目
CLI	Command Line Interface Reference
Concepts	コンセプトガイド
DR	ディザスタリカバリガイド
GS	スタートガイド
GRE-Exchange	Granular Recovery Extension User Guide for Microsoft Exchange Server
GRE-SPS	Granular Recovery Extension ユーザーガイド - Microsoft SharePoint Server
GRE-VMware	Granular Recovery Extension User Guide for VMware vSphere
Help	ヘルプ
IG-IBM	インテグレーションガイド - IBM アプリケーション: Informix、DB2、Lotus Notes/Domino
IG-MS	インテグレーションガイド - Microsoft アプリケーション: SQL Server、SharePoint Server、Exchange Server
IG-O/S	インテグレーションガイド - Oracle、SAP
IG-OMU	Integration Guide for HP Operations Manager for UNIX
IG-OMW	Integration Guide for HP Operations Manager for Windows
IG-Var	インテグレーションガイド - Sybase、Network Node Manager、Network Data Management Protocol Server
IG-VirtEnv	インテグレーションガイド - 仮想環境
IG-VSS	Integration Guide for Microsoft Volume Shadow Copy Service
Install	インストールおよびライセンスガイド
MO-GS	Media Operations Getting Started Guide
MO-PA	Media Operations Product Announcements, Software Notes, and References
MO-UG	Media Operations User Guide
PA	製品案内、ソフトウェアノートおよびリファレンス
Trouble	トラブルシューティングガイド
ZDB-Admin	ZDB 管理者ガイド

略称	ドキュメント項目
ZDB-Concept	ZDB コンセプトガイド
ZDB-IG	ZDB インテグレーションガイド

## 対応表

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

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

## 統合ソフトウェア

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

ソフトウェアアプリケーション	ガイド
HP Network Node Manager(NNM)	IG-Var
HP Operations Manager	IG-OMU、IG-OMW
IBM DB2 UDB	IG-IBM
Informix Server	IG-IBM
Lotus Notes/Domino Server	IG-IBM
Media Operations	MO-UG
Microsoft Exchange Server	IG-MS、ZDB IG、GRE-Exchange
Microsoft Hyper-V	IG-VirtEnv
Microsoft SharePoint Server	IG-MS、ZDB-IG、GRE-SPS
Microsoft SQL Server	IG-MS、ZDB-IG

ソフトウェアアプリケーション	ガイド
Microsoft ボリュームシャドウコピーサービス (VSS)	IG-VSS
ネットワークデータ管理プロトコル (NDMP) サーバー	IG-Var
Oracle Server	IG-O/S、ZDB-IG
SAP MaxDB	IG-O/S
SAP R/3	IG-O/S、ZDB-IG
Sybase Server	IG-Var
VMware vSphere	IG-VirtEnv、GRE-VMware
VMware vCloud Director	IG-VirtEnv

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

ディスクアレイファミリ	ガイド
EMC Symmetrix	すべての ZDB
HP P4000 SAN ソリューション	ZDB-Concept、ZDB-Admin、IG-VSS
HP P6000 EVA ディスクアレイファミリ	すべての ZDB、IG-VSS
HP P9000 XP ディスクアレイファミリ	すべての ZDB、IG-VSS
HP P10000 Storage Systems	ZDB-Concept、ZDB-Admin、IG-VSS

## 表記上の規則および記号

表 2 表記上の規則

規則	要素
青色のテキスト:「表記上の規則」 (13 ページ)	クロスリファレンスリンクおよび電子メールアドレス
青色の下線付きテキスト: <a href="http://www.hp.com">http://www.hp.com</a>	Web サイトアドレス
<b>太字</b> テキスト	<ul style="list-style-type: none"> <li>押すキー</li> <li>ボックスなど GUI 要素に入力するテキスト</li> <li>メニュー、リストアイテム、ボタン、タブ、およびチェックボックスなどクリックまたは選択する GUI 要素</li> </ul>
<b>斜体</b> テキスト	テキスト強調
等幅テキスト	<ul style="list-style-type: none"> <li>ファイルおよびディレクトリ名</li> <li>システム出力</li> <li>コード</li> <li>コマンド、引数、および引数の値</li> </ul>
等幅、斜体テキスト	<ul style="list-style-type: none"> <li>コード変数</li> <li>コマンド変数</li> </ul>
等幅、太字テキスト	強調された等幅テキスト

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

① **重要:** 詳細情報または特定の手順を示します。

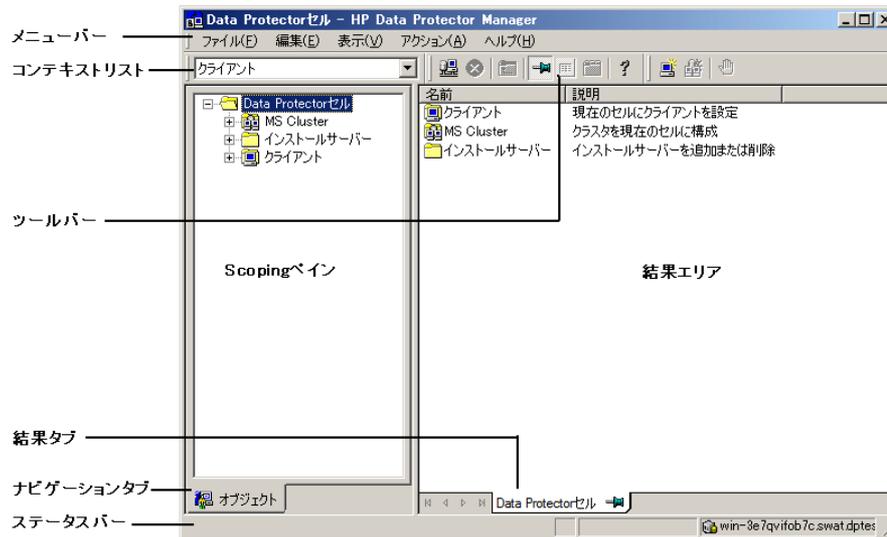
**注記:** 補足情報を示します。

💡 **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ーフェース

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ーフェースを提供します。オリジナルの Data Protector GUI (Windows のみ) または Data Protector Java GUI を使用できます。Data Protector グラフィカルユーザーインターフェースに関する詳細は、『HP Data Protector ヘルプ』を参照してください。

図 1 Data Protector グラフィカルユーザーインターフェース



## 一般情報

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

## HP テクニカルサポート

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

<http://www.hp.com/support>

HP に問い合わせる前に、以下の情報を集めておいてください。

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

## メールニュース配信サービス

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

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

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

## HP Web サイト

その他の情報については、次の HP Web サイトを参照してください。

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

# 1 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、人為的ミス、ハードウェアまたはソフトウェア障害、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、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、その他のユーザー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。影響を受け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に必要なファイルを含むパーティションを示します。

**ホストシステム**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。

**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 の実行可能ファイルがインストールされているボリューム
- IDB があるボリューム (Cell Manager のみ)

**注記:** IDB が複数のボリューム上にある場合は、IDB があるすべてのボリュームがクリティカルボリュームになります。

CONFIGURATION も Windows システムと Linux 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。

Windows では、サービスは、CONFIGURATION の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

Linux では、CONFIGURATION オブジェクトに含まれるのは、自動ディザスタリカバリ方式を実行するために Data Protector に必要なデータ構造だけです。

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

**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 (ネットワーク問題や 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**計画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。

- オペレーティングシステムと、Data Protector を含む環境を定義するすべての構成情報が(元どおりに)フェーズ 2 で復元されます。
- 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(フェーズ 3) が可能となります。

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方法のリストについては、最新のサポート一覧 (<http://support.openview.hp.com/selfsolve/manuals>) を参照してください。

**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。

「ディザスタリカバリの方法に関する概要」(18 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
<b>手動によるディザスタリカバリ</b>			
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 の標準復元手順を使用して、ユーザーデータおよび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」(27 ページ) または 「UNIX Cell Manager の手動でのディザスタリカバリ」(88 ページ) を参照してください。			
<b>ディスクデリバリーによるディザスタリカバリ (DDDR)</b>			
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)。	<b>Windows システムの場合:</b> 交換ディスクをホストシステムに接続します。 <b>UNIX システムの場合:</b> 補助ディスクをターゲットシステムに接続します。 <b>すべてのシステム:</b> 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。	<b>Windows システムの場合:</b> 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ト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。 <b>UNIX システムの場合:</b> 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。 <b>すべてのシステム:</b> システムを再起動します。 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 の標準復元手順を使用して、ユーザーデータおよび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ディザスタリカバリ」(32 ページ) または 「UNIX Cell Manager の手動でのディザスタリカバリ」(88 ページ) を参照してください。			
<b>拡張自動ディザスタリカバリ (EADR)</b>			
フルクライアントバックアップ、IDB バックアップ	DR CD または USB ドライブからシステムを	クリティカルボリュームの自動復元。	Data Protector の標準復元手順を使用して、ユー

**表 3 ディザスタリカバリの方法に関する概要 (続き)**

フェーズ 0	フェーズ 1	フェーズ 2	フェーズ 3
アップ (Cell Manager のみ)。SRD を準備して更新します。DR OS イメージを準備します。	ブートし、復旧範囲を選択します。	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。	ザーデータおよび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」 (35 ページ) または 「Linux システムの拡張自動ディザスタリカバリ」 (90 ページ) を参照してください。			
<b>ワンボタンディザスタリカバリ (OBDR)</b>			
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 の標準復元手順を使用して、ユーザーデータおよび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」 (48 ページ) または 「Linux システムのワンボタンディザスタリカバリ」 (96 ページ) を参照してください。			
<b>自動システム復旧 (ASR)</b>			
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 パ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 の標準復元手順を使用して、ユーザーデータおよび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」 (60 ページ) を参照してください。			

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。「高度な復旧作業」 (66 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、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、影響を受け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、ホスト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働させたまま、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ディザスタリカバリ」 (32 ページ) を参照してください。

## 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) は、Windows クライアント、Linux クライアント、Cell Manager を対象とする Data Protector の自動化されたリカバリ方法で、ユーザーの操作が最小限に抑えられています。

OBDR では、オペレーティングシステム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バックされ、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を行い、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。

- ① **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 (ASR)

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` 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) は、Windows クライアント、Linux クライアント、Cell Manager を対象とする Data Protector の自動化されたリカバリ方法で、ユーザーの操作が最小限に抑えられています。

EADR の手順では、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。障害発生時には、EADR ウィザードを使用して、バックアップメディアから DR OS イメージを復元し (フルバックアップ中に Cell Manager に保存されていない場合)、**ディザスタリカバリ CD ISO イメージ** に変換することができます。次に、任意の CD 書き込みツールを使用して、ディザスタリカバリ CD ISO イメージを CD に書き込むことができます。または、DR OS イメージを USB ドライブに保存できます。

CD または USB ドライブからターゲットシステムをブートすると、Data Protector で DR OS が自動的にインストールおよび構成されます。ディスクのフォーマットとパーティション作成も自動的に実行され、最終的に、オリジナルシステムが Data Protector とともにバックアップ時の状態に復旧されます。

- ① **重要:** ハードウェア、ソフトウェア、または構成を変更するたびに、新たにバックアップを実行して新しい DR OS イメージを準備します。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計画と準備

### 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 システムの場合:

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

##### Windows および Linux システムの場合:

- **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、影響を受けたシステムを復旧します。

- △ **注意:** ディザスタリカバリ用に用意されたシステムで、デフォルトの `Inet` リッスンポートを変更しないでください。変更すると、システムに障害が発生した場合、ディザスタリカバリプロセスが失敗することがあります。

## 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起動直後に開始します (実行レベル 2)。このような初期プロセスは、実行時にデータをメモリーに読み込み、「ダーティフラグ」をファイルに書き込むこともあります。そのため、標準的な動作ステージ (標準実行レベル 4) で実行されたバックアップでは、こうしたアプリケーションのスムーズな再開は期待できません。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働できるのは、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。

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、『HP Data Protector 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 OS 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 または Linux の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 (UTF-16) 形式のテキストファイルです。SRD ファイルは、Windows クライアントまたは Linux クライアントで 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/`

- ① **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 クライアントまたは Linux クライアントでのみ更新できます。更新された SRD ファイルの名前は、`recovery.srd` となります。

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 (Windows の場合のみ)
- `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用して Windows クライアントで SRD ファイルを更新するには、以下の手順を行います。

1. [Data ProtectorManager] 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。

- ① **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」(33 ページ) を参照してください。

### 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 (Windows) または `/opt/omni/bin` ディレクトリ (UNIX) 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」 \(33 ページ\)](#) を参照してください。

どのホスト名を対象として Cell Manager の SRD ファイルを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 `02.05.11-5` 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 02.05.11-5 -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」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」 \(73 ページ\)](#) を参照してください。

- 
- ① **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。サポートされるオペレーティングシステムの詳細は、<http://support.openview.hp.com/selfsolve/manuals> にある最新のサポート一覧を参照してください。

### 概要

Windows クライアントのディザスタリカバ리를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、オリジナルの記憶データ構造を再確立します。

**注:** **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` 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、システムを再起動する必要があります。
- c. Cell Manager の復旧作業が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。詳細は、「高度な復旧作業」(66 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、オリジナル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。これには、SCSI の BIOS 設定 (セクターの再マッピング) 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行う前に、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](#)」(22 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、フロッピーディスクからシステムを起動する標準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. 影響を受け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は、TCP/IP プロパティ情報 (IPv4 の場合は IP アドレス、デフォルトゲートウェイ、サブネットマスクおよび DNS 順序、IPv6 の場合はサブネットプレフィックスの長さ、優先サーバーおよび代替 DNS サーバー) が必要です。
  - クライアントプロパティ (ホスト名、ドメイン)
4. 以下の条件が当てはまることを確認します。
  - 有効なフルクライアントバックアップイメージがある。『HP Data Protector 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」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](#)」(24 ページ) を参照してください。
  - Cell Manager を復旧する場合は、有効な IDB バックアップイメージが必要です。IDB バックアップの構成方法および実行方法の詳細は、『HP Data Protector ヘルプ』の索引キーワード「IDB、構成」を参照してください。
  - Microsoft Cluster Server の整合性のあるバックアップイメージの内容を次に示します。
    - 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](#)」(66 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 ビットプラットフォームで実行する Windows システムについては、  
*Data\_Protector\_program\_data\Depot\DRSetup*(Windows Server 2008 の場合)、  
*Data\_Protector\_home\Depot\DRSetup* (その他の Windows システムの場合)、または  
*\i386\tools\DRSetup* (Data Protector インストール用メディアの場合) の内容を、3  
枚のフロッピーディスク (**drsetup ディスケット**) にコピーします。AMD64/Intel-EM64T  
プラットフォームで実行する Windows システムについては、  
*Data\_Protector\_program\_data\Depot\DRSetupx8664*(Windows Server 2008 の場  
合)、*Data\_Protector\_home\Depot\DRSetupx8664*(その他の Windows システムの場  
合)、または *\i386\tools\DRSetupx8664*(Data Protector インストール用メディアの場  
合) の内容を、4 枚のフロッピーディスクにコピーします。Itanium プラットフォームで実  
行する Windows システムについては、  
*Data\_Protector\_program\_data\Depot\DRSetup64*(Windows Server 2008 の場合)、  
*Data\_Protector\_home\Depot\DRSetup64*(その他の Windows システムの場合)、また  
は *\i386\tools\DRSetup64*(Data Protector インストール用メディアの場合) の内容を、  
6 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、影響を受けたクライア  
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、影響を受けたクライアントの更  
新された SRD ファイルを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](#)」(119 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 Vista
IPv4 用の TCP/IP 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
IPv6 用の TCP/IP プロパティ	IP アドレス	fb43:1234:5678:abcd::9:1000
	サブネットプレフィックスの長さ	64
	デフォルトゲートウェイ	fb43:1234:5678:abcd::9:1004
	優先度の高い DNS サーバー	fb43:1234:5678:abcd::9:1004
	代替 DNS サーバー	fb43:1234:5678:abcd::9:1005
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	

## 復旧

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」(66 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。詳細については、「Internet Information Server (IIS) の復元に固有の手順」(72 ページ) を参照してください。

- ① **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 `%SystemDrive%\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。
- 障害発生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 EUP 情報に基づいて、「ダミー」の FAT パーティションを作成し (障害発生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。詳細については、「準備」(33 ページ) を参照してください。
  - 障害発生前のシステム上に EUP がなかった場合は、障害発生前の状態になるようブートパーティションを作成し (障害発生により失われた場合)、フォーマットします。詳細については、「準備」(33 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 が使用されていなかった場合は、次の情報を設定して、障害発生前と同様に TCP/IP プロトコルを構成します。影響があったクライアントのホスト名、IP アドレス、デフォルトゲートウェイ、サブネットマスク、および DNS サーバー。[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 のセットアップ中に 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。『HP Data Protector ヘルプ』の索引キーワード「Data Protector ユーザーの追加」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」(73 ページ) を参照してください。
7. `Data_Protector_home\Depot\drsetup\Disk1`(Windows Cell Manager) または `\i386\tools\drsetup\Disk1`(Data Protector インストール用メディア) のいずれかのディレクトリから `drstart` 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」(28 ページ) を参照)、`drstart` コマンドを実行することもできます。
8. `drstart` は、まず現在の作業ディレクトリ、フロッピーディスク、CD-ROM 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\O2DR` 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 のインストール元] テキストボックスにパスを入力するか、ブラウザ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 omnica.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 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 ファイルのパス] 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 4**で追加した一時ユーザーアカウント **Data Protector** を Cell Manager 上の Data ProtectorAdmin 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. システムを再起動し、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](#)」 (70 ページ) および「[高度な復旧作業](#)」 (66 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。
  - 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 [デバッグ] 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。

サポートされるオペレーティングシステムの詳細は、<http://support.openview.hp.com/selfsolve/manuals> にある最新のサポート一覧を参照してください。



**ヒント:** この方法では、電源を切らずにシステムを稼働させたまま、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。

## 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. ホスト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。
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. ホスト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。

## 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: 両方のシステムで同じアドレス モードの使用が必要: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行う前に、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](#)」(22 ページ) も参照してください。

- ① **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

- 問題のある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、影響を受け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必要があります。

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

「半自動ディザスタリカバリ準備用テンプレートの例」(30 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」(119 ページ)を参照してください。

## 復旧

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」(66 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) を使用して、影響を受け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上の影響を受け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。
- 
- ① **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. Data Protector の標準復元手順を使用して、ユーザーデータおよびアプリケーションデータを復元します。これでクライアントの復旧は完了です。

ディスクデリバリーは、マルチブートシステムのディスクのうち 1 つで障害が発生したときに、ユーザーが少なくとも 1 つの構成をブートできる場合にも、有効な手段になります。

**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 システムの拡張自動ディザスタリカバリ

Data Protector には、WindowsCell 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。サポートされるオペレーティングシステムの詳細は、<http://support.openview.hp.com/selfsolve/manuals> にある最新のサポート一覧を参照してください。

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、拡張自動ディザスタリカバリウィザードで、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、ブート可能 USB ドライブに保存するか、ブート可能ネットワークイメージを作成します。CD ISO イメージは、任意の CD 記録ツールを使用して CD に記録し、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。

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。

- ① **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、DR OS データを格納している USB ドライブ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

- フルクライアントバックアップを実行します。
- 拡張自動ディザスタリカバリウィザードを使用して、影響を受けたシステムの DR OS イメージファイルから DR CD ISO イメージを作成し、CD に記録します。Windows Vista、Windows 7、Windows Server 2008 システムの場合、ディザスタリカバリ CD の代わりに DR OS イメージを持つブート可能 USB ドライブ、またはブート可能ネットワークイメージを作成できます。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、拡張自動ディザスタリカバリウィザードでは、バックアップメディアからイメージが復元されます。

- ① **重要:** ハードウェア、ソフトウェア、または構成を変更するたびに、バックアップを実行して新しい DR OS イメージ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、ネットワークを変更した場合にも当てはまります。

- 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

- 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 または USB ドライブから、あるいはネットワーク経由でターゲットシステムを起動し、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。

- ① **重要:** ドメインコントローラを復旧する場合、ディザスタリカバリウィザードが表示される前に、標準的な Windows ログオンダイアログボックスが表示され、ディレクトリサービス復元モードの管理アカウントのユーザー名 (Administrator) とパスワードの入力が求められます。

### 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. Data Protector の標準復元手順を使用して、ユーザーデータおよびアプリケーションデータを復元します。

- ① **重要:** 最初に復元する必要が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、DR OS イメージを持つディザスタリカバリ CD またはブート可能 USB ドライブ、あるいはネットワークブート可能イメージを前もって準備します。

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」](#) (66 ページ) も参照してください。

## 前提条件

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システムと、DR OS 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。詳細は、『HP Data Protector インストールおよびライセンスガイド』を参照してください。
- ターゲットシステムのハードウェア構成は、オリジナル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。これには、SCSI の BIOS 設定 (セクターの再マッピング) 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必要があります。
- 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」](#) (73 ページ) を参照してください。
- 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 規格で定義されている起動可能 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 アドレッシングによるハードディスクドライブへの読み取り/書き込みアクセスをサポートしている必要があります。BIOS のオプションは、システムของผู้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。
- 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 500MB で十分ですが、オペレーティングシステムによっては 1GB が必要になることもあります。
- クラスタ環境では、各クラスターノードのバスアドレス一覧が同じであれば、クラスターノードは正常にバックアップできます。これには、以下のものが重要です。
  - 同等のクラスター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。
- オペレーティングシステムは、バックアップ時にアクティブ化する必要があります。そうでない場合は、アクティベーション期間が期限切れになったときにディザスタリカバリは失敗します。
- Windows Vista、Windows 7、または Windows Server 2008 システム用の DR OS 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適切なバージョンの Windows Automated Installation Kit (WAIK) をインストールしておく必要があります。

#### **Windows Vista および Windows Server 2008:**

Windows Vista SP1 および Windows Server 2008 用の自動インストールキット (AIK)

#### **Windows 7 および Windows Server 2008 R2:**

- Windows Automated Installation Kit (AIK) for Windows 7
- Windows Automated Installation Kit (AIK) Supplement for Windows 7 SP1 (Microsoft Windows 7 SP1 および Windows Server 2008 R2 SP1 用は、オプション)
- ブート可能 USB デバイスからの災害復旧の場合、USB ストレージデバイスの推奨最小サイズは 256 MB です。
- ブート可能 USB デバイスからの災害復旧の場合、ターゲットシステムは USB デバイスからのブートをサポートする必要があります。古いシステムの場合、BIOS のアップデートが必要であったり、USB ストレージデバイスからのブートができない場合があります。
- Windows Vista、Windows 7、または Windows Server 2008 システム用にブート可能ネットワークイメージを作成するには、次の要件を満たす必要があります。
  - ターゲットシステムで、ネットワークアダプタが PXE プロトコルを介して通信できる。このシステムの BIOS は PXE プロトコルに準拠すること。
  - Windows Deployment Services (WDS) サーバーを、Windows Vista、Windows 7、または Windows Server 2008 システム上にインストールし、構成している。WDS サーバーが、Active Directory のメンバであるか、Active Directory ドメインのドメインコントローラのメンバである必要がある。
  - アクティブ範囲にある DNS サーバーと DHCP サーバーがネットワーク内で実行されている。
- Windows Vista、Windows 7 または Windows Server 2008 システム上にある IIS 構成オブジェクトをバックアップするには、IIS 6 Metabase Compatibility パッケージをインストールしてください。

## 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、影響を受け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 のブートルoader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。
- ブート可能 USB ドライブは、(サポートされているすべてのプラットフォーム上の) Windows 7 と Windows Server 2008 R2 システム、および (Itanium プラットフォーム上の) Windows Server 2008 システムでのみ作成することができます。
- USB デバイスからのブートをサポートしていないシステムの災害復旧を実行すると、USB デバイスがこのシステムに接続できなくなります。
- DR OS イメージのあるブート可能 USB ドライブの作成は、オリジナルの GUI またはコマンドライン (omniusb コマンドを使用) でのみ可能です。
- SAN ブートまたは SAN マルチパス構成の復旧はサポートされていません。
- 論理ボリュームの VSS ディスクイメージバックアップをディザスタリカバリに使用できるのは、Windows Vista、Windows 7、および Windows Server 2008 システムのみです。Java GUI では、ディスクイメージオブジェクトのブラウジングをサポートしていません。この機能についてはオリジナルの GUI を使用してください。
- ネットワーク上のターゲットシステムのブートは、Windows Vista、Windows 7、および Windows Server 2008 システムでのみ実行できます。この機能をサポートしているのは、オリジナルの HP Data Protector GUI のみです。
- HP Data Protector ディザスタリカバリ GUI は、Windows Vista、Windows 7、および Windows Server 2008 システム上でのみ使用できます。他の Windows システムでは、コンソールインタフェースを使用できます。
- Windows Vista、Windows 7、および Windows Server 2008 システムの場合、元々の暗号化されたフォルダを非暗号化フォルダとしてのみ復元できます。

## 準備

この項で挙げられている手順を行う前に、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](#)」(22 ページ)も参照してください。「[高度な復旧作業](#)」(66 ページ)も参照してください。

- ① **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。

## 前提条件

- クライアントシステムのフルバックアップを実行します (CONFIGURATION オブジェクトも含む)。フルクライアントバックアップでは、バックアップ仕様を作成する際に以下のいずれかを選択できます。
  - クライアントシステム全体
  - IDB と構成オブジェクト、およびクライアントシステム上にマウントする各ボリューム

---

**注記:** Windows Vista、Windows 7、および Windows Server 2008 システムでは、論理ボリュームをバックアップするために VSS ライターを使用することでディスクイメージのバックアップを使用できます。IDB と構成オブジェクト、および NTFS フォルダとしてマウントされていない、あるいはマウントされているボリュームは、ファイルシステムのバックアップを使用することでバックアップする必要があります。VSS ディスクイメージのバックアップでは、バックアップ中のボリュームがロック解除されたままの状態、他のアプリケーションからアクセスできます。

---

**Windows 7 および Windows Server 2008 R2:**必ずシステムボリュームをバックアップしてください。

『HP Data Protector ヘルプ』の索引「バックアップ、Windows 固有」および「バックアップ、構成」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」 \(66 ページ\)](#) を参照してください。

- **クラスター共有ボリューム:**クライアントシステムのフルバックアップを実行する前に、まず Data Protector 仮想環境用統合ソフトウェアを使用して仮想ハードディスク (VHD) ファイルおよび CSV 構成データをバックアップしてください。『HP Data Protector インテグレーションガイド - 仮想環境』を参照してください。
- 一貫性を確保するには、仮想ハードディスク (VHD) をアンマウントする必要があります。

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。その手順については、[「EADR 用に全ノードの P1S ファイルをマージ」 \(68 ページ\)](#) を参照してください。

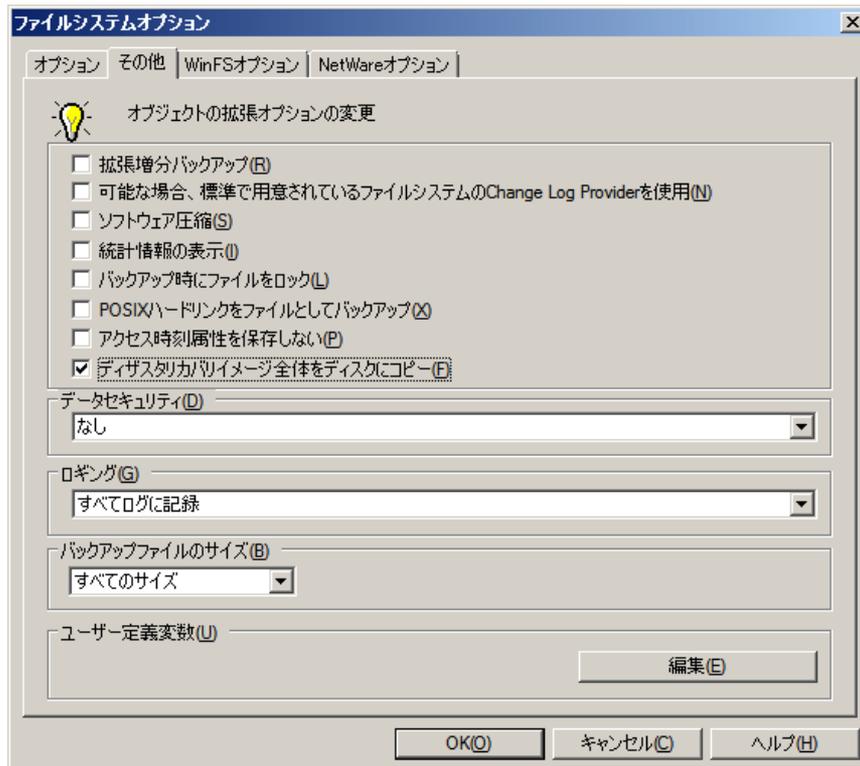
## DR OS イメージファイル

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。詳細は、『HP Data Protector ヘルプ』の索引「作成、バックアップ仕様」を参照してください。

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エイメージ全体をディスクにコピー] を選択します。
7. **Windows Vista、Windows 7、Windows Server 2008 の場合:**[NTFS ハードリンクを検出] も選択します。[シャドウコピーを使用] オプションを選択された状態のままにし、[フォールバックを許可] オプションを選択解除された状態のままにします。

図 2 [WinFS オプション] タブ



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

1. コンテキストリストで [バックアップ] を選択します。
2. Scoping ペインで [バックアップ仕様] → [ファイルシステム] の順に展開します。
3. フルクライアントバックアップに使用するバックアップ仕様を選択します。まだ作成していない場合は作成します。詳細は、『HP Data Protector ヘルプ』の索引「作成、バックアップ仕様」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エイメージ全体をディスクにコピー] を選択します。
7. **Windows Vista、Windows 7、Windows Server 2008 のいずれかのシステムの場合:**[NTFS ハードリンクを検出] も選択します。[シャドウコピーを使用] オプションを選択された状態のままにし、[フォールバックを許可] オプションを選択解除された状態のままにします。

Cell Manager でディザスタリカバリ CD に書き込む場合、あるいはブート可能 USB ドライブまたはブート可能ネットワークイメージを作成する場合は、DR イメージ全体を Cell Manager に保存すると便利です。この理由は、DR イメージはバックアップメディアから復元するよりもハードディスクから読み取る方がはるかに高速であるためです。DR イメージファイルはデ

フォルトで、Cell Manager の `Data_Protector_program_data\Config\Server\dr\pls` ディレクトリ (Windows Server 2008 の場合)、

`Data_Protector_home\Config\Server\dr\pls` (その他の Windows システムの場合)、または `/etc/opt/omni/server/dr/pls` ディレクトリ (UNIX システムの場合) 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。『HP Data Protector ヘルプ』の索引「グローバルオプションファイル、変更」を参照してください。



**ヒント:** あて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、マウントポイントを作成するか (Windows の場合)、他のボリュームへのリンクを作成 (UNIX の場合) できません。

## 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。「[kb.cfg ファイルの編集](#)」(73 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、Cell Manager に自動的にエクスポートされます。エクスポート先のファイルは、`Data_Protector_program_data\Config\Server\export\keys\DR-ClientName-keys.csv` (Windows Server 2008 の場合)、`Data_Protector_home\Config\Server\export\keys\DR-ClientName-keys.csv` (その他の Windows システムの場合)、または `/var/opt/omni/server/export/keys/DR-ClientName-keys.csv` (UNIX システムの場合) です。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ために準備した各バックアップの正しい暗号化キーがあることを確認します。

## フェーズ 1 開始ファイル (P1S)

フルバックアップ中は、DR OS 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\pls` ディレクトリ (Windows システムの場合) または `/etc/opt/omni/server/dr/pls` ディレクトリ (UNIX システムの場合) 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`)。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、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インストールに組み込んで **DR OS イメージ** としてマージできます。ISO9660 形式をサポートする CD 書き込みツールを使用して DR OS イメージを CD に記録

し、USB ドライブに保存するか、またはネットワークブート可能イメージを作成することができます。この DR OS イメージは、**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。

- ① **重要:** ディザスタリカバリ CD、ブート可能 USB ドライブ、またはネットワークブート可能イメージは Cell Manager 用に前もって準備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](#)」(66 ページ)を参照してください。

- ① **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。

## ディザスタリカバリ用の DR OS イメージを準備する

DR OS イメージを作成し、CD に記録し、作成した DR OS イメージを USB ドライブに保存するか、またはブート可能ネットワークイメージに保存できます。

- ① **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 OS イメージを作成します。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イメージを準備する

DR ISO イメージを作成するには、以下の手順を実行します。

1. コンテキストリストで **[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、DR 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、**[バックアップからイメージファイルを復元]** をクリックします。**[次へ]** をクリックします。
7. イメージ形式を選択します。使用できるオプションは次のとおりです。
  - 起動可能な ISO イメージの作成: DR ISO イメージ (デフォルトで、recovery.iso)
  - 起動可能な USB ドライブの作成: ブート可能 USB ドライブ上の DR OS イメージ
  - 起動可能なネットワークイメージの作成: ネットワークブートに使用できる DR OS イメージ (デフォルトで、recovery.wim)
8. ブート可能 ISO イメージまたはブート可能ネットワークイメージを作成する場合は、宛先ディレクトリを選択します。作成したイメージの保存先を選択します。  
ブート可能 USB ドライブを作成する場合は、宛先 USB ドライブまたはドライブ番号を選択します。作成したイメージの保存先を選択します。

- △ **注意:** ブート可能 USB ドライブの作成時には、ドライブ上に格納されたすべてのデータが消失します。

### 9. Windows Vista、Windows 7、および Windows Server 2008 システムの場合:

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

場所を入力すると、Data Protector はその場所に保存し、次回 DR ISO イメージが作成されるときに、その場所が GUI 内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、Data Protector はデフォルトの WAIK パスを使用します。

