高可用性と独立性を実現する次世代クラウド・プラットフォーム

これからのクラウド・プラットフォームは、大きく変わっていきます。いままでは、サーバー、ネットワーク、ストレージ、セキュリティー機能を搭載したIaaS（Infrastructure as a Service）と、その上で動作する PaaS（Platform as a Service）を提供することが、すなわちパブリック・クラウドでした。「IBM Cloud」では、IaaS/PaaSに加え、データ・サービスやIBM Watsonに代表されるAIを支えるプラットフォームを構築し、さらに、高可用性を実現するアベイラビリティ・ゾーンや、お客様専有環境を担保し独立性を実現するパブリック・アイソレーションなどの新しいコンセプトが加わってきています。

本稿では、次世代クラウド・プラットフォームを理解することで、今後のクラウド戦略のヒントをお伝えします。

1. 次世代クラウド・プラットフォームの必要性

IT業界は日進月歩でテクノロジーが進化し続けています。このことは大きなメリットをもたらす反面、今日まで動いていたアプリケーション（以下、アプリ）や作成済みのデータなど、過去の資産を使えないものにしてしまう可能性があります。アプリやデータを変更することなく長期間にわたって安心して使用できるようにするためには、アプリが稼働するためのプラットフォームを十分に考慮して設計することが鍵となります。IBMは過去、System 360ホスト・コンピューター・プラットフォーム、AS/400オフィス・コンピューター・プラットフォーム、IBM パーソナル・コンピューター・プラットフォーム、Power System UNIXコンピューター・プラットフォームを生み出してきました。そして現在、これからのクラウド時代に向けて、IaaS/PaaS、データ・サービス、そしてAI（人工知能）を支える次世代クラウド・コンピューター・プラットフォーム「One IBM Cloud Architecture」を提唱しています（**図1**）。

このOne IBM Cloud Architectureは、クラウド・プラットフォームへの適用のみを考えているわけではありません。お客様要件によっては既存サーバー（オンプレミス）の活用が必要なケースもあります。オンプレミスを採用しているお客様には、One IBM Cloud Architecture

