ホワイトペーパーシリーズ：

Arcserve® r16 の拡張機能

『クラウドの活用 』

2011 年 10 月

Arcserve Japan

---

arcserve

assured recovery

目次

はじめに 3

クラウドテクノロジ 3

クラウドでのシステムおよびデータの保護とリカバリに関する問題 4

バックアップとリカバリにクラウドを使用 5

Arcserve Backup r16 の概要 5

Arcserve D2D r16 の概要 9

Arcserve D2D オンデマンド 13

レプリケーションにクラウドを使用 13

Arcserve Replication r16 の概要 13

システム、アプリケーションデータの高可用性のためにクラウドを使用 17

Arcserve High Availability r16 の概要 18

まとめ 22

はじめに

「クラウド」は多くの意味を持ちます。オンラインで提供されるアプリケーションとプラットフォームを指したり、リモートデータセンタを使用したデータストレージなどのインフラストラクチャサービスを指すこともあります。 クラウドサービスは、Amazon や Microsoft などのベンダによって、あるいはリソースが社内で構築、導入、管理、コントロールされる「プライベートクラウド」によってリモートで提供される場合があります。 クラウドを使用するテクノロジの普及とともに、迅速な Web ベースのアプリケーション開発、分散ネットワークインフラストラクチャ、安全なオフサイトのデータストレージのためにツールとプラットフォームを提供することの重要性が増しています。

業界アナリストはワールドワイドで、43%のエンドユーザがデータ保護目的でクラウドを検討していると述べています。クラウドサービスは、コストを年間運用費として計上でき、 利用時に、あるいは利用に応じて支払いができるため、IT 予算が限られている場合にも有効です。 また、多くの企業で課題となっている事業継続性（BC）や災害復旧（DR）のサービスレベルアグリーメント（SLA）に対応するための社内リソース（たとえばリモートサイト、設備およびスタッフ）が不足しています。 そこで、クラウドベースの Infrastructure-as-a-Service（IaaS）を使用すれば、熟練したスタッフの採用や再研修を行うなどの支出を抑えながら、SLA にも対応することができます。 企業は DR 用のリモートサイトを所有していないことが多いため、クラウドベンダからリモートリソースを「借りる」方法はコスト効果の高い選択肢でもあります。

本書では、Arcserve® シリーズがシステムやアプリケーション、データの保護のためにクラウドリソースを利用できる仕組みの技術概要を解説します。 クラウドをバックアップやレプリケーション、アーカイブとして使用したり、重要なシステムの高可用性を実現するためのオフサイトプラットフォームとして使用する方法について説明します。

クラウド テクノロジ

現在利用可能なクラウドの技術や製品は数多くあり、Gmail や Salesforce.com などの単純なアプリケーションから、クラウド対応ストレージやクラウド型仮想サーバなどインターネットを介して提供されるインフラストラクチャ リソースまでさまざまです。 クラウドベースのアプリケーションは通常、Software-as-a-Service（SaaS）または Application-as-a-Service（AaaS）と呼ばれています。 インターネット上で提供されるコンピューティング、ストレージ、アクセシビリティなどのサービスは、Infrastructure-as-a-Service（IaaS）と呼ばれます。ストレージが主要サービスの場合は、Storage-as-a-Service（これも SaaS と略称されることがあります）と呼ばれています。 多機能なコンピューティング プラットフォームを提供するベンダもあり、これは通常 Platform-as-a-Service（PaaS）と呼ばれています。 これには例えば、Salesforce.com や Amazon Web Services™（AWS）などがあります。 本書では、次のクラウド テクノロジを通して Infrastructure-as-a-Service および Storage-as-a-Service に焦点を当てていきます。 本書ではまた、データ保護、リカバリ、可用性の向上のために Arcserve シリーズがどのようにクラウド サービスを活用するかを説明します。

- **Amazon Web Services（AWS）：** AWS はクラウド サービスのスイートを提供します。 データおよびシステムの保護には、次の AWS サービスが最も重要です。

    - **Amazon Elastic Compute Cloud（Amazon EC2）**はオンライン上でホストされた仮想マシン（VM）を提供します。
    - **Amazon Simple Storage Service（Amazon S3）**はオンラインのストレージサービスです。
    - **Amazon Virtual Private Cloud（Amazon VPC）**は、安全な仮想ネットワーキング サービスを提供し、Amazon EC2 マシンへのアクセスに必要です。
- **Windows Azure™ ：**Windows Azure にはオンライン ストレージサービスとアプリケーション ファブリック サービスが含まれます。
- **パートナー プライベートクラウド：**これには Amazon S3 標準を使用する Eucalyptus パートナーが含まれます。

クラウドのシステムおよびデータの保護とリカバリに関する問題

多くの企業にとっては、クラウドを現実的な保護およびリカバリの選択肢として考えると同時に、優先事項として対応する必要がある重要な問題があります。

- **サービス レベル アグリーメント (SLA)**: ほとんどの企業は、保護されたシステムおよびデータの可用性を確実なものにするために、SLA を要求し、また、クラウド プロバイダのデータセンタでの予期しない障害やサービス中断、データの損失に対する保護を要求します。
- **法令遵守**。 データがリモート サーバに保存されている場合は常に、法的基準とコンプライアンスの問題を解決する必要があります。 たとえば、国によっては規制が厳しく、より厳密に施行される場合があるため、クラウドデータセンタの地理的場所は重要な問題になることがあります。
- **管理性**: 多くの企業は、クラウドへの移行によって自社のシステムおよびデータのコントロールが失われることを理解しているからこそ、クラウドベンダの選択はきわめて重要です。
- **セキュリティ**: クラウドにコピーされたシステムおよびデータは実証可能な方法で保護される必要がありますが、同時に常時アクセス可能であることも必要です。 セキュリティはあらゆるレベルで考慮されるべきで、クラウドデータセンタに転送されるときのネットワーク上でのデータの保護と、データが保管された後のデータセンタ内でのデータ保護も重要です。
- **帯域幅**: 多くの企業にとって、利用可能な広域帯域幅とそのコストの検討は、クラウドベースのシステムとデータの保護およびリカバリ サービスの採用にとっての大きな障壁となっています。 オフサイトの保護とデータセンタへの復旧にとって十分な帯域幅を確保するためには、入念なプランニングが求められます。 IT を提供するためにクラウドに転向する前に、クラウドへのデータ転送と復旧に要する時間をテストし理解しておく必要があります。
- **長期保存ポリシーおよびアーカイブ：** リモート データがアクセス可能で、アーカイブ ポリシーが単純で容易に実装できるものである限り、クラウドは長期的なデータ ストレージの要件を満たすために役立ちます。

- **リカバリのテストと検証**: データおよびシステムの保護戦略はすべて、迅速にリカバリを行う能力で判断されます。 したがって、クラウド ベース リソースのリカバリは、そのようなリカバリが必要にならないうちに、定期的にテストと検証を行えることが必要不可欠です。

クラウドは、アーカイブや災害対策用のリソースとして大いに役立つ可能性があります。 また、入念なプランニングが行われ適切なツールが使用されていれば、事業継続性にとって重要なアプリケーションおよびデータの高可用性を確保するためのフェイルオーバ先になることも可能です。 クラウドは、IT 企業が BC/DR 戦略およびリソースを導入する際の俊敏性と柔軟性を高めることができ、関連するすべてのハードウェアやソフトウェアの購入、導入、管理、維持が排除できることでコスト削減にも貢献します。 またクラウドは、利用できるリモート DR サイトまたはデータセンタを持たない企業にとっても理想的な解決策となりえます。 クラウドのライセンスは通常、使用量に応じた課金で月次請求されるため、クラウドの使用は IT 企業にとって、設備投資（CAPEX）と運用費（OPEX）のバランスをとるためにも役立ちます。

バックアップとリカバリにクラウドを使用

バックアップとリカバリは、ファイル サーバ上のユーザ ファイルおよびフォルダ、Microsoft® Exchange メールボックス、Microsoft SQL Server®データベースなど、会社の IT 環境全体の重要なデータおよびアプリケーションの保護を意味します。 クラウドは、バックアップとアーカイブのためのオフサイトのストレージ リソースを提供できますが、次のような課題を検討する必要があります。