- DR ISO イメージに挿入するドライバ

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。ドライバを手動で追加または削除するには、[追加] または [削除] をクリックします。Windows Vista、Windows 7、または Windows Server 2008 クライアントリカバリセットに付属するドライバを挿入するには、[挿入] をクリックします。ドライバは、リカバリセットの `%Drivers%` 部分から DR OS に自動的に挿入されます。

- ① **重要:** 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が、DR OS での使用に適しているとは限りません。場合によっては、復旧時にハードウェアが適切に機能するよう、Windows Preinstallation Environment(WinPE) 固有のドライバを挿入する必要があります。

10. [完了] をクリックします。ウィザードが終了し、DR ISO イメージが作成されます。
11. ISO9660 形式をサポートしている CD 書き込みツールを使用して、DR ISO イメージを CD に書き込みます。

## 復旧

障害が発生したシステムでディザスタリカバリを正しく実行するには、以下のものが必要です。

- 問題のある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
- 「ディザスタリカバリ用の DR OS イメージを準備する」(42 ページ) で作成した Data Protector ディザスタリカバリ CD、ブート可能 USB ドライブ、またはネットワークブート可能イメージ
- 影響を受けたシステムがドメインコントローラの場合、ディレクトリサービス復元モードの管理者アカウントのパスワード。

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. オフラインディザスタリカバリを行う場合以外は、ターゲットシステムのオペレーティングシステムによって、Cell Manager 上の Data Protector の Admin ユーザーグループに以下のプロパティを持つアカウントを追加します。

### Windows Vista、Windows 7、および Windows Server 2008 システムの場合:

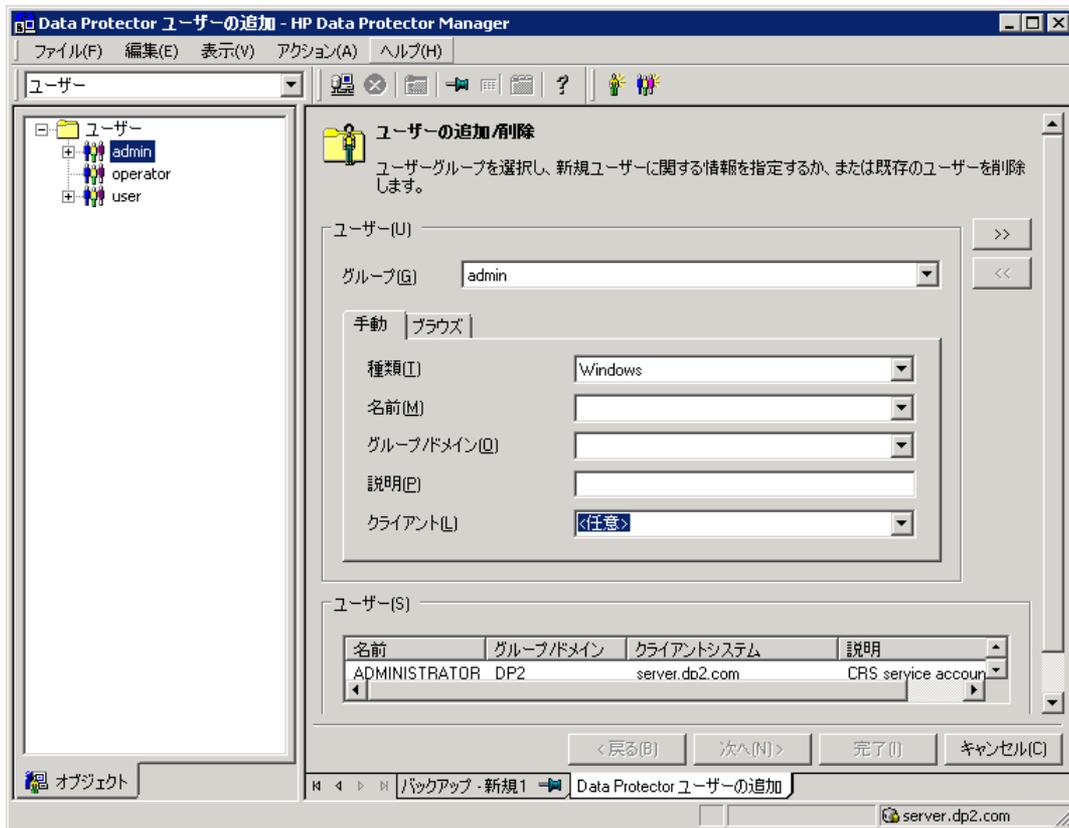
- 種類:Windows
- 名前:SYSTEM
- グループ/ドメイン:NT AUTHORITY
- クライアント:復旧するシステムの一時的なホスト名  
一時的なホスト名は、Windows Preinstallation Environment (WinPE) によってシステムに割り当てられます。WinPE のコマンドプロンプトウィンドウで `hostname` コマンドを実行することによって、ホスト名を取得できます。

### その他の Windows システムの場合:

- 種類:Windows
- 名前:DRM\$Admin
- グループ/ドメイン:ターゲットシステムのホスト名
- クライアント:ターゲットシステムの完全修飾ドメイン名 (FQDN)

ユーザーの追加の詳細については、『HP Data Protector ヘルプ』の検索キーワード「Data Protector ユーザーの追加」を参照してください。

図 3 ユーザーアカウントの追加



**注記:** セル内のクライアント間で暗号制御通信を使用している場合、復旧の開始前に、Cell Manager 上の [セキュリティの例外] リストにクライアントを追加する必要があります。ローカルデバイスを使用している場合を除き、Cell Manager の [セキュリティの例外] リストに Media Agent クライアントも追加する必要があります。

2. オリジナルシステムのディザスタリカバリ CD、ブート可能 USB ドライブ、またはブート可能ネットワークイメージからクライアントシステムをブートします。  
CD からターゲットシステムを起動する場合は、復旧手順の開始前に、システムに外付けの USB ディスク (USB フラッシュドライブを含む) が接続されていないことを確認してください。
3. ドメインコントローラを復旧している場合、[Windows へようこそ] ダイアログボックスが表示されたら、**Ctrl+Alt+Delete** を押して、ディレクトリサービス復元モードの管理者アカウントのパスワードを入力して [OK] をクリックします。
4. 復旧の対象範囲およびリカバリオプションを選択します。次の手順は、オペレーティングシステムによって異なります。

**Windows Vista、Windows 7、および Windows Server 2008 システムの場合:**

- a. HP Data Protector ディザスタリカバリ GUI(インストーラウィザード) が開始され、オリジナルシステムの情報を表示します。[次へ] をクリックします。

**注:** **ヒント:** 進行状況バーが表示されたときに使用可能なキーボードオプションがいくつかあります。進行状況バー上にカーソルを移動すると、使用可能なオプションとその説明を確認できます。

b. [リカバリオプション] ページで、次のリカバリ方法のいずれかを選択し、リカバリオプションを指定します。

- **[デフォルト復旧]:**クリティカルボリューム(システムディスク、ブートディスク、OBInstall 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化されフォーマットされ、フェーズ 3 のために空のままになります。
- **[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)。
- **[完全復旧]:**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障害の影響を受けているときに、最初のノードで 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 つでも稼働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、稼働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。

次の追加のリカバリオプションが使用できます。オプションによっては、ディザスタリカバリが完全に終了しない場合や、追加手順が必要な場合に使用します。

- **[DAT の復元]:**Windows Vista、Windows 7、および Windows Server 2008 システム上でのみ使用できます。選択されている場合、Data Protector は、ディザスタリカバリセッション中にあらかじめ Microsoft VSS ライターのデータも復元して、Data Protector の復元セッションでライターデータを復元します。このオプションは、デフォルトで選択されています。
- **[BCD の復元]:**Windows Vista、Windows 7、および Windows Server 2008 システム上でのみ使用できます。選択されている場合、Data Protector は、ディザスタリカバリセッション中にあらかじめ Boot Configuration Data (BCD) ストアも復元して、Data Protector の復元セッションで BCD ストアを復元します。このオプションは、デフォルトで選択されています。
- **[クラスターボリュームを手動でマップ]:**このオプションは Windows Server 2008 システム上でのみ使用できます。このオプションを選択すると、クラスターボリュームを手動でマップできます。選択しないと、ボリュームは自動的にマップされます。自動的にマップされた後に、すべてのボリュームが適切にマップされていることを確認することをお勧めします。
- **[異なるハードウェア]:**Windows Vista、Windows 7、および Windows Server 2008 システム上でのみ使用できます。このオプションを有効にすると、Data Protector はシステムをスキャンして、復元中に見つからないドライバを探します。ドロップダウンリストから次のいずれかの方法を選択すると、このオプションが有効になります。
  - **[無人](デフォルト):**このモードは、事前定義された構成ファイルを使用してオペレーティングシステムを各種のハードウェアプラットフォームに自動的に構成します。これは、異なるハードウェアでの復旧のためのプライマリモードです。最初のインスタンスではこのモードを使用します。
  - **[ジェネリック]:**おそらく復元したオペレーティングシステムの構成が正しくないために無人モードが失敗した場合、このオプションを選択します。復元された OS レジストリ、そのドライバとサービスの異なるハードウェアの適用に基づきます。
- **[デバイスの削除]:**このオプションは、[異なるハードウェア] オプションが有効な場合にのみ使用できます。このオプションを選択すると、Data Protector は、

復元したオペレーティングシステムのレジストリからオリジナルのデバイスを削除します。

- **[起動記述子の削除]:** 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。 [\[Windows Itanium システム上の問題\] \(116 ページ\)](#) を参照してください。
- **[手動ディスク選択]:** Intel Itanium システムでのみ使用可能です。ディスク設定が大幅に変更された場合、ディザスタリカバリモジュールはブートディスクを見つけることができなくなる可能性があります。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。 [\[Windows Itanium システム上の問題\] \(116 ページ\)](#) を参照してください。

[完了] をクリックします。

- c. リカバリプロセスが開始します。進行状況を監視できます。

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、暗号化されたドライブのロックを解除することを促すメッセージが表示されます。ボリュームをロック解除しないと、**ディザスタリカバリ後ボリュームは暗号化されません**。

[\[Windows の BitLocker ドライブ暗号化でロックされたボリュームのロック解除\] \(76 ページ\)](#) を参照してください。



**ヒント:** HP Data Protector ディザスタリカバリ GUI で、[タスク] をクリックして、次の操作を実行できます。

- コマンドプロンプト、タスクマネージャ、ディスクアドミニストレータの実行
- ネットワークドライブのマッピングおよびドライブのロードツールへのアクセス
- 特定のディザスタリカバリプロセスのログファイルの表示
- DRM 構成ファイルの有効/無効化、テキストエディタでのこのファイルの表示と編集
- ヘルプへのアクセスと GUI アイコンの凡例の表示

### その他の Windows システムの場合:

- a. 以下のメッセージが表示されたら、**F12** を押します。マシン *HOSTNAME* の復元を開始するには、**F12** を押します。
- b. 範囲選択メニューはブートプロセスの最初に表示されます。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、システムが再起動されます。
- **[デフォルト復旧]:** クリティカルボリューム (システムディスク、ブートディスク、OBInstall 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化されフォーマットされ、フェーズ 3 のために空のままになります。
- **[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 OBDP のみで使用可能)。
- **[完全復旧]:** 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障害の影響を受けているときに、最初のノードで 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) が復元されません。

1 つでも稼働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、稼働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。

次の追加のリカバリオプションが使用できます。オプションによっては、ディザスタリカバリが完全に終了しない場合や、追加手順が必要な場合に使用します。

- **[起動記述子の削除]:** 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。[Windows Itanium システム上の問題] (116 ページ) を参照してください。
- **[手動ディスク選択]:** Intel Itanium システムでのみ使用可能です。ディスク設定が大幅に変更された場合、ディザスタリカバリモジュールはブートディスクを見つけることができなくなる可能性があります。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。[Windows Itanium システム上の問題] (116 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、Windows 7、および Windows Server 2008 の各システムでは、この手順が省略され、再起動は行われません。

"To start recovery of the machine *HOSTNAME* press F12" というプロンプトが表示されてから 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、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、次のプロンプトが表示されます。

復号に AES キーファイルを使用しますか? [Y/N]

[Y] キーを押します。

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) クライアントで使用可能であることを確認し、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。[編集後の SRD ファイルを使用した復旧] (73 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。
- 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 [デバッグ] 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、Windows 7、および Windows Server 2008 の各システムでは、一時 DR OS が残されることはありません。

9. **ステップ 1** で作成したクライアントのローカル管理者アカウントを、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 ProtectorAdmin 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](#)」(70 ページ) および「[高度な復旧作業](#)」(66 ページ) を参照してください。
11. Data Protector の標準復元手順を使用して、ユーザーデータおよび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 の復旧方法の 1 つで、ユーザーの操作は最小限に抑えられています。サポートされるオペレーティングシステムの詳細は、<http://support.openview.hp.com/selfsolve/manuals> にある最新のサポート一覧を参照してください。

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。

- ① **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 ワンボタンディザスタリカバリ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。

① **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](#)」(66 ページ) も参照してください。

## 前提条件

- この方法による復旧を可能にしたいシステムには、Data Protector の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イスコンポーネントをインストールしておく必要があります。また、DR OS イメージを準備するシステムには、自動ディザスタリカバリコンポーネントをインストールしておく必要があります。詳細は、『HP Data Protector インストールおよびライセンスガイド』を参照してください。
- OBDR を実行できるシステム構成にしておく必要があります。システムの BIOS は、El-Torito 規格で定義されている起動可能 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 アドレッシングによるハードディスクドライブへの読み取り/書き込みアクセスをサポートしている必要があります。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。  
サポートされるシステム、デバイス、メディアの詳細については、テープとハードウェアの互換性一覧表および最新のサポート一覧 (<http://support.openview.hp.com/selfsolve/manuals>) を参照してください。
- ターゲットシステムのハードウェア構成は、オリジナル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。これには、SCSI の BIOS 設定 (セクターの再マッピング) 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必要があります。
- 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。

- Windows Vista、Windows 7、または Windows Server 2008 システム用の DR OS 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適切なバージョンの Windows Automated Installation Kit (WAIK) をインストールしておく必要があります。
  - Windows Vista および Windows Server 2008 システム:WAIK 1.1
  - Windows 7 および Windows Server 2008 R2 システム:WAIK 2.0
- Windows Vista、Windows 7 または Windows Server 2008 システム上にある IIS 構成オブジェクトをバックアップするには、IIS 6 Metabase Compatibility パッケージをインストールしてください。

## 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、影響を受け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。
- Windows Vista、Windows 7、および Windows Server 2008 の各システムでは、LDM ディスク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。
- SAN ブートまたは SAN マルチパス構成の復旧はサポートされていません。
- 論理ボリュームの VSS ディスクイメージバックアップをディザスタリカバリに使用できるのは、Windows Vista、Windows 7、および Windows Server 2008 システムのみです。Java GUI では、ディスクイメージオブジェクトのブラウジングをサポートしていません。この機能についてはオリジナルの GUI を使用してください。
- HP Data Protector ディザスタリカバリ GUI は、Windows Vista、Windows 7、および Windows Server 2008 システム上でのみ使用できます。他の Windows システムでは、コンソールインタフェースを使用できます。
- Windows Vista、Windows 7、および Windows Server 2008 システムの場合、元々の暗号化されたフォルダを非暗号化フォルダとしてのみ復元できます。

## 準備

この項で挙げられている手順を行う前に、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](#)」(22 ページ)も参照してください。「[高度な復旧作業](#)」(66 ページ)も参照してください。

- ① **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。『HP Data Protector 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。

**Windows 7 および Windows Server 2008 R2 システム:** 必ずシステムボシューム (存在する場合) をバックアップしてください。

**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)

詳細は、「[Microsoft Cluster Server の復元に固有の手順](#)」(66 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。

**クラスター共有ボリューム:** クライアントシステムのフルバックアップを実行する前に、まず Data Protector 仮想環境用統合ソフトウェアを使用して仮想ハードドライブ (VHD) ファイルおよび CSV 構成データをバックアップしてください。『HP Data Protector インテグレーションガイド - 仮想環境』を参照してください。バックアップは別個のデバイス上で実行する必要があります。OBDR バックアップは、追加不可能メディア上でのみ実行できるためです。

## OBDR 用のバックアップ仕様を作成する

OBDR を使用して復旧を実行するシステム上でインストールされた GUI からローカルに OBDR バックアップを実行するには、以下の手順を実行します。

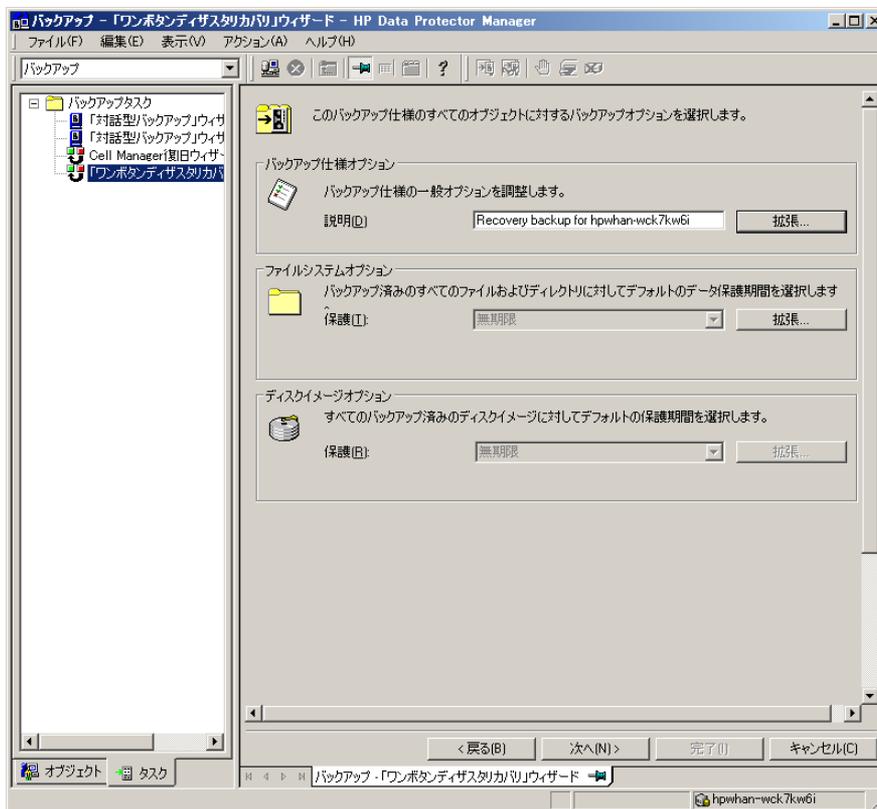
1. コンテキストリストで [バックアップ] を選択します。
2. Scoping ペインで [タスク] ナビゲーションタブをクリックし、[ワンボタンディザスタリカバリウィザード] を選択します。
3. [次へ] をクリックします。
4. クリティカルオブジェクトはすでにすべて選択された状態になっていて (Cell Manager OBDR バックアップの場合は IDB も含む)、選択を解除することはできません。復旧手順の中で、Data Protector はシステムからパーティションをすべて削除してしまうため、他のパーティションを復旧後も使用する場合、手動で選択します。[次へ] をクリックします。
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、『HP Data Protector ヘルプ』の検索キーワード「バックアップオプション」を参照してください。

**Windows Vista、Windows 7、または Windows Server 2008 システムの場合:**

## 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  
場所を入力すると、Data Protector はその場所に保存し、次回 DR OS イメージが作成されるたびに、その場所が GUI 内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、Data Protector はデフォルトの WAIK パスを使用します。
  - DR OS イメージに挿入するドライバ  
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。ドライバを手動で追加または削除するには、[追加] または [削除] をクリックします。Windows Vista、Windows 7、または Windows Server 2008 のクライアントリカバリセットに含まれるドライバを挿入するには、[復元セットからドライバを自動挿入] を選択します。リカバリセットの `%Drivers%` 部分のドライバが自動的に DR OS イメージに挿入されます。ただし、そのドライバは [ドライバを挿入] テキストボックスには表示されません。
- ❶ **重要:** 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が、DR OS での使用に適しているとは限りません。場合によっては、復旧時にハードウェアが適切に機能するよう、Windows Preinstallation Environment (WinPE) 固有のドライバを挿入する必要があります。

## 図 4 Windows Vista、Windows 7、および Windows Server 2008 のクライアントバックアップオプション



7. [次へ] をクリックして、[スケジュール] 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。『HP Data Protector ヘルプ』の索引「特定の日時に対するバックアップのスケジュール設定」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。ディスクイメージオブジェクトを指定する必要がある場合など、修正したバックアップ仕様を標準バックアップ仕様として保存することもできます。標準バックアップ仕様として保存しても、OBDR 用に使用できます。
  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。
- ① **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。
- 

## ディスクイメージバックアップを使用するために OBDR バックアップ仕様を変更する

Windows Vista、Windows 7、および Windows Server 2008 システムでは、VSS ライターを使用することで論理ボリュームをディスクイメージとしてバックアップできます。この方法では、バックアップ中のボリュームがロック解除されたままの状態、他のアプリケーションからアクセスできます。論理ボリュームをディスクイメージとしてバックアップするには、OBDR 用に作成したバックアップ仕様を次のように変更する必要があります。

1. Scoping ペインで、作成した OBDR バックアップ仕様をクリックします。この仕様を OBDR バックアップ仕様として処理するか、または通常のバックアップ仕様として処理するかを確認するメッセージが表示されたら、[いいえ] をクリックします。

**注記:** OBDR バックアップ仕様を通常のバックアップ仕様として保存しても、OBDR として使用できます。

---

2. [バックアップオブジェクトのサマリー] ページで、ディスクイメージとしてバックアップする論理ボリュームを選択して、[削除] をクリックします。

**注記:** 論理ボリュームのみをバックアップすることができます。IDB と構成オブジェクト、および NTFS フォルダとしてマウントされていない、あるいはマウントされているボリュームは、ファイルシステムのバックアップを使用することでバックアップする必要があります。

---

3. [手動で追加] をクリックして、ウィザードを起動します。
4. [バックアップオブジェクトの選択] ページで [ディスクイメージオブジェクト] オプションをクリックし、[次へ] をクリックします。

5. [一般的な選択項目] ページで、バックアップするディスクイメージのあるクライアントを選択し、適切な説明を入力します。[次へ] をクリックします。

**注記:** 説明は、各ディスクイメージオブジェクトで一意である必要があります。わかりやすい名前を使用します。たとえば、C: ボリュームには [Disk Image C] と入力します。

6. [一般オブジェクトオプション] プロパティページでは、データ保護を [なし] に設定します。[次へ] をクリックします。

**注記:** データ保護を [なし] に設定すると、OBDR テープの内容を新しい OBDR バックアップで上書きできます。

7. [拡張オブジェクトオプション] プロパティページでは、ディスクイメージオブジェクトの拡張バックアップオプションを指定できます。[次へ] をクリックします。
8. [ディスクイメージオブジェクトオプション] プロパティページでは、バックアップ対象のディスクイメージセクションを指定します。以下の形式で指定します。

\\.\DriveLetter: のように指定します。例: \\.\E:

**注記:** ボリューム名をドライブ名として指定すると、バックアップ中にボリュームがロックされません。NTFS フォルダとしてマウントされない、またはマウントされるボリュームは、ディスクイメージバックアップには使用できません。

9. [完了] をクリックしてウィザードを終了します。
10. [バックアップオブジェクトのサマリー] ページで、バックアップ仕様のサマリーを表示します。ディスクイメージとして指定した論理ボリュームは、ディスクイメージタイプである必要があります。[適用] をクリックします。

## 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。「kb.cfg ファイルの編集」(73 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、Cell Manager に自動的にエクスポートされます。エクスポート先のファイルは、`Data_Protector_program_data\Config\Server\export\keys\DR-ClientName-keys.csv` (Windows Server 2008 の場合)、`Data_Protector_home\Config\Server\export\keys\DR-ClientName-keys.csv` (その他の Windows システムの場合)、または `/var/opt/omni/server/export/keys/DR-ClientName-keys.csv` (UNIX システムの場合) です。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ために準備した各バックアップの正しい暗号化キーがあることを確認します。

## 復旧

障害が発生したシステムでディザスタリカバリを正しく実行するには、以下のものがが必要です。

- 影響を受け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. オフラインディザスタリカバリを行う場合以外は、ターゲットシステムのオペレーティングシステムによって、Cell Manager 上の Data Protector の Admin ユーザーグループに以下のプロパティを持つアカウントを追加します。

### Windows Vista、Windows 7、または Windows Server 2008 システムの場合:

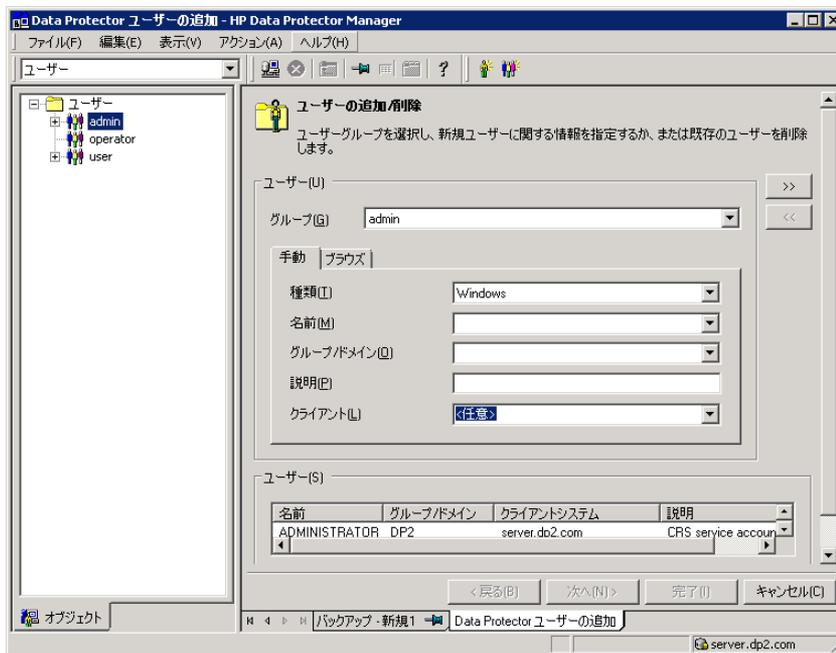
- 種類:Windows
- 名前:SYSTEM
- グループ/ドメイン:NT AUTHORITY
- クライアント:復旧するシステムの一時的なホスト名  
一時的なホスト名は、Windows Preinstallation Environment (WinPE) によってシステムに割り当てられます。WinPE のコマンドプロンプトウィンドウで `hostname` コマンドを実行することによって、ホスト名を取得できます。

### その他の Windows システムの場合:

- 種類: Windows
- 名前:DRM\$Admin
- グループ/ドメイン:ターゲットシステムのホスト名
- クライアント:ターゲットシステムの完全修飾ドメイン名 (FQDN)

ユーザーの追加の詳細については、『HP Data Protector ヘルプ』の検索キーワード「Data Protector ユーザーの追加」を参照してください。

## 図 5 ユーザーアカウントの追加



**注記:** セル内のクライアント間で暗号制御通信を使用している場合、復旧の開始前に、Cell Manager 上の [セキュリティの例外] リストにクライアントを追加する必要があります。ローカルデバイスを使用している場合を除き、Cell Manager の [セキュリティの例外] リストに Media Agent クライアントも追加する必要があります。

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 フラッシュドライブなど) 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。詳細は、デバイス付属のドキュメントを参照してください。
5. 復旧の対象範囲およびリカバリオプションを選択します。次の手順は、オペレーティングシステムによって異なります。

### Windows Vista、Windows 7、および Windows Server 2008 システムの場合:

- a. HP Data Protector ディザスタリカバリ GUI(インストーラウィザード) が開始され、オリジナルシステムの情報を表示します。[次へ] をクリックします。

**注:** **ヒント:** 進行状況バーが表示されたときに使用可能なキーボードオプションがいくつかあります。進行状況バー上にカーソルを移動すると、使用可能なオプションとその説明を確認できます。

- b. [リカバリオプション] ページで、次のリカバリ方法のいずれかを選択し、リカバリオプションを指定します。
  - **[デフォルト復旧]:**クリティカルボリューム(システムディスク、ブートディスク、OBInstall 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化されフォーマットされ、フェーズ 3 のために空のままになります。
  - **[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)。
  - **[完全復旧]:**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障害の影響を受けているときに、最初のノードで EADR を実行する場合に使用しません。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) が復元されません。

1 つでも稼働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、稼働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。

次の追加のリカバリオプションが使用できます。オプションによっては、ディザスタリカバリが完全に終了しない場合や、追加手順が必要な場合に使用します。

- **[DAT の復元]:**Windows Vista、Windows 7、および Windows Server 2008 システム上でのみ使用できます。選択されている場合、Data Protector は、ディザスタリカバリセッション中にあらかじめ Microsoft VSS ライターのデータも復元して、Data Protector の復元セッションでライターデータを復元します。このオプションは、デフォルトで選択されています。
- **[BCD の復元]:**Windows Vista、Windows 7、および Windows Server 2008 システム上でのみ使用できます。選択されている場合、Data Protector は、ディザスタリカバリセッション中にあらかじめ Boot Configuration Data (BCD) ストアも復元して、Data Protector の復元セッションで BCD ストアを復元します。このオプションは、デフォルトで選択されています。
- **[クラスターボリュームを手動でマップ]:**このオプションは Windows Server 2008 システムでのみ使用できます。このオプションを選択すると、クラスターボリュームを手動でマップできます。選択しないと、ボリュームは自動的にマップされます。自動的にマップされた後に、すべてのボリュームが適切にマップされていることを確認することをお勧めします。
- **[異なるハードウェア]:**Windows Vista、Windows 7、および Windows Server 2008 システム上でのみ使用できます。このオプションを有効にすると、Data Protector はシステムをスキャンして、復元中に見つからないドライバを探します。ドロップダウンリストから次のいずれかの方法を選択すると、このオプションが有効になります。
  - **[無人](デフォルト):**このモードは、事前定義された構成ファイルを使用してオペレーティングシステムを各種のハードウェアプラットフォームに自動的に構成します。これは、異なるハードウェアでの復旧のためのプライマリモードです。最初のインスタンスではこのモードを使用します。
  - **[ジェネリック]:**おそらく復元したオペレーティングシステムの構成が正しくないために無人モードが失敗した場合、このオプションを選択します。復元された OS レジストリ、そのドライバとサービスの異なるハードウェアの適用に基づきます。
- **[デバイスの削除]:**このオプションは、[異なるハードウェア] オプションが有効な場合にのみ使用できます。このオプションを選択すると、Data Protector は、復元したオペレーティングシステムのレジストリからオリジナルのデバイスを削除します。
- **[起動記述子の削除]:**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。 [[Windows Itanium システム上の問題](#)] (116 ページ) を参照してください。
- **[手動ディスク選択]:**Intel Itanium システムでのみ使用可能です。ディスク設定が大幅に変更された場合、ディザスタリカバリモジュールはブートディスクを見つけることができなくなる可能性があります。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。[Windows Itanium システム上の問題] (116 ページ) を参照してください。

[完了] をクリックします。

- c. リカバリプロセスが開始します。進行状況を監視できます。  
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、暗号化されたドライブのロックを解除することを促すメッセージが表示されます。ボリュームをロック解除しないと、**ディザスタリカバリ後ボリュームは暗号化されません**。  
[Windows の BitLocker ドライブ暗号化でロックされたボリュームのロック解除] (76 ページ) を参照してください。



**ヒント:** HP Data Protector ディザスタリカバリ GUI で、[タスク] をクリックして、次の操作を実行できます。

- コマンドプロンプト、タスクマネージャ、ディスクアドミニストレータの実行
- ネットワークドライブのマッピングおよびドライブのロードツールへのアクセス
- 特定のディザスタリカバリプロセスのログファイルの表示
- DRM 構成ファイルの有効/無効化、テキストエディタでのこのファイルの表示と編集
- ヘルプへのアクセスと GUI アイコンの凡例の表示

#### その他の Windows システムの場合:

- a. 以下のメッセージが表示されたら、**F12** を押します。マシン *HOSTNAME* の復元を開始するには、**F12** を押します。
- b. 範囲選択メニューはブートプロセスの最初に表示されます。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、システムが再起動されます。
- **[デフォルト復旧]:**クリティカルボリューム (システムディスク、ブートディスク、OBInstall 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化されフォーマットされ、フェーズ 3 のために空のままになります。
- **[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)。
- **[完全復旧]:**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障害の影響を受けているときに、最初のノードで 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 つでも稼働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、稼働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。

次の追加のリカバリオプションが使用できます。オプションによっては、ディザスタリカバリが完全に終了しない場合や、追加手順が必要な場合に使用します。

- **[起動記述子の削除]:**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。[Windows Itanium システム上の問題] (116 ページ) を参照してください。
- **[手動ディスク選択]:**Intel Itanium システムでのみ使用可能です。ディスク設定が大幅に変更された場合、ディザスタリカバリモジュールはブートディスクを見つけ

ることができなくなる可能性があります。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。[Windows Itanium システム上の問題] (116 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、Windows 7、および Windows Server 2008 の各システムでは、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、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、次のプロンプトが表示されます。

復号に AES キーファイルを使用しますか? [Y/N]

[Y] キーを押します。

キーストア (DR-ClientName-keys.csv) がクライアントで使用可能であることを (たとえば、CD-ROM、フロッピーディスク、USB フラッシュドライブを挿入することで) 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。[編集後の SRD ファイルを使用した復旧] (73 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 [デバッグ] 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、Windows 7、および Windows Server 2008 の各システムでは、一時 DR OS が残されることはありません。

