ケーススタディ

Lucidica、KeeperMSP®の導入によりコンプライアンス体制を強化し、顧客からの信頼向上を実現

背景

Lucidicaは、英国全域の中堅・中小企業を対象に、ITサポート、サイバーセキュリティ、コンサルティングまでを包括的に提供する、実績あるマネージドサービスプロバイダ (MSP) です。

Lucidicaは、数多くの組織から信頼されるITパートナーとして、コンプライアンスや信頼性を重視するとともに、業界水準に沿った高度なセキュリティ対策を顧客に適用できる体制を整えています。英国政府が主導するサイバーセキュリティ認証制度であるCyber EssentialsやISOの認証要件を満たすため、分散したチーム間でも安全に情報を共有・管理できる、エンタープライズ向けのパスワード管理ソリューションが必要でした。

業種
マネージドサービスプロバイダー (MSP)

従業員数
50人未満

ソリューション
KeeperMSPとBreachwatch

課題

Keeper導入以前、Lucidicaでは旧来型のパスワード管理ツールを使用しており、業務の遅延を招くことが多く、不要なセキュリティリスクも生じていました。その結果、いくつかの基本的な要件を十分に満たせない状況にあり、安全で使いやすいパスワード管理ソリューションの必要性が明確になっていました。こうした課題を解決するため、LucidicaはKeeperを採用しました。従来のソリューションでは、特に次のような点が問題となっていました。

ボルトの同期不具合 - パスワードの内容が端末ごとに異なって表示されることがあり、どの情報が正しいのかを確認するために技術者が時間を取られ、業務の混乱や無駄が生じていました。

一貫性と信頼性に欠けるパスワード共有 - 共有した認証情報が正しく同期されなかったり、相手に届かなかったりするケースが頻繁に発生していました。その結果、クレジットカード番号を含む機密情報を、メールや文書、パスワード付きの表計算ファイルでやり取りせざるを得ない状況が生じていました。こうした安全性の低い共有方法により、重要なデータが漏えいするリスクが大きく高まっていました。

顧客への助言業務への影響 - LucidicaはMSPとして、日常的に顧客へサイバーセキュリティに関する助言を行っています。しかし、従来の仕組みには課題があり、パスワード管理の適切な運用を自信をもって提案しにくい状況にありました。

> **「まずは自社が手本となる必要がありました。従来のプラットフォームは信頼性に欠けていただけでなく、パスワード管理ツールそのものを使うことに対して、顧客に消極的な印象を与えてしまっていました。」**
>
> **Maria Nagle (マリア・ネーグル、サービスデリバリー/プロジェクトマネージャー)**

Lucidicaでは、欧州全域で求められる最新の運用要件やコンプライアンス基準に対応するため、安全性が高く、直感的に使えるクラウド型のソリューションが必要だと早い段階で判断しました。

Keeperのソリューション

複数のパスワード管理プラットフォームを比較検討した結果、LucidicaはKeeperMSPにBreachWatchアドオンを組み合わせて採用しました。これにより、エンタープライズ水準のパスワード管理機能と、ダークウェブ上の情報漏えいを監視する仕組みを利用できるようになりました。このソリューションによって、チームがこれまで求めていたマルチテナント対応のクラウド環境を、違和感なく利用できるようになり、従来のツールで課題となっていた処理速度や信頼性の問題も早期に解消されました。

特に大きな利点となったのが、KeeperのMicrosoft SSO連携です。認証の運用を強化しつつ、ユーザーのオンボーディングも簡素化できました。加えて、LucidicaはKeeperのカスタマーサポートの質の高さも評価しています。初回の打ち合わせからデモ、最終的な展開に至るまで、導入プロセスは迅速かつ円滑で、従来のベンダーと比べても格段に効率的でした。

> 「最初の問い合わせからデモ、導入まで、すべてがスピーディーでした。他のベンダーとは比べものになりません。」
>
> Nubia Coleman (ヌビア・コールマン、ゼネラルマネ　ージャー)

KeeperMSPの導入により、Lucidicaが重視してきた英国政府が主導するサイバーセキュリティ認証制度であるCyber EssentialsおよびISOへの準拠体制も強化されました。その結果、MSPとして顧客に対し、高いセキュリティ基準を自ら実践し、示していくための基盤が整いました。

コスト効率に優れた設計 - 組織の規模や業種を問わず、ニーズに合わせて導入・拡張できる料金プランを用意しています。明確で分かりやすい価格体系に加え、G2においてエンタープライズ向けカスタマーサポート分野で第1位に評価されたサポート体制により、投資効果を最大限に引き出すことができます。

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のセキュリティ設計を採用し、情報保護とデータ漏えいリスクの低減に取り組んでいます。端末レベルでの楕円曲線暗号 (ECC) に加え、ボルト、フォルダ、レコードの各階層で複数層の暗号化を適用しています。さらに、多要素認証や生体認証、FIPS 140-3に準拠したAES 256ビット暗号とPBKDF2を組み合わせることで、堅牢なセキュリティ基盤を実現しています。Keeperは、SOC 2およびISO 27001に準拠しており、業界の中でも長年にわたりこれらの認証要件への対応を継続してきました。また、FedRAMPおよびGovRAMPの認可も取得しています。

> 「Keeperは使いやすく、直感的に操作できます。同期も高速で、安心して利用できます。」
>
> Maria Nagle (マリア・ネーグル、サービスデリバリー/プロジェクトマネージャー)

