



Keeper Security インサイトレポート

クラウドベースの特権 アクセス管理



はじめに

デジタル変革と進化するサイバーセキュリティの脅威が席卷する時代において、組織では、センシティブな情報への特権アクセスを保護する重要性の認識が高まっています。特権アクセス管理 (PAM) ソリューションは、不正ネットワークアクセスからの保護と内部脅威の緩和に不可欠な要素として登場しました。

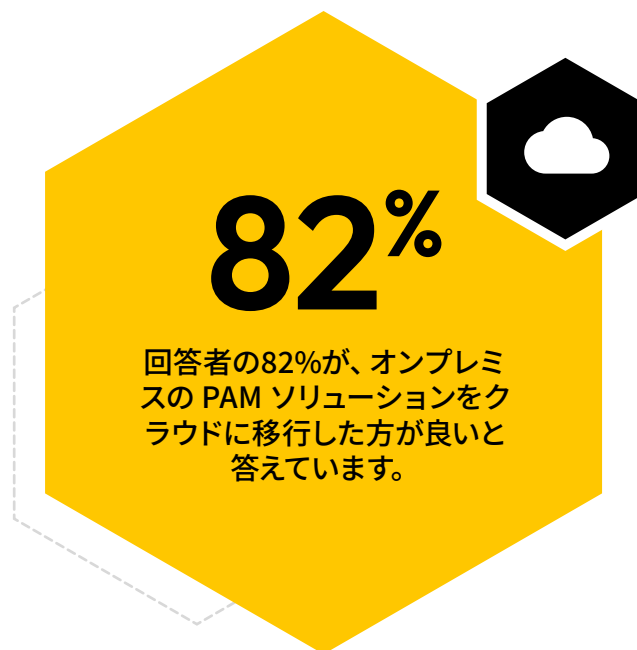
実際、2023 年初旬にリリースされた「Keeper Security インサイトレポート：特権アクセス管理の複雑性」によると、IT 大手企業の 91% が、PAM ソリューションにより特権ユーザーアクティビティを制御しやすくなったと述べています。しかし、同じレポートで、従来の PAM ソリューションでは不十分で、回答者の 87% が、導入および使用がしやすい PAM ソリューションの方がよいと答えています。

PAM の動向をさらに調べるため、Keeper は独立調査会社に依頼して、北米とヨーロッパの IT およびデータセキュリティ大手企業 400 社に PAM をクラウドに移行する戦略および計画について調査を行いました。「Keeper Security インサイトレポート：クラウドベースの特権アクセス管理」は、ユーザーが PAM ソリューションに何を求めているのか、従来のオンプレミスプラットフォームから離れることのメリットを明らかにしています。

