



# Keeper Security インサイトレポート

## 特権アクセス管理に関する調査

### コストと複雑さに関するユーザーインサイト

調査結果によると、PAMソリューションが複雑すぎるため、68%の企業がほとんど使用されない「無駄な機能」のために費用を支払っている

2023年1月にKeeper SecurityがTrendCandy Researchと共同で実施した400人のITおよびセキュリティ管理者を対象としたグローバル調査によると、導入と維持が容易な特権アクセス管理 (PAM) ソリューションに対する業界の強い要望が明らかになりました。この調査結果で、従来のPAMソリューションは、実装や使い方が複雑すぎるのが主な原因で、まったく不十分であることがわかりました。実にITリーダーの84%が、2023年にはPAMソリューションを簡素化したいと回答しています。

現在の高リスクのセキュリティ環境では、すべての組織が特権的資格、特権アカウント、特権セッションを保護し、重要資産を守ることが不可欠とされています。しかし、従来のPAMソリューションの多くは、導入が複雑すぎる、コストがかかりすぎる、またはその両方であるため、コアユースケース以外では、本来の価値を提供できていないのが現状です。リモートワークの時代には、重要なリソースへの不正な特権アクセスを監視、検出、防止することで、サイバーセキュリティの脅威のベクトルから保護できる、俊敏なアイデンティティセキュリティソリューションが必要です。

特権アクセス管理の主要なイノベーターであるKeeper Securityは、ITリーダーがどのようにPAMについて考え、PAMソリューションを展開し、PAM実装を合理化しているかを理解するために、より良い方法を探っていました。Keeperは、独立系調査会社に依頼し、北米と欧州のITおよびデータセキュリティのリーダー400人を対象に、2023年のPAMに関する戦略と計画について調査を実施しました。



# ユーザーのフィードバック PAMソリューションの不足

特権アクセス管理ソリューションは、主にITスタッフ、経営幹部、研究開発スタッフを保護するために設計されています。しかし、デジタル変革の加速とサイバー脅威の絶え間ない増加により、組織内のすべてのエンドユーザーを保護することがますます重要となっています。

PAMの導入は今日、企業全体に広がっており、調査回答者の91%がすでに何らかのPAMソリューションを使用していると回答しています。しかし、シンプルさへの欲求が広がっており、87%の回答者が導入や使用がより簡単な「簡素化された」形態のPAMを希望していると回答しています。また、回答者の58%が「PAMソリューションに間違いなく、あるいは多分何らかの無駄がある」と答え、84%が「2023年にPAMソリューションを間違いなく、あるいはおそらく簡素化したい」と回答しています。




ITリーダーの10人に9人以上（91%）が、PAMソリューションによって特権ユーザーの行動をよりコントロールできるようになったと回答しています。しかし、大多数の組織（85%）は、PAMを管理・維持するために専門のスタッフが必要であると付け加えています。さらに、このソリューションでは、組織の一部のユーザーしか保護できないことが多く、非特権ユーザーを保護するためには、さらにソリューションを購入する必要があります。この支出の結果、ITリーダーの約3分の2（62%）は、経済状況の悪化により、現在のPAMソリューションの規模を縮小する可能性が高いと回答しています。



87%

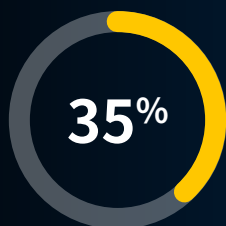
の回答者が、導入と利用が容易な「簡素化された」形態のPAMを希望している

この調査によると、ITチームの半数以上（56%）が、PAMソリューションの導入を試みたが、完全には導入できなかったと回答しています。そのうちの92%は、PAMソリューションが複雑すぎて完全には導入できなかったからだと答えています。これは、回答者がPAMの中核的な機能と利点を求める一方で、よりシンプルなプロビジョニングとより迅速な展開を強く望んでいることを示しています。その他、注目すべき点は以下の通りです。

-  3分の2以上のIT管理者（68%）が、現在のPAMソリューションは複雑すぎる、あるいは必要のない機能が多すぎると回答しています。
-  平均して、ITチームは現在のPAM機能の62%しか使用していません。
-  ITリーダーの3分の2（66%）は、より優れたPAMソリューションが必要だと回答していますが、58%は高価すぎるため持っていないと回答しています。



