VMware vCloud Air
セキュリティに関する FAQ

Q：VMware vCloud® Air™ では、業界の規制やセキュリティ認定に関する監査が行われていますか

A：現時点で、VMware vCloud Air は情報セキュリティ マネジメント システムに関する ISO / IEC 27001:2005 認定を受けています（https://www.brightline.com/certificate-directory/Y8eJUUXMjLA3/）。また、SOC II Type 1、SSAE 16 SOC 1 Type II、および SOC 2 Type II の監査を完了しています。HIPAA / HITECH の該当する規制に対する監査も完了しているため、米国内のデータセンターを使用するお客様は、必要に応じて、Business Associate Agreement（BAA）を締結することが可能です。ISO、SOC、および HIPAA / HITECH の監査は、ANAB から認可された認証機関である Brightline CPAs and Associates 社によって実施されました。vCloud Air は、セーフハーバー認定も受けており、欧州のデータ プライバシー コンプライアンス規制に準拠しています。日本のデータセンターの認定状況に関しては別途お問い合わせください。

Q：ネットワーク境界はどのような方法で保護されますか

A：vCloud Air のアーキテクチャは、お客様に割り当てられるテナントのネットワーク エントリ ポイントを保護するように設計されています。テナント境界を保護するために、可用性に優れたエッジ ゲートウェイと、セグメント化されたネットワークを活用します。これらは各テナントに固有で、各テナントのユーザーが独自に構成できます。制御 / 管理プレーンを攻撃から守るには、お客様固有のポリシー、侵入検知、およびネットワークのセグメンテーションを構成したファイアウォールを使用します。このファイアウォールにより、VMware のソリューションで管理するすべてのインフラストラクチャ コンポーネントへの脅威が削減され、ゼロデイ攻撃などの異常の検出と低減が可能になります。

サブスクリプション契約者が管理者として制御可能なネットワークのセキュリティについては、最終的にその責任を契約者が負うものとなります。これには、効果的なファイアウォール ルールの維持、ビジネスに必要な通信ポートのみの公開、プロミスキャス アクセスの無効化、安全な VPN アクセスなどが含まれますが、これらに限定されません。

Q：このサービスに使用しているデータセンターには、どのような物理セキュリティを採用していますか

A：vCloud Air のデータセンターは世界的な水準の施設に設置されており、さまざまなレベルの物理的なセキュリティを採用しています。これには、次のような対策が含まれます。

- マントラップ / エア ロック
- 許可証による入場規制
- ロックされたセキュリティ ケージ
- 生体認証
- 安全に分離されたストレージ エリア
- 24 時間 365 日警備員が常駐

Q：パブリック テンプレート カタログにパッチは適用されますか。また、その頻度を教えてください

A：VMware は、vCloud Air 内ですぐに利用可能なオペレーティング システムとパッケージングされたアプリケーションを、「パブリック テンプレート カタログ」を通じて提供しています。このパブリック カタログは、最新の更新をまとめたロールアップ アップデートによって定期的に更新されます。重要度と緊急性が高い場合、パッチをカタログ オブジェクトに展開することがあります。

Q：VMware は、サービスのパッチ管理をどのように行っていますか

A：VMware は、vCloud Air の提供に使用するシステムの保守を行います。これには、管理レイヤーのアプリケーションや、パブリック カタログ イメージ / テンプレートへのパッチ適用も含まれます。VMware は、サービスを提供するシステムの脆弱性検査を定期的に行い、リスクのある領域を特定し、必要に応じてパッチを適用します。基盤インフラストラクチャにパッチを適用する際は、サービスのアーキテクチャの仕様上、サブスクリプション契約者やユーザーに透過的にパッチが適用されることがあります。

vCloud Air に展開されているオペレーティング システムとワークロードについては、パブリック テンプレート カタログで提供しているオペレーティング システムとアプリケーションのみ、VMware がパッチとアップデートを適用します。VMware がパッチとアップデートを適用するのは、パブリック カタログ内のテンプレートに限られるため、お客様が展開するワークロードは、お客様自身でパッチを管理していただく必要があります。

