ホワイトペーパーシリーズ：

Arcserve® r16

『仮想環境の保護と可用性の向上』

2011 年 10 月

Arcserve Japan

---

arcserve

assured recovery

目次

はじめに

サーバの仮想化によって、IT コスト削減とサーバインフラの改善を実現している企業は増えています。一方で、仮想化には大規模な障害が発生する可能性もあります。仮想ホストのシステムやストレージに障害が発生すると壊滅的な被害となり、複数のシステムに同時に影響するリスクがあります。そのため、仮想環境を保護し、復旧の手段と可用性を確保することは非常に重要です。また、100%仮想環境に移行した企業は依然として少なく、大半が物理環境と仮想環境から構成される複合的な環境の保護と復旧が必要となっています。そのため、物理と仮想の両方の環境のニーズに対応できるソリューションが理想的といえます。

仮想サーバ環境では、災害復旧対策を柔軟かつ簡単に実装できます。適切なツールを使用すれば、仮想化環境のシステム、アプリケーション、そしてデータは、複数の物理サーバで構築するよりも短時間で復旧ができます。本書では、Arcserve®シリーズ製品で物理と仮想の混在環境のシステム、アプリケーション、データの保護、復旧および可用性の向上に関して説明します。

仮想サーバ保護の主な課題

バックアップの戦略には、適切な技術を使用して環境の課題に取り組むことが重要です。仮想サーバを保護するソリューションには、対応しなければならない課題がいくつかあります。それは、適切な保護レベルの選択、個別の復旧、大量のデータとバックアップ パフォーマンスの管理、そしてバックアッププロセスの大幅な自動化などです。

仮想環境において、復旧の目標に合せて適切な保護レベルを選択することは非常に重要です。

- **ホストベースのバックアップ：**仮想ホスト全体とそのホストで実行しているすべての仮想マシン（VM）は保護されますが、個々の VM や VM 上のアプリケーションとファイルの個別の復旧に対応していない可能性があります。
- **ゲストレベルのバックアップ：**個々の VM が保護され、VM のデータを個別に復旧できますが、アプリケーション固有の保護が行えない可能性があります。
- **アプリケーションレベルのバックアップ：**Microsoft® Exchange、Microsoft SharePoint®、Internet Information Services（IIS）など、VM 上で実行している個々のアプリケーションが保護されます。また、Exchange のメールボックスや個々のメッセージ、SharePoint のフォルダなど、アプリケーション固有のデータを個別に復旧できます。
- **レプリケーション：**定期的なバックアップとスナップショットの作成に必要なデータ、ファイル、データベースへの変更が複製されるため、障害による業務停止のリスクを排除できます。また、レプリケーションは遠隔地の災害復旧サイトに切り替えて実行できます。通常、データのリワインドや継続的データ保護（CDP）の機能が含まれているため、データが損失または破損する前の適切な時間に戻すことができます。

- **高可用性：**システムおよびアプリケーションの復旧時間が最も短く、システムとアプリケーションが監視され、自動的に他のサーバや仮想マシンにフェイルオーバされるため、予想外の障害を回避できます。

データとシステムを保護するエージェントをゲストにインストールして、ゲスト VM を物理サーバと同様に扱うだけでは、仮想環境を十分に保護することはできません。管理者はホストレベルのバックアップに加え、個別に復旧できるようにするために、従来のバックアップツールのすべての機能を駆使する必要があります。また、ホスト、ゲストおよびアプリケーションの保護を可能な限り簡略化するために、すべての VM にソフトウェアをインストールする必要のない**シングル パス バックアップ**のツールも必要です。さらに、同じ技術で物理と仮想の両方のサーバを保護できれば、同種と異種、仮想と物理など環境を問わず復旧を簡略化できます。

仮想サーバの保護戦略で重要なのは、個別でも復旧が可能な豊富な選択肢です。つまり、個々のファイルやフォルダはもちろん、Microsoft SharePoint のオブジェクト、Microsoft Exchange の電子メール、Microsoft SQL Server®のテーブルおよびすべての VM を個別に復旧するオプションです。

物理サーバであろうと仮想サーバであろうと、多くの企業では、電子メール、ファイルおよびデータベースのストレージはストレージ ディスクのコスト低下に伴って、ますます増え続けています。これらのデータは量が多い上に、同一のストレージ ボリューム内や異なるストレージ ボリューム間で多くのデータが複製されるため、大容量のストレージが必要です。現在では仮想サーバで大量のデータを処理することが一般化しているため、バックアップやレプリケーションを実行すると、復旧元と復旧先の両方のコンピュータ システムでパフォーマンスの問題が発生する可能性が高く、ネットワーク帯域幅も大量に消費されます。そのため、データ保護の実行時、特に、ディスク I/O の障害対応時にはパフォーマンスを管理して、システム パフォーマンスの低下を最小限に抑える必要があります。

仮想サーバ環境では、バックアップとシステム保護に加え、復旧プロセスも可能な限り自動化することが重要です。現在のバックアップ プロセスは、各マシンで異なる物理ハードウェアを使用していた頃に比べ、仮想インフラのリソースへの直接的な影響がはるかに大きくなっています。そのため、仮想環境におけるデータとシステムの保護への影響の防止、バックアップや復旧の自動化などの技術の使用、スナップショット ベースのバックアップと従来の長期保管が可能なバックアップの統合、そして、レプリケーションと高可用性を確保できるツールをバックアップ機能と組み合わせることが課題となっています。また、バックアップとシステムの保護技術によって低コストのスタンバイ システムをサポートし、必要に応じて自動フェイルオーバを実行することも重要です。

バックアップと復旧

バックアップと復旧はファイルやフォルダをはじめ、Exchange のメールボックス、SQL Server のデータベースなど、重要なデータとアプリケーションをサーバ環境全般で保護することを目的としています。仮想サーバの効果的なバックアップと復旧には、システム全体、または個々の VM やアプリケーションのバックアップ オプションのほか、ホストサーバ上のすべての VM の整合性あるバックアップをシングル パスで作成できる機能が必要です。VM に不具合が発生したり、

ホストサーバに致命的な障害が発生した場合、復旧技術によって、異なる仮想環境や異なる物理ハードウェアで構成されるホストサーバであっても迅速に復旧する必要があります。

Arcserve Backup r16

Arcserve® Backup は、データを安全にバックアップして長期保管できるだけでなく、ディザスタ リカバリツールを使用して、オペレーティングシステムやアプリケーション ソフトウェアを過去のバックアップの状態に復旧できます。バックアップ データはディスクやテープに加え、クラウド ストレージにも保存でき、段階的なバックアップによってデータも移行できます。たとえば、VM の定期的なバックアップをローカル ディスクに作成して、そのディスクのデータをテープやクラウドにオフサイトのストレージとしてコピーして長期間保存できます。

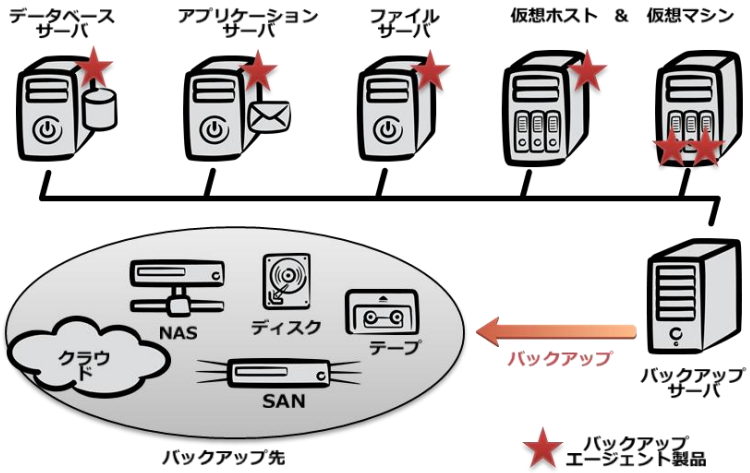
Arcserve Backup による仮想サーバのバックアップでは、以下の 2 つのレベルがサポートされます。

1. ホストサーバの保護によるすべての VM とその仮想ハードディスクの自動的な保護
2. 各 VM とアプリケーション固有のエージェントの使用による保護の強化、および VM とそのアプリケーションの個別の復旧