10. **ステップ 1** で作成したクライアントのローカル管理者アカウントを、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 ProtectorAdmin 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] (70 ページ) および [高度な復旧作業] (66 ページ) を参照してください。

12. Data Protector の標準復元手順を使用して、ユーザーデータおよび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 `drstart` 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。

サポートされるオペレーティングシステムの詳細は、<http://support.openview.hp.com/selfsolve/manuals> にある最新のサポート一覧を参照してください。

- ① **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。

**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. 再起動後に、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 の標準復元手順を使用して、ユーザーデータおよび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](#)」(66 ページ) も参照してください。

## 要件

- この方法による復旧を可能にするシステムには、Data Protector の自動ディザスタリカバリコンポーネントをインストールしておく必要があります。詳細は、『HP Data Protector インストールおよびライセンスガイド』を参照してください。
- 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-ROM 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 のフラッシュ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必要があります。
- ターゲットシステムの各交換ディスクの記憶容量は、元のシステムの対応するディスクの記憶容量以上である必要があります。さらに、交換ディスクのジオメトリも交換前のディスクと同じである必要があります。
- ターゲットシステム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する必要があります (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)。

## 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。
- IPv6 のみの環境では、ASR を使用できません。ASR は、DHCP v4 サーバーが稼働している環境でのみ使用可能です。

## 準備

この項で挙げられている手順を行う前に、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」(22 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」(66 ページ) も参照してください。

- ① **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。

### 前提条件

- 自動システム復旧を正常に行うためには、フルクライアントバックアップ (CONFIGURATION も含む) が必要です。『HP Data Protector ヘルプ』の索引「バックアップ、Windows 固有」および「バックアップ、構成」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」(66 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を実行したら、ASR セットを用意する必要があります。ASR セットは、3 枚 (32 ビットシステムの場合)、4 枚 (AMD64/Intel EM64T システムの場合)、または 6 枚 (Itanium システムの場合) 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) を実行するとき、元のシステム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ユーザーデータの自動復旧を実行するときに必要になります。これらのファイルは、バックアップメディア上に保存されると共に、Cell Manager 上の

`Data_Protector_program_data\Config\server\dr\asr` ディレクトリ (Windows Server 2008 の場合)、`Data_Protector_home\Config\server\dr\asr` ディレクトリ (その他の Windows システムの場合)、または `/etc/opt/omni/server/dr/asr` ディレクトリ (UNIX システムの場合) に保存されます。障害が発生すると、ASR アーカイブファイルが 3 枚 (32 ビットシステムの場合)、4 枚 (AMD64/Intel EM64T システムの場合)、または 6 枚 (Itanium システムの場合) 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。

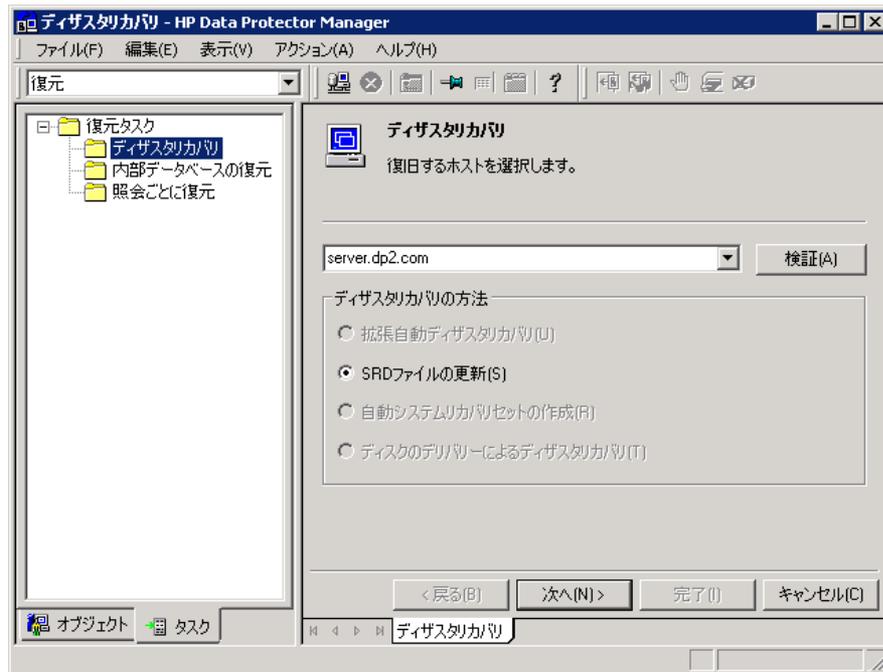
**注記:** Cell Manager 用の ASR セットは、前もって作成しておく必要があります。これは、障害後には ASR アーカイブファイルを取得できないためです。

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 6 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、フロッピーディスク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、3 枚 (32 ビットシステムの場合)、4 枚 (AMD64/Intel EM64T システムの場合)、または 6 枚 (Itanium システムの場合) のフロッピー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。

- 
- ① **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。『HP Data Protector ヘルプ』の索引「新しいデバイスのサポート」を参照してください。
4. `scsitab` ファイル名前を元に戻します。

## 復旧

影響を受け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、以下のものがが必要です。

- 問題のある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. 再起動後にディザスタリカバリウィザードが起動され、[DR のインストール元] と [SRD ファイルのパス] の入力が求められます。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](#)」(73 ページ) を参照してください。

---

### 注記:

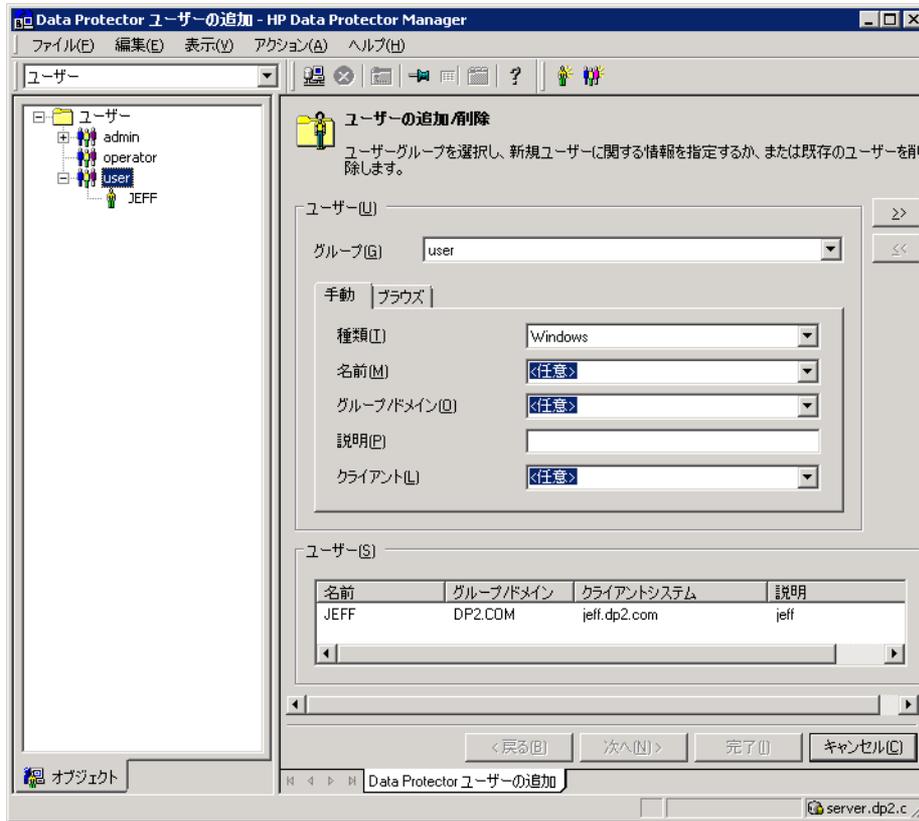
オリジナルの OS メディアに適切なドライバが用意されていないと、ASR を実行できません。[ハードウェアの追加] ウィザードを使用して、ネットワークをインストールすることができます。このウィザードは以下のコマンドで起動できま

```
%SystemRoot%\system32\rundll32 shell132.dll,Control_RunDLL  
hdwwiz.cpl
```

---

- 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。  
『HP Data Protector ヘルプ』の索引「ユーザー、Data Protector」を参照してください。  
「ASR のユーザー名」(65 ページ) に示されている情報を入力します。

図 7 ASR のユーザー名



**注記:** セル内のクライアント間で暗号制御通信を使用している場合、復旧の開始前に、Cell Manager 上の [セキュリティの例外] リストにクライアントを追加する必要があります。ローカルデバイスを使用している場合を除き、Cell Manager の [セキュリティの例外] リストに Media Agent クライアントも追加する必要があります。

- 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。
- 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。
- 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。

復号に AES キーファイルを使用しますか? [Y/N]

[y] キーを押します。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) クライアントで使用可能であることを確認し、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。

- ステップ 5 で作成したクライアントのローカルシステムアカウントを、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 ProtectorAdmin ユーザーグループから削除します。
- Data Protector の標準復元手順を使用して、ユーザーデータおよび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。概念と一般的な情報については、『HP Data Protector コンセプトガイド』のクラスター化の項、および『HP Data Protector ヘルプ』の索引「クラスター」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
- クラスター内のすべてのノードに障害が発生した場合

- ① **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是、MSCS のディザスタリカバリにも当てはまります。サポートされるオペレーティングシステムの詳細は、<http://support.openview.hp.com/selfsolve/manuals> にある最新のサポート一覧を参照してください。

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、稼働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ーに追加されます。

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。『HP Data Protector ヘルプ』の索引「構成オブジェクトの復元」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」(69 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 -full_clus` 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. システムを再起動します。

3. クラスタ 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。『HP Data Protector ヘルプ』の索引「構成オブジェクトの復元」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) (70 ページ) を参照してください。
5. 定数ボリュームと IDB ボリュームが復元されます。他のすべてのボリュームは影響を受けず、破損していなければ復元された一次ノードにより所有されます。  
他のボリュームが破損していた場合は、以下を行う必要があります。
  - a. クラスタサービスとクラスタ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. クラスタサービスとクラスタ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」(66 ページ) を参照してください。

#### EADR 用に全ノードの P1S ファイルをマージ

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

```
merge 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 システムの場合:** `merge.exe` コマンドは、Data Protector 自動ディザスタリカバリコンポーネントがインストールされている Windows システムでのみ動作します。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: merge

```
Data_Protector_home\Config\server\dr\pls\node1.company.com
```

```
Data_Protector_home\Config\server\dr\pls\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せん。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、そうでない場合は、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。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、フェーズ 1 でハードディスク署名が変わったために、クォーラムリソースが識別されないためです。この問題は、(`Data_Protector_home\bin\ins` にある) `clubar` ユーティリティを実行して、元のハードディスク署名を復元することで解決できます。`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 共有ディスクとその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 リソースキットに含まれている `dumpcfg` ユーティリティを使用します。`dumpcfg` の使用法の詳細は、`dumpcfg /?` を実行するか、Windows 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。

### クラスター共有ボリュームと VHD ファイルを復元する

CSV は次の 2 つのセッションで復元する必要があります。

1. すべてのボリュームを復元するためにディザスタリカバリセッションを実行します。Data Protector によりボリューム情報が復元されますが、ボリューム内のデータは復元されません。
2. Hyper-V バックアップセッションから CSV(CSV 構成データと CHD ファイルを含む) の復元を実行します。『HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service』を参照してください。

## マジョリティノードセットクラスターでの自動システム復旧

マジョリティノードセット (MNS) クラスター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 クラスターを設定し、そのクラスターに Data Protector クライアントをインストールします。  
MNS クラスターに 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 を使用する復旧方法については、『HP Data Protector ヘルプ』の索引「自動システム復旧」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の準備方法などについての詳細な手順は、『HP Data Protector ヘルプ』の索引「ディザスタリカバリ」を参照してください。

ノードが復旧し、クラスター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。メディアのリサイクルの詳細については、『HP Data Protector ヘルプ』の検索キーワード「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。

#### Windows Vista、Windows 7、および Windows Server 2008 の場合:

```
Data_Protector_home\bin\omnisv -stop  
del Data_Protector_program_data\tmp\*.*  
Data_Protector_home\bin\omnisv -start
```

#### その他の Windows システムの場合:

```
Data_Protector_home\bin\omnisv -stop  
del Data_Protector_home\tmp\*.*  
Data_Protector_home\bin\omnisv -start
```

2. 復元対象として残っているパーティションのバックアップが保存されたメディア (1 つ以上) を Data ProtectorGUI を使ってエクスポートします。メディアのエクスポートの詳細については、『HP Data Protector ヘルプ』の検索キーワード「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 ProtectorGUI を使ってインポートします。メディアのインポートの詳細については、『HP Data Protector ヘルプ』の検索キーワード「インポート、メディア」を参照してください。

### 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、WindowsCell 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。

- ディザスタリカバリ CD、または Cell Manager の DR OS イメージを格納している USB ドライブ、または Cell Manager のネットワークブート可能イメージをあらかじめ準備する必要があります。

① **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 OS イメージを作成します。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」(28 ページ)を参照してください。
- 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」(28 ページ)を参照してください。

① **重要:** バックアップメディア、DR イメージ、SRD ファイル、暗号化キーが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、DR OS データを格納している USB ドライブ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 が障害の影響を受けている場合は 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おく必要があります。

- 
- ① **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」(28 ページ)を参照してください。

---

- ① **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。
- 

- ① **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。

## トラブルシューティング

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

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

---

3. IIS 管理サービスと IIS に必要なすべてのサービスを開始します。

## 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 ファイルの先頭に記載されている形式で kb.cfg ファイルに追加します。

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」(38 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。

システムハードウェアとアプリケーションの構成は多様であるため、すべての構成に使用できる「万能」なソリューションを用意することはできません。したがって、ご自身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。

**△ 注意:** 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システム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)  
指定可能な-devtype オプションの値については、sanconfman 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 (-devioct1)
- ライブラリスロット (-physloc)
- 論理ライブラリ名 (-storname)

ファイルの編集が完了したら、Unicode(UTF-16) 形式で元の場所に保存します。

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、同じバックアップデバイスが同じ SCSI アドレスのクライアント new\_mahost.company.com に接続されているとします。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 -devioct1。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 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には、MA クライアント kerala (linux) に接続されている Ultrium\_kerala というドライブを使用し、論理ライブラリ名が Autoldr\_kerala である HP Ultrium ロボティクスライブラリを使用するとします。

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
-devioct1 /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。

- 
- ① **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(UTF-16) 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. 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 が自動的に開始されません。

図 8 ディザスタリカバリウィザードの Install only オプション



2. Windows タスクマネージャーを実行します (**Alt+Ctrl+Del** キーを押し、[タスクマネージャー] 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」(24 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 10/04/2011-1 -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\Diskdisk\_number フォルダから  
DRdisk\_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 の BitLocker ドライブ暗号化でロックされたボリュームのロック解除

Windows Vista、Windows 7、および Windows Server 2008 システムでのディザスタリカバリプロセス中、BitLocker ドライブ暗号化で暗号化されたボリュームのロックを解除できます。

### 制限事項

復旧するボリュームをロック解除しない場合、あるいはボリュームが損傷していてロック解除できない場合、**ディザスタリカバリ後にボリュームは暗号化されません**。このような状況では、ボリュームを再度暗号化する必要があります。

なお、システムボリュームは**常に**暗号化されない状態で復元されます。

## 手順

ディザスタリカバリモジュールが暗号化されたボリュームを検出した場合、暗号化されたボリュームのロック解除を促すメッセージが表示されます。

暗号化されているボリュームをロック解除するには、以下の手順を実行します。

1. **[はい]** をクリックしてロック解除ウィザードを起動します。**[いいえ]** をクリックすると、暗号化されたボリュームはロックされたままになります。
2. **[ロックされたボリュームの選択]** ページで、検出した暗号化されたボリュームが一覧されます。ロック解除するボリュームを選択して、**[次へ]** をクリックします。
3. **[ボリュームのロック解除]** ページ (選択した各ボリュームの 1 ページ) で、ロック解除方法を指定することが求められます。以下のロック解除方法を使用できます。
  - **パスワード (Windows 7 および Windows Server 2008 R2 でのみ使用できる)**  
ボリュームを暗号化したときに使用した文字列。
  - **パスフレーズ**  
ボリュームを暗号化したときに使用した通常のパスワードより長い文字列。
  - **リカバリキー**  
暗号化した各ボリュームに対して作成した特殊な隠しキー。リカバリキーには `BEK` という拡張子が付き、これはリカバリキーテキストファイルに保存されます。リカバリキーファイルを参照するには、ブラウズをクリックしてください。
4. テキストボックスに要求された情報を入力して、**[次へ]** をクリックします。  
ボリュームが正しくロック解除されたかどうかを確認して、**[完了]** をクリックします。

---

**注記:** ロック解除プロセスが失敗した場合、エラー情報を確認し、ロック解除手順を再試行するか、スキップします。

---

## 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 2)、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。詳細については、『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、ハードウェアの構成と OS のリリースが共通するシステムが多数含まれる 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、個々のシステムに応じてカスタマイズされ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」を割り当てることで、ネットワークに基づくクライアントの復旧を実行できます。その場合、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 共有上に存在する必要があります。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 環境には、同じハードウェアとソフトウェアをベースとするシステムが多数含まれることがよくあります。このような場合は、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ると、OS、アプリケーション、および必要パッチのインストールに要する時間を大幅に短縮できます。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。この機能は、システムを障害から復旧するときを使用できます。

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**
  - b. 問題のあるディスクを交換ディスクと交換します。
  - c. 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。
  - d. 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. Data Protector の標準復元手順を使用して、ユーザーデータおよびアプリケーションデータを復元します。

#### 準備

以下に、クライアントシステムのゴールドイメージをターゲットシステム上に作成する手順を示します。ターゲットシステムは、NFS を介してゴールドイメージをネットワークに提供します。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」に含まれることとなります。

1. Ignite-UX サーバーの `/opt/ignite/data/scripts/make_sys_image` ファイルを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で、`make_sys_image -d`アーカイブのディレクトリ `-n`アーカイブ名.gz `-s` ターゲットシステムの IP アドレス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、そ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.11.31/archive_HPUX11_31_DP70_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_1"
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_31_DP70_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. 新しく作成したデポを Ignite-UX に認識させるには、`/var/opt/ignite/INDEX` ファイルに `cfg` エントリを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_31_DP70_Client" {
description "HPUX 11.i OS incl Patches and DP70 Client"
"/opt/ignite/data/Rel_B.11.31/config"
"/var/opt/ignite/data/Rel_B.11.31/archive_HPUX11_31_DP70_CL.cfg"
"
}
```

8. 起動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/inst1_boottab` ファイルで構成されていることを確認します。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テープ/CD を作成することができます。詳細については、『Ignite-UX 管理ガイド』を参照してください。

---

## 復旧

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

### 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 serverinstall`
- 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 の標準復元手順で、追加する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。

## 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、Data Protector のファイルやディレクトリなど) 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。この復旧テープは使用しているシステム用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起動することで、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起動するか、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の起動は、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. Data Protector の標準復元手順を使用して、ユーザーデータおよびアプリケーションデータを復元します。

### 準備

HP-UX クライアントの復旧アーカイブを最も簡単に作成するには、Ignite-UX サーバー上で Ignite-UX GUI を使用します。GUI コマンドはすべて、コマンドラインからも実行できます。詳細については、『Ignite-UX 管理ガイド』を参照してください。

### 前提条件

システム障害に対する準備を行う前に、Ignite-UX ファイルセットをクライアントにインストールして、Ignite-UX サーバ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 ファイルセットのリビジョンが、Ignite-UX サーバーとクライアントで同じであることを確認します。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. 次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し、**[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ことです。

1. 次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を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し、**[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。

---

## 復旧

### バックアップテープからの復旧

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

1. 障害が発生したハードウェアを交換します。
2. 影響を受けた 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。どれがテープド

ライブであるかを確認して、ブートコマンド `boot hardware path` または `boot Pnumber` を入力します。

4. 復旧プロセスが自動的に開始されます。
5. 復旧が正常に完了したら、Data Protector の標準復元手順でその他のユーザーデータやアプリケーションデータを復元します。

### 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 serverinstall`
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、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. 復旧が正常に完了したら、Data Protector の標準復元手順でその他のユーザーデータやアプリケーションデータを復元します。

## 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ザスタリカバリをディスクデリバリーで実行するには、影響を受けたシステムに、最低限の OS のインストールと Data Protector Disk Agent が含まれているブート可能なディスクを接続します。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。

サポートされるオペレーティングシステムの詳細は、(<http://support.openview.hp.com/selfsolve/manuals>) にある最新のサポート一覧を参照してください。

### 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再起動します。
- 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 の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. Data Protector の標準復元手順を使用して、ユーザーデータおよびアプリケーションデータを復元します。

## 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が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 **init1 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」](#) (23 ページ) を参照してください)。詳細については、お手持ちのオペレーティングシステムのドキュメントを参照してください。

### HP-UX システムの場合:

#### 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。設定例は、[「抹消リンクの移動 \(HP-UX 11.x\)」](#) (119 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、システムを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` (`FS_mounted`, `hostname_set`, `date_set`, `syncer_running`)
- 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 の場合:

### 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、システムを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 の場合:

### 例

1. システムの電源がオフになっている場合は、システムをブートし、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 コンソールから次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. システムが既に電源オンおよび稼動中である場合は、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 システムの場合:

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します。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。
  - バックアップの実行中に他のユーザーがシステムにログオンできないように、システムへのネットワークアクセスを制限します (たとえば、HP-UX の場合、`inetd.sec` を上書きして、`inetd -c` を使用します)。
  - 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 (ディスクディスクカバリを使用)、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に実行します (HP-UX では、LVM を使用)。

## 復旧

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。

- 問題のある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 を使用)。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` の詳細については、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、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) ディスクから再起動します。

---

**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 の手動での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、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. Data Protector の標準復元手順を使用して、ユーザーデータおよびアプリケーションデータを復元します。
- b. システムを再起動します。

## 制限事項

サポートされるオペレーティングシステムの詳細は、(<http://support.openview.hp.com/selfsolve/manuals>)にある最新のサポート一覧を参照してください。

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)。「準備」(84 ページ)を参照してください。上記の手順とは別に、以下の手順も実行することが必要です。

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

## 復旧

以下の手順に従って、UNIX Cell Manager を復元します。

### 前提条件

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. 影響があっ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。手順については、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. データベースと `/etc/opt/omni` の最新バックアップ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:** データベースを直接復元することはできません。その手順については、『HP Data Protector ヘルプ』を参照してください。この手順には、`/opt/omni/sbin/omnisv -stop` コマンドを使用してすべての Data Protector プロセスを終了する操作が含まれます。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、すべての使用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。

## Linux システムの拡張自動ディザスタリカバリ

Data Protector には、Linux Cell Manager や Linux クライアント用の拡張ディザスタリカバリの手順が用意されています。サポートされるオペレーティングシステムの詳細は、(<http://support.openview.hp.com/selfsolve/manuals>) にある最新のサポート一覧を参照してください。

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。クライアントシステム全体のフルバックアップの際に、DR OS の一時的な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** にバックされ、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。障害発生時には、拡張自動ディザスタリカバリウィザードを使用して、バックアップメディアから DR OS イメージを復元し (フルバックアップ中に Cell Manager に保存されていない場合)、**ディザスタリカバリ CD ISO イメージ** に変換することができます。CD ISO イメージは、任意の CD 書き込みツールを使用して CD に記録し、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。

その後、DR OS が自動的に実行されます。ディスクのフォーマットとパーティション作成も自動的に実行され、最終的に、オリジナルシステムが Data Protector とともにバックアップ時の状態に復旧されます。

- ① **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

Linux 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. クライアントシステム全体のフルバックアップを実行します。Cell Manager をバックアップする場合は、内部データベースも対象に含めてください。
- b. 拡張自動ディザスタリカバリウィザードを使用して、リカバリ対象システムの DR OS イメージファイルからディザスタリカバリ CD ISO イメージ (DR 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、拡張自動ディザスタリカバリウィザードでは、バックアップメディアからイメージが復元されます。

- ① **重要:** ハードウェア、ソフトウェア、または構成を変更するたびに、新たにバックアップを実行して新しい DR CD 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、ネットワークを変更した場合にも当てはまります。

- 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 (ブートボリューム、ルートボリューム、Data Protector のインストール先と構成情報を含むボリューム) は自動的に復元されます。

### 4. フェーズ 3

- a. Data Protector の標準復元手順を使用して、ユーザーデータおよびアプリケーションデータを復元します。

- ① **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、Linux 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、準備手順、および復旧手順を説明します。「Linux システムでの高度な復旧作業」(101 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システムと、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。詳細は、『HP Data Protector インストールおよびライセンスガイド』を参照してください。
- ターゲットシステムのハードウェア構成は、オリジナル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。これには、SCSI の BIOS 設定 (セクターの再マッピング) 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必要があります。
- 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 800MB 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。
- システムの BIOS は、El-Torito 規格で定義されている起動可能 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 アドレッシングによるハードディスクドライブへの読み取り/書き込みアクセスをサポートしている必要があります。BIOS のオプションは、システムของผู้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。
- SAN ブート構成では、ターゲットシステムの次の項目が、オリジナルシステムの項目と同一であることを確認します。
  - ローカルの HBA の BIOS パラメータ
  - SAN ディスクの LUN 数
- マルチパス SAN ディスク構成では、ターゲットシステムのディスクの LUN と WWID はオリジナルシステムのディスクの LUN と WWID と同一でなければなりません。

## 制限事項

- Linux システム上に Linux システム用の DR ISO イメージを作成する必要があります。他のシステム (Windows、HP-UX、Solaris) 用の DR ISO イメージを作成することはできません。この制限事項は SRD ファイルの更新や他のタスクには適用されません。
- 新しいディスクのサイズは、リカバリ対象ディスク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。
- CONFIGURATION という名前のマウントポイントがあり、そこに SystemRecoveryData ディレクトリが含まれている場合、SystemRecoveryData ディレクトリ内のデータはバックアップされません。

- ディスク ID は一意であり、ディスクのシリアル番号によって異なるため、ディスク ID を使用してディスクをマウントしないでください。障害発生時に、ディスクを交換して新しいディスクに新しい ID を割り当てることも可能ですが、その場合は結果的にディザスタリカバリが失敗します。
- SAN ブート構成のリカバリは、Red Hat Enterprise Linux 5.x システム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行う前に、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『HP Data Protector ディザスタリカバリガイド』を参照してください。  
[「Linux システムでの高度な復旧作業」 \(101 ページ\)](#) も参照してください。

- ① **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。

### 前提条件

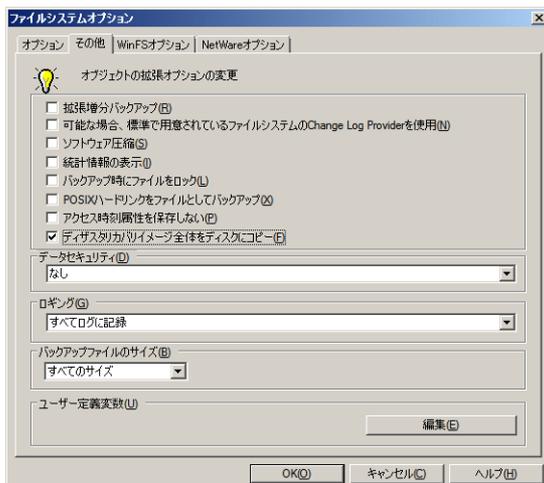
- クライアント全体のフルバックアップを実行します (CONFIGURATION オブジェクトを含む)。Cell Manager をバックアップする場合は、内部データベースも選択してください。  
 『HP Data Protector ヘルプ』の索引の「バックアップ、構成」を参照してください。

## DR IOS 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、クライアントシステム全体のフルバックアップ時に 1 つの大きなファイルにパックされてバックアップメディアに保存されます (場合によっては 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. クライアントシステム全体のフル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、『HP Data Protector ヘルプ』の索引「作成、バックアップ仕様」を参照してください。
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. [その他] タブをクリックし、[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。

### 図 9 [その他] 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. クライアント全体のフル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、『HP Data Protector ヘルプ』の索引「作成、バックアップ仕様」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. [その他] タブをクリックし、[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 イメージファイルはデフォルトで、Cell Manager の

`Data_Protector_program_data\Config\Server\dr\p1s` ディレクトリ (Windows Server 2008 の場合)、`Data_Protector_home\Config\Server\dr\p1s` (その他の Windows システムの場合)、または `/etc/opt/omni/server/dr/p1s` ディレクトリ (UNIX システムの場合) 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` など) を指定します。『HP Data Protector ヘルプ』の索引「グローバルオプションファイル、変更」を参照してください。



**ヒント:** あて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、マウントポイントを作成するか (Windows の場合)、他のボリュームへのリンクを作成 (UNIX の場合) できません。

## 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、Cell Manager に自動的にエクスポートされます。エクスポート先のファイルは、`Data_Protector_program_data\Config\Server\export\keys\DR-ClientName-keys.csv` (Windows Server 2008 の場合)、`Data_Protector_home\Config\Server\export\keys\DR-ClientName-keys.csv` (その他の Windows システムの場合)、または `/var/opt/omni/server/export/keys/DR-ClientName-keys.csv` (UNIX システムの場合) です。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ために準備した各バックアップの正しい暗号化キーがあることを確認します。

## 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 システムの場合) または `/etc/opt/omni/server/dr/p1s` ディレクトリ (UNIX システムの場合) 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`)。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、ディザスタリカバリ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、PIS 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。

① **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。

**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 ISO イメージの作成

DR ISO イメージを作成するには、以下の手順を実行します。

1. コンテキストリストで **[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、DR 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、**[バックアップからイメージファイルを復元]** をクリックします。**[次へ]** をクリックします。
7. DR ISO イメージ (recovery.iso) の保存先のディレクトリを選択します。
8. **[完了]** をクリックします。ウィザードが終了し、DR ISO イメージが作成されます。
9. ISO9660 形式をサポートしている CD 書き込みツールを使用して、DR ISO イメージを CD に書き込みます。

① **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

障害が発生したシステムでディザスタリカバリを正しく実行するには、以下のものが必要です。

- 問題のある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全体の正常なフルバックアップ
- Data Protector ディザスタリカバリ CD

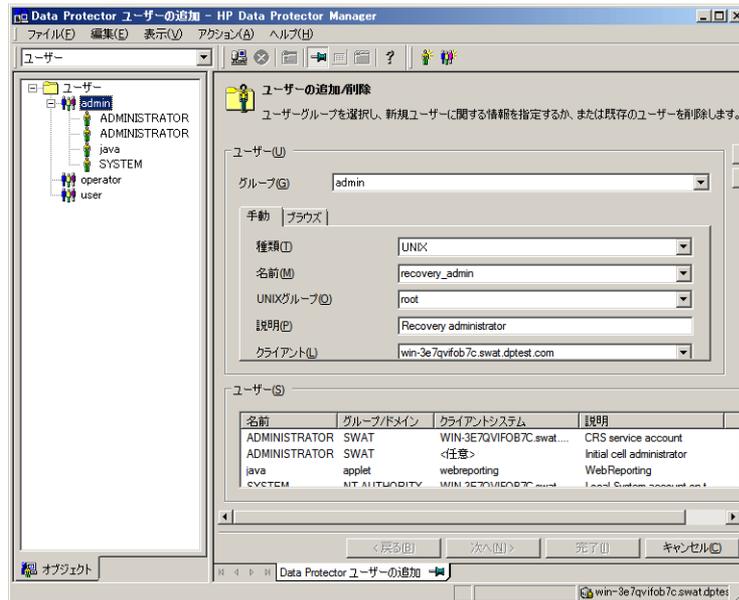
Linux クライアントのディザスタリカバリを実行する手順を以下に示します。

1. オフラインディザスタリカバリを行う場合を除き、Cell Manager の Data Protector の Admin ユーザーグループに、以下のプロパティが設定されたアカウントを追加します。
  - 復元の開始
  - 別のクライアントへ復元
  - ルートユーザーとして復元

**注記:** ディザスタリカバリ手順を実行できるのは、**ルートユーザーのみ**です。

ユーザーの追加の詳細については、『HP Data Protector ヘルプ』の検索キーワード「Data Protector ユーザーの追加」を参照してください。

## 図 10 ユーザーアカウントの追加



**注記:** セル内のクライアント間で暗号制御通信を使用している場合、復旧の開始前に、Cell Manager 上の [セキュリティの例外] リストにクライアントを追加する必要があります。ローカルデバイスを使用している場合を除き、Cell Manager の [セキュリティの例外] リストに Media Agent クライアントも追加する必要があります。

- 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。
- 以下のメッセージが表示されたら、**Enter** を押します。Enter を押してディザスタリカバリ CD からブートします。
- 先に DR OS がメモリーにロードされてから、範囲メニューが表示されます。復旧の対象範囲を選択します。4 つの異なる復旧対象範囲があり、2 つの追加オプションがあります。
  - [再起動]:**ディザスタリカバリは実行されず、システムが再起動されます。
  - [デフォルト復旧]:**Data Protector インストールファイルと構成ファイルが格納されている /boot ボリュームと /(ルート) ボリューム (/opt、/etc、および /var) を復旧します。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]:**/boot ボリュームと /(ルート) ボリュームだけが復旧されます。
  - [完全復旧]:**重要なボリュームだけでなく、すべてのボリュームが復元されます。
  - [共有ボリュームを含む完全復旧]:**ボリュームがすべて復旧されます。バックアップ時にロックされていた共有ボリュームもこれに含まれます。
  - [シェルの実行]:**  
Linux シェルを実行します。これは、詳細な構成や復旧作業に使用できます。
- 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リカバリプロセスを停止した後、オプションを変更します。[復元の実行] を選択すると、リカバリが続行されます。

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。  
復号に AES キーファイルを使用しますか? [Y/N]  
**[Y]** キーを押します。  
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) クライアントで使用可能であることを確認し、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。「編集後の SRD ファイルを使用した復旧」(103 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。
9. ステップ 1 で作成したクライアントのローカル Data Protector アカウントがディザスタリカバリ前に Cell Manager に存在していなかった場合は、このアカウントを Cell Manager の Data ProtectorAdmin ユーザーグループから削除します。
10. Cell Manager の復旧や、高度な復旧作業 (SRD ファイルの編集など) を行っている場合は、特別な手順が必要になります。詳細については、「Data Protector Cell Manager 固有の復元手順」(101 ページ) および「Linux システムでの高度な復旧作業」(101 ページ) を参照してください。
11. Data Protector の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。

## Linux 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、Linux クライアントと Cell Manager 用の自動化された Data Protector の復旧方法の 1 つで、ユーザーの操作は最小限に抑えられています。サポートされるオペレーティングシステムの詳細は、(<http://support.openview.hp.com/selfsolve/manuals>) にある最新のサポート一覧を参照してください。

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。

その後、ディザスタリカバリオペレーティングシステム (DR OS) が実行され構成されます。ディスクのフォーマットとパーティション作成も実行され、最終的に、オリジナルのオペレーティングシステムが Data Protector とともにバックアップ時の状態に復旧されます。

- ① **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。

OBDR の手順では、選択した復旧範囲に応じてボリュームが復旧されます。その他のパーティションは、Data Protector の標準復元手順で復旧できます。

## 概要

Linux 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 ワンボタンディザスタリカバリ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**

デフォルトでは、クリティカルボリューム (ブートボリューム、ルートボリューム、Data Protector のインストール先と構成情報を含むボリューム) が復元されます。
4. **フェーズ 3**

Data Protector の標準復元手順を行って、残りのボリュームを復元します。

① **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、Linux システム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、および復旧作業について説明します。[Linux システムでの高度な復旧作業] (101 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 Java GUI クライアントコンポーネントが、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。また、DR CD ISO イメージを準備するシステムには、自動ディザスタリカバリコンポーネントをインストールしておく必要があります。詳細は、『HP Data Protector インストールおよびライセンスガイド』を参照してください。
- OBDR を実行できるシステム構成にしておく必要があります。システムの BIOS は、El-Torito 規格で定義されている起動可能 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、El-Torito 規格で定義されている起動可能 CD をサポートしている必要があります。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。

サポートされるシステム、デバイス、メディアの詳細については、テープとハードウェアの互換性一覧表および最新のサポート一覧 (<http://support.openview.hp.com/selfsolve/manuals>) を参照してください。
- ターゲットシステムのハードウェア構成は、オリジナル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。これには、SCSI の BIOS 設定 (セクターの再マッピング) 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必要があります。
- Data Protector がインストールされているボリュームの空き容量は 800MB 以上でなければなりません。このスペースは、一時イメージの作成に使用されます。
- 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。
- SAN ブート構成では、ターゲットシステムの次の項目が、オリジナルシステムの項目と同一であることを確認します。
  - ローカルの HBA の BIOS パラメータ

- SAN ディスクの LUN 数
- マルチパス SAN ディスク構成では、ターゲットシステムのディスクの LUN と WWID はオリジナルシステムのディスクの LUN と WWID と同一でなければなりません。

## 制限事項

- 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。
- 新しいディスクのサイズは、リカバリ対象ディスク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。
- CONFIGURATION という名前のマウントポイントがあり、そこに SystemRecoveryData ディレクトリが含まれている場合、SystemRecoveryData ディレクトリ内のデータはバックアップされません。
- USB テープデバイスはサポートされていません。
- ディスク ID は一意であり、ディスクのシリアル番号によって異なるため、ディスク ID を使用してディスクをマウントしないでください。障害発生時に、ディスクを交換して新しいディスクに新しい ID を割り当てることも可能ですが、その場合は結果的にディザスタリカバリが失敗します。
- SAN ブート構成のリカバリは、Red Hat Enterprise Linux 5.x システム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行う前に、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『HP Data Protector ディザスタリカバリガイド』を参照してください。  
[Linux システムでの高度な復旧作業] (101 ページ) も参照してください。

- ① **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。『HP Data Protector 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。

## OBDR バックアップ

OBDR を行って復旧するシステムにインストールされている GUI で OBDR バックアップ仕様をローカルに作成します。作成後、その仕様を他のシステムから実行します。

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、『HP Data Protector ヘルプ』の検索キーワード「バックアップオプション」を参照してください。
7. [次へ] をクリックして、[スケジューラ] ページを表示します。ここでは、バックアップの実行スケジュールを設定できます。『HP Data Protector ヘルプ』の索引「特定の日時に対するバックアップのスケジュール設定」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。変更されたバックアップ仕様を OBDR バックアップ仕様として保存すると、そのバックアップ仕様の OBDR に固有のオプションが上書きされなくなります。標準のバックアップ仕様として保存すると、OBDR に使用できなくなることがあります。
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。  
バックアップが暗号化されている場合、実行後コマンドとして実行される `omnisrupdate` ユーティリティによって暗号化 ID が自動的にエクスポートされます。

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。

- ① **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。

## 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、Cell Manager に自動的にエクスポートされます。エクスポート先のファイルは、`Data_Protector_program_data\Config\Server\export\keys\DR-ClientName-keys.csv`(Windows Server 2008 の場合)、`Data_Protector_home\Config\Server\export\keys\DR-ClientName-keys.csv`(その他の Windows システムの場合)、または `/var/opt/omni/server/export/keys/DR-ClientName-keys.csv`(UNIX システムの場合) です。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ために準備した各バックアップの正しい暗号化キーがあることを確認します。

## 復旧

障害が発生したシステムでディザスタリカバリを正しく実行するには、以下のものがが必要です。

- 影響を受け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。

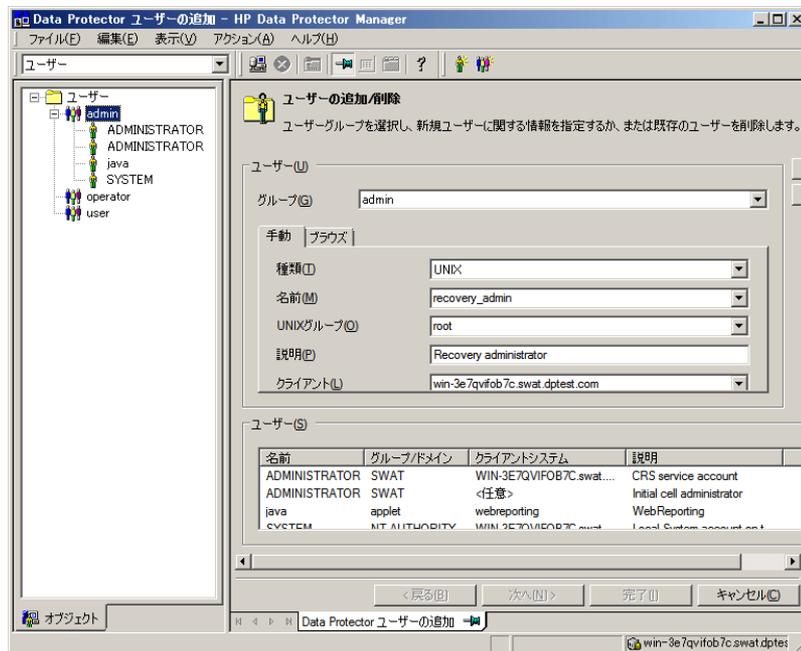
Linux システムのワンボタンディザスタリカバリの詳細な手順を以下に示します。

1. オフラインディザスタリカバリを行う場合を除き、Cell Manager の Data Protector の Admin ユーザーグループに、以下のプロパティが設定されたアカウントを追加します。
  - 復元の開始
  - 別のクライアントへ復元
  - ルートユーザーとして復元

**注記:** ディザスタリカバリ手順を実行できるのは、**ルートユーザーのみ**です。

ユーザーの追加の詳細については、『HP Data Protector ヘルプ』の検索キーワード「Data Protector ユーザーの追加」を参照してください。

### 図 11 ユーザーアカウントの追加



**注記:** セル内のクライアント間で暗号制御通信を使用している場合、復旧の開始前に、Cell Manager 上の [セキュリティの例外] リストにクライアントを追加する必要があります。ローカルデバイスを使用している場合を除き、Cell Manager の [セキュリティの例外] リストに Media Agent クライアントも追加する必要があります。

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。
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。詳細は、デバイス付属のドキュメントを参照してください。

5. 先に DR OS がメモリーにロードされてから、範囲メニューが表示されます。復旧の対象範囲を選択します。4 つの異なる復旧対象範囲があり、2 つの追加オプションがあります。
  - **[再起動]**:ディザスタリカバリは実行されず、システムが再起動されます。
  - **[デフォルト復旧]**:Data Protector インストールファイルと構成ファイルが格納されている /boot ボリュームと /(ルート) ボリューム (/opt、/etc、および /var) を復旧します。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]**:/boot ボリュームと /(ルート) ボリュームだけが復旧されます。
  - **[完全復旧]**: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]**:ボリュームがすべて復旧されます。バックアップ時にロックされていた共有ボリュームもこれに含まれます。
  - **[シェルの実行]**:  
Linux シェルを実行します。これは、詳細な構成や復旧作業に使用できます。
6. 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、オプションを変更します。**[復元の実行]** を選択すると、ディザスタリカバリが継続されます。
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、次のプロンプトが表示されます。

復号に AES キーファイルを使用しますか? [Y/N]

**[Y]** キーを押します。

キーストア (DR-ClientName-keys.csv) がクライアントで使用可能であることを (たとえば、CD-ROM、フロッピーディスク、USB フラッシュドライブを挿入することで) 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継続されます。
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、この手順を継続する前に 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」 \(103 ページ\)](#) 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。
10. **ステップ 1** で作成したクライアントのローカルの Data Protector 管理者アカウントがディザスタリカバリ前に Cell Manager に存在していなかった場合は、このアカウントを Cell Manager の Data ProtectorAdmin ユーザーグループから削除します。
11. Cell Manager の復旧や、高度な復旧作業 (SRD ファイルの編集など) を行う場合は、特別な手順が必要になります。詳細は、[「Linux システムでの高度な復旧作業」 \(101 ページ\)](#) を参照してください。
12. Data Protector の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。

## Linux システムでの高度な復旧作業

この項では、Cell Manager の詳細の復元など、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。

### Data Protector Cell Manager 固有の復元手順

この項では、Linux 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 ProtectorGUI 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。メディアのリサイクルの詳細については、『HP Data Protector ヘルプ』の検索キーワード「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、以下のコマンドを実行して Data Protector プロセスを停止し、Data Protector の tmp ディレクトリの内容を削除します。

