

## Intelligent Disaster Recovery

### **VERITAS Backup Exec™ 9.1 *for Windows Servers***

Intelligent Disaster Recovery™ オプション

## 目次

はじめに.....	3
ソリューション: ポイントインタイム ディザスタ リカバリ.....	3
比較:.....	4
手作業によるディザスタ リカバリ プロセスの短所.....	4
手作業によるディザスタ リカバリは人為的ミスの温床.....	4
手作業によるディザスタ リカバリは長時間の格闘.....	4
手作業によるディザスタ リカバリには難しい技術が必要.....	4
Intelligent Disaster Recovery によるプロセスの自動化と統合.....	5
ディザスタ リカバリ自動化の仕組み.....	5
1. ディザスタ リカバリ ファイルの作成.....	5
2. フルバックアップの実行.....	6
3. ディザスタ リカバリ メディアの準備.....	6
4. Windows システムのリカバリ.....	6
異なる Windows オペレーティングシステムにおける.....	7
Intelligent Disaster Recovery の違い.....	7
Windows 2000.....	7
Windows XP および Windows Server 2003.....	7
Backup Exec のオプションとエージェントのサポート.....	7
Intelligent Disaster Recovery オプション利用上の要件.....	8
Intelligent Disaster Recovery オプションのライセンス形態.....	8
1. IDR オプションライセンス.....	8
2. IDR オプション追加クライアント ライセンス (CAL).....	8
まとめ.....	9

©Copyright 2003 VERITAS Software Corporation. All rights reserved. VERITAS, VERITAS SOFTWARE, VERITAS ロゴ、およびその他の VERITAS 製品は、米国および各国の VERITAS Software Corporation の商標または登録商標です。その他の会社名、製品名等は、それぞれ各社の商標または登録商標です。製品の仕様・性能等は予告なく変更する場合がありますので、ご了承ください。

VERITAS Backup Exec™ 9.1 for Windows Servers Intelligent Disaster Recovery™ オプションは VERITAS Backup Exec 9.1 for Windows Servers に追加してご利用いただく有料オプションとして、別ライセンスにより提供させていただきます。Intelligent Disaster Recovery(以下 IDR)オプションをご利用いただくと、システムクラッシュ時にオペレーティングシステム全体を手動で再インストールせずに済むようになります。起動可能なメディアの使用により、IDR オプションは、最後に作成されたフル、差分、増分バックアップ、ワーキングセット バックアップ、修正ファイルのバックアップを基にデータファイルをリストアすることによって迅速なリカバリを実現します。

## はじめに

人為的ミス、ハードウェア障害、あるいは大規模なディザスタによってネットワーク サーバーに障害が発生した場合、アプリケーションやバックアップデータをリストアする前に、システムそのものを慎重にリカバリする必要があります。ディザスタ リカバリ テクノロジは、バックアップとリストアを補完する意味で戦略的に重要です。バックアップとリストアの最大の目的がアプリケーションとデータをリストアすることであるのに対して、ディザスタ リカバリはコンピューティング環境そのものを元に戻すことを目的としています。一方バックアップとリストアは、データリカバリを支えるコンピューティング環境が存在することを前提としています。ディザスタ リカバリはコンピューティング環境を使用可能な状態に戻し、さらにネットワークシステム全機能がリカバリに要する時間を最小限に抑えます。

ディザスタ リカバリは自動的に実行するテクノロジーが開発される以前は手作業により行われていました。この作業は労働集約的で、人為的ミスが発生しやすい長時間の作業のため、収益と生産性の損失につながります。さらに手作業では、準備不足、設定理由の説明不足、作業を正常に完了できない不適切な作業手順の制定などの原因から失敗することも珍しくありません。オペレーティングシステムの更新が相次ぐ中、オペレーティングシステムとビジネスの基幹データを安全にリカバリする環境を確保するため、安定した自動プロセスへのニーズがますます高まっています。

