

早く、安く、安全にサービスを提供できる ICT基盤の構築

Virtual Private Data Center Providing Cloud Services Swiftly and Securely at Low Cost

池谷 直紀 IKETANI Naoki 鹿野 市郎 KANO Ichiro

CPS (サイバーフィジカルシステム) をマネージドサービスで提供する基盤としては、クラウドサービスが適している。企業は、これまでビジネスの目的に合わせてシステムごとにクラウドサービスを選定した結果、複数のクラウドサービスとそれぞれ個別に定義した運用をすることになり、これらを一元的に管理することが課題になっている。

東芝デジタルソリューションズ(株)は、セキュリティー技術、ネットワーク技術、監視技術、及び運用技術を共通化してこの課題に取り組み、素早い基盤準備と運用コスト低減を実現した。更に、これらの技術を組み合わせた仮想プライベートデータセンター (VPD) というフレームワークを構築し、基幹システム (プライベートクラウドシステム) にもその適用範囲を拡大した。

In line with the recent trend toward the introduction of cloud managed services aimed at realizing cyber-physical systems (CPS), various companies have found it necessary to replace the individual management of multiple cloud services designed for specific purposes with unified management common to all cloud services, in order to further improve operating efficiency and ensure higher security.

Toshiba Digital Solutions Corporation has responded to this need by developing a framework for a virtual private data center as a solution enabling the operation of multiple cloud services through the standardization of security, network, monitoring, operation technologies. This virtual private data center makes it possible to swiftly construct a unified cloud system incorporating the user's private cloud systems while also reducing operating costs.

1. まえがき

業務システムのIT (情報技術) 革新やCPSの実現には、アプリケーションを実行するICT (情報通信技術) 基盤としてクラウドサービスが適している。クラウドサービスを活用する企業の対象業務システムは、情報系から基幹系にまで拡大していることや、DX (デジタルトランスフォーメーション) を推進するためにマルチクラウドやコンテナを採用していることなど、クラウドサービス活用の多様化が進んでいるが、これらを統合的に管理する仕組みが必要になる。

東芝デジタルソリューションズ(株)は、“東芝マネージドサービスAlbacore”⁽¹⁾の一環として、ITにおける多様なシステムの設計と運用を共通化する標準化アプローチと運用技術を開発し、異なる特性を持つマルチクラウド及びハイブリッドクラウドを一つの手法で管理できるようにした。そしてこれらの技術を組み合わせたVPDというフレームワークを構築して、サービスの提供を開始した。

ここでは、その技術の概要と効果について述べる。

2. クラウドシステムの設計及び運用の課題

各クラウドシステムは、企業の既設機能と連携する基幹

システムや、数万のインターネット上デバイスを活用するIoT (Internet of Things) システムなど多種多様であり、これを個別に設計及び運用することは多大な労力を要する。

クラウドシステムには、以下の多様性が存在し、設計や運用を複雑化する要因となっている。

- (1) クラウドサービス活用による多様化 パブリッククラウドサービスでは、多種多様なサービスが提供されている。これらを適切に活用したシステムを構成することで、運用対象となるシステムごとに最適な設計ができるが、設計及び運用の要素の多様化につながっている。
- (2) ネットワーク接続形態の多様化 パブリッククラウドシステムは、他の既設システムと連携して利用される場合も増加しており、その接続形態にも幾つかの選択肢がある。接続形態に応じてシステム設計及び運用を速やかに実施することは、容易ではない。
- (3) セキュリティー要件の多様化 クラウドシステムによって、そのセキュリティーレベルが異なる場合がある。また、パブリッククラウドシステムで利用するサービスによって、セキュリティーに関する設計も異なる。これに対応した適切なセキュリティーレベルを実現する設計と運用を効率的に行うことは、容易ではない。

ここで対象とする課題は、上述の多様性を持つ複数のクラウドシステムを効率的に設計、構築、及び運用する方式を実現することである。

3. システムの設計と運用を共通化する標準サービス

2章で述べた課題に対し、当社は多様なシステムに対応できる共通サービスを提供するアプローチで、効率化を実現した。機能面と運用面の二つのアプローチで取り組んでいる。

アプローチ1 各種システムで、高頻度に用いられる機能を標準サービスで提供

アプローチ2 運用コストを低減する自動化機能の作成と、それを利用したマネージド運用の提供

実際に提供している標準サービス群の幾つかを、図1に示す。これらは、個別に設計・活用されるシステムに対して、共通機能をサービスとして提供しているものである。クラウドサービスを活用して実現されるCPSなどの各種システムは、これらのサービスも活用することで、設計及び運用の共通化と省力化の効果が得られる。

