ZJTM190821101

ManageEngine
Password Manager Pro

ベストプラクティスガイド

www.passwordmanagerpro.com

内容

1.0 概要

1.1 Password Manager Proについて

Password Manager Proは、情報システム部門やヘルプデスクがパスワード、SSHキー、SSL証明書などの特権IDを管理できるだけでなく、単一のコンソールから重要な情報システムへの特権アクセスを制御および監視できるWebベースの特権ID管理ソリューションです。また、特権アクセス制御を義務付けるPCI DSS、NERC CIP、SOXなどの規制への準拠を証明するのにも役立ちます。

1.2 ガイドについて

このガイドでは、エンタープライズネットワーク環境でPassword Manager Proをセットアップして使用するためのベストプラクティスについて説明します。世界中の企業がPassword Manager Proを正常に展開し、特権IDのアクセス管理を合理的に支援する経験から生まれたこのIT管理者向けガイドでは、迅速かつ効率的なソフトウェアセットアップと安全な特権アカウント管理の実装について説明します。　製品のインストール、構成、展開、およびメンテナンス。すべての段階でベストプラクティスを採用できます。以下では、データセキュリティ、スケーラビリティ、およびパフォーマンスに重点を置いて説明します。

2.0 推奨されるシステム構成

2.1 最小システム要件

Password Manager Proをインストールする前に、システム構成を決める必要があります。Password Manager Proを実行するための最小システム要件については、こちらをご覧ください。

一般に、パフォーマンスとスケーラビリティは以下の要因に依存します。

- ユーザーとグループの数。
- リソースとグループの数。
- リソースまたはパスワード共有の頻度。
- スケジュールされたタスクの数。

上記の要因に基づいて、中規模および大規模企業には以下のシステム設定が推奨されます。

中規模企業

ユーザー数：100-500

リソース/パスワードの数：10,000まで

- デュアルコアプロセッサー以上
- 8 GB RAM
- 40 GBのハードディスク容量

大規模企業

ユーザー数：500以上

リソース/パスワードの数：10,000以上

- クアッドコアプロセッサー以上
- 16 GB RAM
- 100 GBのハードディスク容量

注記：優れたパフォーマンスとセキュリティの強化されたハイエンドサーバーにPassword Manager Proをインストールすることをお勧めします。

3.0 インストール

3.1 Windows対Linux

Password Manager Proは、Windows、Linuxどちらにもインストールできます。ソフトウェアは両方のプラットフォームで等しく実行されますが、Windowsにインストールすると、以下の固有の利点が得られます。

Active Directory（AD）との統合：WindowsにインストールしたPassword Manager ProをActive Directoryと直接統合して、ユーザーとグループをインポートできます。さらに、ドメインアカウントの認証情報でWindowsシステムにログインしているユーザーは、シングルサインオン（NTLM-SSO）によりPassword Manager Proに自動的にログインできます。Active Directoryサービスを Linuxで使用する場合、LDAPベースの認証に依存する必要があります。

Windowsリソースのパスワードのリセット：WindowsにインストールされたPassword Manager Proでは、インターネットに接続されている限り、サポートされているすべてのターゲットシステムに対してエージェントレスモードでパスワードリセットを実行できます。一方、Linuxでは、すべてのWindowsリソースにエージェントを展開し、ドメインコントローラーがWindowsドメインアカウント、サービスアカウント、およびローカルアカウントのパスワードをリセットする必要があります。

さらに、Windowsのサービスアカウント、スケジュールされたタスク、IIS Web.Configファイル、およびIISアプリのプールアカウントにおけるパスワードのリセットは、Windowsにインストールされたパスワード Password Manager Proからのみサポートされます。

3.2 バックエンドデータベース

Password Manager Proは、PostgreSQLデータベースとMS SQL Serverのバックエンドサポートを提供しています。本製品にはデフォルトでPostgreSQLデータベースがバンドルされており、中小企業に最適です。一方、大企業では、スケーラビリティ、パフォーマンス、クラスタリング、および障害復旧を最適化するために、MS SQL Serverをバックエンドとして使用することを強くお勧めします。

MS SQL Serverをバックエンドとして使用している場合は、以下の方法をお勧めします。

- Password Manager Proは、有効な証明書構成を使用してSSL経由でのみMS SQL Serverと通信できます。したがって、既存のデータベースとの競合や混乱を避けるために、Password Manager Pro専用のSQLインスタンスを用意することをお勧めします。

- MS SQL Serverをバックエンドとして使用している間、データベースレベルの暗号化を確保するために一意のキーが自動生成され、デフォルトでは、このキーは<PMP HOME/conf>ディレクトリの<masterkey.key>という名前のファイルに保存されます。不正アクセスから保護するためにキーファイルは別の場所に移動することをお勧めします。このキーファイルは、高可用性構成と障害復旧に必要であるため、安全性の担保が重要です。キーを失うと、MS SQL Serverを再構成する必要があり、データが失われる可能性があります。

- MS SQL Serverをバックエンドとして構成する際は、SQLローカルアカウントではなくWindows認証を使用します。

- SQLサービスとSQLエージェントサービスを実行できるように、同じドメインアカウントを使用してPassword Manager ProサーバーとMS SQLサーバーの両方を実行することをお勧めします。

- すべてのクライアントがこのSQLインスタンスに接続できるようにするには、強制暗号化オプションを有効にする必要があります。これが完了すると、すべてのクライアントからサーバーへの通信が暗号化され、暗号化をサポートできないクライアントはアクセスを拒否されます。

- MS SQLサーバーが実行されているマシンでTCP/IP以外のすべてのプロトコルを無効にします。

  SQLインスタンスを非表示にすることで、他のツールで列挙されないようにし、Password Manager Proのサービスアカウントを除く他のすべてのユーザーに対してこのデータベースへのアクセスを無効にします。