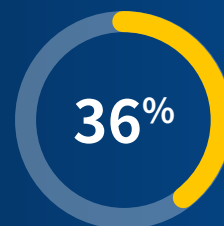
また、調査回答者の約3分の2は、高価で余分なPAM機能はユーザーにとって複雑すぎるため、組織の規模に関わらずユーザーの満足度を低下させると回答しています。



のITリーダーが、現在のPAMソリューションに高い満足度を示している



の大企業のITリーダーが、現在のPAMソリューションに高い満足度を示している








の中堅企業のITリーダーが、現在のPAMソリューションに高い満足度を示している

## 企業は、業務上の課題 に対応するための新しい ソリューションを求 めています。

パンデミック後の仕事場では、今後もハイブリッドな働き方が求められます。また、ネットワークの境界がオフィスの枠を大きく超えたため、IT専門家、特に意思決定者は、セキュリティ目的のためにネットワークの監視と管理が非常に重要であることを認識する必要があります。セキュリティリーダーは、組織全体でSaaSアプリケーション、Wi-Fi接続、エンドユーザー体験を合理化するIT戦略を策定する必要があります。

この調査結果から、ITおよびセキュリティのリーダーは、従来のPAM製品のようなコストや複雑さを伴わずに、最も機密性の高いシステムを保護できるPAMソリューションの採用に強い関心を持っていることがうかがえます。条件として、より早く導入できること、より手頃な価格であること、よりシンプルに理解・統合できることなどが挙げられました。また、メンテナンスが容易で、コストを押し上げる不要な機能が少ない小規模なPAMソリューションを求めているとのことでした。

調査結果によると、ITリーダーがPAMソリューションに求めるメリットの上位5項目は以下の通りです。

-  特権ユーザーのアクセス管理およびモニタリング
-  情報漏えいの防止
-  外部脅威者による特権的資格情報の侵害からの保護
-  企業内部の人間による特権的なアクセスの偶発的または意図的な誤用からの保護
-  特権ユーザーのアクセスを確実に更新し「特権のクリープ」を防ぐ



また、回答者は、簡素化されたPAMソリューションの利点の上位5つを共有しています。

  
導入が容易

  
他システムとの統合が容易

  
コスト削減

  
連結プラットフォーム

  
より少ない人員で済む



## 結論

# 企業は「従来のPAM」を統一的なソリューションに置き換えるべき

この調査結果は、高価で使いにくくなっている従来のPAM製品にユーザーが不満を抱いている理由を明らかにしています。従来のPAMソリューションは、高価なオンプレミス管理が必要で、導入に時間がかかり、すべてのユーザー、すべてのデバイス、すべての場所から監視・保護することができません。回答者は、組織全体にわたる完全な可視性、セキュリティ、コントロール、コンプライアンス、およびレポートングを提供する統一されたPAMソリューションを求めています。

ゼロトラストのコンセプトは、効果的なPAMソリューションの基礎となるもので、SaaSが企業にとって好ましい導入方法となるにつれ、厳格なゼロ知識アプローチの重要性が増しています。ゼロ知識アーキテクチャは、攻撃者やベンダーの両方からユーザーデータを保護し、すべてがクライアント側で暗号化されるため、ベンダーによる侵害や内部脅威も軽減されます。しかし、従来のPAMソリューションのほとんどは、ゼロ知識の原則を厳密に守っていません。企業は、特権的なユーザーだけでなく、すべてのユーザーの認証情報を保護することにますます関心を寄せています。ゼロトラストやゼロ知識のセキュリティ・プラットフォームは、従業員クレデンシャルの運用を全面的に可視化し、管理することができます。

デジタル環境は、平均的なITプロフェッショナルの手に負えないほど進化し続けており、テクノロジーの進化と職場の変化に伴い、今後もその傾向が続くと思われます。リモートのハイブリッドワーカーに対応するため、組織のデジタル化が急速に進み、「見えないものは守れない」ということが重要視されるようになりました。サイバー脅威の可視性を維持し、次の波の先を行くために、ITおよびセキュリティリーダーは、変化し続ける職場環境に適応し、自動化し、進歩する必要があります。