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!

「IBM Cloud Kubernetes Service」&「IBM Cloud Private」概説

かつてITシステムはバックオフィスに陣取るツールとして、ビジネスを支える脇役でした。デジタル・ビジネスたけなわの今、自動車配車サービスや宿泊施設仲介サービスを例に取るまでもなく、システムによって提供されるサービスがビジネスの主役になりつつあります。他社に先駆けてマーケットを開拓し、消費者のニーズにタイムリーに応えるには、システム開発のスピード・アップと、変更を許容する柔軟性が求められます。

本稿では、スピード・アップと柔軟性を実現するテクノロジーとして、コンテナとオーケストレーション・ツール「Kubernetes」(クバネティス)を解説し、IBMのソリューション「IBM Cloud Kubernetes Service」と「IBM Cloud Private」を紹介します。

1. クラウドネイティブ・コンピューティングの全体像

クラウド技術は、IT基盤の仮想化や構築自動化、Infrastructure as Code(コード化された構成情報に基づいた基盤構築手法)やImmutable Infrastructure(構築済みのサーバー構成は変更しないというコンセプト)などの手法を利用することで、デジタル・ビジネスに求められるスピードと柔軟性という2つの要件に応えてきました。また、マイクロサービス・アーキテクチャー(Microservice Architecture:MSA)(技術解説「マイクロサービス構築を始めるには」48ページ参照)やアジャイル開発を取り込むことで、アプリケーションの観点からもこの動きを加速しています。

MSAとは、アプリケーションを複数のソフトウェア・コンポーネント(サービス)で構成し、各サービスを独立した稼働環境で運用するソフトウェア・アーキテクチャーです(**図1**)。MSAでは各サービスの独立性が高いので、他のサービスの稼働を妨げることなく各サービスのメンテナンスを可能にする柔軟な構造を実現できます。また、アジャイル開発を採用することでアプリケーション開発のスピード・アップが期待できます。このようにMSAやアジャイル開発を活用して開発・運用されるアプリケーションをクラウドネイティブ・アプリケーションと呼びます。またクラウド基盤とクラウドネイティブ・アプリケーションから成るITのトレンドをクラウドネイティブ・コンピューティングと呼びます。

クラウドネイティブ・コンピューティングの普及を主導している業界団体が、Cloud Native Computing Foundation(以下、CNCF)です。CNCFは、クラウドネイティブとは「モダンで動的な環境の上でスケーラブルなアプリケーションを開発し運用すること」とし[1]、その中核のソリューションとしてコンテナ・オーケストレー

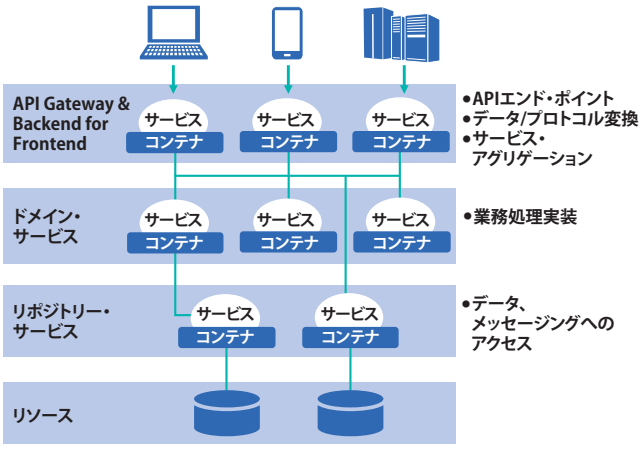

図1. マイクロサービス・アーキテクチャー構造例

ション・フレームワーク「Kubernetes」を開発していることで知られています。コンテナとは今脚光を浴びている仮想化技術です。なぜCNCFは仮想環境として長い歴史と数多くの実績を有すハイパーバイザーではなく、コンテナの利用を取り入れているのでしょうか。また、なぜコンテナ・オーケストレーションが必要なのでしょうか。

2. コンテナが選ばれる理由

コンテナとは仮想化技術の一つです。2013年3月、Docker, Inc.がDockerコンテナをリリース後、瞬く間にマーケットの支持を得て、今や主要な仮想化技術の一つと見なされています。