- MS SQLサーバーが実行されているマシンの必要なポートにのみアクセスを許可するようにファイアウォールのルールを設定します。

3.3 インストールマスターキーの保護

Password Manager ProはAES-256暗号化により、パスワードやその他の機密情報を保護します。暗号化キー（pmp_key.key）はインストールごとに別個に自動生成されます。このキーはデフォルトで<PMP HOME/conf>ディレクトリにある<pmp_key.key>ファイルに保存されます。このキーのパスは、「PMP HOME / conf」ディレクトリにある「manage_key.conf」ファイルで設定する必要があります。
Password Manager Proは、起動する際にpmp_key.keyファイルを読み取れるように、必要な権限を所持してこのフォルダーにアクセスできる必要があります。正常に起動した後はファイルにアクセスする必要がなくなるため、ファイルを含むデバイスをオフラインにすることができます。このキーを別の安全な場所に移動し、Password Manager Proのサービスアカウントに読み取り専用アクセスを付与することでキーをロックダウンすることを強くお勧めします。また、ソフトウェアが起動時に暗号化キーを読み取れるように、「manage_key.conf」ファイルでこのリモートパスを更新します。このキーは、USBドライブまたはディスクドライブに保存することで保護することもできます。セキュリティの強度を確保するには、このキーをコピーするためにスクリプトファイルを読み取り可能な場所に作成し、サービスの起動時にかかるコピーを破棄します。

3.4 データベースの認証情報の管理

AES暗号化とは別に、Password Manager Proのデータベースは個別のパスワードで保護されます。パスワードは、自動生成され、インストールごとに一意です。このデータベースパスワードは暗号化されており、Password Manager Proへ安全に保存できます。また、製品サーバーによってアクセスされる他の安全な場所にパスワードを保存するオプションもあります。

デフォルトでは、JDBC URL、ログイン認証情報、およびその他のパラメーターなどのデータベース情報は、「database_params.conf」というファイルに保存されます。このファイルは以下のディレクトリにあります：<PMP HOME/conf>
データベースはリモート接続を許可しないように設定されていますが、このファイルを安全な場所に移動し、アクセスを制限し、Password Manager Proのサービスアカウントでのみ使用できるようにすることをお勧めします。

- このファイルのパスは、<PMP HOME/conf>ディレクトリにある「wrapper.conf」ファイルで構成されます。このファイルを編集して、以下の行を検索します：

  `wrapper.java.additional.9=-Ddatabaseparams.file.`

- Linuxの場合、<PMP HOME/conf>ディレクトリにある「wrapper_lin.conf」ファイルを編集する必要があります。

- デフォルトのパスは、「./../conf/database_params.conf」として設定されています。「database_params.conf」ファイルを安全な場所に移動し、上記のファイルでそのパスを指定します。

  例：`wrapper.java.additional.9=-Ddatabaseparams.file=\\remoteserver1\tapedrive\sharedfiles`。

- ファイルを保存し、Password Manager Proを再起動して変更を有効にします。

注記：上記の手順は、PostgreSQLおよびMySQLにのみ適用されます。MS SQLサーバーをバックエンドとして使用している場合は、セクション3.2を参照してください。

4.0 サーバーおよび環境設定

4.1 サーバー強化

デフォルトでは、Password Manager Proが機能するために必要なすべてのコンポーネントはインストールディレクトリ（ManageEngine / PMP）に保存されています。そのため、Password Manager Proがインストールされているサーバーを強化することを強くお勧めします。実行する必要がある基本的な手順の一部は以下のとおりです。

- ドメイングループポリシーを使用して、組織内すべてのドメインユーザーに対してサーバーへのリモートアクセスを無効にします。すべての管理者の読み取り権限を制限し、1人または2人のドメイン管理者のみにPassword Manager Proドライブまたはディレクトリへの書き込み権限を付与します。

- 着信および発信トラフィックを保護するために、着信および発信ファイアウォールを設定します。この設定を使用して、どのサーバーポートを開く必要があるかを指定することもできます。リモートパスワードリセットなどのさまざまなパスワード管理操作を実行するために使用します。

4.2 専用のサービスアカウントの使用

ドメインコントローラーでPassword Manager Pro用の別のサービスアカウントを作成し、Password Manager Proのすべての領域で使用します。Password Manager Proの実行にも同様のアカウントが使用されます。Password Manager Pro用に作成されたサービスアカウントの使用を開始するには、Password Manager Proがインストールされているサーバーのサービスコンソール（「services.msc」）に移動し、Password Manager Proのプロパティに移動します。作成されたサービスアカウントで構成済みのローカルシステムアカウントを変更します。この同じサービスアカウントを使用して、Active Directoryからユーザーとリソースをインポートすることもできます。

4.3 Webサーバー用のバインド化IPアドレスの構成

デフォルトでは、Password Manager Proのウェブサーバーは、アプリケーションがインストールされている利用可能なサーバーすべてのIPアドレスにバインドします。このため、Password Manager Proは、構成されたポート（7272）を持つ任意またはすべてのIPアドレスで到達可能です。これを制限するには、単一のIPアドレスにバインドし、そのIPアドレスのみから着信通信を受信するようにWebサーバーを構成することをお勧めします。以下の手順を使用して、バインドされたIPを構成できます。

- Password Manager Proが実行されている場合は停止します。
- 「<PMP_HOME>\conf」フォルダーにある「server.xml」ファイルを開きます。
- 以下の行を検索します：

- 上記の行で、「port=”7272”」の値の隣りに、「address=”127.0.0.1”」の属性を追加します。「127.0.0.1」を、バインドに使用するサーバーの実際のIPアドレスに置き換えます。