Q：すでに所有しているセキュリティ ソフトウェアやその他のツールを環境の監視に使用できますか

A：はい。サブスクリプション契約者が管理スタックを直接監視することはできませんが、VMware Solution Exchange で提供されているようなネットワーク アプライアンスや、エージェント ベースのセキュリティ / 監視ツールを展開することができます。ユーザーはこれらを使ってサービスの安定性と整合性を確保することができます。また、vCloud Network and Security Edge Gateway によって、ロード バランシング、VPN、ファイアウォール、および NAT サービスが提供されますが、サブスクリプション契約者がサードパーティ製のネットワークおよびセキュリティのソリューションを追加することも可能です。このようなネットワークやセキュリティのサードパーティ製ユーティリティを vCloud Air 内に展開する場合は、セキュリティ要件を満たしていることをお客様自身で検証する必要があります。VMware Solution Exchange で提供される仮想アプライアンスはサポート対象とみなされますが、VMware はその保守を行いません。vCloud Air では、お客様が vCloud Air と同じデータセンター内でコロケーション スペースを確保し、そこに設置した設備を利用できます。そこで任意のセキュリティ ツールなどを展開することで、プライベート データセンターと同じ制御、セキュリティ ツールなどを柔軟に活用することができます。

Q：VPN トンネルを使用してこのサービスに接続することはできますか

A：はい。このサービスでは、VMware vCloud Director® のユーザー インターフェイスから Edge Gateway サービスを使用して、IPsec VPN トンネルを作成できます。セルフサービスでの VPN トンネル作成にはいくつかの方法があります。同じ組織の仮想データセンター内のネットワーク間、異なる組織の複数の仮想データセンターのネットワーク間（専有型クラウドのみ）、およびローカル データセンター内のネットワーク間を、ソフトウェアまたはハードウェアの VPN ソリューションを使用して接続できます。

IPsec VPN の確立はセルフサービスでご利用いただく機能ですが、必要な場合は vCloud Air の運用チームがサポートいたします。

また、VMware vCloud® Connector™ の Stretch Deploy 機能を使用して、仮想マシン単位または vApp 単位で、レイヤー 2 の SSL-VPN トンネルを自動的に作成することもできます。

Q：データセンターはどこに配置されていますか

A：vCloud Air のデータセンターは、米国ネバダ州、バージニア州、テキサス州、カリフォルニア州、ニュージャージー州、英国、および日本にあります。サービスを契約したユーザーは、複数のデータセンターを利用できます。vCloud Air のクラウドおよびプライベートの VMware vSphere® データセンターを含む複数のデータセンターに複数のサービス インスタンスを分散する場合、vCloud Connector の Content Sync 機能を使用して、クラウド間でカスタム テンプレート ライブラリの同期を維持できます。

Q：サブスクリプション契約者は、vCloud Air 環境がホストされているデータセンターを見学できますか

A：当社のデータセンターは、専任のエキスパートによって管理されており、厳重なセキュリティ管理を行っています。お客様のセキュリティとプライバシーを守るため、データセンターの見学は認められていません。ただし、コンプライアンスの認定を監査する目的で、第三者がデータセンターを訪問することは許可されています。このような方法で、データセンター運用の安全性とコンプライアンスを維持し、お客様とお客様のデータを保護しています。

Q：VMware は、vCloud Air 環境内の可用性と冗長性をどのように確保していますか

A：vCloud Air のインフラストラクチャは、高可用性を提供するために設計されています。vSphere vMotion™、vSphere DRS、および vSphere HA を使用して、ワークロードのライブ マイグレーションが実行され、障害が発生した場合には仮想マシンが自動的に再起動されます。VMware vCloud® Network and Security™ が提供する高可用性対応のアクティブ / パッシブ エッジ ゲートウェイにより、高負荷のトラフィックにも対応するネットワークが提供されます。

Q：信頼性の高いビジネス継続性とディザスタ リカバリを実現するため、VMware はどのようなサポートを提供していますか

A：vCloud Air は、ディザスタ リカバリと Data Protection の 2 種類のビジネス継続性ソリューションを提供しています。

vCloud Air では、End-to-End の サービスとしてのディザスタ リカバリをパッケージとして提供しています。このサービスによりお客様は、vCloud Air をディザスタ リカバリ サイトとして使用して、既存の社内クラウドを保護できます。ディザスタ リカバリは、セットアップが容易で費用対効果に優れた、ウォーム スタンバイのレプリケーション ソリューションです。

vCloud Air には、Data Protection というアドオンもあります。Data Protection は、お客様が指定するワークロードを定期的にバックアップするオプションです。これらのワークロードは、いつでも容易にリストアできます。また、サービス用インフラストラクチャの基本コンポーネントに冗長性機能が組み込まれており、VMware の vMotion と高可用性機能を透過的に使用して、vCloud Air テナント環境内のすべてのワークロードにビジネス継続性を提供します。