- **バックアップウィンドウ**。 バックアップをローカル　リソースに行う場合に比べ、クラウド リソースに直接バックアップする方法はより多くの時間を要します。つまり、広域ネットワーク（WAN）上のバックアップは、バックアップウィンドウで許容されている時間を超過する場合があるということです。 この問題を解決するのがハイブリッド　モデルと呼ばれるものです。 このモデルでは、バックアップ性能をより向上させるために、最初にローカルへバックアップを行ってから、その後、パフォーマンスに余裕があるときにバックアップのコピーをクラウドに送信する方法です。
- **リカバリ時間**。 もう 1 つの検討事項は、クラウドからデータを復旧するのにかかる時間です。 ハイブリッド ソリューションがあれば、データをローカル　ソースから復旧する選択肢ができるため、リカバリ時間もより短くなります。 この場合クラウドは、災害復旧とファイル アーカイブ プロセスのためのオフサイト データ ストレージ用に保持しておくことができます。

Arcserve Backup r16 の概要

Arcserve® Backup は安全なテープへのバックアップの作成と世代管理を行い、詳細なベアメタル復旧ツールを提供します。 この方法では、コンピュータは単独で、またはオペレーティング システムやアプリケーション ソフトウェアとともに、前回のバックアップ状態に復旧できます。 バックアップ データはディスクまたはテープ、またはクラウド ストレージに保存され、Arcserve Backup は段階的なバックアップ ジョブによってデータの移行を行います。 たとえば、大規模

なデータベースは定期的かつ迅速にローカル ディスクにバックアップされ、その後このディスクのデータは長期保存のためにクラウドにコピーされアーカイブされます。 Arcserve Backup の一元管理機能によって、データの保管場所に関わらず、単一の場所からリカバリ作業を管理することが可能です。 また、標準装備の暗号化によって、データの機密性は常に保持されます。

クラウド サポートの概要

Arcserve Backup は、バックアップ データのクラウド ストレージへのコピー機能を提供します。これによって、追加のオフサイト データ ストレージまたはリカバリの場所、アーカイブ目的のために、ディスクからディスク、そして クラウド（D2D2C）へのバックアップ ポリシーの一部として、バックアップ データをパブリック/プライベート・クラウド ストレージに移行できます。

サポート対象のクラウド サービス

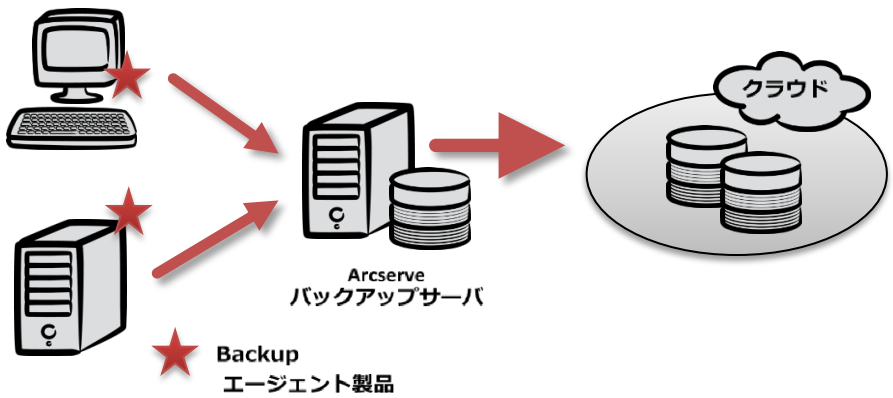
Arcserve Backup は次のクラウド構成をサポートします。

- 標準装備のクラウド機能(Amazon S3）を提供する Amazon Web Services ストレージへのクラウド コネクタ
- Eucalyptus を介したプライベート クラウドのサポート これは、Amazon S3 標準が使用されている場合にサポートされます（Eucalyptus 2.0 および 2.0.2）。

Arcserve Backup をクラウドで使用

Arcserve Backup ではオンプレミスでバックアップを作成してから、バックアップデータをクラウド ストレージに移行することができます。クラウドに直接バックアップするわけではありません（図 1）。 この方法ではバックアップ プロセスが最短時間で完了でき、バックアップを時間内に予定通り行えるため、アプリケーション インフラストラクチャへの影響が長引きません。

図 1. Arcserve Backup のクラウド ストレージへの移行



クラウド ストレージの構成

バックアップの保存にクラウド ストレージを使用するには、クラウド ベンダで有効なアカウントを作成する必要があります。 Amazon S3 ストレージの場合、これには Amazon Web Services（AWS）に登録した後、Amazon S3 に登録

して、クラウド ストレージとアクセスのための秘密鍵を取得する必要があります。 この段階で AWS Management Console を使用してストレージ バケットを作成するか、あるいは Arcserve Backup Manager Console でクラウド接続を設定しながらストレージ バケットを作成するかを選択できます。

Arcserve Backup Manager Console は**クラウド接続**を使用して、バックアップがクラウド ストレージを使用する方法を設定します。 たとえば、こうしたストレージは通常、保存されるメガバイト当たりで課金されるため、Amazon S3 の**低冗長化ストレージ**（RRS）には、重要性の低いデータを標準ストレージよりも冗長性の低いレベルで保存するよう選択すれば、コストを削減することもできます。 標準的なストレージも RRS の場合も、データは複数のサイトの複数のデバイスに保存されますが、RRS の場合はデータのレプリケーション回数が少ないためストレージ コストを低く抑えられます。

Arcserve Backup クラウド接続は、仮想**クラウド ベース デバイス**を使用して、データをクラウド ベンダのストレージに送信します。 クラウド ベース デバイスでは圧縮を有効にしてクラウドに保存したバックアップ データを圧縮でき、ストレージ コストや帯域幅の削減に役立ちます。

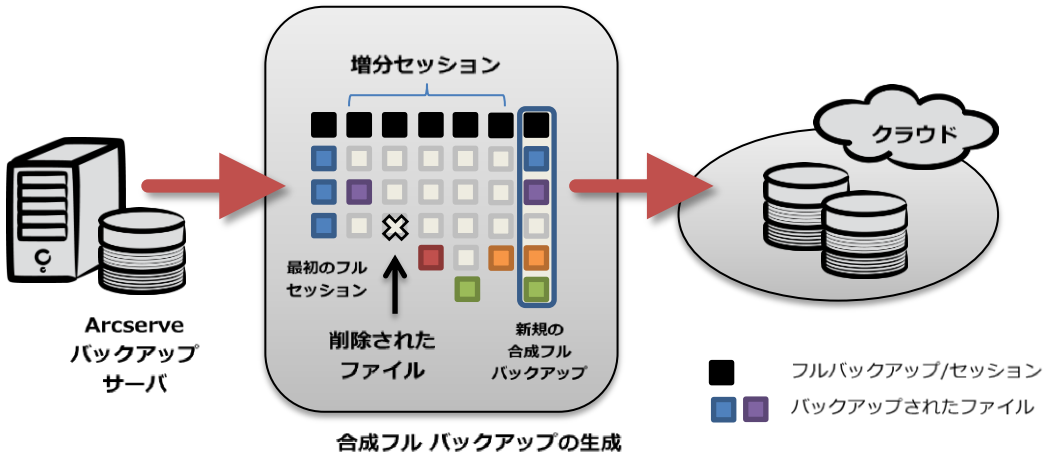
移行ジョブにクラウド デバイスを使用

データをクラウド ベース デバイスに移行するには、ステージング バックアップ ジョブを使用します。 ステージング ジョブの設定時に、中間ステージング デバイス（通常はローカル ディスク ストレージ）にデータを保存する期間を指定します。 さらに、指定の保存期間が過ぎた後にデータをステージング デバイスから削除するか、あるいは、クラウド ストレージなど最終的な保存先デバイスに移行するよう設定することができます。 また、最終保存先（この場合はクラウド ストレージ）の保存ポリシーを指定期間が過ぎたクラウド　セッションを削除して領域を開放し、コストを抑えるように設定することもできます。