4.4 IPアドレスのブラックリストまたはホワイトリストによるWebサーバーアクセスへの制限

Password Manager Proは、接続されている限り、どのクライアントシステムからでもアクセスできます。そのため、Password Manager Proにアクセスできるクライアントシステムの数を制限してプロビジョニングすることをお勧めします。IPベースの制限を設定するには、**管理 >> 設定 >> IP制限 >> Webアクセス**に移動します。IP制限は、定義済みのIP範囲や個々のIPアドレスなど、さまざまなレベルと組み合わせで設定できます。特定のIP範囲とアドレスへのWebアクセスを許可したり、IPアドレスを「ブロックするIPアドレス」フィールドに追加してアクセスを制限したりすることができます。

5.0 ユーザーのオンボーディングと管理

5.1 認証とプロビジョニングにAD/LDAP統合を活用

Password Manager Proを、Active DirectoryやLDAPコンプライアントディレクトリと統合することで、以下のような利点を実現することができます：

ユーザープロビジョニング、またはデプロビジョニング：AD/LDAP統合により、Password Manager Proにおけるユーザーの追加が、迅速かつ簡単になります。統合すると、ディレクトリからPassword Manager Proへと、ユーザープロファイルや、グループ、OUを直接インポートすることができます。さらに、商品におけるユーザーアカウントのプロビジョニングプロセスがシンプルになります。例えば、「データベース管理者」の既存OUをディレクトリからPassword Manager Proへインポートする場合、データベースパスワードをインポート対象のグループに簡単に割り当てることができます。

さらに、Password Manager Proとディレクトリを統合するときに同期を有効化することで、OUでのユーザーの追加・移動などのあらゆる変更が自動でPassword Manager Proに反映されるようになります。また、Password Manager Proをディレクトリと同期することで、あるユーザーが各ユーザーディレクトリから完全に削除されたときに、通知を受けることもできます。Password Manager Proは、そのようなユーザーアカウントを無効化・ロックして、メールやアラートで通知します。そして、その通知時に、それらのアカウントを削除または再度、有効化するか選択することができます。

Active Directory認証：もう一つの利点は、ディレクトリの各認証メカニズムを活用して、ユーザーにシングルサインオン(SSO)オプションを提供できるということです。このオプションを有効にすると、ユーザーは、ディレクトリにおける自身の認証情報でシステムにログインしている限り、Password Manager Proで自動的に認証されます（NTLMベースの認証により）。ADの認証情報をPassword Manager Proの認証に使用することで、ユーザーがディレクトリから直接認証を行うため、ログインパスワードがPassword Manager Proに保存されないようにできます。

5.2 ローカル認証の無効化

Password Manager ProをAD/LDAP準拠したディレクトリと統合した後は、ローカル認証を無効にして、ユーザーが自身のAD/LDAP認証情報を使ってPassword Manager Proにログオンするように促すことを推奨します。ローカル認証を無効にするには、**管理 >> 設定 >> 全般設定 >> ユーザー管理**に移動します。

ただし、緊急アクセス目的でPassword Manager Proのローカルアカウントを構成した場合、ローカル認証を無効にすることはできません。そのような場合でもAD/LDAP認証のみを使用したいのであれば、その選択から、**「パスワードを忘れた」**オプション（Password Manager Proのすべてのユーザーがローカル認証パスワードをリセットするためのオプション）を無効にすることを推奨します。このオプションを無効にすることで、ローカル認証が有効な場合でも、ユーザーはAD/LDAPの認証情報によってのみPassword Manager Proにログインできるようになります。

5.3 2要素認証の使用

ユーザー認証の安全性を高めることで、不正なユーザーが機密リソースにアクセスできないようにしましょう。Password Manager Proは、製品のウェブインターフェイスへのアクセスを提供する前に、2段階目の認証方法を構成するために複数のオプションを提供しています。2段階目のオプションとしては、電話認証、RSA SecurIDトークンによる認証、Duo Security、Google Authenticator、メールによる固有のパスワード、RADIUS認証、YubiKeyなどが含まれています。ユーザーのために2要素認証を構成することを強く推奨します。

5.4 職責に基づいたユーザーの役割を割り当てる

ユーザーを追加したら、適切な役割を割り当てましょう。Password Manager Proには、事前設定された4種類のユーザーの役割、すなわち、管理者、パスワード管理者、パスワード監査役、パスワードユーザーがあります。各役割の権限については、ヘルプ文書をご覧ください。

管理者の役割は、以下を実行する必要のある一部のユーザーにのみ限定する必要があります。その役割とは、ユーザー管理操作、商品レベルの構成、パスワード管理です。

スーパー管理者の役割：Password Manager Proにおけるスーパー管理者は、保存されたすべてのパスワードにアクセスできます。緊急目的で使用するための専用のアカウントが必要な場合、組織のスーパー管理者を作成することができます。セキュリティのことを考えると、この役割は、組織の階層構造における最上位のユーザーにのみ限定する必要があります。また、そのような場合のベストプラクティスは、スーパー管理者を1人だけ作成 することです。 管理者がスーパー管理者に昇格されると、そのスーパー管理者は、必要に応じて、その後のスーパー管理者の作成を却下することができるようになります。これは、スーパー管理者が**管理 >> 認証 >> スーパー管理者**に移動して、**管理者によるスーパー管理者の作成を拒否**することで可能です。

5.5 ユーザーグループの作成

例えば、ユーザーをWindowsの管理者、Linuxの管理者などのグループに組織化。ユーザーのグループ化は、リソースの共有やパスワードの割り当てを行う際に大いに役立ちます。Password Manager ProをAD/LDAPと統合すると、ユーザーグループをディレクトリから直接インポートして、同様の階層構造を使用することができるようになります。

