パブリック クラウドに関する推奨事項トップ 10

パブリック クラウドへの移行は、インターネットが爆発的に普及した 2000 年台初頭以降に進展した最大のコンピューティング パラダイムです。451 Group® によると、エンタープライズの IT 役員は、2018 年までにワークロードの 60% がクラウドで動作するようになると予想しています。[1] この成長を牽引する要因として、企業の競争優位性の確保に貢献する俊敏性や拡張性の向上、パフォーマンスの向上、革新的なテクノロジへの早期アクセスなどが挙げられます。

パブリック クラウドを初期段階で導入すれば、ビジネス、生産性、俊敏性の新たな機会が生まれると同時に、潜在的なセキュリティ リスクにもさらされることになります。パブリック クラウドに関して、周知の事実が 2 つあります。1 つ目は、パブリック クラウドは本質的に他人のコンピュータであるということです。仮想化されたリソース (コンピューティング、ネットワーク、およびアプリケーション) の一式をサード パーティが所有するシステム上で制御しているに過ぎません。2 つ目は、パブリック クラウドはネットワークを拡張したものであるということです。その一方で、パブリック クラウド上のアプリケーションとデータがどの程度安全であるのかは、あまり理解されていません。クラウド サービス プロバイダのインフラストラクチャは極めて安全である可能性が高いものの、利用者側の取り組みがなければ、パブリック クラウド上のアプリケーションとデータを保護することはできません。

攻撃者は場所を問いません。パブリック クラウドであろうと、プライベート クラウドであろうと、物理的データセンターであろうと、その目的は、ネットワークを侵害して、そこにあるユーザー データや知的財産、コンピューティング リソースを盗むことです。パブリック クラウド上のアプリケーションやデータを保護するために必要な対策を講じる責任は利用者側にありますが、パブリック クラウドの導入を推進するビジネス グループや DevOps チームの多くは、この事実を十分に認識していません。このホワイトペーパーは、セキュリティ チームが早い段階から関与して適切な質問を提示し、データセンターと同じように入念にパブリック クラウドを保護できるよう、セキュリティ チームに必要な情報を提供することを目的としています。

1. https://451research.com/blog/764-enterprise-it-executives-expect-60-of-workloads-will-run-in-the-cloud-by-2018

目次

パブリック クラウド ワークロードの保護に関する考慮事項トップ 10

以下に、パブリック クラウド上にあるデータやアプリケーションを効果的に保護するための 10 の主な考慮事項について説明します。パブリック クラウドは、絶えず進化する多数のセキュリティの脅威にさらされており、そのほとんどは従来のオンプレミスのデータセンターが直面する脅威に酷似しています。

共有セキュリティ モデルの採用

Amazon® Web サービス (AWS®) や Microsoft® Azure® などのパブリック クラウド プロバイダでは、セキュリティが共有責任であることを明言しています。このモデルでは、プラットフォームの常時稼働と可用性を維持し、最新状態に保つことなどはプロバイダの責任とされます。

実際、大半の人は、クラウド プロバイダが持つグローバル データセンター インフラストラクチャの方が、自社が保有するインフラストラクチャよりも安全であると信じています。しかし、パブリック クラウド内で動作しているアプリケーションやデータを保護する責任は顧客側にあるという事実についてはあまり知られていません。

図 1 は、責任範囲の内訳を解説しています。パブリック クラウドのワークロード (わかりやすくするため赤で示しています) を保護することは、オンプレミスのワークロードを保護することと何ら違いはありません。どのようなセキュリティを実装するのかはパブリック クラウドの利用者側ですべて管理するため、顧客データであれ、知的財産であれ、自社のコンテンツを保護するための手段を講じる必要があります。

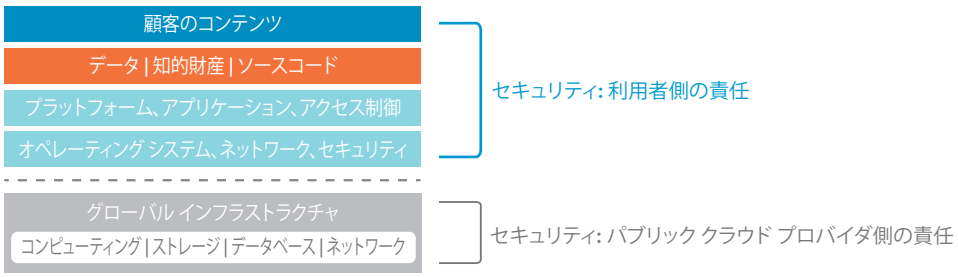


図 1: パブリック クラウドの責任共有モデル

ビジネス グループや DevOps チームとの早期の協働

多くのパブリック クラウド プロジェクトは、新たな製品や機能プロトタイプを迅速に展開する DevOps などのビジネス グループによって推進されます。課題が発生するのには 2 つの要因があります。1 つは新たなアプリケーション アプローチの一般提供によるもので、もう 1 つは導入支援のために投入されることが多いセキュリティ チームによるものです。どちらであっても、アーキテクチャに潜むセキュリティ ホールが明らかになります。