コンテナが受け入れられた理由の一つがコンパクトなサイズにあります。ハイパーバイザー型仮想化モデルにおいて仮想環境はOS、ミドルウェア、アプリケーションという3つのソフトウェア・スタックから構成され、仮想マシンのサイズは数GBに上ります。一方でコンテナ型仮想化モデルにおける仮想環境（コンテナ・イメージ）は、ミドルウェアとアプリケーションの2つから構成されます（**図2**）。コンテナ・イメージにはサイズの大きいOSが不要なので、数百MB程度のコンパクトなサイズに収まり、秒単位の高速なデプロイが可能となるのです。コンテナはデジタル・ビジネスに求められるスピード感に合った仮想環境と言えるでしょう。

コンテナのもう一つのメリットが、ポータビリティーです。コンテナの稼働環境であるコンテナ・エンジンはオープンソース・ソフトウェア（以下、OSS）としてさまざまなプラットフォーム向けに提供されています。コンテナ・エンジンによって、プラットフォームを越えてコンテナのポータビリティーが保証されるのです。またDockerコンテナでは、コンテナ上のソフトウェアのチューニングやアプリケーションの導入を定義する仕組み（Dockerfileとインストラクション）が備わっています。Dockerfileを活用することで、どのようなプラットフォームであっても、コンテナ上で同じ構成でアプリケーションを稼働させることが可能になります。

3. コンテナ・オーケストレーションの重要性

分散システムを本番環境として運用するには、可用性を考慮して複数のサーバー・プロセスからなるクラスターを構成します。クラウドにおいても、可用性要件を満たすために同様の対応が必要です。コンテナは、従来の分散システムのプロセスに相当するため、複数のコンテナからなるクラスターを構成し運用します。この時、各コンテナを個別に管理するのは手間がかかるだけでなく、作業ミスを誘発する可能性があります。そこで求められるのが、コンテナ・クラスターを統合管理するコンテナ・オーケストレーション・フレームワークです。

Kubernetesは、OSSのコンテナ・オーケストレーション・フレームワークの一つで、主要な大手クラウド・ベンダーがサポートを表明しています。オープン・スタンダードなコンテナとKubernetesは、ベンダー・ロックインを排除し、ユーザー企業の投資を保護します。

Kubernetesの源流はGoogle Inc.の社内プロジェクトで、その後2014年よりCNCF所管のOSSプロジェクトとして開発されており、2015年にバージョン1.0がリ

