WHITE PAPER

クラウド環境における脅威の検知と対応

脅威の検知に関する従来のシステム環境との違い

VECTRA AI, INC.

はじめに

クラウド環境における脅威の検知と対応の方法は、これまでの従来のシステム環境とは根本的に異なるものです。

ワークロードが動的に入れ替わるクラウド環境において、システムは常に変化しています。ここでは多くのプロセスが自動化されており、システム設定におけるヒューマンエラーが大きな影響を及ぼす可能性があります。また、クラウドサービスプロバイダー（CSP）とセキュリティ上の責任を共有することは、攻撃のライフサイクルにおける潜在的な脅威の検知にギャップを生じさせます。

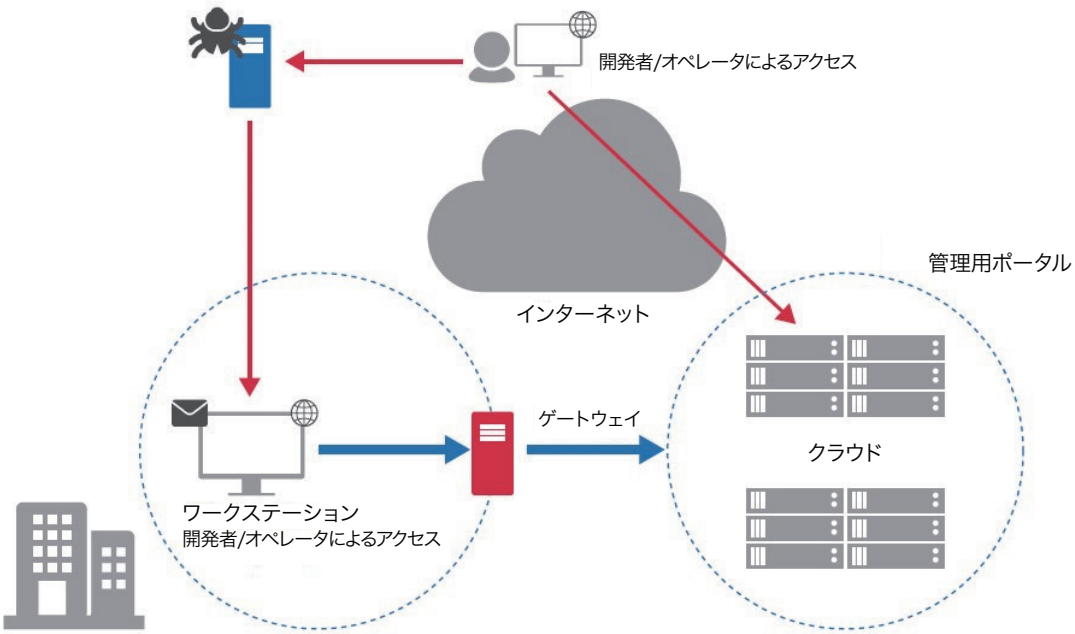
クラウド内の全ての仕組みが API によるデータアクセス方式に移行しつつある現在、トラフィックフローを監視する従来の手法は、もはや通用しなくなっています。

脅威の検知と対応では、システム環境面の課題だけでなく、クラウドの急速な進化のスピードに業務が追いついていけないという問題もあります。市場競争の激化に伴い、多くの企業は新たな機能の提供を最優先し、中核となる機能以外はアウトソースする形態のビジネスモデルに移行しています。そして、その犠牲となっているのが情報セキュリティなのです。

クラウドサービスの加速度的な広がりによって、境界防御という概念は過去のものとなり、もはや意味をなさないとさえ考えられるようになっています。新たなインフラストラクチャーや構築ツールの普及は、新たなセキュリティモデルを生み出すと同時に、これまでにはない攻撃に晒されるというリスクを生み出す要因にもなっています。さらに、次々とリリースされる新たな機能やサービスによって、セキュリティの専門家不足がいっそう深刻化しています。

特に見逃せないのは、クラウドへ展開するための複数のアクセス機能や管理機能の採用が、様々な形で大きなリスクになっているという点です。管理を担当するユーザーが企業の内部、あるいは外部からクラウドリソースへのアクセス権限を与えられている場合、これらの厳密な管理、トラッキング、監査は決して容易ではありません。