SFB 移行ジョブにクラウド　デバイスを使用

合成フル　バックアップ（SFB）を使用すると、前回のフル バックアップ セッションとその後の増分セッションをフル セッションに合成することができます。 SFB は Arcserve Backup r16 で新しく導入された機能で、r16 以上を実行している Windows®クライアント エージェント（UNIX®または Linux®以外）にのみ適用可能です。 SFB はバックアップ内のデータ ボリュームを削減し、その結果保存するデータが少なくなるため、特にクラウド ストレージに有用です。 SFB ジョブはどの Arcserve Backup サーバからも送信可能ですが、データ重複排除機能やディスクからディスク、そしてテープ（D2D2T）またはディスクからディスク、そしてクラウド（D2D2C）などのディスク ステージング デバイスでの使用に限られています。 ディスク ステージングを使用すると、長期アーカイブや法令順守のため、またはデータのコピーをオフサイトで確実に保存する目的で、SFB セッションを簡単にクラウド ストレージに移行することができます。 図 2 は、Arcserve Backup が合成フル バックアップ セッションを作成する仕組みを解説しています。

図 2. 合成フル バックアップとクラウド



データおよびシステムのリカバリにクラウド バックアップを使用

Arcserve Backup を使用すると、Windows ネットワークに接続した大抵のコンピュータに、クラウド デバイスからデータをリストアすることができます。 通常であれば、リカバリ速度のためにローカル ステージング ロケーションを選択する方法が妥当です。アプリケーション エージェントが使用されていれば、クラウドや個別のファイル リストアに保存されたデータから詳細なアプリケーション リカバリを実行することができ、障害に対して最速のリカバリが行える柔軟性が提供されます。

Arcserve Backup クラウド バックアップの管理

Arcserve Backup は、クラウド ストレージ管理に使用できる各種ツールおよびオプションを提供します。

- **SRM レポート付きダッシュボード**。 これはプロアクティブに環境を監視でき、予定外のシステム障害やダウンタイムを回避するために役立ちます。 クラウド ストレージへのデータのバックアップに関するレポートについては、次のダッシュボードレポートを使用できます。
  - バックアップ データ保管場所レポート
  - メディア レポートのデータ配信
  - 目標復旧時点レポート
- **インフラストラクチャの視覚化**。 環境全体の簡単なネットワーク図を提供します。 クラウド ベース デバイスを含め、サーバ、ストレージ、その他のデバイスのすべてが表示されます。 ドリルダウンして特定のデバイス設定の詳細を確認したり、サーバやデバイスのステータスの概要、関連するレポートへのリンクを表示することができます。

Arcserve Backup クラウド バックアップのセキュリティ確保

Arcserve Backup は、バックアップの保存先がオンプレミスであってもクラウドであっても、安全な業界標準の暗号アルゴリズムを使用し、データのセキュリティと機密性保護を実現しています。 Windows クライアント エージェントは Advanced Encryption Standard（AES）-256 を使用してバックアップ データを暗号化します。 クラウド デバイスに

移行ジョブを送信するときは、移行プロセス中に Arcserve Backup サーバで暗号化ができるよう選択することもできます。 また、Arcserve Backup ではソースまたは本番サーバでの暗号化も可能で、重要な機密データが本番サーバを離れる前に保護することができます。 データは、保存されている場所に関わらず、保護されます。

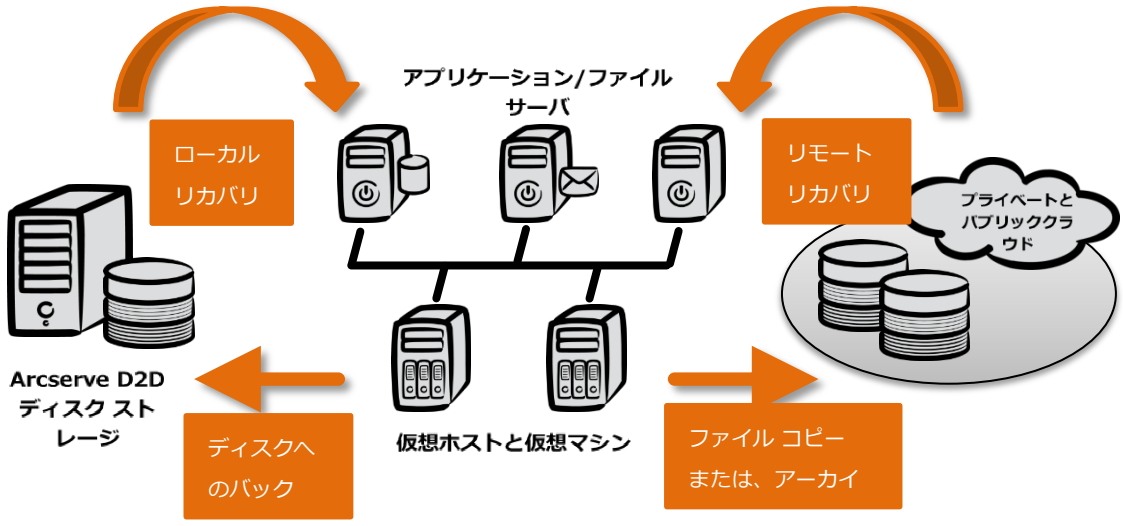
Arcserve D2D r16 の概要

Arcserve® D2D は、物理および仮想 Windows サーバにディスク ベースの保護を提供します。 このようなバックアップを使用すると、ファイル、ボリューム、データベース、e メール、およびシステム全体の迅速なリストアが可能です。 たとえば、サーバが Microsoft Exchange を実行している場合、メールボックス単位のきめ細かいリカバリが自動的に有効になります。 サーバが Microsoft SQL Server を実行している場合は、個々のデータベースが復旧できます。 バックアップはファイル コピー機能を使用してローカル ディスクに保存でき、重要なデータはオフプレミスのクラウド ストレージにコピーまたはアーカイブできます。

クラウド サポートの概要

Arcserve D2D ファイル コピー機能を使用すると、指定したファイルのコピーまたは保存の基準に基づきファイルをディスクまたはクラウドに移動またはコピーすることができます。 これによって、ストレージコストの削減、コンプライアンス要件への対応、データ保護を強化できます。 クラウドへのファイルのコピーによるローカル バックアップを使用するこのハイブリッド ソリューションは、同じ簡単なバックアップ プロセスを使用してローカル データからの迅速なバックアップとリカバリを行うことができ、災害復旧と長期的なアーカイブのための安全なオフサイト ストレージも提供します。

図 3. Arcserve D2D r16 とクラウド



サポート対象のクラウド

Arcserve D2D は次のクラウドサービスをサポートします。

- Windows Azure

- Amazon Simple Storage Service（Amazon S3）
- Eucalyptus を介したプライベートクラウド（Amazon S3 標準が使用されている場合にサポート）

Arcserve D2D をクラウドとともに使用

Arcserve D2D はクラウドを二次ストレージ場所として使用するため、まず Arcserve D2D バックアップを使用してローカル ディスク ストレージでシステムを保護する必要があります。 定期的な Arcserve D2D バックアップが設定された後、ファイル コピー ジョブと、バックアップ データをクラウドにコピーまたは移動する方法を設定するためのポリシーを作成します。 バックアップ データが移動されたら、ローカル バックアップが削除されます。 Amazon S3 ストレージの場合は、待ち時間を最適化してコストを最小限に抑え、規制要件に対応できるように、バックアップを保存する Amazon S3 データセンタの地理的場所を選択できます。 また Amazon S3 では、ストレージ コストを削減するために重要度の低いデータに RRS を有効にするよう選択できます。 また、ポリシーの一部として、ファイル コピー プロセスを実行する頻度も指定します。 デフォルトでは、バックアップが 5 回正常に完了するたびにファイル コピーが実行されます。