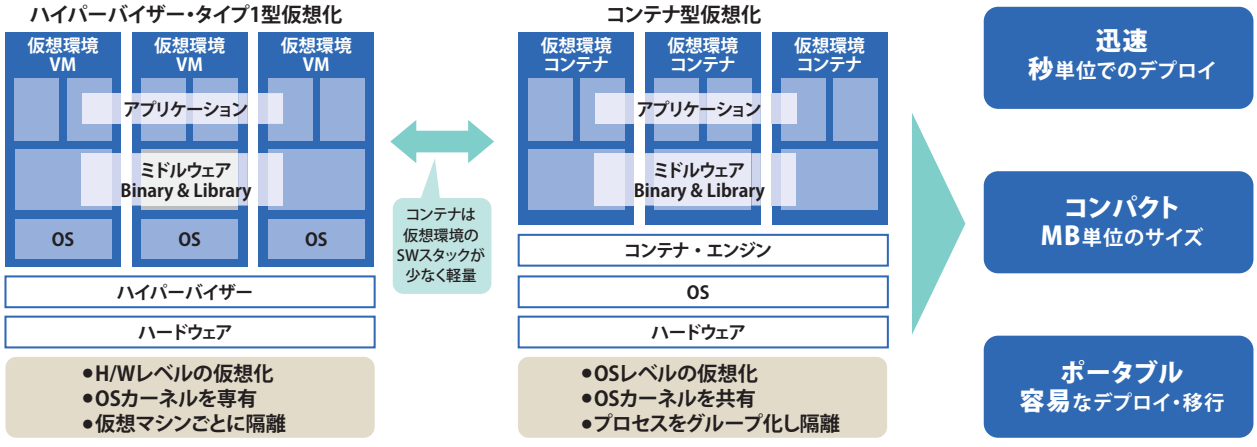

図2. コンテナ型仮想化とハイパーバイザー型仮想化の比較

リースされました。Kubernetesの出発点はコンテナ・クラスターの管理にありましたが、今や従来のOSのようにネットワーキングやリソースのスケジューリング、コンテナのパッケージ管理など、クラウド基盤上でシステムを運用する上で、不可欠な機能を提供するに至りました（**図3**）。Linux Foundationのエグゼクティブ・ディレクターJim Zemlin氏は、これを評して、「Kubernetes is becoming the Linux of the cloud」[2]（Kubernetesは、クラウドにおけるLinux、すなわちOSになりつつある）とツイートしています。単に仮想環境としてコンテナを採用するだけでなく、Kubernetesをコンテナの統合管理の基盤として使いこなすことが、クラウドネイティブ・コンピューティングを成功に導く上で重要なのです。

4. IBM CloudのKubernetesサポート ～IBM Cloud Kubernetes ServiceとIBM Cloud Private

IBMは、コンテナとKubernetesに早くから着目しコミットしてきました。IBMが提供するクラウド・ソリューションである「IBM Cloud」では、2015年にコンテナのサポートを開始しました。2017年5月には、Kubernetesマネージド・サービスであるIBM Cloud Kubernetes Service（以下、IKS）を正式にリリースし、2017年12月からは東京データセンターでも提供しています。

IBM Cloudは、IaaS/PaaS/SaaSの形態で170以上のサービス/APIを提供すると同時に、パブリック・クラウドからオンプレミスのお客様データセンターまでカバーするハイブリッド・クラウド・ソリューションです（**図4**）。パブリック・クラウドではIBM Cloud PublicのIKSが、オンプレミスのお客様データセンターではIBM Cloud Private（以下、ICP）が、Kubernetesクラスター上にデプロイされたコンテナ・アプリケーションをホスティングします。また、IKSとICPは、企業の基幹システムを支える信頼性の高いクラウド基盤を提供します。ここからIBM CloudのKubernetesサポート機能、IKSとICPの特徴を紹介します。

4-1. 豊富なサービスとAPI

IBM Cloudを利用すれば、IBM Cloudが提供するIBM Watson（AI）、ブロックチェーンなど先進的なサービスを利用して、素早く効率的にデジタル・ビジネス向けのシステム開発を始められます。例えば、AIを活用するときには、その前段階として学習データの整備や処理モデル構築にそれなりの手間と時間を要しますが、IBM CloudはAIの処理エンジンだけでなく、このような前段階の処理を効率化するサービスとして「IBM Watson Studio」（IBM Cloud Public上で稼働）と「ICP for Data」（ICP上で稼働）を提供します（技術解説「AI時代に求められるクラウド分析基盤と統合データ・プラットフォーム」54ページ参照）。これらのサービスを介してIBM CloudはAIシステム開発運用のライフサイクル全体を支援します。

