CYBERARK®
The Identity Security Company™

デジタルトランスフォーメーションを推進するための特権アクセスの保護

Barak Feldman,
CyberArk、特権アクセス管理およびアイデンティティセキュリティ、シニアバイスプレジデント

米国を代表する産業拠点にある多くの企業が、特権アクセス管理の過去、現在、そして未来についてさまざまな取り組みに関する情報を提供しています。本書では、シカゴで開催されたCyberArkのグローバルアイデンティティセキュリティサミットにおいて、30名以上のセキュリティリーダーとの会話から得られた知見を共有します。

このサミットには、クラウドネイティブなハイテク企業のCISOであり、シカゴの経済的な未来に対して重要な役割を担っている方や、100年以上の歴史を持つ地元企業で、人間とマシンによる製品製造の仕組みを再構築するプロジェクトに貢献している方も参加していました。これらのリーダーの方々に共通する課題は、イノベーションを迅速に進める過程で、リスクの高いアクセスを保護するための対策がかつてないほど複雑になっていることでした。

特権アクセス管理（PAM）は、リスクの高いITユーザーとアカウントを集中的に保護しなければならないという切迫した状況から生まれました。PAMは、資格情報の保管やローテーションといった基本的な管理から始まり、アカウント検出や最小権限の原則といった機能へと拡大しています。これらの基本的なセキュリティ対策は依然として重要です。100年の歴史がある銀行がクラウドに移行する場合でも、創業して間もない新興のフィンテック企業がクラウドに移行する場合でも、以下の共通する課題を抱えています。

- 特権ユーザー、アカウント、資格情報が存在する。
- 攻撃者はこれらのアイデンティティを侵害し、ラテラルムーブメントを行い、特権の昇格している。
- そのために厳格な保護機能が求められている。

今日のPAMプログラムは、広大で動的な脅威に直面しています。

新たなテクノロジーが登場し、管理者、ベンダー、クラウドエンジニアや開発者など、強力なアクセス権限を誰にでも委譲できます。一般のビジネスユーザーでさえ、それぞれのドメインで管理者レベルのタスクを実行する場合があります。製造業企業の運用テクノロジーで利用されている自動アカウントなど、人以外のアイデンティティにも同じように特権が付与されています。

また、特権はIT環境とともに移動します。企業のオンプレミス環境にあったITの特権がクラウドに移動するケースも増加しています。ITリーダーの10人に8人以上が、自社がハイブリッドクラウド環境を採用していると述べています1。

このような時代において、PAMには特権と同様に一貫性があり動的であることが求められています。企業や組織は、確実に常に利用できるPAMを必要としています。同時に、PAMプログラムは時代とともに進化しなければなりません。このホワイトペーパーでは、このようなバランスが求められるクラウド環境と運用テクノロジーの2つの事例について説明します。

[1] Cisco, "2022 Global Hybrid Cloud Trends Report," May 2022

クラウドにおける特権アクセスの保護

クラウドにおける特権アクセスについてセキュリティリーダーと対話をするとき、その議題の中心はテクノロジーの役割ではなく、人の役割に帰結することが多くあります。クラウド環境ではすべてが仮想化されており、目まぐるしく変化しています。しかし、舞台裏に目を向けると、次のような状況も見えています

- アーキテクトは、リフト＆シフト型のマイグレーションを完了させなければならないという時間的なプレッシャーにさらされている。
- 開発者はクラウドで共同作業し、継続的にアプリを構築および保守している。
- クラウドが停止し、アプリケーションユーザーに影響が及ぶ場合、オンコールエンジニアが対応している。

これらのアイデンティティは常に時間的な制約に縛られています。そのプレッシャーはセキュリティリーダーにも及んでおり、摩擦のないユーザーエクスペリエンスを実現することがクラウドIAMの最優先事項であり、セキュリティよりも優先されているケースも多くあります。

これは、これまでにもPAMで発生していた「セキュリティの強化」と「生産性の確保」のバランスという課題を彷彿とさせますが、今では利害関係はさらに大きくなっています。セキュリティ管理がITユーザーの業務の足かせとならないようにするなどの社内的な影響に加えて、PAMのオーナーは外部への影響についても考慮しなければなりません。開発者が、顧客向けのアプリケーションの修正に長い時間を要するようになれば、収益性が低下するリスクになります。

開発者はイノベーションを迅速に推進しなければなりません。アクセスする必要のあるサービスやワークロードごとに共有アカウントが作成され、保護されるのを待つことはできません。特に短期間で実施しなければならないプロジェクトではその傾向は顕著になります。このような柔軟性に欠けるアプローチは、クラウドプロバイダーのベストプラクティスとはかけ離れており、エンジニアリングのスケジュールに許容できない遅延を生じさせることもあります。

