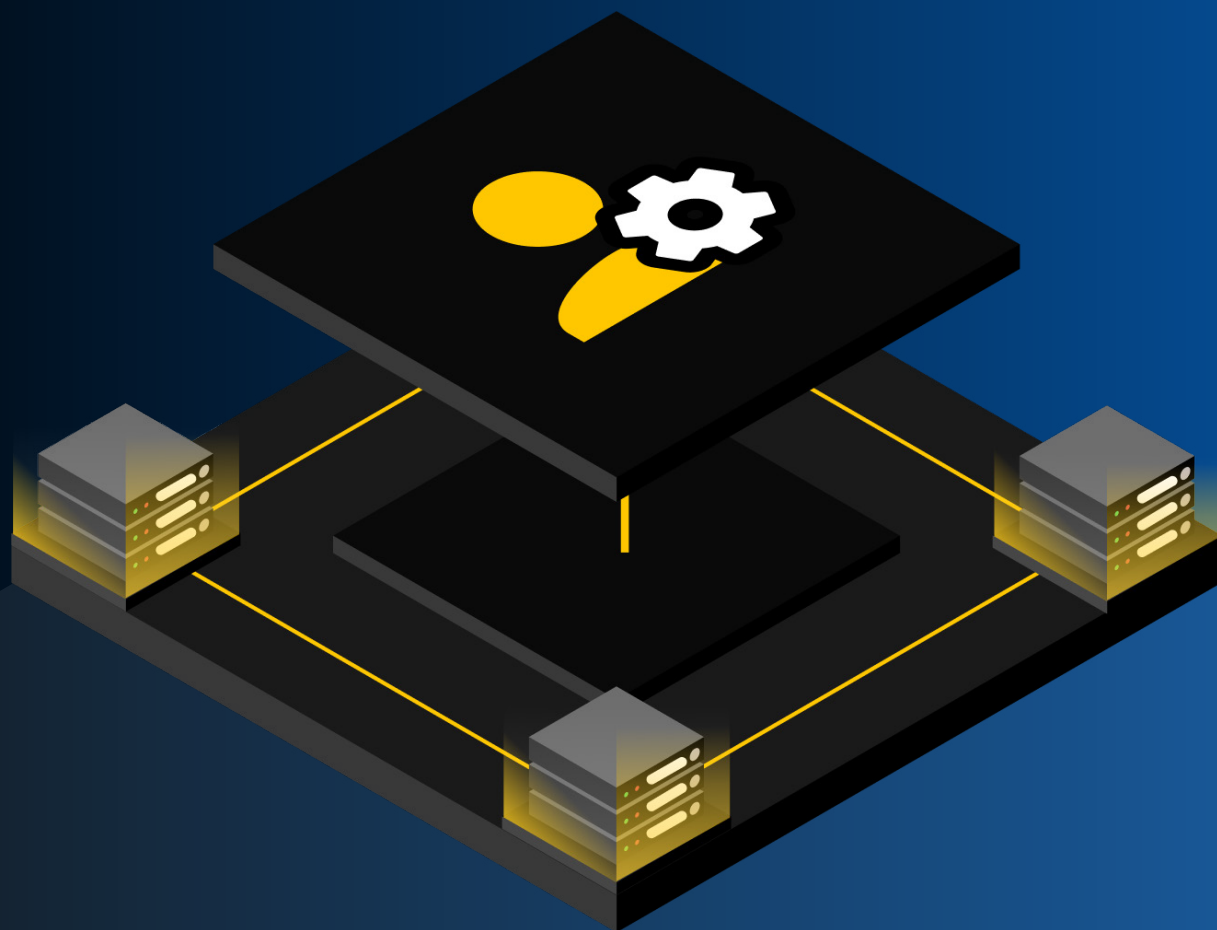




## Keeper Security インサイトレポート

### 特権アクセス管理調査

景気の先行き不透明感の中での展開

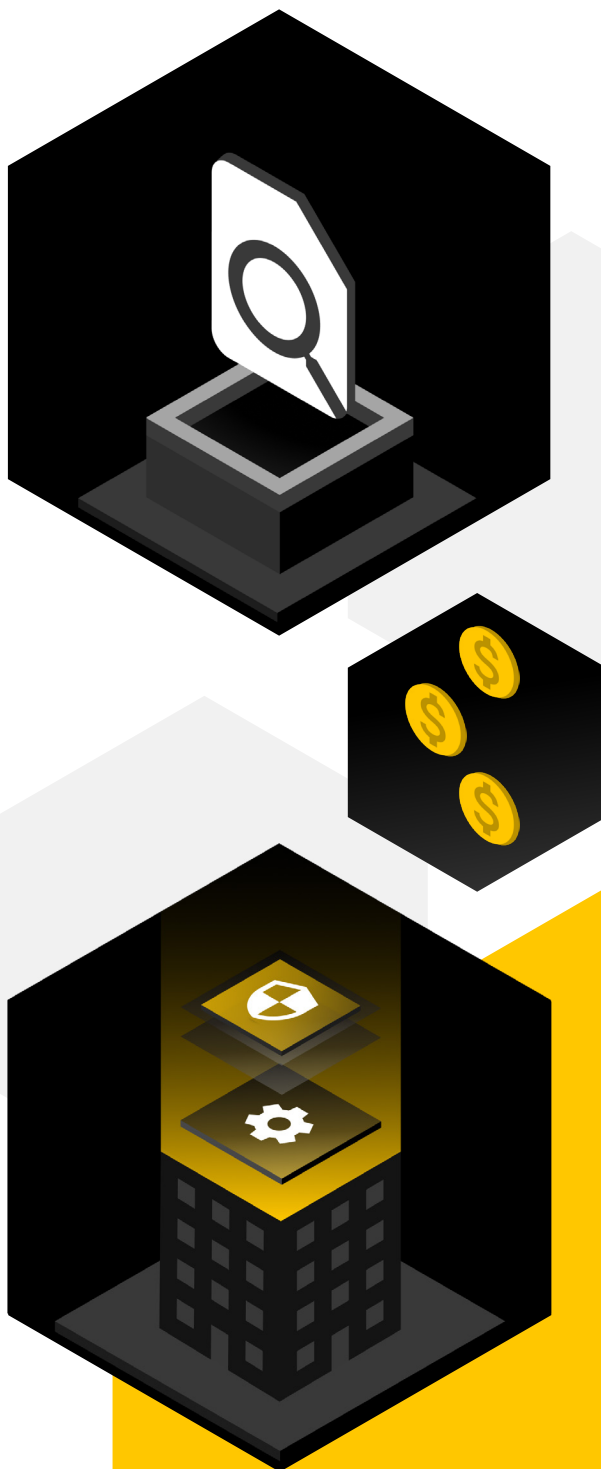


## 調査によると、ITチームの58%がPAMソリューションを高価すぎるという理由で導入していないことが判明しました

Keeper SecurityがTrendCandy Researchと共同で2023年に実施した400人のITおよびセキュリティ担当役員を対象としたグローバル調査では、特権アクセス管理 (PAM) ソリューションが重要視されているものの、コストの制約や複雑すぎるソリューションが導入の足かせになっていることが明らかになりました。実際、回答者の56%がPAMソリューションの導入を試みたものの完全には実装しなかったと回答しており、92%が効率的に導入するには複雑すぎるため完全には実装しなかったと回答しています。この調査結果から、使いやすく手頃な価格のPAMソリューションを業界が必要としていることは明らかです。

脅威の状況が進化し、攻撃対象領域が拡大している中、効果的な PAMソリューションの重要性はかつてないほど高まっています。情報漏洩のほとんどは、盗まれた、あるいは漏洩した認証情報と、ラテラルムーブメントによる権限の昇格に起因しており、PAMはこのような事態を防ぐのに理想的なソリューションです。しかし、景気の先行き不透明感から予算が厳しくなると、PAMの導入は後回しにされてしまいます。組織は、サイバー犯罪者に先手を打つために、シンプルで手頃な価格のソリューションを必要としています。

