

ケーススタディ

グローバルIT企業、Keeperでセキュリティとコンプライアンスを強化



背景

この組織はテクノロジーサービス企業であり、金融、通信、メディア、小売、ヘルスケアなど、さまざまな業界に顧客を抱えています。

業種

テクノロジーサービス

従業員

11,000人以上

ソリューション

企業向けパスワードマネージャー

- プラチナサポート



課題

この急成長を遂げている組織は、世界中に従業員を抱えており、パスワードセキュリティを強化したいと強く考えていました。従業員はさまざまなパスワード管理ソリューションを使用していたため、断片化や一貫性のない状態が発生しており、認証管理には可視化が欠けていました。

また、IT管理者は、セキュリティのベストプラクティスを部門を超えて共有したいと考えていました。組織がISOやその他のサイバーセキュリティ標準を強化する中、一元化されたパスワード管理ソリューションが欠如していることで、コンプライアンスにギャップが生まれ管理が非効率になっていました。

主な課題は次のとおりです。

限定的な可視性とアクセス制御: 従業員は、[ブラウザベースのパスワードマネージャー](#) など、各自がさまざまなツールを使用していたため、セキュリティを強化しデータ衛生を維持するのが困難でした。

コンプライアンス要件とセキュリティリスク: ISOや各種サイバーセキュリティ認証の基準に継続的に適合し、改善を図るためには、エンタープライズグレードの体系的なソリューションが必要でした。組織は、認証情報の管理状況をさらに可視化し、データセキュリティのベストプラクティスを確実に適用できる、シームレスな仕組みを求めています。

「パスワード管理を、当社のサイバーセキュリティチームが確認して管理することができる単一のセキュアソリューションに統合したいと考えていました。」

- プロジェクトデリバリー管理責任者

Keeperのソリューション

同組織は、Keeper Securityを選択する前に、複数のパスワード管理ソリューションを検討・評価しました。Keeperは、エンタープライズクラスのパスワード保護、安全な認証情報の共有、クラス最高水準のセキュリティを提供しており、最も安全で機能が豊富なオプションの1つとして際立っていました。Keeperのソリューションは、以下を含む多くのメリットを提供します。

一元化されたパスワード管理 - Keeperは、組織のパスワードを保存および管理することができる安全な単一プラットフォームを提供しました。これにより、すべての認証情報が、Keeperの[ゼロトラストおよびゼロ知識](#)アーキテクチャによって確実に保護されるようになりました。

ユーザーの導入とトレーニング - Keeperは、あらゆる規模の組織に最適な優れたパスワードマネージャーとして認知されており、使いやすさと迅速な導入を実現するよう設計されています。Keeperの広範な情報をカバーする[ドキュメントポータル](#)では、詳細な手順やシステムのベストプラクティスを提供しており、管理者は導入時に大いに活用することができます。エンドユーザーに向けた詳細な[製品ガイド](#)や[トレーニング動画](#)は、エンドユーザーの高い導入率につながります。

「当社は、エンドユーザー向けトレーニングと管理者向けトレーニングの両方をチームに提供しました。非常に直感的に操作できるインターフェースで、実装もたいへんスムーズに進みました。」

- プロジェクトデリバリー管理責任者

高度なセキュリティ機能 - 多要素認証 (MFA) とエンドツーエンドの暗号化などが含まれるKeeperの堅牢なセキュリティ対策が、機密性の高い内部でのやり取りやデータを確実に保護します。チーム間で認証情報を安全かつシームレスに共有できるようになりました。メンバーがセンシティブデータを公開することがないため、保護レイヤーが強化されます。

優れた費用対効果 - Keeperでは、組織の規模や職種にかかわらず、組織のニーズに適合し、ニーズに合わせて拡張できる費用対効果の高いプランを提供しています。Keeperが提供する透明性の高い価格設定モデルと、[G2](#)のエンタープライズカスタマーサポート部門で第1位にランク付けされた世界レベルのカスタマーサポートの組み合わせにより、組織は投資費用を最大限に活かすことができます。

クラス最高水準のセキュリティ - Keeperのゼロトラストおよびゼロ知識セキュリティアーキテクチャは、情報の保護とデータ漏洩のリスクの軽減において、比類のないアーキテクチャです。Keeperでは、デバイスレベルの楕円曲線暗号 (ECC) と[多層暗号化](#) (ボルト、フォルダ、およびレコードレベル)、多要素認証と生体認証、さらにFIPS 140-3で検証済みのAES 256ビット暗号化およびPBKDF2を組み合わせています。Keeperは [SOC 2](#)と[ISO 27001](#)に[準拠](#)しており、業界で最も長期に渡るコンプライアンスを維持しています。また、FedRAMPおよびStateRAMPの認証も受けています。

組織への影響

11,000人以上の従業員を世界中に擁する同組織は、全社にKeeperを導入することで、パスワードとパスキーセキュリティを一元管理できるようになりました。これにより、ITチームは強力なパスワードポリシーを施行し、認証情報の衛生状態を監視し、安全なアクセス管理を促進できるようになりました。主な影響は次のとおりです。

