Keeper SSO Connect®でパスワード管理とゼロ知識セキュリティをシングルサインオン（SSO）ソリューションに統合

概要

従業員が業務に必要なパスワードを管理できない場合、生産性が損なわれ、費用が無駄になり、企業全体のIDとアクセスの管理（IAM）、そしてセキュリティを複雑にしてしまいます。

シングルサインオン（SSO）はこうした問題の一部を解決しますが、組織にはロジスティクス上およびセキュリティ上の課題が残ります。Keeper SSO Connectは、高度なパスワード管理、パスワード共有、セキュリティ機能を提供する統合型のゼロ知識パスワード暗号化システムであり、SSOの機能を拡張することで、こうした課題を解決することができます。

Keeper SSO Connectは、統合型のゼロ知識パスワード暗号化システムであり、SSOの機能を拡張することで、IAMやセキュリティの課題を解決します。

企業がSSOを導入するメリット

パスワード疲れの解消

従業員は、いくつもの異なるパスワードを管理するのではなく、たった1つのパスワードを記憶するだけです。

生産性の向上

従業員は、平均して毎年11時間近くをパスワードの入力とリセットに費やしています。リソースへのアクセスを簡素化することで、SSOはユーザーの生産性を維持することができます。

ヘルプデスク業務の最小化

ガートナー社では、ヘルプデスクへのサポートコールの約50%がパスワードのリセットに関するもので、1つのパスワードのリセットにかかる平均人件費は70ドルであると推定しています。パスワードのリセットに関する問い合わせを大幅に低減もしくは排除できれば、費用を削減できる上、ヘルプデスクの従業員をより複雑なサポート業務に集中させることができます。

IDとアクセス管理（IAM）をサポート

SSOは、エンタープライズIAMスタックにおける一般的なコンポーネントです。SSOを利用することで、管理者は強力な認証やアクセス制御を簡単に構成でき、IAMの導入を簡素化、迅速化できます。また、SSOが適用された範囲全体にわたってユーザーのアクセス状況を可視化することができます。

ゼロトラスト環境への対応

IAMの導入を簡素化、迅速化することで、SSOはすべてのユーザーに強力な認証を求めるゼロトラスト環境に対応することができます。

コンプライアンスレポートの作成をサポート

SSOシステムは、多くのコンプライアンスフレームワークで要求されるユーザーのサインオンデータを含めた、監査やレポート作成機能を拡張する簡単な方法です。

SSOの欠点

SSOは多くの利点を備えていますが、万能ではありません。SSOソリューションにはセキュリティと機能に大きな課題が残されています。皮肉なことに、これらの課題には、企業がSSOで解決しようとしている問題、つまりパスワード管理とセキュリティが含まれています。

単一障害点

SSOプラットフォームにおける最も大きな欠点の1つは、単一障害点となりうることです。ユーザーがパスワードを忘れた場合、1つではなく複数のサイトやアプリからロックアウトされてしまいます。逆に、ユーザーのパスワードが侵害された場合、サイバー犯罪者は1つだけでなく複数のシステムにアクセスできるのです。

互換性のないアプリとサービス

一般的な組織では、数百から数千のクラウドアプリを使用しています。すべての従業員が使用する業務効率化アプリケーションに加えて、特定の部署やチームでは業務に特化した独自のアプリケーションも使用しています。これらのアプリケーションにはSSOをサポートしていないレガシーな基幹業務（LOB）アプリが含まれている場合が多く、これらは重要なデータが含まれる、もしくは重要な業務機能を実行しているため、リファクタリングや置き換えが不可能です。

ユーザーのパスワード利用状況を可視化および制御できない

SSOアカウント以外のパスワード管理は自己裁量に任されているため、個人ユーザーやチームは、テキストファイルやスプレッドシートに保存する、付箋に書き留めるなど、各自の方法で対処しています。こうした「自作」のソリューションは効率的でも安全でもありません。また、脆弱なパスワードの使用、アカウント間でのパスワードの再利用、許可なくパスワードを共有する、二要素認証（2FA）、多要素認証（MFA）を有効にしないなど、不適切なパスワード管理が行われている場合もあります。

その結果、SSOの導入に投資したにもかかわらず、管理者がデータ環境におけるこれらの場面でパスワードの使用を可視化および制御できないため、組織はパスワード関連のデータ漏えいに対する脆弱性を改善できないままとなります。管理者は、SSO以外のアカウントに強力かつ一意のパスワードを使用させる、二要素認証（2FA）をサポートするすべてのアカウントで二要素認証（2FA）を有効にするなどのセキュリティポリシーを適用することはできません。

KEEPER SSO CONNECTとは...

