

マルチクラウドモニタリング の戦略



急増する マルチクラウド

クラウドへの移行が進んでいます。**ガートナー社は、大企業の80%**が2025年までにインフラをオンプレミスから完全に移行すると予測しています。クラウドコンピューティングにおける最新の傾向は、マルチクラウドの急増です。マルチクラウドとは、1つのアーキテクチャで少なくとも2つのクラウドサービスを利用する戦略です。たとえば、社内アプリにはGoogle Cloud Platform、顧客向けアプリにはAmazon Web Services (AWS)を利用するのように、タスクごとに異なるクラウドスタックを使用します。このようなアプローチはかなり普及が進んでおり、**現在は80%の企業で採用**されています。

マルチクラウド環境を構成できるクラウドソリューションは多岐にわたります。パブリッククラウドサービスには、AWS、Microsoft Azure、Google Cloud Platformのほか、サードパーティプロバイダーが提供するクラウドコンピューティングサービスがあります。一方でプライベートクラウドは、特定の組織のみがアクセスできるものです。サービスとインフラはプライベートネットワーク上で管理され、パブリッククラウドよりもセキュリティが強固で管理も容易です。

タスクごとに異なるスタック

複数のパブリッククラウドを使用する理由



マルチクラウド環境を理解する

ここで、「ハイブリッドクラウド」と「マルチクラウド」の定義も確認しておきましょう。ハイブリッドクラウドソリューションとは、オンプレミス、パブリッククラウド、プライベートクラウドのインフラを組み合わせることを意味します。一方でマルチクラウドとは、クラウド導入において、同じ種類の複数のクラウドプロバイダーを使用することです。たとえば、異なるベンダー 2社のパブリッククラウドを利用し、部門のニーズに応じて、いずれかのクラウドベンダーを選択します。

それぞれの比較

マルチクラウド	ハイブリッドクラウド
同種(パブリックまたはプライベート)の複数のクラウドを別々のベンダーから導入	サービス(オンプレミス、プライベート、パブリック、サードパーティ)を組み合わせ、統合またはオーケストレーション
例： 2つのパブリッククラウド (AWSとAzure)	例： パブリッククラウドと、自社で管理するオンプレミスのデータセンターインフラ

企業がマルチクラウドを採用する理由

パフォーマンスの最適化：プライマリの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。この戦略により、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ることができます。

コスト削減：信頼性の向上とパフォーマンスの最適化を図ることで、コスト削減を実現できます。例えば銀行でダウンタイムが発生すれば売上の機会損失につながります。病院でのダウンタイムは、それに加えて人命を危険にさらす可能性もあります。どのような組織でも、正常な状態を保つには、何が起きてもしっかり稼働を維持することが不可欠です。

柔軟性：マルチクラウドのアプローチを使用すればベンダーロックインを防ぐこともできます。ベンダーロックインとは、特定のクラウドプロバイダーのインフラとサービスに依存し、ベンダーを変えようとするとき相当なコストや制限が発生する可能性を抱えている状態です。さまざまなベンダーを採用すれば、自社のニーズに応じたサービスを選択して組み合わせられるため、パフォーマンスも最適化できます。たとえばひとつの企業で、ある用途にはMicrosoftのツールを使用し、別の用途(インフラや開発)にはGoogleやAWSなどを使用するといったことが可能になります。



信頼性の向上



パフォーマンスの最適化



コスト削減



ベンダー
ロックインの回避



拡張性

マルチクラウド環境 の課題

マルチクラウド戦略には多くの利点がありますが、看過できない課題もあります。柔軟性や信頼性を高める機能が、一方でセキュリティリスクやITの課題を生むためです。

IT部門が抱えているクラウドコンピューティングの課題は、マルチクラウド環境ではさらに増大します。クラウドで起きている重大な問題を特定し、調査、解決することがより困難になります。また、サービス数が増えれば複雑さが増し、システムがサイロ化すれば包括的な監視がさらに難しくなります。

セキュリティ面では、使用しているクラウドサービスの数と侵害の発生しやすさとの関係が最近の研究で明らかになっています。**Nominet社が実施した2019年の調査**によると、マルチクラウド環境の52%が過去1年以内に侵害を受けているのに対し、ハイブリッドクラウドを使用する組織では24%、シングルクラウドを使用する組織では24%にとどまっています。また、マルチクラウド環境では侵害の発生件数も多くなります。11～30件の侵害を受けたと回答したのは、マルチクラウドを使用する組織では69%だったのに対し、シングルクラウドを使用する組織では19%、ハイブリッドクラウドを使用する組織では13%でした。

マルチクラウド環境がもたらす課題は、IT部門とセキュリティ部門にさまざまな影響を与えます。

複数システムのサイロ化：マルチクラウドのアプローチは、サービスが複数のクラウドソリューションに分散されるため、セキュリティとシステムの信頼性の向上が見込めます。しかし、すべてのホストとサービスを見渡す統合的な可視性を確保しにくくなるため、リスクが上昇する可能性もあります。

さまざまなクラウドソリューションを使用し、それぞれに監視用とセキュリティ用の独自のネイティブツールがある場合、特定のサービスに起因するサービス品質の低下やダウンタイムが起きている時や、システムが想定どおりに動作していない時に、IT部門は効率的にスタック全体を見渡せず、状況を把握することが困難になります。

