従来のPAMに潜む危険性

既存のセキュリティソリューションに潜在的なリスクがある理由

執筆者：クレイグ・ルーリー、CTO兼共同創業者 ｜ Keeper Security

サイバーセキュリティ業界で長年CTOを務めてきた立場から、多くの組織が従来の特権アクセス管理（PAM）ソリューションに依存し続けていることに強い懸念を抱いています。かつてはセキュリティの金字塔とされたこれらの仕組みも、クラウドネイティブが当たり前となった現代においては、もはや「危険な負債」となりつつあるのです。なぜ従来のPAMが、単に時代遅れで役に立たないだけでなく、組織そのものをリスクにさらす存在になっているのか ー その理由をお伝えします。

境界型セキュリティの過ち

従来のPAMソリューションが抱える根本的な問題は、それらの構造的な特徴にあります。これらのシステムは、ネットワークの境界が明確で、境界が強力であれば脅威を防ぐのに十分だった時代に合わせて構築されたものです。ハイブリッドクラウドやリモートワーク、相互接続されたシステムが混在する今日の環境において、このモデルは時代遅れであるだけではなく、重大な脅威となり得るのです。

> **「私たちは、セキュリティコントロールに制約された『信頼できる』ネットワークと『信頼できない』ネットワークという考えに固執しています。Keeperは、シークレットとパスワードがどこに存在していても、それらのライフサイクル全体にわたって保護することにより、境界のないネットワーク環境を円滑にします。」**

連邦政府機関が従来のPAMを導入する典型的な事例について考えてみましょう。基本的な機能を導入するだけでも、多数のファイアウォールポート(443、80、8080、22、23、1434)を解放する必要があります。それぞれのポートは、攻撃者に侵入される潜在的なエントリポイントとなり、組織を侵害するのに十分な穴が境界線に多数存在する状態、いわゆる「スイスチーズ・セキュリティ」が形成されてしまうことになるのです。

対照的に、Keeper のような最新のソリューションは、ゼロトラストモデルに基づいて機能しています。すべてのアクセス要求がデバイスレベルで認証および暗号化されるため、ファイアウォールを永続的に解放する必要性が省かれます。

極めて厄介な導入

夜も眠れないほど心配なのは、従来のソリューションに存在する構造上の弱点だけではありません。これらが実際に、いかに使用されているかという現実を案じているのです。私の経験では、組織が従来のPAMソリューションに搭載された機能のわずか20~30%しか活用していない例を常に目にしてきました。理由は簡単です。このようなシステムは、非常に複雑かつ煩雑になるため、完全に導入することは事実上不可能になるのです。システムを部分的に導入することで、誤った安心感が生じますが、これはとても危険です。組織は、PAMソリューションを導入したことで、保護されているものと思い込みの確信をします。しかし、気づかないうちに、シャドーITという悪夢を作り出しているのです。ユーザーは、本来のシステムが煩雑すぎると感じると、自己判断で解決策を編み出します。例えば、許可されていない場所にパスワードを保存したり、非公式なチャネルで認証情報を共有したり、あるいは、「単に仕事を完了させるために」監視されていない管理者アカウントを作成したりするのです。

クラウドネイティブとの断絶

従来のPAMソリューションが抱える非常に重大な欠点は、最新のクラウドネイティブでの運用をサポートできないことです。今日のインフラは、コンテナが瞬時にスピンアップする、あるいはスピンダウンしたり、インフラがハードウェアではなくコードによって定義されたりする動的な性質を持っています。しかし、従来のシステムは、このような性質に合わせて設計されたものではありません。

> **「従来のPAMソリューションには実装されていない機能があるため、攻撃対象領域が拡大し、企業のセキュリティが低下します。機能の肥大化はバグであり、特徴ではありません。」**

その影響は深刻です。DevOpsチームは、CI/CDパイプラインとの統合や動的なシークレットの注入の処理が不可能なPAMソリューションに直面し、多くの場合、セキュリティ対策を完全に無視してしまうことが多くなります。

最新のソリューションは、APIを重視した設計と開発ワークフローとのネイティブな統合を通じて、この問題に対処します。例えば、Keeperのシークレットマネージャーを導入すると、CI/CDパイプラインとシームレスに統合するゼロ知識暗号化が実現します。セキュリティや開発の作業量に支障をきたすことなく、シークレットの自動取得やローテーションが可能になります。

