KEEPER®

AIで加速するサイバー攻撃
今見直すべき認証情報と特権管理

～攻撃のスピードは変わる。
守るべき認証情報と権限の重要性は変わらない。～



Keeper Security APAC 株式会社
エンタープライズ営業本部
荒堀 太郎

Corporate Overview

Keeper Security

アンケートはこちら

- 2011年創業　（米国イリノイ州シカゴ）
- 2023年5月 APAC本社設立（東京）
  - 企業・組織向け認証情報（パスワード&シークレット）管理
  - 特権アクセス管理
  - エンドポイント特権管理（AIエージェント管理）
- グローバル顧客数 10万社、国内 約850社
- SaaSソリューションのデータセンターは米国、カナダ、欧州、日本（東京、大阪）、オーストラリアに配置
- グローバル 120カ国以上、21言語での展開
- Williams Racing とのパートナーシップ締結
- 業界最高位の受賞歴とユーザー評価

© 2026 Keeper Security, Inc.

AIが変えるのは、攻撃の「速度」と「規模」

アンケートはこちら

事例① フィッシング

従来：不自然な文章や一斉送信

AI活用：自然な日本語で、部署・役職に合わせた偽メールを短時間で作成

事例② 脆弱性探索

従来：情報収集・コード分析に時間

AI活用：公開情報の整理、コードの解析、攻撃候補の調査を効率化

事例③ 侵入後の活動

従来：手作業で情報や権限を調査

AI活用：盗まれた情報の分類やアクセス先の分析を効率化

従来から存在する攻撃を、より早く、より大きな規模で実行可能に。

© 2026 Keeper Security, Inc.

AIによる攻撃は、すでに現実の脅威に

アンケートはこちら

約15秒

ダミーサイトで、脆弱性診断から
個人情報の収集まで実行したと報道

01　脆弱性を診断

攻撃対象の弱点を探索

02　攻撃を実行

検証環境で処理を自動化

03　情報を収集

短時間でデータを取得

AIによって、攻撃のスピードと自動化は新たな段階へ。その中で、攻撃者が狙うものは？

出典：読売新聞（2026/10/22）

© 2026 Keeper Security, Inc.

AIで攻撃は進化する。しかし、重要な標的は変わらない。

アンケートはこちら

AIによって変わるもの

- 攻撃の速度
- 攻撃の規模
- 攻撃の自動化

↓ しかし、攻撃者が狙う重要な標的は変わらない

認証情報
パスワード・トークン

アクセス権限
正規ID・管理者権限

重要な情報資産
業務システム・機密データ

盗まれた認証情報は、攻撃者にとって正規のアクセス手段となる。

© 2026 Keeper Security, Inc.

盗まれた認証情報は、どのように悪用されるのか

アンケートはこちら

01

認証情報・セッションの窃取

パスワード・トークン・Cookieなどが狙われる

→

02

正規ユーザーになりすまし

業務アプリ・クラウド・管理システムへアクセス

→

03

情報漏洩・不正操作

情報の閲覧・持ち出し・設定変更など

認証情報の悪用が、重要なシステムへの不正アクセスや情報漏洩につながる。

© 2026 Keeper Security, Inc.

企業に残る、認証情報と権限管理の盲点

AIで攻撃が高速化する一方、企業には従来からの管理上の弱点が残っている

アンケートはこちら

パスワード管理の分散

Excel・個人管理・使い回し

恒常的な特権

常時管理者・過剰な権限

共有ID・シークレット

共有アカウント・APIキーの管理不足

証跡の不足

操作内容と責任を追跡しづらい

以前から存在していた管理上の弱点が、より大きなリスクに。

© 2026 Keeper Security, Inc.

認証情報・権限・操作を守る、3つの防御



アンケートはこちら

認証情報を守る

パスワード・秘密情報の悪用リスクを低減

暗号化保管 / 漏洩パスワードの排除 / 安全な共有

アクセスを制御する

一般利用者も管理者も、権限を最小限に

最小権限 / JIT・承認 / セッション管理

操作を把握/制御する

不審なアクセスや行動を追跡・調査

監査ログ / セッション記録 / 分析 / リアルタイム対処

認証情報の保護からアクセス後のリスクまで3つの組み合わせで対応。

© 2026 Keeper Security, Inc.

人・システム・AIエージェントへ広がる認証情報管理



アンケートはこちら

人

認証情報を保護
パスワード・パスキー

アクセス・特権操作を把握

システム

認証情報を保護
APIキー・トークン

システム間アクセスを把握

AIエージェント

認証情報を保護
APIキー・シークレット

ツール利用・アクセス先・権限行使を監視

組織内のあらゆる認証情報を保護し、エージェントのアクセス・操作も把握する。

© 2026 Keeper Security, Inc.

Keeper：認証情報・アクセス・操作を統合的に保護

人のパスワードから、システム・AIのシークレット、特権操作まで



アンケートはこちら

管理の課題

パスワード管理の分散

Excel・メール・使い回し

秘密情報の露出

APIキー・トークンの埋め込み

アクセス権限の過剰付与

一般ID・管理者IDの権限

操作の把握不足

特権操作・AIエージェント

→

KEEPER PASSWORD MANAGER

人の認証情報

暗号化保管
安全な共有

自動入力・
漏洩リスク検知

フィッシング対策

KEEPER SECRETS MANAGER

システム・AIの秘密情報

APIキー・
トークン保護

アプリへの
安全な提供

KEEPER PAM

特権アクセス管理

パスワード秘匿

最小権限・
セッション監査

Keeper AIによる
操作分析・
リアルタイム対処

ENDPOINT PRIVILEGE MANAGER

端末権限AI監視

必要時のみ
プロセス単位で
権限昇格

AIエージェント監視

1プラットフォームで
認証情報・シークレットの暗号化保護 × アクセス権限の管理 × 操作の可視化

© 2026 Keeper Security, Inc.

AIで攻撃が進化しても、
守るべき本質は変わらない。

アンケートはこちら

01

認証情報を守る

暗号化と適切な管理で
悪用リスクを低減

02

権限を最小化する

必要な人・システムに
必要な権限だけを付与

03

アクセスと操作を制御する

アクセスを制御し、操作を
記録・監視してリスクに対応

攻撃が加速する今、人・システム・AIの認証情報とアクセスを見直す。

ぜひ、Keeper Securityのブースにお立ち寄りください！

© 2026 Keeper Security, Inc.


KEEPER