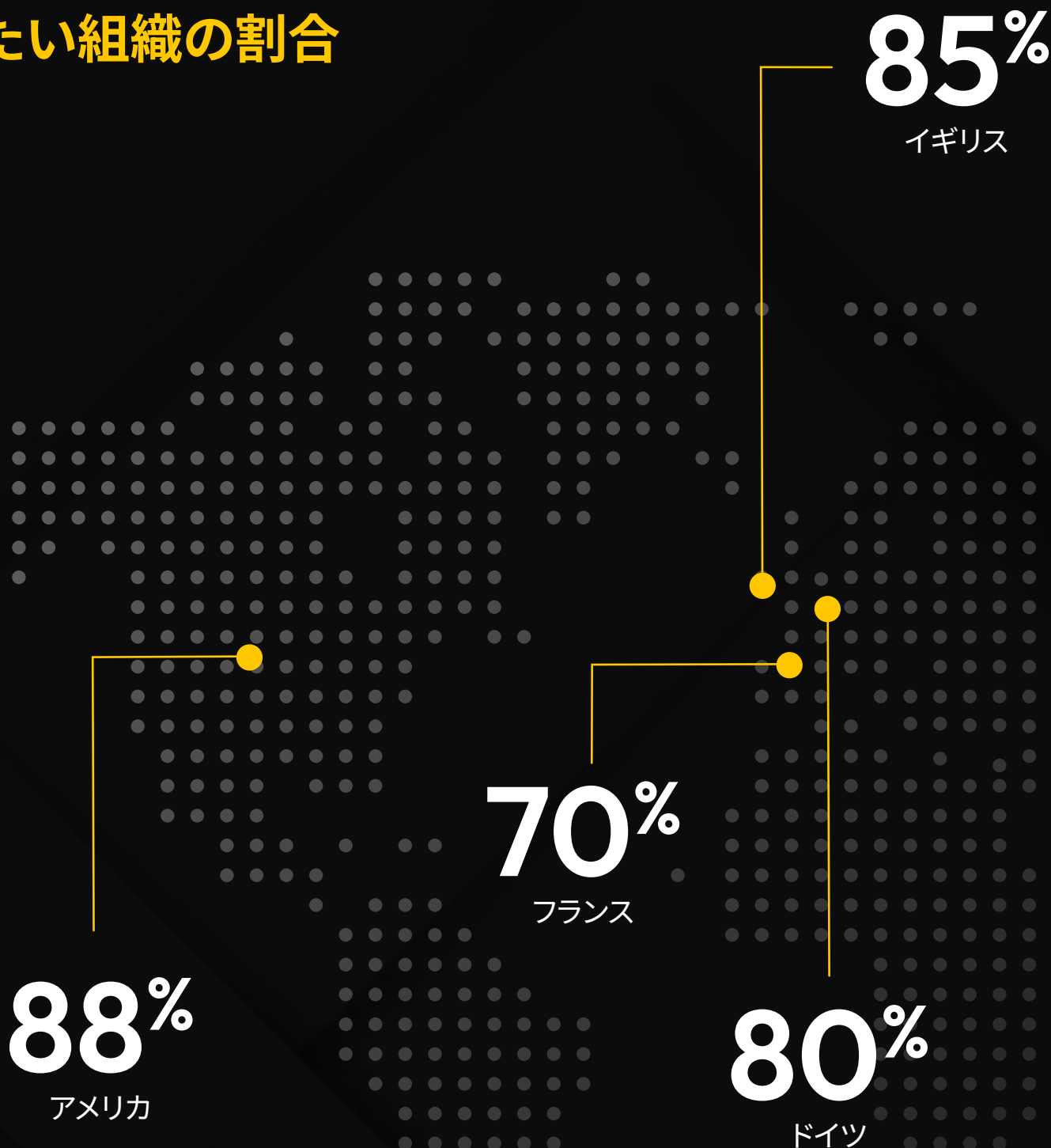
組織は圧倒的にクラウドのメリットを求めている

クラウドへの移行はもはや目標ではなく、柔軟性の増加、回復力の改善、セキュリティの向上を目指す組織にとって新たな常識となっています。ガートナーは、パブリッククラウドに対する世界のエンドユーザーの支出は、2022 年の 5,000 億ドル、2021 年の 4,210 億ドルから増加して、2023 年には 5,990 億ドルを越えるの見積もっています。従来の IT 支出は依然としてクラウドを上回っていますが、ガートナーは、クラウドの支出は増加し続け、2025 年までに従来の IT 支出を越えると予測しています。

次世代のクラウドベースセキュリティソリューションの可用性が増加するにつれて、特権アクセス管理のためにオフプレミスに移行する関心も高まっています。Keeper の調査によると、回答者の 82% が、オンプレミスの PAM ソリューションをクラウドに移行した方が良いと答えています。国別に見ると、アメリカが最も多く、アメリカの組織の 88% がクラウドベースの PAM の代替手段を求めていることがわかりました。



地域別 PAM をクラウドに移 行したい組織の割合



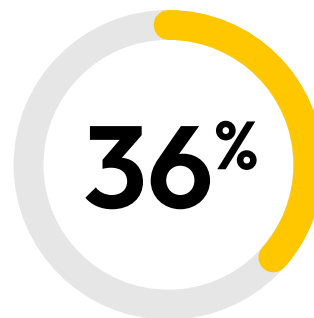
オンプレミスの費用により、 unnecessary 経済的負担が発生する

「企業は、従来のオンプレミス PAM ソリューションの複雑さと高いコストに悩まされてきました」Keeper Security の共同創設者であり最高経営責任者 (CTO) である Craig Lurey 氏は、このように述べています。「クラウドベースや導入が容易なソリューションに移行するにつれて、主要なユースケースのサイバーセキュリティ対応が向上します。」