多くの組織がスピードを重視しています。セキュリティに関する重要な懸念は、今日の企業がクラウド環境における権限とロールのマッピングに使用している、共有型ではなく連携型のアクセスモデルに暗黙的に存在する関係に存在します。

クラウドサービスプロバイダーが新しいサービスを展開するたびに、多くの新しいロールと権限が提供されます。スピードを優先し、この問題を回避するために、企業はクラウドユーザーに必要以上に多くの権限を与える結果になっています。

アイデンティティには、そのロールで必要とされる以上の権限が付与され、強力なアクセス権限を常に利用できるようになっています。アメリカ国家安全保障局（NSA）は、攻撃者がクラウド環境に侵入するために最も多く利用しているのは、設定ミスであると指摘しています。セキュリティの意思決定者のほぼ全員（99%）が、今後1年間にアイデンティティ関連の侵害に直面すると回答しており、その理由の第1位は、クラウド移行のようなデジタルトランスフォーメーションになっています2。

クラウド環境におけるリスクとITスピードのトレードオフに、PAMはどのように対応できるのでしょうか？PAMに関連し、急速に広がりつつある重要な概念であるゼロスタンディング特権について見ていきましょう。

今日のPAMプログラムは、広大で動的な脅威ランドスケープに直面しています。イノベーションにより大きな影響を受け、新たなアイデンティティ、新たな環境、新たな脅威によって再構築を余儀なくされています。

[2] CyberArk 2023 Identity Security Threat Landscape Report, June 2023

本書の読者の方は、ジャストインタイム（JIT）アクセスによるリスク軽減の仕組みについてはよくご存知でしょう。JITアクセスは、パスワードをシステム、アプリケーション、その他のリスクの高い領域への一時的なアクセス権限に置き換えることで、資格情報の窃取を防止します。ゼロスタンディング特権（ZSP）を使えば、セキュリティチームはJITのコンセプト、そしてPAMプログラム全体を新たなレベルに引き上げることが可能になります。

ZSPを使えば、ユーザーには、自分が実行しようとしているタスクに必要な権限だけがジャストインタイムで付与されます。このような仕組みが必要なのは、高度な特権がある管理ロールを常に利用できるアクセス権限には高いリスクが存在するためです。クラウドユーザーのアイデンティティを狙っている攻撃者は、企業の業務を妨害したり、データを窃取したりする恐れがありますが、ZSPによってセキュリティチームは以下を実現できます。

CyberArkが主要なクラウドサービスプロバイダー3社を分析したところ、ユーザーは約1,400のネイティブサービスにアクセスできることが明らかになりました。

これらのサービスを合計すると、40,000以上の異なるアクセスコントロールがあります。

- 高度なアクセス権限を常時提供しないようにして、資格情報盗難のリスクを低減します。
- クラウドでユーザーが必要なときに必要な権限のみを付与することで、最小権限の原則をリアルタイムに適用します。これにより、アカウントの乗っ取りを低減します。管理者レベルのアクセス権限がなければ、攻撃者が実行できる操作は、極めて限定されます。
- 開発者は使いやすいワークフローと統合し、ユーザーは適切なアクセスを簡単に利用できるようになります。これにより、エンドユーザーの採用率が大幅に向上します。
- カスタマイズ可能なポリシーを定義でき、クラウドユーザーの業務に関連する幅広いユースケースに対応できます。

アイデンティティセキュリティが必要なアイデンティティの問題

「PAMを導入し始めたときは、ITユーザーとアカウントを中心に関連すればよかったのですが、特権アクセスがあるアイデンティティが急増し、どのように保護すべきか、わからなくなりました。」

これは、CyberArkが対話をしているセキュリティチームの多くが抱えているフラストレーションです。

当然ながら、CISOやその他のリーダーは、論理的に問題の根本原因を突き止めようし、PAMが解決できる特権の問題なのか？アイデンティティガバナンスと管理（IGA）ソリューションが軽減できるアイデンティティ管理の問題なのか？と質問してきます。

組織の84%が、過去1年間にアイデンティティに関連する侵害を受けています3。あらゆるアイデンティティは攻撃の起点となる恐れがあります。つまり、PAMの問題でも、IGAの問題でもありません。包括的なアイデンティティの問題であり、包括的なアイデンティティセキュリティソリューションが求められています。

