KEEPER

従来型PAMの枠を超えて, 現代企業にふさわしい高度なアクセス管理へ

2025年7月 EMAホワイトペーパー (著者: ケン・ バックラー [Ken Buckler] (CASP)、情報セキュリティ・ リスク・ コンプライアンス管理部門 リサーチディレクター)

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

目次

はじめに

絶え間ないサイバー攻撃の脅威と急速なデジタル変革の時代において、特権アクセス管理 (PAM) は、セキュリティの基盤となる分野として確立されました。現代の企業が求めているのは、単なる認証情報の保管ではありません。重要資産を保護し、最小権限アクセスを徹底し、オンプレミスとクラウドの両環境でシームレスに統合できる、包括的なフレームワークです。

効果的なPAMの第一歩は、堅牢な本人確認と多要素認証の導入です。ハードウェアトークン、モバイル承認、生体認証などを組み合わせ、エンドツーエンドの暗号化とゼロ知識セキュリティによって支えられた仕組みが必要とされます。ゼロトラストアーキテクチャのもと、細やかなロールベースの制御とジャストインタイム型の権限付与により、ユーザーには業務に必要最小限の権限のみが付与され、不正アクセスや侵害による影響を大幅に軽減できます。同時に、すべての特権セッションに対して、実行されたコマンド、画面の再生、セッションの継続時間まで含めた監査ログが記録されます。これらの監査ログは自動化されたコンプライアンスエンジンに取り込まれ、HIPAA、SOX、PCI DSSといった各種規制への準拠を支援します。さらに、定期的な再認証キャンペーンにより、不要なアカウントや過剰な権限が排除されます。

クラウドサービスや既存ツールとのシームレスな統合は不可欠です。スクリプト、CI/CDパイプライン、リモートアクセスゲートウェイへの認証情報のインジェクションにより、ユーザーの生産性を損なうことなく、監視と制御を維持できます。さらに、高度な行動分析とエージェント型AIによって、PAMは「能動的な防御」へと進化します。リアルタイムのアラートとアクションにより、脅威を即座に遮断し、特権の剥奪も即時に行うことが可能です。こうした制御を、共有時間やデバイスを制限したアクセス、パスワードの自動ローテーション、厳格な承認フローといった仕組みを通じて外部関係者にも拡張することで、業務委託先やサプライチェーンに関連するリスクを大幅に軽減できます。

本ホワイトペーパーでは、企業がこれらのPAMの優先課題にどのような困難を抱えているのかを考察するとともに、Keeper Securityのプラットフォーム「KeeperPAM」が業界全体の中でどのような位置づけにあるのかを評価します。

ゼロトラストを前提とした設計

ゼロトラストとゼロ知識セキュリティ

特権アクセス管理において、ゼロトラストの原則を最初から組み込むことはもはや選択肢ではなく必須の要素です。「ゼロトラスト設計 (Zero Trust by Design) 」に基づくフレームワークでは、すべての特権アクセス要求を本質的に信頼されていないものとして扱い、継続的な検証、厳格なセグメンテーション、最小権限の徹底を求めます。静的で万能な認証情報の使用から、状況に応じた一時的なアクセストークンへの移行により、組織は攻撃対象領域を大幅に縮小し、侵害発生時の横展開リスクを最小限に抑えることができます。ゼロトラスト設計のもとでは、あらゆるアクセス判断が、ユーザーの身元、デバイスの状態、場所、時間帯、行動コンテキストといった複数の要素に基づいて行われます。ジャストインタイム型の権限付与によって、必要なタイミングと期間だけ特権アクセスが許可され、使用後には自動的に権限が剥奪されます。さらに、きめ細かなロールベースのアクセス制御により、過剰な権限付与が防止されます。多要素認証とセッションの継続的な監視は、認証情報の漏洩や内部脅威に対する強力な防御手段となります。

「[特権アクセス管理に関して優先したいのは]
ゼロトラストアーキテクチャとの統合と継続的な検証フレームワークです」
- - ITディレクター (従業員数500〜749人の企業、KeeperPAMユーザー)

Keeperは、製品設計においてゼロ知識アプローチを採用することで、このセキュリティモデルをさらに強化しています。暗号化および復号処理はすべてユーザーの端末上で行われ、Keeperのクラウドに送信されるのは暗号化されたデータ (暗号文) のみです。マスターパスワードやそこから導かれる鍵情報は、ユーザーが選択した端末から外部に送信されることはありません。そのため、Keeperのサーバーは復号されたデータや、データを保護する鍵にアクセスすることも、保存することもできません。仮にKeeperのインフラが侵害されたとしても、攻撃者が取得できるの

