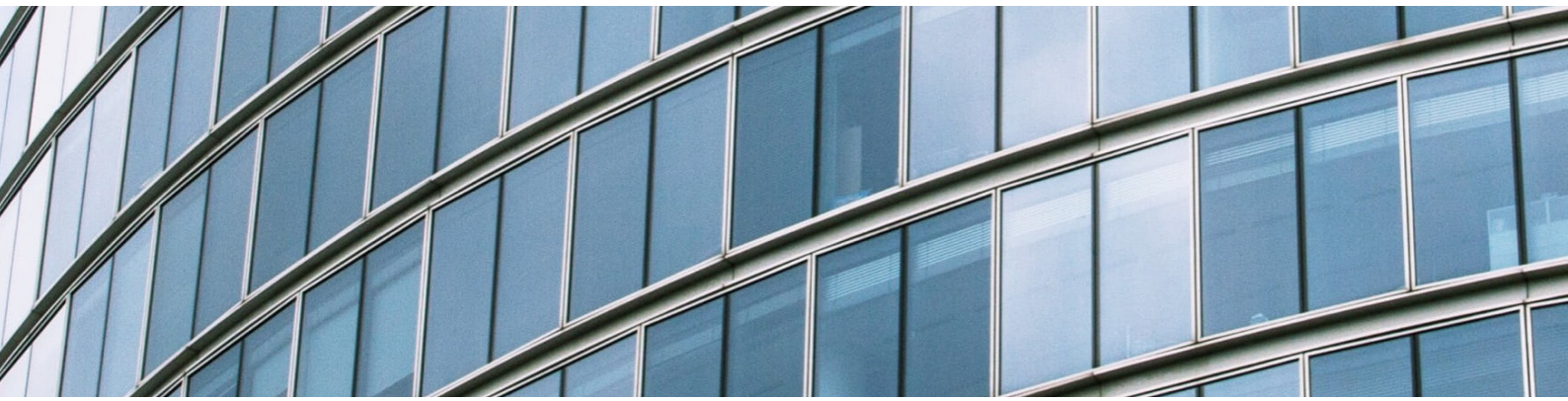
パブリッククラウドへの移行をスムーズに
－不可欠な４つのセキュリティとは－

ディプティ・パルマー */ フリーライター



最高レベルのセキュリティを引き継ぎながら、ITインフラがプライベートクラウドからパブリッククラウドへ移行する方法について解説する。

＊

エンタープライズソフトウェアとサービスのクラウド移行は、もはや企業にとっては必須課題で、あとはそのタイミングと方法が肝となる。

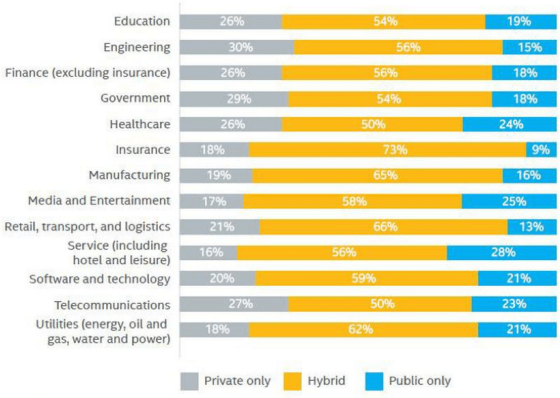


Figure 7. Which type of cloud architecture is your organization currently using? (grouped by industry)

クラウドプロバイダーは移行することのメリットを確信しているために、企業が重い腰を上げてそれを実行に移すまではそう待ってはくれない。ガートナーによると、クラウドプロバイダーの３分の１は、今年末までにクラウドファーストのソフトウェアからクラウドオンリーのソフトウェアの提供にシフトする予定だ。過去 10 年間の状況を見る限り、残りのプロバイダーも追随することになるだろう。

保険業界のように厳しい規制が敷かれている産業から、サービス業界やホスピタリティ業界など比較的規制が緩い産業に至るまで、プライベートクラウドからパブリッククラウドへと移行する傾向は急速に進んだ。そして、まだこれを進めていない企業がこの社会の潮流を避けることは今後不可能といえるだろう。

