



APIキー、データベースパスワード、アクセスキー、認証情報などのインフラ機密を保護する最新のクラウドベースのプラットフォームで、サプライチェーン攻撃を防御します。

## 課題

盗まれた、あるいは脆弱なDevOpsの秘密は、サプライチェーン攻撃の主な原因となっています。シークレットはソースコード、設定ファイル、CI/CDシステム全体に広がっており、組織はハッカーに晒されていると言っても過言ではありません。このように攻撃対象が拡大することで、DevOps、セキュリティ、ITの専門家にはいくつかの課題が生じます

01

開発チームはしばしばセキュリティよりも生産性を優先し、善意の従業員が環境全体に認証情報をハードコーディングしてしまう。

02

地域、システム、環境を超えて、分散された遠隔地の従業員が共同作業を行う。異なる機種間の機密保管につながる

03

一元管理されたアクセス制御がないと、従業員が過剰な特権を持つようになるリスクがある。

04

多くの組織では、社内ポリシーやコンプライアンス・ポリシーにより、定期的なクレデンシャルのローテーションが義務付けられています。これは包括的な保管庫によってのみ可能です。

組織には、安全で使いやすく、費用対効果の高い方法が必要です。

機密の拡散を抑制し、最小特権アクセスを強制する、安全で使いやすく費用対効果の高い方法が必要です。アクセスの調整、自動化された認証情報のローテーションを実施し、エンドツーエンドの暗号化を保証します。

## 解決策

Keeper シークレットマネージャーは、DevOps、IT、セキュリティ、およびソフトウェア開発チームに、インフラストラクチャの秘密を管理し、組織の最も機密性の高いデータを保護するためのクラウドベースのゼロトラストおよびゼロ知識セキュリティプラットフォームを提供します。Keeper シークレットマネージャーはシークレットを一元管理し、無許可アクセスを防止し、監査とロギングを提供します。広範なソフトウェア開発キット (SDK) とアプリケーションプログラミングインターフェース (API) 機能により、あらゆるプログラミング言語に認証情報を即座に注入することができます。

## Keeperでハッキングされないための対策を。

詳しく見る  
[keepersecurity.com/ja\\_JP/](https://keepersecurity.com/ja_JP/)

デモを予約する  
[meetings.hubspot.com/yuki-dobashi-lortie/apac-rr](https://meetings.hubspot.com/yuki-dobashi-lortie/apac-rr)

### Keeper Securityについて

Keeper Security は世界中の人々と組織のサイバーセキュリティを変革しています。Keeper の手頃な価格で使いやすいサイバーセキュリティソリューションは、すべてのデバイス上のすべてのユーザーを保護するために、ゼロトラストおよびゼロ知識セキュリティの基礎の上に構築されています。数百万人の個人と数千の組織は、クラス最高のパスワード、パスキー、秘密管理、特権アクセス管理 (PAM)、安全なリモートアクセスと暗号化されたメッセージングのために Keeper に依存しています。当社の次世代サイバーセキュリティプラットフォームは、数分で導入でき、あらゆる技術スタックとシームレスに統合することで、侵害を防止し、ヘルプデスクのコストを削減し、コンプライアンスを確保します。Keeper Security は、大手プライベートエクイティ企業の Insight Partners と Summit Partners の支援を受けています。

ユーザー

セキュリティ運用、開発運用、IT


Entra ID、Oktaなどの  
IDプロバイダおよびシ  
ングルサインオン

パスワード管理

シークレット管理

ゼロトラスト  
ネットワークアクセスリモートブラウザ  
分離

管理コンソール


SSOアプリ  
SCIM  
多要素認証  
パスワードレス  
OIDC  
プロビジョニング

パスワードベース  
アプリ  
パスワードの共有  
パスキーの保存と  
共有  
インフラシーク  
レット  
TOTPコード  
ファイルの保存と  
共有

CI/CD  
カスタムアプリ  
CLI  
コマンダー  
外部チケット参照

デスクトップ  
RDP  
SSH  
VNC  
データベース  
トンネリング接続

ウェブアプリ  
ウェブサイト  
クラウドアプリ  
インターネットサ  
イト

強制ポリシー  
可視性&分析  
セキュリティ監査  
イベントログ&通知  
コンプライアンス報告  
SIEM統合  
ダークウェブモニタリ  
ング  
リスク管理


SAMLアプリ

パスワードや  
パスキーを使用する  
アプリJenkins、Github,  
Terraform、  
PowershellなどWindows, Linux,  
MySQL、SQL  
Server、  
PostgreSQLなどユーザーデバイス、  
マシン、ブラウザユーザーデバイス、  
マシン、ブラウザ

## ビジネスバリュー

高度に特権化されたシステムとデータを保護

シークレットを統一プラットフォームに統合し、ソースコード、  
設定ファイル、CI/CDシステムからハードコードされた認証情  
報を削除することで、シークレットの乱立を解消します。

柔軟で迅速な統合

Github Actions、Jenkins、Ansibleなどの一般的なCI/CDプラ  
ットフォームとすぐに統合できます。

簡単で使いやすい

完全なクラウドベース、ゼロトラスト、ゼロ知識のプラットフォー  
ムで、複雑なネットワーク、ストレージ、HA設定を必要としませ  
ん。

## 主要機能

- インフラストラクチャおよびマルチクラウド環境全体で、サー  
ビスおよび管理者アカウント、ユーザーID、RESTベースの  
APIアカウント、マシン、ユーザー アカウントの認証情報を自  
動的にローテーションします。
- ロールベースのアクセス制御により、アクセス権とアクセス  
許可を管理します。
- クライアントデバイスは、取得後に保管庫の秘密をローカル  
で復号化します。Keeperには、保存されたデータ保管庫のデ  
ータを復号化する機能はありません。
- Keeper シークレットマネージャーは、無制限のスケーリング  
容量を持つフルマネージドサービスです。