は意味を持たない文字列だけであり、真のエンドツーエンド暗号化による機密性が保証されます。

調査データは、このアプローチの効果を裏付けています。Keeper Securityのユーザーのうち60%が、自社のPAM実装を「ゼロ知識」かつ「ゼロトラスト設計」と捉えているのに対し、他のベンダーのユーザーではその割合はわずか34.9%にとどまっています。この差は、Keeperユーザーがより積極的なセキュリティ姿勢を取っていることを示しています。Keeperの導入企業は、継続的な検証の実施、共有アカウントの排除、自動化された特権ライフサイクル管理を重視する一方、他社ユーザーの多くは、より受動的でコンプライアンス重視の考え方にとどまっています。

ゼロトラスト型のPAMは、コンプライアンス対応と監査準備の迅速化にも貢献します。すべての特権セッションは、実行されたコマンド、画面の再生、セッションの継続時間を含めてエンドツーエンドで記録され、HIPAA、SOX、PCI DSSなどの要件に準拠した自動コンプライアンスエンジンに送られます。実際に、ゼロトラストをPAMアーキテクチャに組み込んでいる組織は、防御力を高めるだけでなく、運用の効率化、孤立アカウントに伴うコストの削減、そして侵害対応力の定量的な改善といった効果も得ています。

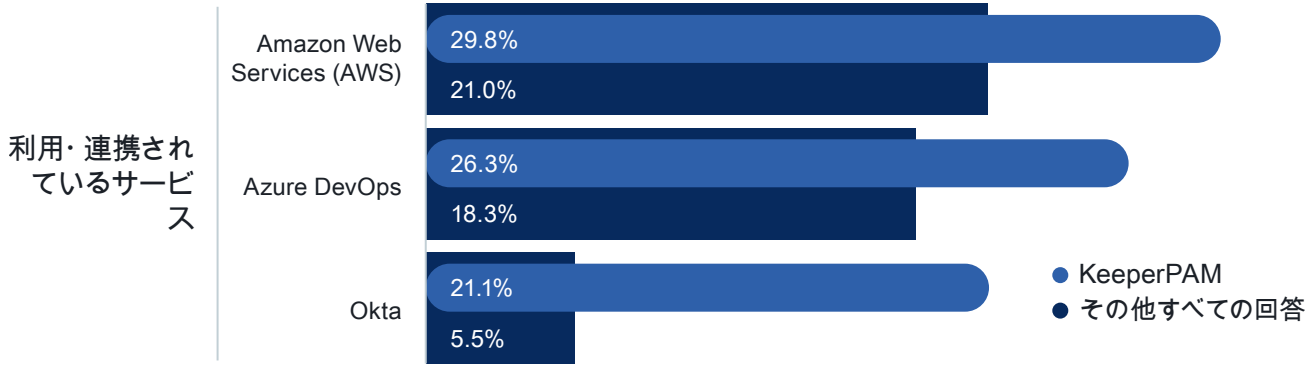
最終的に、Keeperのゼロ知識アプローチとゼロトラスト設計により、特権アクセスはリスク要因ではなく、制御され、検証可能なプロセスへと変わります。これにより、変化し続けるリスクにリアルタイムで対応しながら、重要なシステムのセキュリティ、コンプライアンス、レジリエンス (回復力) を確保することができます。

導入· 設定· 他システムとの連携のしやすさ

すべてを簡単にする魔法のボタンはないものの、それに迫るKeeper

PAMプロジェクトのROI (投資対効果) は、導入· 設定· 他システムとの連携のしやすさによって大きく左右されます。EMAの調査によると、Keeper Securityのユーザーの60%が初期導入を「非常に簡単だった」と評価しているのに対し、他のPAMプラットフォームではその割合はわずか22.1%にとどまっています。一方で、他社ソリューションのユーザーの10%は、導入を「やや難しい」または「非常に難しい」と感じており、KeeperPAMユーザーからは

このような不満は一切見られませんでした。レガシーのオンプレミス型PAMツールをクラウドに移行する際、39%の組織が依然として複雑さに直面していますが、Keeperのクラウドネイティブアーキテクチャはこの課題を回避しています。また、Keeper以外の導入事例では、11%がSIEM、チケット管理、DevOpsパイプラインなどとの統合に課題を抱えており、その多くは独自コネクタや手動スクリプトを必要としています。これに対し、KeeperPAMはモジュール型API、プラグアンドプレイのコネクタ、シームレスなクラウドオーケストレーションにより、価値実現までの時間を短縮し、運用上の負荷を最小限に抑えています。