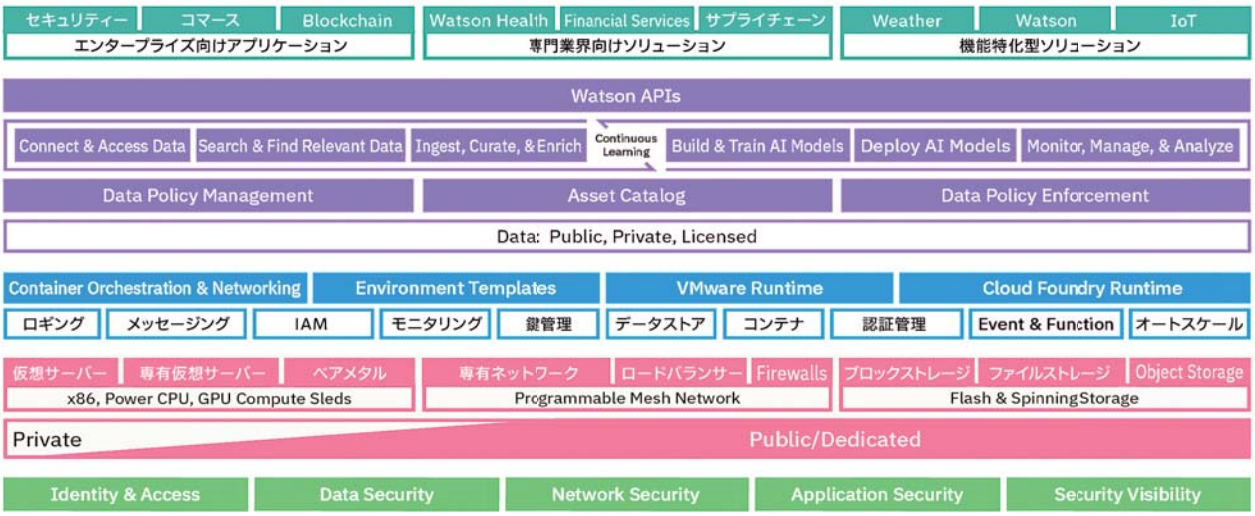

図1. One IBM Cloud Architecture

のコンセプトを基に作られた「IBM Cloud Private」(以下、ICP)、「ICP for Data」、「IBM Watson Assistant for ICP」などのソフトウェア製品群を提供しています。これにより、一度開発したアプリをクラウド上でも既存サーバー上でも、そして他社のパブリック・クラウド環境でも、長期間にわたって動作させることができます。またプラットフォーム部分を構成するテクノロジーに大幅な革新があったとしても、お客様アプリのAPIの互換性を保持することで、アプリへの影響を最小限にできます。

2. リージョンとアベイラビリティ・ゾーン

IBM Cloudには、「リージョン(Region)」と「アベイラビリティ・ゾーン(Availability Zone:AZ)」(以下、ゾーン)のコンセプトが取り入れられています。リージョンはその名のとおり"地域"という意味で、ゾーンは地理的に独立した"データセンター"のことです。東京リージョンは、ゾーンを3つ組み合わせた形になり、「マルチ・ゾーン・リージョン(Multi Zone Region: MZR)」と呼びます。

MZRは全世界で最初は6つのリージョンに構築されており、アメリカ大陸はダラスとワシントンD.C.、ヨーロッパはロンドンとフランクフルト、そしてアジアは東京とシドニーです。全世界6カ所のMZRは3つのゾーンでアプリを同時稼働させることで理論的には99.999%の高可用性(High Availability:HA)を実現できますが、さらにMZRを2ペアで組み合わせることで超高可用性構成もデザイン可能になります。なお、一つのリージョンに一つのゾーンの構成は、「シングル・ゾーン・リージョン(Single Zone Region:SZR)」となり、One IBM Cloud Architectureの機能を限定的に提供します。

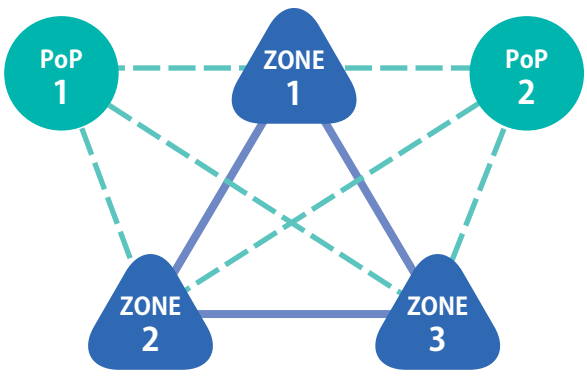

図2. MZRの構成

図2はMZRの構成を示しています。3つのゾーンは相互に接続され、それぞれのゾーンはネットワーク・アクセス・ポイントであるPoint of Presence(PoP)に接続されています。この図では点線が物理接続、実線が論理接続を示しています。この構成により、一つのゾーン、または一つのPoPが停止しても、リージョンとして動作継続が可能な高可用性が実現できるデザインになっています。

次章では、MZRのゾーンの組合せによって東京リージョンでも実現される高可用性の詳細について説明します。

3. MZRが実現する高可用性

3-1.高速ネットワークと高稼働率

高可用性を実現する方法として、アプリを同時に複数データセンターで動作させることが考えられます。この際に重要になってくるのが、データセンター間ネットワークです。ゾーン間ネットワーク速度は1.2Tbit/sのダークファイバー接続を4本組み合わせた構成となっており、今後増加するクラウドネイティブ・アプリが必要とする通信速度にも十分耐えうる設計になっています。ゾーン間の距離は厳密に60km未満に設計されていますが、これはゾーン間通信遅延を2ミリ秒未満にするためです。この遅延時間は、実際には地理的に離れた3つのデータセンターが、一つのデータセンター上でアプリが稼働しているのと同じ要件を満たすための条件となっています。