従来のサイバーセキュリティの基本概念は、マルチクラウド環境では必ずしも通用しません。複数のソリューションを使用してクラウドサービスをそれぞれ監視することもできますが、この方法は業務を減速させ、特に一刻を争う問題が発生した場合にはコストもかさみます。

MTTR(平均解決時間)の増加：マルチクラウドシステムの障害や侵害に関する情報をかき集めるのは、ITチームやセキュリティチームにとっては悩ましい問題です。マルチクラウドシステムに障害や侵害が発生すれば、時間とコストがかかるだけでなく、顧客の満足と信頼が損なわれます。

スタック全体の可視性が低下すると、障害の発生場所や原因の特定により多くの時間がかかります。問題の全体像を把握するためには、複数の監視システムを切り替えながら、イベントデータの関連付けと分析を行うことになるからです。サービスの障害や悪意のある攻撃の発生時にはわずかな時間が重要な意味を持ち、マルチクラウドシステムの複雑さは最終的な結果に直接的な影響をもたらします。

データガバナンス、コンプライアンス、インフラの脆弱性：さらに、複数のスタックで可視性が不足していると、コンプライアンスだけでなく、ハッカー対策もいっそう難しくなります。企業のインフラの分散化が進むと、ハッカーたちは容易に脆弱性を発見して悪用できます。基本的には、クラウドサービスを追加するとネットワークへのアクセスポイントの数が増えます。


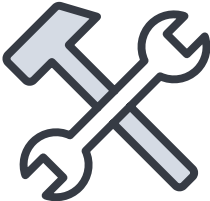


可視性の問題は、データガバナンスとコンプライアンスの問題にもつながります。複数のクラウドを利用することで柔軟性は向上しますが、規制遵守の課題も生じます。たとえば、許可されていない環境で誤ってアプリケーションを実行してしまうと、場合によっては一般データ保護規則(GDPR)の規制違反となります。こうしたガイドラインなどに違反すると、多額の罰金が科せられることもあります。

さまざまなネイティブクラウドツールによる 監視が引き起こす問題

- 視野のサイロ化
- 部門のサイロ化
- データのサイロ化



以下の要因により、クラウドにおける重大な問題の
特定、調査、解決が困難になります。

<p>可視化の欠如</p>  <p>クラウドサービスであるが故に起こる サービス品質の低下やダウンタイムを 把握できない</p>	<p>複雑なツール構成</p>  <p>複数のクラウドサービスを使用していると、 統一された監視戦略の確立が困難</p>
<p>MTTRの低下</p>  <p>障害の発生場所と原因の特定に 時間がかかりすぎる</p>	<p>規模に伴う困難</p>  <p>複数リージョン、複数アカウント、 複数クラウド環境からのデータ収集が困難</p>

マルチクラウド監視への 取り組み方

では、以上のような課題はどうすれば克服できるでしょうか。クラウドインフラの範囲が広がり、複雑さが増すにつれて、セキュリティチームやITチームが抱えるこれらの課題に対処する監視のソリューションと戦略を持つことの重要性が高まっています。

幸いなことに、マルチクラウドの利点を享受しながら、それに伴うリスクを軽減することは可能です。最近のITインフラはますます複雑化して

いるため、マルチクラウド環境全体の監視とトラブルシューティングを行える一元的な手段を持つことが不可欠です。適切なツールがなければ、現代の企業が障害やインシデントへの適切な対処に必要なデータを取得するはますます困難になります。一方、最新のITツールに投資している企業は、優れたカスタマーエクスペリエンスを提供できるだけでなく、イノベーションを推進し収益を最大化できます。

監視の課題を克服する方法



そのための最初のステップは、数多くの監視ツールやトラブルシューティングツールの代わりとなる、統合型のITインフラ監視ソリューションを見つけることです。監視とトラブルシューティングを別々のツールで行うと、いたずらに複雑さが増し、重大な問題が発生したときに迅速に対応できません。一方でツール構成をシンプルにすれば、どちらも同じソリューションで実行することができます。次に、データの取得をシームレスに行う必要があります。ここでは、データのオンボーディングをガイド付きで行うことが重要です。そのため、複数のクラウドベンダーからデータを収集し、すべてを1つにまとめて表示できるソリューションが適しています。さらに、さまざまなすべてのクラウド環境の運用、セキュリティ、コストを常に把握しておくことができます。

最後に、すべてのインフラ、アプリ、サービスの監視を統合し、AI(人工知能)や機械学習の機能を活用するソリューションがあれば、クラウドの障害を発生前に予測して防止するのに役立ちます。マルチクラウド環境で求められるのは、複数のクラウドからのデータを簡単に収集して保存でき、異なるクラウドサービスをまとめて一元的に表示し、環境全体のクラウドの使用状況を追跡できるソリューションです。

詳細はこちら

マルチクラウド環境の監視には多くの課題がありますが、クラウドインフラで起きていることを常に把握するためにツールをいくつも使う必要はありません。ツール構成をシンプルにしませんか。

[マルチクラウドに関する問い合わせまで、ぜひお問い合わせください。](#)