従来のシステム環境では、サーバーにアクセスする際、企業の境界防御機能に対する認証が必要であり、プライベートネットワークの内部には、管理のためにアクセスをトラッキングし監視するためのモニタリング機能が導入されていました。



クラウド環境における攻撃のライフサイクル

攻撃者側は、クラウドリソースを侵害する 2 つの攻撃手段を持っています。1 つは、企業のネットワーク境界線の内部のシステムにアクセスし、クラウドリソースへのアクセスが可能なシステム管理者（アドミニストレータ）のアカウントを偵察した上で、自らのアカウントを特権を持つものに昇格させるという従来からの手段です。

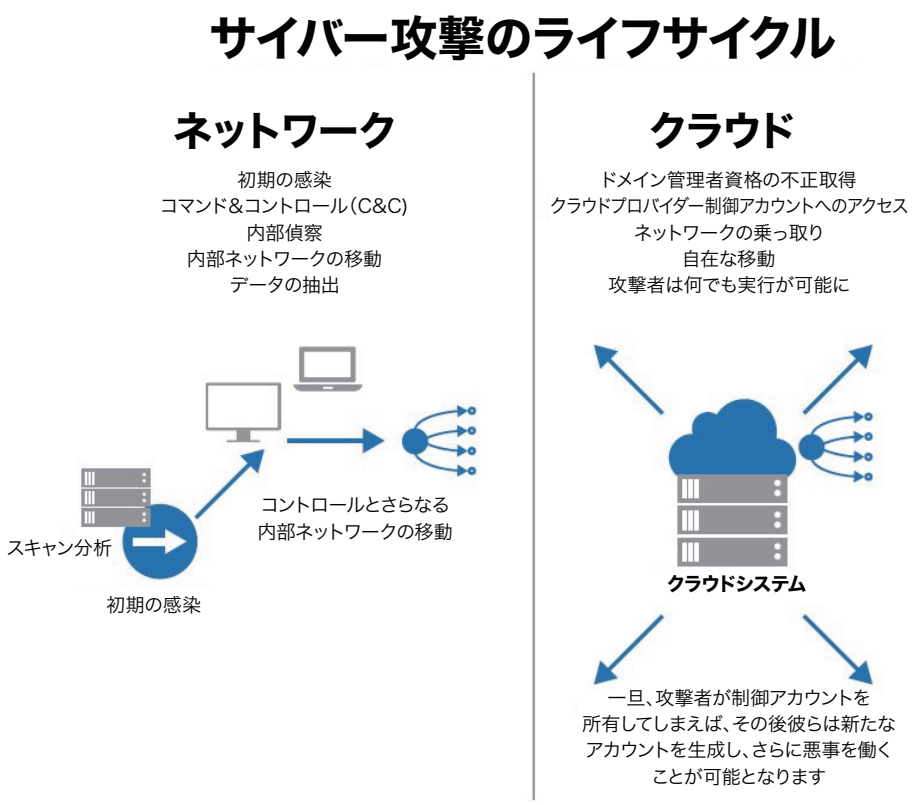
もう 1 つは、上記の攻撃のプロセスを全て省略し、リモート管理や CSP の管理アクセスが可能なシステム管理者アカウントの認証情報を不正使用するものです。

様々な管理におけるアクセスモデルが存在するということは、クラウドサービスの管理に使用するエンドポイントへの不定期なアクセスによって、セキュリティ上での新たな脅威となり得る攻撃対象が広がることを意味します。開発やインフラ操作に用いられる管理されていない各デバイスは、Web ブラウザや E メールなどのような、新たな攻撃対象を生み出しかねません。

メインのシステム管理者アカウントが侵害を受けると、攻撃者は権限の昇格や企業ネットワークへのアクセスを続ける必要がなくなります。メインのシステム管理者アカウントを使用することで、それら全て、あるいはそれ以上のことが実行できるようになるからです。それでは、企業は CSP のシステム管理者権限の不正使用を、どのようにして監視すればよいのでしょうか?

まず、企業はシステム管理やクラウドのアカウントの所有権が、どのように扱われているのかを確認する必要があります。

1. メインアカウントは、何人の担当者によって管理されているのか?
2. パスワードや認証情報は、どのように扱われているのか?
3. この重要なアカウントのセキュリティについて、誰がレビューしているのか?