5.6 デフォルトの管理者アカウントの削除

セキュリティ上の理由で、管理者権限を持ったユーザーを追加した後は、Password Manager Proのデフォルト管理者とゲストアカウントを削除することを強く推奨します。

5.7 モバイルアプリとブラウザ拡張機能へのアクセスの制限

デフォルトでは、すべてのユーザーがPassword Manager Proのネイティブモバイルアプリケーションとブラウザー拡張機能にアクセスできます。ユーザーが、職場外のデバイスからパスワードにアクセスすることを禁止したい場合は、組織全体におけるモバイルアプリアクセスを無効にしてください。必要ならば、一部のユーザーや管理者にのみアクセスを有効にすることができます。同様に、ブラウザー拡張機能へのアクセスを有効または無効にすることもできます。これらの制限は、**ユーザー >> その他の操作**に移動して、ドロップダウンメニューから**モバイルアクセス/ブラウザー拡張機能の制限**を選択することで可能です。

6.0 データと組織

6.1 リソースの追加：便利な方法の選択

Password Manager Proでパスワード管理を始めるための最初のステップはリソースの追加です。リソース追加を行うための最も迅速で便利な方法は、特権アカウントを自動検出することです。他にも、手動で追加したり、CSVをインポートしたりすることもできます。Password Manager Proに切り替える前に別のツールを使っていた場合や、認証情報をスプレッドシートに保存している場合は、CSV/TSVインポート機能を使用しましょう。

6.2 必ずリソースの種類を選択する

手動またはCSVインポートでリソースを追加するときには、リソースの種類が適切に配列されていることを確認してください。これは、パスワードリセットなどの機能を利用するために必要です。なぜなら、Password Manager Proでは、リソースの種類に応じて、リソースごとに異なる通信手段を使用しているからです。種類を指定していない場合、そのリソースは「不明」として配列され、パスワードリセットを行うことができなくなります。Password Manager Proは、32種のリソースの種類を提供しており、これは、**管理 >> リソースの種類**で確認できます。

6.3 不正な特権アカウントの削除

ITリソースと各特権アカウントをネットワークで整理するために自動検出機能を使用する場合、Password Manager Proは、デフォルトで、ネットワーク上で検出されたリソースに関連付けられたすべてのアカウントを取得します。一部のアカウントは、認証されなかったり、不要だったり、孤立していたりする場合があります。例えば、Windowsのリソースを追加する場合、すべてのゲストアカウントも取得されます。

セキュリティ上の観点から、認証されていないアカウントを、特定し、削除することで、将来における想定外の脆弱性を回避することができます。パスワード管理のベストプラクティスとしては、特権アカウントの数を最小限に押さえなければなりません。さらに、不要なアカウントが棚卸できていない状況など、データの整理を困難な業務とする一因になっています。そのため、Password Manager Proで自動検出を実行する前に、対象の端末そのものにおいて、これらの不要なアカウントを削除することを推奨します。

6.4 リソース検出後のパスワードのランダム化

リソース検出とアカウントの精査を終えたら、すべてのアカウントのパスワードをランダム化することを強く推奨します。Password Manager Proを配備する前に、従業員が、スプレッドシートやテキストファイルなどにパスワードを保管していたり、紙に書き写している可能性もあるため、このランダム化は重要な作業です。パスワードを変更しなかった場合、これらの従業員は、外部からリソースに直接アクセスすることが可能になります。そのため、パスワードを適切にランダム化する必要があります。さらに、ランダム化することで弱いパスワードを取り除き、固有で強固なパスワードをリソースに割り当てることもできます。検出されたアカウントのパスワードのランダム化は、**リソース >> 特定のリソースを選択 >> リソース操作**（上部） **>> 構成 リモートパスワードリセット**から行うことができます。

注記：後から検出された新規アカウントへ事前に設定したパスワードのランダム化を行いたい場合、**リソース >> 特定の リソースを選択 >> リソース操作** （上部） **>> アカウントの検出** から、新しいウィンドウで**検出後にパスワードのランダム化**を有効にしてください。

6.5 リソースグループの力の活用

Password Manager Proではリソースグループが非常に強力です。パスワードの自動割当や、パスワード変更のスケジュール設定など、高度なパスワード管理操作の大半は、リソースグループレベルでのみ行うことができます。リソースグループ作成には2種類の方法がありますが、「条件ベース」のグループを強く推奨します。

条件ベースのグループは、基本的に動的なグループです。これにより、複数の条件を満たしたリソースを1つのグループに柔軟にまとめることができます。そして、条件を設定すると、Password Manager Proが条件に合致するすべてのリソースを自動で特定してグループを作成します。手動での操作は必要ありません。

6.6 ネスト済みリソースグループを使用し、部門に基づいてリソースを注文

膨大なデータベースから1つのリソースを取得する際の使用と閲覧を簡易化するために、Password Manager Proでは、エクスプローラーツリー式の表示設定を活用することができます（例えばネスト済みリソースグループの作成）。表示されるツリーは、ユーザーごとに異なります。このツリー表示設定を有効にすることで、組織全体で統一されたエクスプローラーツリーを表示することができます。有効にした後は、メインノードの名前を「リソースグループ」からあなたの組織の名前に変更しましょう。さまざまなチームや、部署に応じて、複数のサブノートがこの下に作成されます。また、チームまたは部署のサブノートの下には、そこに属するリソースグループを割り当てることができます。

上記のようにエクスプローラーツリーを操作することで、簡単にアクセスすることのできる、明瞭な階層構造のリソースグループを作成することができるのです。エクスプローラーツリーの操作を可能にするためには、**管理 >> 全般設定 >> パスワード取得に移動して、「すべての管理ユーザーに、エクスプローラーツリーの操作を許可」**してください。