### ソリューション: ポイントインタイム ディザスタ リカバリ

ベリタスソフトウェアは Microsoft Windows ネットワーク向けアプリケーション開発における数々の経験を積んできました。これを基にしたディザスタ発生対策として、すべての種類のデータとシステム情報に対するポイントインタイム リカバリのプロセスを簡素化するとともに、その自動化に成功しました。IDR オプションをご利用いただくと、Microsoft Exchange Server や SQL Serverなどを運用するネットワーク サーバーやアプリケーション サーバーを素早く簡単に、最新のバックアップ時点までリカバリすることができます。オペレーティングシステムの設定、ユーザープロファイル、アプリケーション、そしてデータファイルのすべてを寸分違わずリカバリします。

IDR がユニークなのは、リカバリに利用できるバックアップがフルバックアップに限らないことです。増分、差分、ワーキングセットからもリカバリ可能であり、ここが他のディザスタ リカバリ製品と異なる点です。結果として、ディザスタが発生したローカルシステム、リモート システム、さらにデータファイルは、他の製品と比較してより元の状態に近い姿でリカバリします。さらにリカバリまでの時間も短縮されます。

IDR はその他にも、リカバリ中にシステム設定を変更する簡単で柔軟な手段を提供します。これにより、耐障害性ディスク ミラーリングやディスクボリュームなどの設定のカスタマイズにも対応することができます。Backup Exec そのものにも、ディザスタ リカバリの進行中にハードウェア変更を処理するという独自の機能が備わっています。Backup Exec では、ハード ドライブやアダプタなどのハードウェアを障害発生前と同一構成にせずとも IDR の処理が可能です。IDR は新規のハードディスク情報、RAID 構成、ネットワーク構成カードを指定できる唯一のディザスタ リカバリ ソリューションです。

IDR は 単一の Windows 環境のみならず、複数の種類の Windows が混在した環境の両方で理想的に機能します。リカバリできるサーバーは多種に及びます。Windows NT 4.0 (Service Pack 6a 以上) Enterprise Server、Small Business Server (NT 4 のみ)、Terminal Server および Workstation 版、Windows 2000 Professional、Server、Advanced Server、Datacenter の各 Edition および Windows Server 2003 のリカバリ可能です。IDR を利用すると、ネットワーク サーバーを最後の増分、差分、ワーキングセットを作成した時点まで迅速にリカバリできるため、データの整合性が向上し、システム全体の信頼性が高まり総所有コストを削減できます。

ここでははじめに、手作業によるディザスタ リカバリ プロセスに対して自動化され統合されたプロセスを備えた(すなわち intelligent な)ディザスタ リカバリ手法を比較し、手作業の欠点について明らかにします。次に IDR オプションを利用してディザスタに備える手順、およびディザスタからリカバリする手順をご紹介します。

## 比較:

### 手作業によるディザスタリカバリプロセス対 Intelligent Disaster Recovery

#### 手作業によるディザスタリカバリプロセスの短所

手作業によるディザスタリカバリには大きく分けて 3 つの短所があります。まず、手作業によるディザスタリカバリでは常に人為的ミスにさらされていることが挙げられます。次に、自動化された統合ソリューションが存在しないと、予備知識のないユーザーや管理者は障害の発生したシステムを復活させるために、長時間で忍耐を必要とする作業の連続に直面します。ユーザー、システム管理者、コンサルタントなどは、初めにネットワーク サーバーそのもののリカバリに貴重な多くの時間を費やし、次にリストアを実施する必要があるため、生産性に悪影響を与えます。第 3 に、ディザスタリカバリを手作業で実施する方法は技術的に複雑であることです。

#### 手作業によるディザスタリカバリは人為的ミスの温床

手作業はすべて人為的ミスの危険にさらされています。ディザスタリカバリを実施する過程で落とし穴にはまると、手間のかかるプロセスが増大する可能性があります。手順を誤るとそれまでの作業がすべて無駄になり、ユーザー、システム管理者、コンサルタントはそれまで以上に長時間の作業を強いられることとなります。

たとえば、バックアップテープをリストアする最後の段階になっても、管理者がハードディスクを誤って再パーティション化していたことに気づいていないこともあります。この後で直面するのはリストア中に発生するデータ エラーやアプリケーションのクラッシュとなります。この場合、ドライブを正しくパーティション化し最初からこの処理全体を繰り返すしかありません。また、データのリストアを完了するまで、使用するバックアップテープを取り違えたことに気づかないこともあります。最悪の場合、バックアップを更新していなかったためにデータの再入力が必要となります。