```
/opt/omni/bin/omnisv -stop  
rm /var/opt/omni/tmp/*  
/opt/omni/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 ProtectorGUI を使ってエクスポートします。メディアのエクスポートの詳細については、『HP Data Protector ヘルプ』の検索キーワード「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 ProtectorGUI を使ってインポートします。メディアのインポートの詳細については、『HP Data Protector ヘルプ』の検索キーワード「インポート、メディア」を参照してください。

## 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、LinuxCell 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。

① **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。

『HP Data Protector ディザスタリカバリガイド』の「ディザスタリカバリの計画と準備」を参照してください。

- 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。

『HP Data Protector ディザスタリカバリガイド』の「ディザスタリカバリの計画と準備」を参照してください。

① **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 が障害の影響を受けている場合は 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おく必要があります。

- ❶ **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。

『HP Data Protector ディザスタリカバリガイド』の「ディザスタリカバリの計画と準備」を参照してください。

- ❷ **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。

## 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。

- ❸ **重要:** このファイルは、Linux システムで一般的な UTF-8 形式ではなく、Unicode UTF-16 形式でエンコードされています。

- ※ **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システム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`)

指定可能な `-devtype` オプションの値については、`sanconfman` 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 (-devioct1)
- ライブラリスロット (-physloc)
- 論理ライブラリ名 (-storname)

ファイルを編集したら、Unicode(UTF-16) 形式で元の場所に保存します。

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、同じバックアップデバイスが同じ SCSI アドレスのクライアント new\_mahost.company.com に接続されているとします。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 -devioct1。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ために、HP Ultrium スタンドアロンデバイスを使用してバックアップを実行した場合を考えてみましょう。デバイス名は Ultrium\_system1 で、MA ホスト system1 (linux) に接続されているとします。ただし、ディザスタリカバリには、MA クライアント system2 (linux) に接続されている Ultrium\_system2 というドライブを使用し、論理ライブラリ名が Autoldr\_system1 である HP Ultrium ロボティクスライブラリを使用するとします。

最初に、system2 で devbra -dev コマンドを実行し、構成済みデバイスと構成情報のリストを表示します。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_system1" -devaddr /dev/nst0 -devtype 13 -devpolicy 1
-mahost system1.company.com
```

これを次のように置き換えます。

```
-dev "Ultrium_system2" -devaddr /dev/nst1 -devtype 13 -devpolicy 10
-devioct1 /dev/sg1 -physloc " 2 -1" -storname "AutoLdr_system2" -mahost
system2.company.com.
```

① **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。

手順

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. 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 [Q] キーを押してこのウィザードを停止し、[Install Only] オプションを選択します。このオプションでは、最低バージョンの Data Protector がターゲットシステムにインストールされるだけです。**[Install Only]** オプションを選択した場合は、ディザスタリカバリのフェーズ 2 は自動的に開始されません。

2. 別のシェルに切り替えます。

SRD ファイル `/opt/omni/bin/recovery.srd` を編集します。詳細については、「[システム復旧データ \(SRD\) の更新と編集](#)」(24 ページ) を参照してください。

3. SRD ファイルを編集して保存したら、`/opt/omni/bin` ディレクトリで以下のコマンドを実行します。

```
omnidr -srd recovery.srd -drimini /opt/omni/bin/drim/drecovery.ini
```

4. 復旧が終了したら、元のシェルに戻り、通常の EADR/OBDR 復旧手順の次の作業に進みます。

## 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」(106 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。確認方法については、『HP Data Protector ヘルプ』の検索キーワード「パッチ」を参照してください。
- Data Protector の一般的な制限事項、既知の問題、および回避方法については、『HP Data Protector 製品案内、ソフトウェアノートおよびリファレンス』を参照してください。
- サ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://support.openview.hp.com/selfsolve/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 (Windows システム) または `/var/opt/omni/tmp` ディレクトリ (UNIX システム) にあるログファイルで、自動ディザスタリカバリ方法 (EADR、OBDR、ASR) に関するメッセージが記録されています。エラーが発生した場合は、このファイルを調べてください。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次の 4 つのタイプ (レベル) がありますが、そのレベルは、バックアップセッションの最後に Data Protector GUI に表示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: 重大なエラー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、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 AUTODR.log に記録されていたとします。
- 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。

Windows システムで AUTODR.log ファイルに記録される最も一般的なメッセージを以下に示します。

- `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

ディザスタリカバリセッションの際のデバッグ設定とデバッグログの場所は、以下のようにディザスタリカバリ段階によって異なります。

- DR OS の準備中は、デバッグログは `x:\$DRM$\log` (Windows Vista、Windows 7、および Windows Server 2008 の場合)、`c:\$DRM$\log` (その他の Windows システムの場合)、または `/opt/omni/bin/drim/log/Phase1.log` (Linux システムの場合) に自動的に保存されます。
- データ復元手順の際は、ディザスタリカバリウィザードで**手動でデバッグオプションを選択**して、デバッグを有効にする必要があります。

### Windows システム

データの復旧中にデバッグログを作成できるようにするには:

1. ディザスタリカバリ ウィザードで、[デバッグ] ボタンの左のチェック ボックスを選択します。

図 12 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

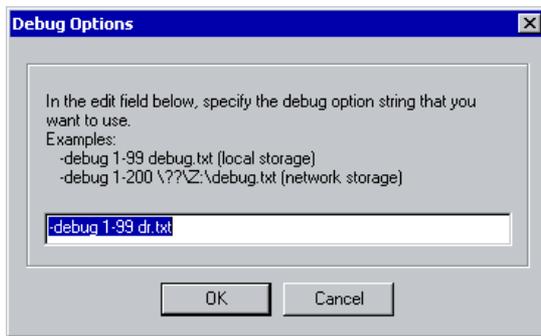


2. デバッグを保存する場所などのデバッグオプションを指定するには、[デバッグ] をクリックします。デフォルトでは、%SystemRoot%\system32\OB2DR\tmp ディレクトリにデバッグが保存されます。

**注記:** Windows Vista、Windows 7、および Windows Server 2008 の各システムでは、ディレクトリ %SystemRoot%\system32\OB2DR\tmp は RAM ディスク上にあります。RAM ディスクのサイズは、一般に 32 MB 未満に制限されています。RAM ディスクの使用量がこの制限値に到達すると、Data Protector は予期しない動作を始める可能性があります。したがって、ディザスタリカバリセッションで大量のデバッグ情報が発生することが予想される場合は、デバッグ情報の保存場所を変更する必要があります。

3. [デバッグオプション] ウィンドウが表示されます。

図 13 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ネットワーク上の共有領域をドライブ文字にマッピングします。例:

```
NET USE X:\\SystemName\SharedFolderForDebugOutput Password /USER:Username
```

## Linux システム

データの復旧中にデバッグログを作成できるようにするには:

1. ディザスタリカバリウィザードで、[ディザスタリカバリプロセスの開始]→[デバッグの使用] を選択します。
2. デバッグオプション画面で、デフォルトオプションの使用またはデフォルトオプションの変更を選択します。

以下のオプションから1つを選びます。

- 1) [デフォルトのデバッグオプション"-debug 1-99 dr.txt"を使用する]
- 2) [別のデバッグオプションを指定する]
- 3) [デバッグオプションを無効にする]

Command [1-3]:

---

**注記:** Linux システムでは、デバッグログが保存されるディレクトリは RAM ディスク上にあります。RAM ディスクのサイズは通常制限されています。RAM ディスクの使用量がこの制限値に到達すると、Data Protector は予期しない動作を始める可能性があります。したがって、ディザスタリカバリ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変更する必要があります。場所を変更するには、[別のデバッグオプションを指定する] を選択します。

---

3. デバッグパラメータを入力できる新しい画面が表示されます。

例:

```
-debug 1-99 debug.txt (ローカルストレージ)  
-debug 1-200 //servername/sharename/debug.txt (Windows共有)  
-debug 1-200 servername:/sharename/debug.txt (NFS共有)
```

Specify the debug option string that you want to use:

デバッグファイルを Windows 共有ディスクまたは NFS 共有フォルダに保存することを選択できます。

デバッグログをそこに保存するには、共有フォルダをマウントする必要があることに注意してください。Alt-F3 を押して別のコンソールに切り替え、共有をマウントします。

## 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 システム

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除く) の実行中に omnirc オプションを設定する必要がある場合は、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 14 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. 以下のコマンドを実行します。

```
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。

### Linux システム

1. ディザスタリカバリウィザードで、**Alt-F3** キーを押して別のコンソールに切り替えます。
2. コンソールで、次のコマンドを実行します。

```
echo variable > /opt/omni/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。例:

```
echo OB2RECONNECT_RETRY=1000 > /opt/omni/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。

3. `exit` と入力してシェルを終了し、ディザスタリカバリウィザードでディザスタリカバリを続行します。

## Windows システムでの 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.tmp1` 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。

## 共通の問題

### 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。

### 対処方法

オリジナルメディアセットが使用できないまたは損傷した場合に、メディアコピーまたはオブジェクトコピーから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。  
『HP Data Protector ヘルプ』の索引「エクスポート、メディア」および「[システム復旧データ \(SRD\) の更新と編集](#)」(24 ページ)を参照してください。
- メディアコピー: SRD ファイル内のオリジナルメディアのメディア ID をメディアコピーのメディア ID に書き換えます。その後、Data Protector の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。  
「[システム復旧データ \(SRD\) の更新と編集](#)」(24 ページ)を参照してください。

## Windows システム上の問題

### 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。

#### 対処方法

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。詳細は、「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

##### **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。

#### 対処方法

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。

「ディザスタリカバリ中の `omnirc` オプションの設定」 (109 ページ) を参照してください。

#### 問題

##### **ディザスタリカバリの実行時のデフォルトのネットワーク設定が正しくないためにディザスタリカバリに失敗する**

例:

Windows Server 2003 では、障害の発生後にネットワークが再構成されるので、復旧中に Data Protector によってデフォルトで使用される以前のネットワーク構成は失われてしまいます。

#### 対処方法

Windows Server 2003 の場合:

次の手順を行って DHCP ネットワーク構成を選択します。

ディザスタリカバリを開始すると、Data Protector に「ネットワークを DHCP に切り替えるには、この後 10 秒以内に F8 を押します」と表示されます。

F8 を押します。Data Protector で以前のネットワーク設定が無視され、DHCP に基づいた新しい構成に切り替えられます。

#### 問題

### Cell Manager とクライアントが異なるドメインに存在する場合に、EADR と OBDR オンラインリカバリが失敗する

#### 操作

次の操作を実行して、ネットワークが適切に構成されていることを確認します。

1. Cell Manager とクライアントシステムの両方にある `host` ファイルを更新します。これらのファイルには、Cell Manager のホスト名と、クライアントのホスト名、および IP アドレスが記述されている必要があります。
2. Cell Manager とクライアントの間の `ping` リクエストが正しい値を返すかどうかを確認します。問題が発生する場合、ネットワーク管理者に問い合わせてください。
3. `omnicheck -dns` コマンドを使用して Cell Manager とクライアントの間の DNS 解決が正しいかどうかを確認します。詳細は、`omnicheckman` ページを参照してください。問題が発生する場合、ネットワーク管理者に問い合わせてください。

## 半自動ディザスタリカバリ

#### 問題

**Drstart レポート: <filename>" をコピーできない。**

このエラーメッセージは、`drstart` ユーティリティが指定ファイルをコピーできないことを意味します。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

#### 対処方法

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の実行中に、以下のエラーメッセージが返されることがあります。

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。)

以前は使用していなかったドライブ文字を選択した場合は、新しいディスク上にパーティションが作成される時点でオブジェクトが復元されます。

ディザスタリカバリ処理では、オブジェクトを復元する前にディスク情報がチェックされます。このとき内部関数により、ディスクアドミニストレータにより作成された `Information`

レジストリ値が読み取られます。ディスクアドミニストレータが複数回開始された場合は、Information 値の形式が変更されて、パーサーは失敗します。

#### 対処方法

HKEY\_LOCAL\_MACHINE\SYSTEM\Disk レジストリ値から Information 値を削除して、ディスクアドミニストレータを再起動します。

#### 問題

##### オペレーティングシステムが見つからない

ディスクデリバリーによるディザスタリカバリの実行中に、以下のエラーメッセージが返されることがあります。

オペレーティングシステムが見つからない

Windows システムの最後のスタートアップ時にエラーが報告され、失敗します。

#### 対処方法

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」 \(24 ページ\)](#)」の項のステップ 4 を参照してください。

#### 問題

##### Media Agent クライアントのディスクデリバリーによる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せん。

#### 対処方法

これを回避する方法には以下の 2 通りがあります。

- メディアを別のメディアプールに移動します。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

### EADR および OBDR の共通の問題

#### 問題

##### 自動ディザスタリカバリ情報が収集できない

EADR 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

## 対処方法

- 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ーがデバイスを「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でない場合、`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`)。

## 対処方法

- `%SystemRoot%` フォルダにないサービスやドライバ (ウイルス 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

## 対処方法

スイッチ、ケーブルなどに問題がないかどうかを確認します。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) が復旧中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。Windows では、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

### コンピュータが応答しなくなった

## 対処方法

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。

## Windows システム上の問題

### 問題

#### 自動ログオンが正常動作しない

### 対処方法

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

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

### 対処方法

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

### 問題

#### Microsoft Cluster Server クライアントで CD ISO イメージの作成が失敗する

Microsoft Cluster Server 環境では、ISO イメージをクラスタクライアントに作成することはできません。ファイルシステムの復元は、期待どおりに機能します。

この問題が発生するのは、Data Protector が、ドメイン名 (物理的なクライアントの IP に解決される) ではなくクラスタ IP (仮想的な IP) の使用を試みるのが原因です。

### 対処方法

ネットワークサービスの接続順序を、ローカルエリア接続が先頭になるように変更します。

### 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。

### 対処方法

- 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、Windows 7、Windows Server 2008 のいずれかのシステムで、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。

## 対処方法

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。「ディザスタリカバリ用の DR OS イメージを準備する」(42 ページ) (EADR の場合) または「OBDR 用のバックアップ仕様を作成する」(51 ページ) (OBDR の場合) を参照してください。

## 問題

### 暗号制御通信が有効になっている場合に、Cell Manager がクライアントのオンライン復元中に応答しない

Windows Vista、Windows 7、または Windows Server 2008 システムでは、Cell Manager で暗号化制御通信が有効に設定され、例外としてクライアントが追加されている状態で、DHCP 環境でクライアントのオンラインディザスタリカバリを実行すると、オンライン復元が失敗し、ディザスタリカバリはオフライン復元で続きます。これは、新しい一時的なホスト名はデフォルトで DR OS に対して生成されるからです。

## 操作

ディザスタリカバリで、Data Protector が表示されているときに **F8** を押すことで、オリジナルネットワーク構成に切り替えます。

F8 を押してオリジナルネットワークに切り替えてください...

また、DR OS が起動した後にシステムのホスト名を確認し、復元を開始する前に Cell Manager で例外としてこの名前を追加します。詳細は、『HP Data Protector ヘルプ』の索引「暗号制御通信」を参照してください。

## Windows Itanium システム上の問題

## 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。

## 対処方法

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리를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)。

## 対処方法

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。

- 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。
- 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。
- 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。

## Linux システム上の問題

### 問題

#### クライアントバックアップ中に警戒域のエラーまたは警告が表示される

クライアントバックアップ中に次の警戒域のエラーが表示される場合があります。

stat() を実行できません: ([2] そのようなファイルまたはディレクトリはありません)  
ファイルの容量が、ファイルを開いたときよりも減っています

このような警告およびエラーは、Data Protector の一時ディレクトリ内のファイルが変更されたことにより表示される可能性があります。この問題は、/CONFIGURATION マウントポイントと / (ルート) マウントポイントを同時にバックアップした場合などに発生する可能性があります。