攻撃者は常に新しい攻撃手法を考案していますが、特権アクセスを標的にすることには変わりはありません。多くの攻撃は、高度なアクセス権限が付与されたアイデンティティを侵害し、その権限を昇格し、さらに高位のアイデンティティを侵害するためにラテラルムーブメントを行います。これらの攻撃を防ぐためには、従来のサイロ化した対策から脱却し、以下を実現しなければなりません。

- ポリシーベースの最小特権の原則
- 堅牢な多要素認証
- インテリジェントな特権管理の柔軟な適用

セキュリティチームは、システムの統合や統合プラットフォームへの集約を通じて、このアプローチを実現できます。

最も重要なのは、リスクを軽減するために包括的なアプローチを採用することです。

[3] The Identity Defined Security Alliance, 「2022 Trends in Securing Digital Identities」、2022年6月

ここでは、エンジニア、開発者、アーキテクトのイノベーションのスピードを低下させることなく、クラウドの特権アクセスを保護するためのベストプラクティスを紹介します。資格情報の保護や使用状況の監査など、基本的なPAMコントロールは、最新のクラウド環境であっても資産を保護するための基盤の一部となります。

1. ベースラインの要件を満たす

   - ゼロスタンディング特権を導入し、常時アクセスを、ロール、ワークロード属性、責任、アクセスの必要性に基づいて設定されるポリシーに置き換えます。
   - 開発者の既存のワークフローに対応し、既存のツールを統合することで、摩擦のないネイティブアクセスをユーザーがそのまま使用できるようにします。
   - 開発者が任意のツールを使用でき、企業は必要な業界標準や社内標準を適用できるように、シークレット管理とガバナンスを単一のハブに集中させます。
   - 初期段階では、業界の規制を継続的に準拠するための基準を満たすことに重点的に取り組みます。

2. 監査と報告の標準化

   - すべてのアイデンティティのアクセス権限を継続的に可視化することを重要な目的として、監査担当者が要求する証拠、成果物、レポートを提供するためのプロアクティブな戦略を構築します。
   - 「緊急事態」レベルのアクセスを許可するモデルを定義し、クラウドエンジニアリングチームがオンコール対応時に承認を待つことなく迅速に問題を解決できるようにします。
   - クラウドワークロードやサービスに対するリスクの高いアクセスを監視し、監査証跡をWebアプリケーションやオンプレミスのセッションログと同じ場所に保存して、プロセスを合理化します。

3. 継続的な改善の推進

   - すべての新しいクラウド環境で、ロールとアイデンティティ設定を正しく構成し、セキュアなアクセスポリシーが適用されていることを確認します。
   - 自動化を利用して、人間およびサービス間のアクセスに関する業界標準および社内標準を適用します。
   - コンプライアンスと監査承認プロセスを自動化し、手動の業務を軽減し、効率性を向上させます。

As the Threat Landscape Shifts, Mind the Fundamentals

多くのセキュリティリーダーは、今後12か月間でアイデンティティの数が240%増加すると予測しています。それに伴い、PAMプログラムは、以下のような新しいクラスのIDを保護することになります。

クラウドユーザ

例：管理コンソールにアクセスするサイトの信頼性エンジニア

人間以外のアイデンティティ

例：企業ネットワークにアクセスするIoTデバイス。

データにアクセスするすべてのアイデンティティ

例：ビジネスアプリケーションを使用する従業員やベンダー

新しいアイデンティティ、環境、脅威に対応するためにPAMプログラムを進化させるとき、基本に忠実に取り組みを進めることが重要です。多くの企業では、資格情報の保護、セッションの保護、監査への対応など、中核となるコントロールについてさらなる対応が必要です。

62%

機密性の高いリソースへの人やマシンなどアクセスの全体像を把握していない組織の割合。

63%

最高機密のアクセスを適切に保護できないプロセスやテクノロジーを使用している組織の割合。

出典：CyberArk 2023 Identity Security Threat Landscape Report、2023年6月

運用テクノロジーシステムおよびデバイスにおける特権アクセスの保護

ビジネスリーダーの約96%が、製造、ヘルスケア、エネルギーなどの分野で使用されるデバイス、機械、システムなどの運用テクノロジー（OT）の保護に投資する必要性があると考えています。しかし、OTに投資している70%近くの組織は、導入の課題に直面しています4。

その問題の詳細を見ていきましょう。

OTは俊敏性、効率性、デジタルトランスフォーメーションみとって不可欠なものです。デバイスの運用を自動化すれば、製造業企業は需要を満たすために運用の規模を大きく拡大できるようになります。しかし、OTは、以下のようなリスクの高いアクセス権限がある人間や人間以外のマシンなどのアイデンティティを悪用する攻撃者にとって、格好の標的でもあります。