Arcserve Backup では一般的なアプリケーションエージェントに加え、Windows®、Linux®、UNIX®で実行している物理および仮想のエージェント製品も提供されています。そのため、同じバックアップ ポリシーを物理と仮想の両方の環境に使用できます。また、Arcserve Backup のエージェント製品を仮想ホストにインストールすると、Microsoft Hyper-V と VMware の環境で、ホスト レベルと VM レベルのバックアップを実行できます。個別に復旧する場合、エージェント製品は Hyper-V、VMware®、Citrix® XenServer プラットフォームの VM にインストールします。アプリケーションレベルの保護では、Agent for Microsoft Exchange Server、Agent for Microsoft SharePoint Server、Agent for Microsoft SQL Server、Agent for Oracle®* などの個々のエージェント製品をインストールして、メールボックスやデータベースの復旧など、アプリケーション固有の保護機能を利用できます。図 1 では、Arcserve Backup のエージェント製品による物理および仮想のリソースの保護を示しています。

＊ サポート条件については動作要件を参照してください。ゲスト OS 上で問題が発生した場合、物理環境上での問題再現が必要なケースがあります。

図 1. Arcserve Backup r16 によるバックアップ



Arcserve Backup は Microsoft Hyper-V、VMware vSphere および VMware vCenter Server のサーバの複数の VM を同時にバックアップできます。スナップショットを使用して、VM のパフォーマンスに影響を与えずにバックアップできます。 また、VM のバックアップは、VM の電源のオン/オフにかかわらず実行できます。

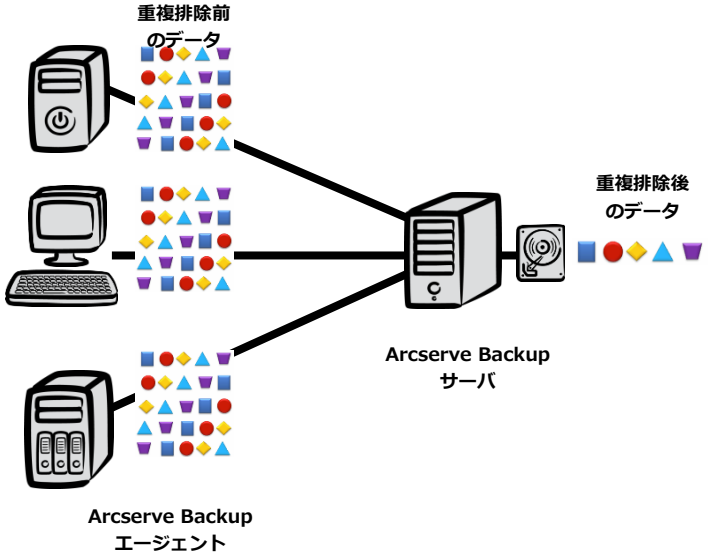
さらに、Arcserve Backup では、さまざまなオプションを使用して、個別に復旧が可能です。Arcserve Backup Agent for Virtual Machines Bundle では、Windows システム上の VM のバックアップや RAW バックアップ、あるいは VM のファイル レベルのバックアップを実行できます。VM 全体のバックアップを作成する場合、ファイルレベルで個別に復旧できる RAW バックアップが効果的です。RAW バックアップでもファイル レベルでの復旧が不要な場合、各 VM にエージェントをインストール必要はありません。Arcserve Backup Agent をインストールするだけで、VMware Consolidated Backup（VCB）、他のプロキシ コンピュータまたは Hyper-V のホストコンピュータの仮想マシンに対応できます。RAW バックアップでは、［仮想マシンのリカバリ］オプションを使用すると VM を完全に復旧できます。また、ファイルやフォルダを個別にリカバリする場合、［セッションによるリカバリ］オプションを使用してセッション番号を選択すると、選択したセッション内で VM ファイル（Hyper-V VM の場合、.vhd、.bin、.vsv ファイルなど）を確認できます。

Arcserve Backup エージェント製品を各 VM にインストールすると、個別の保護が強化され、すべてのバックアップや RAW バックアップからファイルとフォルダをリカバリする場合など、増分/差分バックアップを作成できます。個別の復旧に対応する場合、混在モードを使用すると、RAW バックアップとファイル レベルのバックアップを同じジョブに含めることができます。また、追加のエージェント製品を VM にインストールすると、Microsoft SharePoint、Microsoft SQL Server および Oracle をアプリケーションごとにバックアップすることができます。

Arcserve Backup のデータ重複排除機能では、重複するデータは排除されるため、ストレージの消費を抑制できます（図 2）。バックアップのプロセスでは重複するデータは無視され、一意のデータのみがその後のバックアップのために重複排除デバイスに保存されます。重複排除機能を使用すると、より多くのバックアップ データをストレージに長期間保存できます。重複排除機能を使用する場合、データ重複排除デバイス（DDD）にデータのバックアップを作成します。DDD には一意のデータのほかに参照ファイルとインデックスファイルが保存され、Arcserve Backup ではこれらのファ

イルを使用して、一意のデータ ブロックで構成されるファイルが管理されます。パフォーマンスを向上させるためには、データとインデックス ファイルは実際のデータとは異なるディスクに保存します。バックアップから重複排除したデータを復旧する場合、Arcserve Backup ではインデックス ファイルを使用して、元のデータ ストリームを組み替える前にデータ セグメントを認識します。

図 2. Arcserve Backup r16 の重複排除機能



Arcserve Backup のエージェント製品を導入すると、Arcserve Backup の **Infrastructure Visualization** のビューには、サーバ、ストレージなどのデバイスを含め、物理と仮想の環境全体をわかりやすく示したネットワーク図が表示されます。また、Arcserve Backup では VM の自動検出とバックアップ機能によって、仮想環境が拡張や変更されても、すべての VM のバックアップを確実に実行できます。自動検出機能は毎時間ごと（デフォルトは 24 時間ごと）の頻度で設定でき、自動的に新しい VM が検出されます。稼動中に移行する場合、たとえば、パフォーマンス上の理由、あるいは、ホストサーバ保守のための計画的なシステム ダウンではホスト間で VM を移動できますが、その場合でも VM のバックアップと保護は継続して実行することが重要です。

Arcserve Backup には、アンチウイルス機能が統合されています。そのため、バックアップ中にアンチウイルスのスキャンを実行して保護を強化し、バックアップがウイルスに感染するのを予防できます。ウイルス用のシグネチャは

Arcserve Backup ジョブ スケジューラ ウィザードを使用して自動で、またはコマンド ラインを使用して手動で更新できます。

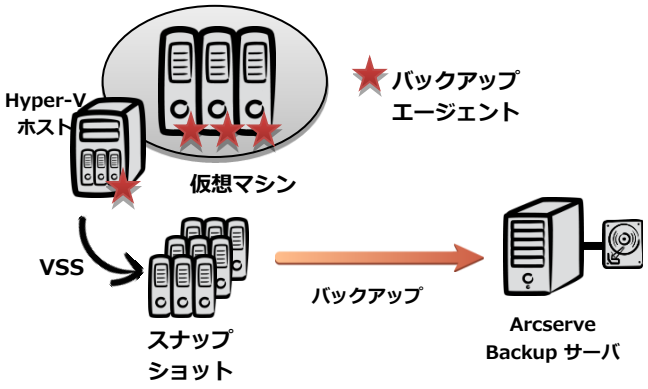
また、Arcserve Backup では VM 固有のツールが提供されているため、VM のバックアップを実行するときに仮想環境個別の違いを吸収できます。たとえば、vSphere 4.x、Hyper-V および VSS の統合技術をバックアップ プロセスに利用して、本番環境の VM へのバックアップの影響を最小化できます。Microsoft Hyper-V の場合、スクリプトの作成や設定をせずに、VM を Arcserve Backup マネージャ コンソールに表示できます。また、VMware の VM は VMware Virtual Disk Development Kit（VDDK）for VMware vSphere を利用して、Arcserve Backup マネージャ コンソールに統合できます。

Arcserve Backup による Hyper-V の保護

Arcserve Backup では、スタンドアロンの Microsoft Hyper-V Server 2008 および 2008 R2、または、Hyper-V を実行している Windows Server® 2008 および 2008 R2 の VM もサポートします。また、システム全体と Server Core のインストールもサポートします。