6.7 簡単な参照と検索のための追加フィールド

リソースを追加するときに、追加フィールドを使用して、カスタム列と値を作成することができます。追加フィールドは、条件ベースのグループを作成したり、特定のリソースやパスワードを検索したり、リソースを共有したりするときに便利です。例えば、あなたの組織には3段階のIT管理者がいるとします。そこで、**「アクセスレベル」**というタイトルの追加リソースフィールドを作成することで、リソースを「レベルI/II/III」に簡単に分類することができるようになります。作成時に**「アクセスレベル」**のフィールドがあれば、3種類の異なるリソースグループを作成することができるのです。同様に、3種類のユーザーグループを作成して、各グループに、異なるレベルのユーザーを所属させて、「レベルI」のリソースを「レベルI」のユーザーに割り当てるなどの操作が可能になります。

7.0 パスワードの共有と詳細な制限

7.1 様々なアクセス特権でのパスワードの共有

リソースを共有するときに、パスワードの所有者は、以下の権限のいずれかを選択することで、ユーザーとグループに対してさまざまな権限を付与することができます：

- **パスワード閲覧**：ユーザーはパスワードにアクセスできるのみです。
- **パスワード変更**：ユーザーは共有パスワードにアクセスし、変更できます。
- **フルアクセス**：ユーザーはリソースまたはグループを完全に管理し、リソース、グループ、個人アカウントのパスワードを再共有することができます。

ユーザーに対しては「パスワード閲覧」権限のみを提供すればパスワードに関連する様々な操作を十分に行うことができるために推奨しています。「フルアクセス」権限を提供する場合、パスワードに対する「フルアクセス」権限を有するユーザーは共同所有者となり、パスワード変更、削除、他のユーザーと再共有することができるようになるため、細心の注意を払う必要があります。

注記：これらの共有権限以外にも、パスワードをプレーンテキストで開示することなく共有することもできます。これは、リソースの自動ログインが有効な場合に可能です。　この機能の詳細については、セクション10.1を参照してください。

7.2 リソースグループの使用によるユーザーグループの共有

Password Manager Proでは、単一のパスワードやリソースをユーザーまたはグループと共有することができますが、ベストプラクティスは、ユーザーグループとリソースグループを共有することです。この方法は、一括操作を効率的に実行し、時間を節約したいときに最適です。例えば、あなたの組織のWindows管理者に、すべてのWindowsリソースへのアクセス権限を提供したい場合、その操作を2段階の単純な手順で完了することができます：

- 条件ベースのリソースグループを作成します（「Windows」のリソース種類を一致条件として）。それにより、既存のすべてのWindowsリソースがグループに追加され、その後に作成された新しいリソースが自動的にそのグループに追加されるようになります。

- Windows管理者のためのユーザーグループを作成します。AD/LDAPを統合すると、グループを直接インポートして、ユーザーデータベースを自動で同期できるようになります。それにより、新しいWindows管理者が組織に加わったときに、そのADアカウントをパスワードユーザーグループに直接追加して、新しいユーザーがグループの権限を継承して、Windowsサーバーのパスワードを閲覧できるようにすることができます。

7.3 アクセス制御ワークフローの活用

Password Manager Proにおけるアクセス制御は、リクエストリリースメカニズムであり、ユーザーがパスワードに直接アクセスすることを許可していません。その代わりに、ユーザーは、管理者にアクセス承認のリクエストを行うことができます。この機能は、時間制限アクセス、同時並列制御、使用期間後の自動リセットなどの、リソースに対するさまざまな制限を導入することができます。そのため、この重要なリソース認証の情報に対しては、アクセス制御を有効にすることを強く推奨します。

セキュリティ向上のために、重要なリソースの二重承認を構成して、パスワードを一時的にリリースする前に2人の管理者が承認しなければならないように設定することもできます。この設定は、管理者の認証情報が、組織内の2つの異なる部署によって主に所有されている場合に役立ちます。アクセス制御は、**リソース >> リソース操作 >> アクセス制御の構成**から構成することができます。

7.4 ユーザーにパスワード取得の理由を提供するための要求

デフォルトでは、すべてのパスワードに関連した操作が、タイムスタンプとIPアドレス情報を完備した状態で、Password Manager Proの監査証跡で把握されます。オプションとして、ユーザーがパスワードアクセスを必要とした理由を入力させることができます。これらの理由は監査証跡に記録され、横断的な検証やフォレンジック調査において使用することができます。そのため、ユーザーがリソースのパスワードを取得しようとしたときには、アクセス制御が構成されているか否かにかかわらず、ユーザーがアクセス権限を要求する妥当な理由を申告するように義務付けることを推奨します。このオプションは、**管理 >> 設定 >> 全般設定 >> パスワード取得**から有効にすることができます。

7.5 Password Manager Proのエンタープライズチケット発券システムへの統合化

Password Manager Proでは、チケットシステムを統合して、自動的に、特権アクセス関連のサービスリクエストを検証することができます。統合により、有効なチケットIDを持つユーザーだけが、認証された特権パスワードにアクセスできるようになります。重要なリソースのパスワード取得に対して、より強固なワークフローを有効化するためには、Password Manager Proをチケットシステムと統合することを推奨します。現在、Password Manager Proは、ManageEngine ServiceDesk Plus On-Demand、ServiceDesk Plus MSP、ServiceDesk Plus、ServiceNow、JIRA Service Deskといつでも統合できるようになっています。Password Manager Proを上記のチケットシステムと統合するには、**管理 >> 統合 >> チケットシステム統合**に移動してください。

