ハイブリッドクラウドに関する心得

NUTANIX™
YOUR ENTERPRISE CLOUD

プライベートクラウドおよびパブリッククラウドのどちらを選ぶかということは、多くのITマネージャーが昔から抱えている疑問です。ただし、それはハイブリッドクラウドを検討したことがない場合です。

ハイブリッドクラウドには、堅固なオンプレミスの基盤が必要です。そこからは、入念な計画と時間をかけた慎重な対応が求められます。

ハイブリッドクラウドに関する心得7選に目を通して、貴社のハイブリッドクラウドイニシアティブをスムーズに軌道に乗せましょう。

やるべきこと

やるべきこと その1

まずは強力なプライベートクラウドを構築する

プライベートクラウド化への流れは無視できないものになっており、**ForresterによるとITリーダーの79%はプライベートクラウドに投資していることが分かっています。**そのため、ハイブリッドクラウドに移行し始める前に、堅固かつセキュアなオンプレミス型アーキテクチャーを確保する必要があります。

今日の堅固なプライベートクラウドは、企業がパブリッククラウドに期待する俊敏性と柔軟性を提供できます。実際、プライベートクラウドに自動化、セルフサービス、およびAIを設計して、自社のデータセンターにパブリッククラウドのような俊敏性を備えることも可能です。なお、重要なデータ、またクライアントおよび財務情報の保護に必要な管理権限は維持できます。

高性能なプライベートクラウドを確立した後は、パブリッククラウドの性能に機能を拡張できます。ただし、オンプレミス型環境への管理性能を確実に保持することが重要なポイントとなります。**O'Reilly氏は、**次の3段階アプローチに基づく移行を推奨しています:

1. 単一のフレームワーク(「クラウドOS」)を選択しましょう。これは、オンプレミスおよびクラウドの両方におけるワークロードの管理を可能にします。
2. このフレームワークに従い、オンプレミス型環境を最新化します。
3. このフレームワークと互換性のあるパブリッククラウドとクラウドサービスプロバイダーのみを選択します。

なぜ、こうしたアプローチが必要なのでしょうか?理由は、クラウド間の相互運用性を維持する必要があるからです。これがなければ、ハイブリッドクラウドの「ハイブリッド」の部分が手に入らなくなります。単一のオペレーティングシステムであれば、単一のシンプルなツール一式で、各クラウド環境の監視、管理、そして自動編成が可能になるのです。

やるべきこと その2

ハイブリッドクラウド運用を標準化する

「やるべきこと」としては当然のように思えますが、それにはしっかりとした根拠があります。リクエストまたは開始する運用の種類は、クラウドの種類よりも重視されるべきであり、標準化でワークストリームを簡略化できます。

単にプライベートクラウドのツールをパブリッククラウドに拡張するのではなく、プライベートおよびパブリッククラウドにまたがる共通のツール一式を利用しましょう。結局のところ、全てのツールセットがクラウド対応型なわけではないため、希望通りにスケールアウト／アップできないかもしれません。また、この発想の下では、パブリッククラウドを自社データセンターの延長として捉えています。パブリッククラウドは強力な資産ではあるものの、別々かつ固有のアーキテクチャーとして本来取り扱う必要があります。

標準化ソリューションを採用することで、より優れたバランスを手に入れることができます。例として、IDおよびアクセス管理(IAM)、アプリケーションライフサイクル管理、セキュリティコンプライアンス、監視、およびコストガバナンスが挙げられます。こうしたソリューションは、プライベートおよびパブリッククラウド双方にまたがる環境を運用可能にする上で役立ちます。

やるべきこと その3

単一のマネージメントペインを利用する

どのようなクラウドを管理する場合でも、その実現には複数の担当者の関与が必要となりますが、ハイブリッドクラウドには独自の課題が存在します。こちらのGigaOmペーパーは、ハイブリッドクラウドが実装時の障害、高額なコスト、そして管理が不適切な場合は高リスクを露呈する可能性があると指摘しています。