- データやインフラストラクチャなどへのアクセス権限があり高リスクのマシンアイデンティティが組み込まれたデバイス。これには、サイバー攻撃で頻繁に標的になっている産業制御システムも含まれます。
- 多くの場合にリモートから、顧客組織のOTシステムの運用と保守を実施するベンダー。
- OTと連携しているアプリケーションやエンドポイントへのアクセス権限が、単純なパスワードによって保護されている内部ユーザー。これらのパスワードは、フィッシングやランサムウェアによって漏洩することが多くあります。

セキュリティチームは、こうしたリスクを十分に認識していますが、OTは多くの場合、ビジネスチームが管轄しており、テクノロジーの調達、保守、利用について、保護のための十分な指針が確立されていません。OTのオーナーは、これらのシステムを稼働させることが最優先の課題であり、サイバー攻撃の脅威については十分に警戒していないことがあります。

長年にわたり、企業はデバイス、機器、システムを安全に維持する方法として、OTをインターネットや外部システムから物理的に分離する「エアギャップ」の手法を利用してきました。多くの企業は今でもこの方法を採用していますが、エアギャップツールは、あらゆるデバイスがつながり合うOT環境向けには設計されていません。

88%

IoTデバイスをインターネットに接続していると回答した組織の割合。

51%

OTネットワークを企業のIT（ビジネス）ネットワークに接続している組織の割合。

56%

OTネットワーク上のデバイスを、リモートアクセスなどのシナリオのためにインターネットに接続している組織の割合5。

[4] Barracuda, 「2022年産業セキュリティの現状」、2022年6月

[5] Microsoft, 「企業におけるIoTとOTサイバーセキュリティの現状」、2021年

OT攻撃の影響

攻撃者は、1つでもアイデンティティを侵害できれば、OTを制御するマルウェアをインストールするなどの攻撃を実行でき、以下のような甚大な影響が発生する恐れがあります。

- 製造業者の設備を停止して、収益にダメージを与える。
- 企業が規制を遵守できない状況に陥らせ、信頼を低下させる。
- 病院が治療を提供できないようにし、患者に深刻な影響を及ぼす。

主な例：

コロニアルパイプライン社：この石油パイプライン企業に対するランサムウェア攻撃により、同社は操業ができなくなり、パイプラインの一時停止を余儀なくされ、米国東海岸のエネルギー供給に影響が生じました。

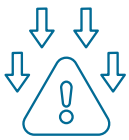
SolarWinds：攻撃者は、ITサービス企業のソフトウェアサプライチェーンを侵害し、重要インフラ関連のプロバイダーなどの組織にマルウェアを展開するために利用しました。

フロリダ州オールズマー市：攻撃者は水処理施設の制御装置を操作し、有害なレベルの化学物質を添加し、水源を汚染しようとしました。

一方で、セキュリティチームは、解決済みであるはずの脆弱性に未だに悩まされています。多くの組織では、数年前にサポートが打ち切られ、パッチが提供されなくなった旧式のOSを使用してOTを稼働させています。例えば、製造業企業の半数近く（46%）が、2001年にリリースされ、2014年にサポートが終了したWindows XPをいまだに使用しています6。

セキュリティチームは皮肉な状況に直面しています。運用に欠かすことができないテクノロジーが、攻撃者によって悪用され、その運用を停止される恐れがあるのです。また、OT環境のサーバーにアクセスするアカウントを保護するためのアイデンティティセキュリティ管理を実施している組織は、わずか36%に過ぎません7。

ここからは、OTの機能停止を防止する方法について説明します。進化したPAMを活用することで、インテリジェントな特権管理をすべてのアイデンティティに適用し、リスクを低減し、トランスフォーメーションを実現する方法を紐解いていきましょう。ここでは、OT環境におけるアイデンティティのリスクの高いアクセスを保護するための6つの領域を最初に紹介します。



1. OT資産全体のリスクの評価

OTは、あらゆる部門で利用されており、リモートからアクセスされることも、クラウドサービスに接続されていることもあります。例えば、資産管理ソリューションを使用して、すべてのOTを特定することで、脆弱性を完全に理解し、十分な情報に基づいた意思決定を行うことができます。

2. リスクの高いアクセスの検知

OTシステムに接続されているソフトウェア、ハードウェア、または物理的アセットのアカウントを特定します。機密性の高いリソース、インフラ、環境にアクセスできるユーザー数を把握し、これらのユーザーが何にアクセスでき、どのようなアクションが可能かを把握します。