バックアップ データをクラウドへ移動することは、ファイル アーカイブに有益なオプションです。 データはオフサイトで保護されるため、ローカル ストレージは低減され、また、古くなったデータを定期的にクラウドにアーカイブすることによって、ローカル バックアップのサイズが削減されるか、少なくとも継続的に拡大することを防げます。 Arcserve D2D は、バックアップ データを識別して検出しリストアを可能にする方法を複数提供します。 ユーザは利用可能なバックアップとファイル コピーの場所（ローカル ディスク/ネットワーク ドライブまたはクラウド）を参照して、リストア対象の特定のファイルまたはフォルダを検出できます。 個別のファイルを復旧する際は、そのファイルの複数のバージョンが利用可能な場合、リストアするバージョンを選択することもできます。 クラウド バックアップからシステム全体を復旧するには、最初にクラウド バックアップをローカル デバイスにリストアします。 次に Arcserve D2D ベアメタル復旧（BMR）ツールを使用して、復旧時点のローカル コピーから障害が発生したシステムをリストアできます。

Arcserve D2D クラウド保護の管理

Arcserve D2D は、バックアップおよびリカバリ タスクの設定と管理に Web 2.0 インタフェースを使用します。 Arcserve D2D は、Arcserve D2D コンソールを使用し、名前を指定して手動でノードを追加して、ネットワークを介してリモートで導入することができます。 導入した後は、基本の Arcserve D2D 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は、個別の Arcserve D2D サーバの管理に使用できますが、Arcserve D2D が大規模導入されている場合は、Arcserve® Central Applications が特に役に立ちます。

- **Arcserve® Central Protection Manager** は Arcserve D2D コンソールに代わる管理機能を提供し、ネットワークを介して Arcserve D2D バックアップにも簡単にアクセスできます。 これは Arcserve D2D のすべてのローカルおよびクラウド ベースの復旧時点からファイル、フォルダ、アプリケーションをリストアするために使用できます。 Arcserve Central Protection Manager はまた、Active Directory®で管理されているコンピュータ オブジェクトを使用することで物理および仮想環境上の Arcserve D2D サーバを自動検出できる機能

や、ポリシーベースの管理および導入ツールも提供します。 機能や場所などで Arcserve D2D サーバをグループ化できるため、大規模環境での管理も容易になります。

- **Arcserve® Central Reporting** は、Arcserve D2D ノードと Arcserve Backup サーバのパフォーマンスについての情報を収集したり、レポートを表示するための一元管理ツールです。 ブラウザベースの表やチャート、ダッシュボードインタフェース、レポートを表示でき、保護対象のコンピュータの特定の部門またはグループに関するレポートを表示することができるため、共通の性質を持つ一連のシステムに固有のレポートデータを対象にすることもできます。 たとえば、クラウドを含むデバイスにバックアップされたデータ量を表示することができます。 レポートは、CSV ファイルとしてエクスポートするか、または e メールで送信できます。

高い操作性の Web ベースの Arcserve Central Applications は、複数の Arcserve D2D サーバと Arcserve 製品が存在する環境向けに、管理オーバーヘッドを削減するよう設計されています。 たとえば、Arcserve Central Reporting は、Arcserve D2D と Arcserve Backup の両方から情報を収集します。Central Applications アーキテクチャは、Arcserve シリーズ全体に新しい統合機能を提供し、サードパーティ ベンダがお客様の Arcserve 環境を拡大するために活用いただくこともできます。

Arcserve D2D クラウドでのセキュリティ確保

Arcserve D2D は、機密データを暗号化して保護し（暗号化パスワードを使用）、暗号化されたデータをリカバリ後に復号化する機能が追加されました。 Arcserve D2D データ保護は安全な AES-256 暗号化アルゴリズムを使用して、保護対象データのセキュリティと機密保護を提供します。 暗号の設定は簡単です。Arcserve D2D ホームページまたは Arcserve D2D モニタから、保護設定を選択して、使用する暗号化アルゴリズムとパスワードを指定するだけです。

帯域幅のボトルネックを回避

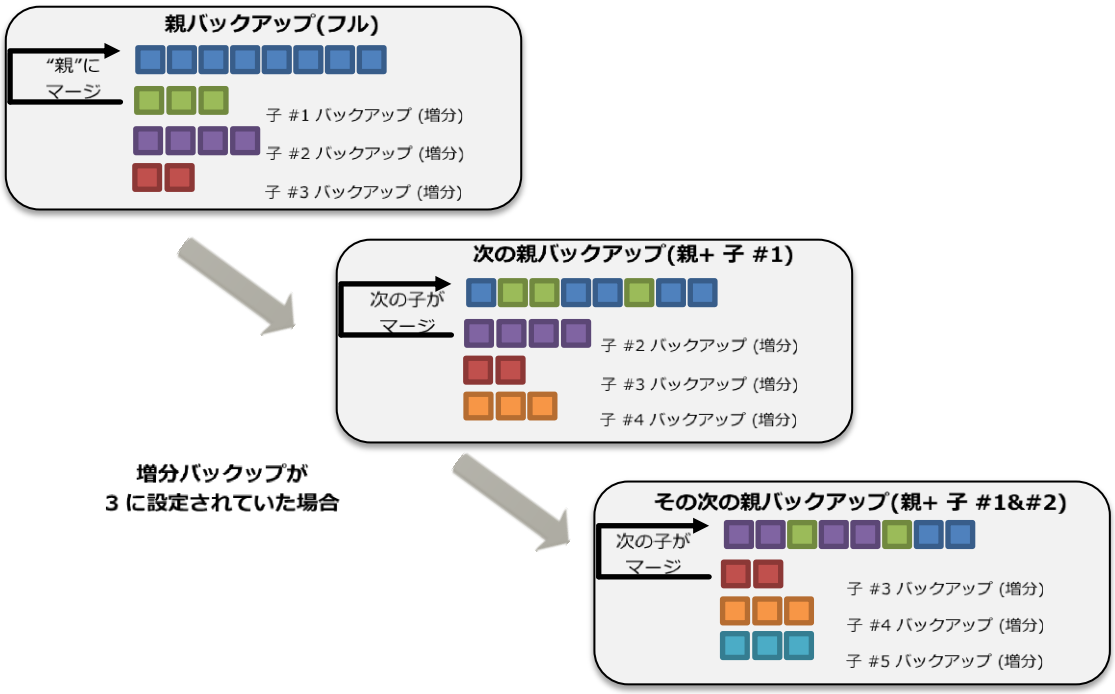
Arcserve D2D はクラウドへのバックアップ時に帯域幅のボトルネックを減らすことが可能です。

Arcserve D2D は、すべてのバックアップに**ブロックレベルの無限増分（I² technology™）**を使用します。 この技術は自動的にストレージコストを低減し、それによってクラウドとの間でやり取りするデータ量を削減します。

復旧ポイントを作成するためにバックアップ プロセスを開始すると、指定されたボリュームを複数のデータブロックに分割してからバックアップします。 最初のバックアップは、「親バックアップ」として、監視するベースライン ブロックを確立するためのボリューム全体のフル バックアップとなります。 バックアップを実行する前に、VSS スナップショットが作成されます。 次に、内部のモニタ ドライバが各ブロックをチェックして変更を検出します。 次からのバックアップは Arcserve D2D は、前回のバックアップ以降に変更されたブロックのみを継続的にバックアップします。 Arcserve D2D は、後続のブロックレベルのバックアップ（「子バックアップ」）を 15 分に 1 回の頻度でスケジュールでき、常に正確な最新のバックアップ イメージを得られます。 ローカルまたはネットワークのストレージ上に Arcserve D2D 復旧ポイントが作成された後、データをクラウドに転送するためにファイル コピー プロセスが実行されます。 前のバックアップとの間で変更されたデータだけがクラウドにコピーされるため、I² テクノロジは必要な帯域幅とクラウド ストレージを大幅に減らすことができます。 Arcserve D2D は Windows VSS ライタを使用するため、VSS

ライタをサポートする Windows オペレーティング システムでのみ実行できます。 サーバについては、Windows Server® 2003 Service Pack 1（SP1）以降、デスクトップおよびラップトップコンピュータは Windows® XP 以降です。

図 4.ブロックレベルの継続的増分バックアップ



Arcserve D2D は、**バックアップ速度のスロットリング制御**機能を提供します。バックアップを書き込む最大速度（MB/分）を指定して、CPU またはネットワークの使用量を減らすことができます。 これによって、バックアップがネットワーク ストレージの場所にコピーされている間に、利用可能なすべての帯域幅が消費されてしまうことを防ぐことができます。 バックアップ速度のスロットリング制御は、クラウドにアップロード中はファイル コピー データに適用されません。

