ケーススタディ

イリノイ・カレッジ、学内全体でデータセキュリティと認証情報管理を強化

背景

イリノイ・カレッジは、イリノイ州ジャクソンビルにある私立のリベラルアーツ系大学です。1829年に創立され、イェール大学から派遣された長老派の宣教師によって設立されました。州内でも最も歴史ある大学の一つです。

業種
私立大学

従業員数
300人

ソリューション
Keeperパスワードマネージャー
- BreachWatch
- コンプライアンスレポート
- 高度なレポートとアラートモジュール (ARAM)

課題

Keeper導入以前、イリノイ・カレッジでは旧来型のパスワード管理ツールを使用しており、技術面・運用面の両方で大きな負担が生じていました。ユーザーアカウントの同期は常に課題となり、情報の整合性を保つために、追加の作業時間や手動対応、継続的なトラブルシューティングが必要でした。その結果、利用はなかなか定着せず、システムに対する信頼も次第に低下していきました。

こうした課題に追い打ちをかけるように、従来のツールでは情報漏えいが公に発覚し、ソリューション全体に対する信頼は大きく損なわれました。さらに管理者は、分散的かつ安全性に欠ける認証情報の共有方法にも頭を悩ませていました。職員が認証情報を共有ドキュメントやスプレッドシート、さらには物理的な金庫に保管した紙資料に保存するケースも少なくありませんでした。こうした状況はリスクを高めるだけでなく、業務の遅延やチーム全体の可視性低下を招いていました。

大学としてサイバーセキュリティ強化に取り組む中で、従来の方法では、現在求められる要件に対応しきれないことが明らかになりました。Microsoft Azureのシングルサインオン (SSO) とスムーズに連携し、ユーザーのプロビジョニングに対応し、多要素認証 (MFA) の利用を簡素化しつつ、法令や学内のセキュリティ基準への準拠を支える、統合型の安全な基盤が必要だったのです。そこで同校は、日常業務を効率化でき、かつ利用しやすい、より信頼性の高いパスワード管理ソリューションの検討を開始しました。

Keeperのソリューション

従来のツールからの移行を決めた後、同校は複数の選択肢を比較検討し、最終的にKeeperを採用しました。Keeperは、認証情報の保護に対して現代的なアプローチを備えており、学内の学生と職員の双方を柔軟に支えられる基盤を提供しています。

認証情報の一元管理 - Keeperのゼロトラストおよびゼロ知識アーキテクチャにより、学内のパスワードを安全に保管・管理できる単一の基盤を確立しました。すべての認証情報を一か所で管理でき、Keeperのアーキテクチャに基づいて高い安全性を確保しています。

既存インフラとのスムーズな連携 - SSOプロバイダとスムーズに連携し、ユーザーは個別にマスターパスワードを作成することなく認証できるようになりました。SCIMプロビジョニングにより、ITチームはユーザーのオンボーディングとオフボーディングを自動化でき、Duoの多要素認証 (MFA) が追加の防御層として機能しています。さらに、Google Workspaceを通じて、KeeperFill®ブラウザ拡張機能を全ユーザーに自動配布できるようになりました。これにより、ウェブサイトやアプリで即座に自動入力が利用でき、直感的でスムーズな導入を実現しています。