また、アプリを複数同時稼働させることのみならず、複数台のサーバー、ネットワーク、ストレージを組み合わせて稼働率を上げることでも高可用性を実現できます。一般的なPCサーバー技術やネットワーク技術でのアプリ稼働率は99.5%と言われています。これは1日に換算すると約7分間の停止を意味します。今後クラウド・プラットフォームは、より高可用性が求められるようになります。単体で稼働率99.5%のシステムを2カ所で動作させれば99.75%、3カ所で動作させれば99.99%(Four 9s)となります。これに仮想環境の高可用機能を組み合わせて99.999%(Five 9s)まで上げることができます。MZRを使うことで、今までよりも容易に99.99%や99.999%

の稼働率を実現するシステムがデザインできます。

MZRを活用した高可用性を実現する例として、コンテナ・アプリ実行環境であるKubernetesを3つのゾーンにまたがるクラスターとして構築した場合の例を**図3**に示します。

3-2. MZRで稼働・利用可能なPaaSサービス群

IBM Cloud Public（旧Bluemix）で利用可能なPaaSサービスは、従来では可能な限りデータセンターをまたぐようにサービスが配置されていましたが、リージョンによっては必ずしもそのようになっていませんでした。そのため、稼働率を高めるために利用者側で複数のリージョンにサービス・インスタンスを作成し、ロード・バランサーを用いて稼働中のリージョンで要求を処理するようにする必要がありました。

今後は、PaaSサービスをMZR内の3つのゾーンで稼働させ、組み合わせて一つのサービスとして利用できるようになることで、MZRで提供されるサービスはゾーンをまたがった高可用性構成のサービスとして利用できるようになります。また、One IBM Cloud Architectureに基づく次世代プラットフォームでは、基本的なサービスはすべてのリージョンで同じように稼働し、利用できるようになります。

なお、各リージョンで利用できようになるのは主にクラウドネイティブ・アプリケーションを構成するために必要となるPaaSサービスで、**表1**に含まれるサービスが第一弾として近々稼働する予定です。また、これらに続いてIBM Watson関連サービスも順次利用可能となる予定です。

4. 次世代クラウド・プラットフォームがもたらす独立性

パブリック・クラウドは、物理的リソースを共有使用することでシステム使用率を上げるのが最初の目的でしたが、お客様によっては専有の（Dedicated）環境を望まれる場合があります。高可用性要件と同じく、このようなクラウド環境でのお客様独自の独立性（Isolation）の要件も高まっています。

従来では、VLANによるプライベート・ネットワークの構築や、専有ベアメタル、独立したVMware環境などの物理サーバーによって、独立性を担保してきました。次世代クラウド・プラットフォームでは、従来の手法に加え、新たに仮想サーバー技術によるバーチャル・プライベート・クラウドや、PaaSとの専有接続を行うパブリック・アイソレーションにより、インフラストラクチャーからアプリケーションやデータまでお客様システムを構成するすべてのスタックで、さらなる独立性を実現していきます。

