

## ケーススタディ

# VaynerX、Keeper を全社展開



### 背景

VaynerXは、ゲイリー・ヴェイナチャック (Gary Vaynerchuk) 氏によって設立された、ブランド、カルチャー、テクノロジーの交差点で事業を展開するグローバルなモダンメディアおよびコミュニケーション企業です。本社をニューヨークに置き、VaynerMediaをはじめとする複数の専門企業を擁する持株会社として機能しています。これらの企業群は、広告、コマース、メディア、インフルエンサーマーケティング、デジタルトランスフォーメーションの分野において、世界的に知名度の高いブランドを支援しています。

業種  
広告・コミュニケーション

従業員数  
2000人以上

#### ソリューション

Keeperパスワードマネージャー

- 高度なレポート機能とアラートモジュール (ARAM)
- プラチナサポート



### 課題

Keeper導入以前、VaynerXでは認証情報の管理が分散していました。VaynerXは、日々の業務を効率化すると同時に、クライアントのアカウント管理におけるセキュリティ態勢を強化できる最適なソリューションを求めています。社内チームは日常的にクライアントが所有するシステムへアクセスするため、認証情報の保護は社内業務の安全性だけでなく、クライアントからの信頼や長期的なパートナーシップを守るうえでも不可欠でした。

「Keeper導入以前は、組織全体を一つの画面で把握できるような統合的な管理基盤がありませんでした。」

ジョン・ジョーガトス (VaynerX グローバル  
最高情報責任者)



### Keeperのソリューション

これらの課題に対応するため、VaynerXではエンタープライズ向けパスワード管理プラットフォームを評価し、最終的にKeeperを採用しました。Keeperの強固なセキュリティアーキテクチャ、管理機能の充実度、複数の事業体を擁する複雑な組織構造においても、生産性を損なうことなく展開できる点が、採用の決め手となりました。

「Keeperを選んだ理由は、機能性と使いやすさに加え、システムを一元管理でき、エンタープライズレベルのセキュリティ管理が可能だった点です。」

ジョン・マールーフ (VaynerX グローバル調達責任者)

認証情報の一元管理 - ゼロトラスト・ゼロ知識アーキテクチャに基づき、エンタープライズレベルのガバナンスと統制を維持しながら、認証情報を安全に管理するための一元的なプラットフォームが導入されました。Keeperは、VaynerXのすべての事業体における標準のパスワード管理ソリューションとして全社展開され、集中管理と各チームのコラボレーションの両立を実現しています。当初からの目的は、単なるパスワードボルトの導入ではなく、認証情報のライフサイクル管理を担う、全社規模の仕組みを確立することでした。

「Keeperを採用する決め手となったのは、Oktaとの連携が非常にシンプルで、両プラットフォームがスムーズに連携できたことです。」

ジョン・ジョーガトス (VaynerX グローバル最高情報責任者)

既存インフラとのシームレスな統合 - KeeperはOktaとシームレスに連携し、シングルサインオン (SSO)、ユーザーの自動プロビジョニングおよびデプロビジョニングに対応することで、シンプルで使いやすい認証体験を実現しました。従業員は通常のログインフローの一部としてKeeperにアクセスでき、IT部門は一元的な管理を維持できます。さらにGoogle Workspaceを通じて、管理者はKeeperFill®ブラウザ拡張機能を全社展開し、導入の迅速化と、ウェブサイトやアプリケーションにおける安全な自動入力を可能にしました。

「KeeperのGoogle Chrome拡張機能は、ネイティブに統合されている点が非常に印象的でした。ログインしようとしているウェブサイトから離れることなく、パスワード欄に自動入力できる点が特に優れています。」

ジョン・マールーフ (VaynerX グローバル調達責任者)

ユーザー定着とトレーニング支援 - Keeperは、エンタープライズ全体への導入を支援するために、充実した製品ドキュメント、導入リソース、カスタマーサクセスによるサポートを用意しています。VaynerXでは、これらのリソースに社内コミュニケーションやライブトレーニングセッションを組み合わせ、グローバルな従業員全体への円滑な展開を実現しました。Keeperは、あらゆる規模の組織向けパスワード管理ツールとして高く評価されており、使いやすく、迅速に導入できる点が特長です。エンドユーザー向けには、詳細な製品ガイドやトレーニング動画が、利用定着の促進に寄与しています。