セキュリティ上の問題が発生した場合、その責任は誰にあるのか? CSP か、それともテナント企業か?これらの責任の所在は、問題の性質によって判断されるべきものですが、中には全ての責任をテナント企業に転嫁しようとする CSP も存在します。

重要なのは、管理のための認証情報の存在や不正使用を、企業がどうやって監視すればよいのかという点です。クラウドのテナント企業が、CSP のバックエンドにある管理インフラストラクチャーを確認できない場合には、CSP アクセス権の不正使用が侵入を目的としたものかどうかを、自社の環境内で見極める必要があります。

クラウド環境で上位を占めるセキュリティ上の脅威

クラウドセキュリティアライアンス (CSA) では、2017 年に行った調査において、クラウドコンピューティングにおける、現在最も差し迫ったセキュリティ課題は何かという点について、専門家からの意見を集約しました。

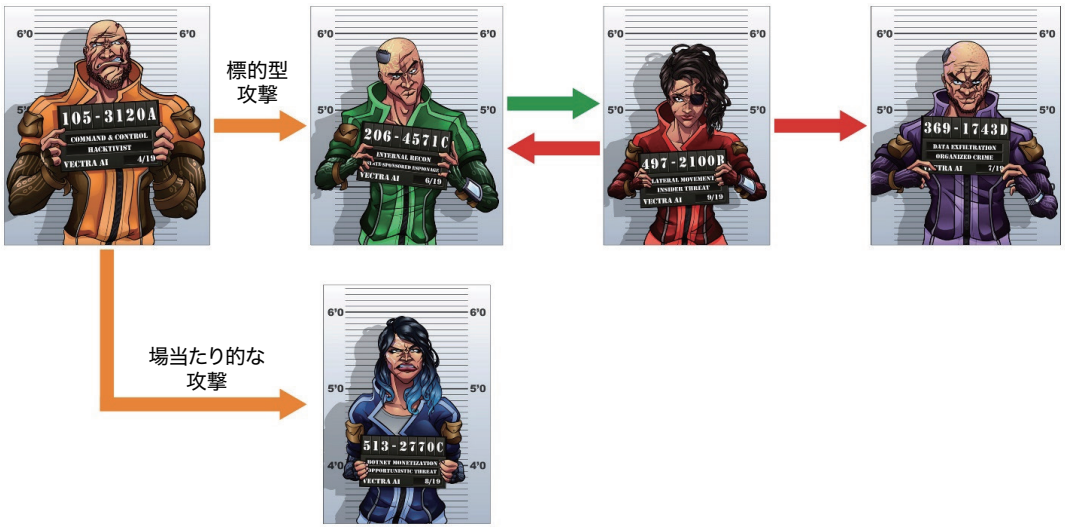
12 の懸念事項の中の 5 つは、認証情報の管理と不正を目的にクラウド環境へのアクセス権を得るための、認証情報の侵害に関するものでした。この 5 つの懸念事項に関しては、重要度順に、以下のようになっています。

1. 不十分な ID 情報や認証情報、そしてアクセスの管理 ー 拡張性に優れた ID 管理システムの欠如、多要素認証に対応できない脆弱なパスワード、そして自動ローテーションができない暗号化キー、パスワード、認証情報。
2. 安全性に欠けたインターフェースと API ー インターフェースは、認証やアクセスコントロール、さらに暗号化やアクティビティ監視に至るまで、偶発的な事象だけでなく、ポリシーを回避するような悪質な試みからも保護できるように設計されている必要があります。
3. アカウントの乗っ取り ー 攻撃者は、ユーザーのアクティビティやトランザクションを盗聴し、データを操作して虚偽の情報を返し、クライアントを違法なサイトへとリダイレクトします。
4. 不正なインサイダー ー 企業のネットワークやシステム、さらにデータへのアクセス権限を持つ（あるいは持っていた）、現在や過去の社員、契約社員、ビジネスパートナーなどによる意図的、または誤って行われた権限を越えたアクセス行為が、企業の情報や情報システムの機密性や整合性、さらに可用性に悪影響を与える可能性があります。
5. 不十分な適正評価 ー 適正な評価の仕組みが整備されていない状況下では、営業や財務、技術、法務などの領域において発生する、企業の成長を妨げる様々なリスクを払拭することができません。