セキュリティ チームと DevOps が連携してパブリック クラウド プロジェクトの範囲を把握し、その上でセキュリティ リスクを軽減しつつもビジネス上の開発ニーズを確実に満たすアプリケーション導入アーキテクチャを構築することが理想的です。

漏えいの可能性について

パブリック クラウドではアカウントを容易に取得できるため、パブリック クラウドの使用は、よく「シャドウ IT」と呼ばれます。環境が適切に設定されていなければ、従業員が「業務的に正しいこと」を行うことがセキュリティ ホールの発生につながりかねません。組織内の誰がパブリック クラウドを利用しているかを把握し、環境を正しく設定することが必要不可欠です。

- **パブリック クラウドの使用の監視 :** パブリック クラウドの使用の有無を判断するには、最寄りのパブリック クラウド プロバイダの営業担当者に連絡して、自社がどの程度 AWS または Azure を利用しているのかを聞くのが最も手っ取り早くて正確な方法です。また、ネットワーク可視化ツールを使えば、ネットワーク アプリケーション トラフィックに基づいて、利用状況に関する洞察を得ることができます。

- **適切な設定の徹底 :** 環境の設定にあたっては、セキュリティのベスト プラクティスを念頭に置きます。例えば、AWS の各サービスでは一連のアプリケーション プログラミング インターフェイス (API) が公開されていますが、API を利用しない場合は無効化する必要があります。AWS の新規ユーザーの多くは、Amazon Simple Storage Service が公開サービスであり、ポリシーによってロック ダウンしない限り、保管データはすべてインターネット上で公開されることを知らない可能性があります。Azure では、リソース グループ内に初期 VNet を構築する場合、アウトバウンド ポートはデフォルトですべて開いており、不要な漏えいを招くおそれがあることを理解する必要があります。
- **2 要素認証の強制的な適用 :** Verizon が公開している「データ漏洩 / 侵害調査報告書」の最新版によると、ハッキング関連の侵害の 81% は、盗み出された認証情報または脆弱なパスワードを利用しています。盗み出された認証情報を使用して攻撃者がアクセスを得るリスクを最小化するために、2 要素認証を適用します。
- **SSH のロック ダウン :** Secure Shell (セキュア シェル - SSH)® は、クラウド サービスの安全な制御方法として推奨されていますが、AWS や Azure の環境では、公開された状態で放置されていることがほとんどです。多くの場合、組織には暗号鍵や証明書インベントリに関する明確な理解が不足しているため、サイバー攻撃者が巧みに利用する脆弱性をさらしてしまっています。SSH アクセスが可能なサイバー攻撃者は、組織のクラウド インフラストラクチャを活用して、容易にボットネットベースの攻撃を仕掛けることができます。