幸い、中央管理ペインがあれば、コストとリソース消費に対する優れた可視性を手に入れることができます。最近のダッシュボードの多くは、カスタム最適化の推奨、リザーブドインスタンスなど、その他にも多くの性能を 提供できます。

Nutanix Beamは、チームのハイブリッドおよびマルチクラウド環境に対する洞察と可視性を提供できるため、最初の取り掛かりとしては最適です。ポリシーベースのガバナンスを備えたBeamは、企業がクラウドリソースを適正サイジングし、セキュリティ上の脆弱性が問題に変わる前に修正できるよう、リアルタイムの推奨を提供します。

Beamを2週間無料で試すにはこちらをクリック

やるべきこと その3

単一のマネージメントペインを利用する

どのようなクラウドを管理する場合でも、その実現には複数の担当者の関与が必要となりますが、ハイブリッドクラウドには独自の課題が存在します。こちらのGigaOmペーパーは、ハイブリッドクラウドが実装時の障害、高額なコスト、そして不適切な管理による高リスクを露呈する可能性があると指摘しています。

幸い、中央管理画面があれば、コストとリソース消費に対する優れた可視性を手に入れることができます。最近のダッシュボードの多くは、カスタム最適化の推奨、リザーブドインスタンスなど、その他にも多くの性能を 提供できます。

Nutanix Beamは、チームのハイブリッドおよびマルチクラウド環境に対する洞察と可視性を提供できるため、最初の取り掛かりとしては最適です。ポリシーベースのガバナンスを備えたBeamは、企業がクラウドリソースを適正サイジングし、セキュリティ上の脆弱性が問題に変わる前に修正できるよう、リアルタイムの推奨を提供します。

Beamを2週間無料で試すにはこちらをクリック

やるべきこと その4

セキュリティを1カ所で管理する

プライベートクラウドとパブリッククラウドが点在している場合、自動セキュリティ対応評価および修復ツールなしには、ハイブリッドクラウド全体にまたがるセキュリティギャップの追跡が困難になります。人的エラー、またクラウドの境界線にまたがるセキュリティポリシーのコンプライアンス欠如は、セキュリティギャップをさらに拡大し、大きな犠牲を伴うデータ漏洩を誘発する主要原因となっています。

ITチームは、クラウドリソースの管理、VM構成のセットアップ、仮想ネットワークの構築、クラウドワークロードの展開、可用性および性能基準の保持など、絶え間なく続き、反復的かつ骨の折れるタスクの責任を負っています。人間の力では、何千ものリソースおよび数百人のユーザーにまたがるセキュリティベースラインを手動で構築・維持することが不可能です。

集中管理セキュリティプログラムまたはサービスが無ければ、人的エラーのリスクが高まり、クラウドを危険に晒しかねないセキュリティ上の脆弱性を露呈してしまう可能性があります。脆弱性が出現した場合、企業はトラブルシューティングの必要性に駆られるため、貴重な時間が使い果たされることになります。

企業がクラウド全体にまたがるセキュリティを集中管理できる場合、複数のセキュリティツールに投資する必要も、データ漏洩事件をめぐって新聞の一面に掲載されるリスクを負うこともありません。NutanixのXi Beam のような自動化されたクラウドセキュリティ監査および修復サービスは、以下を通じてクラウド向けの高レベルなセキュリティ基準を確保して適用します:

- 1000件以上の自動クラウドセキュリティ監査
- 1-クリックでセキュリティの脆弱性を修正
- HIPAA、PCI-DSS、NISTなどに関するコンプライアンスチェック

やるべきでないこと

やるべきでないこと その1

サイロ化した知識がハイブリッドの導入を妨げる

ハイブリッドクラウドの崇拝者と導入者の間には、非常に大きな隔たりが存在します。2019年 Enterprise Cloud Index では、回答者の85%が、希望するクラウドコンピューティングモデルにハイブリッドクラウドの名を挙げています。ところが、同じレポートでは、実際の導入者がわずか12.6%であり、これは2018年のレポートから5.4%減少した割合だったことが明らかになりました。