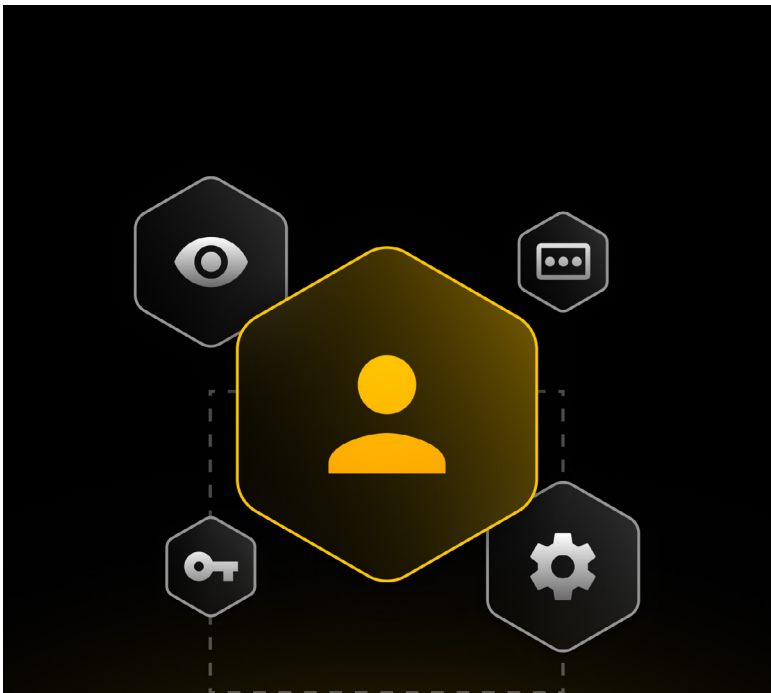
> **「教職員はマスターパスワードでサインインするだけで、ボルトにアクセスできます。Keeperのおかげで、導入直後から迷うことなくボルトを使い始めることができました。」**
>
> **パトリック・ブラウン | 最高情報責任者**

ユーザー定着とトレーニング支援 - Keeperは、わかりやすい製品ドキュメント, や導入時の支援資料、ユーザー向けの案内を用意しており、スムーズな導入を支えます。これらを活用し、学内向けの専用サイトを整備しました。Keeperは、組織の規模を問わず利用されているパスワード管理ツールで、直感的に使えて、短期間で展開できます。エンドユーザー向けには、製品ガイドやトレーニング動画を通じて使い方を丁寧に案内し、利用の定着を後押ししています。

コストパフォーマンス - Keeperは、組織の規模や業種を問わず、ニーズに合わせて無理なく拡張できる料金プランを用意しています。わかりやすい料金体系に加え、充実したカスタマーサポートにより、投資効果を最大限に引き出せます。

最高水準のセキュリティ - Keeperは、ゼロトラストおよびゼロ知識に基づくセキュリティアーキテクチャにより、情報を強固に保護し、情報漏えいのリスクを最小限に抑えます。デバイスレベルの楕円曲線暗号 (ECC) に加え、ボルト (保管庫)、フォルダ、レコード単位での多層暗号化を採用しています。さらに、多要素認証や生体認証、FIPS 140-3検証済みのAES 256ビット暗号とPBKDF2を組み合わせ、高い安全性を実現しています。また、KeeperはSOC 2およびISO 27001に準拠しており、業界でも長い実績を誇ります。加えて、FedRAMP HighおよびGovRAMPの認証も取得しています。

> **「Keeperは期待を上回る使いやすさでした。複数のデバイスで利用できる点も安心感につながり、業務の流れをスムーズにしてくれています。」**
>
> **- マーク・ベナー | アシスタントCIO兼ネットワーク管理者**



組織への影響

Keeperを学内全体に導入したことで、認証情報管理を一元化でき、サイバーセキュリティ態勢も強化されました。技術担当者だけでなく、非技術部門の利用者にとっても業務がスムーズになっています。さらに、運用面の負担を軽減し、パスワードや多要素認証(MFA) を安心して管理できる、信頼性の高い環境を実現しました。

セキュリティとコンプライアンスの強化 - Keeperの安全なアーキテクチャに加え、SSO連携や多要素認証(MFA) への対応により、機密データを扱うアカウントをより確実に保護できるようになりました。パスワードはエンドツーエンドで暗号化されたゼロ知識環境に保管され、FERPAなどの厳格な規制への対応も支えています。

ITサポート負荷の軽減 -SSOと自動プロビジョニングにより、ユーザーのオンボーディングが大幅に簡単になりました。職員がKeeper専用の認証情報を新たに作成・管理する必要がなくなったことで、導入はスムーズに進み、同期も迅速化しています。さらに、直感的な認証情報の共有が可能になり、パスワードへのアクセスや紛失に関するヘルプデスクへの問い合わせも大きく減少しました。

> **「アカウント作成後の運用負担が大きく減り、ITヘルプデスクへの問い合わせも大幅に減少しました。」**
>
> **ケルシー・シマート | エンドユーザーセキュリティ&サポート担当マネージャー**