8.0 パスワードポリシー

8.1 重要なリソースグループへの個別パスワードポリシーの設定

パスワードポリシーは、文字の複雑性を指定することで、パスワードを強化するのに役立ちます。Password Manager Proでは、異なるリソースグループごとに、さまざまなパスワードポリシーをカスタマイズすることができます。最も機密性の高いリソースが大量にある場合、それらすべてを1つのリソースグループに整理して、非常に厳格な要件を有する個別のポリシーを構成することができます。リソースグループのポリシーは、**グループ >> 特定のグループを選択 >> 一括構成 >> パスワードポリシーを関連付ける**から構成することができます。

8.2 アカウントレベルのパスワードポリシー

通常、各リソースには1個または複数の管理アカウント、およびその他の通常アカウントがプロビジョンされます。これらの特権アカウントを保護するために、重要なリソースの機密アカウントに個別の強固なパスワードポリシーを構成することを推奨しています。
アカウントレベルのパスワードポリシーは、**リソース >> 特定のリソースを選択 >> リソース操作**（上部）**>> パスワードポリシーを関連付ける**から構成することができます

8.3 ポリシーの作成中にパスワードの有効期間を定義

新しいパスワードポリシーを構成する際には、常にパスワードの最長使用期間を設定するように心がけましょう。使用期間を指定することで、Password Manager Proは、使用期間が過ぎたときに、自動でパスワードをリセットするようになります。この項目を入力しなかった場合、パスワードは失効しなくなります。こうした状況はセキュリティリスクの温床になる可能性があります。

9.0 パスワードのリセット

9.1 定期的なパスワードのランダム化

特権アカウントを安全に管理するには、定期的にリセットされる強力でユニークなパスワードを使用する必要があります。加えて、パスワードを少なくとも90日ごとにリセットすることがベストです。これは、PCI-DSSのようなIT規格で定められた一般的な期間です。当社では、パスワードリセットのスケジュール設定機能を使用して、Password Manager Pro内のリソースグループのパスワードを定期的にリセットすることを推奨しています。以下のような場合に自動でリセットされるようにすることが重要です：

- ユーザーがパスワードの使用とチェックをやめた場合。
- パスワードを最初に共有したユーザーの共有権限が撤回された場合。
- パスワードがパスワードポリシーに則って失効した場合。

9.2 最適なパスワードリセットモードの選択

Password Manager Proのパスワードリセットは、以下の2つのモードのいずれかで実行されます: エージェントレス、またはエージェントベース。

エージェントレスモードの場合、Password Manager Proは、直接ターゲットシステムに接続して、パスワードを変更します。パスワード変更を実行するためには、管理者の認証情報を入力する必要があります。より具体的に言うと、WindowsにインストールしたPassword Manager ProからLinuxのパスワードリセットを実行するためには、2つのアカウント、すなわち、ルート権限のあるアカウントと、リモートログイン可能な通常のユーザー権限のアカウントが必要です。

一方、エージェントベースのモードでは、直接の接続がないリソースのパスワードをリセットしなければならない場合、例えば、DMZロケーション、あるいはファイアウォール制限などがあるときに有用です。パスワードリセットを実行するために、Password Manager Proはリモートホストでエージェントを展開し、タスクを実行します。エージェントとアプリケーションサーバー間でのすべての通信はHTTPS上での一方通行なものであり、インバウンドトラフィック用にファイアウォールポートを開く必要はありません。

基本的に、2つのモード間では、エージェントレスモードが最も便利で信頼できるパスワード変更方法であり、リソースに直接到達できる場合でも、パスワードリセット機能を使用することを推奨しています。ただし、以下のような場合にはエージェントベースモードを選択する必要があります：

- 特定のリソースに関して、Password Manager Proで管理者の認証情報が利用できない場合。
- Password Manager Proでリセットに必要なサービスが対象のリソース（Linuxの場合Telnet/SSH、Windowsの場合RPC）で実行されていない場合。
- Password Manager ProはLinuxで実行されていて、Windowsのリソースでパスワードを変更する必要がある場合。
- 互いにファイアウォールを有する2つの環境「A」と「B」がある場合。 そのような場合、Password Manager ProをAの環境にインストールして、環境Aの端末でエージェントレスモードを使用することができます。一方、環境Bの端末にエージェントをインストールして、パスワードリセットを行うこともできます。それにより、ファイアウォールの例外を追加することなく、AとBの両方ですべてのパスワードを管理できるようになります。

9.3 完全な管理ルーティンを達成するためのサービスの再起動

Password Manager Proでは、さまざまなサービスとIISアプリケーションプールを実行するために使用されているWindowsドメインアカウントを、定期的にパスワードリセットして、すべての依存サービスとアプリケーションプールにパスワードを適用することもできます。サービス、タスク、アプリプールで適切にパスワード変更が行われるようにするために、Password Manager Proは、パスワードがリセットされたときの自動再起動オプションを提供しています。この機能の使用は推奨対象です。

10.0 セッションの管理

10.1 ユーザーが遠隔システムに、パスワードを公開することなく自動的にログオンできるよう確保

自動ログオンオプションを使用してリソースにリモート接続した場合、Password Manager Proは、ユーザーが、ワンクリックでそのリソースに直接アクセスできるようにすることで、パスワードをコピー&ペーストする必要をなくします。そのような場合、ユーザーが平文でパスワードを取得する必要がなくなります。
パスワードの平文取得は、**管理 >> 設定 >> 全般設定 >> パスワード取得**から無効にできます。

10.2 重要なセッションをリアルタイムで監視

Password Manager Proは操作画面録画機能を提供しており、これを使って、特権セッションを二重に制御することができます。この機能を使用して、リモートセッションをリアルタイムに監視して、ユーザーのアクティビティを監視する事ができます。基本的に、二重制御は、リモートサポートを提供して、悪質なアクティビティを防ぐのに役立ちます。管理者の場合、アクティブセッションに参加し、監視することで、エンドユーザーに影響を与えることなく、アプリから開始された重要なセッションを追跡することができます。疑わしいアクティビティが検出された場合には、セッションを即座に終了し、特権アクセスの悪用を防ぐことができます。