なぜでしょうか？実は、多くの企業はハイブリッドクラウドの管理に必要な人的資源または知識を備えていないと危惧しているのです。企業は、ハイブリッドクラウドを稼働し続けるには専属のマネージメントチームまたは高額な専門家が必要ではないかと心配しています（特に、パブリッククラウド側）。また、際限のないIT予算を抱えた企業は数少ないため、専門家への支払いまたは既存チームの再訓練費用は、いずれも当然の懸念になります。

しかし、ハイブリッドクラウドの運用と管理を容易に 実現できる機会は、多数存在します。GigaOmは、ハイブリッドクラウド管理における自動化への投資が、特にクラウド支出、管理時間、そしてセキュリティギャップの削減において非常に重要であることを解説しています。

やるべきでないこと その2

パブリッククラウドをプライベートクラウドと同様に扱う

時に、企業は自社のオンプレミスの問題を解決できるのはパブリッククラウドであると考え、問題を実質的にパブリッククラウドベンダーに「引き渡す」場合があります。

しかし、現実的には、プライベートクラウドとパブリッククラウドには別々のアプローチが必要です。貴社のプライベートクラウドはセキュリティ規格に加え、セキュリティ自動化ツールも備えているかもしれませんが、パブリッククラウドと融合した場合はセキュリティ監査に関してより多くの責任を果たすことになります。

厳密には、共通責任モデルを確立し、不適当なリソースの割当てがないか継続的に確認して、パブリッククラウドにおけるワークロードを保護し続ける必要があります。ただし、パブリッククラウドベンダーはクラウドのセキュリティを担当しているものの、クラウド内のリソースのセキュリティは貴社の責任であることを忘れてはいけません。こうした理由から、プライベートからハイブリッドへの移行時にセキュリティおよび規制ポリシーのコンプライアンスを失うことがないよう、クラウドセキュリティポスチャ管理ツールが重要となります。

ビジネスプロセスとコンプライアンス要件をしっかりと保つ責任は、貴社にかかっています。重大なワークロードを移行する前に、ツールを確立してリアルタイムでハイブリッドクラウドを管理し、クラウドパートナーと選択肢を協議して、こうしたツールが貴社に適しているか確認しましょう。

やるべきでないこと その3

ハイブリッドクラウド固有の運用上の留意事項を無視する

ハイブリッドクラウドは素晴らしいものです。しかし、そのコスト、セキュリティ、そしてコンプライアンス対策に加え、健全性とアップタイムの測定・最適化手段はハイブリッド固有のものです。必ずしも複雑なわけではなく、単にユニークだと言えるでしょう。

その理由を説明しましょう。貴社のハイブリッドクラウドは、プライベートとパブリックという、2つの全く異なるタイプのクラウドに依拠しています。両者の構造、コンポーネント、ライセンスモデルは異なるため、片方のクラウドで上手く機能しないワークロードが他方では上手く機能する可能性もあります。しかし、違いがあるからといってサイロ化して導入するべきではありません。これでは、最終的に2組の複雑な運用基準と消費モデルが出来上がってしまいます。

求めているのは、ばらばらのクラウドではなく、シームレスな相互運用性です。自動化を実装することで、両方のクラウド上のユニークな環境を取り込み、最も適当な環境にワークロードを展開できます。そして、自動化はどのような環境でも理にかなっているものの、特にハイブリッドクラウドで高い利便性を発揮します。

本当のハイブリッドクラウドにたどり着くために

ハイブリッドクラウド環境の運用が複雑であるという話を聞いたことがあるならば、まだ思い切って一歩踏み出す気になれないかもしれません。

是非、当社にお問い合わせください。ハイブリッドクラウドへのスムーズな移行をご案内します。

NUTANIX™
YOUR ENTERPRISE CLOUD