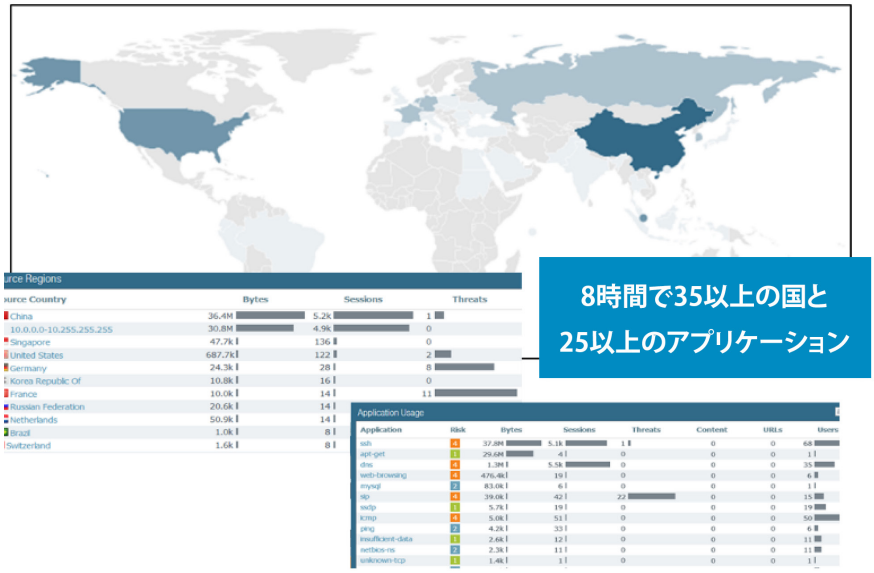


図 2: パブリック クラウドの自動化テスト環境

攻撃者の理解

攻撃者は自動化を活用することで、攻撃可能な候補を数分以内に見つけます。候補を特定したら、デフォルト パスワードが使用されていないか、SSH の設定にミスがないかなど、弱点を探り始めます。

攻撃者の自動化機能の効果を浮き彫りにするため、SQL データベースと WordPress® サーバのインスタンスをインストールしたテスト環境をパブリック クラウドに設置してみました。図 2 が示すように、この環境は、8 時間以内に 35 か国以上から 25 以上の異なるアプリケーションによってプローブされたのです。プライベートなデータセンターでは一般への漏えいに関する懸念はそれほどありませんが、パブリック クラウド上にあるリソースは幅広い脅威にさらされています。この例から、パブリック クラウドにおけるセキュリティがいかに重要であるかが改めてわかります。

セキュリティ オプションの評価

パブリック クラウドへ移行する際には、さまざまなセキュリティ オプションを選択できます。そのほとんどは物理的なネットワークと同様のオプションです。

- **ネイティブのパブリック クラウド セキュリティ :** クラウド サービス プロバイダは、セキュリティ グループや Web アプリケーション ファイアウォール (WAF) など、ネイティブのセキュリティ サービスを提供しています。これらのツールを使えば攻撃対象領域を縮小することができますが、それでもセキュリティ ギャップは存在します。
  - セキュリティ グループは実質的にはポート ベースのアクセス制御リストで、フィルタリング機能を提供するものです。ただし、許可されている特定のアプリケーションを識別したり、効果的に制御したりすることはできない上に、脅威を防止したり、ファイル移動を管理したりすることもできません。
  - WAF は HTTP および HTTPS アプリケーションのみを保護し、その他のトラフィックは無視します。ファイアウォールは常に重要ですが、WAF は必ずしも必要ではありません。また、Microsoft Lync®、SharePoint®、Active Directory® などは、正常に機能するためには隣接する広範なポートを使用する必要がありますが、このようなアプリケーションは WAF では保護できません。さらに、SSH や Microsoft RDP といったリモート管理ツールやアクセス ツールを識別して制御するには、あまり効果的な手段ではありません。
- **ポイント製品 :** パブリック クラウドの保護に採用される最も一般的なアプローチの 1 つでは、ホストベースのポイント製品を使用して脅威の検出と防止を行います。このアプローチの人気の背景には、ネイティブのセキュリティを IDS または IPS と組み合わせれば、導入環境を十分に保護できるとする考えがあります。しかし実際には、IDS では手作業による操作や修復が必要なため、クラウドの速度や俊敏性に対して直感的とはいえません。一方、IPS は既知の脅威しか検出できないため、ゼロデイ攻撃や未知の脅威を見逃す可能性があります。そのため、どちらの手法でもパブリック クラウド環境を包括的に捉えることはできません。
- **内製型のセキュリティ :** 一部の組織では、スクリプトや可視化ツールを使用して導入環境を保護するなど、内製型のアプローチによってパブリック クラウドのワークロードの保護に当たっています。この戦略には、十分なリソースがない、セキュリティの実装や運用を管理するための専門知識が不足している、セキュリティ侵害が発生した場合のサポート体制がない、といった欠点が潜んでいる可能性があります。

パブリック クラウドとセキュリティの導入環境の管理を社内の人材に頼っている組織は、消耗戦になることを覚悟しておく必要があります。一般的に、環境を熟知しているエンジニアは数人しかおらず、ドキュメントを適切に整備したり、知識共有の要件を管理したりする余裕はないのが現状です。わずか 1 名が退職しただけでも、今後のセキュリティ ニーズの効果的な管理体制を維持できなくなる可能性があります。