### 対処方法

バックアップ仕様から /opt/omni/bin/drim/tmp および /opt/omni/bin/drim/log の各ディレクトリを除外してください。

## 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。

### 対処方法

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。

### 対処方法

- 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 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 (needs 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 need to be modified for this system"
# exit 1
#
cd /sbin/rc1.d
mv K430dce../rc0.d/K109dce
mv K500inetd../rc0.d/K110inetd
mv K660net../rc0.d/K116net
mv K900swagentd ../rc0.d/K120swagentd
```

### 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、「Windows 上でのディザスタリカバリ」(27 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		
IPv4 用の TCP/IP 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	
IPv6 用の TCP/IP プロパティ	IP アドレス	
	サブネットプレフィックスの長さ	
	デフォルトゲートウェイ	
	優先度の高い DNS サーバー	
	代替 DNS サーバー	
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	

## B 異なるハードウェアへの復旧

**注記:** 異なるハードウェアへの復旧は、「Windows システムの拡張自動ディザスタリカバリ」(35 ページ)の拡張です。ここに記載されている情報と併せてそちらも参照してください。

ハードウェア障害または同様の障害が発生した後で、一部またはすべてのハードウェアがオリジナルのハードウェアと異なるシステム(**異なるハードウェア**)に対してバックアップを復元する必要がある場合があります。

異なるハードウェアの復旧では、標準的な EADR と OBDR の手順に次の手順を追加します。

1. バックアップ時にディザスタリカバリモジュールは、ネットワーク構成情報とハードウェア情報も収集します。
2. これにより、DR OS イメージへのクリティカルデバイスのドライバの挿入が可能になり、これらのドライバが復元時に使用可能になります。見つからないドライバがある場合は、復元時にそれらを手動で挿入することもできます。
3. 復元中ネットワークとハードウェア情報は、復元された OS に対してネットワークを適切に構成およびマッピングし、さらに見つからない不可欠なハードウェアを検出するために使用されます。

### 異なるハードウェアの復旧が必要になる場合

- **ハードウェア障害**

異なるハードウェアの復旧が必要になるのは、ストレージコントローラやプロセッサ、マザーボードなどのブートに必要なハードウェアの一部に障害が発生し、同一でないハードウェアとの交換が必要になったときです。

- **障害**

マシン全体の障害が発生して次のような状況になった場合、異なるハードウェアの復旧が必要になります。

- 予算に対する制限や、障害が発生しているマシンの使用期間、またはその他の原因により、適合するマシンが見つからない。
- システムの停止期間が長期間にならないようにするため、システムをすぐに稼働させる必要がある。

このような状況で、異なるハードウェアの復旧を使用すると、オリジナルシステムの正確なクローンが必要なくなるため、経費を低減させることができます。

- **移行**

次の状況では、異なるハードウェアの復旧が必要になります。

- OS の再インストールおよび再構成を選択できない、より高速またはより新しいハードウェアである別のマシンへの移行。
- 物理マシンから仮想環境へ、またはその逆への移行。

ディザスタリカバリモジュールの見地では、仮想環境は、他の仮想プラットフォームまたは物理プラットフォーム上で作成されたシステムバックアップを復元するために、重要なドライバを用意するのに必要となる別のハードウェアプラットフォームとなります。仮想環境には、後述する制限と要件も適用されます。

### 概要

異なるハードウェアの復旧フェーズは 54 ページで説明したとおりですが、次の点で異なります。

- **フェーズ 0:** ネットワーク構成とハードウェアについての追加情報を収集します。

- **フェーズ 1:** マシンは、ディザスタリカバリ実行可能ファイルがディスク、ファイルシステム、ネットワーク、WIN32 API にアクセスできる状態になります。復旧に必要なデバイスがチェックされます。見つからないドライバがあると、それらを用意するよう促すメッセージが表示されます。
- **フェーズ 2:** OS の復元は同じ処理を実行しますが、その後、さらに次のサブフェーズが発生します。
  - **フェーズ 2a:** 重要なドライバの挿入、レジストリの更新、ネットワークのマッピングを通して、復元されたオペレーティングシステムを準備し、ハードウェアに適用します。
- **フェーズ 3** は同じ処理を実行しますが、フェーズ 2 で復元されなかったデータを復元します。

## 要件

- ターゲットマシンに対して少なくともブートに必要なドライバ (ネットワークドライバなど) をすべて用意する必要があります。これらのドライバは、イメージ作成時に直接イメージに追加する (推奨) ことも、復元 (フェーズ 1) 時に読み込むこともできます。また、ローカルの復元を試行する場合は、ローカルに接続しているテープデバイスなどのバックアップデバイスのドライバも使用可能にする必要があります。  
詳細については、「[ドライバ](#)」 (123 ページ) を参照してください。
- 復元された OS の自動ネットワーク構成復元では、復元時にネットワークドライバを用意しておく必要があります。
- システム復元を行うには、少なくとも、バックアップシステムと同じディスク数 (ディスクサイズが同じまたはそれ以上) が必要になります。
- オリジナルの OS は、ターゲットマシン (サーバーまたはワークステーション) 上でハードウェアメーカーによってサポートされる必要があります。
- 異なるハードウェアを復旧する前に、ターゲットマシンのシステムファームウェアを最新の状態にすることをお勧めします。
- バックアップ中に異なるハードウェアのサポートを**無効にする**場合、バックアップするシステム上で `drm.cfg` ファイルを編集し `enable_disshw` オプションを 0 に設定します。
- システムには少なくとも 1 つの NTFS ボリュームを含める必要があります。NTFS ボリュームはバックアップフェーズ中に、VSS のストレージポイントとして機能します。

## 制限事項

- ディザスタリカバリモジュールでは、VSS ベースの OS バックアップに対する異なるハードウェアの復旧のみがサポートされます。ただし、Data Protector では、サポートされる OS プラットフォームに対する VSS ベースのバックアップは、デフォルトで有効になっています。
- 異なるハードウェアのサポートは、DR OS ベースのディザスタリカバリソリューションに対してのみ提供されます。これは、次の 32 ビットおよび 64 ビット (x64) の OS バージョン (最新のサービスパックがインストールされているもの) に対してのみ提供されます。
  - Windows Vista
  - Windows Server 2008
  - Windows 7
  - Windows Server 2008 R2

- 次の OS プラットフォームの復元の組み合わせがサポートされています。

復元元	復元先
64 ビットの OS プラットフォーム	64 ビットのハードウェア
32 ビットの OS プラットフォーム	32 または 64 ビットのハードウェア

- アップグレードされた OS の異なるハードウェアの復旧は、「ジェネリック」リカバリモードオプションを使用する場合のみサポートされます(「システムの復元」(124 ページ)を参照)。
- ネットワークカードのチーミング構成はサポートされていません。必要な場合は、OS を復元した後に再構成する必要があります。ディザスタリカバリモジュールは、物理的なネットワークカード構成のみを復元します。
- ディザスタリカバリモジュールは、INF ファイルを提供するドライバのみを挿入できます。グラフィックドライバのように独自のインストール手順があるドライバはサポートされておらず、これらのドライバはフェーズ 1 またはフェーズ 2a 時には挿入できません。ただし、ブートに必要なデバイスドライバについては、一般にメーカーが INF ファイルを提供します。
- ターゲットマシンのディスクは、同じホストアダプタバスタイプ (SCSI または SAS など) に接続しておく必要があり、そうでない場合は、復旧が失敗する場合があります。

## ドライバ

**注記:** DR OS イメージには、汎用の重要なドライバ (特にストレージコントローラ) の大規模なデータベースが含まれます。挿入するオリジナルドライバが見つからない場合、汎用のドライバが DR OS イメージに既に存在している可能性が高いです。

異なるハードウェアの復旧を可能にするには、新しいシステムの復元と起動に不可欠なドライバを入手する必要があります。以下のドライバを用意する必要があります。

- ターゲットシステムのすべてのストレージコントローラのドライバ。このドライバによって、復元またはブート時での基盤となるストレージの検出が可能になります。
- ネットワークの復元を可能にし、既存のドライバの保存場所にアクセスするためのネットワークカードドライバ、およびローカルの復元を試行する場合は、ローカルに接続されているバックアップデバイス (テープドライブなど) のドライバ。

準備フェーズ (フェーズ 0) のバックアップ中にオリジナルのハードウェアのドライバを DR OS イメージに含めることも、イメージの作成中に新しいハードウェアのドライバを追加することもできます。また、復元プロセス中にこれらのドライバを手動で追加することもできます。

ディザスタリカバリモジュールは復元プロセス中にブートに必要なドライバのみを検索しますが、ブートに必要でないドライバを DR OS イメージに追加し、その後「ドライバの読み込み」タスクメニューオプションを使用して復元中に挿入できます。

オペレーティングシステムをブートしたら、その他の見つからないハードウェアドライバをインストールする必要があります。

ドライバは、CD-ROM、DVD、USB キー/ドライブ、ネットワーク共有、または任意のローカルフォルダから挿入できます。

## 準備

### 注記:

この準備は、システムに対して各ハードウェア構成を変更した後に実行する必要があります。

準備は、EADR(「準備」(38 ページ)を参照) および DBDR(「準備」(50 ページ)を参照) の場合と同じですが、以下の変更点があります。

- ディザスタリカバリモジュールは、ネットワーク構成とハードウェア情報も収集します。

- ストレージやネットワーク、テープなどの重要なデバイスドライバを用意する必要があります。したがって、ディザスタリカバリモジュールは、イメージの作成時にドライバを DR OS イメージに挿入できます。「[ドライバ](#) (123 ページ) を参照してください。

## 復旧

### システムの復元

HP Data Protector ディザスタリカバリ GUI の「リカバリオプション」ページ ([ステップ 4](#)を参照) で異なるハードウェアの復旧を有効にすると、復元プロセス中にターゲットシステムに対してスキャンが実行され、見つからないドライバがないかがチェックされます。ストレージアダプタやテープデバイスとネットワークデバイス、ディスクコントローラなどの復元に必要なデバイスに見つからないドライバがあると、復元プロセスを続行するために、見つからないドライバを読み込むことを促すメッセージが表示されます。

次のステップを実行します。

1. ディザスタリカバリ手順中に「見つからないドライバを読み込みますか?」というメッセージが表示されたら、[はい] をクリックしてディザスタハードウェアウィザードを開始します。[いいえ] をクリックすると、ドライバの挿入手順がスキップされます。
2. [デバイスの選択] ページで、ドライバを読み込むデバイスを選択します。[次へ] をクリックします。
3. [ドライバの検索場所] ページで、ドライバを保存している実行中のシステム上の検索場所を指定します。お使いのシステムに対する検索を調整するには、[検索ツリーの深さ] オプションを使用できます。指定した場所に対して検索を実行して、見つからないドライバを探します。[次へ] をクリックします。

---

**注記:** 検索リストから指定した場所を削除するには、この場所を右クリックして、[削除] を選択します。

---

4. 指定した場所を検索して見つからないドライバを探すと、次のような結果が考えられます。
  - デバイスドライバが見つかった場合: [ドライバのパス] テキストボックスに、対応するドライバ情報ファイル (\*.inf) への完全パスが指定されます。このドライバが該当するドライバであれば、[次へ] をクリックします。
  - デバイスドライバが見つからなかった場合: [ドライバのパス] テキストボックスは空になります。次のいずれかの作業を行います。
    - 別のドライバを検索する場合は、[ブラウズ] をクリックします。[ファイルのブラウズ] ダイアログで、デバイスドライバのパスを選択して、[次へ] をクリックします。
    - このデバイスに対してドライバを読み込まない場合は、[ドライバのパス] テキストボックスを空のままにして、[次へ] をクリックして次のページに進むか、または [スキップ] をクリックしてウィザードを終了します。

---

**注記:** デバイスに対応しないドライバを指定すると、このドライバは無効となり、読み込むことはできません。このドライバが適切でない場合、変更するか、または読み込みをスキップできます。

---

5. [ドライバインストールの進行状況] ページで、デバイスドライバが正常に読み込まれたかどうかを確認できます。エラーが報告された場合、[再試行] をクリックしてドライバの再読み込みを試してください。[完了] をクリックします。

### OS の復元と準備

OS の復元プロセスは、標準的な EADR([ステップ 5](#)) および OBDR([ステップ 6](#)) プロセスでの処理と同じです。復元プロセスでは、この OS の復元プロセスの後のアプリケーションとファイルの復元に向けて OS を準備するために、復元した OS を異なるハードウェアに対して準備し、適合させます。このプロセスでは、ブートに必要なドライバの挿入、復元した OS のレジストリの更新、ネットワークのマッピングを実行します。

フェーズ 0 で実行中の DR OS イメージに読み込むか、OS の復元中に手動で追加したことにより、ブートに必要なドライバがすべて存在しているはずなので、これらのドライバの挿入は自動的に実行されます。ただし、ネットワークのマッピングを修正するには、ユーザーの操作が必要になる場合があります。

## ネットワークマッピングの修正

異なるハードウェアへの復旧が完了したら、ディザスタリカバリモジュールによって、復元しようとするシステム上のネットワークアダプタが、オリジナルシステムのネットワークアダプタと同じかどうかをチェックされます。ディザスタリカバリモジュールは、オリジナルシステムのネットワーク構成をターゲットシステムのネットワーク構成に常にマッピングできるわけではありません。たとえば、ターゲットシステムに1つのネットワークカードが搭載されているが、オリジナルシステムに複数のネットワークカードが搭載されている場合や、ターゲットシステムにネットワークアダプタを追加した場合などがそうです。こうした不一致が検出されたり、または適切なネットワークマッピングが自動的に決定できない場合、オリジナルのネットワークアダプタをターゲットシステム上で検出されたネットワークアダプタにマッピングできます。

---

**注記:** ネットワークマッピングは、使用可能なネットワークアダプタにのみ実行されます。ドライバが存在しないネットワークアダプタはマッピングできません。このため、復旧プロセスを開始する前に、ネットワークカードドライバを読み込む必要があります。

---

1. [ネットワークアダプタマッピング] ページで、[オリジナルネットワークアダプタ] ドロップダウンリストからオリジナルシステムのネットワークアダプタを選択します。[現在のネットワークアダプタ] ドロップダウンリストで、ターゲットシステムで使用可能なネットワークアダプタのいずれか1つを選択します。[マッピングの追加] をクリックします。作成したマッピングがリストに追加されます。

---

**注記:** リストからマッピングを削除するには、マッピングを右クリックして、[削除] を選択します。

---

2. 必要なネットワークドライバすべてをマッピングしたら、[完了] をクリックします。

## OS を正常に復元した後

異なるハードウェアを復旧すると、OS のアクティブ化はリセットされます。OS を正常に復元したら、次の操作を実行する必要があります。

- OS を再アクティブ化します。
- 確認し、必要に応じて、見つからないシステムドライバを再インストールします。

## ユーザーデータとアプリケーションデータの復元

このフェーズは、EADR で実行する処理と同じです (ステップ 11 を参照)。

---

### 注記:

OS のブート後に、サードパーティ製アプリケーションサービスおよびドライバの読み込みが失敗することがあります。これらのアプリケーションは再インストールして再構成する必要があります。これらのアプリケーションが不要な場合は、現在のシステムから削除する必要があります。

---

# 用語集

## A

- ACSL** **(StorageTek 固有の用語)**Automated Cartridge System Library Server の略語。ACS(Automated Cartridge System: 自動カートリッジシステム) を管理するソフトウェア。
- Active Directory** **(Windows 固有の用語)**Windows ネットワークで使用されるディレクトリサービス。ネットワーク上のリソースに関する情報を格納し、ユーザーやアプリケーションからアクセスできるように維持します。このディレクトリサービスでは、サービスが実際に稼動している物理システムの違いに関係なく、リソースに対する名前や説明の付加、検索、アクセス、および管理を一貫した方法で実行できます。
- AES 256 ビット暗号化** 256 ビット長のランダムキーを使用する AES-CTR(Advanced Encryption Standard in Counter Mode) 暗号化アルゴリズムを基にした Data Protector ソフトウェア暗号化。暗号化と復号化の両方で同じキーが使用されます。データはネットワークを介して転送される前およびメディアに書き込まれる前に、AES256 ビット暗号化機能によって暗号化されます。
- AML** **(ADIC/GRAU 固有の用語)**Automated Mixed-Media library(自動混合メディアライブラリ) の略。
- AMU** **(ADIC/GRAU 固有の用語)**Archive Management Unit(アーカイブ管理単位) の略。
- Application Agent** クライアント上でオンラインデータベース統合ソフトウェアを復元およびバックアップするために必要なコンポーネント。  
Disk Agent も参照。
- ASR セット** フロッピーディスク上に保存されたファイルのコレクション。交換用ディスクの適切な再構成 (ディスクパーティション化と論理ボリュームの構成) およびフルクライアントバックアップでバックアップされたオリジナルシステム構成とユーザーデータの自動復旧に必要となります。これらのファイルは、バックアップメディア上に保存されると共に、Cell Manager 上の `Data_Protector_program_data\Config\Server\dr\asr` ディレクトリ (Windows Server 2008 の場合)、`Data_Protector_home\Config\Server\dr\asr` ディレクトリ (その他の Windows システムの場合)、または `/etc/opt/omni/server/dr/asr` ディレクトリ (UNIX システムの場合) に保存されます。障害が発生すると、ASR アーカイブファイルは複数のフロッピーディスクに展開されます。これらのフロッピーディスクは、ASR の実行時に必要となります。

## B

- BACKINT** **(SAP R/3 固有の用語)**SAP R/3 バックアッププログラムが、オープンインタフェースへの呼び出しを通じて Data Protector backint インタフェースソフトウェアを呼び出し、Data Protector ソフトウェアと通信できるようにします。バックアップ時および復元時には、SAP R/3 プログラムが Data Protectorbackint インタフェースを通じてコマンドを発行します。
- BC** **(EMC Symmetrix 固有の用語)**Business Continuance の略。BC は、EMC Symmetrix 標準デバイスのインスタントコピーに対するアクセスおよび管理を可能にするプロセスです。  
BCV も参照。
- BC Process** **(EMC Symmetrix 固有の用語)** 保護されたストレージ環境のソリューション。特別に構成された EMC Symmetrix デバイスを、EMC Symmetrix 標準デバイス上でデータを保護するために、ミラーとして、つまり Business Continuance Volumes として規定します。  
BCV も参照。
- BCV** **(EMC Symmetrix 固有の用語)**Business Continuance Volumes の略。BCV デバイスは ICDA 内であらかじめ構成された専用の SLD です。ビジネスの継続運用を可能にするために使用されます。BCV デバイスには、これらのデバイスによりミラー化される SLD のアドレスとは異なる、個別の SCSI アドレスが割り当てられます。BCV デバイスは、保護を必要とする一次 EMC Symmetrix SLD の分割可能なミラーとして使用されます。  
BC および BC Process も参照。
- BRARCHIVE** **(SAP R/3 固有の用語)**SAP R/3 バックアップツールの 1 つ。アーカイブ REDO ログファイルをバックアップできます。BRARCHIVE では、アーカイブプロセスのすべてのログとプロファイルも保存されます。  
BRBACKUP および BRRESTORE も参照。

<b>BRBACKUP</b>	<b>(SAP R/3 固有の用語)</b> SAP R/3 バックアップツールの 1 つ。制御ファイル、個々のデータファイル、またはすべての表領域をオンラインでもオフラインでもバックアップできます。また、必要に応じて、オンライン REDO ログファイルをバックアップすることもできます。BRARCHIVE および BRRESTORE も参照。
<b>BRRESTORE</b>	<b>(SAP R/3 固有の用語)</b> 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。 <ul style="list-style-type: none"> <li>• 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</li> <li>• BRARCHIVE でアーカイブされた REDO ログファイル</li> <li>• BRBACKUP で保存された非データベースファイル</li> </ul> ファイル、テーブルスペース、バックアップ全体、REDO ログファイルのログシーケンス番号、またはバックアップのセッション ID を指定することができます。BRBACKUP および BRARCHIVE も参照。
<b>BSM</b>	Data Protector バックアップセッションマネージャー (Backup Session Manager) の略。バックアップセッションを制御します。このプロセスは、常に Cell Manager システム上で稼働します。
<b>C</b>	
<b>CAP</b>	<b>(StorageTek 固有の用語)</b> 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。
<b>CDB</b>	Catalog Database(カタログデータベース) の略。CDB は IDB の一部で、バックアップ、復元、オブジェクトコピー、オブジェクト集約、オブジェクト検証、メディア管理の各セッションに関する情報が格納されます。選択したロギングレベルによっては、ファイル名とファイルバージョンも格納されます。CDB は、常にセルに対してローカルとなります。MMDB も参照。
<b>CDF ファイル</b>	<b>(UNIX 固有の用語)</b> Context Dependent File(コンテキスト依存ファイル) の略。CDF ファイルは、同じパス名でグループ化された複数のファイルからなるファイルです。通常、プロセスのコンテキストに基づいて、これらのファイルのいずれかがシステムによって選択されます。このメカニズムにより、クラスター内のすべてホストから同じパス名を使って、マシンに依存する実行可能ファイル、システムデータ、およびデバイスファイルを正しく動作させることができます。
<b>Cell Manager</b>	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。
<b>Certificate Server</b>	Windows Certificate Server をインストールして構成すると、クライアントに証明書を提供することができます。証明書サーバーは、エンタープライズ用の証明書を発行および管理するためのカスタマイズ可能なサービスを提供します。これらのサービスでは、公開キーベースの暗号化技術で使用されている証明書の発行、取り消し、および管理が可能です。
<b>Change Log Provider</b>	<b>(Windows 固有の用語)</b> ファイルシステム上のどのオブジェクトが作成、変更、または削除されたかを判断するために照会できるモジュール。
<b>CMMDB</b>	Data Protector の CMMDB(Centralized Media Management Database: メディア集中管理データベース) は、MoM セル内で、複数セルの MMDB をマージすることにより生成されます。この機能を使用することで、MoM 環境内の複数のセルの間でハイエンドデバイスやメディアを共有することが可能になります。いずれかのセルからロボティクスを使用して、他のセルに接続されているデバイスを制御することもできます。CMMDB は Manager-of-Manager 上に置く必要があります。MoM セルとその他の Data Protector セルの間には、できるだけ信頼性の高いネットワーク接続を用意してください。MoM も参照。
<b>COM+ クラス登録データベース</b>	<b>(Windows 固有の用語)</b> COM+ クラス登録データベースと Windows レジストリには、アプリケーションの属性、クラスの属性、およびコンピュータレベルの属性が格納されます。これにより、これらの属性間の整合性を確保でき、これらの属性を共通の方法で操作できます。
<b>Command View VLS</b>	<b>(VLS 固有の用語)</b> LAN 経由で VLS を構成、管理、モニターするのに使用する Web ブラウザベースの GUI。仮想ライブラリシステム (VLS) も参照。

<b>CRS</b>	Data Protector Cell Manager 上で実行され、バックアップと復元セッションを開始、制御する、Cell Request Server のプロセス (サービス)。このサービスは、Data Protector が Cell Manager 上にインストールされるとすぐに開始されます。Windows システムでは、CRS はインストール時に使用したユーザーアカウントで実行されます。UNIX システムでは、CRS はアカウントルートで実行されます。
<b>CSM</b>	Data Protector コピーおよび集約セッションマネージャー (Copy and Consolidation Session Manager) の略。このプロセスは、オブジェクトコピーセッションとオブジェクト集約セッションを制御し、Cell Manager システム上で動作します。
<b>D</b>	
<b>Data_Protector_home</b>	Data Protector のプログラムファイルを含むディレクトリへの参照 (Windows Vista、Windows 7、および Windows Server 2008 の場合)、または Data Protector のプログラムファイルおよびデータファイルを含むディレクトリへの参照 (他の Windows オペレーティングシステムの場合)。デフォルトのパスは、 <code>%ProgramFiles%\OmniBack</code> ですが、パスはインストール時に Data Protector セットアップウィザードで変更できます。 Data_Protector_program_data も参照。
<b>Data_Protector_program_data</b>	Windows Vista、Windows 7、および Windows Server 2008 上の Data Protector データファイルを含むディレクトリへの参照。デフォルトのパスは、 <code>%ProgramData%\OmniBack</code> ですが、パスはインストール時に Data Protector セットアップウィザードで変更できます。 Data_Protector_home も参照。
<b>Dbobject</b>	<b>(Informix Server 固有の用語)</b> Informix Server 物理データベースオブジェクト。blobpace、dbspace、または論理ログファイルなどがそれにあたります。
<b>DCBF</b>	IDB の詳細カタログバイナリファイル (DCBF) 部には、ファイルのバージョンと属性に関する情報が格納されます。IDB の約 80% を占めるファイルバージョンと属性に関する情報を格納します。バックアップに使用される Data Protector メディアごとに 1 つの DC バイナリファイルが作成されます。サイズの最大値は、ファイルシステムの設定による制限を受けます。
<b>DC ディレクトリ</b>	詳細カタログ (DC) ディレクトリには、詳細カタログバイナリファイル (DCBF) が含まれており、そのファイルの中にはファイルバージョンについての情報が保管されています。これは、IDB の DCBF 部分を表し、IDB 全体の約 80% の容量を占めます。デフォルトの DC ディレクトリは <code>dcbf</code> と呼ばれ、 <code>Data_Protector_program_data\db40</code> ディレクトリ (Windows Server 2008 の場合)、 <code>Data_Protector_home\db40</code> ディレクトリ (その他の Windows システムの場合)、または <code>/var/opt/omni/server/db40</code> ディレクトリ (UNIX システムの場合) の Cell Manager に置かれます。他の DC ディレクトリを作成し、独自に指定した場所を使用することができます。1 つのセルでサポートされる DC ディレクトリは 50 個までです。DC ディレクトリのデフォルト最大サイズは 16GB です。
<b>DHCP サーバー</b>	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。
<b>Disk Agent</b>	クライアントのバックアップと復元を実行するためにクライアントシステム上にインストールする必要があるコンポーネントの 1 つ。Disk Agent は、ディスクに対するデータの読み書きを制御します。バックアップセッション中には、Disk Agent がディスクからデータを読み取って、Media Agent に送信してデータをデバイスに移動させます。復元セッション中には、Disk Agent が Media Agent からデータを受信して、ディスクに書き込みます。オブジェクト検証セッション中に、Disk Agent は Media Agent からデータを取得し、確認処理を実行しますが、データはディスクには書き込まれません。
<b>Disk Agent の同時処理数</b>	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。
<b>DMZ</b>	DMZ (Demilitarized Zone) は、企業のプライベートネットワーク (イントラネット) と外部のパブリックネットワーク (インターネット) の間に「中立地帯」として挿入されたネットワークです。DMZ により、外部のユーザーが企業のイントラネット内のサーバーに直接アクセスすることを防ぐことができます。
<b>DNS サーバー</b>	DNS クライアント/サーバーモデルでは、DNS サーバーにインターネット全体で名前解決を行うのに必要な DNS データベースに含まれている情報の一部を保持します。DNS サーバーは、このデータベースを使用して名前解決を要求するクライアントに対してコンピュータ名を提供します。

<b>DR OS</b>	ディザスタリカバリを実行するオペレーティングシステム環境。Data Protector に対して基本的な実行時環境 (ディスク、ネットワーク、テープ、およびファイルシステムへのアクセス) を提供します。Data Protector ディザスタリカバリを実行する前に、DR OS をディスクにインストールするかメモリにロードして、構成しておく必要があります。DR OS には、一時 DR OS とアクティブ DR OS があります。一時 DR OS は、他のオペレーティングシステムの復元用ホスト環境として排他的に使用されます。このホスト環境には、ターゲットとなるオペレーティングシステムの構成データも置かれます。ターゲットシステムを元のシステム構成に復元し終えた後、一時 DR OS は削除されます。アクティブ DR OS は、Data Protector ディザスタリカバリプロセスのホストとして機能するだけでなく、復元後のシステムの一部にもなります。その場合、DR OS の構成データは元の構成データに置き換わります。
<b>DR イメージ</b>	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。
<b>E</b>	
<b>EMC Symmetrix Agent</b>	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。
<b>Event Log(Data Protector: イベントログ)</b>	イベントログには、Data Protector 関連のすべての通知が書き込まれます。デフォルトの送信方法では、すべての通知がイベントログに送信されます。イベントは Cell Manager で記録され、 <i>Data_Protector_program_data\log\server\Ob2EventLog.txt</i> (Windows Server 2008 の場合)、 <i>Data_Protector_home\log\server\Ob2EventLog.txt</i> (その他の Windows システムの場合)、 <i>/var/opt/omni/server/log/Ob2EventLog.txt</i> (UNIX システムの場合) に書き込まれます。このイベントログにアクセスできるのは、Data Protector の Admin ユーザーグループに所属しているユーザーか、Data Protector の「レポートと通知」ユーザー権限が付与されているユーザーのみです。イベントログに書き込まれているイベントは、いずれも表示と削除が可能です。
<b>Exchange Replication Service</b>	<b>(Microsoft Exchange Server 固有の用語)</b> ローカル連続レプリケーション (LCR) か、クラスター連続レプリケーション (CCR) テクノロジーのいずれかを使用して複製されたストレージグループを表す Microsoft Exchange Server のサービス。 クラスター連続レプリケーションおよびローカル連続レプリケーション も参照。
<b>F</b>	
<b>FCブリッジ fnames.dat</b>	ファイバーチャネルブリッジ を参照。 IDB の <i>fnames.dat</i> 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。
<b>G</b>	
<b>GUI</b>	Data Protector には、構成、管理、および操作に関するあらゆるタスクに簡単にアクセスできる、グラフィカルユーザーインターフェースが用意されています。Windows 用のオリジナルの Data Protector GUI の他に、Data Protector には、さまざまなプラットフォームで実行できる、外観も操作も変わらない Java ベースの GUI も用意されています。
<b>H</b>	
<b>Holidays ファイル</b>	休日に関する情報を格納するファイル。このファイルは、 <i>Data_Protector_program_data\Config\Server\holidays</i> ディレクトリ (Windows Server 2008 の場合)、 <i>Data_Protector_home\Config\Server\holidays</i> ディレクトリ (その他の Windows システムの場合)、または <i>/etc/opt/omni/server/Holidays</i> ディレクトリ (UNIX システムの場合) の Cell Manager の Holidays ファイルを編集することで、各種の休日を設定できます。
<b>HP Business Copy (BC) P6000 EVA</b>	<b>(HP P6000 EVA ディスクレイファミリー固有の用語)</b> ローカル複製ソフトウェアソリューションの 1 つで、P6000 EVA ファームウェアのスナップショット機能およびクローン機能を使用して、ソースボリュームの特定時点のコピー (複製) を作成できます。複製、ソースボリューム、スナップショット、および HP Continuous Access + Business Copy (CA+BC) P6000 EVA も参照。

<b>HP Business Copy (BC) P9000 XP</b>	<p><b>(HP P9000 XP ディスクアレイファミリ固有の用語)</b> HP P9000 XP ディスクアレイファミリ構成の 1 つで、データ複製やバックアップなどのさまざまな目的のために LDEV の内部コピーの作成および保守を可能にします。これらのコピー (セカンダリボリューム:S-VOL) は、プライマリボリューム (P-VOL) から分離して、別のシステムに接続することができます。Data Protector ゼロダウンタイムバックアップを目的とする場合、アプリケーションシステムで P-VOL を使用可能にし、S-VOL セットのいずれかをバックアップシステムで使用可能にする必要があります。</p> <p>LDEV、HP Continuous Access (CA) P9000 XP、メインコントロールユニット、アプリケーションシステム、およびバックアップシステム も参照。</p>
<b>HP Command View (CV) EVA</b>	<p><b>(HP P6000 EVA ディスクアレイファミリ固有の用語)</b> P6000 EVA ストレージシステムを構成、管理、モニターするためのユーザーインターフェース。さまざまなストレージ管理作業を行うために使用されます。たとえば、仮想ディスクファミリの作成、ストレージシステムハードウェアの管理、仮想ディスクのスナップショットやスナップクローン、ミラークローンの作成などに使用されます。HP Command View EVA ソフトウェアは HP ストレージマネジメントアプライアンス上で動作し、Web ブラウザからアクセスできます。</p> <p>HP P6000 EVA SMI-S Agent および HP SMI-S P6000 EVA アレイプロバイダ も参照。</p>
<b>HP Continuous Access + Business Copy (CA+BC) P6000 EVA</b>	<p><b>(HP P6000 EVA ディスクアレイファミリ固有の用語)</b> HP P6000 EVA ディスクアレイファミリ構成の 1 つで、リモート P6000 EVA 上にソースボリュームのコピー (複製) を作成および保守し、このリモートアレイでローカル複製を行うときにソースとしてこのコピーを使用できます。</p> <p>HP Business Copy (BC) P6000 EVA、複製、およびソースボリューム も参照。</p>
<b>HP Continuous Access (CA) P9000 XP</b>	<p><b>(HP P9000 XP ディスクアレイファミリ固有の用語)</b> HP P9000 XP ディスクアレイファミリ構成の 1 つで、データ複製やバックアップ、ディザスタリカバリなどのために LDEV のリモートコピーの作成および保守を可能にします。HP CA P9000 XP を使用するには、メイン (プライマリ) ディスクアレイユニットとリモート (セカンダリ) ディスクアレイユニットが必要です。メインディスクアレイユニットはアプリケーションシステムに接続され、オリジナルのデータを格納しているプライマリボリューム (P-VOL) を格納します。リモートディスクアレイはバックアップシステムに接続され、セカンダリボリューム (S-VOL) を格納します。</p> <p>HP Business Copy (BC) P9000 XP、メインコントロールユニット、および LDEV も参照。</p>
<b>HP Operations Manager</b>	<p>ネットワーク内の多数のシステムとアプリケーションの運用管理を強力な機能でサポートする HP Operations Manager。Data Protector には、この管理製品を使用するための統合ソフトウェアが用意されています。この統合ソフトウェアは、Windows、HP-UX、Solaris および Linux 上の HP Operations Manager 管理サーバー用の SMART Plug-In として実装されています。以前のバージョンの HP Operations Manager は、IT/Operations、Operations Center、Vantage Point Operations、および OpenView Operations と呼ばれていました。</p>
<b>HP Operations Manager SMART Plug-In(SPI)</b>	<p>ドメイン監視機能を強化する完全に統合されたソリューションで、HP Operations Manager に追加するだけですぐに使えます。HP Operations Manager SMART Plug-In として実装される Data Protector 用統合ソフトウェアを使用して、ユーザーは HP Operations Manager の拡張機能として任意の数の Data Protector Cell Manager を監視できます。</p>
<b>HP P6000 EVA SMI-S Agent</b>	<p>HP P6000 EVA ディスクアレイファミリ統合に必要なすべてのタスクを実行する Data Protector のソフトウェアモジュール。P6000 EVA SMI-S Agent を使用すると、受信した要求と HP CV EVA 間のやり取りを制御する HP SMI-S P6000 EVA アレイプロバイダを通じてアレイを制御できます。</p> <p>HP Command View (CV) EVA および HP SMI-S P6000 EVA アレイプロバイダ も参照。</p>
<b>HP P9000 XP Agent</b>	<p>Data Protector HP P9000 XP ディスクアレイファミリ統合に必要なすべてのタスクを実行する Data Protector コンポーネント。P9000 XP アレイストレージシステムとの通信に RAID Manager ライブラリを使用します。</p> <p>RAID Manager ライブラリ も参照。</p>
<b>HP SMI-S P6000 EVA アレイプロバイダ</b>	<p>HP P6000 EVA ディスクアレイファミリを制御するために使用するインターフェース。SMI-S P6000 EVA アレイプロバイダは HP ストレージマネジメントアプライアンスシステム上で個別のサービスとして動作し、受信した要求と HP Command View EVA 間のゲートウェイとして機能します。Data Protector HP P6000 EVA ディスクアレイファミリ統合を使用すると、SMI-S P6000 EVA アレイプロバイダは P6000 EVA SMI-S Agent からの標準化された要求を受け入れ、HP Command View EVA と通信して情報の取得またはメソッドの起動を行って、標準化された応答を返します。</p> <p>HP P6000 EVA SMI-S Agent および HP Command View (CV) EVA も参照。</p>