#### 手作業によるディザスタリカバリは長時間の格闘

これまで検討したように、ディザスタリカバリのプロセスは複雑で難解であり、常に予期しない結果が生じる危険性にさらされています。さらに大きな問題は、リカバリおよび(または)リストアのプロセスではサーバーが使用できないことです。障害が発生したサーバーがミッションクリティカルなサーバーで、組織が日常に必要とするビジネス アプリケーションを運用している場合、ビジネスおよび企業収益に重大な影響を与える可能性があります。当然、サーバーを利用する個々の社員の生産性にも影響があります。仮に障害の影響が 1 台のワークステーションにしか及ばなかった場合でも、そのユーザーのみでなくビジネスの生産性に大きな衝撃を与える可能性があります。

#### 手作業によるディザスタリカバリには難しい技術が必要

手作業によるディザスタリカバリは複雑な作業です。一連の手順を手作業で行うため、何時間もかかる場合があります。

- 故障したハードディスクや設備の修理または交換
- クリティカルなシステム設定情報(文書化されていると仮定して)およびリカバリ メディアの収集
- 手作業によるハードディスクの再パーティション化およびフォーマット
- 手作業によるオペレーティングシステムの再インストール
- 手作業によるアップデート、ドライバ、プロファイルなどの再インストール
- 手作業によるバックアップ アプリケーションの再インストール
- 最新のバックアップテープの特定および検出
- バックアップテープの再カタログ化
- バックアップテープのデータファイルおよびアプリケーションのリストア

どの段階でもミスが存在するとシステムのリカバリは妨げられ、管理者は最初から手作業で処理を繰り返す必要があります。

## Intelligent Disaster Recovery によるプロセスの自動化と統合

ベリタスソフトウェアは IDR の開発にあたって、それまでになかったことを試みました。ディザスタ リカバリ機能を自動化し、Backup Exec のバックアップとリストア機能と統合することです。Backup Exec との統合によりいっそう自動化が進んだソリューションが可能になり、ローカルおよびリモートのいずれの Windows サーバーにおいても簡単に短時間のリカバリを実現しました。オペレーティングシステムの設定、ユーザープロファイル、アップデートの適用、アプリケーションそしてデータファイルはすべて元に戻り、障害が発生したシステムは完全にリカバリします。

IDR は高度に自動化されているため、人間の介入を最小限にとどめ、結果として人為的ミスが発生する可能性を最小化します。さらにはリカバリとバックアップを統合し、次のソリューションを自動化して提供します。

- 通常は別個の 2 つのプロセスを統合することでシステム管理の負担を軽減
- システムリカバリのプロセス管理と実行を自動化する結果、ダウンタイムを最小化
- 個人の生産性と業務全体に与える影響を低減
- TCO の削減
- ディザスタ リカバリの高度で複雑な技術手順を簡素化

前述の手作業とは異なり、IDR ではネットワークの設定、ボリューム パーティションの大きさ、ユーザープロファイルなどの詳細をシステム管理者が把握している必要はありません。すべての設定データがバックアップ機能により自動的に保護されているため、ディザスタ リカバリ エンジンが必要な場面でこれを利用できます。IDR により人間の介入を排除する結果、障害が発生したシステムの正確なリカバリが実現します。

## ディザスタ リカバリ自動化の仕組み

IDR オプションは Microsoft Windows オペレーティングシステム向けとして開発されました。Windows 環境の保護には独特の問題が存在しています。これについては「異なる Windows オペレーティングシステムにおける Intelligent Disaster Recovery の違い」の項で検討します。

IDR オプションをインストールした後、最初に Backup Exec を起動した際に IDR 構成ウィザードが現れます。このウィザードでは、管理者を体系的にガイドすることによってディザスタ リカバリの準備作業を行い、ローカルまたはリモートの Windows システムをディザスタ発生前の状態にリカバリできます。IDR は 4 つの手順で構成されています。