Arcserve Backup では VSS のスナップショットを使用して、稼動中の VM の特定の時点のバックアップをオンラインで実行できます。また、Hyper-V の VSS ライタを統合すると、稼動中の VM ではなく、その VM と同じデータを持つ VM のスナップショットからバックアップを実行できます。Arcserve Backup エージェント製品は、実行中の VM のスナップショットを VSS で作成してから、そのスナップショットでバックアップを作成するため、ゲスト VM に大きな影響はありません（図 3）。

図 3. Arcserve Backup r16 による Hyper-V の保護



VSS では、最後にシャドーコピーを作成した後の変更のみのシャドーコピーを作成できるため、わずかなボリューム サイズしか使用されません。それに対して、ハードウェアのスナップショットでは、ボリューム全体がコピーされます。ボリューム全体をコピーするため、ボリュームと同じディスク スペースが必要になります。また、Hyper-V では VSS ライタを使用しますので、シャドーコピーのバックアップ時に VM のバックアップの一貫性を維持できます。シャドーコピーを作成するときに、VSS ライタですべてのデータ バッファをフラッシュし、ボリュームへの書き込みを一時停止して、バックアップに指定したファイルの一貫した状態が確保されます。Windows の仮想化では、VSS のサポートは

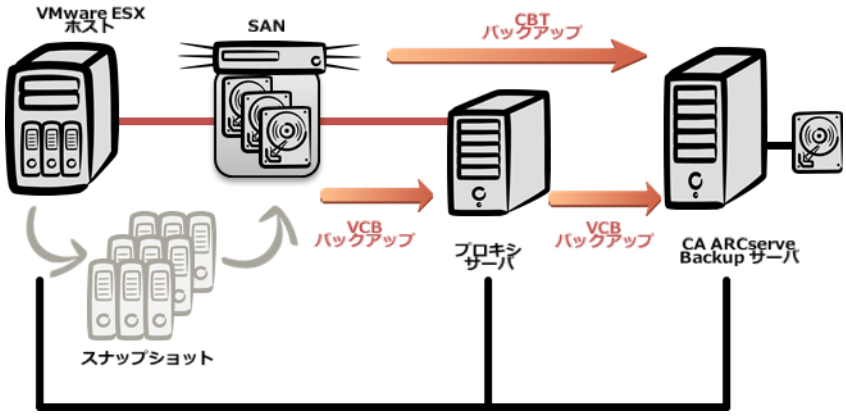
Microsoft Hyper-V の VSS ライタを通して提供されます。VSS ライタはアプリケーション ベンダが提供しサポートするため、VSS ライタのアップデートはアプリケーションのアップデートに含まれています。そのため、この技術を使用すると、新しいアプリケーションのバージョンがリリースされるたびに Arcserve Backup エージェント製品をアップデートしなくても、バックアップ データの一貫性が確保されます。Arcserve Backup では、Agent for Open Files および Enterprise Option for VSS Hardware Snap-Shot を通して VSS がサポートされます。Arcserve Backup VSS は、Agent for Open Files をインストールすると自動的にサポートされます。

Arcserve Backup による VMware の保護

Arcserve Backup は、VMware ESX Server 3.0 以上と vSphere 4.0 以上で実行している VM をサポートし、Microsoft Hyper-V 環境と同じ自動検出プロセスが使用されます。

VMware をそれ以前の VMware Virtual Infrastructure の ESX ホストで実行している場合、Arcserve Backup で VMware Consolidated Backup（VCB）の統合機能を使用して、VM のバックアップ作業を専用のバックアップ プロキシにオフロードし、このプロキシ システムから VM のスナップショットにアクセスしてバックアップを実行できます（図 2）。また、バックアップ プロキシ サーバによって定期的に VM のスナップショットが取得され、Arcserve Backup ではそのスナップショットを使用して、バックアップ プロキシからバックアップが作成されるため、ESX ホストには影響しません。

図 4. Arcserve Backup r16 による VMware の保護



VMware vSphere 環境の場合、Arcserve Backup では Changed Block Tracking（CBT）など、vSphere の統合機能（VDDK で提供）を使用してスナップショットのバックアップを迅速に実行できるため、バックアップ プロキシは必要ありません。CBT では VMware ESX 4.0 以上のホスト（仮想ハードウェアのバージョン 7 に設定）で実行している VM で、ディスク内の変更が追跡されます。これらの仮想ディスク ブロックの変更に関する情報は、ハイパーバイザ（VMkernel）で監視され、Arcserve Backup で VMware vStorage APIs for Data Protection を使用して、その情報にアクセスします（図 4）。Arcserve Backup では物理モードの Raw デバイス マッピングを除き、あらゆるデータ ストア タイプ（NFS と iSCSI）のあらゆる仮想ディスクに CBT を使用できます。

このような VMware vSphere の統合アプリケーション プログラミング インタフェース（API）を通して、Arcserve Backup では他の VMware 固有の機能（VM のバックアップ スケジュール設定による物理リソースとの競合の回避、VM からバックアップ デバイスへのデータの直接転送、バックアップから VM へのデータの直接保存など）を使用できます。また、Arcserve Backup r16 の統合機能によって VMware 環境のステージング サーバが不要になるだけでなく、バックアップ データを VMware のストレージ レベルで使用できます。

Arcserve D2D r16

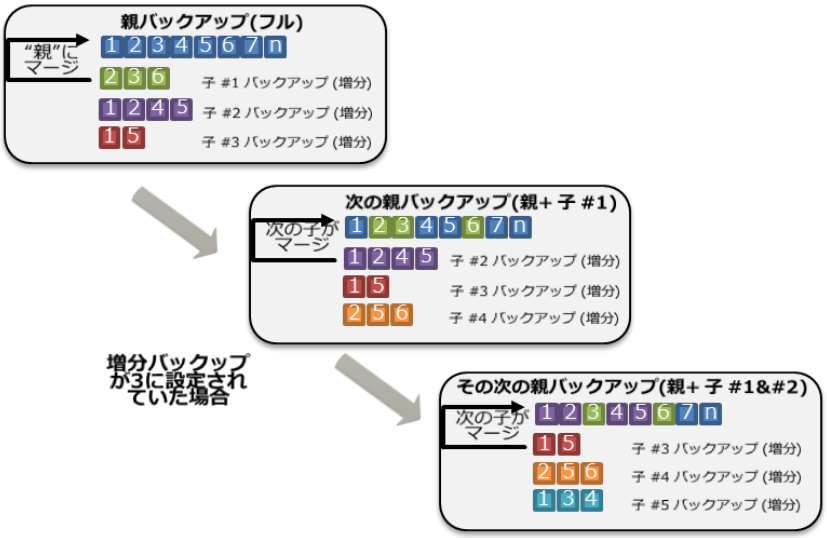
Arcserve® D2D では、Hyper-V または VMware ESX ホストで実行している Windows 仮想マシンがディスクベースで保護されます。データとシステムの情報は復旧ポイントとして保護され、ローカルまたは NAS（Network Attached Storage）ディスクや SAN（Storage Area Network）に保存したり、ファイルをオフプレミスのストレージに転送できます。また、復旧ポイントはクラウドのストレージにもコピーできます。Arcserve D2D では VM のスナップショットのバックアップと復旧機能を使用して、バックアップからファイル、ボリューム、データベース、電子メールおよび VM 全体を短時間で復旧できます。たとえば、Arcserve D2D r16 Advanced Edition を使用すると、Microsoft Exchange で VM を実行している場合、個別のメールボックスを自動的に復旧できます。また、Microsoft SQL Server で VM を実行している場合、個々のデータベースを復旧できます。

ファイルとフォルダの復旧をより簡単に操作するため、Arcserve D2D では Windows Explorer を統合できます。Arcserve D2D の復旧ポイントが含まれるフォルダを右クリックして、［ARCserve D2D ビュー］に変更すると、Windows Explorer にそのフォルダのすべての復旧ポイントのリストが表示されます。この統合機能を使用すると、復旧ポイントを簡単に表示することができます。また、その復旧ポイントの個々のファイルとフォルダを選択して手動でコピーすると、特定の復旧ポイントから迅速に個々のファイルを復旧できます。