データ保存ポリシーとアーカイブの管理

Arcserve D2D は、クラウドに保存されたデータの長期的な管理に最適なオプションが備わっています。

クラウドなど二次サイトに移動された復旧ポイントのデータには、**保存期間**を使用して、バックアップ データが保存される期間を指定できます。 指定した保存期間が終わると、保存データは保存先からパージされます。 このオプションではデータに適用するデータアーカイブの要件を自動的に実装することができます。

二次サイトにコピーされたデータについては、**ファイル バージョン**を使用すると、すべてのファイルについて保存場所に保存される旧バージョンの数を指定できます。 指定数を超えると、最も古いバージョンが破棄されます。 最も古い保存バージョンを破棄するこのサイクルは、新しいバージョンが保存先に追加されるたびに繰り返され、指定された保存

バージョン数が常に維持されます。 このオプションを利用すれば、データの破損に気付かなかった場合でも、いつでも破損されていない旧バージョンに戻ることができます。

Arcserve D2D オンデマンド

Arcserve D2D オンデマンドはクラウド特有のソリューションで、Arcserve D2D r16 と同等の機能を利用できます。この SaaS 製品は Windows Azure と直接統合し、Arcserve D2D オンデマンド製品ライセンスと Windows Azure ストレージをすべて 1 社のベンダから購入することができます。 一方、標準バージョンの Arcserve D2D では、クラウドをデータに使用したい場合、クラウド ベンダと個別にクラウド ストレージの契約を結ぶ必要があります。 Arcserve D2D オンデマンド サービスは月次のサブスクリプション ライセンスとして提供されます。Arcserve D2D オンデマンドは、標準バージョンの Arcserve D2D と同じ機能をサポートしていますが、次の点が異なります。

- Arcserve D2D オンデマンドは、設定プロセス中に自動的に **CA クラウド**（Windows Azure サービス）に接続し、他のクラウド ベンダを選択するオプションはありません。
- Arcserve D2D オンデマンドは、現在 Arcserve Central Applications でサポートされていません。

レプリケーションにクラウドを活用

多くの企業が、特に重要なデータの定期的なバックアップを補完するためにレプリケーションを活用しています。 レプリケーションは通常、リアルタイムで継続的に実行され、ファイルやデータ、データベースへの各変更をすべて監視して、予期しないデータの損失や破損が起きた場合や災害時に効果的な対策となります。 レプリケーションはまた、バックアップ完了後に災害復旧に備えてバックアップを遠隔地にコピーするためにも使用されます。 多くの企業は、目標復旧時点（RPO）と災害復旧戦略の両方に対応するために、リモートまたは遠隔地へのレプリケーションを実行していますが、利用可能なリモートサイトがない場合はどうすればいいでしょうか? クラウドは遠隔地レプリケーションのための理想的な手段で、特に自前のリモートサイトがなかったり運用管理スタッフがいない場合に有用です。

Arcserve Replication r16 の概要

Arcserve® Replication は、主に災害復旧（DR）の目的で、物理および仮想サーバからのデータとバックアップを遠隔地およびクラウドへコピーするために使用されます。 業務継続中のデータ損失のリスクを最小限に抑え、ストレージ デバイスの障害から保護するために、継続的なデータ保護（CDP）を提供します。 Arcserve Replication は本番サーバのデータを保管しているオンサイトや遠隔地、あるいはクラウド上のレプリカサーバと同期します。 Arcserve Replication は、ファイルとデータベースの変更をすべて監視し、それを自動的にリアルタイムで本番サーバからレプリカサーバにコピーします。 Arcserve Replication エンジンは自動的に導入されるため、本番サーバやクラウドにホストされているレプリカサーバに手動でインストールする必要はありません。 また、本番サーバもレプリカサーバのいずれも再起動の必要はありません。

Arcserve Replication では、サーバ、アプリケーション、データベースを保護するためのさまざまなシナリオを作成できます。 Arcserve Replication はまた、**システム全体**のレプリケーションシナリオを作成することで、オペレーティングシステム、システム状態、アプリケーションおよびデータを含めてシステム全体が物理または仮想サーバから、アクティブなサーバのゲスト側オペレーティングシステムの仮想サーバに複製できます。

データ損失をさらに減らすため、Arcserve Replication は**データのリワインド**機能を提供します。この機能は、レプリカ サーバをデータベース チェックポイントなど、データの損失や破損が起きる前の適切な時点に戻します。 この機能は通常、最後のバックアップ後に失ったデータの復旧を行うために使用されます。 このプロセスはレプリカ サーバで実行されるため、損失または破損したデータを復旧してから本番サーバとレプリカ サーバを再同期するまで本番環境は影響を受けず、業務を中断する必要もありません。 また、レプリカ サーバおよびストレージを使用して VSS スナップショットが繰り返されるようスケジュールすれば、本番サーバへの影響を回避すると同時にデータ リカバリをさらに簡単なものにすることができます。

クラウドサポートの概要

Arcserve Replication は、災害復旧に備えたシステム、アプリケーション、データのクラウドへのリアルタイムの継続的かつ定期的なレプリケーションを提供します。 また、使用するバックアップの種類に関わらず、災害復旧に備えてバックアップをクラウドへコピーするためにも使用できます。 データ リワインドや VSS スナップショットなどの機能は、クラウド ベンダによって提供されるサービスのレベルに依存するため、すべてのクラウド製品で利用できるわけではありません。

サポート対象のクラウド

Arcserve Replication には 2 種類のクラウドサポートがあります。 1 種類目は統合クラウドサポートで、これは Amazon EC2 に特化した機能を備えています。 もう 1 種類は非統合「クラウド」/WAN サポートで、これはたとえば仮想プライベート ネットワーク（VPN）上のリモート サイトまたはプライベート クラウド内にある、リモート Windows レプリカ　サーバを使用します。

レプリケーション シナリオのサポート対象クラウド（システム全体を除く）は次の通りです。

- **「クラウドへのレプリケート」オプション：**これは Amazon EC2 サーバとストレージ リソースに該当します。
- **ホスト名/IP による定期的なレプリケーション：** これは、レプリケーション エンジンと、安全な IP アクセスのための VPN 接続をサポートするクラウド ベースのサーバすべてに該当します。 これには Amazon EC2 サーバと Amazon VPC 接続が含まれますが、サポート対象のクラウド ベースのホストおよび VPN も使用可能です。

システム全体のシナリオの場合のサポート対象クラウドは次の通りです。

- Amazon EC2 サーバとストレージ リソース。
- Microsoft Hyper-V™、VMware、Citrix® XenServer VM、安全な IP アクセスのための VPN 接続をサポートするクラウド ベースのサーバすべて。

Amazon EC2 クラウドとともに Arcserve Replication を使用

Arcserve Replication には Amazon Elastic Compute Cloud（Amazon EC2）との統合が標準装備されており、クラウドへの迅速かつ容易なレプリケーションが可能です。 Arcserve Replication は、リモート サイトまたはオフィスとその他の社内およびプライベート クラウド プロバイダへの、オンプレミスでのレプリケーションに使用することも可能です。 Amazon クラウド レプリケーションは、バイトレベルのレプリケーションをサポートするため、ファイルへの変更のみ（ファイル全体である必要はない）がネットワークを介してクラウドに転送されます。 これによって帯域幅が減り、レプリケーションは確実にリアルタイムに近い状態で行われます。 複数の Amazon EC2 のインスタンスがサポートされるため、単一のオンプレミスのサーバを 2 つ以上のクラウド ベースのレプリカ サーバに複製することができます。 こうした 1 対多のシナリオは、Microsoft Exchange のようなアプリケーションなどで使用すれば、Exchange データベースのコピーを複数存在させることができます。 レプリケーションは、スケジュール別、または定期的、継続的に順方向に構成することができます。 継続的なレプリケーションでは、本番サーバで行われたすべての変更が自動的にレプリカ サーバに複製されます。 ただし、WAN 接続上でのレプリケーション制御のため、定期的なレプリケーションを設定することができ、これによってレプリケーションが手動またはスケジュール別にトリガされるか、または統合されて定期的に送信されます。 DR については、クラウド ベースのサーバに保持されているデータを使用して、ローカル オンプレミス サーバが復旧できます。

