

マイクロソフト社アーキテクチャによるハイブリッドクラウドの実現

Realization of Hybrid Cloud with Microsoft Architecture

田 川 和 史

要 約 2006年にパブリッククラウドのサービスが提供され始めて以来、クラウドコンピューティングは急速に発達しており、各社から多くのサービスが提供されサービスの拡充と機能強化が図られている。このクラウドコンピューティングの活用によりシステム更改負荷の軽減やシステムリソースの迅速かつ柔軟な調達などが実現されている。このようなクラウドサービスの利便性は受容しつつも、様々な要因からオンプレミス環境に構築されたシステムを並行して継続利用することが考えられる。クラウドのサービスを含む複数の環境を組み合わせる構成されるシステムをハイブリッドクラウドと呼ぶ。マイクロソフト社では、パブリッククラウドで提供しているサービスをオンプレミス環境でも使用可能とする Azure Stack HCI と Azure Portal を提供している。BIPROGY ではそれらの製品について仕様の確認と機能の検証を行った。

Abstract Since the provision of public cloud services began in 2006, cloud computing has developed rapidly. A lot of services has been provided, which leads to further expansion and enhancement of public cloud. The utilization of this cloud computing has realized the reduction of the system update load and the rapid and flexible procurement of system resources. While taking advantage of the convenience of cloud services, for various reasons it is possible to continue to use system environments built in an on-premises environment in parallel. A system made of multiple environments including the cloud service is called a hybrid cloud. Microsoft provides Azure Stack HCI and Azure Portal, which enable services provided in the public cloud to be used in an on-premises environment. BIPROGY confirmed the specifications and verified the functions of these products.

1. はじめに

2006年に Amazon Web Services がパブリッククラウドのサービスを提供し始めて以来、クラウドコンピューティングは急速に発達しており、マイクロソフト、Google、Oracle など各社からサービスが提供されている。このようなクラウドコンピューティングのサービスの進化と拡大を受けて、2010年ごろからクラウドファーストの言葉で表されるようなクラウドの利用を優先するシステムインフラの考え方が広がってきている*1。

クラウド利用には様々な利点があるが、多くの企業や団体ではクラウド利用の問題点のため、すべてのシステムのクラウド化には踏み切れず、オンプレミスを使い続けている。そこで、クラウドの利点を生かしながらオンプレミスなどの環境も併せて利用することでクラウドの問題点を補う、ハイブリッドクラウドというアーキテクチャも採用され始めている。

本稿ではマイクロソフト社のハイブリッドクラウド関連サービスを紹介し、BIPROGY 株式会社（以降、BIPROGY）が実施した機能検証について述べる。2章でハイブリッドクラウドの現状と課題を述べ、3章でパブリッククラウドである「Azure」を提供しているマイクロソ

フト社の取り組みを紹介し、4章で製品仕様の確認と機能検証について述べる。

2. ハイブリッドクラウドの現状

米国国立標準技術研究所（NIST：National Institute of Standards and Technology）より発行されている「The NIST Definition of Cloud Computing」によると、ハイブリッドクラウドは次のように定義されている。

「クラウドのインフラストラクチャは二つ以上の異なるクラウドインフラストラクチャ（プライベート、コミュニティまたはパブリック）の組み合わせである。各クラウドは独立の存在であるが、標準化された、あるいは固有の技術で結合され、データとアプリケーションの移動可能性を実現している。」^[1]

つまりハイブリッドクラウドは、クラウドを含む複数の独立したインフラ（パブリッククラウド、プライベートクラウド、オンプレミスなど）を結合してアプリケーションの稼働環境を構成するものであると捉えることができる。本章では、ハイブリッドクラウドの特徴、利点、課題について述べる。

2.1 ハイブリッドクラウドの特徴

ハイブリッドクラウドは異なるクラウド環境を組み合わせることで、柔軟性と拡張性が高レベルで実現でき、それは以下1)～4)のような特徴をもたらす。また、これらに利点を見出す以外にもハイブリッドクラウドを選択する理由を5)に挙げる。

1) セキュリティとコンプライアンス

セキュリティとコンプライアンスの要件を満たすために、データやアプリケーションを適切に配置できる。例えば、機密データはプライベートクラウドやオンプレミス環境に置き、パブリッククラウドは一般的なワークロードや非機密データに使用することが考えられる。