- **インライン仮想化アプライアンス :** 仮想化次世代ファイアウォールなどのインライン仮想化アプライアンスは、クラウド導入環境におけるすべてのトラフィックを可視化する基盤を提供します。統合された次世代セキュリティを採用することで、アプリケーションベース、ユーザーベース、コンテンツベースの識別テクノロジを使用して、実際に誰が何にどのような目的でアクセスしているかを正確に把握して、パブリック クラウドのアプリケーションやデータの保護を強化することができます。これによって把握した情報を基に動的なセキュリティ ポリシーを適用することで、場所を問わずにアプリケーション、コンテンツ、ユーザーの安全な運用を実現できると同時に、パブリック クラウド展開環境のデータやアプリケーションを標的型攻撃や過失による脅威から保護することもできます。

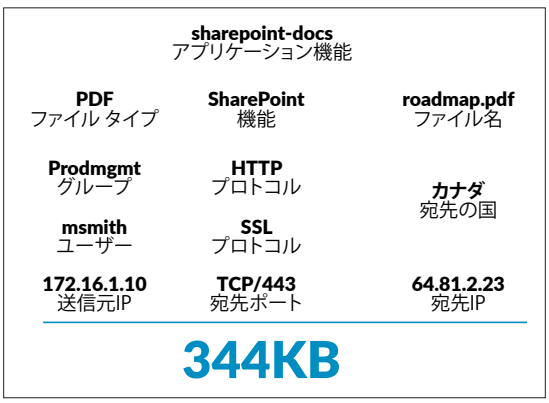


図 3: 完全なトラフィック フロー コンテキスト

知識は力なり

パーソナル ブランド化コンサルタントの John Antonios はかつて「知識に行動を加えれば、それは力となる」と述べています。パブリック クラウド セキュリティにおける「知識」とは、モバイル、ネットワーク、クラウドを横断した、環境を通過するすべてのトラフィックの安全を確保することから始まります。

これらの環境を通過するデジタル データの量は膨大です。組織は、ネイティブに統合された包括的なセキュリティ プラットフォームの一部として仮想化次世代ファイアウォールを活用し、トラフィックの識別情報や特徴に関する必要な洞察を獲得することで、情報に基づくポリシーの意思決定を行い、アプリケーションやデータを脅威から保護することができます。

パブリック クラウドのネイティブのツールでは、アプリケーション層はほとんど可視化できません。また、データを正確に解釈するためには、ネットワークに関する詳細な知識が必要な場合もあります。データを正しく解釈できたとして、344KB のデータが送信元の IP アドレスとポートから宛先のアドレスと TCP 443 に流れていることがわかったところで、TCP 443 を使用できるアプリケーションは数百にものぼるため、あまり価値はありません。

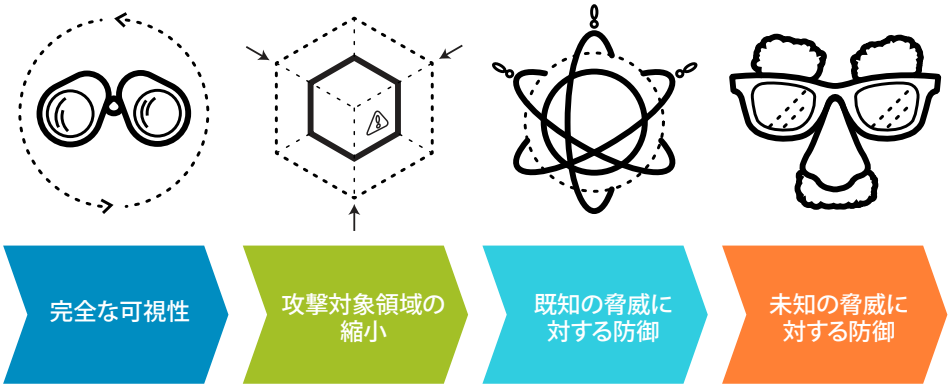
一部のハイブリッド導入環境では、パブリック クラウドは IPsec VPN 経由で企業ネットワークと接続されており、ポートベースの制御を使用してアクセスを TCP 80 と TCP 443 のみに制限すれば十分だと考えられています。漏えいが起きるのは企業側からのアクセスに限定されているというのがその根拠です。これは、根本的に間違った考え方です。

- リモート アクセス ツール、迂回ソフトウェア、プロキシなど、TCP 80 と TCP 443 を使用できるアプリケーションは 500 以上あります。
- 多くの場合、アプリケーションを使用するには、DNS、NetBIOS、そして場合によっては SSH などのプロトコルやサービスを追加する必要があるほか、それぞれに対応したポートを開く必要もあります。
- 最も一般的な開発ツールである Chef や Puppet では、次のようにさまざまなポートを開く必要があります。
    - Chef の外部公開ポート : 80、112、443、4321、5432、5672、8000、8983、9683、9090、15672、16379、7788 ～ 7799
    - Puppet の外部公開ポート : 25、443、8081、8140、61613