他システムとの高い互換性

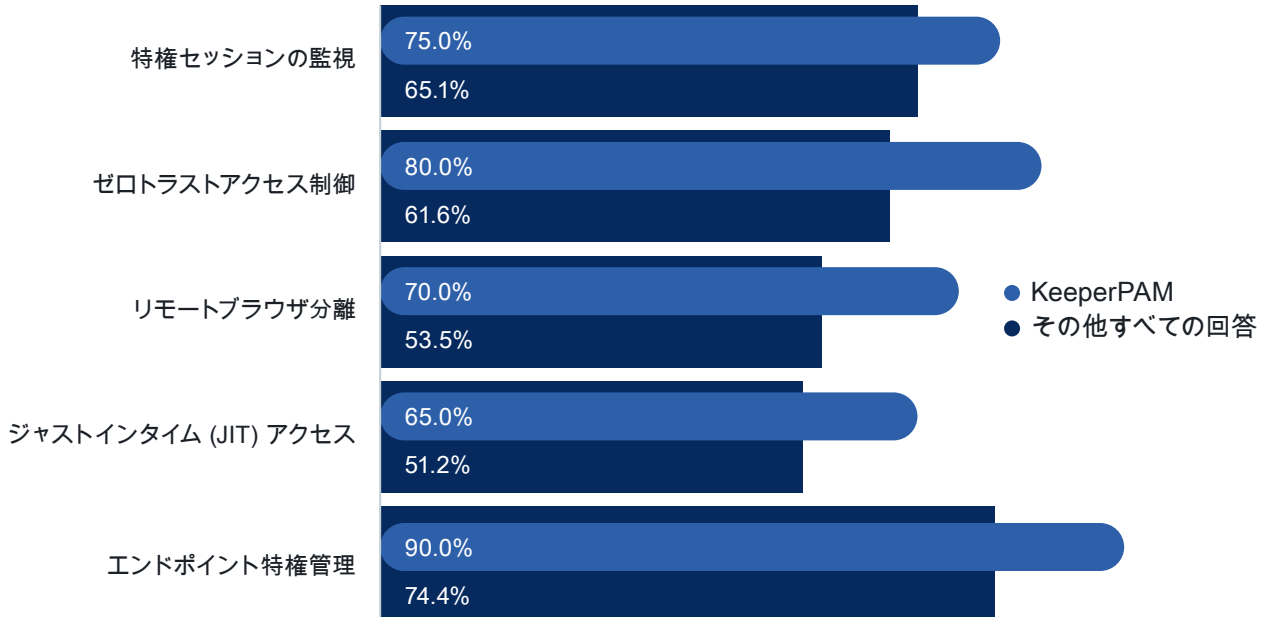
シームレスな統合は、あらゆるモダンなPAM戦略の中核であり、この点においてもKeeperは他社をリードしています。Keeperは、あらかじめ用意されたコネクタとAPIにより、主要なプラットフォームとの迅速かつ双方向の統合を可能にします。たとえば、Amazon Web ServicesでEC2インスタンスを立ち上げる場合や、Azure DevOpsでパイプラインを自動化する場合、あるいはOktaを使って認証を一元化する場合など、幅広い環境に柔軟に対応します。KeeperPAMのユーザーは、これらの統合機能を他のPAMソリューションのユーザーと比べてはるかに高い割合で活用しており、煩雑なカスタムスクリプトやコネクタの手動管理を不要にしています。さらに、CI/CDワークフロー、クラウドコンソール、IDプロバイダーに対して特権認証情報のインジェクションを直接組み込むことで、KeeperPAMは開発者の生産性を向上させ、すべてのレイヤーでシークレットの保護を確実にします。

少人数でも成果を最大化

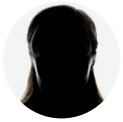
PAMの導入· 運用に必要な人員体制は、プラットフォームによって大きく異なります。Keeper Securityのユーザーで、導入· 設定· 統合に専任の人員が必要だと回答したのはわずか15%にとどまりました。これは、直感的なユーザーインターフェース、ガイド付きセットアップウィザード、充実したドキュメントといったKeeperの特長によるものです。一方で、他のPAMソリューションを使用している組織の39.5%は、環境の維持管理に1人以上の専任管理者が必要だと回答しています。こうしたチームは、複雑なオンプレミスアプライアンスの保守、カスタムスクリプトの作成、手動によるコネクタの更新といった作業に追われ、人員の増加や既存ITリソースの逼迫を招いています。Keeperのクラウドネイティブ設計とセルフサービス型ツール群により、高度な専門スキルへの依存は最小限に抑えられます。管理者は、最小限のカスタマイズで新しいシステムのオンボーディング、特権ポリシーの調整、SIEMやDevOpsパイプラインとの統合を行うことが可能です。結果として、必要な人員負担の軽減は、より迅速な導入と、持続可能かつコスト効率に優れた運用体制につながります。