4-1. バーチャル・プライベート・クラウド

お客様専有環境を実現する手段として、上述のとおり従来ではネットワーク・レイヤーでのユーザー分離を行うVLANという仮想的なLANセグメントを作る技術が

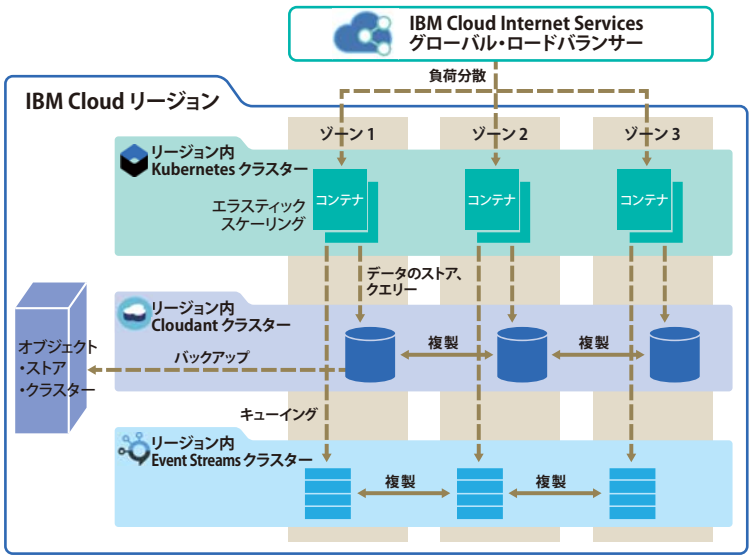

図3. MZRを活用した高可用性システムの構築例

表1. IBM Cloudリージョンで利用可能な主なPaaSサービス
（第一弾として予定される主要なサービス）

サービス名	機能
Kubernetesサービス	コンテナ・アプリケーションの実行環境・オーケストレーション
Container Registryサービス	コンテナ・アプリケーションのイメージ管理
Functionsサービス	イベント駆動型アプリケーションの実行環境
Event Streamsサービス	メッセージング
Continuous Deliveryサービス	継続的デリバリー（ツールチェーン）
AppIDサービス	ユーザー認証
Push Notificationサービス	プッシュ通知
Cloudantサービス Composeデータベース・サービス	データベース
API Connectサービス	API管理

用いられていましたが、この方法はハイブリッド接続を行った場合、クラウド・システムで使用しているIPアドレスとお客様システムのIPアドレスが衝突してしまう問題が発生します。これを柔軟に解決する方法として、バーチャル・プライベート・クラウド（Virtual Private Cloud:VPC）がIBM Cloudに今後搭載されます。

VPCは、パブリック・クラウドの中に仮想プライベート・クラウド環境を作成する技術です。イメージとしては、VLANで隔離されたパブリック・ネットワークの箱の中にVPCで隔離するプライベート・ネットワークの小箱を作るイメージです。このVPCの小箱は外側のVLANの箱からはネットワーク・アドレス的に切り離されます。つまり、VPCの小箱はアプリが動作するアイソレーション環境を提供します（**図4**）。そして、パブリック・クラウドの中にプライベート・クラウドを作るため、費用対効果についても今までの専有環境と比較して優れたものになります。

今後の計画としては、VPC空間とVLAN物理空間をつなげるVPC Peering技術などが検討されています。新しいプライベート環境であるVPCと、VLANで管理されている物理サーバー（ベアメタル）やその他の機能とで通信できるようになります。

4-2.パブリック・アイソレーション

4-2-1. エンタープライズ向け専有環境のコンセプト

パブリック・クラウド上でのPaaS環境ではIBM Cloud Public（以下、Public）が利用できますが、セキュリティー要件が高度でカスタマイズが必要なお客様は、IBM Cloud Dedicated（以下、Dedicated。旧IBM Bluemix Dedicated）を通じ、プライベート・クラウドであるPaaS専有環境が利用可能です。Dedicatedは他のPublicとは別に、任意のIBM Cloudデータセンター上でお客様専有の独立したPaaS環境を稼働させるもので、お客様のビジネスにとって重要なアプリケーションの稼働が想定されます。

Dedicatedのネットワーク接続について、お客様データセンターからIBM CloudデータセンターへVPNや専用線を用いた接続が可能です。また、PaaS環境で利用できるサービスについて、必要に応じアラカルト・サービスの専有環境が利用できるほか、Publicのサービスをシンジケーションと呼ばれる仕組みを使って統合して使用することも可能です。このDedicated専有環境のコンセプトとなっているのは以下の4つの考え方です。