2) レスポンスとパフォーマンス

アプリケーションやワークロードに応じて最適な環境を選択することで、レスポンスとパフォーマンスの向上を実現できる。高レスポンスを求められるアプリケーションやデータはプライベートクラウドやオンプレミス環境で処理し、一時的なスパイクの処理はコスト削減のためにパブリッククラウドを利用することが考えられる。

3) データ管理と移行

特定のデータやアプリケーションを異なる環境に配置することでデータの保存やバックアップ・復元を容易に実現することができる。また、既存のオンプレミス環境のシステムからパブリッククラウドへの段階的移行過程として構成されることがある。

4) コスト効率

パブリッククラウドを利用することにより需要の変動に柔軟に対応できることや、複数の環境での適切なりソースの割り当てや費用の最適化によりコスト効率を高めることが考えられる。

5) ハイブリッドクラウドを選択する他の理由

各企業や団体がハイブリッドクラウドを選択する理由には、他に次のようなものがある。

- 自身が持つ重要情報を他者の環境に置くことが自身のセキュリティポリシーとして認められない。
- パブリッククラウドでは提供されるサービスのサービスレベルが提供ベンダーに依存しており、提供ベンダーの都合や障害によるサービス停止などの影響が問題となる。
- データ生成がオンプレミス環境で多く発生しクラウド環境にデータを連携した場合に通信コストが負担となる。また逆にパブリッククラウド環境から多くのデータを他の利用環境に連携する場合にエグレス通信^{*2}コストが負担になる。
- クラウド利用を開始する前に使用していたオンプレミス環境のソフトウェアの構造的制約や、クラウド環境で使用することでライセンスが高額になることに起因してオンプレミス環境を残す。
- オンプレミス環境で大規模なシステムを構築し利用していた場合など、すべてのシステムをクラウド化するリスクを軽減するために段階的にクラウド化する。その過程でハイブリッドクラウドとなる。

2.2 ハイブリッドクラウドの課題

様々な特徴や利点を持つハイブリッドクラウドは、一方で次のような課題も考えられる。

- 複数の環境のシステムを連携させるため、システム構成やネットワーク構成が複雑になり、設計や構築の負荷が高くなる。
- 複数の環境を運用することになるため、それぞれについて運用ノウハウや使用する運用ツールが異なり、運用を担う要員も多くなる。
- データとアプリケーションが複数の環境に分散して存在するため、セキュリティの管理が難しくなる。
- 複数の環境を連携して使用するため、ネットワークトラフィックが多くなる可能性があり、十分な帯域を確保するコストが高くなる。
- 従量制課金が多いパブリッククラウドのサービスと、初期費用と固定課金が掛かるプライベートクラウドやオンプレミスの環境を組み合わせるため、コスト管理が難しくなる。

3. マイクロソフト社のアーキテクチャ

パブリッククラウドサービスとして Azure を提供しているマイクロソフト社では、この Azure で提供しているサービスをオンプレミス環境でも使用可能とし、オンプレミス環境をシステム全体の一部として統一的に管理できるようにするための様々な新しい製品やサービスを提供している。これらの取り組みにより、2.2 節で挙げた課題について次のように軽減している。

- 設計や構築の負荷の軽減
設計負荷の問題は課題として残るが、Azure で提供されている各種構築ツールと同様のものを使用可能とし、構築時の新しいノウハウ習得の負荷を軽減している。

- 運用負荷の軽減
統一的な管理の仕組みの提供により、パブリッククラウドとオンプレミスの環境を個別に意識して運用する負荷を軽減している。
- データ管理負荷の軽減
3.2.2項で述べる Azure Arc 対応 SQL Server にて、SQL Server とデータベースを一元管理することにより負荷を軽減している。
- 通信コストの軽減
オンプレミスでの業務処理を増やすなど、クラウドとの通信を必要最小限にすることでコストを軽減することが考えられる。
- コスト管理への対応
3.1節で述べるオンプレミスサーバーの Azure Stack HCI の OS はサブスクリプション型の課金で提供されており、他の Azure サービスと同様のコスト管理ができる。

