マルチクラウド環境下のセキュリティ統制
―ツールを利用したコンプライアンス準拠とワークロード保護―

ビジネスインフラとしてのパブリッククラウドの活用が進み、複数のクラウドを使うマルチクラウドも珍しくないが、それは利用者のセキュリティ統制が難しくなることも意味する。本稿では、クラウド活用におけるセキュリティ上の課題と、それを解決するために有効な管理・統制ツールについて紹介する。

野村総合研究所 クラウドサービス事業本部
ネットワークサービスマネジメント部 上級研究員・NRI認定ITアーキテクト
江口（えぐち）　勲（いさお）
専門はネットワークおよびクラウドセキュリティに関する先進技術の研究開発

パブリッククラウドの伸展とマルチクラウド化

パブリッククラウドサービスは主に次の3つに大別される。「Office365」や「Salesforce」などのアプリケーションをクラウド化したSaaS、コンピュート（CPU、メモリー）やストレージなどのハードウェアリソースをクラウド化したIaaS、アプリケーションの実行環境やAI・機械学習などをクラウド化したPaaSである。

Gartner社が2019年4月に発表したプレスリリースによると、世界のパブリッククラウドサービスの2018年～2022年の年平均成長率は16.1%、2022年の市場規模は3,312億ドルになると予測されている*。国内では、2018年～2023年の年平均成長率は20.4%で推移し、2023年の市場規模は2018年比2.5倍の1兆6,940億円になる見込みである（出典：IDC）。いずれの予測でも、IaaSとPaaSの成長率がクラウドサービス全体のそれより高くなっている。これは、従来の自社構築・自社運用のシステムからIaaS/PaaSへの移行が進んでいることと、最近はデジタルトランスフォーメーション（DX）のために、IaaSやPaaSを使ってアプリケーションを迅速かつ頻繁に開発する必要があることを反映した結果と考えられる。

昨今では、自社のプライベートクラウドやパブリッククラウドなど、複数のクラウドを併用するマルチクラウドを採用する企業も増えている。その目的は、IaaSでは、耐障害性の向上（全てのサービスが停止することを避けられる）や、ベンダーに競合させてよりよい条件を引き出すこと、PaaSでは、ベンダーが提供するさまざまな新技術を適材適所で利用することにある。

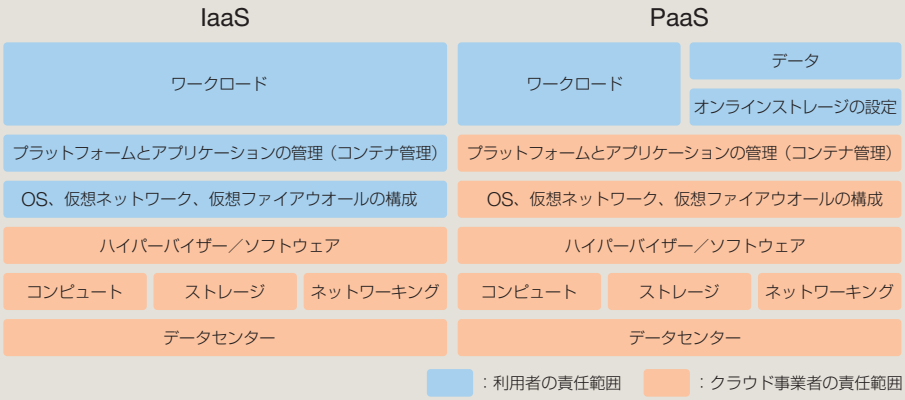
なくならないセキュリティ事故

IaaS/PaaSを利用する大きなメリットの1

＊ Gartner, Press Release, April 2, 2019 “Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019” https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g（パブリッククラウドサービス＝BPaaS/SaaS/IaaS/PaaS/Cloud Management And Security Service）

つは、「誰でもすぐに利用できる」という利便性である。そのため、開発部門が直接IaaS/PaaSを契約し、自身で運用するケースも多い。しかし、利便性を重視するあまりセキュリティ対策がおろそかになっているケースが見られる。

図1　パブリッククラウドにおける責任共有モデル



実際、IaaS/PaaSの設定ミスや設定漏れに起因する、大規模なセキュリティ事故が後を絶たない。ここ数年、オンラインストレージに格納した大量の機密データに、誰でもアクセスできる状態になっていた事例の報告が相次いでいるのである。2019年7月にも、米国金融大手のCapital Oneが、不正アクセスによって1億人を超える個人情報の流出があったことを公表した。これらのセキュリティ事故は、いずれもIaaS/PaaSの設定ミスや設定漏れが原因である。

パブリッククラウドのセキュリティに関しては、クラウド事業者と利用者の責任範囲が明確に定義されており、これを「責任共有モデル」という（図1参照）。例えばIaaSでは、データセンターなどのインフラ設備やコンピュートなどの機器のセキュリティはクラウド事業者側が責任を負い、OS（基本ソフト）や仮想ファイアウオールの構成、ワークロード（リソースとコード）やデータの保護は、原則的に全て利用者側が責任を負う。

この利用者側の管理が煩雑であることが、設定ミスや設定漏れがなくならない要因である。IaaS/PaaSを利用する際は、プロジェクト単位でクラウドアカウントを作成することが多い。また、プロジェクトに委託会社のメンバーが参加していれば、そのメンバーにもアカウントを与える必要がある。さらに、IaaS/PaaSで提供されるサービスは100以上もあるため、アカウントの設定がコンプライアンスの面で妥当かをチェックすることは容易ではない。複数のIaaS/PaaSを利用するマルチクラウドでは、このセキュリティ統制がさらに難しくなる。