特権アクセス管理のイノベーターとして業界をリードするKeeper Securityは、現代の企業や中堅企業での、現在の経済情勢におけるPAMの導入について理解を深めたいと考えていました。Keeperは独立調査会社に依頼して、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、PAMの導入、ユーザビリティ、および2023年のPAMの計画に関する洞察を得るために調査を実施しました。



## ユーザーフィードバック

### 高いコストと複雑性は 導入制限の課題

PAMソリューションのメリットはいくら強調してもしすぎることはありません。ITリーダーの実に91%が、PAM製品によって特権ユーザーの活動の管理が強化されたと述べています。不十分なアクセス管理は「特権のクリープ」につながり、内部および外部からの情報漏洩のリスクを増大させるため、特権ユーザーの管理は極めて重要です。リモートワークやハイブリッドワークモデルへの広範な移行に伴い、組織は、センシティブデータや重要なリソースへの不正な特権アクセスを監視、検出、防止することによりサイバーセキュリティの脅威から保護する、俊敏なIDセキュリティソリューションを必要としています。

特権アクセス管理の重要性が認識されている一方で、ITチームの58%が、PAMソリューションは高価すぎるため導入していないと述べており、ITリーダーの3分の2近く（62%）が、経済状況の悪化により、現在のPAMプラットフォームを縮小する可能性が高そうだと回答しています。