組織への影響

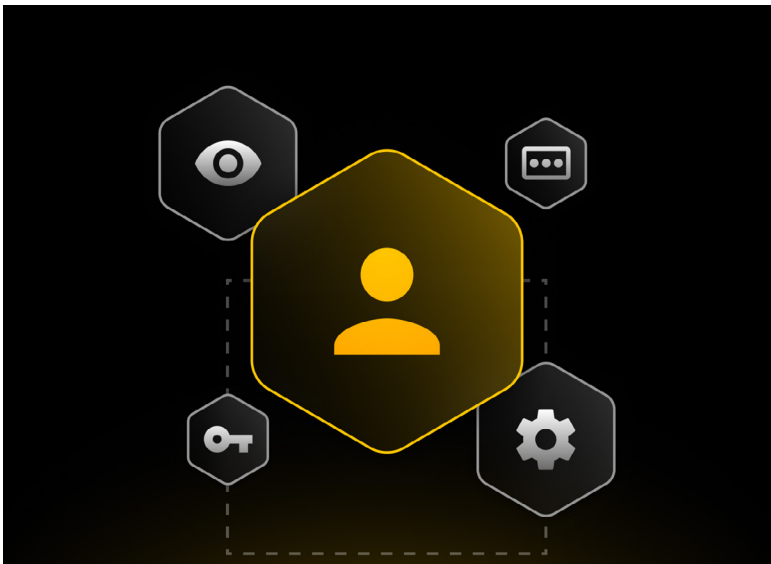
Keeperはチーム全体への展開もスムーズに進みました。管理者は、役割や権限、共有フォルダの管理に短期間で慣れ、操作性の高さや使いやすさも評価しています。さらに、Keeperが用意するトレーニング動画や充実したドキュメントが、新入社員のオンボーディングを円滑にするとともに、顧客へベストプラクティスを共有する際にも役立ちました。

エンドユーザーにとっても、利用体験は非常に良好でした。ブラウザ拡張機能や自動入力機能により、日常の作業が効率化されました。また、付帯するファミリープランは、家庭内でのサイバーセキュリティ意識や習慣の向上にもつながっています。

ダークウェブ監視 - BreachWatchなどの追加機能は、導入後すぐに業務に欠かせない存在となりました。ダークウェブ上で漏えいした認証情報をリアルタイムで把握できるようになったためです。さらに、セキュリティ監査機能により、弱いパスワードや使い回しの状況を可視化でき、組織全体でより適切なパスワード管理を維持できるようになりました。

業務フローの効率化 - Keeperはクラウド型のため、従来のデスクトップ型ツールで頻発していたフリーズやインストール時の不具合、同期エラーに悩まされることがなくなりました。リアルタイム同期により、端末ごとのパスワード不整合や可視性の不足が解消され、継続的なトラブル対応も不要となったことで、業務全体の効率が大きく向上しました。

Keeper導入後、Lucidicaではセキュリティと生産性の両面で明確な改善が見られました。パスワードの保管や共有にあたり、安全性に不安のあるファイルやメッセージツールに頼る必要はなくなり、同期に関する問題も解消されています。その結果、セキュリティとコンプライアンスの体制が強化され、利用者の満足度も高まりました。現在では、Lucidicaはパスワード管理を自信をもって顧客に勧められるようになっています。これは、導入前には実現できなかったことです。



Keeperパスワードマネージャー

多くの企業では、従業員がどのようにパスワードを扱っているのか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増大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の実態が分からなければ、適切な管理や改善は行えません。Keeperは、こうした課題に対し、セキュリティ、可視性、管理性を兼ね備えた仕組みを提供します。

Keeperは、ゼロ知識セキュリティアーキテクチャと世界水準の暗号化技術により、データを強固に保護します。ゼロ知識とは、マスターパスワードと情報の暗号化・復号に使われる鍵を知っているのはユーザー本人だけであることを意味します。

Keeperは、Active DirectoryやLDAPサーバーと連携できるため、アカウントのプロビジョニングやオンボーディングを効率化できます。**Keeper SSOコネクト**は既存のSSO基盤と統合でき、FedRAMPおよびGovRAMPの認可も取得しています。また、Keeperは組織の規模を問わず利用できるよう設計されており、成長に合わせた運用にも対応します。ロールベースの権限管理、チームでの共有、部門単位の監査、管理権限の委任といった機能により、組織の拡大を支えます。さらに、**Keeperコマンダー**は、現在利用しているシステムや将来的なシステムとの連携を可能にする、柔軟なAPIを備えています。

ビジネスにKeeperMSP**を導入すべき理由**

- MSP向けの使いやすいマルチテナント管理
- パスワード管理の不備によるデータ漏えい・サイバー攻撃を防ぐ
- パスキー対応で、スムーズな認証を実現
- 顧客満足度の向上
- 新たな収益源を創出
- パスワードポリシーと運用ルールを徹底
- コンプライアンスとレポート機能を強化
- 短期間で安全な運用を実現し、トレーニングの負担を最小限に
- 従業員のセキュリティ意識と行動を向上

Keeperについて

Keeper Securityは、150か国以上で多数の組織や個人に利用されている、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。あらゆるIT環境に対応する形で、ゼロ知識およびゼロトラストセキュリティをいち早く確立してきました。中核となる製品であるKeeperPAM®は、AIを活用したクラウドネイティブなプラットフォームとして、ユーザー、デバイス、インフラ全体をサイバー攻撃から守ります。ガートナーのマジック・クアドラント (PAM分野) では、その革新性が高く評価されています。KeeperPAMは、ロールベースのポリシー制御、最小権限、ジャストインタイムアクセスを軸に、パスワードやパスキー、インフラ用シークレット、リモート接続、エンドポイントの安全な管理を実現します。現代の高度化するサイバー脅威への対策として、なぜ多くの先進的な組織がKeeperを信頼しているのかについて、詳しくはKeeperSecurity.comをご覧ください。

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