物理サーバー、ハイパーバイザー、クラウドプラットフォーム間でワークロードを安全に移行する方法

はじめに

すべての企業にとって、物理、仮想、クラウドの各環境を包括的に保護し、必要に応じて任意のワークロードを同一プラットフォーム、新しいベアメタルサーバー、その他ハイパーバイザープラットフォーム、またはクラウドへ迅速かつ安全にリカバリできる柔軟なバックアップツールが必要です。移行の柔軟性は、ユーザー要件に適合しなくなったベンダーに起因する、ITシステムへの影響に対する備えを強化します。

最近の顕著な例として、ハイパーバイザーベンダーの VMware が挙げられます。VMware は 2023 年に Broadcom に買収された後、大企業セグメントへの戦略転換を進め、価格を引き上げ、中小企業や IT サービス事業者、付加価値再販業者に対するサポートポリシーを見直しました。こうしたユーザーに不利な契約変更により、多くの顧客が新たなハイパーバイザープラットフォームを模索するようになりました。

こうした移行プロジェクトでは多様な選択肢が考えられますが、安全かつ確実に移行を進めるためには、慎重な計画と適切なツールが求められます。企業が自社環境を適切に保護するためには、ワークロードを柔軟にレプリケーションおよび移行できる能力が求められます。これは単なるハイパーバイザー間の移行にとどまらず、任意の物理サーバー、ハイパーバイザー、またはクラウドプラットフォーム間での移行にも対応できる必要があります。

価格の引き上げとサポートポリシーの変更を受け、多くの VMware ユーザーが新たなハイパーバイザープラットフォームを模索するようになりました。

この柔軟性は企業に以下のメリットをもたらします。

- 新たな環境でパフォーマンスや信頼性に問題が発生した場合に、新プラットフォームから旧プラットフォームへのロールバックを可能にすることで、移行リスクを最小限に抑えます。
- 物理サーバー、ハイパーバイザー、クラウドにわたる一貫したバックアップ、リカバリ、監査管理により、コンプライアンス態勢を向上させます。
- アプリケーションとデータをクラウドにレプリケーションすることで、ディザスタリカバリ態勢を強化します。
- クラウド上のバックアップをスキャンしてマルウェアおよび未修正の脆弱性を検出し、リカバリ作業に先立ってリスクを軽減します。
- ベンダーロックインを回避し、必要に応じてワークロードを新たなプラットフォームへ柔軟に移行します。ハイパーバイザーベンダーが更新費用やサポート費用を引き上げたといった場合にも柔軟に対応できます。

最適なソリューションは、これらの機能を単一の統合バックアッププラットフォームで提供することで、IT 関連ライセンス、トレーニング、統合、およびサポートにかかるコストの削減に貢献します。

新しいプラットフォームへの移行に潜む落とし穴

VMware から新たなハイパーバイザーへ移行するケースを見てみましょう。手順はシンプルです。仮想マシン（VM）をエクスポートし、新しいハイパーバイザー形式に変換して、新たなプラットフォームにインポートします。しかし、この移行手順の各ステップには、潜在的な課題やいくつものリスクが伴います。たとえば、仮想ディスク形式、チップセットのエミュレーションモデル、仮想ハードウェアのバージョン、ドライバスタック、ネットワーク仮想化層の相違などが挙げられます。VM テンプレート、スナップショット、および接続されたストレージボリュームの動作もそれぞれ異なります。互換性の問題は、ワークロードが本番環境で稼働するまで顕在化しないことがあります。

VMware からの移行を進めている顧客からは、VM の安定性低下、ネットワーク構成上の問題、変換後のパフォーマンス低下、さらに問題発生時に完全な切り戻しができないといった深刻な問題が繰り返し報告されています。ハイパーバイザー間の移行には、コスト増大や長時間のダウンタイムに発展する現実的なリスクを伴います。物理サーバー間の移行や、VM からクラウドへの移行など、その他のクロスプラットフォーム移行においても、同様のリスクが生じます。