ICDA	<b>(EMC Symmetrix 固有の用語)</b> EMC の Symmetrix の統合キャッシュディスクアレイ (ICDA) は、複数の物理ディスク、複数の FWD SCSI チャンネル、内部キャッシュメモリ、およびマイクロコードと呼ばれる制御/診断ソフトウェアを備えたディスクアレイデバイスです。
IDB	Data Protector の内部データベース。IDB は、Cell Manager 上に維持される埋込み型データベースです。どのデータがどのメディアにバックアップされたか、バックアップ、復元などのセッションがどのように実行されたか、どのデバイス、ライブラリ、ディスクアレイが構成されているかなどに関する情報が格納されます。
IDB 復旧ファイル	IDB バックアップ、メディア、バックアップ用デバイスに関する情報を含む IDB ファイル (obrindex.dat)。この情報により、IDB の復旧を大幅に簡素化できます。IDB トランザクションログと共にこのファイルを他の IDB ディレクトリとは別の物理ディスクに移動し、さらにこのファイルのコピーを作成することをお勧めします。
Inet	Data Protector セル内の各 UNIX システムまたは Windows システム上で動作するプロセス。このプロセスは、セル内のシステム間の通信と、バックアップおよび復元に必要なその他のプロセスの起動を受け持ちます。システムに Data Protector をインストールすると、Inet サービスが即座に起動されます。Inet プロセスは、inetd デモンにより開始されます。
Informix Server	<b>(Informix Server 固有の用語)</b> Informix Dynamic Server のことです。
Informix Server 用の CMD スクリプト	<b>(Informix Server 固有の用語)</b> Informix Server データベースの構成時に INFORMIXDIR 内に作成される Windows CMD スクリプト。環境変数を Informix Server にエクスポートするコマンド一式が含まれています。
ISQL	<b>(Sybase 固有の用語)</b> 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。

Java GUI クライアント	Java GUI クライアントは Java GUI コンポーネントの 1 つで、ユーザーインターフェース関連の機能 (Cell Manager グラフィカルユーザーインターフェースおよび Manager-of-Managers(MoM) のグラフィカルユーザーインターフェース) のみで構成されており、機能するためには Java GUI サーバーと接続する必要があります。
Java GUI サーバー	Java GUI コンポーネントの 1 つ。Data Protector Cell Manager システムにインストールされています。Java GUI サーバーは、Java GUI クライアントからの要求を受け取って処理し、応答を Java GUI クライアントに戻します。通信には、HTTP (Hypertext Transfer Protocol) とポート 5556 を使用します。

keychain	パスフレーズを手動で入力しなくても秘密キーを復号化できるようにするツールです。セキュアシェルを使用してリモートインストールを実行する場合、このツールをインストールサーバーにインストールして構成する必要があります。
KMS	キー管理サーバー (KMS) は Data Protector の暗号化機能のためのキー管理を提供する、Cell Manager で実行する集中サービス。このサービスは、Data Protector が Cell Manager 上にインストールされるとすぐに開始されます。

LBO	<b>(EMC Symmetrix 固有の用語)</b> Logical Backup Object(論理バックアップオブジェクト) の略。LBO は、EMC Symmetrix/Fastrax 環境内で保存/取得されるデータオブジェクトです。LBO は EMC Symmetrix によって 1 つのエンティティとして保存/取得され、部分的には復元できません。
LDEV	<b>(HP P9000 XP ディスクアレイファミリ固有の用語)</b> HP P9000 XP ディスクアレイファミリのディスクアレイの物理ディスクの論理パーティション。LDEV は、このようなディスクアレイのスプリットミラー機能やスナップショット機能を使用して複製可能なエンティティです。HP Business Copy (BC) P9000 XP、HP Continuous Access (CA) P9000 XP、および複製も参照。
LISTENER.ORA	<b>(Oracle 固有の用語)</b> Oracle の構成ファイルの 1 つ。サーバー上の 1 つまたは複数の TNS リスナを定義します。

<b>log_full シェルスクリプト</b>	<b>(Informix Server UNIX 固有の用語)</b> 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、 <i>INFORMIXDIR/etc/log_full.sh</i> に設定されます。ここで、 <i>INFORMIXDIR</i> 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 <i>INFORMIXDIR/etc/no_log.sh</i> に設定してください。
<b>Lotus C API</b>	<b>(Lotus Domino Server 固有の用語)</b> 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。
<b>LVM</b>	LVM (Logical Volume Manager: 論理ボリュームマネージャー) は、HP-UX システム上で物理ディスクスペースを構造化し、論理ボリュームにマッピングするためのサブシステムです。LVM システムは、複数のボリュームグループで構成されます。各ボリュームグループには、複数のボリュームが含まれます。
<b>M</b>	
<b>make_net_recovery</b>	<i>make_net_recovery</i> は、Ignite-UX のコマンドの 1 つ。Ignite-UX サーバーまたはその他の指定システム上にネットワーク経由で復旧アーカイブを作成できます。ターゲットシステムは、Ignite-UX の <i>make_boot_tape</i> 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 <i>bootsys</i> 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。
<b>make_tape_recovery</b>	<i>make_tape_recovery</i> は、Ignite-UX のコマンドの 1 つ。システムに応じてカスタマイズしたブート可能テープ(インストールテープ)を作成できます。ターゲットシステムにバックアップデバイスを直接接続し、ブート可能な復旧テープからターゲットシステムをブートすることにより、無人ディザスタリカバリを実行できます。アーカイブ作成時とクライアント復旧時は、バックアップデバイスをクライアントにローカル接続しておく必要があります。
<b>Manager-of-Managers (MoM)</b>	
	MoM を参照。
<b>MAPI</b>	<b>(Microsoft Exchange Server 固有の用語)</b> 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。
<b>MCU</b>	メインコントロールユニット (MCU) を参照。
<b>Media Agent</b>	デバイスに対する読み込み/書き込みを制御するプロセス。制御対象のデバイスはテープなどのメディアに対して読み込み/書き込みを行います。復元またはオブジェクト検証セッション中、Media Agent はバックアップメディア上のデータを探して、処理するために Disk Agent に送信します。復元セッションの場合、続いて Disk Agent はデータをディスクに書き込みます。Media Agent は、ライブラリのロボティクス制御も管理します。
<b>Microsoft Exchange Server</b>	多様な通信システムへの透過的接続を提供するクライアント/サーバー型のメッセージング/ワークグループシステム。電子メールシステムその他、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。
<b>Microsoft SQL Server</b>	分散型"クライアント/サーバー"コンピューティングのニーズを満たすように設計されたデータベース管理システム。
<b>Microsoft 管理コンソール (MMC)</b>	<b>(Windows 固有の用語)</b> 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。
<b>Microsoft ボリュームシャドウコピーサービス (VSS)</b>	VSS 対応アプリケーションのバックアップと復元をそのアプリケーションの機能に関係なく統合管理する統一通信インタフェースを提供するソフトウェアサービスです。このサービスは、バックアップアプリケーション、ライター、シャドウコピープロバイダ、およびオペレーティングシステムカーネルと連携して、ボリュームシャドウコピーおよびシャドウコピーセットの管理を実現します。 シャドウコピー、シャドウコピープロバイダ、複製およびライター も参照。

<b>MMD</b>	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。
<b>MMDB</b>	Media Management Database(メディア管理データベース) の略。MMDB は、IDB の一部です。セル内で構成されているメディア、メディアプール、デバイス、ライブラリ、ライブラリデバイス、スロットに関する情報と、バックアップに使用されている Data Protector メディアに関する情報を格納します。エンタープライズバックアップ環境では、データベースをすべてのセル間で共有できます。 CMMDB および CDB も参照。
<b>MoM</b>	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。
<b>MSM</b>	Data Protector メディアセッションマネージャー (Media Session Manager) の略。MSM は、Cell Manager 上で稼動し、メディアセッション (メディアのコピーなど) を制御します。
○	
<b>obdrindex.dat</b>	IDB 復旧ファイル を参照。
<b>OBDR 対応デバイス</b>	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。
<b>ON-Bar</b>	<b>(Informix Server 固有の用語)</b> 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。 <ul style="list-style-type: none"> <li>• onbar コマンド</li> <li>• バックアップソリューションとしての Data Protector</li> <li>• XBSA インタフェース</li> <li>• 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。</li> </ul>
<b>ONCONFIG</b>	<b>(Informix Server 固有の用語)</b> 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 <i>INFORMIXDIR\etc</i> (Windows の場合)、または <i>INFORMIXDIR/etc/</i> (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。
<b>Oracle Data Guard</b>	<b>(Oracle 固有の用語)</b> 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。
<b>ORACLE_SID</b>	<b>(Oracle 固有の用語)</b> Oracle Server インスタンスの一意的な名前。別の Oracle Server に切り替えるには、目的の <i>ORACLE_SID</i> を指定します。 <i>ORACLE_SID</i> は、 <i>TNSNAMES.ORA</i> ファイル内の接続記述子の <i>CONNECT DATA</i> 部分と <i>LISTENER.ORA</i> ファイル内の <i>TNS</i> リスナの定義に含まれています。
<b>Oracle インスタンス</b>	<b>(Oracle 固有の用語)</b> 1 つまたは複数のシステムにインストールされた個々の Oracle データベース。1 つのコンピュータシステム上で、複数のデータベースインスタンスを同時に稼動させることができます。

## Oracle ターゲットデータベースへのログイン情報

(Oracle および SAP R/3 固有の用語) ログイン情報の形式は、`user_name/password@service` です。

- この場合、`user_name` は、Oracle Server およびその他のユーザーに対して公開されるユーザー名です。各ユーザー名はパスワードと関連付けられており、Oracle ターゲットデータベースに接続するにはユーザー名とパスワードの両方を入力する必要があります。ここでは、Oracle の SYSDBA 権限または SYSOPER 権限が付与されているユーザーを指定する必要があります。
- `password` には、Oracle パスワードファイル (`orapwd`) 内に指定したのと同じパスワードを指定しなければなりません。パスワードは、データベースを管理するユーザーの認証に使用されます。
- `service` には、ターゲットデータベースのための SQL\*Net サーバプロセスの識別に使用される名前を指定します。

## P

### P1S ファイル

P1S ファイルには、システムにインストールされているすべてのディスクを拡張自動ディザスタリカバリ (EADR) 中にどのようにフォーマットするかに関する情報が格納されます。このファイルはフルバックアップ中に作成され、バックアップメディアと Cell Manager に保存されます。保存場所は、`Data_Protector_program_data\Config\Server\dr\p1s` ディレクトリ (Windows Server 2008 の場合)、`Data_Protector_home\Config\Server\dr\p1s` ディレクトリ (その他の Windows システムの場合)、`/etc/opt/omni/server/dr/p1s` ディレクトリ (UNIX システムの場合) です。ファイル名は以下のとおりです。recovery.p1s。

## R

### RAID

Redundant Array of Independent Disks の略。

### RAID Manager P9000 XP

(HP P9000 XP ディスクアレイファミリ固有の用語) HP P9000 XP ディスクアレイファミリのディスクアレイに対するコマンドラインインタフェースを提供するソフトウェアアプリケーション。P9000 XP アレイストレージシステムのステータスのレポートと制御を行い、ディスクアレイに対する各種操作を実行するための広範なコマンドセットが用意されています。

### RAID Manager ライブラリ

(HP P9000 XP ディスクアレイファミリ固有の用語) P9000 XP アレイストレージシステムの構成、ステータス、およびパフォーマンス測定へのデータへのアクセスと、ディスクアレイの操作の開始に使用されるソフトウェアライブラリ。このライブラリにより、関数呼び出しが関連の低レベルの SCSI コマンドに変換されます。HP P9000 XP Agent も参照。

### raw ディスクバックアップ

ディスクイメージバックアップを参照。

### RCU

Remote Control Unit(RCU) を参照。

### RCU Remote Control Unit (RCU)

(HP P9000 XP ディスクアレイファミリ固有の用語) HP CA P9000 XP または HP CA+BC P9000 XP 構成におけるメインコントロールユニット (MCU) に対するスレーブデバイスとして機能する HP P9000 XP ディスクアレイファミリユニット。双方向の構成の中では、RCU は MCU としての役割も果たします。

### RDBMS

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

### RDF1/RDF2

(EMC Symmetrix 固有の用語) SRDF デバイスグループの一種。RDF グループには RDF デバイスだけを割り当てることができます。RDF1 グループタイプにはソースデバイス (R1) が格納され、RDF2 グループタイプにはターゲットデバイス (R2) が格納されます。

### RDS

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

### Recovery Manager (RMAN)

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

<b>RecoveryInfo</b>	Windows 構成ファイルのバックアップ時、Data Protector は、現在のシステム構成に関する情報 (ディスクレイアウト、ボリューム、およびネットワークの構成に関する情報) を収集します。この情報は、ディザスタリカバリ時に必要になります。
<b>REDO ログ</b>	<b>(Oracle 固有の用語)</b> 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。
<b>RMAN(Oracle 固有の用語)</b>	Recovery Manager を参照。
<b>RSM</b>	Data Protector 復元セッションマネージャー (Restore Session Manager) の略。復元セッションおよびオブジェクト検証セッションを制御します。このプロセスは、常に Cell Manager システム上で稼働します。
<b>RSM</b>	<b>(Windows 固有の用語)</b> 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。
<b>S</b>	
<b>SAPDBA</b>	<b>(SAP R/3 固有の用語)</b> BRBACKUP ツール、BRARCHIVE ツール、BRRESTORE ツールを統合した SAP R/3 ユーザーインターフェース。
<b>SIBF</b>	サーバーレス統合バイナリファイル (SIBF) は、IDB のうち、NDMP の raw メタデータが格納される部分です。これらのデータは、NDMP オブジェクトの復元に必要です。
<b>SMB</b>	スプリットミラーバックアップ を参照。
<b>SMBF</b>	セッションメッセージバイナリファイル (SMBF) は、IDB のうち、バックアップ、復元、オブジェクトコピー、オブジェクト集約、オブジェクト検証、およびメディア管理のセッション中に生成されたセッションメッセージが格納される部分です。1 つのセッションにつき 1 つのバイナリファイルが作成されます。ファイルは年毎や月毎に分類されます。
<b>SMI-S Agent(SMISA)</b>	HP P6000 EVA SMI-S Agent を参照。
<b>sqlhosts ファイルまたはレジストリ</b>	<b>(Informix Server 固有の用語)</b> Informix Server の接続情報ファイル (UNIX) またはレジストリ (Windows)。各データベースサーバーの名前の他、ホストコンピュータ上のクライアントが接続できるエイリアスが格納されます。
<b>SRDF</b>	<b>(EMC Symmetrix 固有の用語)</b> EMC Symmetrix Remote Data Facility の略。SRDF は、異なる位置にある複数の処理環境の間での効率的なリアルタイムデータ複製を実現する Business Continuation プロセスです。同じルートコンピュータ環境内だけでなく、互いに遠距離にある環境も対象となります。
<b>SRD ファイル</b>	<b>(ディザスタリカバリ固有の用語)</b> Unicode (UTF-16) 形式のテキストファイルで、Windows システムの CONFIGURATION バックアップ中に生成され Cell Manager に格納されます。このファイルには、障害発生時にターゲットシステムにオペレーティングシステムをインストールおよび構成するために必要なシステム情報が含まれています。ターゲットシステム も参照。
<b>SSE Agent(SSEA)</b>	HP P9000 XP Agent を参照。
<b>sst.conf ファイル</b>	/usr/kernel/drv/sst.conf ファイルは、マルチドライブライブラリデバイスが接続されている Data Protector Solaris クライアントのそれぞれにインストールされていなければならないファイルです。このファイルには、クライアントに接続されている各ライブラリデバイスのロボット機構の SCSI アドレスエントリが記述されていなければなりません。
<b>st.conf ファイル</b>	/kernel/drv/st.conf ファイルは、バックアップデバイスが接続されている Data Protector Solaris クライアントのそれぞれにインストールされていなければならないファイルです。このファイルには、クライアントに接続されている各バックアップドライブのデバイス情報と SCSI アドレスが記述されていなければなりません。シングルドライブデバイスについては単一の SCSI エントリが、マルチドライブライブラリデバイスについては複数の SCSI エントリが、それぞれ必要です。

<b>StorageTek ACS ライブラリ</b>	<b>(StorageTek 固有の用語)</b> 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。
<b>Sybase Backup Server API</b>	<b>(Sybase 固有の用語)</b> 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。
<b>Sybase SQL Server</b>	<b>(Sybase 固有の用語)</b> Sybase の「クライアントサーバー」アーキテクチャ内のサーバー。Sybase SQL Server は、複数のデータベースと複数のユーザーを管理し、ディスク上のデータの実位置を追跡します。さらに、物理データストレージ域に対する論理データ記述のマッピングを維持し、メモリ内のデータキャッシュとプロシージャキャッシュを維持します。
<b>SYMA</b>	EMC Symmetrix Agent を参照。
<b>System Backup to Tape</b>	<b>(Oracle 固有の用語)</b> 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。
<b>SysVol</b>	<b>(Windows 固有の用語)</b> ドメインのパブリックファイルのサーバー コピーを保存する共有ディレクトリで、ドメイン内のすべてのドメインコントローラ間で複製されます。
<b>T</b>	
<b>TimeFinder</b>	<b>(EMC Symmetrix 固有の用語)</b> 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。
<b>TLU</b>	Tape Library Unit (テープライブラリユニット) の略。
<b>TNSNAMES.ORA</b>	<b>(Oracle および SAP R/3 固有の用語)</b> サービス名にマッピングされた接続記述子を格納するネットワーク構成ファイル。このファイルは、1 か所で集中的に管理してすべてのクライアントで使用することも、また、ローカルに管理して各クライアントで個別に使用することもできます。
<b>TSANDBS.CFG ファイル</b>	<b>(Novell NetWare 固有の用語)</b> 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、TSANDBS.NLM がロードされるサーバーの SYS:SYSTEM\TSA ディレクトリにあります。
<b>U</b>	
<b>UIProxy</b>	Java GUI サーバー (UIProxy サービス) は Data Protector Cell Manager で実行されます。Java GUI サーバーでは、Java GUI クライアントと Cell Manager との間の通信を行います。また、ビジネスロジック操作を実行し、重要な情報のみをクライアントに送信する必要があります。このサービスは、Data Protector が Cell Manager 上にインストールされるとすぐに開始されます。
<b>user_restrictions ファイル</b>	割り当てられているユーザー権限に応じて Data Protector のユーザーグループが使用できる特定のユーザーアクションを、Data Protector セルの特定のシステムでのみ実行されるように制限するファイル。このような制限は、 <b>Admin</b> および <b>Operator</b> 以外の Data Protector のユーザーグループにのみ適用されます。
<b>V</b>	
<b>VMware 管理クライアント</b>	<b>(VMware(レガシー) 用統合ソフトウェア固有の用語)</b> Data Protector で、VMware 仮想インフラストラクチャとの通信に使用されるクライアント。VirtualCenter Server システム (VirtualCenter 環境)、または ESX Server システム (スタンドアロン ESX Server 環境) のどちらかです。
<b>VOLSER</b>	<b>(ADIC および STK 固有の用語)</b> 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。
<b>VSS</b>	Microsoft ボリュームシャドウコピーサービス (VSS) を参照。
<b>VSS 準拠モード</b>	<b>(HP P9000 XP ディスクアレイファミリ VSS プロバイダ固有の用語)</b> 2 種類ある P9000 XP アレイ VSS ハードウェアプロバイダの操作モードの 1 つ。P9000 XP アレイプロバイダが VSS 準拠モードであると、ソースボリューム (P-VOL) とその複製 (S-VOL) は、バックアップ後、単純非対状態になります。したがって、ローテーションされる複製数 (P-VOL 当たりの S-VOL

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

再同期モード、ソースボリューム、プライマリボリューム (P-VOL)、複製、セカンダリボリューム (S-VOL)、および複製セットローテーション も参照。

## VxFS

Veritas Journal Filesystem の略。

## VxVM (Veritas Volume Manager)

Veritas Volume Manager は、Solaris プラットフォーム上でディスクスペースを管理するためのシステムです。VxVM システムは、論理ディスクグループに編成された 1 つまたは複数の物理ボリュームの任意のグループからなります。

## W

### Wake ONLAN

節電モードで動作しているシステムを同じ LAN 上の他のシステムからのリモート操作により電源投入するためのサポート。

### Web レポート

Data Protector の機能の 1 つ。バックアップステータス、オブジェクトコピーステータスおよびオブジェクト集約ステータスと Data Protector 構成に関するレポートを Web インタフェース経由で表示できます。

### Windows 構成のバックアップ

Data Protector では、Windows CONFIGURATION(構成データ) をバックアップできます。Windows レジストリ、ユーザープロファイル、イベントログ、WINS サーバーデータおよび DHCP サーバーデータ (システム上で構成されている場合) を 1 回の操作でバックアップできます。

### Windows レジストリ

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

### WINS サーバー

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

## X

### XBSA インタフェース

**(Informix Server 固有の用語)**ON-Bar と Data Protector の間の相互通信には、X/Open Backup Services Application Programmer's Interface (XBSA) が使用されます。

## Z

### ZDB

ゼロダウンタイムバックアップ (ZDB) を参照。

### ZDB データベース

**(ZDB 固有の用語)** ソースボリューム、複製、セキュリティ情報などの ZDB 関連情報を格納する IDB の一部。ZDB データベースは、ゼロダウンタイムバックアップ、インスタントリカバリ、スプリットミラー復元の各セッションで使用されます。ゼロダウンタイムバックアップ (ZDB) も参照。

## あ

### アーカイブ REDO ログ

**(Oracle 固有の用語)** オフライン REDO ログとも呼びます。Oracle データベースが ARCHIVELOG モードで動作している場合、各オンライン REDO ログが最大サイズまで書き込まれると、アーカイブ先にコピーされます。このコピーをアーカイブ REDO ログと呼びます。各データベースに対してアーカイブ REDO ログを作成するかどうかを指定するには、以下の 2 つのモードのいずれかを指定します。

- ARCHIVELOG – 満杯になったオンライン REDO ログファイルは、再利用される前にアーカイブされます。そのため、インスタンスやディスクにエラーが発生した場合に、データベースを復旧することができます。「ホット」バックアップを実行できるのは、データベースがこのモードで稼働しているときだけです。
- NOARCHIVELOG – オンライン REDO ログファイルは、いっぱいになってもアーカイブされません。

オンライン REDO ログ も参照。

### アーカイブログイン

**(Lotus Domino Server 固有の用語)** Lotus Domino Server のデータベースモードの 1 つ。トランザクションログファイルがバックアップされて初めて上書きされるモードです。

### アクセス権限

ユーザー権限 を参照。

<b>アプリケーションシステム</b>	<b>(ZDB 固有の用語)</b> このシステム上でアプリケーションやデータベースが実行されます。アプリケーションまたはデータベースデータは、ソースボリューム上に格納されています。バックアップシステムおよびソースボリューム も参照。
<b>暗号化 KeyID-StoreID</b>	Data Protector Key Management Server が、Data Protector で使用される暗号化キーの識別と管理に使用する複合識別子です。KeyID は、キーストア内のキーを識別します。StoreID は、Cell Manager 上のキーストアを識別します。Data Protector を暗号化機能付きの旧バージョンからアップグレードした場合、同じ Cell Manager 上で使用される StoreID が複数存在する可能性があります。
<b>暗号化キー</b>	256 ビットのランダムに生成された数値で、AES 256 ビットソフトウェア暗号化またはドライブベースの暗号化が指定されたバックアップの際に、Data Protector の暗号化アルゴリズムが情報を暗号化するために使用します。これに続く情報の復号化では、同じキーが使用されます。Data Protector セルの暗号化キーは、Cell Manager 上の中央キーストアに保存されません。
<b>暗号制御通信</b>	Data Protector セル内のクライアント間における Data Protector のセキュアな通信は、Secure Socket Layer (SSL) をベースにしており、SSLv3 アルゴリズムを使用して制御通信が暗号化されます。Data Protector セル内の制御通信は、Disk Agent(および統合用ソフトウェア) から Media Agent へのデータ転送とその逆方向のデータ転送を除く、Data Protector プロセス間のすべての通信です。

## い

<b>イベントログ</b>	<b>(Windows 固有の用語)</b> サービスの開始または停止、ユーザーのログオンとログオフなど、Windows がすべてのイベントを記録したファイル。Data Protector は、Windows イベントログを Windows 構成バックアップの一部としてバックアップできます。
<b>インスタントリカバリ</b>	<b>(ZDB 固有の用語)</b> ディスクへの ZDB セッションまたはディスク + テープへの ZDB セッションで作成された複製を使用して、ソースボリュームの内容を複製が作成された時点の状態に復元するプロセスです。これにより、テープからの復元を行う必要がなくなります。関連するアプリケーションやデータベースによってはインスタントリカバリだけで十分な場合もあれば、完全に復旧するためにトランザクションログファイルを適用するなどその他にも手順が必要な場合もあります。複製、ゼロダウンタイムバックアップ (ZDB)、ディスクへの ZDB、およびディスク + テープへの ZDB も参照。
<b>インストールサーバー</b>	特定のアーキテクチャ用の Data Protector インストールパッケージのレポジトリを保持するコンピュータシステム。インストールサーバーから Data Protector クライアントのリモートインストールが行われます。混在環境では、少なくとも 2 台のインストールサーバーが必要です。1 台は UNIX システム用で、1 台は Windows システム用です。

## インターネットインフォメーションサービス (IIS)

**(Windows 固有の用語)** Microsoft Internet Information Services は、ネットワーク用ファイル/アプリケーションサーバーで、複数のプロトコルをサポートしています。IIS では、主に、HTTP (Hypertext Transport Protocol) により HTML (Hypertext Markup Language) ページとして情報が転送されます。

<b>インフォメーションストア</b>	<b>(Microsoft Exchange Server 固有の用語)</b> ストレージ管理を行う Microsoft Exchange Server のサービス。Microsoft Exchange Server のインフォメーションストアは、メールボックスストアとパブリックフォルダストアという 2 種類のストアを管理します。メールボックスストアは、個々のユーザーに属するメールボックスから成ります。パブリックフォルダストアには、複数のユーザーで共有するパブリックフォルダおよびメッセージがあります。キーマネージメントサービスおよびサイト複製サービス も参照。
---------------------	--

## う

<b>上書き</b>	復元中のファイル名競合を解決するモードの 1 つ。既存のファイルの方が新しくても、すべてのファイルがバックアップから復元されます。マージ も参照。
------------	---

## え

<b>エクステンジャ</b>	SCSI エクステンジャとも呼ばれます。
----------------	----------------------

ライブラリ も参照。

## エンタープライズ バックアップ環境

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

MoM も参照。

## お

### オートチェン ジャー

ライブラリ を参照。

### オートローダ

ライブラリ を参照。

### オブジェクト

バックアップオブジェクト を参照。

### オブジェクト ID

**(Windows 固有の用語)** オブジェクト ID(OID) を使用すると、システムのどこにファイルがあるかにかかわらず、NTFS 5 ファイルにアクセスできます。Data Protector では、ファイルの代替ストリームとして OID を扱います。

### オブジェクト検証

Data Protector の観点で見たバックアップオブジェクトのデータ整合性と、それらを必要なあて先に送信する Data Protector の機能を確認する処理です。処理は、バックアップ、オブジェクトコピー、またはオブジェクト集約セッションによって作成されたオブジェクトバージョンを復元する機能に信頼レベルを付与するために使用できます。

### オブジェクト検証 セッション

指定のバックアップオブジェクトまたはオブジェクトバージョンのデータ整合性と、指定のホストにそれらを送信するための選択済み Data Protector ネットワークコンポーネントの機能を確認するプロセスです。オブジェクト検証セッションは、対話式に実行することも、自動ポストバックアップまたはスケジュール仕様の指定通りに実行することもできます。

### オブジェクトコ ピー

特定のオブジェクトバージョンのコピー。オブジェクトコピーセッション中またはオブジェクトミラーのバックアップセッション中に作成されます。

### オブジェクトコ ピーセッション

異なるメディアセット上にバックアップデータの追加コピーを作成するプロセス。オブジェクトコピーセッション中に、選択されたバックアップオブジェクトがソースからターゲットメディアへコピーされます。

### オブジェクト集約

1つのフルバックアップと1つ以上の増分バックアップで構成されたバックアップオブジェクトの復元チェーンを、新たな集約されたバージョンのオブジェクトとしてマージするプロセス。このプロセスは、合成バックアップの一部です。このプロセスの結果、指定のバックアップオブジェクトの合成フルバックアップが出力されます。

### オブジェクト集約 セッション

1つのフルバックアップと1つ以上の増分バックアップで構成されたバックアップオブジェクトの復元チェーンを、新たな統合されたバージョンのオブジェクトとしてマージするプロセス。

### オブジェクトのコ ピー

選択されたオブジェクトバージョンを特定のメディアセットにコピーするプロセス。1つまたは複数のバックアップセッションから、コピーするオブジェクトバージョンを選択できます。

### オブジェクトのミ ラーリング

バックアップセッション中に、いくつかのメディアセットに同じデータを書き込むプロセス。Data Protector を使用すると、1つまたは複数のメディアセットに対し、すべてまたは一部のバックアップオブジェクトをミラーリングすることができます。

### オブジェクトミ ラー

オブジェクトのミラーリングを使用して作成されるバックアップオブジェクトのコピー。オブジェクトのミラーは、通常、オブジェクトコピーと呼ばれます。

### オフライン REDO ログ

アーカイブ REDO ログ を参照。

### オフラインバック アップ

実行中はアプリケーションデータベースがアプリケーションから使用できなくなるバックアップ。オフラインバックアップセッションでは、一般にデータベースはデータ複製プロセス中に休止状態となり、バックアップシステムからは使用できますが、アプリケーションシステムからは使用できません。たとえばテープへのバックアップの場合、テープへのデータストリーミングが終わるまでの間となります。残りのバックアッププロセスでは、データベースは通常の稼働を再開できます。

ゼロダウンタイムバックアップ (ZDB) およびオンラインバックアップ も参照。

<b>オフライン復旧</b>	オフライン復旧は、ネットワーク障害などにより Cell Manager にアクセスできない場合に行われます。オフライン復旧では、スタンドアロンデバイスおよび SCSI ライブラリデバイスのみで使用可能です。Cell Manager の復旧は、常にオフラインで行われます。
<b>オリジナルシステム</b>	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。
<b>オンライン REDO ログ</b>	<b>(Oracle 固有の用語)</b> まだアーカイブされていないが、インスタンスでデータベースアクティビティを記録するために利用できるか、または満杯になっており、アーカイブまたは再使用されるまで待機している REDO ログ。 アーカイブ REDO ログ も参照。
<b>オンラインバックアップ</b>	データベースアプリケーションを利用可能な状態に維持したまま行われるバックアップ。データベースは、データ複製プロセスの間、特別なバックアップモードで稼働します。たとえばテープへのバックアップの場合、テープへのデータストリーミングが終わるまでの間となります。この期間中、データベースは完全に機能しますが、パフォーマンスに多少影響が出たり、ログファイルのサイズが急速に増大したりする場合があります。残りのバックアッププロセスでは、データベースは通常の稼働を再開できます。  場合によっては、データベースを整合性を保って復元するために、トランザクションログもバックアップする必要があります。  ゼロダウンタイムバックアップ (ZDB) およびオフラインバックアップ も参照。
<b>オンライン復旧</b>	オンライン復旧は、Cell Manager がアクセス可能な場合に行います。この場合、Data Protector のほとんどの機能 (Cell Manager によるセッションの実行、復元セッションの IDB への記録、GUI を使った復元作業の進行状況の監視など) が使用可能です。
 か	
<b>階層ストレージ管理 (HSM)</b>	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。
<b>拡張可能ストレージエンジン (ESE)</b>	<b>(Microsoft Exchange Server 固有の用語)</b> Microsoft Exchange Server で情報交換用の記憶システムとして使用されているデータベーステクノロジー。
<b>拡張増分バックアップ</b>	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。
<b>確認</b>	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。
<b>仮想コントローラソフトウェア (VCS)</b>	<b>(HP P6000 EVA ディスクアレイファミリ固有の用語)</b> HSV コントローラを介した HP Command View EVA との通信など、記憶システムの処理すべてを管理するファームウェア。 HP Command View (CV) EVA も参照。
<b>仮想サーバー</b>	ネットワーク IP 名および IP アドレスでドメイン内に定義されるクラスター環境の仮想マシンです。アドレスはクラスターソフトウェアによりキャッシュされ、仮想サーバーリソースを現在実行しているクラスターノードにマップされます。こうして、特定の仮想サーバーに対するすべての要求が特定のクラスターノードにキャッシュされます。
<b>仮想ディスク</b>	<b>(HP P6000 EVA ディスクアレイファミリ固有の用語)</b> HP P6000 EVA ディスクアレイファミリのディスクアレイのストレージプールから割り当てられるストレージユニット。仮想ディスクは、このようなディスクアレイのスナップショット機能を使用して複製可能なエンティティです。 ソースボリュームおよびターゲットボリューム も参照。
<b>仮想テープ</b>	<b>(VLS 固有の用語)</b> テープに保存された場合と同様にディスクドライブにデータをバックアップするアーカイブ式ストレージテクノロジー。バックアップスピードおよびリカバリスピードの向上、運用コストの削減など仮想テープシステムとしての利点がある。 仮想ライブラリシステム (VLS) および仮想テープライブラリ (VTL) も参照。
<b>仮想テープライブラリ (VTL)</b>	<b>(VLS 固有の用語)</b> 従来のテープベースのストレージ機能を提供する、エミュレートされるテープライブラリ。

仮想ライブラリシステム (VLS) も参照。

<b>仮想デバイスインタフェース</b>	<b>(Microsoft SQL Server 固有の用語)</b> Microsoft SQL Server のプログラミングインタフェースの 1 つ。大容量のデータベースを高速でバックアップおよび復元できます。