ディザスタ リカバリ戦略として、vCloud Air をセカンダリ データセンターとして構成し、既存のツールを活用できます。

Q：サービスで保証されている連続稼動時間を教えてください

A：サービス レベル アグリーメントを次の Web ページで公開しています。
http://www.vmware.com/support/product-support/vcloud-hybrid-service/sla.html（英語）

Q：どのような暗号化方式を使用できますか

A：組み込みの vCloud Network and Security エッジ ゲートウェイ経由で確立されたサイト間 VPN トンネルで、プライベートデータセンターと vCloud Air の間のネットワーク トラフィックを暗号化します。

管理インフラストラクチャを通過するトラフィックは完全に暗号化されます。

Q：セキュリティ インシデント対応プロセスはどのようになっていますか

A：VMware のセキュリティ インシデントへの対応は、NIST 800-62 のガイドラインの理念に沿うもので、状況に応じて、vCloud Air のサーバ、ストレージ、アプリケーション、ネットワーク デバイスなど、VMware によって直接管理、または物理的なアクセスと制御が可能な管理インフラストラクチャに関連する検知、重要度 / 脅威の分類、システムやネットワークのフォレンジック、推奨、および経験則から構成されますが、これらに限定されません。

VMware が、お客様のコンテンツへの不正なアクセス、使用、または公開、あるいはその他の問題を確認した場合は、適用される法令、規則、または政府機関の要請を勘案し、商業取引上合理的な対応としてすべての関係者に通知します。

Q：サブスクリプション契約者 / ユーザーのデータには誰がアクセスできますか

A：お客様は、自身のコンテンツについて全ての責任を負うものとします。お客様は、自身が所有するコンテンツとデータにのみアクセスできます。お客様には、サービスを利用するほかのお客様のコンテンツを確認する権限はありません。このサービスは、当初からこの原則に沿って設計されています。VMware は、サービスを提供するため（関連会社、サービス プロバイダ、請負業者と協力する場合あり）、契約上の義務を果たすため、または適用される法令を順守するために必要な場合にのみこのコンテンツにアクセスし、使用します。

Q：VMware の開発者は、セキュア コーディングのトレーニングを受けていますか

A：VMware のエンジニアは、コード レビュー、侵入テスト、脅威モデル、静的分析、脆弱性検出などの分野で、業界で信頼されているコンサルティング企業が提供するセキュリティ関連のトレーニングを受けることが必須です。

Q： お客様のデータはどのように分離されていますか

A： vCloud Air には、次の 3 種類の基本サービスがあり、それぞれデータ分離の程度が異なります。

専有型クラウド

vCloud Air のほかのすべてのテナントから物理的に分離され、予約されたコンピューティング リソースを提供します。

専有型クラウドには、専用の vCloud と vSphere の管理スタックも含まれます。

仮想プライベート クラウド

マルチ テナントの仮想プライベート クラウド環境では、vSphere ハイパーバイザーと vCloud のリソース プールを利用して、ユーザー データが分離されます。仮想データセンターごとに、割り当てられるリソースの量が保証され、VMware がクラウド環境の全体的なパフォーマンスを監視して、共有リソース プールを最適化します。

Disaster Recovery

マルチ テナントのディザスタ リカバリ環境では、仮想プライベートクラウドと同様に、vSphere ハイパーバイザーと vCloud のリソース プールを利用して、ユーザー データが分離されます。仮想データセンターごとに、割り当てられるリソースの量が保証され、VMware がクラウド環境の全体的なパフォーマンスを監視して、共有リソース プールを最適化します。

すべての基本サービスが、論理的に分離されたネットワークとストレージを提供しており、vCloud のリソース プールと VLAN によってテナントが安全に分離されます。

お客様がサービス内で展開するファイル システムとデータベースは、お客様自身で完全に管理できます。

ヴイエムウェア株式会社 〒 105-0013 東京都港区浜松町 1-30-5 浜松町スクエア 13F www.vmware.com/jp

アイテム No. : VMW5167-FAQ-vCLD-AIR-BSQ-A4-104 2014/10