パスワードとシークレット管理のその先へ

高度なPAM機能



現代のPAMには、単なる認証情報の保管を超えた機能が求められています。進化する脅威に対して、能動的に防御し、監視し、適応できる豊富な機能セットが不可欠です。KeeperPAMは、従来型ベンダーの多くが提供していない、あるいは大規模には実装できていない高度な機能を備えている点で際立っています。たとえば、特権セッションの監視は、リスクの高い操作におけるすべてのキー入力、コマンド、画面操作を記録・再生可能にする重要な機能です。Keeperのユーザーはこの機能を他のPAM利用者よりも高い頻度で活用しており、リアルタイムでの脅威検知やフォレンジック分析 (事後調査) に役立てています。



「PAMを活用することで、データの完全性と当社の信頼性が高まりました」
- 開発・エンジニアリング担当副社長 (従業員数1000~2499名の企業、KeeperPAMユーザー)

ゼロトラストネットワークアクセスは、最小権限の原則をパスワードのみにとどめず、すべてのアクセス要求に拡張するものです。Keeperは、デバイスの状態、位置情報、時間帯、ユーザーの行動パターンなどのコンテキストに基づくポリシーチェックを組み込むことで、認証済みのセッションであっても継続的に監視を行います。このように特権操作へのアクセスを細かく制御することで、静的かつ一律のオール・オア・ナッシング型、つまり全てかゼロかの一括許可モデルと比べ、潜在的なリスクの露出時間を大幅に短縮できます。

リモートブラウザ分離 (RBI) も、Keeperが他社を大きくリードしている領域の一つです。管理コンソールへのアクセスを隔離された安全なブラウザを通じてプロキシ化することで、外部委託業者やサードパーティによるエンドポイントへの直接アクセスを排除し、マルウェア感染や認証情報の窃取といったリスクを効果的に隔離できます。RBIをこれほどシームレスに統合しているPAMソリューションはほとんどなく、多くの製品では手動による代替手段に頼らざるを得ず、セキュリティとユーザー体験の両面において妥協を強いられています。

ジャストインタイム型の権限付与と、自動化された特権ライフサイクル管理は、Keeperの高度なツール群を構成する重要な要素です。一時的かつ時間制限付きで特権を付与することで、恒久的な高権限アカウントの蓄積を防ぎます。また、自動的な権限の剥奪や再認証キャンペーンによって、手動作業に頼ることなくコンプライアンス要件を確実に満たすことができます。さらに、エンドポイント特権管理 (EPM) により、ローカル管理者権限を削除しつつ、必要な操作に限定した権限をオンデマンドで付与することで、外部からの攻撃だけでなく内部不正にも有効な防御を実現します。

Keeperは、パスワードやシークレットの管理を超えて、PAMを能動的な防御プラットフォームへと進化させます。攻撃を予測し、あらゆる層でゼロトラストを徹底し、現代の複雑なIT環境に求められる高度な制御を実現します。