ポート制御では、アプリケーション トラフィックや内部にあるコンテンツ、ユーザーなどを、コンテキストを判断して認識することはできず、初期レベルの制御しかできないのが現実です。図 3 に示すように、トラフィック フローの完全なコンテキストを理解することで、確かな情報に基づいたセキュリティ ポリシーの意思決定を行うことができます。コンテキストとして、例えば、送信元 / 宛先の IP や国、プロトコル、活動を支援するユーザーまたはユーザー グループ、URL カテゴリ、アプリケーション ID や使用する特定のアプリケーション機能、特定のファイル名やタイプなどを理解する必要があります。

防御という考え方

攻撃者が既に「侵入に成功している」という考えの人たちは、検出 / 修復アプローチを実装することを選択しています。しかし、自社の環境を完全に把握できていれば、防御という理念を実現可能です。サイバー攻撃からの防御をパブリック クラウドで実現するには、重要な能力として次の 4 つが必要です。



完全な可視性

知識と実行を組み合わせれば、強力なセキュリティ ツールになります。ネットワーク上およびパブリック クラウド内のアプリケーションを識別することは、ポート、プロトコル、回避戦術、暗号化などに関係なく重要です。同様に、アプリケーションの特徴、使用されている特定のアプリケーション機能、相対的なリスクなどを識別することも重要です。これらの知識を活用して、より一貫性のあるセキュリティ ポリシーをグローバルに導入することで、既知および未知の攻撃からネットワークを保護することができます。

攻撃対象領域の縮小

肯定的セキュリティ モデルの執行手段としてアプリケーション ID を使用することで、許可されたアプリケーションのみを使用可能化して他を拒否できるため、攻撃対象領域が縮小されます。ビジネス ニーズに合わせてアプリケーションの使用を調整したり、アプリケーション機能を制御したり (SharePoint ドキュメントは全ユーザーが使用可能だが SharePoint 管理アクセス権限は IT グループに限定するなど)、脅威によるアクセスの取得や、ネットワーク内での横方向の移動を阻止します。

既知の脅威に対する防御

アプリケーション固有の脅威防御ポリシーを許可されたアプリケーション フローに適用することは、防御の理念を維持する上で極めて重要です。アプリケーション固有の脅威防御ポリシーは、既知の脅威を阻止します (脆弱性エクスプロイト、マルウェア、マルウェアを生成する C&C トラフィックなど)。

未知の脅威に対する防御

未知の、潜在的に悪意のあるファイルは数百におよぶ動作に基づいて分析されます。ファイルに悪意があると判定された場合、防御メカニズムが 5 分以内に配信されます。防御手法が配信されると、分析から得た情報を使用して、他のすべての防御機能が継続的に改善されます。

クラウド中心のアプローチ

パブリック クラウドでは、組織は、より俊敏性の高いスケーラブルなアプローチでビジネス課題に対処することができます。クラウドをフル活用するための推奨ベスト プラクティスには、「従来の構造から離れて、データセンターの概念を導入環境に適用すること」が含まれます。こうすることで、高可用性と拡張性を実現できます。

2 デバイス構成の従来型の高可用性を例に取ると、その高可用性の前提条件をパブリック クラウド導入環境にも適用すべきだと仮定できます。ただし、パブリック クラウドでの運用は他人のコンピュータ上での運用であるため、ハードウェアベースのアクセラレータが実現する 1 秒未満のフェイルオーバーといった利点は享受できません。デバイス インスタンス間でのフェイルオーバー プロセスは、ソフトウェアによって実行されます。これは、環境によっては最大 60 秒かかり、異なる地域間ではフェイルオーバーできない可能性があります。クラウド中心のアプローチでは、クラウド プロバイダのファブリックとその固有の復元機能 (ロード バランシングなど) を活用して、高可用性の目標を迅速かつシームレスに達成します。

