WHITE PAPER • 2017 年 5 月

ハイブリッド・アーキテクチャのためのハイブリッド特権IDアクセス管理:クラウド変革のリスクに対する戦略的アプローチ

目次

概要 3

セクション 1 4

新しいアーキテクチャに必要な新しいリスク・マネジメント：
ハイブリッド・アーキテクチャの一貫性、可視化、自動化

セクション 2 5

ハイブリッド・クラウド特権ユーザ管理の課題：
パスワード管理より強力な管理

セクション 3 6

特権管理の新しいアプローチ：
既存の知識からの進化

セクション 4 7

AWS 特権アイデンティティのガバナンス：
権限認証とポリシー適用の自動化対アクセス制御

セクション 5 9

まとめ

概要

課題

リスクの理解、管理、封じ込めは今日、多くの組織のハイブリッド・アーキテクチャ戦略の重要な要素になっています。コスト効果とアジリティ向上のために、クラウド・サービスの戦術的な利用を検討している企業にとって、特権アイデンティティによるアクセスの増加は大きなリスクになります。静的インフラストラクチャのために開発された既存のアプローチでは、初歩的なリスクの懸念は解消できても、動的な分散インフラストラクチャに対してポリシーを一貫して適用し、継続的に可視化するには不十分です。

ビジネス・チャンス

企業が効果的に自動化を進め、変革を成熟させるには、さまざまな要素を考慮する必要があります。特にセキュリティ・ツールは、成熟度モデルの各段階で重要なアクセス・リスクを管理する体系的かつ計画的なアプローチを採用する場合は重要です。適切な特権アクセス・プラットフォームとツール・セットを使用することで、アクセス管理を自動化および拡張して、リスク回避とビジネスニーズのバランスを取ることができます。

メリット

ハイブリッド・クラウド・アーキテクチャとその固有のアクセスを管理するために設計された特権 ID アクセス管理は、環境間を結ぶブリッジとしての役割だけでなく、特権を使用したすべてのアクションに詳細な権限認証ポリシーを適用する動的なポイントとしての役割も担います。また、それによって柔軟性が確保され、ベンダー・ロックインが制限され、特権クレデンシャルを狙った攻撃のプロアクティブな検出が可能になります。クラウドの変革に適したリスク・マネジメントを行うには、機密性の高いすべての要素にアクセスするプロセスを管理する必要があります。

セクション 1

新しいアーキテクチャに必要な新しいリスク・マネジメント：ハイブリッド・アーキテクチャの一貫性、可視化、自動化

ハイブリッド・アーキテクチャとクラウドベース・サービスの特権アクセスを管理するアプローチの多くは、既存のパスワード・ボールト機能をクレデンシャルの新しいカテゴリに拡張したものです。これには、Amazon Web Services（AWS）Admin Console のキー、パブリック・クラウドにアプリケーションをデプロイする開発者の SSH キー、クレデンシャルを組み込んだ AWS EC2 インスタンスの自動プロビジョニングのスクリプトも含まれます。確かに、これらのアプローチでは、特権アクセス制御への既存の投資を活用して新しいユースケースのベースラインのセキュリティと遵守性に対応できます。

しかし、問題は、ハイブリッド・アーキテクチャとクラウドベース・サービスへの影響が大きくなることにあります。このようなユースケースは、IT のデリバリと機能の変革の先駆けとなります。もちろん、ハイブリッド・クラウド・アーキテクチャでは、自社で管理する外部のインフラストラクチャと自社で管理する自社のインフラストラクチャのブリッジが必要になります。多くの遵守性の要件と共通していますが、リスク・マネジメントの最も重要な要件は、すべての環境の特権アイデンティティに対するアクセス・ポリシーと権限認証ポリシーの一貫性を確保し、管理するすべての環境の状態の可視性を統合することです。