レプリカ インスタンスの作成

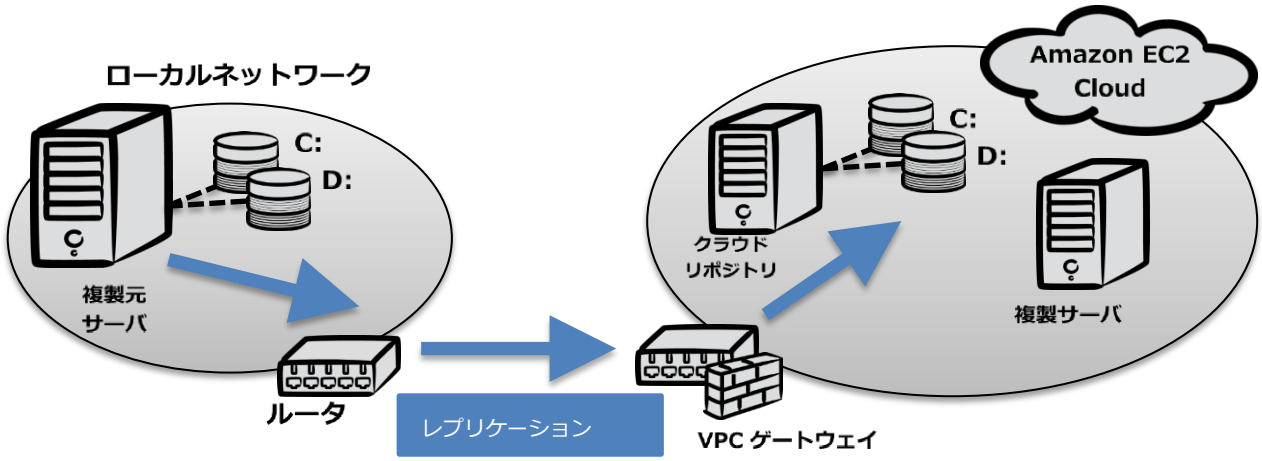
Arcserve Replication クラウド機能を使用するには、有効な Amazon Web Services（AWS）アカウントを使用して、Amazon EC2 レプリカ インスタンス（つまりオンライン仮想マシン）を作成する必要があります。 このインスタンスは Arcserve Replication マネージャを使用するか、AWS Management Console 内の Amazon EC2 ダッシュボードを使用して作成できます。 インスタンス作成時は、Amazon Machine Image（AMI）を使用するよう選択します。 Arcserve Replication については、Amazon Elastic Block Store（Amazon EBS）によってバックアップされている Windows AMI のみが使用可能です。 Amazon EBS はストレージの種類で、特に Amazon EC2 インスタンス用に設計されています。 これを使用すると Amazon EC2 インスタンスがデバイスとしてマウントできるボリュームを作成でき、標準的なハード ドライブと似ています。 プロセスの一部として、インスタンスを割り当てる Amazon Virtual Private Cloud（Amazon VPC)サブネットも指定できます。 Amazon VPC は、Amazon Web Services（AWS）クラウドの単独のプライベート セクションで、通常はご使用のデータセンタ トポロジと同様の方法で仮想ネットワーク トポロジを定義します。

Amazon の詳細を設定したら、Amazon EC2 Data Replication シナリオを作成し、**クラウドへの複製**オプションを使用することで、Amazon EC2 インスタンスをレプリカ サーバとして使用することができます。 またこのプロセスの間に、エンジンが Amazon EC2 VM に自動的にインストールされるように設定できます。

Amazon EC2 データ複製シナリオの実行

シナリオを作成したら、それを実行してレプリケーション プロセスを開始する必要があります。 図 5 は、シナリオ実行後のオンプレミスおよびアマゾン クラウド環境を示しています。

図 5. クラウドへのレプリケーション



クラウド リポジトリ サーバは、Arcserve Replication をインストールした Amazon EC2 インスタンスです。 リカバリ用レプリカ サーバも Amazon EC2 インスタンスで、本番サーバと同じディスク レイアウトになっています。 リカバリ用レプリカ サーバは作成された後、停止します。 すべてのボリュームがそこから切り離され、クラウド リポジトリ インスタンスに接続されます。 その後 Arcserve Replication シナリオが、オンプレミスの本番サーバからクラウド リポジトリ サーバの公開されたボリュームに作成されます。

オフラインの同期は通常、本番サーバとレプリカ サーバを最初に同期するために使用されます。 これによってすべてのデータを外部デバイスにコピーしてから、そのデバイスからレプリカ サーバにコピーすることができます。 これはネットワークを使用せずに大規模なデータ ボリュームを転送するための方法です。 オフライン同期は Amazon EC2 では使用できないことに注意する必要がありますが、クラウド ベンダによってサポートされている場合は、その他のプライベート クラウドで使用可能な場合があります。

リカバリにクラウド ベースのレプリカサーバを使用

リカバリ プロセスは、定期的なレプリケーションと同様ですが、この場合、同期は逆方向に行われ、クラウド ベースのレプリカ サーバからオンプレミスの本番サーバへの方向で行われます。 その方法は、レプリケーション シナリオを選択し、データのリストアを選択するだけです。 これによってリカバリが開始され、複製されたデータがネットワークを介して本番サーバに同期されると、レプリカ サーバは一時的に「マスタ」になります。 リカバリが完了すると、定期的なレプリケーション プロセスが再開できます。

クラウドへのレプリケーションの管理

Arcserve Replication Console には、クラウド管理用のタブが含まれます（クラウドビュー）。 ここでは、管理対象の AWS アカウント、インスタンス、スナップショット、Amazon EBS ボリューム、Elastic IP、セキュリティ グループのリストが示されます。

クラウドへのレプリケーションのセキュリテイ確保

クラウドへの通信を保護するために、Arcserve Replication 標準装備の Secure Sockets Layer（SSL）暗号機能を使用できます。 Amazon VPC 接続はそれ自体が暗号化されていますが、多くの企業は自社の環境内での暗号も必要とします。そこで、Arcserve Replication 暗号が Amazon VPC 暗号を補完しています。

帯域幅のボトルネックを回避

Arcserve Replication には、クラウドを複製するときに帯域幅のボトルネック削減に役立つ複数のオプションが含まれます。

すべてのシナリオ タイプについて、本番サーバおよびレプリカ サーバ間の最初の同期が完了した後、レプリケーション エンジンはファイル レベルまたはブロック レベルの変更のみをレプリカ サーバに送信します。 この技術は、リモートのデータおよびアプリケーションの毎日のバックアップに必要な帯域幅を減らします。

Arcserve Replication は、その他のパフォーマンス関連機能も提供します。 **マルチ ストリーム レプリケーション**機能では、単一のシナリオ内であっても複数の IP セッションでレプリケーション データを送信できます。 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、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制御**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、利用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。

Arcserve Replication と Arcserve High Availability には、データの複製に必要な帯域幅の規模をあらかじめ測定できる**アセスメント モード**が備わっています。 このアセスメント 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。

システム、アプリケーションデータの高可用性のためにクラウドを活用

高可用性とは、システムまたはアプリケーション全体のリアルタイムの保護のことで、セカンダリ システムが手動でも自動でも迅速にオンラインに接続できることを意味します。 多くの企業にとって、高可用性はビジネス上重要なアプリケーションおよびデータへのアクセスを維持するために必要です。 従来のバックアップを使用している場合、システムまたはストレージの障害発生後にシステム全体、アプリケーションおよびデータのリストアを行うと何時間もかかることがあり、ビジネスのあらゆる部分に影響を及ぼし、販売やサービスに多大な損害をもたらす可能性があります。 従業員の生産性ややる気にも影響が及び、企業としての評判やコンプライアンスも影響されます。 ベアメタル リカバリ（BMR）ソリューションは、この時間を大幅に削減しますが、それでも 1 時間またはそれ以上かかる場合があります。可用性の維持に役立つフェイルオーバ クラスタリングなどの技術に目を向ける企業もありますが、こうした技術は導入と維持が複雑でコストがかかることがあります。 クラスタのすべてのサーバはほぼ同一の仕様であり、同じオペレーティング システムとアプリケーションソフトウェアを持つことが必要で、その結果莫大なコストがかかります。 さらに、フェイルオーバ クラスタリングは共有ストレージ デバイスを保護しません。また、個別のレプリケーション ソリュー