本章ではこれら Azure を中心に構成されるハイブリッドクラウドに関するマイクロソフト社の製品とサービスの主なものについて説明する。図1にパブリッククラウドからオンプレミス環境に至る Azure による管理範囲を示す。この図から Azure が旧来のメインフレームや UNIX を除く、多くのシステム環境を管理対象として網羅していることが判る。

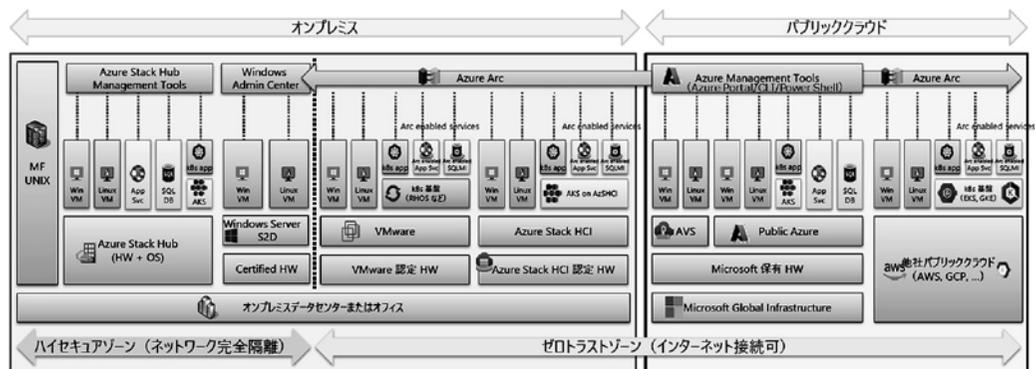


図1 Azure による管理範囲 (日本マイクロソフト社によるハイブリッドクラウド説明資料^[2]から抜粋)

3.1 ハイブリッドクラウドで利用できるオンプレミス環境の製品とサービス

オンプレミス環境では、従来の一つのサーバーに一つの OS を稼働させる形態から、サーバーリソースの有効活用のため一つのサーバーで複数の OS を稼働させる仮想化が一般的になっている。この仮想化の基盤として HCI (Hyper Converged Infrastructure) と呼ばれるサーバーの構成方法が拡がりつつある。

図2に HCI サーバーの構成の概要を示す。図に示す通り HCI サーバー構成では各物理サーバー内のストレージを仮想化し Hypervisor 上で仮想マシン (VM: Virtual Machine) を稼働させることができる。この仮想化により利用者は物理的なサーバーを意識することなく VM を使用することができる。

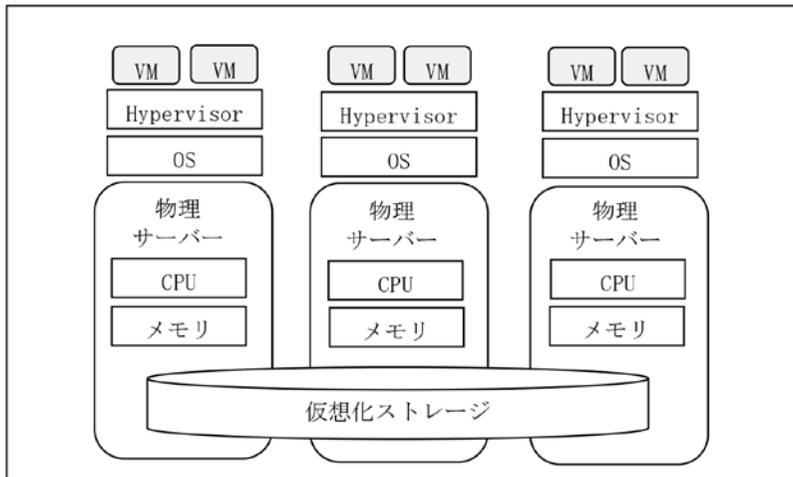


図2 HCI サーバーの構成概要

マイクロソフト社では従来からオンプレミス環境を構成するサーバー OS として Windows Server の提供を行ってきた。加えて、2020 年より HCI サーバー専用の OS をリリースするとともに、各 HW（ハードウェア）ベンダーが提供する HCI サーバーを認定 HW としている。この HCI サーバーを Azure Stack HCI と呼ぶ。他社の HCI サーバーと比較した場合、パブリッククラウドである Azure と親和性が高く、そのパブリッククラウドの各サービスにオンプレミス環境をシームレスに取り込むことができるのが特徴である。マイクロソフト社のハイブリッドクラウドのアーキテクチャでは Windows Server を含んだ構成も管理でき、Azure Stack HCI を使用した場合には Azure Stack HCI およびその仮想環境上の VM についても Azure 上で統一的に管理することができる。Azure Stack HCI に対してはオンプレミスの運用管理ツールとして Windows Admin Center が提供されており、Azure Stack HCI サーバーの管理や Azure Stack HCI 上で稼働する VM の管理を実施できる。