1. コンピュータごとに対応して 1 つ作成されるディザスタ リカバリ ファイルを収容する場所の指定
2. 保護の対象となる Windows システム上に構成するハードドライブのフルバックアップ
3. IDR 準備ウィザードによる、起動可能メディアと各コンピュータ用のリカバリ ディスクの作成
4. IDR 障害回復ウィザードとリカバリ用メディアによる Windows システムのリカバリ

### 1. ディザスタ リカバリ ファイルの作成

最初の起動時に、ユーザーはウィザードに従ってコンピュータ固有のディザスタ リカバリ ファイル(\*.dr ファイルと呼びます)の代替パスの設定を行います。この時アスタリスク(\*)を使用すると、このファイルが作成された Windows システムを指定できます。\*.dr ファイルには保護の対象となるシステムに関して次のような情報が書き込まれます。

- 各コンピュータにおけるハードウェア関連の情報。ハードディスクのパーティション情報(Windows 2000 および NT のみ)、マス ストレージ コントローラに関する情報、ネットワーク インターフェイス カードに関する情報など。
- そのコンピュータのリカバリに使用するバックアップメディアを識別するカタログ エントリのリスト。
- Windows XP および Windows Server 2003 コンピュータの場合、Windows 自動システム回復(ASR)設定情報。ASR ファイルはリカバリを進める途中で Windows XP および Windows Server 2003 コンピュータ上のパーティションを再作成するのに必要です。

デフォルトでは \*.dr ファイルのデータパスはそのメディアサーバー上のハードドライブに設定されています。しかしメディアサーバーのハードドライブが障害を受けた場合を想定して、別に作成したコピーを格納する代替データパスを指定することが最適です。

## 2. フルバックアップの実行

\*.dr ファイルの代替格納場所を設定した後にハードドライブのフルバックアップを実行します。

## 3. ディザスタリカバリメディアの準備

IDR オプションをインストールする過程で、リカバリ エンジン、必要なオペレーティングシステム コンポーネントおよび設定データを記録した一連のディスク、CD、テープができあがります。これらのメディアはすべて、障害を起こしたシステムを起動し、自動化したディザスタ リカバリ プロセスを実行するために使用します。ユーザーは IDR 準備ウィザードに従い、保護するコンピュータをリカバリするための起動可能メディアの準備を行います。\*.dr ファイルとその他のリカバリ情報は IDR ディスクにコピーされます。IDR 準備ウィザードを利用して次の 3 種類の起動可能メディアを作成できます。

- ディスク (Windows XP および Windows Server 2003 はサポート対象外)
- CD-R (CD-Recordable) もしくは CD-RW (CD-Rewritable)
- 起動可能テープ (テープデバイスが起動可能な仕様である必要があります)

作成する起動可能メディアの種類を選択するにあたっては、保護する Windows コンピュータの種類、利用できるハードウェア、システム BIOS について検討しておきます。

\*.dr ファイルを別のメディアに組み合わせると更新が容易になります。

起動可能な CD-R、CD-RW もしくはテープを利用する場合でも、IDR 準備ウィザードを利用して \*.dr ファイルをディスクにバックアップすることができるため、必要に応じて簡単にアップデートできるようになります。

Backup Exec はフルバックアップの際に \*.dr ファイルを作成し、デフォルトおよび代替の格納場所に保存します。カタログ エントリはその次のバックアップの完了時に作成され、自動的に \*.dr ファイルに追加されます。

注: 起動可能テープ イメージの作成は、フルバックアップ実行の前に行ってください。

## 4. Windows システムのリカバリ

サーバーの障害発生に直面した際にシステム管理者やコンサルタントが最初に行うことは、障害を起こしたシステムやコンポーネントの修復または交換です。次にシステム アプリケーションとデータファイルを最後のバックアップ時点まで戻すため、Backup Exec のリストア機能と連動して IDR を使用します。リカバリしたサーバーは、オペレーティングシステムの設定、ユーザープロファイル、アップデートの適用、アプリケーション、データファイルが完全に同一のものになります。必要に応じて、耐障害性ディスク ミラーリングやパーティションのサイズ設定の変更が可能です。リカバリしたシステムは新しい構成で稼働します。