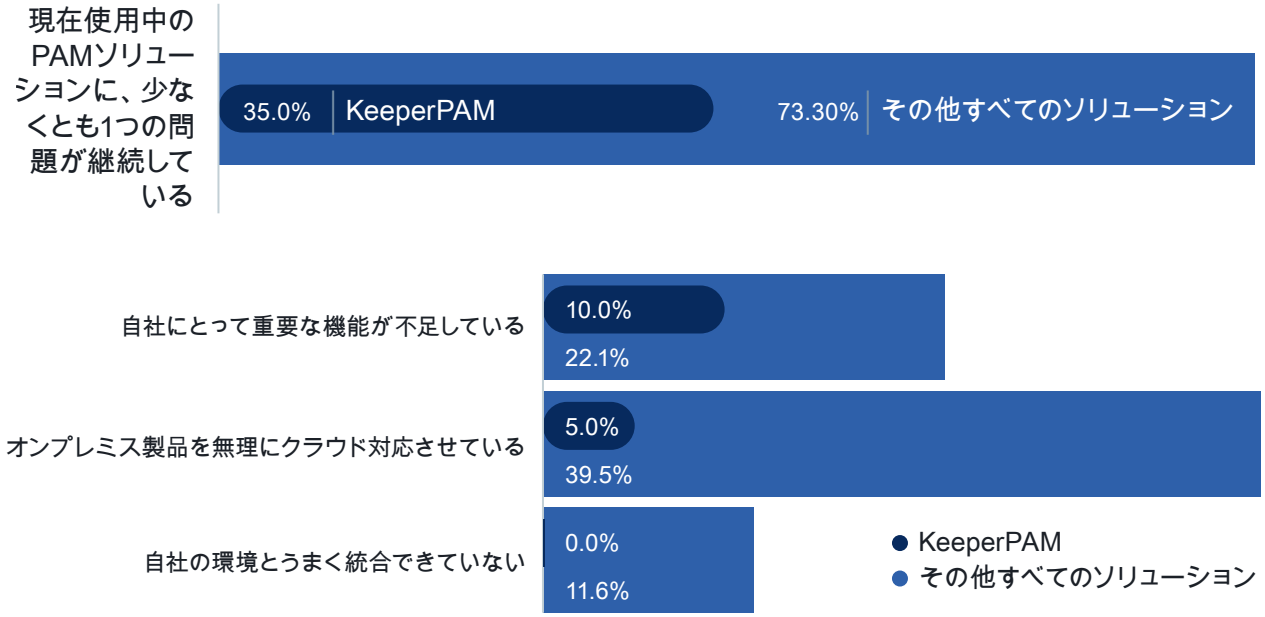
全体的な満足度

PAMは想定外の事態に対応できるか？

顧客満足度は、PAMソリューションの価値と継続性を測る最も重要な指標です。他のプラットフォームを使用している組織のうち5%が、すでに代替製品の導入を検討しているという事実は、そのソリューションにおける信頼性、使いやすさ、あるいはサポート体制に深刻な課題があることを示しています。一方、Keeper SecurityのユーザーでPAMの乗り換えを検討していると回答した組織はゼロでした。この結果は、Keeperが進化するセキュリティ要件と運用ニーズの両方に的確に応えていることを裏付けています。

さらに、Keeperのユーザーのうち75%が、自社のPAMソリューションに対して「非常に満足している」と回答しており、他ベンダー製品のユーザーにおける「非常に満足」の割合 (53.5%) を大きく上回っています。高い満足度は、迅速な導入、効果的なリスク低減、そして総所有コスト (TCO) の削減にも直結します。満足しているチームほど、より深い統合や高度な機能への投資を進める傾向があるためです。特権アクセスが常に攻撃対象となる今日において、ユーザーに選ばれ、支持されるプラットフォームを導入することは、もはや「あると便利」なものではなく、事業の継続に不可欠な要素となっています。

機能面と統合性が大きな障壁に



PAMが果たす役割は極めて重要であるにもかかわらず、多くの導入事例では継続的な課題に直面しています。Keeper以外のPAMソリューションを使用している組織の73%が、何らかの重大な課題を抱えていると回答しているのに対し、Keeperユーザーではその割合はわずか35%にとどまっています。代表的な課題としては、必要不可欠な機能が不足しておりサードパーティ製ツールの追加を余儀なくされること、既存インフラとの統合性の低さ、オンプレミス向けの製品をクラウド環境で無理に使おうとする際の煩雑な対応などが挙げられます。一方、KeeperPAMのユーザーはこれらの問題に悩まされることが圧倒的に少なく、それは同製品が包括的な機能セット、クラウドネイティブな設計、そして豊富な統合コネクタ群を備えていることによるものです。機能のギャップを最小限に抑え、ハイブリッド環境での導入を容易にすることで、Keeperは価値の早期実現を可能にし、トラブルシューティングや手間のかかる回避策に費やす時間を削減します。その結果、セキュリティチームはレガシー製品の限界に対処するのではなく、より前向きなリスク対策に注力できるようになります。

より良いソリューションで、より良い判断を

他のPAMでは、期待される成果が得られない

優先分野	Keeperユーザー	その他のPAMソリューション
認証	継続的かつゼロトラストベース	ロールベース+多要素認証 (MFA)
認証情報の管理	静的· 共有認証情報の排除	基本的なアクセス制御と監視
トレーニング	明確に優先事項として認識	あまり重視されていない
自動化	リスク軽減にフォーカス (プロセスはすでに効率的)	プロセス効率化にフォーカス
コンプライアンス	認証情報の悪用対策と監査対応を重視	最低限の規制準拠レベル

Keeper Securityは、コンプライアンス重視の「保守的な対応」から、積極的でセキュリティ優先の姿勢へと企業を導きます。KeeperPAMのユーザーは、ゼロ知識のボールティングエンジンを通じて静的で共有された不安全な認証情報を排除し、一時的かつ最小権限のシークレットを発行することで、従来のボルト中心のアプローチと比べて外部からの攻撃経路と内部不正のリスクを大幅に低減しています。また、デバイスの健全性チェック、位置情報、行動分析などを含む継続的な認証とゼロトラストのアクセス制御により、一度限りの多要素認証が完了した後のセッションでも監視を継続。認証情報を盗まれても気づかれずに悪用されるリスクをほぼゼロに抑えます。

Keeperは、リスク重視型の自動化機能によって、認証情報の検出· 登録から自動ローテーションや利用終了時の削除に至るまで、特権ライフサイクル全体を管理します。これにより、認証情報の氾濫や孤立アカウントの発生を防止します。他社ソリューションの多くが、承認フローやレポート作成の自動化にとどまっているのとは対照的です。さらに重要なのは、Keeperのユーザーが従業員教育と意識向上をセキュリティ管理の中核に据えている点です。技術だけでなく人の行動が、運用定着とリスクの回避において決定的に重要であることを、彼らは明確に認識しています。