1. コンピュートの分離：お客様のワークロードが稼働するコンピュート環境（サーバー）は物理的に専有する
2. ネットワークの分離：ネットワーク環境を他テナントから分離する
3. データベースの分離：データベースを専有する
4. データの分離：データは他のテナントとは異なる固有の暗号鍵を用いて暗号化する

4-2-2. 次世代専有環境 パブリック・アイソレーションの概要

従来のDedicated環境では高い分離レベルを実現で

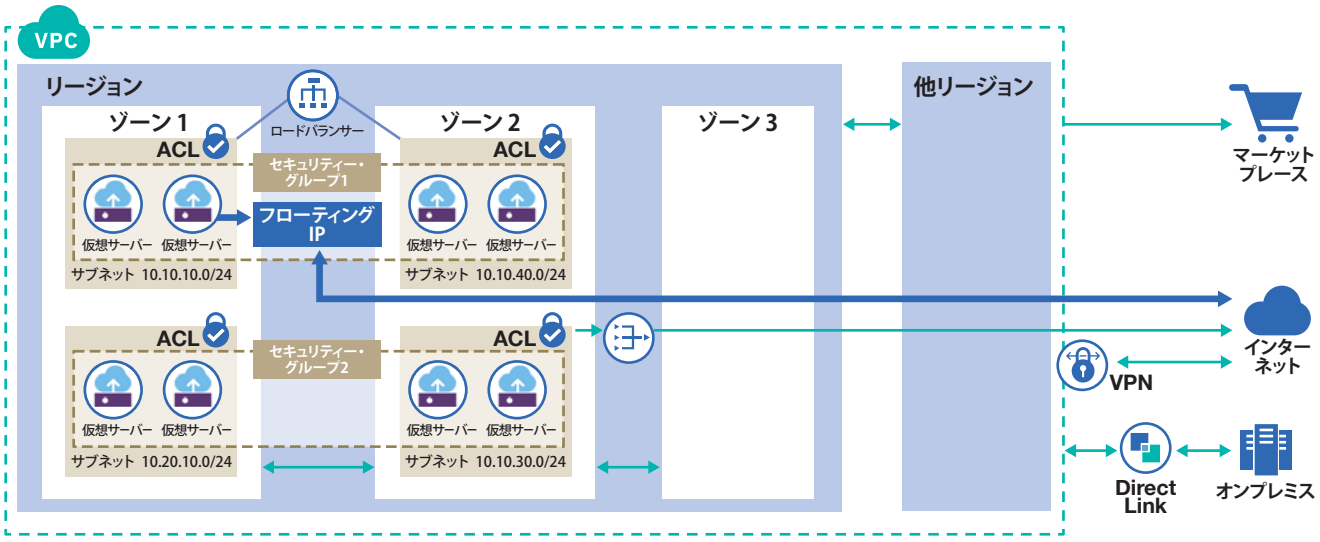

図4. VPCの構成イメージ

きる一方で、プライベート・クラウド環境をあらかじめ構築し独自で運用するため、パブリック・クラウドのメリットを十分に享受できません。中でも迅速に構築できる俊敏性、必要なリソースで稼働させる弾力性については、パブリック・クラウドと同じレベルで実現できることを多くのお客様が要望します。

Dedicated環境の良いところを生かしつつ、課題を克服するために役立つのがパブリック・アイソレーションです。パブリック・アイソレーションは、パブリック・クラウド環境内にお客様向けに専有し分離された環境を稼働するもので、次世代版のDedicated環境です。専有環境における4つのコンセプトに加え、パブリック・クラウドの特徴である俊敏性や弾力性を備え、お客様がセルフ・サービスで環境を構築できるという特長があります。パブリック・アイソレーションは**図5**に示したような構成となります。お客様アプリケーションが稼働するコンピュート環境はお客様専有のセキュアな環境で稼働し、それ以外のサービスはIBM管理の環境の中で稼働します。