実際のクラウド攻撃に関する分析

APT10 グループは、長期間にわたってグローバルで展開された「Operation Cloud Hopper（クラウドホッパー作戦）」を実行したことで広く知られています。これらの攻撃の目的は、機密性の高い知的データや顧客データにアクセスすることでした。

US-CERT では、Operation Cloud Hopper の特徴は、攻撃者が CSP のアクセス権を取得し、クラウドのインフラストラクチャーを踏み台にして、クラウドのテナントを次々とホッピングしながら、機密データにアクセスすることだと指摘しています。この標的は、少なくとも世界数十ヶ国の政府機関をはじめ、ヘルスケアや製造、金融、バイオテクノロジーといった企業にまで及んでいます。



Cloud Hopper 攻撃のライフサイクル

Operation Cloud Hopper の攻撃者は、まずフィッシングメールを使って、CSP の管理権限を持つアカウントを不正に取得します。これは、ごく一般的に見られる侵害の手法であり、現在でもネットワークに最初にアクセスするための最も容易な手段となっています。攻撃者は、マルウェアを使って必要な認証情報を収集し、CSP やクライアント管理インフラストラクチャーに侵入します。

管理インフラストラクチャーのアクセス権を手に入れると、クライアントが管理するインフラストラクチャーで PowerShell を使って、コマンドラインスクリプトを実行します。このスクリプトは、偵察を行いながら横方向に侵入を拡大し、他のシステムのアクセス権を得るための情報収集を行います。

攻撃者は、不正に入手した認証情報を使って、クラウドサービスプロバイダーを踏み台にしながら、セキュリティの境界線を超えて、様々な企業のデータにアクセスします。

管理アカウントが無効になった後でも、クラウドインフラストラクチャーへのコネクティビティを維持できるよう、攻撃者はリモートアクセス型トロイの木馬をインストールして、正規のドメインの偽装サイトに対してコマンドアンドコントロールを実行します。

これらは、Poison Ivy や PlugX など、多くの攻撃に使用されているオープンソースのオフザシェルフ型マルウェアです。リモートアクセスによって侵害を受けるシステムは、その多くがミッションクリティカルではないシステムとなっており、継続的な横方向の感染によって、攻撃者はシステム管理者の検知を避けることができます。

知的財産に関わるデータを外部に転送することが、Operation Cloud Hopper の最後のステップになります。データを収集して圧縮し、CSP インフラストラクチャーから攻撃者がコントロールするインフラストラクチャーに向け送信します。

CSP 側が、テナントからマネージド・インフラストラクチャーに対する管理責任を移譲されると、クラウド内のテナントがコントロールおよび可視化できる範囲は狭まっていきます。APT10 は、この可視性の低下を利用して、CSP と企業インフラストラクチャーの双方にアクセス可能な認証情報とシステムを悪用します。

クラウドのテナントは、CSP のインフラストラクチャー自体を可視化したり、コントロールすることができません。このため、特定のシステムにアクセスした攻撃者を監視して検出した後、CSP インフラストラクチャー内を素早く移動して、別のシステムにアクセスすることは非常に困難です。