「特権アカウントが常に監視されていると思うと、安心して眠れます」
– 開発·エンジニアリング担当副社長 (従業員2500〜4999名の企業、KeeperPAMユーザー)

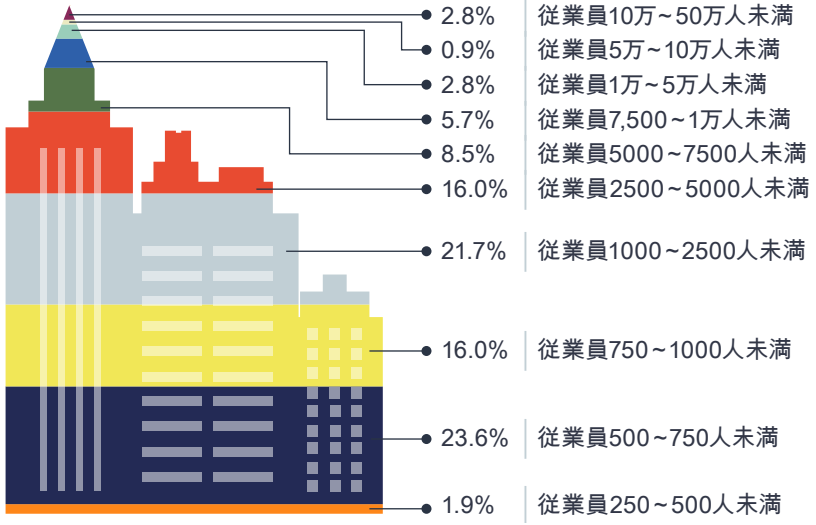
一方、他のPAMツールのユーザーは、ロールベースのアクセス制御、アクセス後の監査、運用効率のような従来型の管理手法を重視する傾向があり、機能の不足、統合の脆弱性、オンプレミス製品をクラウド対応させる複雑さといった課題に直面している「後追い型」の姿勢を反映しています。Keeperはクラウドネイティブなアーキテクチャと、プラグアンドプレイ可能な豊富なコネクタライブラリを備えており、これらの問題を根本から解消します。SIEMプラットフォームや、OktaなどのIDプロバイダ、AWSやAzure DevOpsのCI/CDパイプラインとの統合も迅速に実現します。さらに、Keeperには特権セッションの監視、リモートブラウザ分離、ジャストインタイム型の権限付与、エンドポイント特権管理といった高度な機能が標準搭載されており、導入時の摩擦や運用コスト、人員負荷を大幅に削減します。

これら次世代の機能をシームレスなユーザー体験と組み合わせることで、Keeperはセキュリティチームに脅威を先回りして察知し、継続的な保護を実現し、特権アクセス環境を真に強化する力を与えます。