3.2 パブリッククラウド Azure 提供サービス

本節ではハイブリッドクラウドを実現するパブリッククラウド Azure の主な製品とサービスについて説明する。マイクロソフト社のハイブリッドクラウドへの取り組みとしては、Azure で提供しているサービスの対象範囲をオンプレミス環境に拡大することで、パブリッククラウドとオンプレミス環境の運用管理を統一し、運用管理負荷の軽減を目指しているものと考えられる。なお記載のサービスや機能にはリリース状況が preview のものが含まれる。

3.2.1 Azure Portal

Azure Portal はコマンドラインツールに代えて使用できる Web ベースの統合コンソールであり、グラフィカルユーザーインターフェイスを使用して、Azure の各サービスの設定・管理・運用を行うことができる。Azure Stack HCI の管理ツールである Windows Admin Center の機能を Azure Portal から利用できるように機能拡張を図っている。

3.2.2 Azure Arc

Azure Arc は Azure の無償の PaaS であり、オンプレミス環境や他社のパブリッククラウドを Azure と接続するゲートウェイと位置付けられ、マイクロソフト社のハイブリッドクラウドにおける中核のサービスである。このサービスの特徴として次の機能が挙げられる。

- Azure Arc 対応サーバー
物理、仮想、クラウドを問わず各環境で稼働するサーバーを Azure Arc 対応サーバーとし、統一的に管理・運用できるようにするエージェントを提供している。
- Azure Arc 対応 SQL Server
Azure Arc を使用すると、Azure を単一制御ポイントとしてすべての SQL Server を管理でき、Azure に接続された SQL Server とデータベースの詳細なインベントリを 1 か所に表示できる。
- Azure Arc 対応 Kubernetes
Azure Arc 対応 Kubernetes を使用すると、任意の場所で実行されている Kubernetes クラスタを Azure で構成および管理できる。

3.2.3 関連する Azure サービス

マイクロソフト社のハイブリッドクラウドでは、プライベートクラウドやオンプレミス環境をパブリッククラウドと統一的に管理・運用するためのパブリッククラウドのサービスを拡張し提供している。その中の代表的なサービスを以下 1) から 6) に挙げて説明する。

1) Azure Monitor (Log Analytics & Insight)

Azure Monitor は、クラウド環境とオンプレミス環境からのテレメトリを収集し分析するための包括的な監視ソリューションであり、統合監視とアラートの機能を提供する。Azure Monitor によりアプリケーションおよびサービスの稼働状況の監視や、ログの監視なども実現できる。

2) Microsoft Defender for Cloud

Microsoft Defender for Cloud は、クラウドネイティブアプリケーション保護プラットフォーム (CNAPP : Cloud Native Application Protection Platform) である。さまざまなサイバー脅威や脆弱性からクラウドベースのアプリケーションを保護するように設計された一連のセキュリティ対策とプラクティスを備えており、その機能範囲をオンプレミス環境まで拡げている。また Microsoft Defender for Cloud では、クラウドセキュリティ態勢管理 (CSPM : Cloud Security Posture Management) ソリューションやクラウドワークロード保護プラットフォーム (CWPP : Cloud Workload Protection Platform) の機能が組み合わされて提供されている。

3) Update Management Center

Update Management Center は、すべてのマシンの更新プログラムの管理のための統合サービスであり、単一の Azure Portal から、Azure、オンプレミス、その他のクラウドプラットフォームのデプロイ全体で Windows と Linux の更新プログラムのコンプライアンスを監視する。その更新はリアルタイムで行うか、定義されたメンテナンス期間内にスケジュールするかを設定できる。