「導入前からKeeperのカスタマーサクセスチームが密にサポートしてくれ、すべてのトレーニングを通じて、利用定着率が期待どおりに高まるよう支えてくれました。」

ジョン・ジョーガトス (VaynerX グローバル最高情報責任者)

高い費用対効果 - 組織の規模や業種を問わず、Keeperはニーズに応じて柔軟に拡張できる費用対効果の高いプランを用意しています。透明性の高い料金体系と充実したカスタマーサポートにより、投資価値を最大限に引き出せます。

業界最高水準のセキュリティ - Keeperのゼロトラスト・ゼロ知識セキュリティアーキテクチャは、情報保護とデータ侵害リスクの低減において他に類を見ません。デバイスレベルの楕円曲線暗号 (ECC) に加え、ボルト、フォルダ、レコードの各レベルで多層的な暗号化を実装し、多要素認証や生体認証にも対応しています。さらにKeeperは、業界で最も長いSOC 2およびISO 27001準拠の実績を持ち、FedRAMP HighおよびGovRAMPの認証も取得しています。



## 組織への影響

Keeperの導入はVaynerX全体にわたって持続的な効果をもたらした。全体的なセキュリティ強化、業務効率の向上、そして重要なデータを守るという共通の責任意識の醸成につながりました。

セキュリティ態勢の強化と一元的なガバナンス - Keeperを全社展開したことで、VaynerXは認証情報の作成、保存、共有、アクセス状況を一貫して可視化できるようになりました。セキュリティチームは、パスワードポリシーの適用、使い回しの抑制、リスクの予防的な管理を、社内システムおよびクライアント環境全体で行えるようになっています。この取り組みにより、社内システムだけでなく、VaynerXのチームが日常的に利用するクライアント所有のプラットフォームにおいても、リスク低減が実現しました。

「ここでは全員がKeeperを使っています。選択肢ではなく、その運用が定着しています。」

– クリスティーン・カデッツ (VaynerX 調達担当ディレクター)

ITおよびセキュリティチームの業務効率向上 - Keeperにより、認証情報の安全な引き継ぎとアクセス管理の一元化が可能となり、オンボーディングおよびオフボーディングのプロセスが効率化されました。その結果、VaynerXではパスワード関連のITサポート対応が大幅に減少しました。

安全かつ柔軟なクライアント連携 - クライアント業務はVaynerXの中核であり、Keeperの使いやすい共有機能はその業務モデルを直接支えています。Keeperの**双方向ワンタイム共有**機能により、VaynerXは、メールや共有ドキュメントに頼ることなく、Keeperを利用していないクライアントやベンダーからも機密性の高い認証情報を安全に受け取ることができます。

「双方向ワンタイム共有機能は非常に有用で、クライアントとベンダー間の情報共有を安全に行うことができます。」

ジョン・ジョーガトス (VaynerX グローバル最高情報責任者)

高い利用定着率と業務への影響最小化 - Keeperは、使いやすさに加え、ブラウザ拡張機能やモバイル対応により、技術部門・非技術部門を問わず高い利用定着率を実現しました。VaynerXでは、従業員の99.5%がKeeperへのオンボーディングを完了しています。現在、Keeperは認証情報の保存、管理、生成を支える日常業務に欠かせないツールとなっており、組織全体の業務のあり方に大きな変化をもたらしています。

職場の枠を超えた前向きな効果 - 従業員に無料のファミリープランを提供し、個人利用でもKeeperを使えるようにしたことで、VaynerXの枠を超えてセキュリティ意識の定着が促進されました。従業員は日常生活においても同じベストプラクティスを実践できるようになっています。業務外にも安全な認証情報管理を広げることで、組織全体のリスク低減につながると同時に、セキュリティ意識の高い文化の醸成がさらに進みました。

「Keeperは、集中化、集約、標準化を柱とする当社の組織変革目標の実現に貢献しています。」

ジョン・ジョーガトス (VaynerX グローバル最高情報責任者)

総じて、KeeperはVaynerXのサイバーセキュリティ戦略の中核として、パスワードやパスキーの安全な運用を支え、クライアントの信頼を強化するとともに、これまでにない可視性を実現しています。業務のスピードを落とすことなく、チームが大きな価値を生み出すことを可能にしています。





## 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