導入や拡張が簡単

パスワードレス戦略に対応

数千のユーザーとエンドポイントに拡張可能

あらゆるデータ環境であらゆるIdPとシームレスに統合

Keeper SSO Connectは、オンプレミスまたはお客様管理型のコンポーネントを用意せずに使用できる、フルマネージド型のSaaSソリューションです。Keeper SSO Connectは、ゼロ知識アーキテクチャを維持しながら、ホスティングと管理はKeeper Securityが行います。

Keeperはすべての
主要IDプロバイダと統合

- Azure ADとOffice 365
- Active Directoryフェデレーションサービス
- Microsoft 365
- Google Workspace
- Okta
- OneLogin
- Duo
- Centrify
- JumpCloud
- Ping
- F5 BIG-IP APM
- その他多数!

2ステップのセットアップで迅速な導入を実現

Keeper SSO Connectは、オンプレミスのサービスやお客様のクラウドにホストされたサービスが不要で、追加のソフトウェアや機器も必要ありません。セットアップは簡単な2ステップで完了します。

- **ステップ1:** IdP内でKeeperアプリケーションを有効化する。
- **ステップ2:** Keeper管理コンソール内でSSO Connectを設定する。

合理化されたログインフローが効率向上とセキュリティ強化を実現

Keeper SSO Connectの合理化されたログインフローは、エンドユーザーのログイン手順を簡素化し、効率を高めます。KeeperがエンドユーザーのEメールドメインをSSO対応の企業と認識すると、ユーザーは自動的にIDプロバイダにルーティングされます。SCIMの自動プロビジョニングまたはジャストインタイム（JIT）プロビジョニングと組み合わせた場合、新しいユーザーのオンボーディングが素早く行われ、安全性も高まります。

Keeper + SSO = 100%カバー

ユースケース	Keeper Enterprise	SSO IDプロバイダ
パスワードベースのアプリ	✓	✓
パスワードとシークレットの共有	✓	✓
暗号化されたデータストレージ	✓	✓
ソーシャルメディアサイト	✓	✓
ネイティブアプリ	✓	✓
オフラインアクセス	✓	✓
SSHキーとSSL証明書	✓	✓
API認証情報	✓	✓
暗号化されたプライベートファイル	✓	✓
ゼロ知識暗号化	✓	✓
SAMLベースのアプリ	✓ Keeper SSO Connect経由	✓

ユーザーのログイン認証情報に誰もアクセスできない独自のセキュリティモデル

Keeper SSO Connectは、クライアント側で生成された楕円曲線暗号（ECC）の秘密鍵と公開鍵のペアを利用して、SSO IDプロバイダとシームレスで安全に統合します。Keeperは、デバイスレベルのECCキーを使用してユーザーのボルトを保護することで、ゼロ知識を維持したまま完全なクラウドベースのSSO統合を提供します。転送中および保管中のデータはすべて暗号化されており、たとえKeeper Securityの従業員であっても、外部の第三者が閲覧することはできません。

安全で合理化されたデバイス承認がゼロトラストセキュリティをサポート

デバイス認証は、ゼロトラストセキュリティモデルの核となるコンポーネントです。Keeper SSO Connectを使用すると、承認されたすべてのユーザーデバイスはローカルのプライベートECCキーを持ちます。Keeperの高度なゼロ知識暗号化によって、キーの交換はユーザーのデバイス間またはKeeper管理者の承認を通じて安全に行われます。また、デバイスの承認を自動化することもできます。