10.3 記録されたセッションを定期的に消去

デフォルトで、Password Manager Proは、アプリケーションから開始されたすべてのRDP、VNC、SSH、Telnet、SQLセッションを記録します。あなたの組織規模が大きい場合、各セッション記録のリソース範囲が包括的なため、セッション記録がすばやく増加します。一定期間よりも古い記録が必要でない場合、ディスク容量を維持するためにも、それらを削除することを推奨します。また、これらの記録をローカルドライブに保存して、どこでも移動できるようにすることもできます。一方、選択したセッションや特定のセッションチャット履歴を削除したい場合、以下の方法でそれを行うことができます。 **監査 >> 記録されたセッション**に移動して、選択されたセッションの隣にある「**削除**」のアイコンをクリックします。Password Manager Proでは、特定のセッション記録、またはチャットセッションを削除するために、少なくとも2人の管理者の承認が必要ですので、ご注意ください。

11.0 第三者への特権アクセス

11.1 企業システムへの第三者アクセスを管理

ほとんどの場合、請負業者、コンサルタント、ベンダーなどのサードパーティは、さまざまな契約上の義務やその他のビジネスニーズのために企業のITリソースへのアクセスを必要とします。サードパーティに特権アクセスを提供する場合、時間の規定と最小限の**必要な特権で制限された一時的なアクセスのみを提供することをお勧めします。**それに加えて、重要な情報をサードパーティと共有する際に従うべきいくつかの推奨プラクティスは以下になります：

- 請負業者はリソースにリモートで接続するため、Password Manager Proですべてのサードパーティをユーザーとして追加し、Password Manager Proを介してのみターゲットシステムへの直接セッションを確立するよう要求します。

- リソースの自動ログオンを構成した後のベストプラクティスは、パスワードをプレーンテキストで表示せずにログイン認証情報を共有することです。

- また、そのようなリソースのアクセス制御ワークフローを構成します。これは、使用期間の終わりに自動パスワードリセットを含む、パスワードへのアクセス時間制限の実装に役立ちます。

- シャドウセッションを定期的に実行して、悪意のある動作の痕跡を検出し、即座に修復手段を採用します。

- ベンダーとの契約を終了したら、ベンダーがアクセスしたすべてのリソースに対してパスワードリセットを直ちに実行してください。

12.0 データセンターへのリモートアクセス

12.1 ジャンプサーバーの認証情報の共有範囲を制御

通常、直接アクセスはセキュリティの観点から制限されているため、リモートデータセンターのリソースへの接続には時間がかかります。代わりに、管理者とユーザーは、ターゲットデバイスに接続する前に一連のジャンプサーバーを使用して、各段階で手動認証する必要があります。この複数のプロセスにより、ジャンプサーバーごとに個別の認証情報が導入され、ユーザーはその都度データセンター接続を起動する必要があります。これらの場合、ユーザー間ですべての認証情報を回覧することはセキュリティの観点からおすすめできません。

代わりに、Password Manager Proのランディングサーバー構成機能を使用して、ユーザーがPassword Manager Proを介してのみデータセンターに接続するようにします。このアプリケーションは、データセンターリソースへの安全なワンクリック自動アクセスを提供することで、手動認証の必要がなくなります。また、ジャンプサーバーの認証情報の管理も一元化します。

12.2 事前のパスワードエクスポートで、オフラインアクセスの準備

データセンター環境でインターネット接続が許可されていない場合、ネットワークからPassword Manager Proにアクセスできません。その場合、必要なすべてのパスワードを暗号化したHTMLファイルとして事前にエクスポートし、オフラインでパスワードにアクセスします。エクスポートオプションが有効になっている場合、**[リソース] >> [リソースアクション]**（上部）**>> [パスワードのエクスポート]**からファイルをダウンロードできます。

13.0 監査と報告

13.1 定期的な内部監査を促進

Password Manager Proの監査証跡を使用して、特権アカウント操作、ユーザーログオン試行、スケジュールされたタスク、完了したタスクに関するすべてのイベントを即座に記録します。この情報を適切なレポートに変換することにより、定期的な内部監査とフォレンジック調査を促進し、パスワードを使って誰が何を、どこで、いつ行ったかを簡単に発見できます。

13.2 インスタントアラートで選択したアクティビティの記録を保持

Password Manager Proでは、特定のイベントが発生したときに、素早く選択した受信者にメール通知を送信することもできます。このオプションは、ユーザーが何をしているかを常に更新するのに非常に便利です。そのため、新規ユーザー追加、パスワード削除、パスワード共有などの重要な操作にアラートを構成することをお勧めします。運用レベルのメールアラートは、**監査>>リソース監査**（例）**>>監査アクション>>リソース監査**の構成に移動して有効にできます。パスワードレベルのアラートは、**グループ>>アクション>>通知の構成**から有効にできます。

13.3 ダイジェストメールを精査して、受信トレイを整頓

複数リソースのアラートと更新を有効にした場合、メールの受信ボックスが通知メールであふれることがあります。これが発生した場合、1時間ごとの更新が重要でない場合は、統合された通知リストが記載されたダイジェストメールをその日の終わりに受け取ることを選択できます。

13.4 メールのテンプレートの構成

デフォルトでは、Password Manager Proにはメール通知用の特定のコンテンツがあります。ニーズに合わせてテンプレートを構成し、独自のコンテンツをカスタマイズすることをお勧めします。これを行うには、**[管理] >> [カスタマイズ] >> [メールテンプレート]**に移動します。