ゼロトラスト原則

今日の脅威を取り巻く状況において、ひとたびネットワーク境界内に入れば、「信頼」という言葉を前提にする余裕は、もはや私たちにはありません。しかし、従来のPAMソリューションは、依然としてこの時代遅れの原則に基づいて運用されているのです。ユーザーが従来のPAMシステムに一度認証されると、多くの場合、継続的に検証されることはほとんどなく、ユーザーは広範囲にアクセスを許可されてしまいます。

最新のセキュリティ対策では、すべてのアクセス要求が認証、認可、暗号化されるゼロトラストのアプローチが求められます。これには、記録レベルの暗号化、デバイスレベルのセキュリティ、そしてセキュリティ態勢の継続的な検証を実装することが必要となります。例えば、 **Keeperのアーキテクチャ** では、保存された各ボルト内の記録がAES-256ガロア/カウンターモード(GCM)を使用して、個別に暗号化されることが保証されます。暗号化と復号化がクラウドやセントラルサーバーで発生することはなく、デバイス上でローカルに行われます。

コンプライアンスにまつわる苦境

従来のPAMソリューションがもたらすコンプライアンスへの影響は、ますます深刻になってきています。最新の脅威に対処する規制要件が厳しくなるにつれて、従来のシステムの多くでは、必要とされる制御や可視性の確保が困難になっています。従来のシステムに搭載されたログ機能と監査機能では、重要なアクセスイベントを見逃すことが多いため、コンプライアンスの検証プロセスが手動になり、間違いが起こりやすくなります。

最新のPAMソリューションは、SIEMシステムと直接統合する包括的なログ機能およびレポート機能を備えており、この問題に対処します。例えば、Keeperの高度なレポートとアラート機能により、ゼロ知識暗号化を維持してデータのプライバシーが確保される一方で、すべてのアクセス試行と変更の詳細な監査証跡を把握できます。

KeeperはFedRAMP認証を取得しており、組織が役割に応じたアクセス制御 (RBAC) や二要素認証 (2FA)、FIP 140-3暗号化、HIPAAなどに対応しているので、監査とコンプライアンスを強化することが可能です。

ゼロ知識アーキテクチャの再構築

最新のPAMの中核となるのは **ゼロ知識アーキテクチャ** で、従来のシステムに存在する脆弱性を排除するものです。Keeperを導入すると、多層型の暗号化モデルが実装されることにより、このモデルがさらに強化されます。

ボルトの各記録は、クライアントのデバイスで生成されたGCMで固有の256ビットAESキーを使用して暗号化されます。記録レベルで暗号化することにより、たとえ1件の記録が侵害された場合でも、他の記録の安全は保たれます。暗号化と復号化のプロセスは、すべてユーザーのデバイス上で行われます。クラウドやKeeperのサーバーで行われることは決してありません。

> **「オンプレミスでPAMを導入することは、すでに安全ではないことがわかっているインフラのレイヤー、つまりネットワークやハイパーバイザ、オペレーティングシステムなどのすべてを信頼していることになります。」**

このモデルは、企業での導入でさらに強化されます。共有フォルダ内の記録キーは、256ビットAES共有フォルダキーでラップされ、記録とフォルダのキーは、データキーと呼ばれる別の256ビットAESキーで暗号化されます。これにより、複数の暗号化レイヤーが生成されます。それが侵害されない限りは、どの情報にもアクセスされることはないため、横移動や侵害の拡大を防ぐことができます。

KEEPER

認証の再構築

デバイスの検証

最新のクラウドベースのPAMソリューションでは、デバイスの認証と検証という重要なステップを統合してからユーザーにアクセスを許可します。このセキュリティ層の追加により、ユーザー列挙攻撃が軽減され、総当たり的なログイン試行が阻止されるため、許可されたデバイスのみが接続されるようになります。

ゼロ知識シングルサインオン(SSO)