[6] Blackberry, 「Operational Technology Cyberattacks and the 2023 Threat Landscape」、2023年
[7] CyberArk 2023 Identity Security Threat Landscape Report, 2023年6月

3. 安全な資格情報

Tデバイスのコードに埋め込まれている資格情報など、すべての特権資格情報を保管して、ローテーションします。資格情報から、ジャストインタイムのアクセスへ移行し、生体認証によるMFAなどのパスワードレスオプションで認証します。

4. インテリジェントな特権管理の適用

PAMコントロールをゲートウェイと統合し、特殊なOTテクノロジーへのアクセスを保護します。セッションを監視および分離して脅威を検知し、必要に応じてセッションなどのアクティビティを一時停止します。シークレット管理を採用し、自律的な対策を講じて、マシンのアイデンティティが使用する資格情報を保護します。

5. エアギャップへの対策

エアギャップ環境で動作するユーザーがオフラインで安全に認証情報を取得できるように管理します。ポリシーに基づいて資格情報をローテーションし、ユーザーがオフラインの職場を離れた後、再入場する前に、ユーザーのモバイルデバイスと資格情報を同期させます。

6. 主要な規制の順守

攻撃を防止して監査の要件を満たすためのプロセスとコントロールを文書化していることを確認します。米国大統領令14028やEUのネットワーク情報システムに関するNIS2指令などは、重要インフラのセキュリティを向上させることを目的としています。

PAMのクイックウィンを確認できるように段階的かつ継続的に計画を遂行

ある顧客は、いくつかの段階に分けてPAMを導入していました。いくつかのプロジェクトでは、全体像を把握できない可能性があり、この顧客のセキュリティリーダーはこれらのプロジェクトに着手すべきかどうか検討していました。このリーダーの注意力と集中力は賞賛されるべきものですが、エンドポイントやサーバーからローカル管理者権限を削除するという、小規模なPAMの取り組みから開始することには利点があります。

運用をテクノロジー（OT）は、エンドポイントに適用されている過剰な特権を排除することが大きな効果をもたらす分野の一つです。攻撃者がOTエンドポイントのローカル管理者アカウントを侵害した場合、マルウェアをインストールして使用することができます。OTはランサムウェア攻撃の格好の標的になっています。サイバー攻撃者は、OTを利用している組織にとって業務中断の影響が甚大であることを熟知しています。

時には、計画を100%その通りに遂行することが正しい場合もありますが、ローカル管理者権限を削除したからといって、大規模な取り組みの障害になるわけではありません。計画を調整することで、短期的なセキュリティ対策と法規制へのコンプライアンスを改善し、クイックウィンを得ることができ、PAMソリューションの成果を明確に示すことができる場合もあります。

企業に環境に合わせたPAMプログラムの進化

CyberArkの業務では、さまざまな業界や地域のセキュリティリーダーと会うことがあります。対話をするたびに、企業が直面する課題について知見を得ることができますが、企業はそれぞれ異なっており、それぞれにPAMの過去、現在、未来を反映したニーズがあります。

特権があらゆるところに存在する現在の脅威ランドスケープにおいて、PAMの重要性はかつてないほど高まっています。今日の企業のセキュリティを確保するには、実績のあるPAMの原則とインテリジェントな特権管理のバランスを取りながら、あらゆる環境のすべてのアイデンティティを対象とする必要があります。これは、セキュリティと生産性のバランスを適切に確保する方法です。基本に忠実に、未来を見据えた対策を行ってください。

次のステップ

オンデマンドウェビナー「PAMプログラムを今すぐに向上すべき理由」を参照してください 。

電子ブック「The Gorilla Guide：特権アクセス管理」を参照してください

お問い合わせいただき各業界や業種向けのデモ を予約してください。

About CyberArk

CyberArkはアイデンティティセキュリティのグローバルリーダーです。CyberArkは、インテリジェントな特権管理を中心に、ビジネスアプリケーション、分散ワークフォース、ハイブリッドクラウドワークロード、そしてDevOpsライフサイクル全体において、人間や機械などあらゆるIDに対して最も包括的なセキュリティを提供します。CyberArkは、ビジネスアプリケーション、分散ワークフォース、ハイブリッドクラウドワークロード、およびDevOpsライフサイクル全体にわたって、人間またはマシンのあらゆるアイデンティティに最も包括的なセキュリティを提供します。世界の一流企業が、最も重要な資産のセキュリティ確保にCyberArkを活用しています。

CYBERARK®
The Identity Security Company