(注: どのような場合でも、システム構成を変更する前にシステム管理者にご相談いただくことをお勧めします)。

以上の 3 つの手順を終えた段階で、次のリカバリ方法のいずれかを使用してローカルまたはリモートシステムを正常にリカバリできるようになります。

- ローカルに接続したストレージデバイスによるメディアサーバー (Backup Exec サーバー) のリストア
- リストア対象の Windows コンピュータにメディアとストレージデバイスを移動した後にこのストレージデバイスをローカル接続して実行する、コンピュータのリストア
- メディアサーバーにネットワーク経由で接続して行うリモート Windows コンピュータのリストア

Windows システムのリカバリは、次のような独立した手順をいくつか組み合わせたものになります。

- パーティションの作成
- ボリュームの作成
- ボリュームのフォーマットによるファイルシステムの作成
- オペレーティングシステムのインストール
- システム上への元のデータファイルの再格納

Backup Exec では管理者が行うこのようなタスクを丁寧にガイドするとともに、自動的に処理します。

## 異なる Windows オペレーティングシステムにおける Intelligent Disaster Recovery の違い

IDR ソリューションの導入にあたっては、Windows オペレーティングシステムの種類ごとに留意しておくべき点があります。

### Windows 2000

Windows 2000 には同時にまとめてバックアップが必要な複数のコンポーネントが存在し、システム状態 (System State) として定義されています。システムのリカバリを実行するにはシステム状態のリストアが非常に重要です。最初にブート ファイルを交換し、プロセスの最後の手順としてレジストリのシステム ハイブをコミットする必要があります。Windows 2000 において、Backup Exec は次に挙げるシステム状態の完全なプロテクションを実現します。

- レジストリ
- COM+ クラス レジストレーション データベース
- ブート ファイルおよびシステムファイル
- Certificate Services データベース (認証サーバーとして利用している場合)
- Active Directory (サーバーがドメイン コントローラの場合)
- SYSVOL- システム ボリューム (サーバーがドメイン コントローラの場合)
- クラスタ クォーラム

システム状態のバックアップ処理とリストアは、どの Windows 2000 システムにとってもリカバリ成功の鍵となります。そのため、自動化されたディザスタ リカバリこそが、その複雑なプロセスを処理する理想的なソリューションとして、Windows の種類を問わずサーバーを完全にリカバリすることができます。

### Windows XP および Windows Server 2003

Windows XP および Windows Server 2003 システムは自動システムリカバリ (ASR) テクノロジーを搭載しています。これはオペレーティングシステムのディザスタ リカバリのために Microsoft により開発されたものです。ASR はベリタスソフトウェアのようなサードパーティ ベンダーが開発するリカバリ製品の機能を向上させるためのツールです。たとえば IDR オプションは、ASR を使用してディザスタ発生後の物理ストレージを元の状態に再設定します。ASR の提供する情報は次のとおりです。

- OS のバージョン
- タイムゾーン
- バス情報
- MBR のあるディスクおよびパーティション
- GUID パーティション テーブルのあるディスクおよびパーティション
- リカバリ コマンド
- リムーバブル メディア情報
- LDM ボリューム状態
- デバイス インスタンス
- クラス キー
- デバイス インスタンス ハッシュ値

## Backup Exec のオプションとエージェントのサポート

Backup Exec 9.1 for Windows Servers IDR オプションは、すべてのエージェントとオプションとともに使用することができます。

## Intelligent Disaster Recovery オプション利用上の要件

IDR オプションには次のような利用上の要件があります。

- VERITAS Backup Exec 9.1 *for Windows Servers*
- リモート コンピュータを IDR で保護する場合は、すべてのリモート コンピュータに VERITAS Backup Exec *for Windows Servers* Windows リモートエージェント(CAL) がインストールされている必要があります。
- Windows NT 4.0 (Service Pack 6a 以上) Enterprise Server、Small Business Server (NT 4 のみ)、Terminal Server および Workstation 版、Windows 2000 Professional、Server、Advanced Server、Datacenter の各 Edition および Windows Server 2003
- Windows NT のリカバリには、リカバリするデータを格納する十分なスペースに加えて、最小限のリカバリ システムを維持するために最低 40 MB のハードドライブ空き容量が必要です。1.8 GB のデータを保存する 2.0 GB のパーティションに必要となるハードドライブ空き容量は、1.8 GB に 128 MB と 40 MB を加えた合計、1.97 GB になります。
- Windows 2000/XP/Windows Server 2003 のリカバリには Windows 全体をインストールするために十分なハードドライブ空き容量 (600 MB ~ 2 GB) が必要です。