セキュリティとコンプライアンスの強化 - Keeperにより、組織のセキュリティ体制が改善され、ISO認証要件など、多くの業界標準認証へのコンプライアンスを確保することができるようになりました。IT管理者は、Keeperの一元化されたダッシュボードを活用して認証情報のセキュリティをリアルタイムで監視できます。

オンボーディングとオフボーディングの合理化 - Keeperを導入することで、オンボーディングまたはオフボーディングのプロセス中も、アカウント認証情報へのアクセスをシームレスにプロビジョニングまたは廃止できます。さらに、Keeperを組織全体に展開することで、コラボレーションと運用の効率性が向上しました。

ユーザーの導入とシームレスなコラボレーション - Keeperの直感的に操作できるインターフェースとその使いやすさにより、特に技術担当でない従業員の間で導入率が高まっています。Keeperは、すべての[ビジネスユーザーに無料のファミリープラン](#)を提供しており、これによりさらに導入が促進されています。ユーザーフレンドリーなブラウザ拡張機能により、パスワードとパスキーの管理が簡素化され、部門間のコラボレーションが向上し、共有レコードにアクセス時のストレスが軽減されます。

「チームは、Keeperではファミリープランも無料で利用できる点を特に気に入っていました。この追加特典により、ユーザーの採用率がさらに促進されました。」

- プロジェクトデリバリー管理責任者

セキュリティと可視性 - Keeperは、同組織が採用している[SSOプロバイダー](#)とシームレスに統合します。これにより、従業員は自身のSSO認証情報を使用してKeeperに認証することができ、SSOをサポートしていない組織のクラウドやネイティブアプリケーションにも安全にアクセスできるようになりました。[KeeperFill®](#) は、Keeperのブラウザ拡張機能、モバイルアプリ、デスクトップアプリに搭載された機能で、ユーザーはウェブサイトやアプリ間で認証情報を即座に自動入力できます。

これらの統合機能と使いやすさ、Keeperのクラス最高水準のセキュリティとゼロ知識セキュリティアーキテクチャを活用することで、組織はサイバー攻撃の脅威から保護することができる安全なパスワード管理ソリューションを得ることができました。



Keeperパスワードマネージャー

ほとんどの企業では従業員のパスワードの取り扱いを把握するための可視性が限定的で、サイバーリスクが大幅に増加する可能性があります。パスワードの使用とコンプライアンスに関する重要な情報がなければ、パスワードの健全性を改善することはできません。Keeperは、究極のセキュリティ、可視性、および制御性を提供することでこれを解決します。

データは、Keeperのゼロ知識セキュリティアーキテクチャと、世界クラスの暗号化で保護されます。ゼロ知識とは、その情報を暗号化および復号化するのに使用される暗号鍵とマスターパスワードを知っているのはユーザーのみで、それらにアクセスできるのもユーザーのみであることを意味します。

Keeperは直感的に操作でき、ビジネスの規模に関係なく簡単に導入できます。KeeperはActive DirectoryやLDAPサーバーと統合することができるため、プロビジョニングとオンボーディングが効率化されます。[Keeper SSO Connect®](#)は既存のSSOソリューションと統合し、FedRAMPおよびStateRAMPの認証を受けています。

Keeperは、あらゆる規模の組織に対応できるように設計されています。役割ベースの権限、チーム共有、部門監査、および委任管理などの機能は、組織の成長をサポートします。[Keeper Commander](#)は、既存および将来のシステムに統合できる堅牢なAPIを提供します。

ビジネスユースケース: Keeperパスワードマネージャー

- パスワード関連のデータ漏洩やサイバー攻撃を防止
- パスキー対応で手間のかからない認証を実現
- コンプライアンスを強化
- 従業員の生産性を向上
- パスワードポリシーと手順の順守を確保
- ヘルプデスクにかかるコストを削減
- 迅速に安全性を実現することでトレーニングを最小化
- 従業員のセキュリティに対する認識と行動を改善

Keeperについて

Keeper Securityは、世界中の何百万人もの人々や何千もの組織のサイバーセキュリティを変革しています。エンドツーエンド暗号化で構築されており、直感的に操作できるKeeperのサイバーセキュリティプラットフォームは、「フォーチュン100」に名を連ねる企業から信頼を得ており、あらゆるデバイスをあらゆる場所で利用する、すべてのユーザーを保護します。当社の特許取得済みゼロトラストおよびゼロ知識の特権アクセス管理ソリューションは、企業のパスワード、シークレット、接続管理を、ゼロトラストのネットワークアクセスおよびリモートブラウザ分離に統合することができます。Keeperは、これらの重要なIDおよびアクセス管理の要素を、単一のクラウドベースのソリューションに組み込むことで、比類のない可視性、セキュリティ、制御を実現すると同時に、コンプライアンスや監査要件が確実に満たされるようにします。Keeperが今日のサイバー脅威から組織を保護する仕組みにつきましては、[KeeperSecurity.com](https://www.keepersecurity.com)をご覧ください。

Keeperは、世界中の何千もの企業や何百万というユーザーから信頼を得ており、愛用されています。



G2
エンタープライズリーダー



PCMag
エディターズチョイス



App Store
トップ評価の生産性



Google Play
インストール数1000万
以上