操作を実行するために特権クレデンシャルにアクセスすることは、このような要件に対応する出発点にはなりますが、総合的ソリューションにはなりません。採用が成熟すればより複雑になり、自動化も拡大する必要があります。また、複数のクラウドのデプロイや長期的なベンダー・ロックインは多くの企業の懸念となっているため、すべての環境に拡張でき、特権アクセスのセキュリティに対する脅威を効果的に検出できるモデルが必要です。それによって、不十分な監視やプロビジョニング・スクリプトからクレデンシャルを抽出するマルウェアに起因する特権アクセスの侵害も防止できます。

変革の持続可能なリスク回避には、もう 1 つ問題があります。それは、特権アクセス・セキュリティは分離して解決できないことです。

既存のアプローチに依存しない目的への適合

企業がクラウド・アーキテクチャを採用する一般的な理由は、規模の経済による運用コスト削減、アジリティの推進、アプリケーションやサービスのデリバリの加速です。これらのビジネスニーズによって、技術的には特権アイデンティティが多様化（開発者、API、コンテナ・フォームのコード、IoT ゲートウェイなど）し、ソフトウェア・デリバリ・プロセス（一般的には DevOps）の利点を最大化するために自動化が必要になります。

また、アクセス権の効果的なリスク・マネジメントのためは、クラウド・リソースへのアクセスとアクションに対する権限認証が自動化されたワークフローとプロセスにどのように統合するかも問題になります。最小限の特権アクセスと役割ベースのアクセスの考え方を十分に理解して適用することは、ガバナンスの基盤となりますが、それにはポリシー適用自体が動的な分散インフラストラクチャに容易に統合され、インスタンス化されることが前提となります。

クラウド・サービスの検出機能を統合すると、管理が必要なアカウントとクレデンシャルを判断するのに役立ちます。ただし、基本的な課題は、新しいクレデンシャルに対応するだけでなく、特権アクセスを自動化して以下を可能にすることです。

- 特権クレデンシャルを使用したアクションと ID の関連付け
- 役割ベースのアクセス・ポリシーに対する個別のアクションのリアルタイム評価
- 分析を介した監視、レポーティング、プロアクティブな検出のための複数のクラウド環境のすべての活動の統合

クラウドのエンドポイントではなく、唯一の適用ポイントでクレデンシャルへのアクセスが制限される場合、リスク・マネジメントはフロント・ドア程度にしか拡張されず、インフラストラクチャが動的でクラウド・エンドポイントが一時的であっても特権アイデンティティのアクションや変更までには拡張されません。フロント・ドアのみに焦点を当てて、クラウド・エンドポイント（AWS EC2 インスタンスなど）のアクションを軽視すると、過剰な特権を持つユーザ・クラスの監視が最小限になるという本来の目的と真逆の結果になります。物理サーバの共有アカウント管理のアプローチではベースラインの要件には対応できても、クラウド変革の成熟度モデルを実現する基盤にはなりません。

セクション 2

ハイブリッド・クラウド特権ユーザ管理の課題：パスワード管理より強力な管理

アイデンティティ / アクセス管理では、ユーザにアクセスを許可すればリスクが発生するのは当然です。ハイブリッド・アーキテクチャとクラウドベースのサービスの場合、管理者や特権エンティティにリソース・プロビジョニング機能を提供すると、リスクはさらに深刻になります。高位特権のハイパーバイザやクラウド・サービスの管理コンソール・アカウントを 1 つ攻撃されれば、個々のサーバ・インスタンスだけでなく、クラウドのデータセンタ全体に影響が及ぶ可能性があります。

チェックポイントが多数あり、リソースを手作業でプロビジョニングする物理的なデータセンタとは異なり、クラウドでは、管理者がリソースとサービスのプロビジョニング、稼働およびプロビジョニング解除を行う範囲ははるかに広くなります。たとえば、Amazon Web Services はその文書の中で、セキュリティ・グループのアクセス・ポリシーによって特に制約および管理しない限り、セキュリティ認証によって「AWS のリソースの無制限の使用が許可される」と指摘しています。また、企業に AWS マネジメント・コンソールに対するクレデンシャルを許可されたユーザは、その企業の AWS リソースに「許可の適用範囲で」アクセスすることができます。