ションを購入しない限り災害復旧のための遠隔地へのレプリケーションには使用できません。 多くの企業にとっては、ホストベースの高可用性ソフトウェア　ソリューションの方がよりよいオプションである可能性があります。 このソリューションは物理および仮想サーバとストレージを保護し、オンサイト、オフサイト、クラウドで導入できます。 多くの企業は高可用性を事業継続性のためのオンサイト ソリューションとして導入していますが、同じ技術を使用することで、事業継続性と災害復旧ニーズを満たすためにこうしたソリューションをオフサイトまたはクラウドに導入することもよくあります。 自社の DR サイトまたはリモート サイトを持たない企業にとっては、クラウドの使用は理想的なソリューションとなります。

Arcserve High Availability r16 の概要

Arcserve® High Availability は、Arcserve Replication のすべての機能に加えて、物理および仮想サーバ環境の両方に対応する自動のンフェイルオーバ、自動ユーザ リダイレクション、フェイル バックを備えたリアルタイムのサーバおよびアプリケーション監視を追加します。 フェイルオーバ機能は Microsoft SharePoint®、Microsoft Exchange、Microsoft Dynamics® CRM、Microsoft Hyper-V、VMware vSphere™仮想環境などのアプリケーションで利用可能です。

フェイルオーバおよびフェイルバックとは、本番サーバとレプリカ サーバの間でアクティブ/パッシブの役割が変わる Arcserve High Availability プロセスを意味します。

- **フェイルオーバ：** Arcserve High Availability は、本番のシステムとアプリケーションがリアルタイムで監視される自動フェイルオーバ プロセスを提供します。 予期しない障害が発生すると、業務はレプリカ サーバに移動され、エンドユーザは自動的にリダイレクトされます。 事前定義された監視事項を使用して自動フェイルオーバを設定できます。これには、特定のアプリケーションに対応するためにフェイルオーバをカスタマイズするための ping チェック、データベースチェック、またはユーザ定義の確認事項などが含まれます。 また、近い将来の危機発生やシステム保守に備えて、プロアクティブに業務とエンドユーザをレプリカ サーバに移動するためにフェイルオーバを使用することもできます。
- **フェイルバック：** フェイルバックは本番サーバが修復されたり交換された後に、元の本番サーバを最新のレプリカ サーバと再同期するために使用します。

Arcserve High Availability はまた、**Assured Recovery** オプションも提供します。 Assured Recovery は、レプリカ サーバにあるデータの復旧可能性の詳細なテストを無停止で実施でき、データおよびアプリケーションの復旧に使用できる自動災害復旧テストです。 必要に応じて手動のテストも使用できます。 Assured Recovery テストは通常の操作を妨害せず、再同期も必要なく、高可用性または災害復旧作業にも影響を及ぼしません。

クラウドサポートの概要

Arcserve High Availability は、フェイルオーバのためにサーバとストレージ リソースを提供するプライベートおよびパブリック クラウドで使用できます。 Assured Recovery とデータリワインド、VSS スナップショットは Amazon EC2

ではサポートされていませんが、クラウド ベンダが提供するサービスのレベルによっては、別のプライベート クラウド製品で利用可能な場合があります。

サポート対象のクラウド

すべての高可用性シナリオでのサポート対象クラウド（システム全体を除く）は次の通りです。

- **ホスト名/IP による定期的なフェイルオーバおよびフェイルバック：** 高可用性エンジンと、安全な IP アクセスのための VPN 接続をサポートするクラウド ベースのサーバすべて。

クラウドへのフェイルオーバを使用するシステム全体のシナリオのサポート対象クラウドは次の通りです。

- Amazon EC2 サーバとストレージ リソース（Windows ベースシステムのレプリケーションおよびフェイルオーバのみ）。
- Hyper-V、VMware、Citrix XenServer VM、安全な IP アクセスのための VPN 接続をサポートするクラウド ベースのサーバすべて。

Amazon EC2 クラウドとともに Arcserve High Availability を使用

Arcserve High Availability は Amazon EC2 と統合されますが、オンプレミスやリモート オフィスまたは支社、その他のサポートされている社内およびプライベートのクラウド サービスにも使用できます。 Arcserve High Availability を Amazon EC2 とともに導入するには、システム全体の高可用性シナリオを使用して、オペレーティングシステム、システム状態、アプリケーションおよびデータを含むシステム全体を、物理または仮想サーバから Amazon クラウドのオフラインの仮想サーバにレプリケートします。 システム全体のレプリケーションを使用して、複数の物理サーバおよび/または仮想サーバのレプリケーションが、Amazon EC2 クラウド内で実行されているプロキシ/ゲートウェイ サーバ上にレプリカ ボリュームとして保存されます。 障害発生時には、新しい仮想マシンが作成され、適切なレプリカ ボリュームがプロキシ サーバから切り離されてフェイルオーバ目的でマウントされ、レプリカ（フェイルオーバ）サーバが本番システムとなります。 この独自のプロセスでは使用するストレージと実際に使用されたフェイルオーバ システム時間に対してのみ料金を支払えばよいため、クラウド サービスのコストが削減できます。 レプリカ（フェイルオーバ）サーバはオフラインであるため、レプリケーション プロセス中はシステムの使用料金は課金されません。

この「クラウドへのフェイルオーバ」（システム全体）シナリオは Amazon EC2 に特有のものですが、Windows Server 2003、Windows Server 2008、Windows Server 2008 R2 サーバで利用できます。この場合、本番サーバはローカルの物理または仮想サーバで、レプリカ サーバは Amazon EC2 サーバです。 クラウドを使用してスムーズなフェイルオーバを提供するために、このシナリオとともに自動的に **DNS をリダイレクト**するよう指定し、Amazon Virtual Private Cloud（Amazon VPC）設定を使用して本番サーバに対するユーザ要求が自動的に Amazon EC2 サーバにリダイレクトされるようにします。

フェイルオーバシナリオは、SharePoint サーバファームまたはその他のアプリケーション環境など、サービスの整合性が複数の物理または仮想サーバに依存する、分散されたサーバグループ全体に適用できます。 Arcserve High

Availability とともにサーバグループを使用することで、共通シナリオのプロパティをグループ全体に適用できます。 グループ内ですべてのシナリオが同時に開始および停止するように設定してグループ フェイルオーバを使用することも可能です。これを行うと障害発生時にすべてのサーバが同時に自動的にフェイルオーバされます。 分散されたグループは Amazon EC2 とともにシステム全体のシナリオ使用するよう設定するか、またはプライベート クラウドとともに Hyper-V、VMware、Citrix XenServer を使用するように設定することができます。