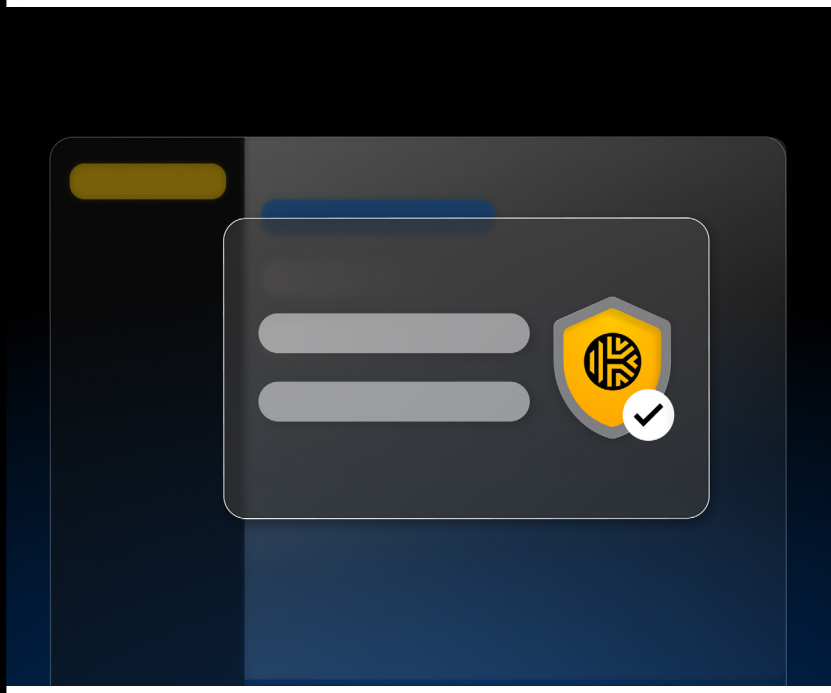
KeeperのPAMソリューションは、ゼロ知識のセキュリティを維持する一方で、エンタープライズIDプロバイダーとのシームレスな統合を可能にします。このことは、暗号化の秘密鍵の生成とローカルストレージなど、革新的な暗号化方法によって実現します。ブラウザベースの暗号鍵、ネイティブデバイスのiCloudキーチェーン、または安全なAndroidキーストアを活用する高度なPAMソリューションを使用することにより、機密性の高いユーザーデータを漏洩させることなく安全な認証が実現します。

多要素認証 (MFA)

クラウドネイティブのPAMプラットフォームでは、FIDO2 WebAuthnハードウェアキー、生体認証、時間ベースのワンタイムパスワード (TOTP) など、堅牢なMFA方式を使用することも可能です。着目すべき点は、通常は、デバイスを検証した後にMFAが実施されますが、これがパスワード入力前に実施されることです。このため、連続的かつ多層的な防御システムが構築され、不正アクセスを効果的に防ぎます。

リアルタイムで漏えい防止

最新のPAMソリューションには、漏えいしたパスワードを積極的に特定する漏洩検出メカニズムが組み込まれています。多くの場合、このようなシステムでは、自己完結型アーキテクチャと暗号プロセスを活用することでセキュリティの確保を実現します。例えば、ユーザー側のパスワードハッシュはHMAC_SHA512などのアルゴリズムを使用して処理されますが、サーバー側の検証はエクスポートできない鍵を備えたハードウェアセキュリティモジュール (HSM) を介して発生します。「ハッシュ・オブ・ハッシュ」アプローチを採用することで、実際のパスワードが完全に保護され、漏洩検出のプロセス中にパスワードが公開されることはありません。



DevOpsとの真の統合を実現

Keeperシークレットマネージャーを使用すると、セキュリティが損なわれることなく、開発チーム向けに適切なDevOps統合が可能になります。統合には以下が含まれます。

01

ゼロ知識APIアクセス

ユーザー側での暗号化方式 (GCMモードでの256ビットAES暗号化など) を使用し、アプリケーションがシークレットを安全に取得できるようにします。各シークレットは個別に暗号化され、すべての暗号化と復号化プロセスはデバイス上でローカルに発生するため、機密性の高い情報の保護と維持が達成されます。

02

鍵の安全な配布

ユーザーやアプリケーション間でシークレットを共有する必要がある場合、Keeperは**楕円曲線暗号**を使用して、ユーザーやアプリケーション間で鍵を安全に配布します。これにより、鍵交換の際でも機密情報が漏えいすることはなく、プロセス全体でゼロ知識のアプローチが維持されます。

03

シークレットの自動ローテーション

固有のゲートウェイがユーザーの環境にインストールされることにより、Keeperのインフラストラクチャとの安全なアウトバウンド接続が確立されます。これにより、内部のシステムを漏えいさせることなく、パスワードローテーションの自動化が可能になります。

セッションの安全性の再構築

リモートアクセス環境には、Keeperコネクションマネージャーを使用することで、安全なセッション管理が再構築されます。

01

ゼロトラスト接続

ゼロトラストモデルを使用することで、リモートセッションの安全性が確立されます。このモデルでは、接続はWebRTCなどの暗号プロトコルを通じて安全に確立され、対称鍵で保護されます。これらの鍵は安全に保管され、関連する記録と結び付けられます。

02

安全なトネリング

ポートフォワーディングやリモートアクセスでは、WebRTC接続などの暗号化トンネルを介してデータが安全に送信されます。セッションは、安全なゲートウェイで動的に生成されたAES-256暗号鍵で保護されるため、送信されたすべてのデータに対するエンドツーエンドの保護が保証されます。