注: 仮想デバイスからのディザスタ リカバリには、仮想デバイスへのアクセスを行うメディアサーバーを利用して IDR オプション追加リモートエージェントのライセンスが必要です。

## Intelligent Disaster Recovery オプションのライセンス形態

IDR オプションには 2 種類のライセンスがあります。まず始めに、IDR を使用する最初の Backup Exec サーバー向けのライセンスが必要です。もう 1 種類のライセンスは IDR に必要となる各種の追加リソース向けのものです。

### 1. IDR オプションライセンス

このライセンスは、Backup Exec を運用しているサーバーに適用した場合にプライマリ IDR オプションライセンスとなります。もしくはネットワークに接続された 1 台のクライアントを保護する場合にもご利用いただけます。クライアントの保護を実施したい場合は、Windows リモートエージェント(CAL) をインストールする必要があります。

必要ライセンス: バックアップサーバー 1 台につき 1 ライセンス

### 2. IDR オプション追加クライアント ライセンス (CAL)

このオプションによりネットワーク上でリカバリするサーバーを追加できます。保護にあたっては、IDR ライセンスをインストールした Backup Exec サーバーが必要です。この機能は IDR オプションと同じですが、ディスカウント価格で入手できます。

必要ライセンス: 保護対象とするリモートサーバーもしくはワークステーション 1 台につき 1 ライセンス

必須条件: クライアントには Windows リモートエージェント(CAL) がインストールされている必要があります。また、Backup Exec サーバーには IDR オプションライセンス が必要です。

## まとめ

IDR オプションは日常バックアップ業務を補完する戦略的役割を担います。バックアップとリストア テクノロジーを組み合わせることで、ディザスタリカバリ プロセスの自動化と統合を実現します。IDR のメリットを次にまとめます。

- ポイントインタイム リカバリのみをローカルおよびリモート システムに行うことで実現したリカバリの最小化
- 自動化された段階的なウィザードシステムにより容易なりカバリプロセスを提供
- すべてのパーティション、レジストリ、設定情報など、Windows サーバーまたはワークステーションの種類を問わない完全なりカバリ
- Backup Exec との統合による、日常バックアップの一部としてのディザスタリカバリ情報のアップデート
- 同一ハードウェアまたは同一設定に限定されないリカバリの柔軟性

さらに大きなメリットとして、IDR をご利用いただくとディザスタに対する備えとリカバリは、次のような簡単な手順になります。

1. コンピュータごとに対応して 1 つ作成されるディザスタリカバリ ファイルを収容する場所の指定
2. 保護の対象となるコンピュータのハードドライブのフルバックアップ
3. IDR 準備ウィザードによる、起動可能メディアと各コンピュータ用のリカバリ ディスクレットの作成
4. IDR 障害回復ウィザードとリカバリ用メディアによるコンピュータのリカバリ

ベリタスソフトウェアは Windows システムとデータの保護を提供する世界的なリーダーとして、お客様の管理作業負荷およびビジネス用ネットワーク システムにおける総所有コストの削減を実現するため、今後も IDR の改善と発展を継続することをお約束いたします。

ベリタスソフトウェアの詳細な製品情報につきましては、弊社の Web サイト(<http://www.veritas.com/jp/>)をご覧ください。

© Copyright 2003 VERITAS Software Corporation. All rights reserved. VERITAS, VERITAS SOFTWARE, VERITAS ロゴ、およびその他の VERITAS 製品は、米国および各国の VERITAS Software Corporation の商標または登録商標です。その他の会社名、製品名等は、それぞれ各社の商標または登録商標です。製品の仕様、性能等は予告なく変更する場合がありますので、ご了承ください。

### ベリタスソフトウェア株式会社

〒100-0011 東京都千代田区内幸町 2 丁目 2 番 2 号 富国生命ビル  
TEL.03-5532-8241 FAX.03-5532-0887  
<http://www.veritas.com/jp>

お問い合わせ先