KEEPER®
CONNECTION MANAGER

データシート：リモートデスクトップとサーバーアクセス

VPN を使用せずにリモートデスクトップやマシンに安全で簡単にアクセス

どこにいても、どのデバイスからでも、どのウェブブラウザからでも、システムに安全にアクセスできます。

リモートワークを長期的に成功させるためには、従業員がデスクトップやアプリケーションに素早くアクセスできる、安全で信頼性が高く、拡張性の高い方法が必要となります。

仮想プライベートネットワーク（VPN）は一般的な選択肢ですが、いくつかのエリアにおいては不十分な点があります。VPN は高価で、IT 担当者が設定や維持するのが難しく、エンドユーザーが使用するのも難しいことで有名です。VPN は、遅延、信頼性、可用性の問題にも悩まされています。

リモートデスクトップは、適切に実装されれば、VPN に代わる有力な選択肢となります。

- 標準化されたリモートデスクトップ環境の展開、サポート、維持のための管理負担は、エンドユーザーが使用する分散型物理デバイスのサポートに比べて大幅に軽減されます。
- リモートデスクトップ・ソリューションがエンドポイントにエージェントを必要としない限り、基本的に従業員は個人のノートパソコンやスマートフォンなどのあらゆるマシンをアクセスに使用することができます。
- エンドユーザーのデバイスに物理的にアクセスする必要がほとんどないため、会社資産のサポートコスト全般を削減できます。
- リモートデスクトップは、ほとんどの VPN では不可能なゼロトラストアーキテクチャを採用することができるため、分散型ワーカーのセキュリティを強化します。
- リモートデスクトップを介して分散チームが実行するアクションは、エンタープライズ・ファイアウォールの内側で実行されます。結果として、物理的なオフィス環境で作業しているときと同じように、企業のセキュリティシステムにより保護されるようになります。
- リモートデスクトップでは、ユーザーがローカルのマシンではなく、エンタープライズネットワーク上にデータを保管することを推奨しています。データを適切にバックアップし、保護することができるため、ファイアウォールの内側での保護はより強靭なものとなります。さらに、データが紛失する可能性がはるかに低く、他者と共有することもはるかに簡単です。
- リモートデスクトップは、高いスケーラビリティを発揮します（特にエンドポイントにエージェントを必要としない場合）。個々のデバイスにアクセスする必要がないため、画像の標準化が容易で、デスクトップやアプリケーションのアップデートを自動化できます。

Keeper Connection Manager のお客様事例：製造業

Keeper Connection Manager にできるのは在宅勤務者にリモートデスクトップを提供する以上のことです。拡張性が高く、安全で、簡単に使用できるため、多くの組織がラボやトレーニング環境のデスクトップを提供するために使用しています。

ある大手消費者デバイスメーカーは、グローバルオフィスにトレーニングラボを設置しました。デスクトップへの直接アクセスを提供すると、メンテナンスが難しく、ユーザーにとってわかりにくいものとなっていました。

Keeper Connection Manager は、ラボベースのリモートデスクトップでトレーニングするチームのために、更新、保護、アクセス提供用の内部システムを簡素化しました。そのセキュリティとスピード感がメーカーのトレーニング環境を一変させました。研修生が必要とするのは、ウェブブラウザと URL、ログインクレデンシャルのみとなりました。

KEEPER CONNECTION MANAGER

データシート
リモートデスクトップとサーバーアクセス

ユーザーがどこにいても、完全なリモートデスクトップを体験できます。ゼロトラスト、ゼロ知識セキュリティと世界水準のサポートで支えられています。

Keeper Connection Manager が従来のリモートデスクトップソリューションよりも安全である理由は?

- すべてのトラフィックは、安全な認証済みゲートウェイを通過します。デスクトップが公共のインターネットに公開されることはありません。ゼロトラスト原則に基づき、許可された認証済みの接続のみが許可されます。
- すべてのデスクトップ機能は、企業のファイアウォールの内側で実行されます。リモートユーザーは、企業ネットワーク上のオフィス内で作業しているのと同じ保護を受けることができます。
- クライアント証明書と多要素認証により、さらに強固なセキュリティを実現できます。
- Keeper Connection Manager は最小特権の原則に基づいて動作するよう設計されています。アクセス権は、Keeper Connection Manager によって自動的に作成されるユーザーとグループ、および厳格なファイル許可を通じて慎重に委任されます。
- エンドユーザーは、ブラウザから安全なセッションを介してリモートデスクトップと通信します。パフォーマンスを妨げることなく、エンドユーザーとゲートウェイ間のトラフィックを暗号化するためのシンプルで効果的な方法です。
- エンドユーザーにログインクレデンシャルを公開することなく、特権的なシステムへのアクセスを許可することができます。
- RDP、SSH、VNC、K8s、MySQL のエンドポイントと連携します。

使用事例	Keeper Connection Manager
ウェブベースのアクセス	✓
多段階認証	✓
エージェントレスアクセス	✓
複数のデータストア	✓
ゼロ知識セキュリティ	✓
ゼロトラストフレームワーク	✓
セッションの記録	✓
パスワードレス認証	✓
マルチプロトコルのサポート	✓
Keeper Secrets Managerとの統合	✓

Keeper Security, Inc. 情報

Keeper Security, Inc.（Keeper）は、パスワード関連のデータ漏洩やサイバー脅威を防止するための、市場をリードする最高評価のサイバーセキュリティプラットフォームです。Keeper のゼロトラスト、ゼロ知識のセキュリティおよび暗号化ソフトウェアは、世界中の何百万人もの人々と何千もの企業に信頼されています。Keeper は PC Magazine の年間最高パスワードマネージャーとエディターズチョイス、PCWorld のエディターズチョイスに選ばれ、複数の G2 Best Software Award を受賞しています。Keeper は SOC-2 と ISO 27001 認証を受けており、System for Award Management（SAM、アワードマネジメントシステム）を通して米国連邦政府による使用リストにも選ばれています。詳細は **https://keepersecurity.com** からご覧ください。