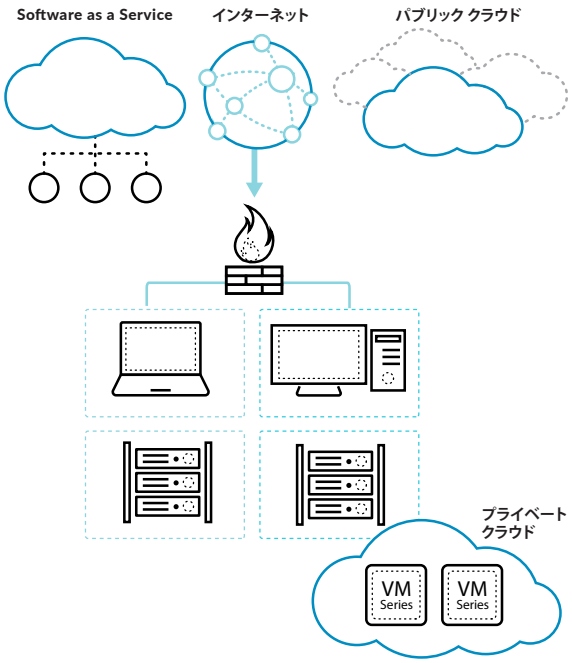


図 4: クラウド中心のアプローチ

自動化の活用によるボトルネックの解消

急速な変化が一般的であるパブリック クラウドにおいては、自動化が中心的な理念になります。セキュリティのベスト プラクティスの変更管理策を踏襲した場合、変更管理策が有効になるまでには時間がかかります。そのため、その遅延によって摩擦が生じ、導入が遅れる可能性があります。さらに、変更管理策が有効になるのを「待たずに」導入を行うと、セキュリティが低下することすらあります。パブリック クラウドのセキュリティを自動化することで、組織はセキュリティがもたらす“摩擦”を解消し、パブリック クラウドが提供する柔軟性と俊敏性といった利点を享受することができます。パブリック クラウドのセキュリティを実現する上で組織が求めるべき自動化ツールには、次のようなものがあります。

- **タッチレス導入 :** ブートストラップなどの機能を活用することで、わずか数分で完全に設定されたファイアウォールを導入し、パブリック クラウド上の分離された仮想ネットワーク環境 (Azure リソース グループ、AWS 仮想プライベート クラウドなど) を保護することができます。
- **サードパーティ リソースとの双方向の統合 :** サードパーティのツールやデータと API を主体として統合すると、セキュリティ運用の合理化に役立ちます。例えば、ServiceNow® と統合することで、サービス チケットやワークフローを効率的に生成できます。
- **「コミットなし」のポリシー更新 :** XML API やダイナミック アドレス グループなどの自動化機能を活用することで、ワークロードの変化に合わせた動的なセキュリティ ポリシー更新を実現できます。環境の変化に基づくセキュリティ ポリシー更新を迅速化、正確化することで、組織はクラウドの速度で運用を行うことができます。

管理の一元化による一貫したポリシーの適用

パブリック クラウド上のデータやアプリケーションに対して効果的なセキュリティを維持するには、一貫したポリシーが欠かせません。物理および仮想ファイアウォールの分散ネットワークを一元管理し、ネットワークからパブリック クラウドに至るまで、一貫した単一のセキュリティ ルール ベースを適用することは、セキュリティの機能と効率を維持するために重要です。管理の一元化により、ネットワーク全体のトラフィックや脅威に関する洞察が得られ、パブリック クラウドにおけるワークロードが変化する中で、管理を簡素化し、セキュリティ ポリシーの遅れを最小限に抑えます。

まとめ

市場投入期間の効率化、ビジネス全体の改善、継続的な競争優位性の確保などを実現するためにパブリック クラウドを導入する組織が増えています。しかし、導入を進めているのはビジネスを中心に考えるグループであり、必ずしも導入プロセスにセキュリティ チームが十分に関与しているとはいえません。前述したセキュリティに関する考慮事項は、一般的な経験に基づいており、啓発的で役立つ内容となっています。セキュリティ グループとビジネス グループ間の対話を促し、双方のグループの需要を満たすパブリック クラウド アーキテクチャの構築と導入を実現することが理想的な目標です。

詳細については、以下のリソースを参照してください。

- Web ページ : **パブリック クラウドの保護**
- ホワイトペーパー : **Securely Enabling a Hybrid Cloud in Microsoft Azure (Microsoft Azure におけるハイブリッド クラウドの安全な使用)**
- ホワイトペーパー : **VM-SERIES FOR AWS ハイブリッド クラウド デプロイメントガイドライン**

〒 102-0094
千代田区紀尾井町 4 番 3号
泉館紀尾井町 3F
電話番号 : 03-3511-4050
www.paloaltonetworks.com

top-10-public-cloud-security-recommentation-eg-080217