ハイパーバイザーユーザーには多くの魅力的な選択肢がある

不満を持つ VMware ユーザーの出口戦略のケースを踏まえると、市場には検討に値するハイパーバイザーの選択肢が数多く存在します。

Microsoft Hyper-V/Azure Stack HCI
Windows/Azure 環境を採用している企業に適した選択肢であり、Active Directory や Azure セキュリティ、既存の Microsoft ライセンスと密結合されています。

Proxmox VE
透明性の高いライセンス体系、高可用性機能、活発なユーザーコミュニティを特徴とする、人気のあるオープンソースプラットフォームです。

Nutanix AHV
統合プラットフォームを通じて、仮想化、ストレージ、管理を効率化し、コストが予見しやすいサブスクリプションモデルを提供します。

Scale Computing HC3
シンプルな運用を重視し、小売業、製造業、分散マルチサイト環境といったエッジ環境向けに最適化されたハイパーコンバージドプラットフォームです。
その他の VM 環境として、Citrix XenServer、Red Hat Virtualization、Linux KVM などがあります。

しかし、VMwareからこれらの代替環境への移行、さらにあらゆるワークロードを新しい物理・仮想・クラウドプラットフォームへ移行するプロセスには、事前に想定し、対処すべきリスクが伴います。

適切なデータ保護ツールで移行リスクを軽減

プラットフォームの移行に着手する前に、企業は潜在的なリスクの軽減に役立つ適切なツールへの投資を検討する必要があります。たとえば、プラットフォームにとらわれないバックアップソリューションは、VMware から Hyper-V、Proxmox、Nutanix、Scale Computing への移行、あるいは物理サーバーやクラウドプラットフォームといったハイパーバイザー以外の環境への移行において、安全な橋渡しとして機能します。あらゆる環境間での復元を可能にする真の any-to-any バックアップソリューション、すなわち、あらゆるソースからワークロードを取得し、あらゆるデスティネーションに復元できるソリューション、すなわち 物理、VM、クラウドのいずれのプラットフォーム間でも自在に移行可能な仕組みは、困難で不安定な移行局面を、滑らかで確実な移行経路へと変えます。前述した VMware の例で挙げたように、多くの問題が発生し得ることを踏まえると、パフォーマンス、互換性、または運用上の問題が発生した際に、ワークロードを迅速に元のプラットフォームへ戻せる機能も不可欠です。

場合によっては、新旧のハイブリッド環境を数ヵ月間維持することで、移行リスクへの備えを強化できます。そのためには、さまざまな要因（ランサムウェア、人的ミス、ハードウェア障害など）によるデータ損失から保護する仕組みの導入が必要です。これにより、企業はコンプライアンス要件および法的なデータ保持義務を継続して満たすことができます。これらの保護対策には、ベンダーロックインを回避できるというメリットもあります。仮に新しいハイパーバイザー環境が長期的に最適でないと判断された場合でも、将来、別の代替環境へ安全に移行できます。

アクロニスは、旧環境からの移行をスムーズで安全なプロセスへと変えます。

こうした移行、たとえば VMware から別のハイパーバイザーへの移行を検討している企業に向けて、アクロニスは、そのプロセスをシンプル、高信頼で低リスク、かつ必要に応じて元の環境へ戻すためのツールを提供しています。Acronis Cyber Protect プラットフォームの移行機能と、必要に応じて利用可能な Acronis Professional Services の支援により、企業は次のようなメリットを享受できます。

- 移行時間を最大 60% 短縮できるオプションには、エージェントレスによる直接移行、オーケストレーションされた一括移行と監視、そして連続同期による増分移行があり、業務への影響を最小限に抑制。
- 移行前、移行中、移行後のすべての段階で完全な保護を確保する、ゼロデータ損失保証。
- 新しい環境への移行、バックアップ、継続的な保護を実現する統合プラットフォーム。
- 移行プロセス全体を通じてセキュリティ態勢を維持するサイバーセキュリティ検証機能。
- 移行後のデータ整合性を検証することによる品質保証。
- 企業固有の環境に合わせて、専門コンサルタントが設計するオーダーメイドの移行戦略。