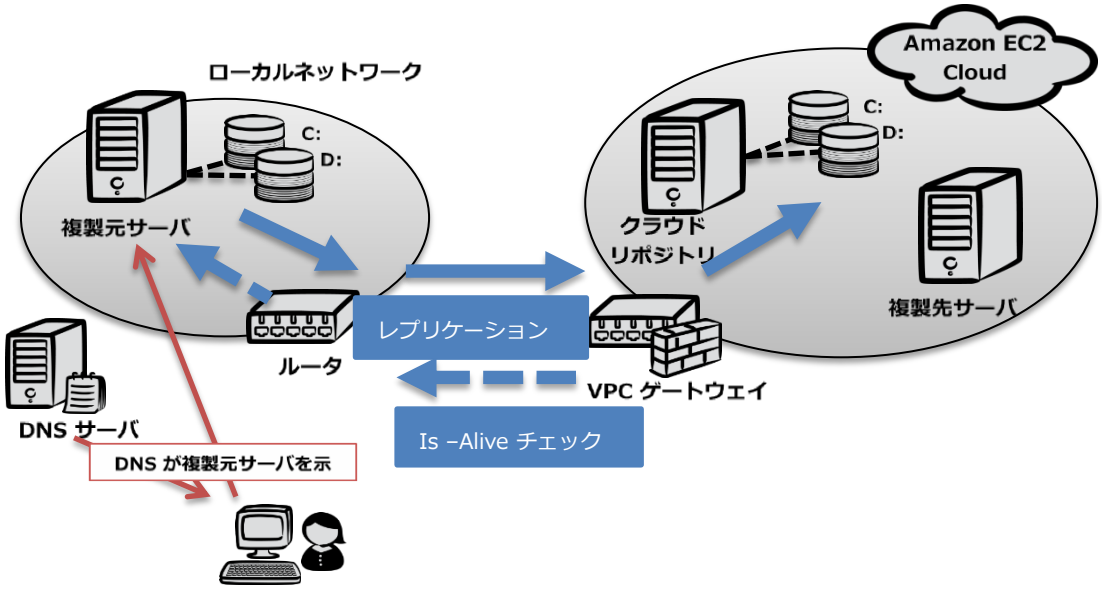
Amazon EC2「クラウドへのフェイルオーバ」（システム全体）シナリオの作成

Amazon EC2 レプリカ サーバでシステム全体の高可用性シナリオを作成するには、AWS アカウントが必要で、オンプレミス ネットワークと Amazon VPC の間に VPN 接続を作成しておく必要があります。 次に、シナリオ作成ウィザードでシステム全体のシナリオを作成し、**クラウドへの複製**オプションを指定します。 またこのプロセスの間に、エンジンが Amazon EC2 VM に自動的にインストールされるように設定できます。

Amazon EC2「クラウドへのフェイルオーバ」（システム全体）シナリオの実行

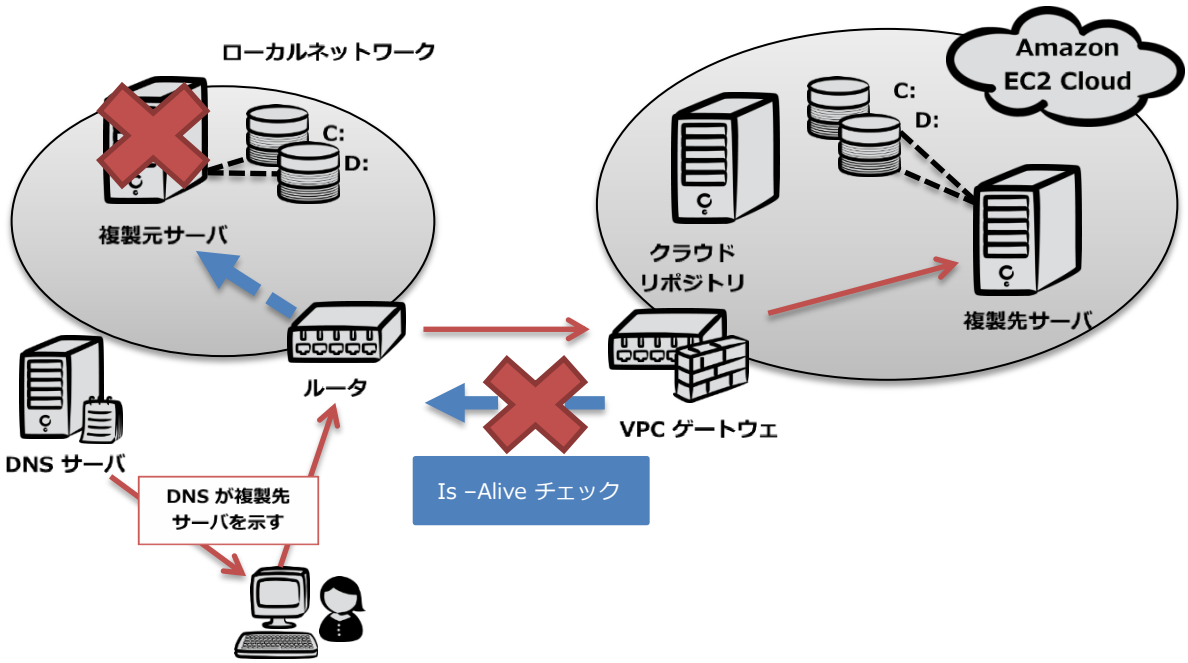
システム全体のレプリケーションの間に、1 台または複数の本番サーバからのシステム情報とデータがリモート インスタンスに複製され、Amazon AMI（クラウドベースの VM）上の仮想イメージとして Amazon EC2 ストレージ ボリュームに保存されます。 **Is-Alive** チェックが有効な限り、データはクラウドに継続的に複製されます（図 6）。

図 6.「クラウドへのフェイルオーバ」（システム全体）シナリオ: フェイルオーバ前



Is-Alive チェックが失敗し、本番サーバでの障害が発生すると、レプリカ サーバ（VM）が起動し適切なイメージが Amazon EC2 インスタンスに送信されます（図 7）。 クラウドへのフェイルオーバに Amazon EC2 を使用する方法では、使用したフェイルオーバ処理時間のみに料金を支払い、レプリケーション時間のコンピューティング コストは支払わないため、AWS コンピューティング コストを大幅に削減します。

図 7.「クラウドへのフェイルオーバ」（システム全体）シナリオ: フェイルオーバ後



Amazon EC2 クラウドへのフェイルオーバ後のシステムおよびデータのリカバリ

Amazon EC2 サービスでは高可用性のためのシステム全体のレプリケーションおよびフェイルオーバ シナリオのみが使用できるため、標準装備のフェイルバック機能は使用できません。

元の本番サーバが物理サーバだった場合、元のサーバと**同一**のハードウェア、オペレーティングシステム、アプリケーション設定で新しい本番サーバを構築する必要があります。 その後クラウド レプリカ サーバからのデータのみを新しい物理サーバにリストアできます。これは Arcserve High Availability が一時的な逆方向レプリケーション シナリオを作成し、ファイルシステム レベルでデータを複製するためです。 復旧プロセスの最後に物理サーバを再起動して、逆方向同期プロセス中にアップデートできなかったシステム ファイルを置き換えます。 新しい本番サーバのリストアを行ったら、次に Amazon クラウドへのレプリケーションおよびフェイルオーバ シナリオを再開して、本番システムおよびデータの保護を再開します。 また、新しい本番サーバに仮想サーバを使用できる場合、クラウド レプリカ サーバ上でシステム全体のレプリケーション シナリオを使用してオペレーティング システム、システム状態、アプリケーションおよびデータを同時に新しい本番サーバに再同期することで、新しい本番サーバをより簡単にリストアできます。

元の本番サーバが仮想サーバだった場合、クラウド レプリカ サーバ上でシステム全体のレプリケーション シナリオを使用してオペレーティング システム、システム状態、アプリケーションおよびデータを同時に新しい仮想サーバに再同期することで、新しい本番サーバをより簡単にリストアできます。 次にレプリケーションおよびフェイルオーバシナリオを再開し、本番システムおよびデータの保護を再開します。

基本的な Arcserve High Availability レプリケーションおよびフェイルオーバ シナリオを使用できるクラウド サービス プロバイダを使用している場合、製品に標準装備されているフェイルバック機能を使用できます。

まとめ

クラウドはデータおよびシステムの保護戦略の重要な構成要素となりえます。 また、バックアップと長期データ ストレージ用のリモート サイトとして使用したり、高可用性環境で CDP やバックアップサーバ用の安全なオフサイト ホストとしても使用できます。

Arcserve シリーズは、Amazon、Microsoft、または Eucalyptus インタフェースから利用できるクラウド サービスを活用して、アプリケーションとデータのバックアップとリカバリのために、災害復旧とシステム全体やアプリケーション全体のレプリケーションのために、また、ミッションクリティカルなサービスの高可用性実現のために、仮想および物理サーバの保護を実現します。

Arcserve 製品ファミリに関する詳細については、arcserve.com/jp をご覧ください。