以下では、提供する標準サービスについて述べる。

3.1 ネットワーク構成の標準化と接続サービスの提供

CPSを含めたクラウドシステムは、そのネットワーク接続方式として以下の観点で選択肢があり、最終的なシステムのネットワークには幾つかの形態がある。

- (1) インターネット接続の有無
- (2) オンプレミスや既設システムとの閉域接続の有無
- (3) 運用・保守の接続経路と方式
- (4) マルチリージョン、マルチクラウド利用の有無

これらを個別のシステムで設計すると、設計も運用もコストが高くなる。そこで、マネージドサービスでは典型的な接続形態をパターン化するとともに、閉域接続サービスを標準化されたオプションサービスとして提供することで、設計及び運用の標準化を推進している。

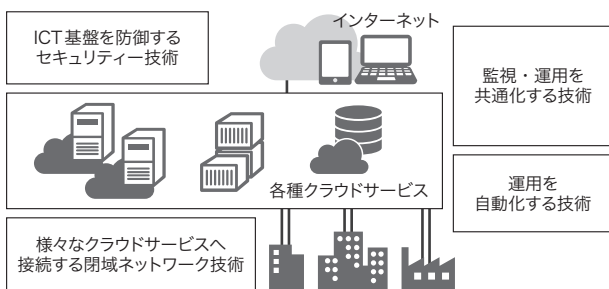


図1. マネージドサービスを支える技術

多様なシステム運用を、複数の標準サービスで共通化している。

Technologies supporting cloud managed services

インターネット側のサービス公開の有無は選択可能であり、閉域接続だけを選択することで、パブリッククラウドサービスを自社データセンターの拡張としても活用できる。

そして、複数のパブリッククラウドサービスとの接続についても、共通化された方式での閉域接続を提供している。この概念を、図2に示す。

3.2 セキュリティーサービスの標準化と提供

セキュリティに関する標準サービスとして提供しているマネージドサービスの一部を、以下に示す。

- (1) クラウド型 WAF 運用サービス インターネット側に向けたWebアプリケーションやWeb API (Application Programming Interface) においては、その各種脆弱(ぜいじゃく)性をWAF (Web Application Firewall)で保護するのが望ましい。当社は、これをパブリッククラウドサービスの選択肢に依存せずに経路上に配置できるサービスとして提供することで、共通化されたインターネット側からの防御機能を提供している。
- (2) セキュリティーサービス (ウイルス対策, IPS)

仮想サーバーにおけるウイルス対策や、WebサーバーにおけるIPS (Intrusion Prevention System) も必要とされる場合が多い。当社は、ホスト型(仮想サーバーにエージェントをインストールするタイプ)のウイルス対策及び脅威対策ソフトウェアを、標準サービスとして提供している。アンチウイルスのパターンなどを提供するサーバー部分はマネージドサービスとして提供しており、運用対象の各システムでは接続経路だけを設計すればよく、個別のサーバー設計をする必要はない。

3.3 共通化された運用・監視サービスの提供

システムの状態を収集及び可視化し、障害を検知したときに対処する運用・監視機能は、マネージドサービスの中心的なサービスである。これについても、各種システムについての個別設計要素を極力低減するように、共通化している。

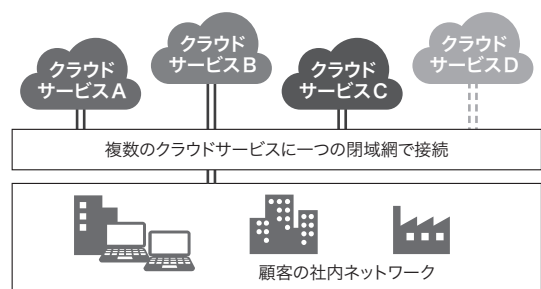


図2. 複数のクラウドサービスとの接続概念

複数のクラウドサービスとの閉域接続を、一つの方法で提供している。

Connections between closed network and multiple cloud services

当社は、運用・監視機能をクラウドサービスとして構成・活用することで、以下を実現している。

- (1) 対象システムが利用しているパブリッククラウドサービスに依存せずに、監視することが可能
- (2) 仮想サーバーだけでなく、利用頻度の高いパブリッククラウドサービス（例えば、データベースサービスやストレージサービスなど）についても監視が可能
- (3) 監視設定のひな型を提供することで個別の設計要素を減らし、カスタマイズだけで監視サービスを利用可能
- (4) 多数の運用対象システム群について、統一的可視化と運用を提供
- (5) 仮想サーバーやストレージなどの基盤の状態と、プロセスやURL (Uniform Resource Locator) 及びAPIの死活とレスポンス状況などのアプリケーション状態について、統一かつ包括的なモニタリングが可能