パブリッククラウドの魅力

パブリッククラウドは、アプリケーション開発者やソフトウェアプロバイダーの間で高い注目を集めたのが始まりだ。現在多くの企業がプライベートクラウドを減らし、パブリッククラウドを組み合わせたハイブリッドクラウドを導入している。

このクラウドが普及したきっかけを作ったのはこうした開発者たちだ。 ハードウェア、ライセンスおよびメンテナンスなど先行投資にかかるコスト削減を考慮す

ると、パブリッククラウドはIT部門と財務部門の両方にとって魅力的で価値のある選択肢である。

ハイブリッドクラウドは、通信速度と信頼性を両立しているため、常に優れたパフォーマンス性能が不可欠なアプリケーションやソフトウェアを管理できる理想的なエコシステムなのだ。

パブリッククラウドプロバイダー間の競争により、イノベーション主導型のクラウド環境を維持している。ある程度は開発者側で既存のインフラに構築できるため、企業はアップグレードの頻度を減らして支出を最小限に抑えることができる。

また、クラウドサービスでは変化するワークロードと予算に基づいて、フットプリントを拡大または縮小することも可能だ。

理想の世界ここにあらず

このようなメリットは、パブリッククラウドを使用する際の警告とともに、事業運営を効果的かつ効率的に進める。

パブリッククラウドはスケーラビリティを瞬時に提供するだけでなく、IT管理者の管理権限を無効にし、データとシステムをCSP（クラウドサービスプロバイダー）のポリシーに組み込む。

通常、パブリッククラウドでの自社アプリケーションの実行場所やデータを保存場所となる地理的地域を企業が選択できる。

しかし、特定の国や都市など正確な場所を常に選択できるとは限らず、パブリッククラウドに重要なサービスやアプリケーションがあると、サーバーの問題やCSP側のシステム障害による機能停止に関わらず業務が中断されてしまう。

パブリッククラウドに存在するデータの安全性は、CSPが管理するネットワークの最も脆弱なゲートウェイと同程度だ。

パブリッククラウドで保存される、顧客、医療および財務などの詳細が含まれた機密性の高い企業データが増加するにつれて、CSPはハッカーにとって非常に魅力的な標的となる。

問題が完全に制御不能になることもある。テナントのひとつがシステムのセキュリティ保護に失敗した場合、他のテナントのデータにもサイバー攻撃または侵害が及ぶ。

業務を中断せずにパブリッククラウドへ乗り替える方法

パブリッククラウドとハイブリッドクラウドは広く普及している。それらにまつわる課題やサイバー攻撃よりも、導入するメリットがはるかに多いからだ。ポリシーとクラウドの実行を適切に組み合わせることで、多くの攻撃を制御して軽減することができる。

【1】クラウドのセキュリティモデルを再考

クラウド運用に必要なセキュリティシステムの開発における従来の認識は、このクラウドコンピューティングの移行期には悩みの種。従来のオンプレミスのアプリケーションとインフラでシステムが動作していても、パブリッククラウドを中心にクラウドでは機能しない。

パブリッククラウドはオンプレミスシステムとは異なり、クラウド内のアセットを保護するための制御やカスタマイズできる範囲が制限されている。そのような状況では、パブリッククラウドのネットワークにアプリケーションのアーキテクチャが存在することを念頭に入れながら再調整することで、セキュリティを強化することが適切だ。

別のアプローチとして、ネットワークの境界を明確に定義してデータとアプリケーションへの侵害を抑制する方法がある。

【2】DIY（自分のことは自分でやる）への誘惑を避ける

プライベート、オンプレミスまたはハイブリッドの環境からパブリッククラウドに移行する主な理由はコスト削減だ。

コスト削減に注力するあまり、IT管理者はデータ、アプリケーションおよび関連インフラを扱うには安全性や信頼性に欠けるありきたりな戦略に基づいたDIYプロセスに頼ることが多すぎる。