Arcserve D2D では、ブロック レベルの継続的増分バックアップ（Infinite Incremental：I^2 technology）のスナップショットをすべてのバックアップに使用できます。そのため、バックアップに必要なストレージと CPU リソースが削減され、バックアップの時間も短縮できます。バックアップを開始すると、指定したボリュームが複数のデータブロックに分割され、バックアップが作成されます。最初のバックアップは「親バックアップ」として、ボリューム全体のフル バックアップが作成され、監視のベースラインのブロックになります。バックアップ前に VSS のスナップショットが作成され、その後、内部の監視ドライバによって各ブロックが検証されて、すべての変更が検出されます。それ以降のすべてのバックアップでは、このバックアップの後で変更されたブロックのみで構成される増分バックアップが作成されます。Arcserve D2D ではこのブロックレベルの増分バックアップ（「子バックアップ」）が 15 分ごとの頻度でスケジュールできるため、常に正確で最新のバックアップ イメージが提供されます。また、保存する子バックアップの増分数を指定することもできます。指定した数量を超えると、最も古い増分子バックアップが親バックアップにマージされ、「親と最も古い子供」のブロックで構成される新しいベースラインのイメージが作成され、フル　バックアップのイメージが作成されます（変更されていないブロックはそのままです）。最も古い子バックアップと親バックアップのマージは、後続のバックアップのたびに繰り返され、継続的増分バックアップ I（I^2）のスナップショットのバックアップを作成しても、

バックアップ イメージが保存（および監視）される数量は変わりません（図 5）。そのため、時間のかかるバックアップ後の VM のバックアップの統合は不要で、古いバックアップを削除して新しいバックアップのスペースを確保する必要もありません。ボリュームの情報を復元する場合、各ブロックの最新のバックアップを検出し、現在のブロックを使用してボリューム全体を再構築します。

図 5. 継続的増分バックアップ（I^2）のバックアップ



Arcserve D2D は、VSS ライタをサポートする Windows オペレーティングシステムとの連携が可能です。これには、Windows Server 2003 Service Pack 1（SP1）およびそれ以降の Windows Server オペレーティングシステム、Windows® XP およびそれ以降の Windows デスクトップのオペレーティングシステムが含まれます。

Arcserve D2D では、**バックアップ スピードのスロットリング**機能が標準で装備されています。この機能を使用すると、バックアップを実行する速度（MB/分）を指定して、CPU やネットワークの利用を削減できます。そのためには、測定によってスロットリングの適切なレベルを決定する必要があります。バックアップの速度が高まると、バックアップにかかる時間が短縮します。Arcserve D2D のバックアップ データは圧縮されて、Advanced Encryption Standard（AES）-128、AES-192 または AES-256 を使用して暗号化されますので、セキュリティが強化されます。

また、**Arcserve D2D** のバックアップは、以下の方法で Windows サーバと仮想プラットフォーム間の移行にも使用できます。

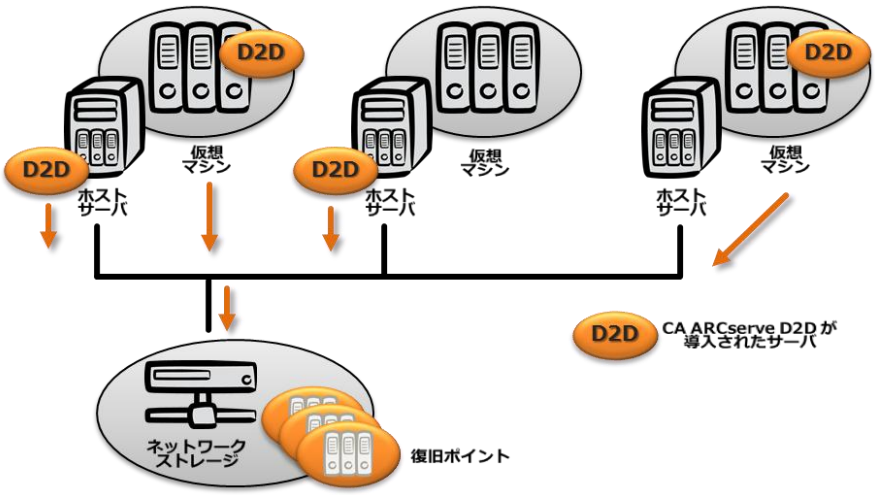
- **ベアメタル復旧**（BMR）は同種または異種のハードウェアに対して実行できます。また、バックアップ先のボリューム サイズの変更オプションも使用できます。Arcserve D2D でバックアップを作成したデータでサーバを復旧できます。
- **物理から仮想への移行**(P2V)では、物理サーバのバックアップを作成し、仮想サーバに復元できます。

- **復旧ポイントのコピー、または移行**では、バックアップデータを取得して、自動的にオフサイトなどの場所にコピーを作成できます。

Arcserve D2D による Hyper-V の保護

Hyper-V のホストを保護することによって、Arcserve D2D ではホストレベルと VM レベルの両方を保護できます。Hyper-V のホストレベルのみを保護する場合は、Arcserve D2D を Hyper-V のホストサーバにインストールします。Hyper-V のホストサーバに障害が発生したら、Arcserve D2D 標準の BMR 手順に従って、Hyper-V のホストサーバを復旧します。ファイルを指定して復旧する場合、Arcserve D2D 標準の復旧手順を使用して、復旧するファイルを検索します。図 6 では、Hyper-V の VM を保護する場合に Arcserve D2D をインストールする場所を示しています。

図 6. Arcserve D2D r16 による Microsoft Hyper-V の保護



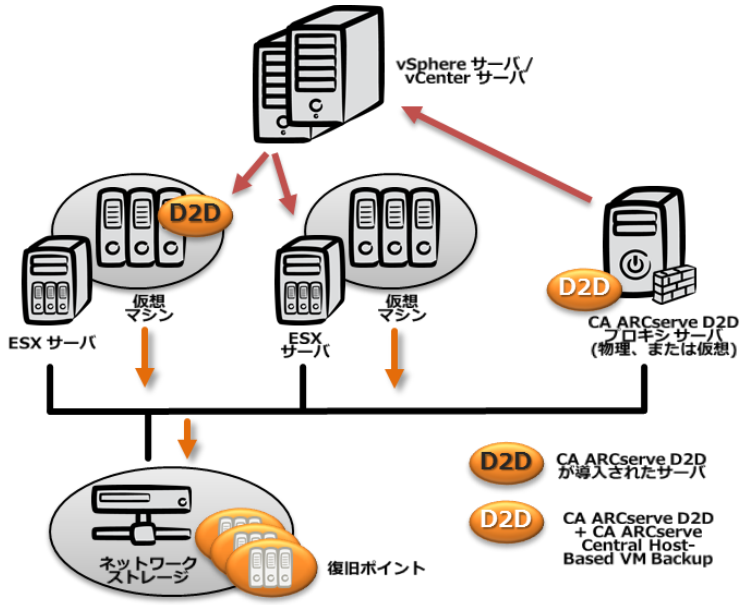
Hyper-V をホストレベルと VM レベルで保護する場合は、Arcserve D2D を Hyper-V のホストサーバにインストールします。Arcserve D2D のバックアップから個々の VM を復旧する場合は、VM を復旧する場所（元の場所または他の場所）を選択してから、Arcserve D2D の復旧ウィンドウで個々の VM のファイル（.vhd、.avhd、.vsv および.xml の構成ファイル ）を選択します。また、Arcserve D2D を Windows の個々の VM にインストールすると、ホストとは別に VM のみを保護できます。iSCSI の論理ユニット番号（LUN）を直接 VM 内に割り当てている場合、LUN 内のデータのバックアップは Arcserve D2D の Hyper-V のホストレベルのバックアップでは作成されないため、この方法が必要になります。

Arcserve D2D による VMware の保護

VMware 環境の場合、Arcserve D2D を個々の VM にインストールすると、あらゆる物理サーバと同じアプローチを使用して VM を保護できます。また、Arcserve D2D を **Arcserve® Central Host-Based VM Backup** と連携させて使用できます。この技術では、シングルパスのバックアップを VMware のホストサーバ上の各 VM に対して実行するために、エージェントなどのソフトウェアを各ゲスト VM にインストールする必要はありません。Arcserve Central Host-Based

VM Backup では、VMware vSphere 4.0 以降のシステム上で実行している VM が保護され、シングルパスの VM のバックアップから VM レベル、アプリケーション レベルおよびファイル レベルのデータを復旧できます（図 7）。