この模式図を、**図3**に示す。監視機能には、障害に気付くことだけでなく、障害に気付いた際にシステムを見渡して、状況把握と原因究明を速やかに行うことが期待される。この観点で、上記の統一かつ包括的なモニタリングは効果的である。

3.4 運用自動化機能の提供

運用・監視中に発生した事象の幾つかについては、所定手順による対処の実施が必要な場合がある。運用時に想定されたイベントへの対処は、従来は手順書に従って運用者が実施する場合も多かったが、マネージドサービスでは自動化機能を実現している。これは、次のように機能する。

- (1) 準備として特定のイベントへの対処方式を、運用設計の一環としてプログラムで作成して設定
 - (2) 運用時に想定されたイベントが発生すると、マネージドサービスの自動化機能により該当プログラムを実行
- この自動化機能は、以下を実現している。
- (1) 対処の際にパブリッククラウドサービスのAPIを呼び

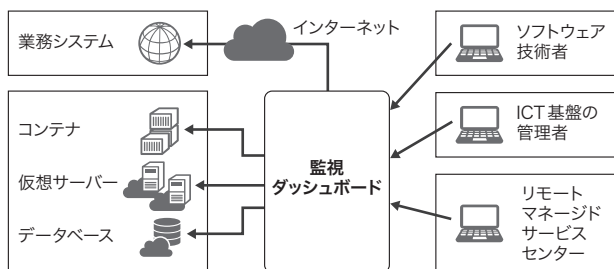


図3. 監視・運用技術を用いた統合監視

一つの運用・監視基盤による統合監視を、サービスとして提供している。
Unified monitoring system using monitoring and operation technologies

出すことで、対象システムが利用しているパブリッククラウドサービスの挙動を指定可能

- (2) 典型的な復旧処理のプログラムをマネージド運用で用意することにより、各CPSの設計者は、それを再利用及びカスタマイズすることで活用可能
- (3) マネージドサービスのインシデント管理基盤にも事象の発生を通知しておくことで、自動対処が発生したことを運用者がタイムリーに確認可能

4. クラウド運用技術を組み合わせたフレームワークVPD

3章で述べたクラウド運用技術は、個別の要請を持つシステムを共通的に扱う部分を増やす仕組みであった。当社は、更にこれらの技術を組み合わせてフレームワークとすることで、マルチクラウドとハイブリッドクラウドの導入から運用までを一貫して提供するVPDを定義した（**図4**）。

単一の業務システムをクラウドサービスで運用する要件ではなく、エンタープライズ企業の基幹系システムやインターネット公開向け情報系システムの全てを対象としている。数十台から数千台の規模になる業務システムを一つの手法で運用することをターゲットにしたフレームワークであり、従来IT型のオンプレミスデータセンターをクラウドサービスで置き換える構想である。このフレームワークを活用することで、新たな業務システムを導入する際に、その都度要件定義をして設計・構築するよりも、早く、安く、クラウドサービスのICT基盤を利用できる。導入はもちろん統一された継続的モニタリング手法でセキュリティリスクを低減させ、安心してクラウドサービスを運用できるように、フレームワークには

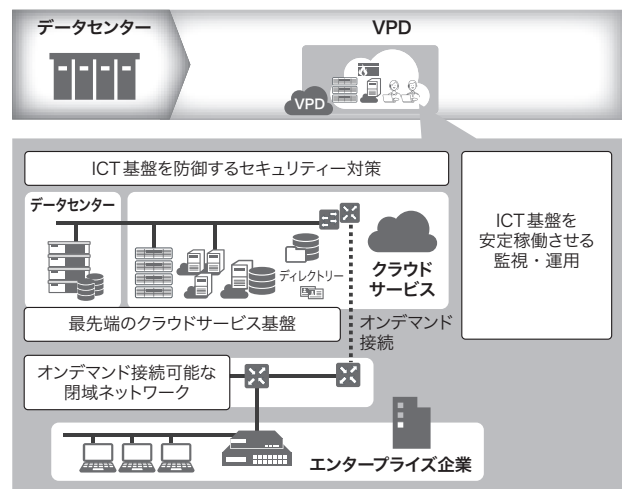


図4. VPDの概要

標準サービスを活用したフレームワークを、VPDとして提供している。
Overview of virtual private data center

セキュリティー対策も組み込まれている。同様に、監視・障害対応も組み込まれている。24時間365日モニタリングを実行するリモートマネージドサービスセンターに集約・統合することで、サービス実行体制をシェアードサービス化して運用のコスト低減を進めている。