また、RDBやメッセージング、Webアプリケーション

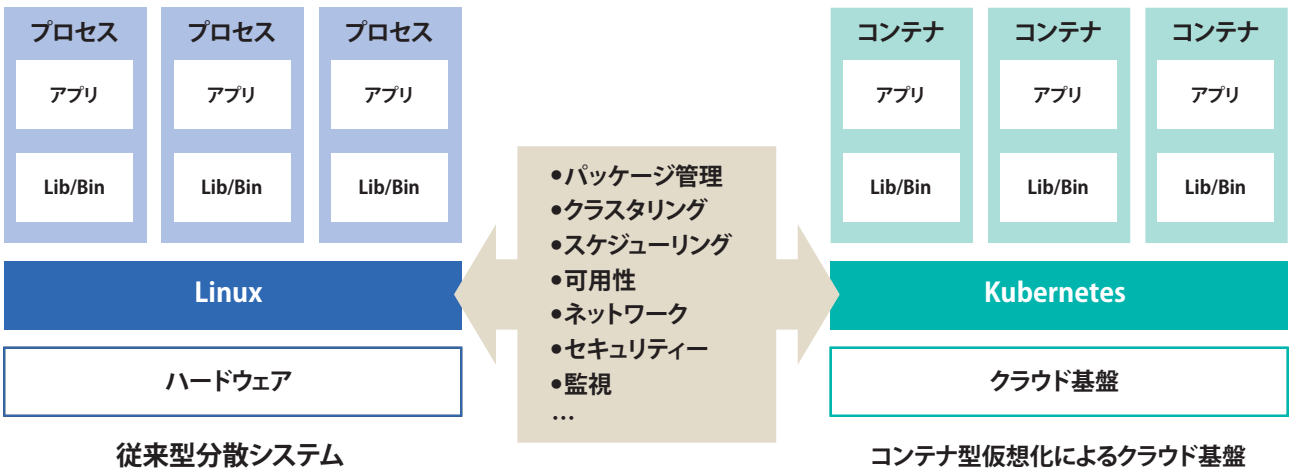

図3. Kubernetesの位置づけ

を活用した基幹システムをコンテナ化するには、実績のあるミドルウェアが必要になります。IBM Cloudは、「Db2」「WebSphere Application Server」(以下、WAS)「MQ」といったこれまで多くのミッション・クリティカル・システムで利用されてきたミドルウェアを、クラウド上でも提供します。IKSとICP上では、WASアプリケーションを動かし、Db2やMQを利用するという基幹システムのトランザクション処理を従来と同様の品質で実現することができます。

4-2. 高いパフォーマンスを誇るベアメタル

IBM Cloud Publicは、Kubernetesマネージド・サービス向けにベアメタル・サーバーを提供します。最大構成で28コアCPU、512GB RAM、2x2TB RAID1 Primary Disk、4x4TB RAID10 Secondary Disk 10Gbpsネットワークのモデルをラインナップし(2018年8月時点)、高速処理に長けたGPUを選択することも可能です。AIにおける機械学習やディープ・ラーニング、従来型の基幹業務等、CPUインテンシブ、メモリー・インテンシブ、大量データ処理といった高いパフォーマンス要件に応えることができます。

4-3. 可用性を高めるマルチ・ゾーン・リージョン

IBM Cloudデータセンターは、マルチ・ゾーン・リージョン(以下、MZR)をサポートします[3]。MZRとは、個別のデータセンター障害に耐えうるよう可用性を高める新たなデータセンター・モデルであり、電源やネットワークが物理的に独立した3つのデータセンター(アベイラビリティ・ゾーン。以下、ゾーン)と2つのPoint of Presence(PoP:ネットワーク・アクセス・ポイント)で一つのリージョンを構成します(技術解説「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」24ページ参照)。MZRでは、Kubernetesクラスターを異なる複数のゾーンにデプロイすることが可能です。万一個別のゾーンの障害が生じても、正常稼働している他のゾーンでサービスの提供を継続することができます。2018年11月時点で、MZRは東京リージョンでサービスを開始しています。

4-4. ハードウェアからコンテナ・イメージまで フル・カバレッジのセキュリティー脆弱性対応

コンテナ型仮想化においては、ベンダーやコミュニティーが提供するコンテナ・イメージを入手し、アプリケーションの導入などのカスタマイズを加えて利用することが一般的です。すなわち、第三者が作成したコンテナ・イメージを利用することになるため、オリジナルのコンテナ・イメージの信頼性の確認が非常に重要となります。IBM Cloudは、組み込み機能によって、コンテナ・イメージの信頼性の確認からハードウェア・レベルのセキュリティー上の脆弱性まで、フル・カバレッジでセキュリティーの脅威に対応します(**図5**)[4]。

IKSとICPは、コンテナ・イメージの保管・共有の場としてそれぞれのコンテナ・レジストリーを提供します。IKSのIBM Cloudコンテナ・レジストリーは、署名を介してコンテナ・イメージの提供元の確認と改ざん