コンピュート環境については、従来のCloud Foundryに変わり、Docker/Kubernetes環境を利用可能な「IBM Cloud Kubernetes Service」(以下、IKS)(技術解説「コンテナ・オーケストレーションでシステム・モダナイゼーションを加速する！」30ページ参照)が標準的な構成となります。IKSでは専有型の仮想サーバーを選択することでコンピュート環境を物理的に専有できます。また、クラウドらしい俊敏性については、オーダーしてから数十分程度で、仮想サーバー上で稼働するクラスターのコンピュート環境を構築できます。コンピュート環境はお客様専有のセキュアな領域内で稼働でき、将来的にはVPCの内部に配置できます。

サービスについては、実際に稼働する環境に加え、管理機能など一式を専有環境として用意する従来のアラカルト・サービスの稼働形態ではなく、Publicで提供するサービスの一部として利用する形態となります。これはIBMが管理するネットワーク領域で稼働するPublic環境と同じ領域で稼働することを意味します。ただし、アイソレーションを実現するために、各サービスがお客様専有のコンピュート環境で稼働できるプランを設定し、お客様専有のサービス・インスタンスを実現します。さらにパブリック・ネットワークを使用せず、IBM Cloudのプライベート・ネットワーク上のエンドポイントを利用できるオプションを選択することで、ネットワークの分離も実現します。お客様専有のサーバーで稼働できるプランとプライベート・エンドポイントを組み合わせて使用することで、専有環境のコンセプトを満たすことができます。データベースのサービスやその他の多くのサービスにおいてもこの専有環境が利用できるようになります。

データが格納されるストレージについては、インフラストラクチャー・サービスとして利用いただけるストレージ・サービスに加え、IBM Key Protectサービスを通じて、お客様が暗号鍵の管理を行う機能が実現されます。テナントごとの暗号化に加えて、お客様が自らの暗号鍵を管理することを可能とします。