図 7. Arcserve D2D r16 による VMware の保護



Arcserve Central Host-Based VM Backup では、VMware vSphere の CBT 機能を使用して、最後のバックアップ以降の VM の変更をキャプチャし、ファイルとフォルダを個々の VM から個別に復旧できます。また、VM 内のサポート対象アプリケーションも復旧でき、仮想サーバの保護と復旧を簡単に実装できます。バックアップ セッションは Arcserve D2D に復旧ポイントとして保存され、Arcserve D2D および Arcserve D2D のベアメタル復旧（BMR)ツールを使用して、VMware ESX の VM を他の VM や物理サーバに復旧できます。

Arcserve Central Host-Based VM Backup では、新しく追加された仮想マシンが自動的に検出されます（VM を Windows オペレーティングシステムで実行している場合）。また、Arcserve Central Host-Based VM Backup では、Arcserve D2D をバックアップ プロキシにインストールする必要があります。

Arcserve D2D の運用管理

Arcserve D2D では、Web 2.0 のインタフェースを使用してバックアップと復旧のタスクを設定および管理します。また、Arcserve D2D コンソールを使用すると、Arcserve D2D をリモートで導入し、手動でノードを指定して追加できます。導入後は、Arcserve D2D のホームページから、これらのリモートノードを選択して管理できます。このインタフェースを使用すると個々の Arcserve D2D サーバを管理できますが、Arcserve D2D の大規模な導入の場合、Arcserve® Central Applications の以下の追加ツールを使用すると効果的です。

- **Arcserve® Central Protection Manager** は、Arcserve D2D の集中管理ツールとして機能し、ネットワーク上のすべての Arcserve D2D への簡単なアクセスを提供します。また、Arcserve D2D のすべての復旧ポイントからファイル、フォルダ、アプリケーションを復旧する場合にも使用できます。Arcserve Central Protection Manager は、Active Directory®に保存されたコンピュータオブジェクトを使用して、Arcserve D2D の物理と仮想のサーバを自動検出する機能も搭載しています。
- **Arcserve® Central Reporting** では、Arcserve D2D のノードと Arcserve Backup のサーバのパフォーマンスに関する情報収集およびレポート表示を一元化できます。レポートは表やチャート形式でブラウザ ベースのダッシュボード インタフェースに表示できます。また、データをフィルタリングして、保護対象のコンピュータの特定の階層やグループに関するレポートを表示できるため、共通の特性を備えた複数のシステムに固有のレポート データを確認できます。たとえば、**仮想化保護ステータス レポート**には、VCB または Hyper-V を使用した VM のバックアップの状態がすべて表示されます。また、データは CSV ファイルとしてエクスポートしたり、電子メールで送信できます。

Arcserve D2D と Arcserve Backup の連携

Arcserve Backup を使用すると、Arcserve D2D の復旧ポイントを複数の Arcserve D2D サーバからインポートして、データをテープなどの Arcserve Backup のメディアに保存できます。Arcserve D2D の VM のひとつのバックアップから、Arcserve Backup Manager コンソールを使用して復旧する場合、［ツリー単位］オプションで［D2D Server RAW Session］を選択します。Arcserve D2D のセッション全体を他の場所に復旧した後、復旧したセッションを使用して、Arcserve D2D のデータを復旧します。Arcserve Backup を使用して、Arcserve D2D のデータ（Microsoft SQL Server および Microsoft Exchange Server のアプリケーションデータなど）をファイル、フォルダおよびアプリケーションレベルで復旧できます。Arcserve D2D を Arcserve Backup と連携させると、バックアップの時間を削減または排除できます。また、I^2 テクノロジを使用すると、Arcserve D2D の復旧ポイントを短時間で作成できます。作成した復旧ポイントは、Arcserve Backup でオフラインに移動して管理されるため、VM やホストサーバには影響しません。

また、Arcserve Backup で作成した Arcserve D2D のデータのバックアップを使用して、Arcserve D2D サーバのベアメタル復旧（BMR）を実行できます。RAW バックアップのセッションを使用する場合、BMR のプロセスは以下の 2 段階に分かれます。

1. BMR のプロセスが完了するまで、RAW バックアップのセッションは、問題が発生したサーバがアクセスできる共有フォルダ、ネットワークファイル共有またはデバイスに復元されます。
2. Arcserve D2D の BMR メディアを使用して復旧するサーバを起動してから、RAW バックアップセッションを復元した場所を検索します。画面の指示に従って、BMR のプロセスを完了します。

レプリケーション

レプリケーションとは、すべてのシステムとデータをリアルタイムで継続的に保護し、バックアップとデータを遠隔地のサーバとストレージに災害復旧のために複製または移行することを意味します。

Arcserve Replication r16

Arcserve® Replication では、Arcserve Backup や Arcserve D2D をはじめとする多様なバックアップ ソリューションを補完し、継続的なレプリケーション、災害復旧（DR）を強化するための遠隔地へのデータ保護、CDP のためのデータ リワインドなどの機能が装備されています。Arcserve Replication を使用すると、ファイルとデータベースの変更がリアルタイムで自動的に本番サーバからレプリカ サーバに複製されます。また、レプリケーションによって、すべての VM が他のストレージ（ローカル、オフサイトまたはクラウドのストレージなど）に複製できますので、別途ストレージを用意する必要がありません。すでに Windows のフェイルオーバ クラスタなどの技術を導入している場合でも、Arcserve Replication の遠隔地へのレプリケーションを通して保護が大幅に強化されます。Arcserve Replication では、VMware ESX、vSphere および Citrix XenServer は VM レベルで、Microsoft Hyper-V はハイパーバイザと VM レベルでそれぞれ保護されます。 また、物理と仮想の両方のサーバの Windows システムも保護されます。

Arcserve Replication の管理モジュールでは、管理サービスと関連するユーザ インタフェースが提供されるため、レプリケーション モジュールやエンジンを本番サーバやレプリカ サーバに簡単に導入できます。また、導入、管理、レポート、保守が一元化されたツールを使用できます。Arcserve Replication のエンジンは、本番サーバやレプリカ サーバに手動でインストールする必要がありません。これは、レプリケーションのシナリオにエンジンの自動導入が含まれているためで、インストールのために本番サーバやレプリカ サーバを再起動する必要もありません。

Arcserve Replication の管理サービスによってエンジンがインストールされた後、VM とアプリケーションを保護するためのシナリオを作成できます。たとえば、Hyper-V のホストサーバとそのすべての VM を保護する場合、**Microsoft Hyper-V のレプリケーションとデータ復旧**のシナリオを作成します。シナリオに使用する本番とレプリカのホストサーバを選択してから、そのホストサーバの Arcserve Replication エンジンの検証を選択します（エンジンがインストールされていない場合やアップデートが必要な場合はインストールします）。それによって、Hyper-V の本番サーバで実行しているすべての VM が自動的に検出され（デフォルトの場合）、レプリケーションの対象として選択されます。

アプリケーション レベルで保護が行われるため、Arcserve Replication ではアプリケーション環境が自動的に検出され、簡単かつ迅速に導入できます。また、自動設定を使用してレプリケーションのシナリオを作成し、Microsoft Exchange、Microsoft SQL Server、Microsoft SharePoint、IIS、Microsoft Dynamics® CRM および Oracle を保護できます。その他の Windows アプリケーションはカスタム アプリケーション保護ウィザードまたはカスタム スクリプトで保護します。リアルタイムの継続的データ保護（CDP）機能によって、ローカルまたはリモートの物理/仮想サーバとストレージにデータを複製して、災害復旧に使用できます。

すべてのシナリオで、本番サーバとレプリカ サーバ間の最初の同期の完了後、Arcserve Replication エンジンからはバイトレベルの変更のみがレプリカ サーバに送信されます。そのため、リモートのデータとアプリケーションの日常的なバックアップに必要な帯域幅を削減できます。また、VM を保護するために、ブロックレベルで同期が行われます。Arcserve Replication エンジンでは、本番サーバとレプリカ サーバのファイルをブロックごとに比較して、異なるブロックのみが複製されます。また、大きいサイズの VHD ファイルが変更された場合、VHD ファイル全体を転送せずに、ブロックを同期して変更のみが転送されます。導入時間を短縮する場合、［**オフライン同期**］を使用して、データを物理メディアからレプリカ サーバにインポートします。これは、ワイドエリアネットワーク（WAN）を経由して最初のレプリケーションを実行するときには特に便利な機能です。