場所を問わない業務効率の向上 - Keeperにより、教職員は場所やデバイスを選ばずに安全にアクセスできるようになり、日常業務の負担が大きく軽減されました。これまでデスクに戻る必要があった、MFAコードの確認、部門で共有する認証情報へのアクセス、レコードの更新といった作業も、より簡単かつ迅速に行えるようになっています。

教職員と学生への利用拡大 - Keeper導入後、教職員の間で利用が急速に広がりました。学生についても、アカウントの配布や初年次セミナーへの組み込みを通じて、利用が着実に拡大しています。学内での統一的な利用が進むことで、教職員と学生の双方に適切なパスワード管理が根付き、大学全体のセキュリティ意識の向上につながっています。

> **「教員は授業でKeeperの重要性を学生に伝え、自らのアイデンティティ保護にも活用しています。」**
>
> **パトリック・ブラウン | 最高情報責任者**

安定したアクセスと高い運用信頼性 - Keeperの高い信頼性により、認証情報管理の仕組みに対する安心感が高まりました。他のクラウドサービスで大規模な障害が発生した際も、Keeperは影響を受けることなく稼働を続け、プラットフォームへの信頼をさらに強めています。

Keeperへの移行により、学内で特に重要なシステムを守るための基盤が整い、キャンパス全体で一貫したセキュリティ運用を維持できるようになりました。Keeperという信頼性の高いパスワード管理ソリューションにより、サイバー脅威に対しても安心して備えられる環境を実現しています。

Keeperパスワードマネージャー

多くの企業では、従業員のパスワード運用状況を十分に把握できておらず、そのことがサイバーリスクの大幅な増加につながっています。パスワードの利用状況やポリシー遵守に関する情報がなければ、適切なパスワード管理を徹底することはできません。Keeperは、最高水準のセキュリティ、高い可視性、確実な統制によって、この課題を解決します。

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最高水準の暗号化によって保護されています。ゼロ知識とは、マスターパスワードおよび情報の暗号化・復号に使用される暗号鍵を把握・保持しているのがユーザー本人のみであることを意味します。

Keeperは、企業規模を問わず直感的に使いやすく、容易に導入できます。Active DirectoryやLDAPサーバーと連携することで、プロビジョニングやオンボーディングを効率化します。**Keeper SSOコネクト**は既存のSSOソリューションと統合でき、FedRAMP HighおよびGovRAMPの認証を取得しています。

Keeperは、あらゆる規模の組織に対応できるよう設計されています。ロールベースの権限管理、チーム共有、部門別の監査、委任管理といった機能により、組織の成長を継続的に支援します。**Keeperコマンダー**は、既存システムおよび将来的なシステム連携を可能にする強力なAPIを備えています。

Keeperパスワードマネージャーのビジネスでの活用事例

- パスワード関連の情報漏えいやサイバー攻撃の防止
- パスキーに対応し、スムーズな認証を実現
- コンプライアンスの強化
- 従業員の生産性向上
- パスワードポリシーと運用ルールの徹底
- ヘルプデスクのコストを削減
- 短期間でセキュリティを確保し、トレーニングの手間を最小限に抑える
- 従業員のセキュリティ意識と行動を向上させる

Keeperについて

Keeper Securityは、150以上の国で幅広い企業や利用者を守る、急成長中のサイバーセキュリティソフトウェア企業です。ゼロ知識とゼロトラストを基盤とし、あらゆるIT環境に対応できるセキュリティの先駆けとして知られています。主力製品のKeeperPAM®は、AIを搭載したクラウドネイティブのプラットフォームであり、ユーザーやデバイス、インフラを包括的にサイバー攻撃から保護します。特権アクセス管理 (PAM) の分野では、ガートナー社の「Magic Quadrant (マジック・クアドラント)」において革新性が高く評価されました。Keeperではロールベースのポリシー、最小権限、ジャストインタイムアクセスを組み合わせることで、パスワードやパスキー、インフラのシークレット、リモート接続、エンドポイントを安全に管理しています。世界中の多くの先進的な組織がKeeperを採用している理由については、**KeeperSecurity.com**にてご確認ください。

Keeperは、世界各地の企業や利用者から高い信頼を得ています。

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
生産性向上分野で高評価

Google Play
1000万件以上のインストール