PAMソリューションの導入に当たっては製品の複雑さも課題の一つです。回答者の56%がPAMソリューションを導入しようとしたが、完全には実装できなかったと回答しており、92%が効率的に行うには複雑すぎるため導入しなかったと回答しています。これらの結果は、迅速なプロビジョニング、使いやすさ、今日のITプロフェッショナルが必要とする機能を備えた、よりシンプルなソリューションの必要性を示唆しています。

マクロ経済的な圧力によって予算が厳しくなり、企業はセキュリティの予算を削減する傾向にあります。組織がPAMの導入はこれまで以上に重要となっていま

す。Keeperの2022 Cybersecurity Census報告書によると、米国の企業は年間平均42件のサイバー攻撃を経験しており、回答者の圧倒的多数が2023年にはこうした攻撃が増加すると予測しています。このことから、シンプルで効果的なサイバーセキュリティソリューションは不可欠です。PAMソリューションがなければ、組織は可視性と管理の不備、コンプライアンス要件への対応の困難さ、データ漏洩やサイバー攻撃のリスク増大といった課題に直面します。



# 91%

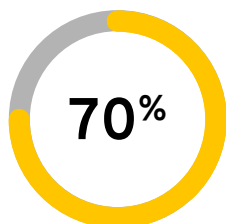
のITリーダーがPAM製品によって  
特権ユーザーの活動の管理が  
強化されたと述べています

## 業界が望む、IT リーダーが必要とする機能を備えた、よりシンプルなPAMソリューション

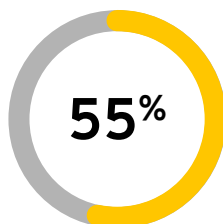
PAM製品は昔から非常に複雑で、購入するには高価で、導入とメンテナンスにコストがかかり、使いこなすのが非常に難しく、多くの場合、運用には相当な専任スタッフが必要です。中小企業でもFortune100企業でも一時解雇が行われる中、導入とメンテナンスが容易なPAMソリューションの重要性は増すばかりです。現在、業界にはこのようなソリューションが不足しており、調査対象となったITリーダーの85%が、PAMの管理とメンテナンスには専任のスタッフが必要であると回答しています。多くの企業や中堅企業は、PAMソリューションの管理とメンテナンスに専任のスタッフを投入できるだけのリソースを持っていませんが、だからといってPAMプラットフォームの導入を躊躇すべきではありません。

国際通貨基金 (IMF) が来年、先進諸国経済の成長鈍化が特に顕著になると予測する中、組織は、導入にもメンテナンスにもコストのかかるこうした従来のソリューションの財政的実現可能性に取り組まなければなりません。

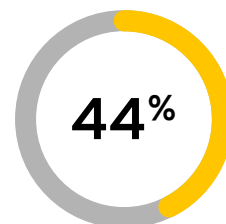
調査回答者は、小規模なPAMソリューションへの強い要望を示し、  
以下のメリットTOP3を挙げています。



管理/メンテナンスが容易

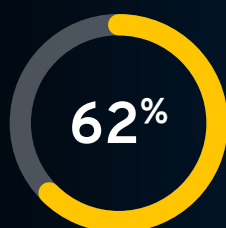


既存の技術スタックへの  
統合が容易



組織にとって不要な機能の  
ためのコストを減らす/負担  
しない

どのような機能が重要かという質問に対して、回答者が組織で最も頻繁に  
使用されていると答えた主なPAM機能は以下の通りです。



二要素認証



役割ベースのセキュリティ



レポーティング/監査

## 結論

# PAMの広範な導入のために重要なのは、コスト削減と複雑さを軽減することです。

サイバー犯罪者が巧妙になり、新たなテクノロジーが悪意のある目的に利用されるようになるにつれ、今日のITおよびセキュリティリーダーは、かつてないほどの脅威に対処しています。現代の脅威の状況は、広範な予算および人員の削減と相まって、ITリーダーを困難な立場に追い込んでいます。ITリーダーは、迅速な導入、リーズナブルな価格、使いやすく統合しやすいソリューションを求めています。これにより、最も慎重なセキュリティが必要なシステム、パスワード、シークレット、特権アクセスの管理機能を統合した、新しいPAMソリューションへの需要が高まっています。PAMの広範な導入を実現するには、よりシンプルで手頃な価格のソリューションが必要です。PAMプロバイダーは、ソリューションの開発と革新を進める際に、高額な価格設定を参入障壁とせず、組織が求める高い価値とセキュリティを提供することが重要です。