Acronis Cyber Protect は、データ保護、サイバーセキュリティ、エンドポイント管理を単一のプラットフォームにネイティブ統合したサイバー保護を提供します。VMware移行専任のプロフェッショナルサービスチームとともに、アクロニスは導入時間を最大 60%（従来比） 短縮し、データ損失保証とカスタマイズした移行戦略を提供します。

移行プロセスを始めるには

1. Acronis Cyber Protect に登録して、完全な保護を始めましょう。
2. Acronis Professional Services の専門家による移行コンサルテーションをご予約ください。
3. 専門家のガイダンスのもとで移行し、リスクと業務への影響を最小限に抑えましょう。

移行完了後における新環境の保護

古い環境からの安全な移行を可能にするアクロニスのプラットフォームは、以下の表に示すように、新しい環境に対しても高度なバックアップとリカバリ機能を提供できます。

VMware に代わる主要ハイパーバイザー環境向けの、安全で信頼性の高いバックアップ

ハイパーバイザー	アクロニスのバックアップの主な機能
Microsoft Hyper-V	Hyper-V VMを、新規・ベアメタル・異機種ハードウェアを含む任意のシステムに、わずか数クリックでリカバリ。 Hyper-V バックアップを VM として実行することで、目標復旧時間（RTO）を短縮。
Nutanix	Windows および Linux VM 向けに、効率的で負荷の少ないエージェントレス保護を提供。Prism と完全統合されており、ゲストエージェント不要でオーバーヘッドを削減しつつ、Nutanix Ready Validation による一貫性のある信頼性の高いバックアップを実現。 Acronis Cloud、Nutanix Objects/Files、サードパーティのパブリッククラウドを含む柔軟なストレージオプション。 増分バックアップと重複排除機能により、ストレージコストを削減。 バックアップをスキャンしてマルウェアを検出し、リカバリ時の再感染を防止。 企業の成長や再編成に応じて、保護対象のワークロードを追加または削除できる拡張機能。 高度な暗号化、ロールベースのアクセス制御、データ不変性により、コンプライアンス遵守を支援し、データの不正利用から保護。 フルイメージおよびファイル単位の保護により、Nutanix AHV VM 全体をキャプチャ可能。必要に応じて特定のファイルやフォルダのみを選択して小規模・ターゲット型バックアップも実施でき、システム全体または個別アイテムの迅速な復元を実現。
Proxmox	Proxmox VM と LXC コンテナ向けに、効率的で負荷の少ないエージェントレスバックアップを提供。 ファイル単位のリカバリおよびシステム全体の復元に対応し、高速で細かなデータ保護を実現。 ローカルディスク、NAS デバイス、Acronis Cloud、S3 互換パブリッククラウドを含む柔軟なストレージオプション。 増分バックアップと粒度リカバリにより、バックアップ時間とリカバリ時間を短縮。 データ不変性、マルウェアスキャン、および FIPS 140-2 暗号化により、バックアップアーカイブの安全性とコンプライアンスを維持。 新しい VM やコンテナに自動適用可能な保護ポリシーにより、保護の抜け漏れを防ぎ、すべてのテストおよび本番環境を自動的にバックアップ。 VM とコンテナを、1 つのポリシーでまとめてバックアップ可能。
Citrix XenServer	XenServer ワークロードを、ディスクイメージ全体のバックアップで保護。VM 障害が発生しても、OS やアプリケーションの再インストールは不要。 XenServer VM バックアップは、ローカルディスク、NAS、SAN、テープ、Acronis Cloud など、最大 5 ヵ所まで柔軟に保存可能。
Red Hat Virtualization (RHV)	RHV の VM を、同じ VM または別の VM に数分で復元可能。 ドキュメント、ファイル、フォルダ、または VM 全体をバックアップから直接即座にリカバリ。 RHV VM のディスクイメージバックアップにより、新しいハードウェアへのベアメタル復元が可能。
Linux KVM	Linux KVM のバックアップ。Linux ホストはディスクイメージバックアップ、VM はエージェントベースのバックアップが可能。 単一の Web ベース管理コンソールから、すべてのローカルおよびリモート KVM ホストの保護を一元管理。

Acronis

詳細は以下をご覧ください。
acronis.com