Arcserve Replication には、そのほかにもパフォーマンスに関連した技術が追加されています。**マルチストリームレプリケーション**では、ひとつのシナリオでも、レプリケーション データを複数の IP セッションに送信できます。それによって、レプリケーションと同期の時間が大半のシナリオで短縮されますが、高い遅延の発生する WAN 接続のシナリオでは最も効果的です。**帯域幅のスロットリング**では、受信帯域幅の範囲をレプリカのホストに合せて制御できます。一定の値を 1 日 24 時間適用したり、時間によって異なる値を設定することができます。帯域幅スケジューラを使用して、利用の多い時間に帯域幅を減らし、レプリケーションのピーク後に増やして、帯域幅のリソースを最適化できます。

また、Arcserve Replication では**評価モード**によって、実行前にデータ レプリケーションに必要な帯域幅の量を測定できます。 この評価モードを使用すると、帯域幅の要件を予測して、それぞれの要件に合わせて複製するデータの量や帯域幅を調整できます。

Arcserve Replication では、**Arcserve® Assured Recovery®**無停止復旧テスト機能を使用して、複製したデータとアプリケーションを確実に復旧できます。Arcserve Assured Recovery によるテストが完了したら、Microsoft Volume Shadow Copy Service（VSS）を使用して、データとアプリケーションのスナップショットを作成し、重要なデータの保護を強化するための復旧ポイントとして使用できます。また、VSS のスナップショットから、その時点でのボリューム データのイメージのコピーを作成できます。Arcserve Replication コンソールでは、特定のスナップショットをファイル システム デバイスとして使用して、システム障害時やデータ破損時に個々のファイルやボリューム全体を迅速に復旧できます。

Arcserve Replication では、レプリカ サーバの VSS スナップショットのスケジューリングがサポートされます。それによって、データ復旧のためのフェイル オーバの選択肢が増えます。このスナップショットを使用すると、指定した時点のボリューム全体または個々のファイルやフォルダを復旧できます。Arcserve Replication では、Windows ベースのアプリケーションに対してカスタム アプリケーション保護ウィザードが提供されるため、シナリオが標準装備されていないアプリケーションを保護する場合などでも、アプリケーション固有のフェイル オーバや復旧プロセスのスクリプトを作成する必要はありません。

Arcserve Replication の**データリワインド**機能を使用すると、損失または破損したデータとデータベースを指定した時点の状態に迅速に復旧できます。データリワインドではリワインド ジャーナルを使用して、ファイル変更の原因となった

I/O の操作に関する情報が保存されます。リワインド ジャーナルを使用することにより、I/O の操作を取り消して、過去の時点（破損前の有効な状態など）まで遡ってファイルをリワインドできます。データ リワインドによってバックアップ ソリューションの機能強化、次回の定期的なバックアップまでのデータ保護、復旧時間の短縮が可能になります。また、個別の復旧ポイントを設定できますが、レプリカ サーバをオンラインにする必要があります。

Arcserve Replication では、**システム全体**のレプリケーションのシナリオも提供されます。このシナリオを使用すると、物理/仮想サーバのオペレーティングシステム、システムの状態、アプリケーションおよびデータを含めたシステム全体を仮想サーバにレプリケートできます。システム全体のレプリケーションでは、物理または仮想のマシンを 3 つの異なる形式の仮想サーバ（Hyper-V、VMware ESX、Citrix XenServer）にレプリケートできます。また、クラウドでホストする Windows ベースの仮想マシンの場合、Amazon Elastic Compute Cloud（Amazon EC2）にもレプリケートできます。レプリカをオフライン ストレージに保存すると、本番稼動しているホットスタンバイのサーバに必要な VM のオペレーティングシステムとアプリケーションの追加のライセンスは不要になります。また、仮想サーバの複製先へのオーバー プロビジョニングも可能になり、災害復旧で必要なときに使用できます。オフラインのレプリカ サーバは本番サーバが停止した場合に使用します。レプリカ VM は実質的に本番サーバのクローンであるため、IP、名前、ネットワークの競合を防止するために、フェイル オーバを行うまでオフラインの状態にしておく必要があります。

また、Arcserve Replication では P2V と V2V（仮想から仮想）の移行にも対応しています。物理サーバから仮想サーバへ迅速に移行できるだけでなく、仮想化の統合プロジェクトなどの場合、仮想サーバのプラットフォーム間（VMware から Hyper-V など）の移行も簡単に実行できます。

Arcserve Replication による Hyper-V の保護

Hyper-V の場合、Arcserve Replication では柔軟な導入オプションが提供されます。ハイパーバイザ レベルのレプリケーションまたは個々のゲスト オペレーティングシステムとアプリケーションのレプリケーションを選択でき、ゲスト VM のそれぞれに Arcserve Replication エンジンをインストールする必要もありません。

Hyper-V 環境を保護するため、それぞれの Hyper-V のサーバに対して Hyper-V のシナリオを作成できます。Arcserve Replication ではサーバ上の Hyper-V のゲストのそれぞれに対して自動的に個別のシナリオが作成されます。たとえば、サーバ A に Hyper-V の VM が 10 台ある場合、シナリオ作成ウィザードでサーバ A のシナリオを作成し、Hyper-V のレプリカ サーバに複製できます。また、サーバ A 上の Hyper-V の VM のそれぞれに対して個別に保護のシナリオが自動で作成されるため、各 VM のフェイル オーバが簡単になります。たとえば、サーバ A で実行している VM に対して 10 個のシナリオを作成し、これらのシナリオを同じシナリオ グループ「サーバ A」に含める作業がすべて自動化されます。Arcserve Replication をハイパーバイザ レベルで使用する場合、いくつかの機能が使用できない場合があります。たとえば、Arcserve Assured Recovery が使用できなかったり、データ リワインド機能でリワインド ポイントを選択するときに個別の設定が制限されることがあります。これらの機能が必要な場合、ハイブリッド シナリオを使用すると、ハイパーバイザとゲストレベルの両方で効果的なレプリケーションが行えます。少数の VM やゲスト（Microsoft Exchange や SQL Server で実行しているサーバなど）を指定するハイブリッド シナリオの場合、Arcserve Assured

Recovery の効果が発揮され、データリワインド機能でより詳細に個別の復旧が行えます。これらの VM には、それぞれのレプリケーションのシナリオと ArcserveReplication エンジンを割り当て、その他すべての VM は、ハイパーバイザ レベルの保護シナリオの一部として設定します。また、個々の VM レベルでシナリオを作成することもできます。

Arcserve Replication による VMware の保護

Arcserve Replication を使用して VMware の VM を保護する場合、個別のファイル サーバ、アプリケーションまたはシステム全体のシナリオを各 VM に対して作成し、各 VM に Arcserve Replication エンジンを配置する必要があります。なお、ホストレベルのレプリケーションのオプションはありません。

VMware の環境では、VMware vCenter のインフラストラクチャを保護して、すべての VM を継続的に管理する必要があります。**VMware vCenter Server** のシナリオでは、Arcserve Replication を使用して、単一サーバの環境であっても、複数サーバを使用した分散環境であっても、すべての VMware vCenter コンポーネント（データベース サーバ、ライセンス サーバ、Web サーバ）を複製できます。

高可用性

高可用性によってリアルタイムでシステム全体やアプリケーションが保護され、複製先のシステムが手動または自動で瞬時にオンラインに接続できます。

Arcserve High Availability r16

Arcserve® High Availability では、Arcserve Replication と同様の機能に加え、システムレベルとアプリケーション レベルの監視、自動、または手動のフェイルオーバおよび手動のフェイルバックの機能を利用できます。

このソリューションを導入すると、独自の物理または仮想のレプリカ サーバを構築し、そのレプリカ サーバをオンサイトまたは遠隔地に配置して、データを同期および複製できます。あるいは、システム全体の保護機能を使用して、物理または仮想のシステム全体（オペレーティングシステム、システムの状態、アプリケーション、データなど）をオンサイトまたは遠隔地に配置したオフラインの仮想レプリカ サーバに複製することも可能です。