5. 標準サービス及びVPDによる効果

3章で述べた標準サービス、及び4章で述べたVPDにより、多数のシステムを運用する際に従来は個別の設計と運用が必要であったが、VPDの運用という一つの方法に共通化することができた。この模式図を、図5に示す。この共通化により、安全なシステムを素早く安価に導入・運用することが可能となった。

具体的には、以下の効果が得られている。

- (1) 設計及び構築の効率化 標準サービスの活用により、その部分を個別に構築する必要がなくなり、該当部分の開発・運用コストを数分の一のサービス利用費で素早く実現できるようになった。
- (2) 多様な業務システム運用の集約 数十の多様なクラウドシステム基盤の運用を、一つのチームで実施できている。従来は、サーバー台数の規模に応じた労力を掛けていた運用が、一つの運用サービスの継続的な改善に集約された。これは、運用手順を数十分の一に集約できる効率化に相当する。

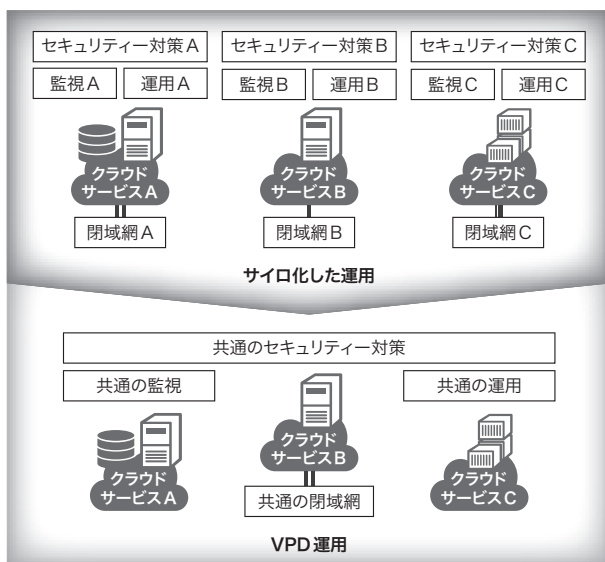


図5. サイロ化した運用から共通化されたVPD運用への移行

システムごとの個別運用ではなく、多数システムを一つのVPD運用の方法に集約できるようになった。

Replacement of operations of individual cloud services with standardized operations using virtual private data center

(3) マルチクラウドとオンプレミスの計算リソースの統合的な活用 メガクラウドベンダーの6社以上が提供するクラウドサービス(マルチクラウド)、及びオンプレミスとクラウドシステムで統一した技術によるサーバー仮想化集約基盤(ハイブリッドクラウド)が混在する環境をVPDの標準フレームワークで構成することで、必要な機能を利用することが可能になった。

(4) クラウドサービスとともに継続的に進化するVPDの実現 クラウドサービスについては、クラウド事業者が常に進化を続けるため、結果としてVPD自体も常に進化するフレームワークとなり、追加の開発投資なしに最新のクラウドサービスの恩恵を享受できることになった。

6. あとがき

特性の異なる複数のクラウドサービスを活用した複数のシステムを運用するための課題を解決する手段として、マネージドサービス及びVPDで提供するサービスの標準化や、利用するツールの統合、省力化・自動化の方式について述べた。

日々進化するIT技術やクラウドサービスを最大限に活用するために、今後も継続的なクラウド技術の把握と標準サービス化を行い、早く、安く、安全にサービスを提供できるICT基盤を進化させることで、CPSの実現に貢献する。

文献

- (1) 東芝デジタルソリューションズ, “東芝マネージドサービス Albacore™ ビジネスと、その進化をとめない”. Albacore (アルバコア). <<https://www.global.toshiba.jp/products-solutions/ict-platform/albacore.html>>, (参照 2021-06-23).



池谷 直紀 IKETANI Naoki
東芝デジタルソリューションズ(株)
ICTソリューション事業部 マネージドサービス第一部
Toshiba Digital Solutions Corp.



鹿野 市郎 KANO Ichiro
東芝デジタルソリューションズ(株)
ICTソリューション事業部 マネージドサービス推進部
Toshiba Digital Solutions Corp.