SPONSORED CONTENT | WHITE PAPER

Cybersecurity

ゼロトラスト時代の特権アクセス管理（PAM）を容易にするには？

高機能と使いやすさを兼ね備えたオールインワンPAM「ManageEngine PAM360」

ますます高度化・巧妙化するサイバー攻撃、さらには内部不正による情報流出など、昨今のセキュリティリスクを考慮したとき、PAM（Privileged Access Management：特権アクセス管理）は、あらゆる企業や組織が備えるべき必須の対策となっている。特に従業員の働き方が多様化するとともに、さまざまなクラウドサービスの活用が進む中で、分散するITリソースに対するアクセスを厳しく検証する必要があり、ゼロトラストの仕組みの中心に特権アクセス管理を位置づけて徹底する必要がある。この課題を解決すべくゾーホーが提供している統合特権アクセス管理ソリューション「ManageEngine PAM360」について解説する。

世界で28万社以上の企業や組織に導入される、ゾーホー「ManageEngine」

ゾーホージャパン株式会社は、ワールドワイドで事業を展開するZoho Corporation Pvt. Ltd.（本社インド）の日本法人で、IT運用管理製品群「ManageEngine」やクラウドサービス群「Zoho」、それに関連するサポート、コンサルティングを提供している。本資料で紹介するManageEngineシリーズは、世界で28万社以上の企業や組織に導入され、必要十分な機能、リーズナブルな価格、直感的な操作感で日本でも多くの導入実績がある。

CIO

SPONSORED BY ZOHO

Cybersecurity

特権アクセス管理の不備が招くリスク

サイバー攻撃の多くが特権アカウントの悪用が原因だ。システムに侵入した攻撃者は権限昇格を試み、最終的に特権アカウントを奪い取ろうとする。特権アカウントとは、その名のとおりシステムやデータに対して最高レベルのアクセス権限を持つアカウントであり、これが悪用されると機密情報の漏えいやデータの改ざん・破壊、システム停止といった深刻なインシデントを発生させることになる。また、特権アカウントの悪用は外部からの攻撃だけに限らず、従業員や派遣社員、業務委託者による犯行も発生しており、内部不正のリスクが高まっている。

だが、企業における特権アクセス管理は、多くの課題を抱えているのが実情だ。特権アクセス管理が特定の運用担当者による属人的な対応に依存しており、複数システム間でのパスワードの使い回しやデフォルトのままでのパスワード利用を見逃していたり、特権ユーザーが退職や異動した後も、そのアカウントがしばらく放置されていたりといったケースが散見される。

加えて特権アカウント利用の監査体制にも大きな問題がある。誰が、いつ、どこから、どのシステムやデータにアクセスし、どんな操作を行ったかという履歴（ログ）の記録が不十分で、万一インシデントが起こった際にも追跡は困難だ。

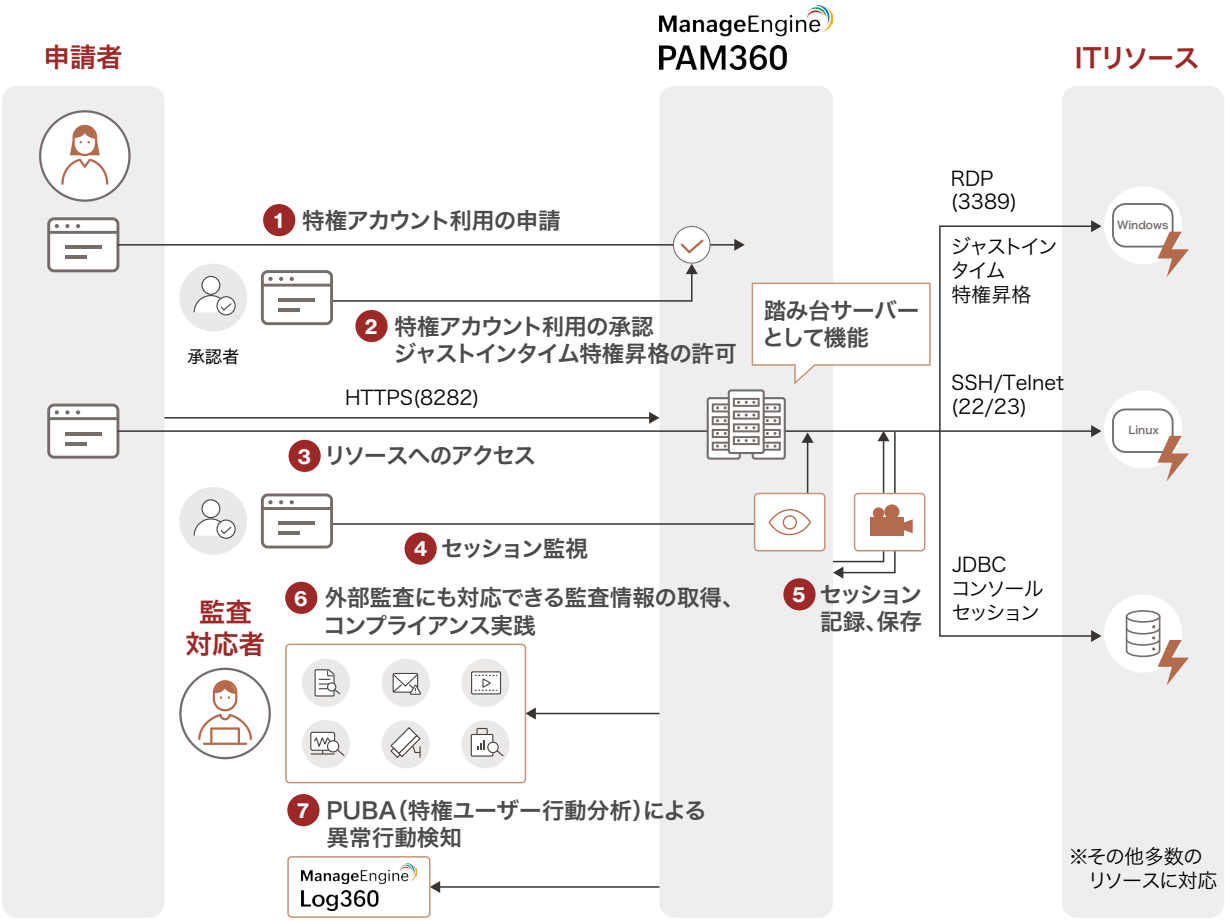
特権アクセスの一連のプロセスを管理する「ManageEngine PAM360」