これに加えて、アプリケーション開発にコンテナという新しい基盤技術を利用することが多くなり、セキュリティ保護の考え方が従来とは変わってきた。コンテナとは、1つのOS（基本ソフト）上に、独立したサーバーと同じ振る舞いをする複数の区画をつくり、それぞれを個別のサービスに割り当てる技法である。

コンテナを使った開発では、新しいサービスを開発環境から本稼働環境に迅速かつ頻繁に移行できるようになった。しかし、本稼働環境でサービスのコードに既知のぜい弱性が見つかり、修正のために手戻りしていては対

応コストも膨らみ、アジリティ低下の要因となる。そのため、本稼働環境にリリースする前にコードをチェックする必要がある。

これらの理由から、利用者側のコンプライアンス基準への準拠や、コンテナを使った開発におけるセキュリティ統制をいかに実施するか、また、いかにして開発のアジリティを損なうことなく開発のプロセスに統制を組み込むかが課題になっている。

CSPMによるセキュリティ統制

上記の課題を解決する技術として登場したのがCSPM（Cloud Security Posture Management。クラウドセキュリティ態勢管理）である。CSPMツールは、マルチクラウド環境下で、利用者側の責任範囲における、サービスの設定・構成（オンラインストレージの設定、OSや仮想ファイアウオールの構成など）のセキュリティ統制を主に支援する。海外では、IaaS/PaaSを積極的に利用しようという動きに合わせてCSPMツールが注目され、導入も進んできている。

(1) CSPMツールの機能

CSPMツールの機能は、主に以下の3つである。

①オートディスカバリー

利用者が契約するIaaS/PaaSの仮想サーバーやオンラインストレージなどのサービスを、API（Application Programming Interface。あるプログラムの機能やデータを他のプログラムから利用するための手続きを定めた規約）によって自動検出する機能である。どのアカウント利用者が、どのサービスを、どれだけ利用しているかをモニター画面上で確認することができる。

②設定・構成のモニタリングと分析

利用しているサービスの設定・構成の状況をモニタリングし、各種コンプライアンス基準への準拠状況をモニタリングする機能である。照合されるコンプライアンス基準には、各企業のポリシー、PCI DSS（Payment Card Industry Data Security Standard。クレジットカード業界のセキュリティ基準）、CIS（Center for Internet Security。米国のインターネットセキュリティの標準化組織）によって定義されたCIS Controlsなどがある。

③レコメンド

サービスの設定・構成を分析した結果、「非準拠」と判定されたサービスの設定・構成を修正する手順を推奨する機能である。その手順に従えば、IaaS/PaaSの管理ツールを用いて均一な修正が可能となる。

(2) CSPMツール選定のポイント

ツール選定のポイントの1つは、自社が利用するIaaS/PaaSで、自社の業界のコンプライアンス基準がサポートされているかということと、IaaS/PaaSの準拠状況を見ることのできるAPIを備えているかということである。Amazon Web Services（AWS）やMicrosoft AzureなどのIaaS/PaaSで提供されているサービスは100以上もあるため、自社が所属する業界のコンプライアンス基準に照らして、利用するサービスの準拠状況をAPIによって可視化できる必要がある。

もう1つのポイントは、設定・構成の自動修正機能である。「非準拠」と判定された設定・構成の修正を手動ではなく自動で行える

ツールもある。この機能があれば、開発のアジリティをより高めることが期待できる。

CWPPによるセキュリティ統制

前記の課題を解決するもう1つの技術としてCWPP（Cloud Workload Protection Platform。クラウドワークロード保護プラットフォーム）がある。CWPPツールは、利用者側の責任範囲におけるワークロードのセキュリティ統制を、マルチクラウド環境下でも支援する。

(1) CWPPツールの機能

CWPPツールの機能は、主に以下の3つである。

①ぜい弱性管理・構成管理

コンテナを用いたアプリケーション開発では、コンテナイメージの作成から運用までの各フェーズで、イメージをスキャンしてぜい弱性を検知する。また、PCI DSSやCIS Controlsなどのコンプライアンス基準に対するコンテナ構成の準拠状況を可視化することもできる。

②ネットワーク論理分割

サイバー攻撃や不正アクセスからワークロードを守るセキュリティ対策の基本は、外部通信を行うネットワークを論理的に分離することである。さらに、マルウェア感染の拡大を防ぐため、環境内のネットワークを細かく論理分割すること（マイクロセグメンテーションという）も有効である。CWPPツールの中には、独自のファイアウオール機能によってネットワークの論理分割を実現するものや、クラウド事業者が提供する仮想ファイアウオールを管理する形で本機能を提供するものもある。

③アプリケーションコントロール

実行を許可するアプリケーションをホワイトリストに登録し、そこに載っていないファイルが実行されるのをブロックする機能である。本機能を利用することで、マルウェアへの強力な防御が実現する。

(2) CWPPツール選定のポイント

ツール選定のポイントは、継続的インテグレーション（CI）ツールと継続的デリバリー（CD）ツールとの連携が可能または容易かという点である。開発がより迅速化すると、これらのツールと連携して統合的にセキュリティスキャンを行う必要が生じるからである。ワークロードを新しく作成する際に、ぜい弱性と構成のチェックを自動化すれば、開発のアジリティを高めることが可能である。

マルチクラウド化に欠かせない管理・統制ツール

最近は、IaaS/PaaSをビジネスインフラとして利用するのが当たり前になっている。また、前述のように複数のIaaS/PaaSを併用するマルチクラウドを採用する企業も珍しくない。しかしそれは、利用者側のセキュリティ管理・統制を複雑化することでもある。このような時代に、利用者に課せられたセキュリティ対策の責任を果たしながら、安全にIaaS/PaaSを利用して企業の競争力を高めていくために、本稿で紹介したCSPMツールやCWPPツールなど、セキュリティ管理・統制ツールの導入を強く勧めたい。 ■