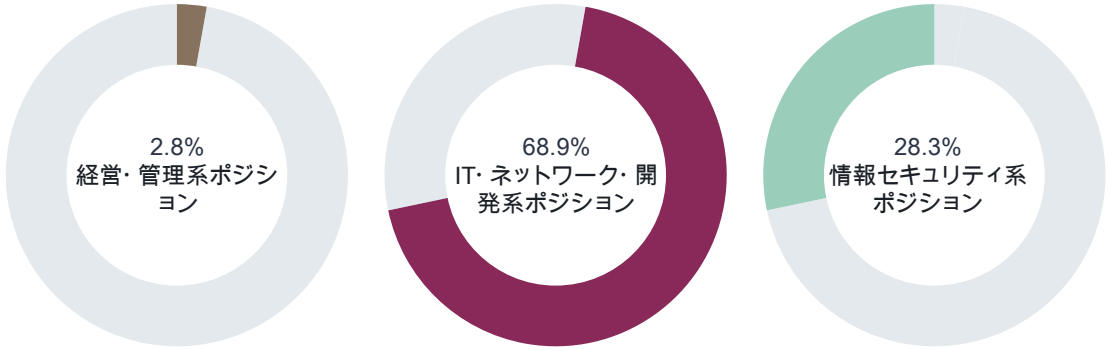
調査方法

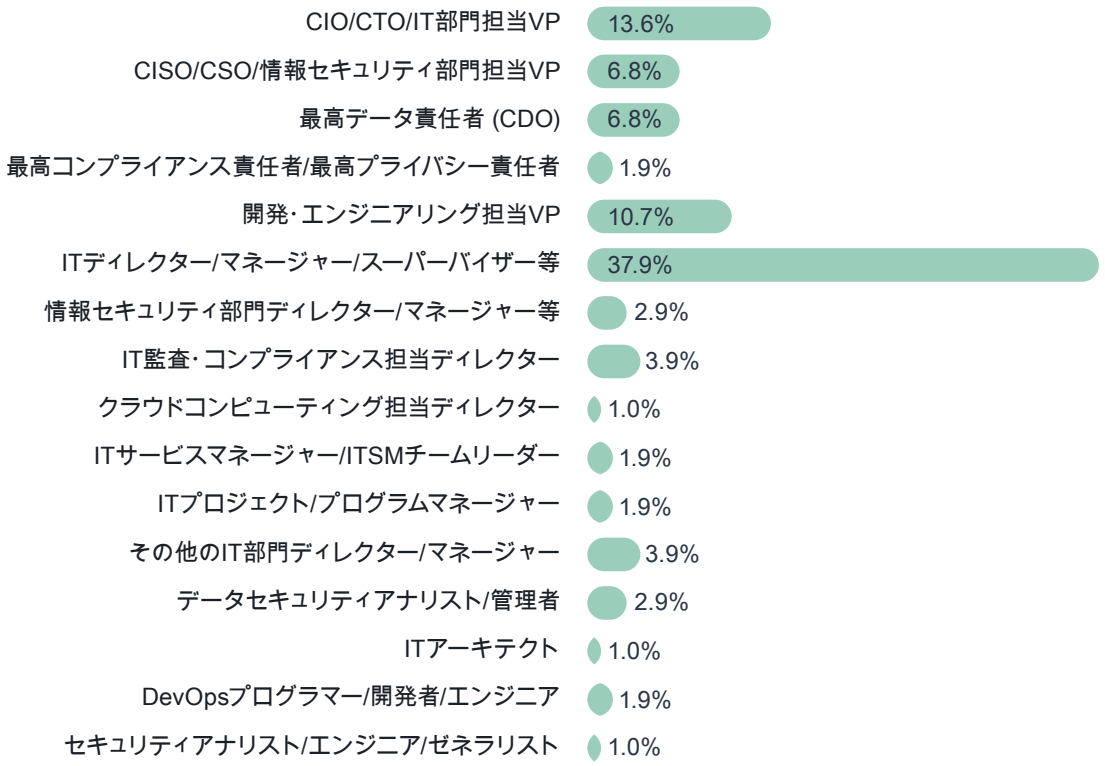
本ホワイトペーパーのデータは、2025年6月時点でBeyondTrust、CyberArk、Delinea、Devolutions、Keeper Security、ManageEngine、One Identity、StrongDMのいずれかを利用している106名の専門職を対象とした調査結果に基づいています。特権アクセス管理に関する企業の優先事項や課題について、アンケート回答および自由記述による意見を収集・分析したものです。