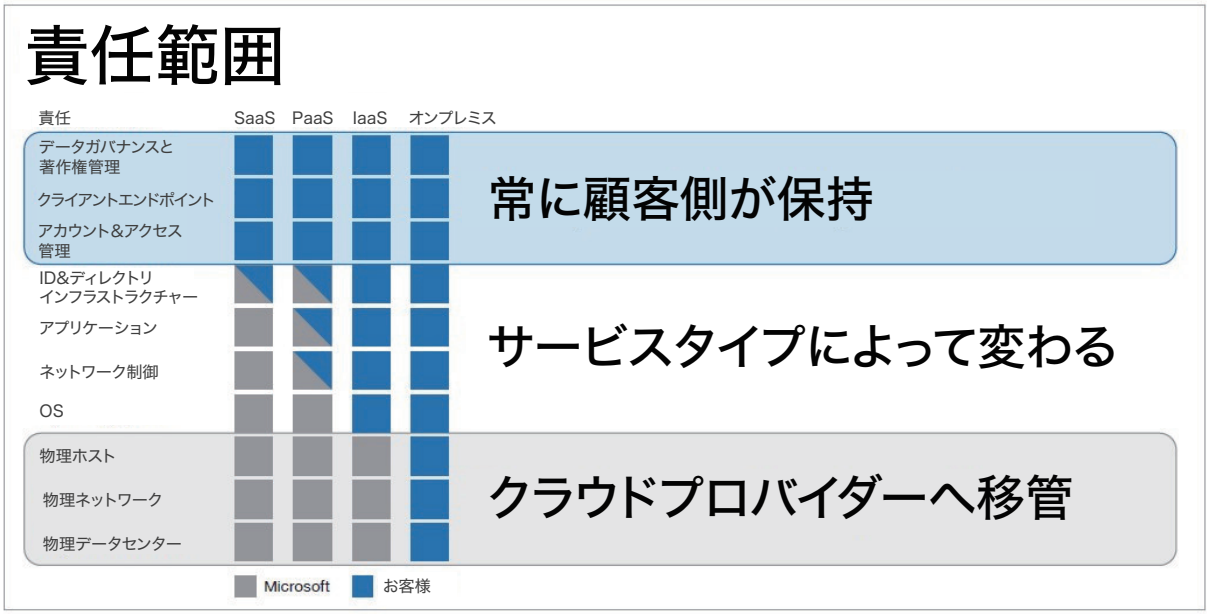
CSP やオンプレミスシステムで構成されるハイブリッド環境の複雑さに対しては、注意が必要です。認証情報の盗難や、クラウドのテナントから CSP へ、さらに次のクラウドのテナントへと横方向に拡散する攻撃者といった問題への適切な対処は、決して容易ではありません。クラウド内のたった 1 つの不注意なテナントの行為が、他の適正な運用を行っているテナントのリスクを高める結果につながる可能性があります。

責任共有モデル

クラウド環境における脅威の検知と対応は、責任共有モデルの基本的な理解と、それがセキュリティの管理や監視機能に与える影響を理解するところから始まります。

クラウドサービスのセキュリティは、クラウドのテナントと CSP の間のパートナーシップと、責任共有によって確保されます。CSP は、クラウドプラットフォームと自身のデータセンターの物理的セキュリティに対して責任を負っています。

テナントは、クラウドのデータや ID を保有し、その保護やオンプレミスにあるリソースのセキュリティ、さらに自身がコントロールしているクラウド上のコンポーネントのセキュリティに対して責任を負っています。CSP は、セキュリティのコントロールや、データとアプリケーションの保護を支援するための機能を提供し、セキュリティに対するテナントの責任の度合いは、クラウドサービスのタイプに依存します。



Microsoft の責任共有モデル

CSP とクラウドのテナント間のコントロールのバランスは、使用するコンピューティングモデルに依存します。ここに示した Microsoft for Azure のモデルは、クラウドプラットフォームに応じた責任共有のレベルを表しています。

オンプレミスへの導入には、企業が保有する、仮想インフラストラクチャーを利用するデータセンターも含まれます。このモデルの場合、企業は物理デバイスからデータまで、セキュリティスタック全体に責任を負うことになります。

IaaS（Infrastructure-as-a-Service）としての仮想データセンターモデルは、企業内の既存のデータセンターを複製したものです。この例では、ハードウェアの物理的な分離は不可能で、セキュリティゾーンを構築しリモートアクセスを可能にする、ハイパーバイザーレベルの機能が必要となります。

プライベートクラウドとパブリッククラウドのどちらでインフラストラクチャーを管理するかを選択する場合、ほとんどの企業は、プライベートクラウドとパブリッククラウドに共有リソースと配布コンポーネントを組み合わせた、ハイブリッドクラウドを選択します。重要なバックエンドインフラストラクチャーはプライベートに、アクセスや配布コンポーネントはパブリックに置く形態が一般的です。

仮想データセンターやクラウド環境では、セキュリティとコンプライアンスが最優先課題となります。仮想データセンターとクラウドのセキュリティ要件としては、仮想環境の監視を行いながら、VM ホストのキャパシティとパフォーマンスを最高レベルに維持する機能を挙げることができます。これらの技術には、ハイパーバイザーベースのステートフルなファイアウォール、ネットワークの検知と仮想化固有のエンドポイントの保護などがあります。

