セキュアな
マルチクラウド
構築ガイド

splunk>
turn data into doing™

セキュアなマルチクラウド構築ガイド

インフラやサービスをクラウドに移行する中で、マルチクラウド戦略を採用する組織が増えています。事実、マルチクラウドアーキテクチャを採用する企業のIT部門の割合は、2020年までに90%を超えるとIDC社は予測しています。

マルチクラウドを採用する理由

この構築ガイドでは、マルチクラウドの概要とハイブリッドクラウドとの違い、導入のメリット、さらに最も重要な点として、適切なセキュリティソリューションによってマルチクラウドを保護する方法を説明します。

マルチクラウドとは?

マルチクラウド戦略の採用は、決して難しいものではありません。マルチクラウド戦略とは、単に、さまざまな課題を解決するために単一のアーキテクチャで2つ以上のクラウドサービスを利用することです。

ですがこの概念には、押さえておくべき重要なことがあります。それは、マルチクラウドを構成できるクラウドの種類が多岐にわたるということです。まず、パブリッククラウドがあります。アマゾン ウェブ サービス (AWS)、Microsoft Azure、Google Cloud Platformなどがこれに該当します。そして、プライベートクラウドがあります。パブリッククラウドと似ていますが、アクセスが特定の組織に制限されているか、組織によってオンプレミスで独自にホストされています。さらに、マルチクラウドには利用が広がっている各種SaaSソリューションも含まれることが多くあります。G Suite、Workday、Salesforce、Adobe Creative Cloud、Office 365をはじめ、こうしたサービスは増え続けています。

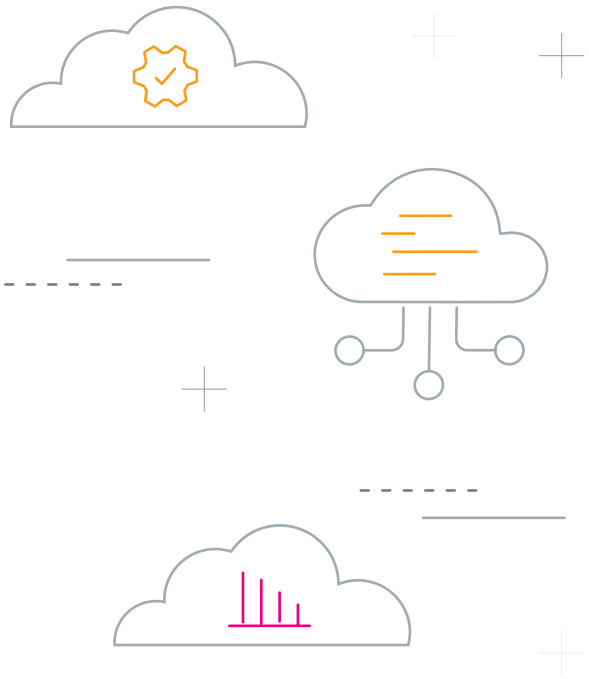
マルチクラウドとハイブリッドクラウドとの違い

マルチクラウド戦略は、ハイブリッドクラウド戦略と同じではありません。ハイブリッドクラウド戦略とは、パブリック、プライベート、あるいはその両方の複数のクラウドを導入するモデルです。たとえば、企業がオンプレミスのプライベートクラウドとサードパーティのパブリッククラウドの両方を使用してインフラを構築する場合などです。このアプローチは、コンプライアンスの目的や、財務などの事業をインフラ内で切り分ける目的で採用されます。

マルチクラウド環境を使用する6つのメリット

マルチクラウド戦略のメリットは6つにとどまりませんが、簡潔に6つに絞ってご紹介します。

1. **信頼性の向上**
2. **コスト削減**
3. **パフォーマンスの最適化**
4. **ベンダーロックインの回避**
5. **優れた製品の利用**
6. **DDoS攻撃のリスクの軽減**