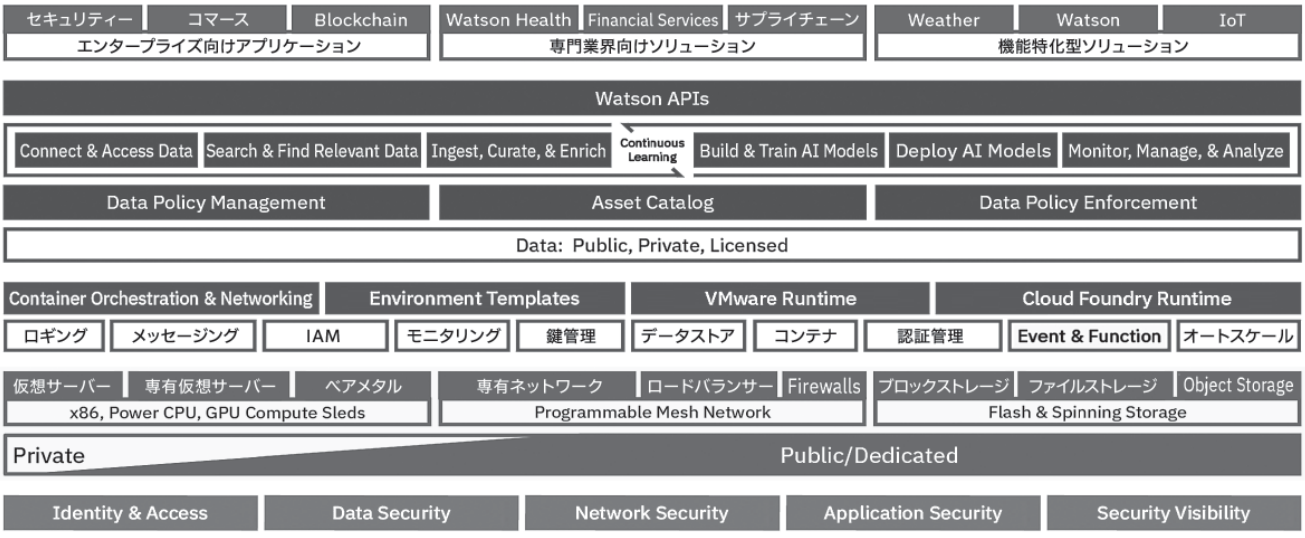

図4. One IBM Cloud Architecture

の有無をチェックする機能を提供します（**図5❶**）。また、IKSとICPでは、レジストリー内に格納されるコンテナ・イメージをスキャンし、脆弱性をレポートする機能を提供します（コンテナ脆弱性スキャナー、**図5❷**）。加えてKubernetesクラスター内で実行されているコンテナの状況を確認する機能も提供します。

さらにIKSでは、ストレージとして暗号化データ・パーティションを有するSSDを提供します。ベアメタル・サーバーを利用している場合には、組み込みのTrusted Platform Moduleチップが当該ノードの改ざんの有無を検証し、改ざんがないと判断された場合のみ、ベアメタル・サーバーを起動します（**図5❸**）。

4-5. コンプライアンス

現代社会では、法律や商習慣、企業倫理への対応から、さまざまな観点でレギュレーションの順守が要求されます。これを受けてITシステムには、セキュリティー対策に加えて、コンピューティング・リソースのロケーションや独立性も求められるようになってきました。例えば、プログラムが稼働しデータが保管される環境を国内データセンターに限定するだけでなく、共有環境（マルチ・テナント）ではなく専有環境（シングル・テナント）であることを求めるケースも出てきています。

このようなニーズに応えるために、IKSはKubernetesクラスターの専有環境として、前述のベアメタルと“仮想専有”を提供します（**図6**）[5]。マルチ・テナントは他のユーザーと共有するハードウェアの上でKubernetesクラスターをホスティングしますが、シングル・テナントの仮想専有とベアメタルではお客様専有のハードウェア上にクラスターをデプロイします。