マカフィーの調査によると、50％近くの企業が「適切なスキルを持つサイバーセキュリティの専門家の不足が原因となり、クラウド移行をためらっている」と回

答している。クラウドへの移行が一見容易だったとしても、専門家は不可欠なのだ。

あるいは、Nutanix Move など専用のアプリケーションを実装し、クラウドの移行に伴うすべての重労働をシームレスかつ自動で行うと良いだろう。

【3】成功も失敗も全体責任

パブリッククラウドに関するマッキンゼーのレポートには、「企業と CSP は、パブリッククラウド環境でのサイバーセキュリティにおける責任を明確に振り分けないと、責任問題が放置される可能性がある」と記載されている。

過去 5 年では、CSP と企業の間で「クラウドネットワークのセキュリティに関わる責任は CSP にある」という暗黙の了解があった。

CSP は、システムの使用状況とリアルタイムのセキュリティアラートの定期的な分析に多要素認証を提供する。一方、企業には、パスワードと個人情報をハッシュ化やソルティングをすることで、クラウド上のすべてのデータのセキュリティを適切に管理する責任がある。

セキュリティを最優先してアプリケーションのアーキテクチャを設計することで、クラウドリソースを適切に管理することができる。

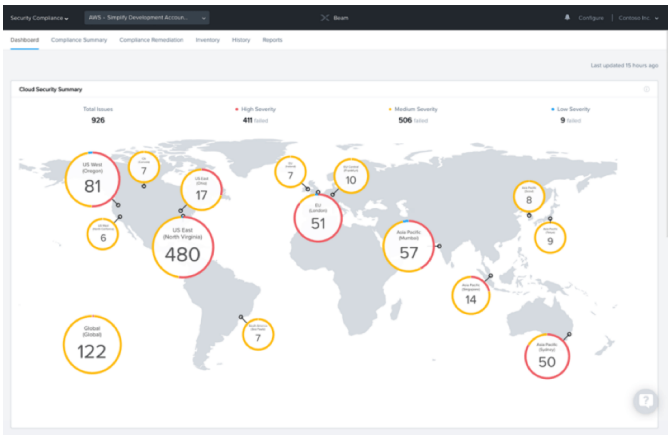
【4】プライベート、パブリックおよびオンプレミスのリソース管理を連携

プライベートクラウド、パブリッククラウド、オンプレミスあるいは全てを組み合わせたものを使い分けて、アプリケーションを実行することは一般的だ。

しかし、上述のとおり、各エコシステムを管理するために必要なセキュリティはそれぞれ異なり、間違った手法をクラウドまたはオンサイトのネットワークに無理やり統合させると大惨事を招きかねない。

クロスプラットフォームの包括的なセキュリティスイートへの投資は、パブリッククラウド上でもそれ以外でも、アセットを保護する優れた方法だ。

例えば、マルチクラウド向けセキュリティソリューションの Nutanix Beam は、IT 管理者にすべてのクラウドデータ、アプリケーションおよびインフラ全体に完全な可視性を与えるだけでなく、セキュリティの脆弱性をリアルタイムで特定し修正を施す。



＊

2019 年の State of the Cloud Survey では、大企業の 84％がマルチクラウド戦略を採用しているのに対し、中小企業は IT エコシステムの一部として、5 つ以上のパブリックまたはプライベートクラウドを使い分けていることが明らかになった。

IT 業界だけではない、急速に変化するビジネスに関わる全ての現実世界では、熟考された明確なクラウドセキュリティのポリシーを詳しく説明し、実行へ移すことが重要であり不可欠なのだ。

(2019 年 9 月 11 日 , THE FORECAST by NUTANIX)
記事構成：ニュータニックス・ニュース！ 編集部 , Nutanix Japan

＊ディプティ・パルマー氏は寄稿ライター、デジタルメディアエディター。彼女は CIO.com、Entrepreneur、CMO.com に寄稿している。

NUTANIX
YOUR ENTERPRISE CLOUD
お問い合わせ：03-4588-0520
info-jp@nutanix.com | www.nutanix.com/jp | @NutanixJapan
東京都千代田区大手町 1-1-1 大手町パークビルディング 7F