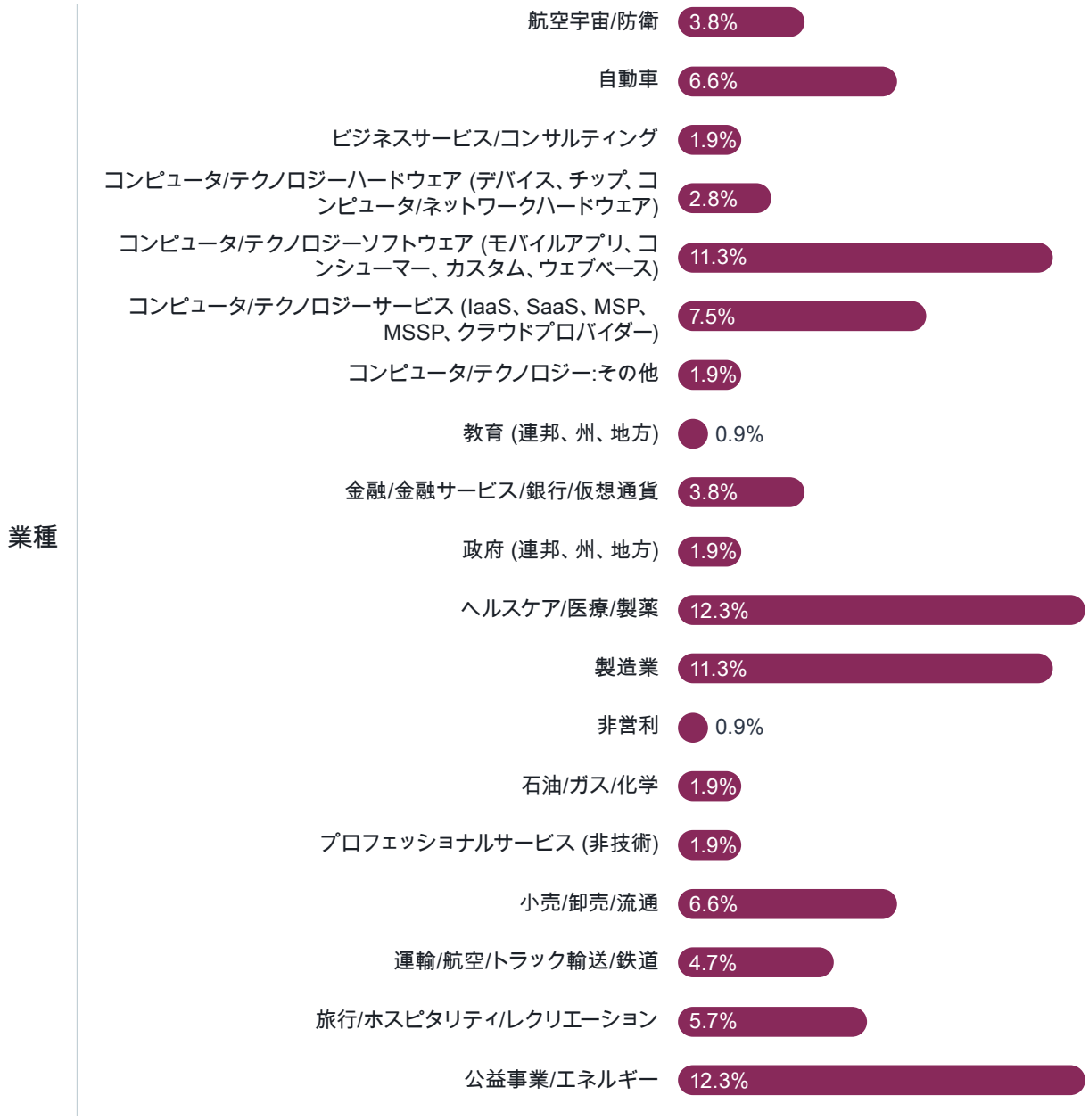
組織の規模



回答者の役職




CIO/CTO/IT部門担当VP
13.6%
CISO/CSO/情報セキュリティ部門担当VP
6.8%
最高データ責任者 (CDO)
6.8%
最高コンプライアンス責任者/最高プライバシー責任者
1.9%
開発・エンジニアリング担当VP
10.7%
ITディレクター/マネージャー/スーパーバイザー等
37.9%
情報セキュリティ部門ディレクター/マネージャー等
2.9%
IT監査・コンプライアンス担当ディレクター
3.9%
クラウドコンピューティング担当ディレクター
1.0%
ITサービスマネージャー/ITSMチームリーダー
1.9%
ITプロジェクト/プログラムマネージャー
1.9%
その他のIT部門ディレクター/マネージャー
3.9%
データセキュリティアナリスト/管理者
2.9%
ITアーキテクト
1.0%
DevOpsプログラマー/開発者/エンジニア
1.9%
セキュリティアナリスト/エンジニア/ゼネラリスト
1.0%


業種
航空宇宙/防衛 3.8%
自動車 6.6%
ビジネスサービス/コンサルティング 1.9%
コンピュータ/テクノロジーハードウェア (デバイス、チップ、コンピュータ/ネットワークハードウェア) 2.8%
コンピュータ/テクノロジーソフトウェア (モバイルアプリ、コンシューマー、カスタム、ウェブベース) 11.3%
コンピュータ/テクノロジーサービス (IaaS、SaaS、MSP、MSSP、クラウドプロバイダー) 7.5%
コンピュータ/テクノロジー:その他 1.9%
教育 (連邦、州、地方) 0.9%
金融/金融サービス/銀行/仮想通貨 3.8%
政府 (連邦、州、地方) 1.9%
ヘルスケア/医療/製薬 12.3%
製造業 11.3%
非営利 0.9%
石油/ガス/化学 1.9%
プロフェッショナルサービス (非技術) 1.9%
小売/卸売/流通 6.6%
運輸/航空/トラック輸送/鉄道 4.7%
旅行/ホスピタリティ/レクリエーション 5.7%
公益事業/エネルギー 12.3%

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT research and consulting firm dedicated to delivering actionable insights across the evolving technology landscape. Through independent research, market analysis, and vendor evaluations, we empower organizations to make well-informed technology decisions. Our team of analysts combines practical experience with a deep understanding of industry best practices and emerging vendor solutions to help clients achieve their strategic objectives. Learn more about EMA research, analysis, and consulting services at www.enterprisemanagement.com or follow EMA on X or LinkedIn.

This report, in whole or in part, may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. “EMA” and “Enterprise Management Associates” are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2025 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common law trademarks of Enterprise Management Associates, Inc.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 www.enterprisemanagement.com

4577.081325-JP