仮想専有とベアメタルの違いの一つが仮想化層の有無です。仮想専有では、ハイパーバイザー上の仮想マシン上にKubernetesクラスターをデプロイしますが、ベアメタルでは仮想化層を介さず直接クラスターをホストします。仮想化層がない分、ベアメタルの方がより効率的にコンテナを稼働させることが可能です。コンプライアンス対応に加えて高いパフォーマンス要件をお持ちの場合には、ベアメタルが最適な選択肢です。

4-6. 柔軟な運用を実現するプライベート・クラウド

パブリック・クラウドを利用すればシステム基盤の定型的運用作業をクラウド・ベンダーに委ね、より戦略的な分野に投資をシフトすることができます。しかし、フィックス適用やサービスの計画停止がクラウド・ベンダーの規程に基づいて実施される可能性があり、必ずしもユーザー企業のニーズに完全に応えることはできません。またパブリック・クラウドではセキュリティーやロケーションなどレギュレーションに対応できない状況も考えられます。これらの懸念を払拭し、従来のオンプレミス・システムと同様の柔軟な運用を実現するIBMのクラウド・ソリューションがICPです。

ICPは、IBM Cloud Publicと共通のアーキテクチャーの下、KubernetesやCloud Foundryをサポートします。また、オンプレミス・データセンター内のVMwareやOpenStack、さらには「IBM Power Systems」、「IBM Z」（共にLinux）上に導入できるだけでなく、IBM Cloud IaaS、さらにはAmazon Web Servicesのようなほ以外のクラウドでも稼働します。

ICPはユーザーが、自身が保有する特権IDを利用して、導入し運用管理するクラウド・プラットフォームです。フィックスの適用やソフトウェアのバージョン・アップといった運用上のイベントは、ユーザー企業の都合に合わせて最適なタイミングで実施できます。ユーザー企業のビジネスに合わせて、柔軟で安全な運用を実施できるのがICPのメリットの一つです。

4-7. マルチクラウド管理

リーズナブルな価格設定から、気軽に利用できる点がクラウドの魅力の一つです。そのため部門ごとに異なる

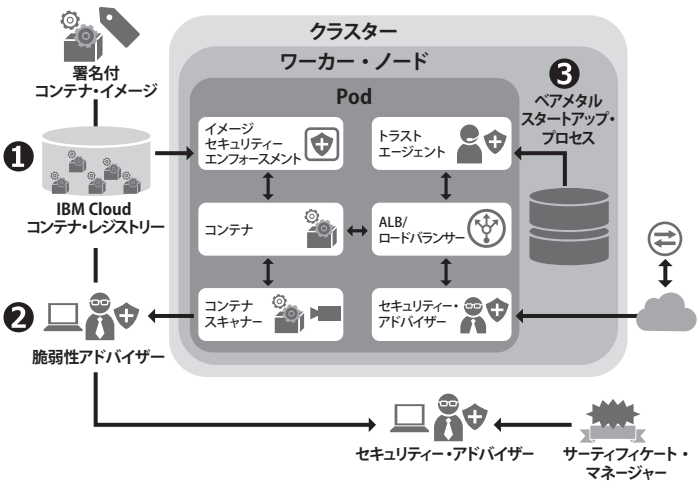

図5. IKSのセキュリティー脆弱性対応（一部ICPによる対応あり）

クラウド・サービスを利用することは少なくありません。また、各クラウド・ベンダーの特徴に合わせて、戦略的に複数のクラウドを使い分けているケースや、コンプライアンスや運用要件に応じて、IBM Cloud PublicとICPを駆使してハイブリッド・クラウドを構築することもあるでしょう。その結果として直面するのが、マルチクラウドの管理です。複数のデータセンターに分散配置された複数のKubernetesクラスターのデプロイや運用管理は複雑でミスが発生する可能性があり、何より工数の上で大きな負担となります。

このようなマルチクラウドの管理作業を軽減するのがICPの「Multi-cloud Manager」です。Multi-cloud Managerは、IBM Cloud PublicやICP、他社クラウド上のIaaSやKubernetesを統合管理するソリューションです。マルチクラウド環境におけるクラスターのデプロイ、ダッシュボードによる運用状況の監視、ログやイベントの監視等を効率化し、ユーザーの負担を大幅に軽減します。