<b>仮想フルバックアップ</b>	コピーするのではなくポインタを使用してデータが統合される、効率の良い合成バックアップ。配布ファイルメディア形式を使用する 1 つのファイルライブラリにすべてのバックアップ (フルバックアップ、増分バックアップ、およびその結果である仮想フルバックアップ) が書き込まれる場合に実行されます。
<b>仮想ライブラリシステム (VLS)</b>	1 つまたは複数の仮想テーブルライブラリ (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。
<b>カタログ保護</b>	バックアップデータに関する情報 (ファイル名やファイルバージョンなど) を IDB に維持する期間を定義します。 データ保護 も参照。
<b>監査情報</b>	Data Protector セル全体に対し、ユーザーが定義した拡張期間にわたって実施された、全バックアップセッションに関するデータ。
<b>監査レポート</b>	監査ログファイルに保存されたデータから作成される、ユーザーが判読可能な形式の監査情報出力。
<b>監査ログ</b>	監査情報が保存されるデータファイル。

き

<b>キーストア</b>	すべての暗号化キーは、Cell Manager のキーストアに集中的に格納され、キー管理サーバー (KMS) により管理されます。
<b>キーマネージメントサービス</b>	<b>(Microsoft Exchange Server 固有の用語)</b> 拡張セキュリティのための暗号化機能を提供する Microsoft Exchange Server のサービス。 インフォメーションストアおよびサイト複製サービス も参照。
<b>共有ディスク</b>	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。
<b>緊急ブートファイル</b>	<b>(Informix Server 固有の用語)</b> Informix Server 構成ファイル <code>ixbar.server_id</code> 。このファイルは、 <code>INFORMIXDIR/etc</code> ディレクトリ (Windows の場合)、または <code>INFORMIXDIR\etc</code> ディレクトリ (UNIX の場合) に置かれています。 <code>INFORMIXDIR</code> は Informix Server のホームディレクトリ、 <code>server_id</code> は <code>SERVERNUM</code> 構成パラメータの値です。緊急ブートファイルの各行は、1 つのバックアップオブジェクトに対応します。

く

<b>クライアントバックアップ</b>	Data Protector クライアントにマウントされているすべてのボリューム (ファイルシステム) のバックアップ。実際に何がバックアップされるかは、バックアップ仕様でどのようにオブジェクトを選択するかによって異なります。 <ul style="list-style-type: none"><li>クライアントシステム名の隣のチェックボックスを選択した場合、[クライアントシステム] の種類の 1 つのバックアップオブジェクトが作成されます。その結果、バックアップ時に Data Protector は選択されたクライアントにマウントされているすべてのボリュームを最初に検出してから、それらをバックアップします。Windows クライアントの場合、<code>CONFIGURATION</code> もバックアップされます。</li><li>クライアントシステムにマウントされているすべてのボリュームを別々に選択する場合、<code>Filesystem</code> タイプの個別バックアップオブジェクトがボリュームごとに作成されます。その結果、バックアップ時に、選択されたボリュームのみがバックアップされます。バックアップ仕様の作成後にクライアントにマウントされたボリュームは、バックアップされません。</li></ul>
---------------------	---

### 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。

<b>クラスター対応アプリケーション</b>	クラスターアプリケーションプログラミングインタフェースをサポートしているアプリケーション。クラスター対応アプリケーションごとに、クリティカルリソースが宣言されます。これらのリソースには、ディスクボリューム (Microsoft Cluster Server の場合)、ボリュームグ
------------------------	--

ループ (MC/ServiceGuard の場合)、アプリケーションサービス、IP 名および IP アドレスなどがあります。

## クラスター連続レプリケーション

**(Microsoft Exchange Server 固有の用語)** クラスター連続レプリケーション (CCR) はクラスター管理とフェイルオーバーオプションを使用して、ストレージグループの完全なコピー (CCR コピー) を作成および維持する高可用性ソリューションです。ストレージグループは個別のサーバーに複製されます。CCR は Exchange バックエンドサーバーで発生した単発箇所の障害を取り除きます。CCR コピーが存在するパッシブ Exchange Server ノードで VSS を使用してバックアップを実行すれば、アクティブノードの負荷が軽減されます。

CCR コピーへの切り替えは数秒で完了するため、CCR コピーはディザスタリカバリに使用されます。複製されたストレージグループは、Exchange ライターの新しいインスタンス (Exchange Replication Service) として表示され、元のストレージグループと同様に VSS を使用してバックアップできます。

Exchange Replication Service およびローカル連続レプリケーション も参照。

## グループ

**(Microsoft Cluster Server 固有の用語)** 特定のクラスター対応アプリケーションを実行するために必要なリソース (ディスクボリューム、アプリケーションサービス、IP 名および IP アドレスなど) の集合。

## グローバルオプションファイル

Data Protector をカスタマイズするためのファイル。このファイルでは、Data Protector のさまざまな設定 (特に、タイムアウトや制限) を定義でき、その内容は Data Protector セル全体に適用されます。このファイルは、

*Data\_Protector\_program\_data*\Config\Server\Options ディレクトリ (Windows Server 2008 の場合)、*Data\_Protector\_home*\Config\Server\Options ディレクトリ (その他の Windows システムの場合)、または */etc/opt/omni/server/options* ディレクトリ (HP-UX または Linux システムの場合) の Cell Manager に置かれています。

## こ

### 合成バックアップ

データに関しては従来のフルバックアップと同じである合成フルバックアップを、生産サーバーやネットワークに負担をかけずに出力するバックアップソリューション。合成フルバックアップは、前回のフルバックアップと任意の数の増分バックアップを使用して作成されます。

### 合成フルバックアップ

バックアップオブジェクトの復元チェーンが新たな合成フルバージョンのオブジェクトにマージされる、オブジェクト集約処理の結果。合成フルバックアップは、復元速度の面では従来のフルバックアップと同じです。

### コピーセット

**(HP P6000 EVA ディスクアレイファミリ固有の用語)** ローカル P6000 EVA 上にあるソースボリュームとリモート P6000 EVA 上にあるその複製とのペア。ソースボリューム、複製、および HP Continuous Access + Business Copy(CA+BC)P6000 EVA も参照。

### コマンドデバイス

**(HP P9000 XP ディスクアレイファミリ固有の用語)** ディスクアレイ内の専用のボリュームで、管理アプリケーションとディスクアレイのストレージシステムとの間のインターフェースとして機能します。データストレージ用に使用することはできません。操作に対する要求のみを受け付け、ディスクアレイによってその操作が実行されます。

### コマンドラインインタフェース (CLI)

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

### コンテナ

**(HP P6000 EVA ディスクアレイファミリ固有の用語)** ディスクアレイ上のスペース。後で標準スナップショット、vsnap、またはスナップクローンとして使用するために事前に割り当てられます。

## さ

### 再解析ポイント

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

<b>再同期モード</b>	<b>(HP P9000 XP ディスクアレイファミリ VSS プロバイダ固有の用語)</b> 2 種類ある P9000 XP アレイ VSS ハードウェアプロバイダの操作モードの 1 つ。P9000 XP アレイプロバイダが再同期モードであると、ソースボリューム (P-VOL) とその複製 (S-VOL) は、バックアップ後、中断ミラー関係になります。MU 範囲が 0-2(つまり、0、1、2) の場合、ローテーションされる最大複製数 (P-VOL 当たりの S-VOL 数) は 3 となります。このような構成でのバックアップからの復元は、S-VOL をその P-VOL と再同期することによってのみ可能となります。VSS 準拠モード、ソースボリューム、プライマリボリューム (P-VOL)、複製、セカンダリボリューム (S-VOL)、ミラーユニット (MU) 番号、および複製セットローテーションも参照。
<b>サイト複製サービス</b>	<b>(Microsoft Exchange Server 固有の用語)</b> Exchange Server 5.5 ディレクトリサービスをエミュレートすることで、Microsoft Exchange Server 5.5 と互換性のある Microsoft Exchange Server 2003 のサービス。 インフォメーションストアおよびキーマネジメントサービスも参照。
<b>差分同期 (再同期)</b>	<b>(EMC Symmetrix 固有の用語)</b> BCV または SRDF 制御操作。BCV 制御操作では、差分同期 (Incremental Establish) により、BCV デバイスが増分的に同期化され、EMC Symmetrix ミラー化メディアとして機能します。EMC Symmetrix デバイスは、事前にペアにしておく必要があります。SRDF 制御操作では、差分同期 (Incremental Establish) により、ターゲットデバイス (R2) が増分的に同期化され、EMC Symmetrix ミラー化メディアとして機能します。EMC Symmetrix デバイスは、事前にペアにしておく必要があります。
<b>差分バックアップ</b>	前回のフルバックアップより後の変更をバックアップする増分バックアップ。このバックアップを実行するには、増分 1 バックアップを指定します。 増分バックアップも参照。
<b>差分バックアップ</b>	<b>(Microsoft SQL Server 固有の用語)</b> 前回のフルデータベースバックアップ以降にデータベースに対して加えられた変更だけを記録するデータベースバックアップ。 バックアップの種類も参照。
<b>差分リストア</b>	<b>(EMC Symmetrix 固有の用語)</b> BCV または SRDF 制御操作。BCV 制御操作では、差分リストアにより、BCV デバイスがペア内の 2 番目に利用可能な標準デバイスのミラーとして再割り当てされます。これに対し、標準デバイスの更新時には、オリジナルのペアの分割中に BCV デバイスに書き込まれたデータだけが反映され、分割中に標準デバイスに書き込まれたデータは BCV ミラーからのデータで上書きされます。SRDF 制御操作では、差分リストアにより、ターゲットデバイス (R2) がペア内の 2 番目に利用可能なソースデバイス (R1) のミラーとして再割り当てされます。これに対し、ソースデバイス (R1) の更新時には、オリジナルのペアの分割中にターゲットデバイス (R2) に書き込まれたデータだけが反映され、分割中にソースデバイス (R1) に書き込まれたデータはターゲットミラー (R2) からのデータで上書きされます。

し

## システムボリューム/ディスク/パーティション

オペレーティングシステムファイルが格納されているボリューム/ディスク/パーティション。ただし、Microsoft の用語では、ブートプロセスの開始に必要なファイルが入っているボリューム/ディスク/パーティションをシステムボリューム/システムディスク/システムパーティションと呼んでいます。

**システム状態** **(Windows 固有の用語)** システム状態データには、レジストリ、COM+ クラス登録データベース、システム起動ファイル、および証明書サービスデータベース (Certificate Server の場合) が含まれます。サーバーがドメインコントローラの場合は、Active Directory サービスと SYSVOL ディレクトリもシステム状態データに含まれます。サーバーがクラスターサービスを実行している場合、システム状態データにはリソースレジストリチェックポイントとクォーラムリソースリカバリ ログが含まれ、最新のクラスターデータ情報が格納されます。

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

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

<b>システム復旧データファイル</b>	SRD ファイル を参照。
<b>事前割り当てリスト</b>	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。
<b>実行後</b>	オブジェクトのバックアップ後、またはセッション全体の完了後にコマンドまたはスクリプトを実行するバックアップオプション。実行後コマンドは、Data Protector で事前に用意されているものではありません。ユーザーは、コマンドを独自に作成する必要があります。Windows 上で動作する実行可能ファイルまたはバッチファイル、UNIX 上で動作するシェルスクリプトなどを使用できます。 実行前 も参照。
<b>実行前コマンドと実行後コマンド</b>	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。
<b>実行前</b>	オブジェクトのバックアップ前、またはセッション全体の開始前にコマンドまたはスクリプトを実行するバックアップオプション。実行前コマンドおよび実行後コマンドは、Data Protector で事前に用意されているものではありません。ユーザーは、コマンドを独自に作成する必要があります。Windows 上で動作する実行可能ファイルまたはバッチファイル、UNIX 上で動作するシェルスクリプトなどを使用できます。 実行後 も参照。
<b>自動移行</b>	<b>(VLS 固有の用語)</b> データのバックアップをまず VLS の仮想テープに作成し、それを物理テープ (1 つの仮想テープが 1 つの物理テープをエミュレート) に移行する操作を、中間バックアップアプリケーションを使用せずに実行する機能。 仮想ライブラリシステム (VLS) と仮想テープ も参照。
<b>自動ストレージ管理 (ASM)</b>	<b>(Oracle 固有の用語)</b> Oracle に統合されるファイルシステムおよびボリュームマネージャーで、Oracle データベースファイルを管理します。データやディスクの管理が簡単になり、ストライピング機能やミラーリング機能によってパフォーマンスが最適化されます。
<b>シャドウコピー</b>	<b>(Microsoft VSS 固有の用語)</b> 特定の時点におけるオリジナルボリューム (元のボリューム) の複製を表すボリューム。オリジナルボリュームからではなく、シャドウコピーからデータがバックアップされます。オリジナルボリュームはバックアップ処理中も更新が可能です。ボリュームのシャドウコピーは同じ内容に維持されます。 Microsoft ボリュームシャドウコピーサービスおよび複製 も参照。
<b>シャドウコピーセット</b>	<b>(Microsoft VSS 固有の用語)</b> 同じ時点で作成されたシャドウコピーのコレクション。 シャドウコピーおよび複製セット も参照。
<b>シャドウコピープロバイダ</b>	<b>(Microsoft VSS 固有の用語)</b> ボリュームシャドウコピーの作成と表現を行うエンティティ。プロバイダは、シャドウコピーデータを所有して、シャドウコピーを公開します。プロバイダは、ソフトウェア (システムプロバイダなど) で実装することも、ハードウェア (ローカルディスクやディスクアレイ) で実装することもできます。 シャドウコピー も参照。
<b>ジュークボックス</b>	ライブラリ を参照。
<b>ジュークボックスデバイス</b>	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。
<b>集中型ライセンス</b>	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せん。すべての Data Protector ライセンスは、エンタープライズ Cell Manager システム上にインストールされます。ライセンスは、実際のニーズに応じてエンタープライズ Cell Manager システムから特定のセルに割り当てることができます。 MoM も参照。
<b>循環ログ</b>	<b>(Microsoft Exchange Server および Lotus Domino Server 固有の用語)</b> 循環ログは、Microsoft Exchange Server データベースおよび Lotus Domino Server データベースモードの 1 つ。このモードでは、トランザクションログファイルのコンテンツは、対応するデータがデータベースにコミットされると、定期的の上書きされます。循環ログにより、ディスク記憶領域の要件が軽減されます。
<b>初期化</b>	フォーマット を参照。

## 所有権

バックアップ所有権は、データを参照および復元するユーザーの能力に影響します。各バックアップセッションとの中でバックアップされたすべてのデータはオーナーに割り当てられます。所有者は、対話型バックアップを開始するユーザー、CRS プロセスを実行するとき使用するアカウント、またはバックアップ仕様オプションで所有者として指定されたユーザーです。

ユーザーが既存のバックアップ仕様を修正せずにそのまま起動した場合、そのバックアップセッションは対話型とみなされません。

ユーザーがバックアップ仕様を修正して起動すると、以下の条件が成立しない限り、そのユーザーがオーナーになります。

- そのユーザーが [セッションの所有権を切り替え] ユーザー権限を持っている。
- バックアップ仕様内でバックアップセッションオーナーを明示的に定義するには、ユーザー名、グループ名またはドメイン名、およびシステム名を指定します。

UNIX Cell Manager 上でスケジュールしたバックアップの場合、上記の条件が成立しない限り、root: sys がセッションオーナーになります。

Windows Cell Manager 上でスケジュールしたバックアップの場合は、上記の条件が成立していない限り、インストール時に指定されたユーザーがセッションオーナーになります。オブジェクトのコピーまたは統合を行う場合のオーナーは、コピー仕様や統合仕様で別のオーナーが指定されていない限り、デフォルトでは、その操作を開始するユーザーです。

## す

### スイッチオーバー スキャン

フェイルオーバー を参照。

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を確認できます。

### スケジューラ

自動バックアップの実行タイミングと頻度を制御する機能。スケジュールを設定することで、バックアップの開始を自動化できます。

### スタッカー

メディア記憶用の複数のスロットを備えたデバイス。通常は、1 ドライブ構成です。スタッカーは、スタックからシーケンシャルにメディアを選択します。これに対し、ライブラリはレポジトリからメディアをランダムに選択します。

### スタンドアロン ファイルデバイス

ファイルデバイスとは、ユーザーがデータのバックアップに指定したディレクトリにあるファイルのことです。

### ストレージグループ

(Microsoft Exchange Server 固有の用語) 同じログファイルを共有する複数のメールボックスストアとパブリックフォルダストアのコレクション。Exchange Server では、各ストレージグループを個別のサーバープロセスで管理します。

### ストレージボ リューム

(ZDB 固有の用語) ボリューム管理システム、ファイルシステム、他のオブジェクトなどが存在可能なオペレーティングシステムや他のエンティティ (たとえば、仮想化機構など) に提示できるオブジェクト。ボリューム管理システム、ファイルシステムはこの記憶域に構築されます。これらは通常、ディスクアレイなどの記憶システム内に作成または存在します。

### スナップショット

(HP P4000 SAN ソリューション、HP P6000 EVA ディスクアレイファミリ、HP P9000 XP ディスクアレイファミリ、および HP P10000 Storage Systems 固有の用語) 特定の複製方法で作成されたターゲットボリュームの種類の一つ。ディスクアレイモデルと選択した複製方法に応じて、特性の異なる、さまざまなスナップショットの種類が使用できます。基本的に、各スナップショットは仮想コピー (ソースボリュームの内容に引き続き依存します)、またはソースボリュームから独立した複製 (クローン) のどちらかです。複製およびスナップショット作成 も参照。

### スナップショット 作成

(HP P4000 SAN ソリューション、HP P6000 EVA ディスクアレイファミリ、HP P9000 XP ディスクアレイファミリ、および HP P10000 Storage Systems 固有の用語) 選択したソースボリュームのコピーをストレージ仮想化技術を使用して作成する複製作成プロセス。スナップショットは、ある特定の時点で作成されたときみなされる複製で、作成後すぐに使用できます。ただし、スナップショットの種類によっては、複製作成後にデータコピープロセスがバックグラウンドで継続して実行されるものもあります。スナップショット も参照。

<b>スナップショット バックアップ</b>	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。
<b>スパースファイル</b>	ブロックが空の部分を含むファイル。例として、データの一部または大部分にゼロが含まれるマトリクス、イメージアプリケーションからのファイル、高速データベースなどがあります。スパースファイルの処理を復元中に有効にしておかないと、スパースファイルを復元できなくなる可能性があります。
<b>スプリットミラー</b>	<b>(EMC Symmetrix Disk Array および HP P9000 XP ディスクアレイファミリ固有の用語)</b> 特定の複製方法で作成されたターゲットボリュームの種類の 1 つ。スプリットミラー複製により、ソースボリュームの独立した複製 (クローン) が作成されます。複製およびスプリットミラーの作成 も参照。
<b>スプリットミラー の作成</b>	<b>(EMC Symmetrix および HP P9000 XP ディスクアレイファミリ固有の用語)</b> 事前構成したターゲットボリュームのセット (ミラー) を、ソースボリュームの内容の複製が必要になるまでソースボリュームのセットと同期化し続ける複製技法。その後、同期を停止 (ミラーを分割) すると、分割時点でのソースボリュームのスプリットミラー複製はターゲットボリュームに残ります。スプリットミラー も参照。
<b>スプリットミラー バックアップ (EMC Symmetrix 固有の用語)</b>	テープへの ZDB を参照。
<b>スプリットミラー バックアップ (HP P9000 XP ディス クアレイファミリ 固有の用語)</b>	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。
<b>スプリットミラー 復元</b>	<b>(EMC Symmetrix および HP P9000 XP ディスクアレイファミリ固有の用語)</b> テープへの ZDB セッションまたはディスク + テープへの ZDB セッションでバックアップされたデータを、最初にバックアップメディアから複製に、その後に複製からソースボリュームにコピーするプロセス。この方法では、完全なセッションを復元することも個々のバックアップオブジェクトを復元することも可能です。テープへの ZDB、ディスク + テープへの ZDB および複製 も参照。
<b>スマートコピー</b>	<b>(VLS 固有の用語)</b> 仮想テープから物理テープライブラリへ作成されたバックアップデータのコピー。スマートコピーのプロセスによって、Data Protector ではソースメディアとターゲットメディアを区別できるため、メディア管理が可能になります。仮想ライブラリシステム (VLS) も参照。
<b>スマートコピー プール</b>	<b>(VLS 固有の用語)</b> 指定されたソース仮想ライブラリに対してどのコピー先ライブラリロットをスマートコピーターゲットとして使用できるかどうかを定義するプール。仮想ライブラリシステム (VLS) およびスマートコピー も参照。
<b>スレッド</b>	<b>(Microsoft SQL Server 固有の用語)</b> 1 つのプロセスのみに属する実行可能なエンティティ。プログラムカウンタ、ユーザーモードスタック、カーネルモードスタック、およびレジスタ値のセットからなります。同じプロセス内で複数のスレッドを同時に実行できます。
<b>スロット</b>	ライブラリ内の機械的位置。各スロットが DLT テープなどのメディアを 1 つずつ格納できません。Data Protector では、各スロットを番号で参照します。メディアを読み取るときには、ロボット機構がメディアをスロットからドライブに移動します。

## せ

<b>制御ファイル</b>	<b>(Oracle および SAP R/3 固有の用語)</b> データベースの物理構造を指定するエントリが記述された Oracle データファイル。復旧に使用するデータベース情報の整合性を確保できます。
<b>セカンダリボ リューム (S-VOL)</b>	<b>(HP P9000 XP ディスクアレイファミリ固有の用語)</b> HP P9000 XP ディスクアレイファミリのディスクアレイの内部ディスク (LDEV) で、もう 1 つの LDEV であるプライマリボリューム (P-VOL) とペアとなっています。プライマリボリューム (P-VOL) セカンダリボリュームは、P-VOL のミラーとして、また P-VOL のスナップショットストレージに使用されるボリュームとして機能することが可能です。S-VOL は P-VOL に使用される SCSI アドレスとは異なるアドレスに割り当てられます。HP CA P9000 XP 構成では、ミラーとして機能する S-VOL を MetroCluster 構成のフェイルオーバーデバイスとして使用することができます。

プライマリボリューム (P-VOL) およびメインコントロールユニット (MCU) も参照。

<b>セッション</b>	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。
<b>セッション ID</b>	バックアップ、復元、オブジェクトコピー、オブジェクト集約、オブジェクト検証、またはメディア管理のセッションの識別子で、セッションを実行した日付と一意の番号から構成されます。
<b>セッションキー</b>	実行前スクリプトおよび実行後スクリプト用の環境変数。Data Protector プレビューセッションを含めたセッションを一意に識別します。セッションキーはデータベースに記録されず、omnimnt, omnistat および omniabort コマンドのオプション指定に使用されます。
<b>セル</b>	1 台の Cell Manager に管理されているシステムの集合。セルは、通常、同じ LAN または SAN に接続されている、サイト上または組織エンティティ上のシステムを表します。集中管理によるバックアップおよび復元のポリシーやタスクの管理が可能です。
<b>ゼロダウンタイム バックアップ (ZDB)</b>	ディスクアレイにより実現したデータ複製技術を用いて、アプリケーションシステムのバックアップ処理の影響を最小限に抑えるバックアップアプローチ。バックアップされるデータの複製がまず作成されます。その後のすべてのバックアップ処理は、元のデータではなく複製データを使って実行し、アプリケーションシステムは通常の処理に復帰します。ディスクへの ZDB、テープへの ZDB、ディスク + テープへの ZDB、およびインスタントリカバリ も参照。

## そ

<b>増分 1 メールボックスバックアップ</b>	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。
<b>増分 ZDB</b>	ファイルシステム ZDB からテープへ、または ZDB からディスク + テープへのセッション。前回の保護されたフルバックアップまたは増分バックアップ以降に変更された内容のみがテープにストリーミングされます。フル ZDB も参照。
<b>増分バックアップ</b>	前回のバックアップ以降に変更があったファイルだけを選択するバックアップ。増分バックアップには複数のレベルがあり、復元チェーンの長さを細かく制御できます。バックアップの種類 も参照。
<b>増分バックアップ</b>	<b>(Microsoft Exchange Server 固有の用語)</b> 前回のフルバックアップまたは増分バックアップ以降の変更だけをバックアップする Microsoft Exchange Server データのバックアップ。増分バックアップでは、バックアップ対象はトランザクションログだけです。バックアップの種類 も参照。
<b>増分メールボックスバックアップ</b>	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。
<b>ソースデバイス (R1)</b>	<b>(EMC Symmetrix 固有の用語)</b> ターゲットデバイス (R2) との SRDF 操作に参加する EMC Symmetrix デバイス。このデバイスに対するすべての書き込みは、リモート EMC Symmetrix ユニット内のターゲットデバイス (R2) にミラー化されます。R1 デバイスは、RDF1 グループタイプに割り当てる必要があります。ターゲットデバイス (R2) も参照。
<b>ソースボリューム</b>	<b>(ZDB 固有の用語)</b> 複製されるデータを含むストレージボリューム。

## た

<b>ターゲットシステム</b>	<b>(ディザスタリカバリ固有の用語)</b> 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。
<b>ターゲットデータベース</b>	<b>(Oracle 固有の用語)</b> 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。
<b>ターゲットデバイス (R2)</b>	<b>(EMC Symmetrix 固有の用語)</b> ターゲットデバイス (R1) との SRDF 操作に参加する EMC Symmetrix デバイス。リモート EMC Symmetrix ユニット内に置かれます。ローカル EMC Symmetrix ユニット内でソースデバイス (R1) とペアになり、ミラー化ペアから、すべての書き込みデータを受け取ります。このデバイスは、通常の I/O 操作ではユーザーアプリケー

ションからアクセスされません。R2 デバイスは、RDF2 グループタイプに割り当てる必要があります。

ソースデバイス (R1) も参照。

## ターゲットボリューム

**(ZDB 固有の用語)** 複製されるデータを含むストレージボリューム。

## ターミナルサービス

**(Windows 固有の用語)** Windows のターミナルサービスは、サーバー上で実行されている仮想 Windows デスクトップセッションと Windows ベースのプログラムにクライアントからアクセスできるマルチセッション環境を提供します。

## ち

### チャンネル

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

- disk タイプ
- sbt\_tape タイプ

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

## て

### ディザスタリカバリ

クライアントのメインシステムディスクを (フル) バックアップの実行時に近い状態に復元するためのプロセスです。

### ディザスタリカバリオペレーティングシステム

DR OS を参照。

### ディザスタリカバリの段階 0

ディザスタリカバリの準備 (ディザスタリカバリを成功させるための必須条件)。

### ディザスタリカバリの段階 1

DR OS のインストールと構成 (以前の記憶領域構造の構築)。

### ディザスタリカバリの段階 2

オペレーティングシステム (環境を定義する各種の構成情報を含む) と Data Protector の復元。

### ディザスタリカバリの段階 3

ユーザーデータとアプリケーションデータの復元。

### ディスク+テープへの ZDB

**(ZDB 固有の用語)** ゼロダウンタイムバックアップの 1 つの形式。ディスクへの ZDB と同様に、作成された複製が特定の時点でのソースボリュームのバックアップとしてディスクアレイに保持されます。ただし、テープへの ZDB と同様、複製データはバックアップメディアにもストリーミングされます。このバックアップ方法を使用した場合、同じセッションでバックアップしたデータは、インスタントリカバリプロセス、Data Protector 標準のテープからの復元を使用して復元できます。特定のディスクアレイファミリではスプリットミラー復元が可能です。

ゼロダウンタイムバックアップ (ZDB)、ディスクへの ZDB、テープへの ZDB、インスタントリカバリ、複製、および複製セットローテーション も参照。

### ディスクイメージ (raw ディスク) のバックアップ

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

### ディスククォータ

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

### ディスクグループ

**(Veritas Volume Manager 固有の用語)** VxVM システムのデータストレージの基本ユニット。ディスクグループは、1 つまたは複数の物理ボリュームから作成できます。同じシステム上に複数のディスクグループを置くことができます。

<b>ディスクステージング</b>	データをいくつかの段階に分けてバックアップする処理。これにより、バックアップと復元のパフォーマンスが向上し、バックアップデータの格納費用が節減され、データの可用性と復元時のアクセス性が向上します。バックアップステージは、最初に 1 種類のメディア (たとえば、ディスク) にデータをバックアップし、その後データを異なる種類のメディア (たとえば、テープ) にコピーすることから構成されます。
<b>ディスクへの ZDB</b>	<b>(ZDB 固有の用語)</b> ゼロダウンタイムバックアップの 1 つの形式。作成された複製が、特定の時点でのソースボリュームのバックアップとしてディスクアレイに保持されます。同じバックアップ仕様を使って別の時点で作成された複数の複製を、複製セットに保持することができます。テープに ZDB した複製はインスタントリカバリプロセスで復元できます。ゼロダウンタイムバックアップ (ZDB)、テープへの ZDB、ディスク + テープへの ZDB、インスタントリカバリ、および複製セットローテーション も参照。
<b>ディレクトリ接合</b>	<b>(Windows 固有の用語)</b> 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。
<b>データストリーム</b>	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。
<b>データファイル</b>	<b>(Oracle および SAP R/3 固有の用語)</b> Oracle によって作成される物理ファイル。表や索引などのデータ構造を格納します。データファイルは、1 つの Oracle データベースにのみ所属できます。
<b>データ複製 (DR) グループ</b>	<b>(HP P6000 EVA ディスクアレイファミリ固有の用語)</b> HP P6000 EVA ディスクアレイファミリ仮想ディスクの論理グループ。共通の性質を持ち、同じ HP CA P6000 EVA ログを共有していれば、最大 8 組のコピーセットを含めることができます。コピーセット も参照。
<b>データベースサーバー</b>	大規模なデータベース (SAP R/3 データベースや Microsoft SQL データベースなど) が置かれているコンピュータ。サーバー上のデータベースへは、クライアントからアクセスできます。
<b>データベースの差分バックアップ</b>	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。
<b>データベースの並列処理 (数)</b>	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。
<b>データベースライブラリ</b>	Data Protector のルーチンのセット。Oracle Server のようなオンラインデータベース統合ソフトウェアのサーバーと Data Protector の間でのデータ転送を可能にします。
<b>データ保護</b>	メディア上のバックアップデータを保護する期間を定義します。この期間中は、データが上書きされません。保護期限が切れると、それ以降のバックアップセッションでメディアを再利用できるようになります。カタログ保護 も参照。
<b>テープなしのバックアップ (ZDB 固有の用語)</b>	ディスクへの ZDB を参照。
<b>テープへの ZDB</b>	<b>(ZDB 固有の用語)</b> ゼロダウンタイムバックアップの 1 つの形式。作成された複製が、バックアップメディア (通常はテープ) にストリーミングされます。このバックアップ形式ではインスタントリカバリはできませんが、バックアップ終了後にディスクアレイ上に複製を保持する必要がありません。バックアップデータは Data Protector 標準のテープからの復元を使用して復元できます。特定のディスクアレイファミリでは、スプリットミラー復元が可能です。ゼロダウンタイムバックアップ (ZDB)、ディスクへの ZDB、ディスク + テープへの ZDB、インスタントリカバリ、および複製 も参照。
<b>デバイス</b>	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。
<b>デバイスグループ</b>	<b>(EMC Symmetrix 固有の用語)</b> 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。
<b>デバイスストリーミング</b>	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、バックアップを続けます。

**デルタバックアップ** 差分バックアップ (delta backup) では、前回の各種バックアップ以降にデータベースに対して加えられたすべての変更がバックアップされます。バックアップの種類 も参照。

と

**統合ソフトウェアオブジェクト** Oracle または SAP DB などの Data Protector 統合ソフトウェアのバックアップオブジェクト。

**同時処理数** Disk Agent の同時処理数 を参照。

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

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

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

**ドライブベースの暗号化** Data Protector のドライブベースの暗号化では、ドライブの暗号化機能が使用されます。バックアップの実行中、ドライブではメディアに書き込まれるデータとメタデータの両方が暗号化されます。

**トランザクション** 一連のアクションを単一の作業単位として扱えるようにするためのメカニズム。データベースでは、トランザクションを通じて、データベースの変更を追跡します。

**トランザクションバックアップ** トランザクションバックアップは、一般に、データベースのバックアップよりも必要とするリソースが少ないため、データベースのバックアップよりもより高い頻度で実行できます。トランザクションバックアップを適用することで、データベースを問題発生以前の特定の時点の状態に復旧することができます。

**トランザクションバックアップ** (**Sybase および SQL 固有の用語**) トランザクションログをバックアップすること。トランザクションログには、前回のフルバックアップまたはトランザクションバックアップ以降に発生した変更が記録されます。

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

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

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

**トランザクションログファイル** データベースを変更するトランザクションを記録するファイル。データベースが破損した場合にフォールトトレランスを提供します。

**トランスポートスナップショット** (**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 ポリリュームシャドウコピーサービス (VSS) も参照。

は

**ハートビート** 特定のクラスターノードの動作ステータスに関する情報を伝達するタイムスタンプ付きのクラスターデータセット。このデータセット (パケット) は、すべてのクラスターノードに配布されます。

**ハードリカバリ** (**Microsoft Exchange Server 固有の用語**) トランザクションログファイルを使用し、データベースエンジンによる復元後に実行される Microsoft Exchange Server のデータベース復旧。

<b>配布ファイルメディア形式</b>	ファイルライブラリで利用できるメディア形式。仮想フルバックアップと呼ばれる容量効率のいい合成バックアップをサポートしています。この形式を使用することは、仮想フルバックアップにおける前提条件です。 仮想フルバックアップも参照。
<b>バックアップ API</b>	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。
<b>バックアップ ID</b>	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。
<b>バックアップオーナー</b>	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。
<b>バックアップオブジェクト</b>	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。 <ul style="list-style-type: none"> <li>• 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</li> <li>• 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。</li> <li>• 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)。</li> <li>• 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」</li> </ul>
<b>バックアップシステム</b>	<b>(ZDB 固有の用語)</b> 1 つ以上のアプリケーションシステムとともにディスクアレイに接続されているシステム。ほとんどの場合、バックアップシステムはターゲットボリューム (複製) を作成するためにディスクアレイに接続されるほか、ターゲットボリューム (複製) のマウント処理に使用されます。 アプリケーションシステム、ターゲットボリュームおよび複製も参照。
<b>バックアップ仕様</b>	バックアップ対象のオブジェクトのリストに、使用するデバイスまたはドライブのセット、仕様に含まれているすべてのオブジェクトのバックアップオプション、およびバックアップを実行する曜日や時刻を加えたもの。オブジェクトとなるのは、ディスクやボリューム全体、またはその一部、たとえばファイル、ディレクトリ、Windows レジストリなどです。インクルードリストおよびエクスクルードリストを使用して、ファイルを選択することもできます。
<b>バックアップ世代</b>	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。