03

セッション録画

すべてのセッション録画は、各セッションに対して生成された固有のAES-256暗号鍵によって保護されます。この鍵は、HKDFベースのAES-256リソース鍵でさらにラップされます。

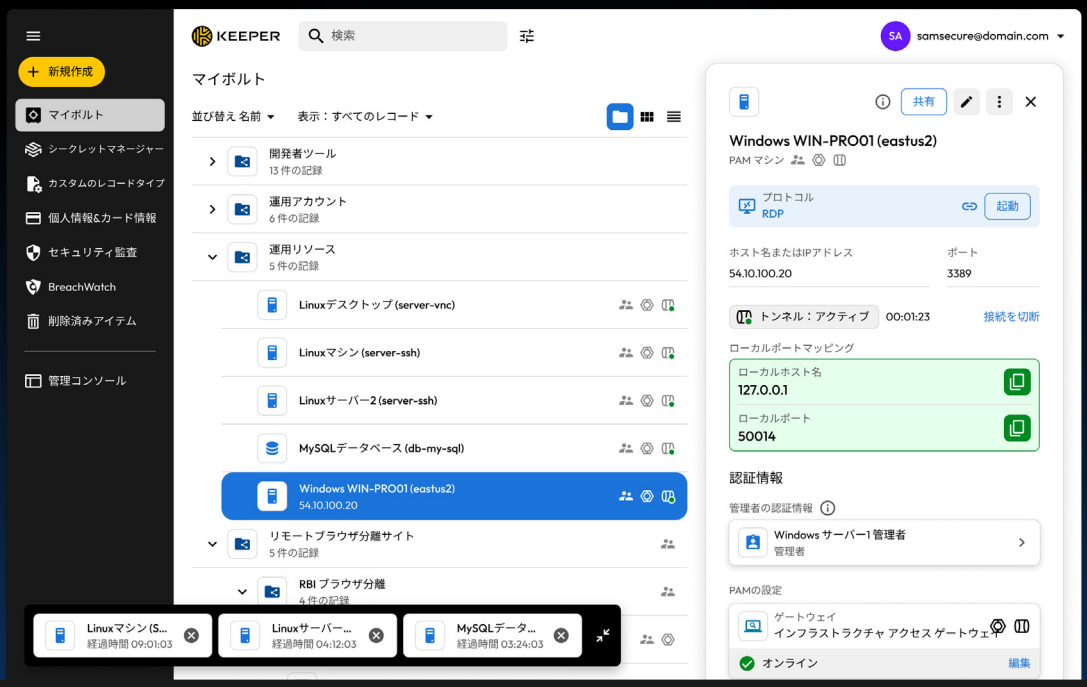
今後の展望

最新のPAMへの移行は、単に新しい技術を取り入れることだけが目的なのではありません。セキュリティに対して、根本的に異なるアプローチを採用することです。組織は、従来のPAMソリューションがセキュリティ資産には程遠いものであり、実は、重大な負担となる可能性があることを認識しなければなりません。

幸いなことに、Keeperのようなソリューションを導入することで、クラウドベースのPAMを活用し、簡単な操作で強固なセキュリティを実現できることが証明されます。ゼロ知識アーキテクチャ、デバイスレベルの暗号化、最新のワークフローとのネイティブ統合を組み合わせることにより、組織は、セキュリティやユーザーエクスペリエンスを損なうことなく、真の特権アクセス管理を実現できます。

現代の脅威の状況において、適切なPAMソリューションを導入することは、単に権限管理を目的としているのではありません。セキュリティの基盤は、ビジネスの進捗を妨げることなく、ビジネスの敏捷性を確保するためのものなのです。組織を守るための十分な技術は存在します。問題は、従来のソリューションのために組織が壊滅状態となる前に、新しいシステムに移行できるかどうかです。

今すぐデモをご予約 いただき、お使いの環境をKeeperPAMが保護する仕組みをご確認ください。



執筆者：クレイグ・ルーリー、CTO兼共同創業者

Keeper Security の最高技術責任者（CTO）および共同創業者。アイオワ州立大学で電気工学の学士号を取得後、モトローラ社でソフトウェア・エンジニアとしてキャリアを開始し、携帯電話基地局のファームウェアを開発。現在は Keeperにおけるソフトウェア開発およびテクノロジーインフラのチームを統括。クレイグと共同創業者のダレンは、20年以上にわたり複数の成功したビジネスを共に手がけてきたパートナー。世界中のニュース出版物や番組で定期的に専門家として出演し、情報技術に関する専門知識や見識を伝えている