フェイル オーバとフェイル バックは、本番サーバとレプリカ サーバの間でアクティブな役割とパッシブな役割を変更する Arcserve High Availability のプロセスです。フェイル オーバは本番サーバに問題が発生した場合に使用し、自動と手動を切り替えられます。フェイルバックは本番サーバの修理または交換の後で、元の本番サーバと現在の本番サーバ（フェイルオーバ前は元のレプリカ サーバ）を再同期させるために使用します。フェイル オーバとフェイル バックでは物理マシンのように、VM 上で実行している 32 ビットと 64 ビットのシステムでのアプリケーションのフェイル オーバがサポートされます。Arcserve High Availability の管理サービスによって本番サーバやアプリケーションのサービス停止が検出された場合、本番サーバとレプリカ サーバ間のフェイル オーバを自動で、または Arcserve High Availability Manager を使用して手動で実行できます。ping、データベースおよびユーザ定義を含む事前定義の監視確認方法を使用

して、VM の自動フェイルオーバを設定できます。ユーザ定義の確認方法では、フェイル オーバをカスタマイズして、アプリケーション固有の要件に対応できます。

手動のフェイル オーバではネットワークとエンドユーザのリダイレクションが自動化され、災害や障害が発生する前に対応できます。また、「ホット」な移行にも最適で、業務時間中でもユーザの作業の中断を最小限に抑えながら実行できます。移行後も、新しいサーバを即座に本番環境で利用できます。

Arcserve High Availability には Arcserve Assured Recovery が統合されているため、業務を中断しない「業務時間終了後」に自動の無停止復旧テストのスケジュールを設定できます。

また、Arcserve High Availability では、「クラウドへのフェイル オーバ」（システム全体）のシナリオが提供され、このシナリオでは Windows の VM が Amazon EC2 にフェイル オーバされます。本番サーバはローカルの物理または仮想のサーバ、レプリカ サーバは Amazon EC2 のサーバです。クラウドを使用してシームレスにフェイル オーバを実行するには、自動の **DNS リダイレクト**をこのシナリオで指定します。それによって、VM に対するユーザ要求はユーザが設定した Amazon Virtual Private Cloud（Amazon VPC）を使用して、自動的に Amazon EC2 サーバにリダイレクトされます。Amazon VPC は Amazon Web Services （AWS）から隔離されたプライベート クラウドで、ユーザ独自のデータセンタ トポロジと同様の独自の仮想ネットワーク トポロジを定義できます。詳細については、ホワイトペーパー シリーズの『Arcserve® r16 の拡張機能：クラウドの活用』を参照してください。

Arcserve High Availability では分散グループも作成できます。これは、SharePoint サーバや他のアプリケーション環境で、複数の物理または仮想のサーバに依存しているサービスを統合する場合に効果的な機能です。デフォルトのグループや通常のグループとは異なり、分散グループには一元管理の機能があります。各サーバには個別のシナリオが必要ですが、シナリオ共通のプロパティをグループ全体に割り当てると、各シナリオで個別に指定する必要がなくなります。一元管理の機能には、以下が含まれます。

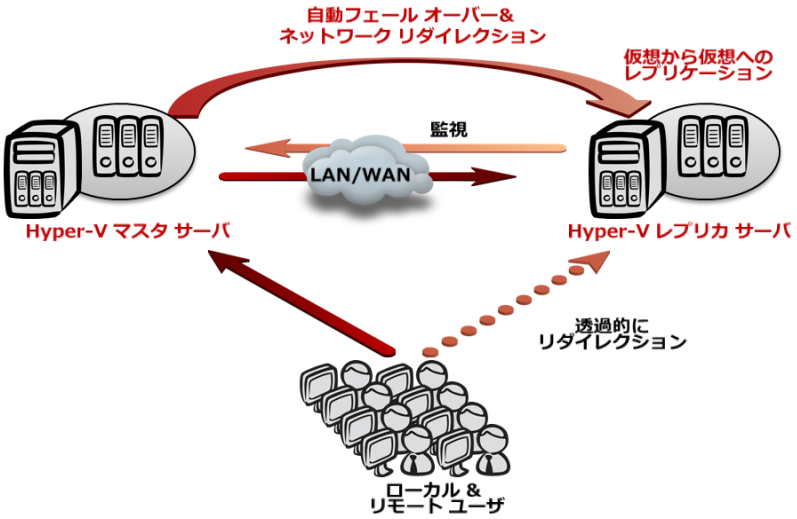
- **グループでの実行とグループでの停止：**すべてのシナリオをグループ全体で開始および停止できます。
- **グループのフェイル オーバ。**すべてのシナリオで手動のフェイル オーバを実行し、いずれかに問題が発生した場合、自動的に切り替えるよう設定できます。
- **グループによるアクティブ サーバのリカバリ：**分散グループの問題（SharePoint サーバのマスタの一部とその他のレプリカ サーバが同時にアクティブになる場合）を解決できます。すべてのシナリオでアクティブなサーバを本番サーバまたはレプリカ サーバに簡単に復旧できます。

Arcserve High Availability による Hyper-V の保護

仮想サーバを保護するには、Arcserve High Availability エンジンを環境内の Hyper-V の本番サーバおよびレ サーバにインストールする必要があります。Arcserve High Availability エンジンを Hyper-V のサーバ 1 台のみにインストールすると、Hyper-V の VM のデータ レプリケーション先が Hyper-V 以外のサーバに制限されます。Hyper-V のホストレベルでのフェイル オーバを有効にするには、Arcserve High Availability エンジンを Hyper-V の 2 台目のサーバにイン

ストールする必要があります。また、VM レベルでのフェイル オーバを有効にするには、Hyper-V の統合コンポーネントを各ゲスト オペレーティングシステムにインストールします。フェイル オーバは自動または手動に設定できます。フェイル オーバの前に統合のテストが必要な場合、Arcserve High Availability では仮想サーバのフェイル オーバを手動で実行できます。Arcserve High Availability による Hyper-V のシナリオでは、VM 全体が保護され、フェイル オーバは VM レベルで実行されます（図 8）。アプリケーション レベル（QL Server、Exchange、Oracle など）でフェイル オーバを実行する場合、Arcserve High Availability エンジンは Hyper-V の本番およびレプリカの VM にインストールして、適切なシナリオを作成します。

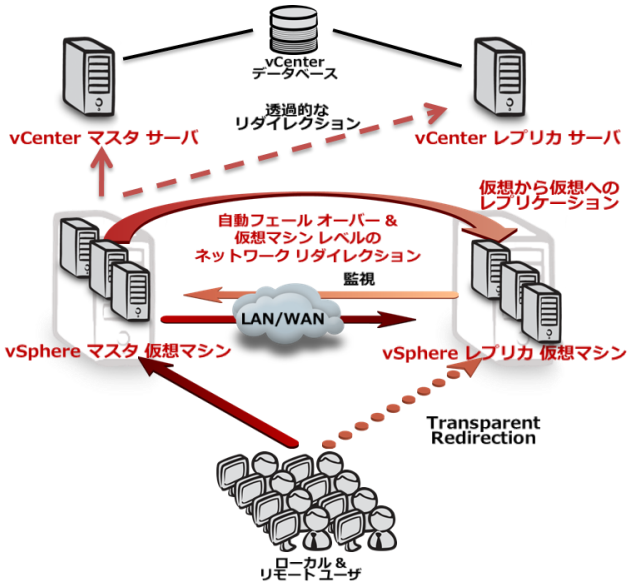
図 8. Arcserve High Availability r16 による Hyper-V のフェイルオーバ



Arcserve High Availability による VMware の保護

Arcserve High Availability では、1 台以上の VMware ESX サーバを管理する VMware vCenter Server のレプリケーションと高可用性がサポートされるため、クラスタ アーキテクチャやストレージ インフラストラクチャの共有は必要ありません。VMware vCenter のインフラストラクチャを保護するため、Arcserve High Availability エンジンを環境内の VMware vCenter の各サーバにインストールします（図 9）。 また、分散環境で VMware vCenter のデータベースが異なるマシンに保存されている場合、Arcserve High Availability の本番サーバとレプリカ サーバに同じ分散データベースを指定します。その後、Arcserve High Availability for SQL Server または Arcserve High Availability for Oracle を使用して、これらリモートのデータベース サーバを保護します。