5. おわりに

今後本格化するデジタル・ビジネス時代では、これまで以上にITシステムが重要になってきます。ユーザー体験やアプリケーションのユニークさだけでなく、システム運用の安定性もビジネスの品質として評価される時代に入りつつあるのです。そうなるとスピードや柔軟性だけでは消費者のニーズに応えることはできません。パフォーマンス、セキュリティー、可用性、コンプライアンス、運用容易性など、地に足の着いた非機能要件の充足が求められます。

IBMは、これまで長きにわたってお客様の基幹システム構築・開発で培ったノウハウをIBM Cloudの設計・実装に役立てています。オープン・スタンダードに準拠しお客様の投資を保護するとともに、システム安定運用を確実に支援するソリューションとしてIKSとICPをお勧めします。

[参考文献]

[1] Cloud Native Computing Foundation : charter, https://www.cncf.io/about/charter/

[2] @kubernetesio : Kubernetes, https://twitter.com/kubernetesio/status/840257886202683392

[3] IBM : IBM Cloud Docs / IBM Cloud Kubernetes Service / Regions and Zones, https://console.bluemix.net/docs/containers/cs_regions.html?locale=en#regions-and-zones

[4] IBM : IBM Cloud資料 / IBM Cloud Kubernetes Service / IBM Cloud Kubernetes Serviceのセキュリティー, https://console.bluemix.net/docs/containers/cs_secure.html#security

[5] IBM : IBM Cloud資料 / IBM Cloud Kubernetes Service / ワーカー・ノード用のハードウェア, https://console.bluemix.net/docs/containers/cs_clusters.html#shared_dedicated_node

日本アイ・ビー・エム株式会社
IBMクラウド事業本部
クラウド・テクニカル・セールス
エグゼクティブ・テクニカル・スペシャリスト

樽澤 広亨
Hiroyuki Tarusawa

IBMソフトウェアのエバンジェリスト、米IBMソフトウェア開発研究所所属の開発エンジニアを経て現職。IBM Academy of Technologyメンバー。また情報処理学会情報企画調査会 SC38専門委員として、ISO IEC JTC1/SC38クラウド国際標準策定に従事。

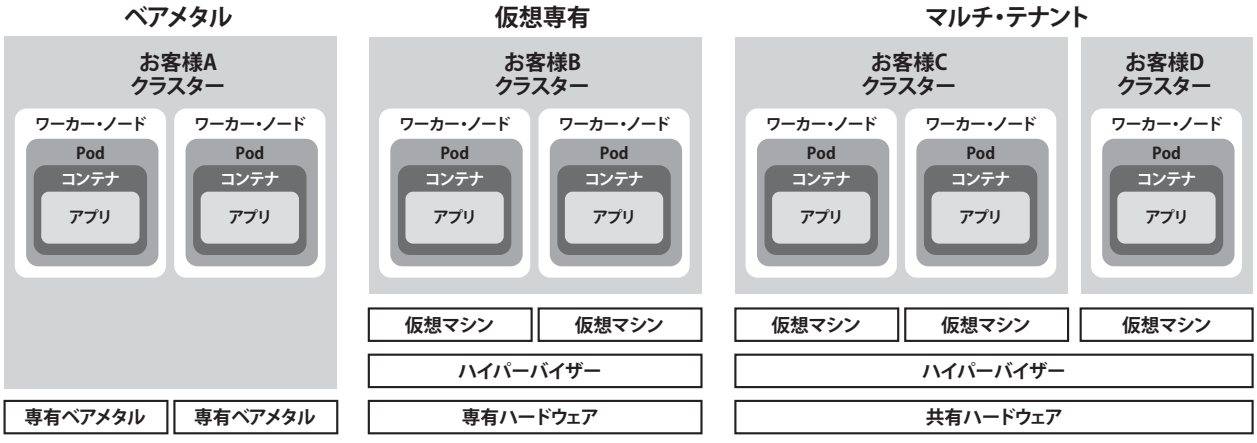

図6. IKSのテナント・モデル