4) Backup Center/Site Recovery

Backup Center/Site Recovery は、単一の Azure Portal より各環境のバックアップの採取指示や管理の機能と、バックアップするデータソース（VM やデータベースなど）の他の環境を使用してのリカバリの機能を提供する。これにより災害対策とデータ保護を実現している。

5) Azure Automation

Azure Automation のインベントリと変更管理機能により、Azure やオンプレミスなどのクラウド環境でホストされている仮想マシンの変更を追跡することで、配布パッケージマネージャーによって管理されているソフトウェアの状況を知ることができる。

6) Azure Policy

Azure Policy はすべての Azure リソースと、Azure Arc 対応のリソースに対して、リソースの整合性、規制コンプライアンス、セキュリティ、コスト、管理のガバナンスのポリシー定義を統一的に適用できる。

4. 製品仕様の確認と機能検証

BIPROGY ではハイブリッドクラウドを活用するための Azure の新しいサービス・拡充されたサービスについて、事前に日本マイクロソフト社から提供を受けた製品仕様の情報^[2]を基に想定していた機能の検証を行った。この検証では、Azure Stack HCI を Azure Arc に接続し、次に挙げる各サービスの動作について確認するとともに、構築ノウハウを獲得することもできた。本章で一部を紹介する。

【確認したサービスの動作】

- Azure Stack HCI 上の VM 操作
- Azure Monitor による Azure Stack HCI の監視
- Microsoft Defender for Cloud による Azure Stack HCI へのセキュリティ機能の提供

【獲得した構築ノウハウ】

得られた構築ノウハウとしては次のものがある。

- Azure Stack HCI の Azure Arc への接続
- Azure Stack HCI 上の VM への Arc 対応サーバーエージェントの適用および、Azure Arc を経由した Azure Portal からの操作環境の設定
- Azure の各種サービスの Azure Stack HCI およびその仮想環境上の VM への展開

なお、この検証については次の点に留意いただきたい。

- 検証対象の Azure サービスの内容や画面イメージは検証時のものであり、その後のサービスの改訂により現在のものとは異なる場合がある。（サービスのリリースが preview のものを含む）
- 検証作業は Azure Stack HCI をエミュレートした環境で実施している。
- Azure Arc の検証した機能のすべてではなく一部を紹介している。
- 記載している検証の範囲を図 3 に太枠で示す。Azure のサービスである Azure Arc ならびに Azure Stack HCI と、Azure Stack HCI 上で稼働する VM を範囲としている。

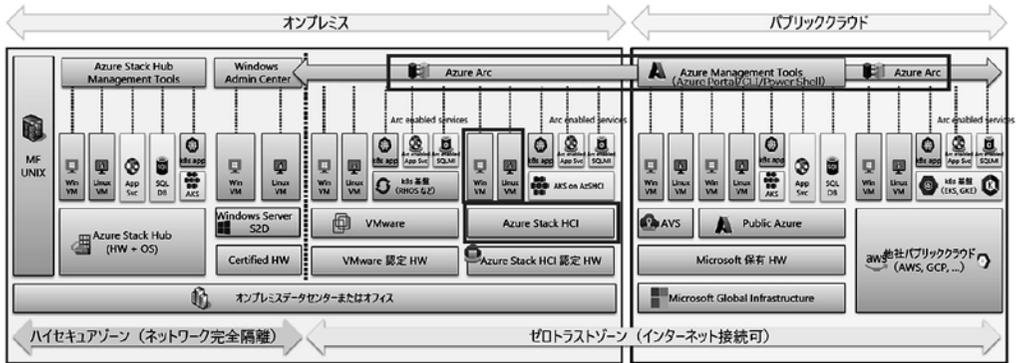


図3 検証の範囲

4.1 Azure Arc 対応サーバー

図4に Azure Stack HCI 上の VM の Azure Portal 上での表示例を示す。Azure Arc 対応サーバーを使用することで Azure Portal から VM の停止や起動、ディスクやリソースサイズの編集ができる。このようにオンプレミスサーバーである Azure Stack HCI 上の VM であっても、Azure 上の VM とほぼ同様の管理性を提供している。