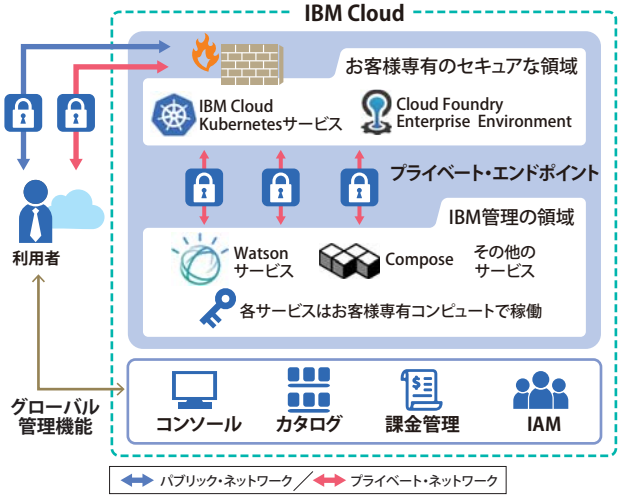

図5. パブリック・アイソレーションの構成例

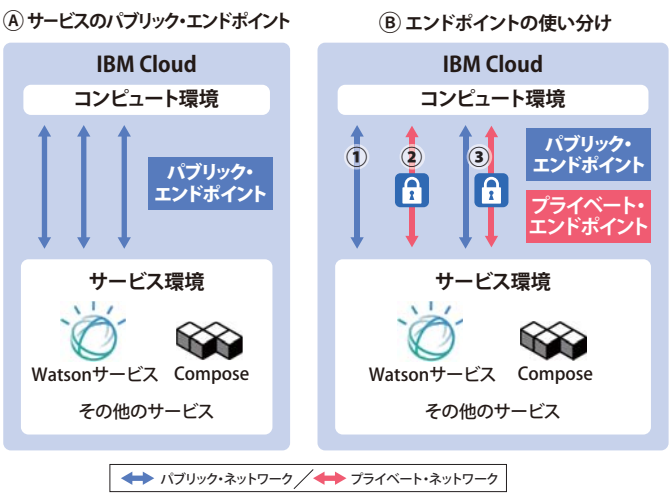

図6. サービスのエンドポイントへのアクセス

Dedicated環境は、フル・マネージドのサービスで、プラットフォームの構築・維持・運用についてはIBMが実施し、お客様はアプリケーションや業務データにかかる運用を中心に実施するという責任分界モデルとなっています。一方でパブリック・アイソレーションはセルフ・サービスを原則としており、インフラストラクチャー・サービスの部分を中心にお客様が構成要素を選択・構築し、その後の維持・運用をお客様の要件に合わせてお客様自身が実施できます。管理の観点で自由度が大きくなり、ベンダーによるマネージド・サービスに対する依存度を大きく低減できます。

4-2-3. プライベート・エンドポイントによるサービスへのアクセス

パブリック・アイソレーション環境において、サービスへの接続に関するネットワークの分離は、前述のとおりプライベート・エンドポイントにより実現されます。このプライベート・エンドポイントについて説明します。

以前からPublic環境で利用できたサービスにおいて、コンピュート環境からサービスを実行・管理するためのエンドポイントに対し、IBM Cloudのパブリック・ネットワークを経由してアクセスします（**図6Ⓐ**）。そのほか、あるサービスが別のサービスを利用している場合もIBM Cloudのパブリック・ネットワークを経由します。パブリック・ネットワークを経由したアクセスは、インターネットからアクセスできるあらゆるユーザー向けのサービスであり、アクセス元を細かく制御する機能を有さず、セキュリティーの厳しい要件を満たすことはできません。

専有環境のコンセプトの一つであるネットワークの分離を実現し、セキュリティーの高度な要求を満たせるのが、プライベート・エンドポイントです。プライベート・エンドポイントはIBM Cloudのプライベート・ネットワークを経由してサービス・エンドポイントへアクセスし、インターネットからのアクセスにかかる脅威の影響を受けなくなります（**図6Ⓑ** プライベート・エンドポイント）。そのほか、IBM Cloudのグローバル管理機能の一部であるIAMが有するリソースへの詳細なアクセス管理機能により、プライベート・エンドポイントへのアクセス権限を設定できます。

プライベート・エンドポイントを利用するためには、各サービス・インスタンスにおいて利用するエンドポイントを選択します。パブリック・ネットワーク経由でのアクセスの利用（**図6Ⓑ-①**）、プライベート・ネットワーク経由でのアクセスの利用（**図6Ⓑ-②**）、パブリック・ネットワークおよびプライベート・ネットワークをともに利用（**図6Ⓑ-③**）の利用形態のいずれかを設定します。

5. おわりに

今後もITの世界は、AIや量子コンピューターのような新しいテクノロジーの出現、ユーザーの価値観や要望要件の変化に対応していく必要があります。その変化を支えられるのが、今回紹介したように進化を続けるIBM Cloudです。お客様のビジネスに貢献できるよう、One IBM Cloudで真の価値を発揮していきます。

日本アイ・ビー・エム株式会社
IBMクラウド事業本部
次世代クラウド

伊佐治 一彦
Kazuhiko Isaji

1984年日本IBM入社。通信端末、通信機器、通信ソフトウェア製品の開発、ネットワーク・サービス事業、グローバル・プロセス・サービス事業にて、エンジニア、オペレーション・マネージメントに従事。2013年SoftLayer買収より現職。IBM Cloudのビジネス計画、選考支援、構築支援を通じて、日本での次世代クラウド・データセンター立上げをリード。

日本アイ・ビー・エム株式会社
IBMクラウド事業本部
Watson & Cloud Platform テクニカルセールス
シニア・テクニカル・スペシャリスト

古川 正宏
Masahiro Furukawa

2003年日本IBM入社。ソフトウェア開発製品の開発、サービス・デリバリー、テクニカル・セールスとして、各種開発製品を用いたソリューションに従事。2015年より現職。IBM Cloud PaaSを用いてお客様の新たなイノベーションを創出するためのソリューション設計を技術的にリード。