各メリットについて簡単に見ていきましょう。

マルチクラウド戦略によって**信頼性が向上する**のには、いくつか理由があります。まず、マルチクラウド戦略ではサービスが複数のクラウドに分散しているため、ハッカーが組織の全サービスをダウンさせるのが難しくなります。

また、プライマリクラウドがダウンした場合やパフォーマンスの問題が生じた場合、パッシブにしておいたクラウドにフォールバックすることができます。これによってプライマリクラウドがオンラインに戻るまでのダウンタイムを削減または完全に無くすことができます。信頼性の向上とダウンタイムの削減は、**コスト削減**にもつながります。

たとえば、**DDoS(Distributed Denial of Service)**攻撃という、ハッカーが複数のコンピューターシステムからサーバーやWebサイト、クラウドプロバイダーに対して、応答が停止するまで過剰な負荷を与え続ける攻撃が起きる可能性があります。

そして、ネットワークの停止は金銭的な損失につながります。ダウンタイムの具体的なコストは、業界やコストの計算方法によって異なります。たとえば銀行の場合は現金を、病院の場合は現金に加えて命を失う可能性があります。

補足しておくと、最近の調査では、98%の組織が1時間のダウンタイムによって平均10万ドル以上の損失が生じると回答し、33%がダウンタイムによって500万ドル以上の損失が生じると回答しました。

マルチクラウド戦略では、トラフィックを複数のクラウドに分散させることで、**DDoS**攻撃のリスクを軽減することができます。サービスを複数のクラウドに分散させている企業は、1つのクラウドだけに依存していないため、**DDoS**攻撃による破壊的な被害を受けにくくなります。

マルチクラウド戦略では、**ベンダーロックイン**を回避することで柔軟性も得られます。具体的には、さまざまなオプションやクラウドが市場にあるため、ベンダーはビジネスを守るために競争力を磨き続けなければなりません。マルチクラウドを採用する顧客はSaaSやクラウドアーキテクチャのニーズに応じて他のベンダーに乗り換えてしまう可能性があるため、ベンダーは、サービスと**コスト**で他社に劣らないように常に努力する必要があります。

このことが、組織にとって**最適なベンダーを選択できる**という柔軟性にもつながります。たとえば、Microsoft社のツールを利用する一方で、インフラにはGoogleを、開発プラットフォームにはAWSを選択することができます。

マルチクラウド戦略を保護する上での課題

マルチクラウド戦略には、メリットもあれば課題もあります。特に、ホストとサービス全体を十分に可視化できなければ、マルチクラウド戦略を適切に保護することができません。可視化できない部分があると、インフラ内の脆弱性がハッカーに見つかりやすくなり、コンプライアンス要件への準拠も難しくなってしまいます。

マルチクラウドを保護する方法

幸いにも、この課題には解決策があります。マルチクラウドのエコシステムは数多く存在し、ベンダー、アプリケーション、システムは多岐にわたります。マルチクラウド戦略を採用する組織は、ダウンタイムを回避してハッカーに先手を打つために、環境全体を可視化することが必要です。

Splunkは、さまざまなクラウドサービス向けの複数のAppsを含むセキュリティポートフォリオを展開しており、これらを通じて環境の可視化を実現します。また、AWS、Azure、Google Cloud Platformといった最も一般的なクラウドサービスに関して、セキュリティおよび運用上のインサイトを迅速に提供します。

マルチクラウド戦略を採用する組織がSplunkのセキュリティポートフォリオを活用すれば、複数のクラウドサービスのアップタイムと可用性を1つのビューで監視し、マルチクラウド環境のセキュリティとコンプライアンスを確保することができます。また、Splunkのプラットフォームには、サードパーティのクラウドサービスもデプロイすることができます。

始めましょう

マルチクラウド戦略の可視性とセキュリティを強化する方法についてご興味をお持ちの場合は、SplunkをSIEMとしてお試しください。ダウンタイムを回避し、発生前に脆弱性を特定することができます。

詳細はこちら

splunk> turn data into doing™

20-13388-A-Brief-Guide-to-Securing-Your-Multi-Cloud-A4-EB-JA-202009