KEEPER

Keeper サイバーエッセンシャル

Keeperでサイバーエッセンシャル要件を簡単に満たす

サイバーエッセンシャルは、英国政府が支援するサイバーセキュリティ認証で、組織がオンライン上の脅威から身を守るための基準を提供するもので、サイバーセキュリティに不可欠な対策を網羅しています。サイバーエッセンシャル・プラスは、効果的な防御をより確実にするため、実地検証を含むより厳格な評価を行う上級認証を指します。どちらの認証も、サイバーセキュリティのベストプラクティスと全体的なレジリエンスの強化に取り組んでいることを示すものです。

Keeper Security の主要なサイバーセキュリティソリューションを活用することで、あらゆる規模の組織が簡単かつ手頃な価格でコンプライアンス過程を合理化し、全体的なセキュリティ体制を改善することができます。

要件	解決策
総当たりパスワードの推測からの保護	組織は、総当たり攻撃、別名ブルートフォース攻撃から保護するために、一定回数失敗した後にアカウントをロックしたり、指定された時間内に許可される推測回数を制限したりするなど、いくつかの規制を遵守する必要があります。 Keeperは、ユーザーがマスターパスワードを入力する前に二要素認証（2FA）を要求することで、これらのタイプの攻撃に対する究極の保護を提供します。このレベルの認証は、許可されたユーザーのみがKeeperのデジタル保管庫にアクセスできることを保証します。
パスワードの長さを最低8文字に設定する	サイバーエッセンシャルは、組織に対して最低でも8文字のパスワードの長さを設定するように求めています。 デフォルトでは、Keeperはマスターパスワードに12文字の長さを必要とします。Keeper管理者は、パスワードの長さと必要な文字の種類を組み合わせて、パスワードの最小複雑度を設定することができます。
パスワードの長さの上限を設定しない	サイバーエッセンシャルは、組織がパスワードの文字数制限を設けないことを義務付けています。 Keeperのパスワードジェネレータは100文字までのパスワード作成をサポートしています。
漏えいが判明した場合、または疑われる場合は、速やかにパスワードを変更する	パスワードが破られる可能性がある、あるいはその疑いがある場合、パスワードは迅速に変更する必要があります。ユーザーのパスワードが侵害されたり、盗まれたり、ダークウェブで販売されたりすると、組織は深刻な事態に直面します。 BreachWatch は Keeperパスワードマネージャーに追加できる強力なダークウェブ監視ツールです。BreachWatchはダークウェブ上で公開されたパスワードをKeeperのデジタル保管庫で常にスキャンし、直ちにユーザーに警告を発し、自分自身と組織を保護します。

要件	解決策
わかりやすく一般的なパスワードを選ばない	推測しやすいパスワードを避けることは、組織のセキュリティ態勢を強化します。さらに、パスワードのランダム化と複雑性の強制も、必須ではないが、セキュリティを大幅に向上させます。 Keeperは、ユーザーが明白なパスワードを選択することに関連するリスクを軽減するために、パスワードジェネレータの使用を組織に要求することをお勧めします。 Keeperのパスワードジェネレータを活用することで、組織は以下のサイバーエッセンシャル要件に準拠することができます： • 好きなペットの名前のような簡単に発見できる情報に基づいたパスワードなど、明白なパスワードを選択しないこと • 一般的なパスワードを選択しない
パスワードを使いまわさない	サイバーエッセンシャルに準拠するために、管理者はユーザーが複数のアカウントで同じパスワードを使用しないことを要求するパスワードポリシーを導入する必要があります。 Keeperは各ユーザーにKeeperデジタル保管庫のセキュリティ監査タブを提供することにより、このポリシーを合理化します。セキュリティ監査はパスワードの強度に関する情報を提供し、パスワードの再利用をユーザーと管理者に通知します。ゼロ知識を維持するために、各セキュリティ監査スコアの概要はエンタープライズ公開鍵で暗号化され、Keeperクラウドに暗号化されて保存されます。
パスワードを安全に保管する場所と方法を定義する	組織は、ユーザーがパスワードを保管する場所と方法を概説し、安全な戸棚に封印された封筒を参照することを義務付けられています。これは時代遅れで安全でないパスワード保護方法です。 Keeperは、すべてのパスワードをパスワードマネージャーに保存することを推奨します。ユーザーはマスターパスワードのみを記憶すればよく、パスワードの使用方法を簡素化し、組織を保護します。