図4 Azure Arc 対応サーバーの表示

4.2 Azure Monitor

図5に Azure Monitor を使用した Azure Stack HCI の監視について Azure Portal 上での表示例を示す。オンプレミスサーバーである Azure Stack HCI のクラスターの稼働状況について監視できる。また、図6に Azure Arc に接続した VM の稼働状況について Azure Portal 上での表示例を示す。Azure 上の VM と同様にオンプレミス環境の VM の状況を把握することができる。このように各環境のリソースの状況を Azure Portal から確認でき、またその他に各環境で採取されたログも評価することができる。



図5 Azure Stack HCI の監視



図6 オンプレミス環境のVMの監視

4.3 Arc 対応サーバーでの Microsoft Defender for Cloud

Microsoft Defender for Cloud は、名称に for Cloud とあるが、その対応範囲は他社のパブリッククラウドやオンプレミスサーバーに及んでいる。その機能はセキュリティ対策状況の評価、脅威や問題点の検出、あらゆるログの記録とレポートである。また、リソースを自動的に保護することもできる。

図7に Microsoft Defender for Cloud のインベントリにある Arc 対応サーバーの表示例を示す。図7の太枠にある通りリソースごとに推奨事項やアラートが確認でき、この推奨事項からどのようなアクションをとるべきかなどを確認できる。



図7 Microsoft Defender for Cloud のインベントリ表示

5. おわりに

本稿ではマイクロソフト社のアーキテクチャを中心に、ハイブリッドクラウドの現状および課題とその対応について整理した。マイクロソフト社ではパブリッククラウドである Azure とオンプレミスの環境および他のパブリッククラウドの環境を統一かつ一元的に管理できるようにサービスの向上と拡大を図っている。同様の取り組みは他のパブリッククラウドベンダーにも見受けられ、今後それぞれの特徴を活かした選択が可能になるものと考えられる。

ビジネスの領域ではサービス提供のリードタイムの短縮が望まれ、スピード感があり柔軟で堅牢な IT インフラが求められている。BIPROGY グループでは様々な IT インフラの要望に応え、パブリッククラウドやオンプレミスサーバー、本稿で紹介したハイブリッドクラウド、オンプレミス相当の VMware 仮想化環境を Azure 上で構成する AVS (Azure VMware Solution) など、様々なシステムを提供している。

今後も日々進化する技術やサービスについて、BIPROGY グループ内での機能検証を継続的に実施することでノウハウを獲得し、顧客の要望に応じていきたい。

最後にハイブリッドクラウドの機能検証を支援いただいたサポートサービス本部の皆様、プラットフォームサービス本部の皆様に、この場を借りて深く御礼を申し上げます。

- * 1 このような考えが広がる理由としてクラウド利用における次のような利点が挙げられる。
 - ・ 一般に 5 年に一度要求されるシステム更改コストを低減できる。CAPEX (CAPital Expenditure: 資本的支出) の OPEX (Operating Expense: 運営費) 化と称されるもので、クラウド利用では HW の購入が不要である点が寄与している。
 - ・ 柔軟なシステムリソースを迅速に獲得できる。オンプレミス環境ではシステムリソースの調達にはサーバー購入に伴いリードタイムがかかるが、クラウド利用では数クリックで調達でき、欲しい量を好きなタイミングで調達できる。
 - ・ 運用負荷を軽減できる。クラウド利用では HW を所有しないことによりその運用・維持・管理の負担が不要である。
- * 2 パブリッククラウド内部から外部への通信を意味している。一般にパブリッククラウド外部から内部への通信はコストがかからないことが多いが、内部から外部への通信では通信量に応じた従量制のコストが発生することが多い。

- 参考文献 [1] Peter Mell, Timothy Grance, 独立行政法人情報処理推進機構 (翻訳), 「NIST によるクラウドコンピューティングの定義 米国国立標準技術研究所による推奨」, National Institute of Standards and Technology, 2011 年 9 月, <https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000025366.pdf> (2023 年 7 月 19 日確認)
- [2] 日本マイクロソフト社によるハイブリッドクラウド説明資料 (非公開), 2022 年 4 月。

執筆者紹介 田川 和 史 (Kazushi Tagawa)

1992年日本ユニシス(株)入社。自社メインフレームの運用管理ソフトウェアを担当。その後、研究職を経て2017年より Azure をベースとした IoT ソリューションを担当。2020年より Azure Stack のビジネス化に従事。