PaaS モデルの場合、アプリケーションは既存のアウトソースプラットフォームにインストールされて管理されます。サーバーへのアクセスの排他性を強化することも、複数のアプリケーションで共有することも可能です。

既存のハードウェアに対するコントロールは一切できないため、機密情報が他のユーザーやサービスプロバイダーに晒される可能性があります。データのコントロールは、仮想環境向けに設計された暗号化や外部キー管理機能を使って、アプリケーションやデータベースの内部で行われる必要があります。

SaaS の場合には、Salesforce のようなサードパーティのアプリケーションを使って、特定のサービスを提供します。データはアプリケーションプロバイダーが提供するアクセスコントロールを使って、バックエンドに保存されます。

エンタープライズアプリケーションは、通信に ADFS や SAML を使って、Active Directory との連携をサポートするようになりました。認証やアクセス管理のコントロールだけでなく、アプリケーションの使われ方に対しても、企業側がコントロールできているかどうかを監視する必要があります。

重要なポイント

APT10 の Operation Cloud Hopper 攻撃の場合、最初の侵入方法はクラウド特有のものですが、クラウドの内部に入ってからの攻撃は、プライベートクラウドや物理データセンターに対するものと同様の手法になります。

これは、特にその目的がデータを流出させることである場合、攻撃を成功させるためには、特定の攻撃ライフサイクルに従う必要があるからです。不正行為を防ぐことは、ますます困難になってきていますが、コマンドアンドコントロールからデータの流出までの間に発生した事象は検知が可能です。忘れてはならないのは、攻撃は数日ではなく数時間のうちに行われるため、検知に要する時間が非常に大きな意味を持つということです。

責任共有モデルで重要なことは、インフラストラクチャー、プラットフォームあるいは SaaS など、そのデータセンターモデルの導入方法に関わらず、企業は常にデータやエンドポイント、アカウント、アクセス管理に対する責任を負っているということです。

アクセス管理

CSP は、クラウドのテナント環境へのアクセスを制限するアクセス管理やコントロールを確実に行うと同時に、テナント自身が不正行為を受ける可能性があるという前提に立って、誰が、何を、いつ、どこでアクセス管理しているかという点を理解しておく必要があります。共有認証情報のインスタンスを減らして、ユーザーのアクセス権限を適切に割り当てることで、テナントはこのような認証情報の使われ方について焦点をあてることができます。また、リソースに対するアクセスポリシーによって、CSP インフラストラクチャーとクラウドテナント間での移動の機会を減らすこともできます。

検知と対応

クラウドとオンプレミスの両方を監視すると同時に、セキュリティ分析に適した実践的な情報に変換するために、どのように双方のデータとコンテキストの関連付けを行うかを決定する必要があります。クラウドのテナント別に導入したリソースを監視し、CSP のインフラストラクチャーからテナントの環境間の横移動を検知する能力を向上させます。クラウドのテナントと CSP 間の連携に限らず、CSP と連携することで、情報の密接な統合を図り、侵入後の不正な活動に対する検知能力を高めることができます。さらに重要なのは、クラウド固有のデータを活用できる適切なツールを導入することで、攻撃者の行動を可視化できるという点です。

セキュリティ運用

適正評価の一環としてインフラストラクチャーを深く理解し、正しく管理することで、Operation Cloud Hopper などに使用されているマルウェアに侵害されたシステムやオペレーションを特定することができます。プロダクションシステムへの変更は、検知が困難かもしれません。しかし、クラウドインフラストラクチャーを可視化することによって、侵害を受けたシステムやサービスでの、明らかに想定範囲を超えた攻撃者の行動の検知がいっそう容易になります。理想的には、セキュリティの運用チームが、インフラストラクチャーの標準的な状況に関する確かな情報を持ち、通常のアクティビティとは異なるマルウェアやそのアクティビティの検出能力を高めることが重要となります。

VECTRA AI, INC.

お問合せ:

製品、ソリューションなどに関するお問い合わせは、info-japan@vectra.ai までお願いします。