“企業は、従来のオンプレミス PAM ソリューションの複雑さと高コストに悩まされてきました。導入が容易なクラウドベースのソリューションに移行することで、重要なユースケースをより適切にサイバーセキュリティでカバーできるようになります。”

Craig Lurey | Keeper Security CTO
& 共同創業者

Keeper の調査によると、85% の組織でオンプレミスの PAM ソリューションの管理と保守に専任スタッフが必要になっていることがわかりました。予算が削減される状況では、この支出を正当化できなくなるかもしれません。実際、IT 大手企業の 36% しか、現在の経済情勢においてオンプレミスの PAM ソリューションを持つ意味があると回答していません。組織が予算を削減するにつれて、費用の掛かる導入や、従来のオンプレミス製品に関連するスタッフを必要としない、より手頃な価格のプラットフォームが必要とされています。



IT 大手企業の 36% しか、現在の経済情勢においてオンプレミスの PAM ソリューションを持つ意味があると回答していません。

クラウドベースの PAM は、運用コストを最小限に抑え、物理的なインフラストラクチャやハードウェアへの大規模な先行投資をなくします。さらに、オンプレミスソリューションは、手動でのパッチの適用や更新という面倒で時間のかかるプロセスを行う必要があります。クラウドベースのソリューションはパッチの適用や更新が自動的に行われるため、社内の IT チームの負担が軽減され、時間の経過とともに大幅なコスト削減につながります。

クラウドソリューションは戦略的目標の達成に役立つ

オンプレミスの PAM ソリューションを使用している組織の半数以上 (60%) が、PAM がオンプレミスであるために目標達成が困難になっていると回答しています。組織がサイバーセキュリティ体制を強化する必要性に取り組む中で、PAM ソリューションのクラウドへの移行が戦略的に不可欠なものとして浮上しています。回答者が PAM ソリューションで求める主なメリットは、外部の脅威アクターによる特権認証情報の侵害からの保護、特権ユーザーアクセスの管理と監視 (それぞれ58%)、データ侵害の防止 (48%) です。

60%

が、PAM がオンプレミスであるために目標達成が困難になっていると回答しています。

PAM をクラウドに移行すると、高度な暗号化、多要素認証、継続的な監視により、セキュリティレベルが高くなります。クラウドサービスプロバイダーは、強化された環境を提供するためにインフラストラクチャの保護に多額の投資を行っていますので、組織は、保有するデータに対して最高レベルのセキュリティ、プライバシー、制御を実現するために、ゼロトラスト、ゼロ知識セキュリティアーキテクチャに基づいて構築されたソリューションを探すべきでしょう。人員が限られ、企業のむだが増える経済状況で、クラウドベースのソリューションは、最大のセキュリティリスクを軽減して企業のサイバーセキュリティ目標を達成する、費用対効果の高い機会を提供します。

PAM ソリューションに求める主なメリット

外部の脅威アクターによる特権認証情報の侵害からの保護



58%

特権ユーザーアクセスの管理と監視



58%

データ侵害の防止



48%

社内関係者による偶発的または意図的な特権アクセスの悪用からの保護



47%

特権ユーザーアクセスの更新と「特権クリープ」の防止



46%

可視性と意識の向上



43%

結論

拡大し続ける脅威環境に対処する中で、企業にとって堅牢な PAM ソリューションは不可欠です。オンプレミスソリューションは時代遅れで費用も非常に高額なため、クラウドベースの PAM ソリューションへの移行は、今日の組織の進化するセキュリティ需要や予算要件と戦略的に一致していることが現れています。特権アクセス管理がもはや贅沢ではなく、交渉の余地のない必須事項となった時代に、クラウドベースの PAM ソリューションを採用することで、組織は防御を強化できます。