そこで求められているのが、システムやクラウドサービスごとに散在する膨大な特権アカウントを一元管理するPAMだ。PAMにより、限られた運用管理者の属人的な対応をなくしセキュリティレベルを大きく向上させるのはもとより、企業のコンプライアンス対応にも寄与する。すべての特権アクセスに関する詳細なログを記録することで内部統制を強化でき、各種セキュリティ監査への対応もスムーズになる。

そうしたPAMのうち、世界中でManage Engineシリーズを展開するゾーホーが提供しているのが、特権アクセス管理をオールインワンで実現する「ManageEngine PAM360」だ。実はゾーホーでは、従来から特権アクセス管理のできる「ManageEngine Password Manager Pro（PMP）」を提供してきたが、PAM360はその上位製品にあたる。より豊富な機能を備え、大手企業や金融機関、官公庁などにおける大規模システムやミッションクリティカル環境にも対応可能だ。

単に特権アカウントのパスワード管理だけにとどまらず、特権アカウントの利用申請・承認、リソースへのアクセス、ジャストインタイム特権昇格、セッション監視、セッション証跡記録などの一連のプロセスをセキュアに管理することで、組織全体のセキュリティレベルを向上する。

特権アカウントの一連のプロセスをセキュアに管理するPAM360



1. 特権アカウント利用の申請
2. 特権アカウント利用の承認、ジャストインタイム特権昇格の許可
3. リソースへのアクセス（PAM360は踏み台サーバーとして機能）
4. セッション監視
5. セッション記録、保存
6. 外部監査にも対応できる監査情報の取得、コンプライアンス実践
7. PUBA（特権ユーザー行動分析）による異常行動検知

さらにPAM360は、導入・操作が容易なことも特長だ。特権ユーザーとのそのアカウント、保護すべきリソースの検出と管理を単一のブラウザ画面から実施することが可能で、複数のクラウドサービスに分散するアカウントの管理にも対応している。また、特権アクセス管理に必要な機能をオールインワンで備えているため導入が容易で、直感的でわかりやすいUI（User Interface）も完備していることから、すぐに運用を開始できる。

ゼロトラスト環境での特権アクセス管理を実現する充実した機能

PAM360が提供している主要な機能と、その特長を掘り下げていこう。

まず注目すべきは、ゼロトラスト環境での特権アクセス管理の要となる「特権昇格および委任管理（PEDM：Privileged Elevation and Delegation Management）」機能だ。

PAM360は重要システムへの特権アクセスに制限時間を設けるジャストインタイム（Just-In-Time、JIT）の特権昇格やリソース上でユーザー自身が特権を一時的に昇格できるセルフサービス特権昇格を実現しており、各エンティティ（管理者、ユーザー、アプリケーション、スクリプト）は、必要なときに、必要な期間だけ、機密情報にアクセスできる権限が付与される。いわゆる「ゼロスタンディング特権 (ZSP: Zero Standing Privilege) 」の原則を導入することが可能となる。常に特権が付与された状態の「スタンディング特権」を排除し、「最小特権の原則 (POLP：Principle of Least Privilege)」を徹底した運用を実現することで、セキュリティ侵害のリスクを最小限に抑えられる。