<b>バックアップセッション</b>	データのコピーを記憶メディア上に作成するプロセス。バックアップ仕様に処理内容を指定することも、対話式に操作を行うこともできます (対話式セッション)。1 つのバックアップ仕様の中で複数のクライアントが構成されている場合、すべてのクライアントが同じバックアップの種類を使って、1 回のバックアップセッションで同時にバックアップされます。バックアップセッションの結果、1 式のメディアにバックアップデータが書き込まれます。これらのメディアは、バックアップセットまたはメディアセットとも呼ばれます。 バックアップ仕様、フルバックアップ、および増分バックアップも参照。
<b>バックアップセット</b>	バックアップに関連したすべての統合ソフトウェアオブジェクトのセットです。

**バックアップセット** (Oracle 固有の用語) RMAN バックアップコマンドを使用して作成したバックアップファイルの論理グループ。バックアップセットは、バックアップに関連したすべてのファイルのセットです。これらのファイルはパフォーマンスを向上するため多重化することができます。バックアップセットにはデータファイルまたはアーカイブログのいずれかを含めることができますが、両方同時に使用できません。

**バックアップチェーン** 復元チェーン を参照。

**バックアップデバイス** 記憶メディアに対するデータの読み書きが可能な物理デバイスを Data Protector で使用できるように構成したもの。たとえば、スタンドアロン DDS/DAT ドライブやライブラリなどをバックアップデバイスとして使用できます。

**バックアップの種類** 増分バックアップ、差分バックアップ、トランザクションバックアップ、フルバックアップおよびデルタバックアップ を参照。

**バックアップビュー** Data Protector では、バックアップ仕様のビューを切り替えることができます。  
[種類別] を選択すると、バックアップ/テンプレートで利用できるデータの種類のに基づいたビューが表示されます。(デフォルト)  
[グループ別] を選択すると、バックアップ仕様/テンプレートの所属先のグループに基づいたビューが表示されます。  
[名前別] を選択すると、バックアップ仕様/テンプレートの名前に基づいたビューが表示されます。  
[Manager 別](MoM の実行時のみ有効) を選択すると、バックアップ仕様/テンプレートの所属先の Cell Manager に基づいたビューが表示されます。

**パッケージ** (MC/ServiceGuard および Veritas Cluster 固有の用語) 特定のクラスター対応アプリケーションを実行するために必要なリソース (ボリュームグループ、アプリケーションサービス、IP 名および IP アドレスなど) の集合。

#### パブリック/プライベートバックアップデータ

バックアップを構成する際は、バックアップデータをパブリックまたはプライベートのいずれにするかを選択できます。

- パブリックデータ – すべての Data Protector ユーザーに対してアクセスと復元が許可されます。
- プライベートデータ – バックアップの所有者および管理者に対してのみ表示と復元が許可されます。

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

ひ

**表領域** データベース構造の一部。各データベースは論理的に 1 つまたは複数の表領域に分割されます。各表領域には、データファイルまたは raw ボリュームが排他的に関連付けられます。

ふ

#### ブートボリューム/ディスク/パーティション

ブートプロセスの開始に必要なファイルが入っているボリューム/ディスク/パーティション。Microsoft の用語では、オペレーティングシステムファイルが入っているボリューム/ディスク/パーティションをブートボリューム/ブートディスク/ブートパーティションと呼んでいます。

**ファーストレベルミラー** (HP P9000 XP ディスクアレイファミリ固有の用語) HP P9000 XP ディスクアレイファミリのディスクアレイの内部ディスク (LDEV) のミラーで、このミラーをさらにミラー化し、セカンドレベルのミラーを作成できます。Data Protector ゼロダウンタイムバックアップおよびインスタントリカバリ目的には、ファーストレベルミラーのみを使用できます。プライマリボリュームおよびミラーユニット (MU) 番号 も参照。

<b>ファイバーチャネル</b>	ファイバーチャネルは、高速のコンピュータ相互接続に関する ANSI 標準です。光ケーブルまたは銅線ケーブルを使って、大容量データファイルを高速で双方向送信でき、数 km 離れたサイト間を接続できます。ファイバーチャネルは、ノード間を 3 種類の物理トポロジー (ポイントツーポイント、ループ、スイッチ式) で接続できます。
<b>ファイバーチャネルブリッジ</b>	ファイバーチャネルブリッジ (マルチプレクサ) は、RAID アレイ、ソリッドステートディスク (SSD)、テープライブラリなどの既存の平行 SCSI デバイスをファイバーチャネル環境に移行できるようにします。ブリッジ (マルチプレクサ) の片側には Fibre Channel インタフェースがあり、その反対側には平行 SCSI ポートがあります。このブリッジ (マルチプレクサ) を通じて、SCSI パケットを Fibre Channel と平行 SCSI デバイスの間で移動することができます。
<b>ファイルシステム</b>	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。
<b>ファイルジョークボックスデバイス</b>	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。
<b>ファイルツリーウォーク</b>	<b>(Windows 固有の用語)</b> どのオブジェクトが作成、変更、または削除されたかを判断するためにファイルシステムを巡回する処理。
<b>ファイルデポ</b>	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。
<b>ファイルバージョン</b>	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。
<b>ファイル複製サービス (FRS)</b>	Windows サービスの 1 つ。ドメインコントローラのストアログオンスクリプトとグループポリシーを複製します。また、分散ファイルシステム (DFS) 共有をシステム間で複製したり、任意のサーバーから複製作業を実行することもできます。
<b>ファイルライブラリデバイス</b>	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。
<b>フェイルオーバー</b>	あるクラスターノードから別のクラスターノードに最も重要なクラスターデータ (Windows の場合はグループ、UNIX の場合はパッケージ) を転送すること。フェイルオーバーは、主に、プライマリノードのソフトウェア/ハードウェア障害発生時や保守時に発生します。
<b>フェイルオーバー</b>	<b>(HP P6000 EVA ディスクアレイファミリ固有の用語)</b> HP Continuous Access + Business Copy (CA+BC) P6000 EVA 構成でソースとあて先の役割を逆にする操作。HP Continuous Access + Business Copy (CA+BC) P6000 EVA も参照。
<b>フォーマット</b>	メディアを Data Protector で使用できるように初期化するプロセス。メディア上の既存データはすべて消去されます。メディアに関する情報 (メディア ID、説明、場所) は、IDB および該当するメディア (メディアヘッダ) に保存されます。Data Protector のメディアは、保護の期限が切れるか、またはメディアの保護が解除されるかメディアがリサイクルされるまで、フォーマットされません。
<b>負荷調整</b>	デフォルトでは、デバイスが均等に使用されるように、バックアップ用に選択されたデバイスの負荷 (使用率) が自動的に調整されます。負荷調整では、各デバイスに書き込まれるオブジェクトの個数を調整することで、使用率を最適化します。負荷調整はバックアップ時に自動的に実行されるので、データが実際にどのようにバックアップされるかを管理する必要はありません。使用するデバイスを指定する必要があるだけです。負荷調整機能を使用しない場合は、バックアップ仕様に各オブジェクトに使用するデバイスを選択できます。Data Protector は、指定した順にデバイスにアクセスします。
<b>復元セッション</b>	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。
<b>復元チェーン</b>	特定の時点までのバックアップオブジェクトの復元に必要なバックアップすべて。復元チェーンは、オブジェクトのフルバックアップ 1 つと、任意の数の増分バックアップで構成されます。
<b>複製</b>	<b>(ZDB 固有の用語)</b> ユーザー指定のバックアップオブジェクトを含む、特定の時点におけるソースボリュームのデータのイメージ。イメージは、作成するハードウェアまたはソフトウェアによって、物理ディスクレベルでの記憶ブロックの独立した正確な複製 (クローン) になる (スプリットミラーやスナップクローンなど) 場合もあれば、仮想コピーになる (スナップショットなど) 場合もあります。基本的なオペレーティングシステムの観点からすると、バックアッ

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

## 複製セット

**(ZDB 固有の用語)** 同じバックアップ仕様を使って作成される複製のグループ。複製および複製セットローテーションも参照。

## 複製セットのローテーション

**(ZDB 固有の用語)** 通常のバックアップ作成のために継続的に複製セットを使用すること。複製セットの使用を必要とする同一のバックアップ仕様が実行されるたびに、新規の複製がセットの最大数になるまで作成され、セットに追加されます。その後、セット内の最も古い複製は置き換えられ、セット内の複製の最大数が維持されます。  
複製および複製セットも参照。

## 物理デバイス

ドライブまたはより複雑な装置 (ライブラリなど) を格納する物理装置。

## プライマリボリューム (P-VOL)

**(HP P9000 XP ディスクアレイファミリ固有の用語)** HP P9000 XP ディスクアレイファミリのディスクアレイの内部ディスク (LDEV) で、これに対して、そのミラー、またはスナップショットストレージに使用されるボリュームのいずれかのセカンダリボリューム (S-VOL) が存在します。HP CA P9000 XP および HP CA+BC P9000 XP 構成では、プライマリボリュームはメインコントロールユニット (MCU) 内に配置されています。  
セカンダリボリューム (S-VOL) およびメインコントロールユニット (MCU) も参照。

## フラッシュリカバリ領域

**(Oracle 固有の用語)** Oracle によって管理されるディレクトリ、ファイルシステム、または自動ストレージ管理 (ASM) ディスクグループであり、バックアップ、復元、およびデータベース復旧に関するファイル (リカバリファイル) 用の集中管理ストレージ領域として機能します。  
リカバリファイルも参照。

## フリープール

フリープールは、メディアプール内のすべてのメディアが使用中になっている場合にメディアのソースとして補助的に使用できるプールです。ただし、メディアプールでフリープールを使用するには、明示的にフリープールを使用するように構成する必要があります。

## フル ZDB

テープへの ZDB セッションまたはディスク + テープへの ZDB セッション。前回のバックアップから変更がない場合でも、選択したすべてのオブジェクトがテープにストリーミングされます。  
増分 ZDB も参照。

## フルデータベースバックアップ

最後に (フルまたは増分) バックアップした後に変更されたデータだけでなく、データベース内のすべてのデータのバックアップ。フルデータベースバックアップは、他のバックアップに依存しません。

## フルバックアップ

フルバックアップでは、最近変更されたかどうかに関係なく、選択されたオブジェクトをすべてバックアップします。  
バックアップの種類も参照。

## フルメールボックスバックアップ

フルメールボックスバックアップでは、メールボックス全体の内容をバックアップします。

## 分散ファイルシステム (DFS)

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

へ

## ペアステータス

**(HP P9000 XP ディスクアレイファミリ固有の用語)** HP P9000 XP ディスクアレイファミリのディスクアレイのディスクペア (セカンダリボリュームとそれに対応するプライマリボリューム) の状態。状況によってペアのディスクはさまざまな状態になる可能性があります。Data Protector HP P9000 XP Agent の操作において特に以下の状態が重要となります。

- ペア - セカンダリボリュームがゼロダウンタイムバックアップ用に準備されています。セカンダリボリュームがミラーの場合、完全に同期化されます。セカンダリボリュームがスナップショットストレージ用に使用されるボリュームの場合、空の状態です。

- 中断 – ディスク間のリンクは中断されています。ただし、ペアの関係は維持されたままとなり、後で再度ゼロダウンタイムバックアップを行うためにセカンダリディスクを準備できます。
- コピー – ディスクペアは現在使用中であり、ペア状態に移行中です。セカンダリボリュームがミラーの場合、プライマリボリュームで再同期されています。セカンダリボリュームがスナップショットストレージに使用されるボリュームの場合、その内容はクリアされています。

## 並行復元

単一の Media Agent からデータを受信する Disk Agent を複数実行して、バックアップされたデータを同時に複数のディスクに(並行して)復元すること。並行復元を行うには、複数のディスクまたは論理ボリュームに置かれているデータを選択し、同時処理数を 2 以上に設定してバックアップを開始し、異なるオブジェクトのデータを同じデバイスに送信する必要があります。並行復元中には、復元対象として選択した複数のオブジェクトがメディアから同時に読み取られるので、パフォーマンスが向上します。

## 並列処理

1 つのオンラインデータベースから複数のデータストリームを読み取ること。

## 変更ジャーナル

**(Windows 固有の用語)** ローカル NTFS ボリューム上のファイルやディレクトリへの変更が発生するたび、それに関するレコードをログに記録する Windows ファイルシステム機能。

## ほ

### 保護

データ保護およびカタログ保護 を参照。

### 補助ディスク

必要最小限のオペレーティングシステムファイル、ネットワークファイル、および Data Protector Disk Agent がインストールされたブート可能ディスク。ディスクデリバリーで UNIX クライアントを障害から復旧するときのフェーズ 1 では、補助ディスクをターゲットシステムのブートに使用することができます。

### ホストシステム

Data Protector Disk Agent がインストールされており、ディスクデリバリーによるディザスタリカバリに使用される稼働中の Data Protector クライアント。

### ボリュームグループ

LVM システムにおけるデータストレージ単位。ボリュームグループは、1 つまたは複数の物理ボリュームから作成できます。同じシステム上に複数のボリュームグループを置くことができます。

### ボリュームシャドウコピーサービス

Microsoft ボリュームシャドウコピーサービス (VSS) を参照。

### ボリュームマウントポイント

**(Windows 固有の用語)** ボリューム上の空のディレクトリを他のボリュームのマウントに使用できるように構成したもの。ボリュームマウントポイントは、ターゲットボリュームへのゲートウェイとして機能します。ボリュームがマウントされていれば、ユーザーやアプリケーションがそのボリューム上のデータをフル (マージ) ファイルシステムパスで参照できます (両方のボリュームが一体化されている場合)。

## ま

### マージ

復元中のファイル名競合を解決するモードの 1 つ。復元するファイルと同じ名前のファイルが復元先に存在する場合、変更日時の新しい方が維持されます。既存のファイルと名前が重複しないファイルは、常に復元されます。  
上書き も参照。

### マウントポイント

ディレクトリ構造内において、ディスクまたは論理ボリュームにアクセスするためのアクセスポイント (/opt や d: など)。UNIX では、bdf コマンドまたは df コマンドを使ってマウントポイントを表示できます。

### マウント要求

マウント要求時には、デバイスにメディアを挿入するように促す画面が表示されます。必要なメディアを挿入して確認することでマウント要求に応答すると、セッションが実行されます。

### マジックパケット

Wake ONLAN を参照。

### マルチスナップ

**(HP P6000 EVA ディスクアレイファミリ固有の用語)** 個々のターゲットボリュームだけでなく、スナップショットを構成するすべてのボリュームでバックアップデータの整合性が取れるように、複数のターゲットボリュームを同時に作成すること。  
スナップショット も参照。

## み

<b>ミラー (EMC Symmetrix および HP P9000 XP ディスクアレイファミリ固有の用語)</b>	ターゲットボリューム を参照。
<b>ミラークローン</b>	(HP P6000 EVA ディスクアレイファミリ固有の用語) ストレージボリュームの動的な複製です。元のストレージボリュームに加えられた変更は、ローカル複製リンクを介して、ミラークローンに反映されます。元のストレージボリュームとそのミラークローン間の複製は中断できません。各ストレージボリュームについてディスクアレイ上に 1 つのミラークローンを作成できます。
<b>ミラーユニット (MU) 番号</b>	(HP P9000 XP ディスクアレイファミリ固有の用語) HP P9000 XP ディスクアレイファミリのディスクアレイ上にある内部ディスク (LDEV) のセカンダリボリューム (S-VOL) を特定する 0 以上の整数。 ファーストレベルミラー も参照。
<b>ミラーローテーション (HP P9000 XP ディスクアレイファミリ固有の用語)</b>	複製セットローテーション を参照。

## む

<b>無人操作</b>	夜間処理 を参照。
-------------	-----------

## め

<b>メインコントロールユニット (MCU)</b>	(HP P9000 XP ディスクアレイファミリ固有の用語) HP CA P9000 XP または HP CA+BC P9000 XP 構成のプライマリボリューム (P-VOL) を含み、マスターデバイスとして機能する HP P9000 XP ディスクアレイファミリのユニット。 HP Business Copy (BC) P9000 XP、HP Continuous Access (CA) P9000 XP、および LDEV も参照。
<b>メールボックス</b>	(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。
<b>メールボックスストア</b>	(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。
<b>メディア ID</b>	Data Protector がメディアに割り当てる一意な識別子。
<b>メディア管理セッション</b>	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。
<b>メディア集中管理データベース (CMMDB)</b>	CMMDB を参照。
<b>メディア状態要素</b>	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。
<b>メディアセット</b>	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。
<b>メディアの位置</b>	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。
<b>メディアのインポート</b>	メディアに書き込まれているバックアップセッションデータをすべて再読み込みして、IDB に取り込むプロセス。これにより、メディア上のデータにすばやく、簡単にアクセスできるようになります。 メディアのエクスポート も参照。

<b>メディアのeksポート</b>	メディアに格納されているすべてのバックアップセッション情報(システム、オブジェクト、ファイル名など)をIDBから削除するプロセス。メディア自体に関する情報やメディアとプールの関係に関する情報もIDBから削除されます。メディア上のデータは影響されません。メディアのインポートも参照。
<b>メディアの種類</b>	メディアの物理的な種類(DDSやDLTなど)。
<b>メディアの状態</b>	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。
<b>メディアの使用法</b>	メディアの使用法は、既に使用されているメディアに対してバックアップをどのように追加するかを制御します。メディアの使用法は、[追加可能]、[追加不可能]、[増分のみ追加可能]のいずれかに設定できます。
<b>メディアのボールディング</b>	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。ボールディング手順は、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。
<b>メディアプール</b>	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。
<b>メディアラベル</b>	メディアに割り当てられるユーザー定義の識別子。
<b>メディア割り当てポリシー</b>	メディアをバックアップに使用する順序を決定します。[厳格]メディア割り当てポリシーでは、特定のメディアに限定されます。[緩和]ポリシーでは、任意の適切なメディアを使用できます。[フォーマットされていないメディアを先に割り当てる]ポリシーでは、ライブラリ内に利用可能な非保護メディアがある場合でも、不明なメディアが優先されます。

や

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

ゆ

<b>ユーザーアカウント(Data Protectorユーザーアカウント)</b>	Data Protector およびバックアップデータに対する無許可のアクセスを制限するために、Data Protector ユーザーとして許可を受けたユーザーにしか Data Protector を使用できないようになっています。Data Protector 管理者がこのアカウントを作成するときには、ユーザーログオン名、ユーザーのログオン元として有効なシステム、および Data Protector ユーザーグループのメンバーシップを指定します。ユーザーが Data Protector のユーザーインター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。
<b>ユーザーアカウント制御(UAC)</b>	Windows Vista、Windows 7 および Windows Server 2008 のセキュリティコンポーネント。管理者が権限レベルを上げるまで、アプリケーションソフトウェアを標準のユーザー権限に限定します。
<b>ユーザーグループ</b>	各 Data Protector ユーザーは、ユーザーグループのメンバーです。各ユーザーグループにはユーザー権限のセットがあり、それらの権限がユーザーグループ内のすべてのユーザーに付与されます。ユーザー権限を関連付けるユーザーグループの数は、必要に応じて定義できます。Data Protector には、デフォルトで admin、operator、user という 3 つのユーザーグループが用意されています。
<b>ユーザー権限</b>	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。
<b>ユーザーディスク割り当て</b>	NTFS の容量管理サポートを使用すると、共有ストレージボリュームに対して、拡張された追跡メカニズムの使用およびディスク容量に対する制御が行えるようになります。Data Protector では、システム全体にわたるユーザーディスク割り当てが、すべてのユーザーに対して一度にバックアップされます。
<b>ユーザープロファイル</b>	<b>(Windows 固有の用語)</b> ユーザー別に維持される構成情報。この情報には、デスクトップ設定、画面表示色、ネットワーク接続などが含まれます。ユーザーがログオンすると、そのユーザーのプロファイルがロードされ、Windows 環境がそれに応じて設定されます。

## ら

**ライター** (Microsoft VSS 固有の用語) オリジナルボリューム上のデータの変更を開始するプロセス。主に、永続的なデータをボリューム上に書き込むアプリケーションまたはシステムサービスがライターとなります。ライターは、シャドウコピーの同期化プロセスにも参加し、データの整合性を保証します。

**ライブラリ** オートチェンジャー、ジュークボックス、オートローダ、またはエクステンジャとも呼ばれます。ライブラリには、複数のレポジトリスロットがあり、それらにメディアが格納されます。各スロットがメディア (DDS/DAT など) を 1 つずつ格納します。スロット/ドライブ間でのメディアの移動は、ロボット機構によって制御され、メディアへのランダムアクセスが可能です。ライブラリには、複数のドライブを格納できます。

## り

**リカバリカタログ** (Oracle 固有の用語) Recovery Manager が Oracle データベースについての情報を格納するために使用する Oracle の表とビューのセット。この情報は、Recovery Manager が Oracle データベースのバックアップ、復元、および復旧を管理するために使用されます。リカバリカタログには、以下の情報が含まれます。

- Oracle ターゲットデータベースの物理スキーマ
- データファイルおよびアーカイブログのバックアップセット
- データファイルのコピー
- アーカイブ REDO ログ
- ストアドスクリプト

**リカバリカタログデータベース** (Oracle 固有の用語) リカバリカタログスキーマを格納する Oracle データベース。リカバリカタログはターゲットデータベースに保存しないでください。

### リカバリカタログデータベースへのログイン情報

(Oracle 固有の用語) リカバリカタログデータベース (Oracle) へのログイン情報の形式は `user_name/password@service` で、ユーザー名、パスワード、サービス名の説明は、Oracle ターゲットデータベースへの Oracle SQL\*Net V2 ログイン情報と同じです。ただし、この場合の `service` は Oracle ターゲットデータベースではなく、リカバリカタログデータベースに対するサービス名となります。

ここで指定する Oracle ユーザーは、Oracle のリカバリカタログのオーナーでなければならぬことに注意してください。

**リカバリファイル** (Oracle 固有の用語) リカバリファイルはフラッシュリカバリ領域に存在する Oracle 固有のファイルで、現在の制御ファイル、オンライン REDO ログ、アーカイブ REDO ログ、フラッシュバックログ、制御ファイル自動バックアップ、データファイルコピー、およびバックアップピースがこれにあたります。フラッシュリカバリ領域 も参照。

**リサイクルまたは保護解除** メディア上のすべてのバックアップデータのデータ保護を解除して、以降のバックアップで上書きできるようにするプロセス。同じセッションに所属しているデータのうち、他のメディアに置かれているデータも保護解除されます。リサイクルを行っても、メディア上のデータ自体は変更されません。

**リムーバブル記憶域の管理データベース** (Windows 固有の用語) Windows サービスの 1 つ。リムーバブルメディア (テープやディスクなど) と記憶デバイス (ライブラリ) の管理に使用されます。リムーバブル記憶域により、複数のアプリケーションが同じメディアリソースを共有できます。

## ろ

**ローカル復旧とリモート復旧** リモート復旧は、SRD ファイルで指定されている Media Agent ホストがすべてアクセス可能な場合にのみ実行されます。いずれかのホストがアクセス不能になっていると、ディザスタリカバリプロセスがローカルモードにフェイルオーバーされます。これは、ターゲットシステムにローカルに接続しているデバイスが検索されることを意味します。デバイスが 1 台しか見つからない場合は、そのデバイスが自動的に使用されます。複数のデバイスが見つかった場合は、デバイスが選択できるプロンプトが表示され、ユーザーが選択したデバイスが復元に使用されます。

<b>ローカル連続レプリケーション</b>	<p><b>(Microsoft Exchange Server 固有の用語)</b> ローカル連続レプリケーション (LCR) はストレージグループの完全コピー (LCR コピー) を作成および維持するシングルサーバー ソリューション。LCR コピーは元のストレージグループと同じサーバーに配置されます。LCR コピーが作成されると、変更伝播 (ログリプレイ) テクノロジーで最新に保たれます。LCR の複製機能では未複製のログが削除されません。この動作の影響により、ログを削除するモードでバックアップを実行しても、コピー中のログと複製に十分な余裕がある場合、実際にはディスクの空き容量が解放されない場合があります。</p> <p>LCR コピーへの切り替えは数秒で完了するため、LCR コピーはディザスタリカバリに使用されます。元のデータとは異なるディスクに存在する LCR コピーをバックアップに使用すると、プロダクションデータベースの入出力の負荷が最小になります。</p> <p>複製されたストレージグループは、Exchange ライターの新しいインスタンス (Exchange Replication Service) として表示され、通常のストレージグループのように VSS を使用してバックアップできます。</p> <p>クラスター連続レプリケーションおよび Exchange Replication Service も参照。</p>
<b>ロギングレベル</b>	<p>ロギングレベルは、バックアップ、オブジェクトのコピー、またはオブジェクトの集約時にファイルとディレクトリに関する情報をどの程度まで詳細に IDB に記録するかを示します。バックアップ時のロギングレベルに関係なく、データの復元は常に可能です。Data Protector には、[すべてログに記録]、[ディレクトリレベルまでログに記録]、[ファイルレベルまでログに記録]、および [記録しない] の 4 つのロギングレベルがあります。ロギングレベル設定によって、IDB のサイズ増加、バックアップ速度、および復元データのブラウザのしやすさが影響を受けます。</p>
<b>ログイン ID</b>	<p><b>(Microsoft SQL Server 固有の用語)</b>Microsoft SQL Server にログインするためにユーザーが使用する名前。Microsoft SQL Server の syslogin システムテーブル内のエントリに対応するログイン ID が有効なログイン ID となります。</p>
<b>ロック名</b>	<p>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。</p>
<b>論理演算子</b>	<p>Data Protector ヘルプシステムの全文検索には、AND、OR、NOT、NEAR の各ブール演算子を使用できます。複数の検索条件をブール演算子で組み合わせて指定することで、検索対象をより正確に絞り込むことができます。複数単語の検索に演算子を指定しなければ、AND を指定したものとみなされます。たとえば、「マニュアルディザスタリカバリ」という検索条件は、「マニュアル AND ディザスタ AND リカバリ」と同じ結果になります。</p>
<b>論理ログファイル</b>	<p>論理ログファイルは、オンラインデータベースバックアップの場合に使用されます。変更されたデータがディスクにフラッシュされる前に書き込まれるファイルです。障害発生時には、これらの論理ログファイルを使用することで、コミット済みのトランザクションをすべてロールフォワードするとともに、コミットされていないトランザクションをロールバックすることができます。</p>
<b>わ</b>	
<b>ワイルドカード文字</b>	<p>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。</p>

# 索引

## A

ASR, 20, 60

## B

BitLocker ドライブ暗号化, 76

## C

Cell Manager

手動によるディザスタリカバリ、Linux, 101

手動によるディザスタリカバリ、UNIX, 89

手動によるディザスタリカバリ、Windows, 70

ワンボタンディザスタリカバリ、Linux, 96

ワンボタンディザスタリカバリ、Windows, 48

## D

Data Protector 統合ソフトウェアとディザスタリカバリ,  
21

DR OS, 16

drm.cfg ファイル, 109

drm.cfg ファイル

enable\_disshw オプション, 122

## E

EADR, 35, 90

## H

HP

テクニカルサポート, 14

## I

Itanium 固有の問題

トラブルシューティング, 116

## L

Linux

拡張自動ディザスタリカバリ、クライアント, 90

ワンボタンディザスタリカバリ, 96

ワンボタンディザスタリカバリ、Cell Manager, 96

Linux システム

トラブルシューティング, 117

## O

OBDR, 20, 48, 96

omnisrupdate

実行後スクリプト, 24

スタンドアロン, 24

OS パーティション

拡張ディザスタリカバリ, 21

ディスクデリバリーによるディザスタリカバリ, 32

## S

SRD ファイルの更新、ウィザード, 24

## U

UNIX Cell Manager

手動によるディザスタリカバリ, 88

復旧手順, 89

UNIX クライアント

ディスクデリバリーによるディザスタリカバリ, 83

## W

Web サイト

HP, 15

HP メールニュース配信登録, 15

製品マニュアル, 8

Windows

ASR, 60

BitLocker ドライブ暗号化, 76

拡張自動ディザスタリカバリ、クライアント, 35

自動システム復旧セット, 62

手動によるディザスタリカバリ、Cell Manager, 27

ディザスタリカバリのトラブルシューティング, 106

ディスクデリバリーによるディザスタリカバリ、クラ  
イアント, 32

半自動ディザスタリカバリ, 27

半自動ディザスタリカバリ、クライアント, 27

ワンボタンディザスタリカバリ, 48

ワンボタンディザスタリカバリ、Cell Manager, 48

## あ

暗号化キー

準備, 41, 93

暗号化されたバックアップ

準備, 23

## お

オリジナルシステム, 16

## か

概念, 16

概要

異なるハードウェアの復旧, 121

ディザスタリカバリ, 16

ディザスタリカバリの方法, 18

半自動ディザスタリカバリ、Windows, 27

拡張自動ディザスタリカバリ, 35, 90

DR OS イメージファイル, 21, 35, 90

DR イメージ, 39, 92

概要、Linux クライアント, 90

概要、Windows クライアント, 35

クライアント, 35, 90

異なるハードウェア, 121

準備、Linux クライアント, 92

準備、Windows クライアント, 38

制限事項、Linux クライアント, 91

制限事項、Windows クライアント, 38

ディザスタリカバリ CD, 42, 94

ディザスタリカバリ CD ISO イメージ, 21, 41, 94

手順、Linux クライアント, 94

手順、Windows クライアント, 43

必要条件、Windows クライアント, 36

フェーズ 1 開始ファイル (P1S), 41, 93  
要件、Linux クライアント, 91  
拡張ディザスタリカバリ  
概要, 21  
トラブルシューティング、Windows, 113  
復旧対象のパーティション, 21  
関連ドキュメント, 8

き  
規則  
表記, 13

く  
クライアント  
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, 83  
半自動ディザスタリカバリ、Windows, 27  
ワンボタンディザスタリカバリ、Linux, 96  
ワンボタンディザスタリカバリ、Windows, 48  
クリティカルボリューム, 16

け  
計画  
ディザスタリカバリ, 22

こ  
異なるハードウェアの復旧, 121  
OS の準備, 124  
OS の復元, 124  
概要, 121  
システムの復元, 124  
準備, 123  
制限事項, 122  
データの復元, 125  
ネットワークマッピング, 125  
必要なドライバ, 123  
要件, 122  
リカバリモード, 124  
異なるハードウェアの復旧でのネットワークマッピング,  
125  
異なるハードウェアの復旧に必要なドライバ, 123

さ  
作成  
整合性と関連性を兼ね備えたバックアップ, 23  
バックアップ仕様, 86  
補助ディスク, 86

し  
システム固有のディザスタリカバリの方法, 19  
システム固有の方法, 19  
システムパーティション, 16  
システム復旧データ (SRD), 24  
システム復旧データ (SRD) の更新, 24  
自動システム復旧, 60  
ASR セット, 62  
ASR ディスク, 63  
準備, 62  
制限事項, 61

復旧, 64  
要件, 61  
自動システム復旧セット, 62  
手動によるディザスタリカバリ, 19  
Cell Manager、Linux, 101  
Cell Manager、UNIX, 88  
Cell Manager、Windows, 70  
準備、UNIX Cell Manager, 89  
制限事項、UNIX Cell Manager, 89  
手順、UNIX Cell Manager, 89  
準備  
暗号化キー, 41, 93  
暗号化されたバックアップ, 23  
拡張自動ディザスタリカバリ、Linux クライアント,  
92  
拡張自動ディザスタリカバリ、Windows クライアント,  
38  
異なるハードウェアの復旧, 123  
自動システム復旧, 62  
手動によるディザスタリカバリ、UNIX Cell Manager,  
89  
ディザスタリカバリ用, 22  
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, 84  
ディスクデリバリーによるディザスタリカバリ、  
Windows クライアント, 33  
半自動ディザスタリカバリ、Windows, 28  
ワンボタンディザスタリカバリ、Linux クライアント,  
98  
ワンボタンディザスタリカバリ、Windows クライ  
アント, 50  
障害, 16

せ  
制限事項  
拡張自動ディザスタリカバリ、Linux クライアント,  
91  
拡張自動ディザスタリカバリ、Windows クライアント,  
38  
異なるハードウェアの復旧, 122  
手動によるディザスタリカバリ、UNIX Cell Manager,  
89  
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, 84  
半自動ディザスタリカバリ、Windows, 28  
ワンボタンディザスタリカバリ, 33  
ワンボタンディザスタリカバリ、Linux クライアント,  
98  
ワンボタンディザスタリカバリ、Windows クライ  
アント, 50

た  
ターゲットシステム, 16  
ダーティフラグ, 23  
対象読者, 8

て  
ディザスタリカバリ  
準備, 22

ディザスタリカバリ CD ISO イメージ, 35, 90  
ディザスタリカバリオペレーティングシステム (DR OS),  
16  
ディザスタリカバリセッション  
デバッグ, 107  
ディザスタリカバリの準備, 22  
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、UNIX Cell Manager,  
88  
ディザスタリカバリの方法の一覧, 18  
ディザスタリカバリプロセスの概要  
準備, 22  
復旧, 22  
プラン, 22  
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, 83  
概要, 20  
クライアント、Windows, 32  
準備、UNIX クライアント, 84  
準備、Windows クライアント, 33  
制限事項、UNIX クライアント, 84  
手順、UNIX クライアント, 87  
手順、Windows クライアント, 34  
トラブルシューティング、Windows, 112  
復旧対象のパーティション, 32  
補助ディスク, 84  
テクニカルサポート  
HP, 14  
サービスロケータ Web サイト, 15  
デバッグ  
ディザスタリカバリセッション, 107

と  
統合ソフトウェアとディザスタリカバリ, 21  
ドキュメント  
HP Web サイト, 8  
関連ドキュメント, 8  
トラブルシューティング  
Itanium 固有の問題, 116  
Linux システム, 117  
Windows 上でのディザスタリカバリ, 106  
拡張ディザスタリカバリ、Windows, 113  
ディザスタリカバリ後のログオン, 110  
ディスクデリバリーによるディザスタリカバリ、  
Windows, 112

は  
ハードウェア、異なるハードウェアへの復旧, 121  
バックアップ  
整合性のある ~ の作成, 23  
バックアップ仕様  
ディザスタリカバリ用に作成, 86  
半自動ディザスタリカバリ  
drsetup ディスク, 29  
Windows システム, 27  
概要、Windows, 27  
準備、Windows, 28  
制限事項、Windows, 28  
手順、Windows, 30

必要条件、Windows, 27

ひ  
表記  
規則, 13

ふ  
ブート可能なインストール用 CD, 28  
ブートパーティション, 16  
拡張ディザスタリカバリ, 21  
ディスクデリバリーによるディザスタリカバリ, 32  
フェーズ, 17  
異なるハードウェアの復旧, 121  
フェーズ 0, 17  
フェーズ 1, 17  
フェーズ 2, 18  
フェーズ 3, 18  
復旧, 17  
Cell Manager、UNIX, 89  
異なるハードウェア, 121  
復旧手順, 89  
拡張自動ディザスタリカバリ、Linux クライアント,  
94  
拡張自動ディザスタリカバリ、Windows クライアン  
ト, 43  
異なるハードウェアの復旧, 124  
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, 87  
ディスクデリバリーによるディザスタリカバリ、  
Windows クライアント, 34  
半自動ディザスタリカバリ、Windows, 30  
ワンボタンディザスタリカバリ、Linux, 100  
ワンボタンディザスタリカバリ、Windows, 55

へ  
別のマシンへの移行, 121  
ヘルプ  
取得, 14

ほ  
方法  
~ の一覧, 18  
概要, 18  
拡張自動ディザスタリカバリ, 35, 90  
拡張ディザスタリカバリ, 21  
自動システム復旧, 20, 60  
手動によるディザスタリカバリ, 19  
手動によるディザスタリカバリ、Windows, 27  
ディスクデリバリー, 32, 83  
ディスクデリバリーによるディザスタリカバリ, 20  
ワンボタンディザスタリカバリ, 20, 48, 96  
補助ディスク, 84  
作成, 86  
ホストシステム, 16

め  
メールニュース配信登録、HP, 15

## よ

### 要件

- 拡張自動ディザスタリカバリ、Linux クライアント,  
91
- 拡張自動ディザスタリカバリ、Windows クライアント,  
36
- 異なるハードウェアの復旧, 122
- 半自動ディザスタリカバリ、Windows, 27

## ろ

### ログオン

- ディザスタリカバリ後の問題, 110

## わ

### ワンボタンディザスタリカバリ, 20

- Linux システム, 96
  - Windows システム, 48
  - 概要, 33
  - 準備、Linux クライアント, 98
  - 準備、Windows クライアント, 50
  - 制限事項, 33
  - 制限事項、Linux クライアント, 98
  - 制限事項、Windows クライアント, 50
- ### ワンボタンディザスタリカバリ (OBDR)
- 手順、Linux, 100
  - 手順、Windows, 55