ただし、最小限の特権アクセスの考え方の点で適切なアクセス権限認証ポリシー・ロジックを用意し、規制遵守や職務の分離などの内部の要件に一致させる責任は顧客が負います。自動登録によってアプリケーション開発者やサービスに広く使用されている SSH キーなど、既存の特権アカウントとクレデンシャルの検出を統合すると、ガバナンスと監視のフレームワークの対象外のアカウントによるリスク、あるいは特権クレデンシャルに対するリスクを回避できます。

本人認証より効果的なアクセス制御

クラウドとアプリケーションの特権クレデンシャルをパスワード・ボールトに登録すると、共有パスワードにアクセスするユーザの管理だけでなく、特権アカウントの管理も簡略化されます。しかし、問題は、特権クレデンシャルの使用方法や特権クレデンシャルがアクセスを許可するリソースのレベル、クラウドのエンドポイントの活動をポリシーによって制御および管理する方法です。特に、コンテナを採用すると、クラウド・インスタンスの平均寿命は数週間から数日に短縮されます。2017 年 4 月現在の調査によると、「従来のクラウドベースの VM の平均寿命は 23 日なのに対し、Docker を採用している企業のコンテナの平均寿命は 2.5 日です」。[1]

役割ベースのアクセス・ポリシーを使用して、1 つの特権アイデンティティでアクセスできるクレデンシャルのクラスを制限することから始めるのは悪くありませんが、以下の課題に体系的に取り組まないと多くのリスクが残ります。

- クレデンシャルにアクセス可能なユーザやサービスにどのような操作を許可するか（個々の操作を指定）。
- 各特権クレデンシャルにはどのような役割が適切であるか（およびそのクレデンシャルにアクセス可能なユーザ）。
- 権限のある役割ベースのアクセス・ポリシーは何をソースにするか。

- 上記のポリシーを複数の環境全体で更新および調整するか（特に複数クラウドのデプロイ）。
- プラットフォームのオペレータに特権アクセスをいつ許可するか。どのレベルの権限認証が適切であるか。
- 開発者のアクセスはどのように管理するか。権限認証に SSH キーを使用する既存の開発プロセスは、どのように特権 ID アクセス管理のガバナンスに統合するか。

オンプレミス、仮想化、複数のクラウド・サービスの環境で構成されるハイブリッド・アーキテクチャのすべての要素に一貫したポリシーを適用し、ポリシー・ロジックが孤立しないようにすることは企業にとって大きな課題です。多くの企業ではすでに過剰な特権という現象が起こっており、正当な運用上の理由から、管理者が制御を緩めたり、役割を広範に定義したりしています。そのため、不適切なアクセス・ポリシーによってリスクが増大するという懸念だけでなく、セキュリティの認知プログラムやプロアクティブな検出のための分析を通して、意味のある詳細なデータを生成するのが困難になる懸念もあります。

セクション 3

特権管理の新しいアプローチ：既存の知識からの進化

特権クレデンシャルに対する本人認証を義務付けることは、ハイブリッド・アーキテクチャのリスク回避には必要不可欠です。特権クレデンシャルを提供する前に本人認証を要求してエンティティを確認することは、遵守性の義務の観点からも、ログ記録、監査、レポーティングの観点からも重要です。AWS Admin Console にアクセスする管理者であっても、CI/CD 環境での処理のために SSH キーを使用したり、スクリプト実行のためにクレデンシャルを使用して API にアクセスする開発者であっても、その重要性は変わりません。権限のストアに対して本人認証の有効性を確認することは、そのエンティティがクレデンシャルへのアクセスを許可されているか判断する第一歩です。ただし、リスクを封じ込めて、クラウド革新のプロセスにアクセス・セキュリティを効果的に統合するには、本人認証だけでは不十分です。

ベースラインの本人認証から効果的に進化させるには、クラウド環境への整合、高度な自動化、職務の分離ポリシーの一貫した適用のほかにもいくつかの要素を追加する必要があります。

アーキテクチャは、特権 ID アクセス管理の簡略化と動的な環境での運用に加え、API 経由で使用するサービスベースの環境にポリシーを適用できるよう設計されている必要があります。また、ポリシーは信頼できるソースによって役割ベースのアクセスが定義され、ネイティブのプラットフォーム・ツールによって最小限の特権アクセスの考え方が簡単に抽象化される必要があります。