また、「信頼スコア」によるユーザーとリソースの総合的なリスク評価もPAM360ならではの大きな特長だ。信頼スコアとはユーザーやリソースの信頼度を数値化したもので、例えばユーザーの信頼スコアの場合、PAM360はユーザーのログイン失敗回数や、使用デバイス、所属グループ、アクセス元IPアドレス、時間帯、二要素認証の有無など、多岐にわたる要素を総合的に捉えてリアルタイムにスコアを計算する。さらに信頼スコアに応じたアクションの自動実行が可能だ。例えばスコアが一定のしきい値を下回った場合、そのユーザーに対して、警告・アクセス理由の要求・アクセス拒否などの措置を講じることができる。

ほかにもPAM360は、下記のような機能を通じて包括的な特権アクセス管理を実現する。

●特権アクセス申請・承認フロー

ユーザーが必要なリソースと期間を指定してアクセスを申請すると、事前に設定された承認者がその妥当性を判断し、承認された場合のみ一時的に特権アクセスが許可される。また、申請履歴はすべて記録され、後からの監査証跡として活用できる。

●セッション録画・監視機能

特権セッションをリアルタイムで監視し、すべての操作を動画として記録する。管理者は実行中のセッションに参加し、ユーザーの操作を監視することが可能。セッション内で不審または不正な行為を見つけ次第、セッションを強制終了できる。録画されたセッションは、改ざん防止機能付きで安全に保存され、問題発生時の原因究明や定期的なコンプライアンスチェックに役立てられる。

●コマンド制御 / アプリケーション制限

特権アカウントで実行できるコマンドや、利用できるアプリケーションを制限することができる。

●SSH鍵・SSL証明書管理

SSH鍵やSSL証明書の生成から配布、更新、失効までライフサイクル全体を一元的に管理する。これにより証明書の失効によるサービス停止といった事態を未然に防ぐとともに、中間者攻撃などのサイバー攻撃を回避してセキュアな通信環境を維持する。

●レポート・監査機能

いつ、誰が、どの特権アカウントにアクセスしたのか、履歴を監査証跡として簡単にレポート化できる。NERC-CIP、GDPR、PCI-DSS、ISO-IEC 27001など、主要な規制に対応したテンプレートを用意している。

●PUBA（Privileged User Behavior Analytics「特権ユーザー行動分析」）機能

ManageEngine Log360 UEBAと連携することで、機械学習アルゴリズムの活用によって、特権ユーザーと特権アカウントの行動パターンを分析し、基準となる標準的な行動パターンを発見・構築することが可能。これにより、不審な行動の迅速な検出・抑止や、フォレンジック分析を用いた根本原因の究明を可能とするとともに、再発防止に向けた対策を支援する。

組織の成長は、セキュアな情報基盤から

いまや、安心して事業を行うためのセキュアな情報基盤の維持が欠かせない。PAM360を導入することで、企業は大きく3つのメリットを享受することができる。

1つ目は、セキュリティリスクの低減だ。

特権アクセスを可視化し、不審な挙動を検知してセキュリティ侵害に対する防御力を強化。またゼロトラストの考えに基づき、必要な時のみ権限を付与するJITアクセスで過剰な権限を防止できる。さらに信頼スコアにより動的にリスクを判定し、必要に応じて警告を表示したり、アクセスを拒否することも可能。NIST、PCI-DSS、ISO/IEC 27001などのセキュリティやコンプライアンスに関わる基準にも準拠している。

2つ目は、運用の効率化と自動化。

PAM360によって申請・承認ワークフロー、パスワードの変更、パスワードの利用履歴の記録・レポート作成が自動化され、これまで運用担当者が手作業で行っていた管理業務が大幅に効率化される。これによりIT部門は、より戦略的な業務にリソースを集中することが可能となる。

3つ目は、長期的なコストパフォーマンスの確保。PAM360には、システムやユーザーの追加・増加にも柔軟に対応できるライセンス体系が用意されている。これにより企業は事業の成長にあわせた投資を行い、計画的なセキュリティ強化を実現できる。

特権アクセス管理にまつわる課題を包括的に解決するPAM360は、組織のセキュリティ体制を大幅に向上させる。また、ゼロトラストを前提とした最小特権の原則（POLP）を徹底した運用を実現することで、マルチクラウド環境にも柔軟に対応しつつ、常に最新のセキュリティ要件に応え続けていく。ますます深刻化するサイバー攻撃や内部不正リスクに備え安心して事業活動を行うために、PAM360の活用を検討してみてはいかがだろう。