パブリッククラウドの利用拡大に向けて
―考慮すべき3つの基本的なポイント―

デジタルトランスフォーメーション（DX）に必要不可欠となったパブリッククラウドの活用は、今後、ますます拡大するとともに、複数のクラウドを併用するマルチクラウドも多くなっていく。本稿では、パブリッククラウドの活用を進め、業務への適応範囲も拡大していくに当たって考慮すべき基本的なポイントを解説する。

野村総合研究所 クラウドサービス事業本部
クラウドサービス統括部 上級テクニカルエンジニア
山元（やまもと） かおり
専門はプライベートクラウド・パブリッククラウド導入・活用の支援

パブリッククラウド活用の3つのポイント

パブリッククラウドが急激に拡大する一方、その活用に不安を感じている企業も多い。確かに、パブリッククラウドの活用に際しては考慮すべき点が多いが、われわれがお客さまにパブリッククラウドを紹介するときに、必ず説明することにしている3つのポイントがある。それはSLA（Service Level Agreement。サービス水準合意）、セキュリティ対策、そして全体リソース管理の3つである。以下で順に述べていこう。

SLAを意識したシステム設計

1つ目のポイントはSLAを意識することである。パブリッククラウドでは必ずSLAが開示され、サービスの契約にはこの内容に同意することが含まれている。

SLAでは、ベンダーが保証する稼働率がサービスごとに明記されており、これを満たさない場合は返金要求が可能だ。ただしSLAをよく読むと、利用者のシステムが、クラウドベンダーが提示するベストプラクティスに基づいて構成されていることが、稼働率計算の条件となっていることが分かる。仮に、サービス停止の原因がベンダー側にあることが明らかでも、利用者側のシステムがSLAに記載された条件を満たしていなければ、返金してもらえない可能性が高い。

先日、あるパブリッククラウドで大規模な障害が発生し、一部のサービスが一時的に利用できなくなった。では、SLAに記載された稼働率が満たされなかったのかというと、そうではなかった。このサービスは、利用者側で冗長性を確保することが稼働率計算の条件となっていたことに加え、他のデータセンターでは障害がなかったため、全体として稼働率が確保されているというのである。

ベンダーが提示するベストプラクティスに従うことは、当然コスト増となる。そのため、SLAを正確に理解し、対象システムで行う業務の重要性とコストとのバランスを考慮して、利用者が責任を持って設計・運用する必要がある。

厳格なセキュリティ対策

2つ目はセキュリティ対策である。パブリッククラウドは、一般にインターネット上に管理コンソール（操作画面）を持っており、設定次第では世界中のどこからでもアクセス可能だ。これは、システム利用者との接点のみ外部に開示され、それ以外は閉じた領域で管理されているオンプレミス（自社構築）環境とは大きく異なる点である。

また、パブリッククラウドは管理コンソールからクリックだけでシステム操作ができる。ITリテラシーが高くなくても操作が行えるのはパブリッククラウドの利点だが、これはセキュリティ面では不安材料でもある。このように、パブリッククラウドはオンプレミス環境とは異なる特性を持つため、利用側ではこれまで以上に高度なセキュリティ対策を実施する必要がある。

セキュリティ対策は、組織共通のセキュリティルールを策定することから始まる。多くの組織はすでにセキュリティルールを定めているだろうが、それがパブリッククラウドの活用に則したものなのか、あらためて精査が必要だろう。特に、世界中から誰でも操作できるという点に関しては、当然ながらルールを追加する必要がある。

セキュリティ対策の基本は「防止」と「検知」である。多くの企業は、「防止」に関しては設計時に適切に検討しているが、「検知」は考慮から漏れてしまいがちである。簡単に変更ができる環境だからこそ、ルールを守っているかを継続的に監視し、問題があれば検知できることが必要である。この対策はそれなりのコストを伴うが、セキュリティインシデントが発生した場合の損失と、インシデントが発生しやすいことを考えれば、「検知」の対策は必須と考えるべきである。

リソースの全体的な管理

3つ目は、リソース管理である。ここでいうリソースとは、サーバーなどのデバイスに限らず、アカウントやユーザー権限など、パブリッククラウドを構成するすべての要素を指す。パブリッククラウドは、簡単に利用できるからこそ、気付けば組織内にアカウントやサーバーの乱立、乱雑な権限管理などが生じやすい。こうして管理不能な状態になった結果、セキュリティインシデントが発生したり、本来は不要なはずのコストがかかっていたりするケースは多い。

パブリッククラウドの全体リソースを組織として管理できていないことは、企業にとって大きなリスクとなる。これを防ぐためには、CCoE（Cloud Center of Excellence。クラウド利用の中核組織）のようなクラウド管理組織の設置が有効である。野村総合研究所でも、社内のパブリッククラウド環境に対して、セキュリティ対策を含めたリソース管理を行う仕組みを導入している。

現在ではマルチクラウドも拡大しており、今後のクラウドサービスの活用環境はより複雑化していくだろう。そのときにも、本稿で述べた3つのポイントを押さえることは、自社のシステム環境を適切にコントロールする上で重要になるはずである。■