お客様は、プッシュベースのデバイス承認を次の2つの方法で設定することができます。

「デバイスの承認」権限を持つ管理者による承認。

自動承認方法を経由して承認（Keeper管理コンソール、Keeper Commander CLI、Azureの機能）。

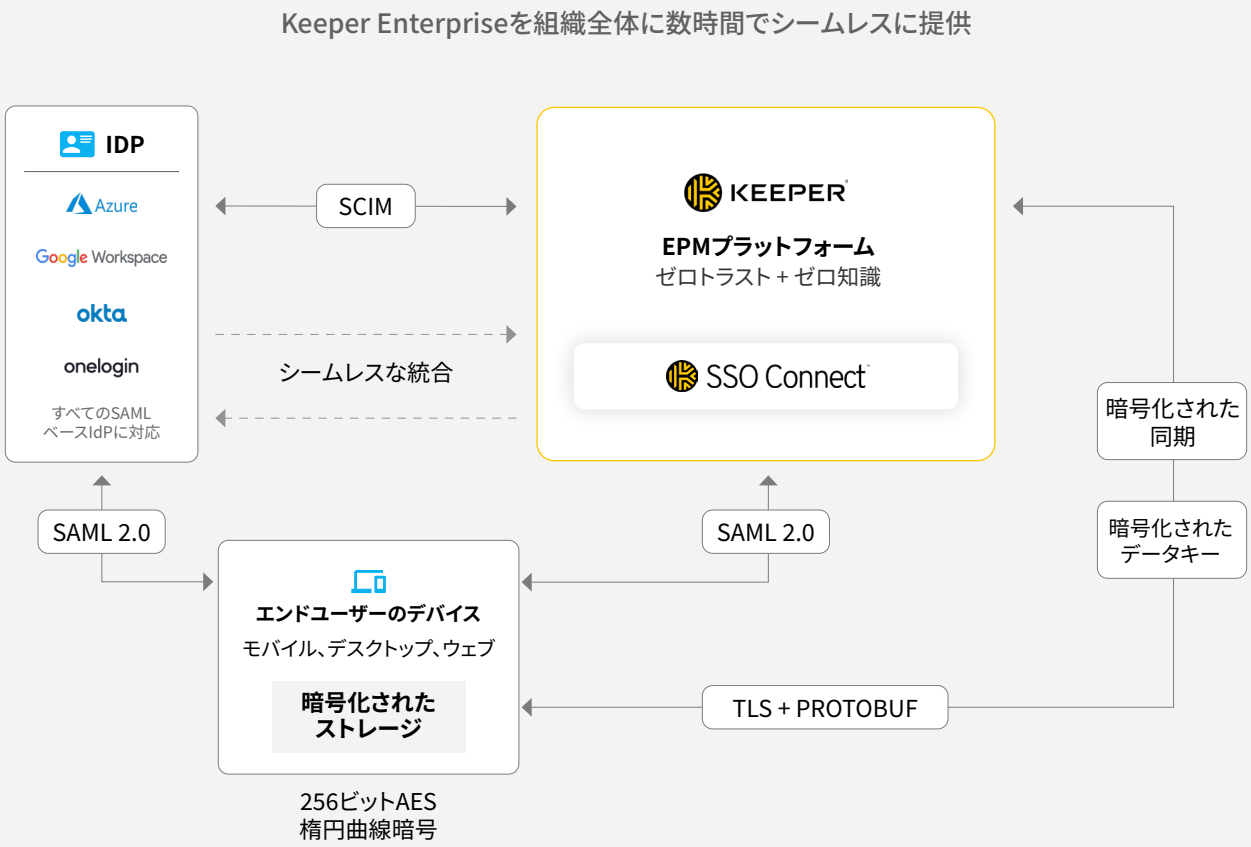
企業全体にわたるエンドツーエンドのパスワード管理

Keeper SSO Connectは、高い評価を受けているKeeperパスワード管理プラットフォームのすべての機能を管理者に提供します。

- 専任のサポートスペシャリストによる、パーソナライズされたオンボーディングと、24時間365日のサポートおよびトレーニング
- RBAC、二要素認証（2FA）、監査、イベントレポートの作成、複数のコンプライアンス基準（HIPAA、DPA、FINRA、GDPRなど）への対応
- パスワードの最大／最小文字数や特殊文字の包含／除外など、パスワードの複雑さに関する要件の指定
- チームで使用する安全な共有フォルダ、サブフォルダ、パスワードの設定
- SSOが利用できない場合にオフラインでのボルトアクセスを有効化
- SCIMを介してボルトを動的に設定
- ダークウェブやクレデンシャルスタッフィング攻撃からの保護

エンドユーザーは、ワークフローの最適化やパスワードセキュリティの向上を支援する以下の機能を利用できます。

- あらゆるOSで動作している、あらゆるデバイスからアクセスできるセキュアなデジタルボルト
- パスワード自動生成機能
- あらゆるウェブサイトやアプリで機能するログイン認証情報の自動入力機能
- デバイスの制限なく機密ファイル、ドキュメント、写真、動画を格納できる安全なストレージ



結論

SSOプラットフォームは、ユーザーパスワードに関連するセキュリティと機能の課題を解決できるよう設計されていますが、組織がパスワード管理ソリューションにも投資しなければ、セキュリティと機能には大きな課題が残ってしまいます。Keeper SSO Connectは、高い評価を受けているKeeperパスワード管理プラットフォームを介し、包括的なパスワード管理と暗号化によってSSOの機能を拡張することで、これらの課題を解決します。

Keeper SSO Connectはあらゆる技術スタックと連携し、広く使われているIdPプラットフォームとシームレスに統合します。導入は簡単で時間もかかりません。このプラットフォームは、エンドユーザーの使いやすさを向上し、管理者にパスワード利用の可視性と制御を提供し、従業員の作業効率を高め、パスワードに関連したヘルプデスクへの問い合わせを排除するとともに、パスワードに関連したデータ漏えいの防止に寄与します。