前述のアーキテクチャを用意したら、適用は自動検出によって行い、環境と運用の基本要素（AWS のアイデンティティ管理ルールや EC2 インスタンスなど）に合わせてポリシーを変換します。信頼できるデータ・ソースを確保してから環境に適したポリシーを適用することで、過剰な特権を制限し、複数クラウドの環境でポリシー・ロジックの一貫性を維持できます。また、このアプローチでは、特定のアイデンティティ（ユーザまたはサービス）の活動の可視性を統合して、すべての環境を連携できます。

クラウドの変革にリスク・マネジメントを整合させるプロセスは、ハイパーバイザや API を通して実行する実際のタスクの管理によって異なります。つまり、特権アクセスのクレデンシャルにアクセスするユーザだけでなく、特権クレデンシャルへのアクセスによっても異なります。

ハイブリッド・アーキテクチャの特権 ID アクセス管理の確認事項

- 動的な分散環境への対応、依存関係の排除、優れた対障害弾力性、AMI または仮想イメージとしての実行、効果的な拡張を可能にします。
- API を活用して仮想とクラウドのリソースを自動検出し、適切なクレデンシャルとアクセス管理ポリシーをプロビジョニング（またはプロビジョニング解除）します。
- API 呼び出しをインターセプトして詳細な権限認証ポリシーを適用するポイント、およびターゲット環境に統合する手段として API を活用します。
- 特権アイデンティティのライフサイクル管理、ポリシーのテスト、分析を組み込んで、最小限の特権アクセスと職務の分離の評価を行います。
- スピードが求められる一時的なインフラストラクチャでも、ログ記録、レコーディング、監視の統合によってプロアクティブな検出をサポートします。
- 企業のクレデンシャルに基づいた SSO との連携によりガバナンスを一元化し、すべての特権 ID のログとイベント・データを統合した単一のソースを確保します。

セクション 4

AWS 特権アイデンティティのガバナンス：権限認証とポリシー適用の自動化対アクセス制御

ハイブリッド・アーキテクチャのセキュリティとクラウド・サービス・コンソールへの管理者アクセスの保護を混同して、静的インフラストラクチャ向けに開発された手法を使用するアプローチもありますが、そのようなアプローチとは対照的に、CA Technologies では、サービスやリソースへの特権アクセスの管理と監視に対し、より効果的で持続可能なアプローチを導入できます。 そのアプローチでは、AWS に一元化されたアクセス制御ポイントが提供されるだけでなく、動的な分散環境における特権クレデンシャルに関係するすべてのインタラクション、アクション、タスクに対して監査済みの詳細な権限認証ポリシーを適用できます。

CA Privileged Access Manager（CA PAM）では、Amazon Web Services や仮想化データセンタなどを使用したハイブリッド・クラウド・アーキテクチャに重要なセキュリティとガバナンスのブリッジが提供されます。また、CA 製品のアーキテクチャでは、クラウド・サービス環境における自動化と柔軟性が向上し、クラウド・データセンタ全体でプロキシをインスタンス化して拡張できます。

最初の重要な要件である許可された特権アイデンティティのみに AWS Admin Consol、タスク、リソース、API へのアクセスが許可され、すべてのアクセスと活動が企業固有のアイデンティティ（管理者、プラットフォーム・オペレータ、開発者、サービスなど）までさかのぼって追跡できます。さらに、広範な特権アクセス管理と AWS 運用の自動化を効果的に行うため、CA PAM ではアクセス・ポリシーと権限認証ポリシーの定義を一元化してローカルに適用する機能が提供されます。アクセス・ポリシーと権限認証ポリシーのローカル（またはコンテキスト別）の適用には大きく分けて 2 つの側面があります。

ポリシーの自動化と伝播

CA PAM では依存関係のない動的で一時的な環境でもシームレスに運用でき、EC2 インスタンスやプロビジョニング・イベントなどのリソースを検出して自動的にポリシーに結び付けることができます。また、アカウントが検出後に登録される 2 段階のプロセスではなく、継続的な権限認証ポリシーの適用モデルが提供されます。