図 9. Arcserve High Availability r16 による VMware vSphere と VMware vCenter のフェイルオーバ



VMware の VM を複製する場合、異なるファイル サーバまたはアプリケーションのシナリオを各 VM に使用して、Arcserve High Availability エンジンを各 VM にインストールします。Hyper-V と同様に、本番サーバが利用できない場合、本番サーバとレプリカ サーバ間のフェイル オーバを自動で、または Arcserve High Availability Manager を使用して手動で実行できます。VMware の環境では、このフェイル オーバの設定は VMware vCenter Protection のシナリオと個々の VM のシナリオの両方に適用されます。それに対して、VMware vCenter Site Recovery Manager では、VM のプロビジョニングを異なるマシン間で実行する場合、イメージのクローンが作成されるため、新しい VM には障害が発生した VM と同じマシン名と IP アドレスが割り当てられます。この方法では、本番 VM へのリモート アクセスと障害の原因の特定、およびシステムの問題解決と障害が発生したアプリケーションの再起動が非常に困難になります。

Arcserve High Availability では、フェイル オーバを実行するため、サーバのトラフィックとユーザが DMS サーバ レベルにリダイレクトされます。そのため、本番やレプリカの VM のサーバ設定は、フェイル オーバ中もその後も変更されることはありません。また、それによって、オフサイトの VM の管理も大幅に簡略化され、DR サイトでの作業のために仮想のローカル エリア ネットワーク（LAN）を構築したり、本番のサブネットから IP アドレスを有効化する（多くの場合、異なる IP サブネット）必要もありません。

Arcserve Central Virtual Standby r16

バックアップと復旧、またはベアメタル復旧の（BMR）手順をきちんと構築していたとしても、時間がかかりすぎて目標復旧時点（RPO）を達成できないソリューションもあります。このような場合、Arcserve D2D と Arcserve® Central Virtual Standby を組み合わせることをお勧めします。Arcserve Central Virtual Standby を Arcserve D2D と連携させ

ることによって、本番サーバが使用できない場合、またはマスタ サーバやソース サーバを保守のためにオフラインにする場合、VMDK や VHD ファイルを使用して、Hyper-V または VMware のスタンバイ用やバックアップ用の VM を手動/自動で起動できます。Arcserve Central Virtual Standby では Arcserve D2D のスナップショットまたは復旧ポイントを使用して、設定可能なポリシーとスケジュールに基づいて、自動的に復旧ポイントが VM のスナップショットに変換されます。完全に自動化されたスタンバイ マシンの場合、ハートビートを使用して、本番サーバの可用性が検出されます。Arcserve D2D の監視サーバ（Hyper-V のハイパーバイザ ホスト）がハートビートの間隔を過ぎても本番サーバと通信できない場合、ホストによって VM の予備のコピーが自動的に起動されます。この技術によって、復旧に「即時対応」可能な VM が提供されるため、ディスク、テープまたはクラウド ベースのバックアップからデータを復元する先のディスクやネットワークにオーバーヘッドが発生することもありません。また、復旧ポイントのスナップショットのデータをソース サーバ（元のソース サーバなど）に復元して、仮想から物理（V2P）への復旧が行えます。

さらに、スナップショットを使用して、V2P の災害復旧を仮想マシンからハードウェア（元のハードウェアなど）に対して実行して、別のホスト（同じハイパバイザの実行は不要）の別の VM（V2V）に復旧できます。物理サーバの状態のバックアップ コピーから作業をするため、物理から仮想（P2V）への移行中のリスクも緩和されます。

Arcserve Central Virtual Standby は基本的に VM の保護を目的としていませんが、VM として実行している物理サーバや本番サーバに復旧のオプションとしてスタンバイ用の VM が提供されます。また、Arcserve Central Virtual Standby のバックアップは Arcserve D2D のツールを使用して復旧でき、個々のファイルとフォルダにも必要に応じてアクセスできます。

Arcserve シリーズによる仮想環境の保護

Microsoft や VMware のような仮想化技術ベンダーは、仮想環境で使用するデータ保護ツール（Microsoft System Center Data Protection Manager、Microsoft Exchange データベース可用性グループ（DAG）、Windows フェイルオーバ クラスタ、VMware クラスタ、VMware SAN レプリケーションなど）を提供しています。それに対して、CA Technologies では仮想化技術の違いに関わらず、データとシステムの保護を統合した技術を提供しています。この技術は、物理と仮想の両方の環境、Microsoft のサーバとアプリケーション、Microsoft Hyper-V、VMware vSphere、VMware ESX、Citrix XenServer のハイパーバイザに対応しています。また、Arcserve 製品は単独でも使用できますが、他のベンダー製品と連携させたり、アプリケーション、サーバまたはデータセットのさまざまな復旧ポイントと目標復旧時点に対応した完全なソリューションとしても利用できます。

Arcserve 製品では、以下をはじめとする仮想化の幅広い統合シナリオがサポートされます。

- **Arcserve Replication** では、以下のように **Arcserve D2D**（および **Arcserve Backup**）のバックアップ イメージをリモート サイトとクラウドまたは他のメディアに複製して保護を強化できます。

    - **Arcserve D2D** では、すべての地方事業所と支社の VM のバックアップをローカル ディスクに作成し、**Arcserve Replication** を使用して、そのバックアップ ファイルを一元化された遠隔地のストレージに複製できます。
    - **Arcserve D2D** では、VM とファイルのバックアップを作成し、**Arcserve Backup** を使用して Arcserve D2D のバックアップをテープに転送し、遠隔地で長期保存できます。
- **Arcserve Replication** では、すべてのデータのレプリケーションの一元化に加え、**Arcserve Backup** または **Arcserve D2D** でバックアップも一元化できます。また、レプリカ サーバから VM のバックアップを作成できるため、バックアップの時間的制約とパフォーマンスの問題を回避できます。この統合に加え、Arcserve Backup のプロパティを Arcserve Replication と High Availability のシナリオを使用することで、バックアップとレプリケーションの作業が統合されるだけでなく、Arcserve Replication の CDP 機能も使用できるため、ホストサーバで障害が発生してもデータが損失することはありません。また、長期的な永久ストレージを利用できるため、アーカイブとコンプライアンスの要件にも対応できます。さらに、仮想サーバをレプリカ サーバとして使用できるため、コストも削減できます。
- **Arcserve High Availability** は **Arcserve Backup** または **Arcserve D2D** と組み合わせることで、高可用性と継続的データ保護が実現し、バックアップの時間的制約の問題も解決できます。また、Arcserve High Availability と Arcserve Backup を統合することにより、業務に影響を及ぼすことなくデータを復旧できます。Arcserve Backup では、まず本番サーバに影響を及ぼさずにデータが Arcserve のレプリカ サーバに復元されます。その後、レプリカ サーバとマスタ サーバを再同期するだけで復元プロセスが完了します。また、レプリカ サーバにデータを復元して、本番環境でのデータの復元をテストできます。
- **Arcserve Backup** ではバックアップ ソースとして、バックアップ可能な **Arcserve Replication** と **Arcserve High Availability** のシナリオのリストを作成できます。また、これらのバックアップ ソースのバックアップは、標準バックアップと同じく簡単な手順で作成できます。これらのシナリオのバックアップから、自動的にデータの VSS スナップショットをレプリカ サーバに作成して、永久ストレージとして保存できます。

まとめ

現在では、物理のみのサーバ環境を導入したり、仮想化やゲスト オペレーティングシステムのベンダーを 1 社に制限している企業はほとんどありません。大半は、物理と仮想のサーバ、Microsoft Hyper-V、VMware およびその他のハイパーバイザ、Windows などのオペレーティングシステムが混在しています。そのためデータとシステムの保護には、複合的な環境を効果的に管理し、仮想サーバのインフラストラクチャにおける障害のリスクを排除することは重要です。

Arcserve は単独でも、また他の技術と統合しても使用でき、仮想と物理のサーバを完全に、しかも簡単に保護できます。また、アプリケーションとデータのバックアップと復旧、システム全体やアプリケーションの災害復旧とレプリケーションにも対応し、基幹システムの高可用性も確保できます。

Arcserve 製品ファミリの詳細については、arcserve.com/jp を参照してください。

※ サポート条件については動作要件を参照してください。ゲスト OS 上で問題が発生した場合、物理環境上での問題再現が必要なケースがあります。