信頼できるポリシー・ソースが使用され、クラウド IAM サブシステムは一元化されたポリシーに依存します。このアプローチによって一貫性が確保され、過剰な特権が制限されるだけでなく、ハイブリッド環境全体でプロセスを実行する場合にポリシー拡張がサポートされ、ベンダー・ロックインも抑制されます。AWS を戦略的な実行環境と考える企業でも、ベンダー・ロックインは重要な懸念です。

詳細なリアルタイムの適用

フロント・ドアからアクセスするユーザの管理に加え、CA PAM ではより層の深い権限認証を適用でき、クラウドのエンドポイント（この場合は EC2 インスタンス）まで拡張できます。また、クラウド管理コンソールでも AWS の管理 API でも、呼び出しをインターセプトして対ポリシーで評価し、リアルタイムでアクションを制限できます。AWS クラウド内の可用性の高い分散リソースとして稼働する AWS API Proxy では、セッション用に動的に生成されたブローカーとして機能し、ターゲット・リソースのすべての利用を管理して、制御と可視化の一貫性が確保されます。

現在のニーズ対応と将来のリスク回避

AWS Admin Console の強力なアクセス、動的なインフラストラクチャやクラウド・エンドポイントを考慮すると、役割と最小限の特権アクセスに基づいた権限認証の判断をリアルタイムで評価することは、リスク・マネジメントと運用成熟度の整合の重要な要素になります。また、企業はベンダー・ロックインを懸念し、プラットフォーム固有のルールやグループからある程度の抽象化を必要とするため、一元化したポリシー・ロジックの再利用とターゲット環境の構造との統合を自動化する必要があります。

CA PAM ではプロキシベースのアーキテクチャが提供されるほか、AWS API の呼び出しと応答を評価し、事前定義された監査済みのポリシーに基づいて管理者、開発者、オペレータ、特権アプリケーションのアクションやコマンド・レベルまで制限できるため、他のテクノロジより一歩進んだ管理が可能になります。これらの制御は CA AWS API プロキシによって、プログラムで呼び出される操作やタスクにまで拡張できます。

そのほかにも、CA のデータ主導の脅威検出アプローチには、分散インフラストラクチャの活動に関するログ収集の一元化、高品質のデータ生成などの利点があります。

セクション 5

まとめ

クラウドベースのサービスをより戦略的に採用し、ハイブリッド・アーキテクチャの成熟度に重点を置けば、新しい環境で特権 ID アクセス管理の既存の課題が繰り返されることはありません。変革と自動化を推進し、攻撃のターゲットになるのを回避するだけでなく、リスク・マネジメントを新しいプロセスや動的なインフラストラクチャに統合するためには、特権アイデンティティとクレデンシャルの管理とセキュリティを考え直す必要があります。

これらの新しい環境では、統合と境界定義の両方で API を活用し、動的な特権 ID アクセス管理を行い、グローバルなアクセス・ポリシーと権限認証ポリシーを適用する必要があります。ただし、機密リソースへの役割ベースのアクセス、プロセス後半への詳細な権限認証ポリシー適用、遵守性の可視化、危険や侵害のプロアクティブな検出が最も重要な要件であることに変わりはありません。

詳細については、**ca.com/jp/pam** をご覧ください。

CA Technologies にアクセスしてください

CA Technologies（NASDAQ：CA）は、企業の変革を推進するソフトウェアを開発し、アプリケーション・エコノミーにおいて企業がビジネス・チャンスを獲得できるよう支援しています。ソフトウェアはあらゆる業界であらゆるビジネスの中核を担っています。計画から開発、管理、セキュリティまで、CA は世界中の企業と協力し、モバイル、プライベート・クラウドやパブリック・クラウド、分散環境、メインフレーム環境にわたって、人々の生活やビジネス、コミュニケーションの方法に変化をもたらしています。詳細については **ca.com/jp** をご覧ください。

1「8 Surprising Facts About Real Docker Adoption,」Datadog（2017 年 4 月）

CS200-270961_0517