13.5 管理システムへのsyslogメッセージとSNMPトラップを生成

組織でサードパーティのSIEMツールを使用している場合、Password Manager Proとそのツールを統合できます。この統合により、Password Manager Pro内でアクティビティが発生するたびにsyslogメッセージをツールに送信できます。オプションで、SNMPマネージャをアプリケーションと統合し、SNMPトラップを生成することもできます。これにより、中央の場所から特権アクセスの全体像と全体的なネットワークアクティビティを取得できます。

13.6 定期的なレポートの生成

Password Manager Proは、パスワードインベントリ、有効期限ステータス、ユーザーアクセス頻度、ユーザーアクティビティなどに関する情報をさまざまなレポートによって提供します。時間を節約するために、これらのレポートを手動ではなく、必要なレポートに**レポートスケジュール**機能を使用することをお勧めします。スケジュールが設定されると、指定された間隔でレポートが自動的に生成され、登録済みのメールに送信されます。

13.7 監査記録の消去

すべての操作が監査されると、監査レコードは急速に拡大します。　指定した日数よりも古い監査レコードが不要な場合は、削除することができます。これは、**[監査] >> [ユーザー監査]**（例）**>> [監査アクション] >> [ユーザー監査の構成]**に移動して構成できます。デフォルトでは、消去オプションは無効になり、日数はゼロ（0）に設定されます。

14.0 データの冗長性と回復

14.1 障害復旧の設定

Password Manager Proのデータベースに保存されているデータは非常に重要です。万が一、プロダクションセットアップで問題が発生した場合、すべてのデータが失われる可能性があります。したがって、災害復旧は不可欠です。このアプリケーションは、ライブデータバックアップと、スケジュールされたタスクによる自動定期バックアップの両方のプロビジョニングを提供します。組織に最適な方法を選択してください。
また、バックアップ用に構成された宛先ディレクトリが安全なリモートの場所にあることを確認してください。

14.2 高可用性アーキテクチャを備えたセカンダリサーバーを展開

Password Manager Proの高可用性アーキテクチャは、ダウンタイムに対処し、パスワードへの継続的なアクセスを確保するのに役立つ推奨セットアップです。これは、プライマリアプリケーションサーバーに加えて、Password Manager Proの別インスタンスをセカンダリサーバーにインストールすることで実現されます。職場内に異なるネットワーク（たとえば、フロアごとに個別のネットワーク）がある場合、異なるネットワークにプライマリアプリケーションサーバーとセカンダリアプリケーションサーバーをインストールすることをお勧めします。

一方、異なる場所にオフィスがある場合、高可用性セットアップのベストプラクティスは、本社にPassword Manager Proのプライマリサーバーを構成し、他のオフィスにセカンダリサーバーを展開することです。このようにして、両方の場所の従業員は、サーバーのダウンタイムが発生した場合でも、パスワードへ中断のないアクセスができます。高可用性を設定するには、**[管理] >> [構成] >> [高可用性]**に移動し、Password Manager Proのスタンバイサーバーを構成します。

15.0 メンテナンス

15.1 インストールを最新の状態に保持

Password Manager Proのチームは、機能強化と修正を含むアップグレードパックを常にリリースしています。メジャーアップグレードは四半期ごとに1回リリースされ、マイナーアップグレードは毎月1〜2回発表されることがあります。これらのアップグレードパックには、製品にバンドルされているTomcatウェブサーバー、PostGresSQLデータベース、およびJREの更新も含まれます。最適なパフォーマンスのためにPassword Manager Proのインストールを適切に維持するために、リリースされた時点でPassword Manager Proのアップグレードパックをダウンロードして適用することをお勧めします。アップグレードパックはここからダウンロードできます。

Password Manager Proがインストールされている Windows OSの更新： Password Manager Proサーバーにインストールするwindowsパッチがある場合、以下の手順を実行します：

1. サービスコンソール（services.msc）を開き、Password Manager Proを停止します。
2. Password Manager Proディレクトリ全体のコピーを作成し、バックアップとして他のマシンに保存します。または、サーバーがVMの場合は、スナップショットだけを作成します。
3. 次に、Windows OSを更新します。

15.2 メンテナンスウィンドウを賢く選択

アップグレードパックを適用するには、Password Manager Proを一時的に停止する必要があります。高可用性が構成されている場合、プライマリサーバーとセカンダリサーバーの両方がダウンします。さらに、Password Manager Proの現在の設計では、アップグレードのたびに高可用性を再構成する必要があります。したがって、週末または営業時間外にメンテナンスウィンドウをスケジュールすることを強くお勧めします。

勤務時間中にアップグレードを実行することを避けられない場合は、Password Manager Proの**メッセージボード**を使用して、今後のメンテナンス操作の前にユーザーに警告できます。**メッセージボード**オプションは、**[管理者] >> [管理]**にあります。入力したメッセージをメールまたはオンラインアラートとしてすべてのユーザーに送信できます。

15.3 モバイルアプリとブラウザ拡張機能を定期的に更新

Password Manager Proのネイティブモバイルアプリとブラウザプラグインのアップデートは定期的にリリースされます。アプリとブラウザストアで更新を定期的に確認することをお勧めします。

15.4 セキュリティ勧告の確認

製品にセキュリティの脆弱性が発見された場合、修正はアップグレードパックを通じて直ちに提供されます。セキュリティアドバイザリは、お客様が当社に登録されたメールにも送信されます。

15.5 Password Manager Proインストールを別マシンへ簡単に移動

Password Manager Proのインストールをあるマシンから別のマシンに移動するには、以下の手順に従ってください：

- Password Manager Proを実行している場合は終了します。
- Password Manager Proのインストールフォルダ全体をあるマシンから別のマシンにコピーします。
- その後、サービスをインストールして実行します。このオプションでは、Windowsからプログラムをアンインストール、プログラムコンソールを追加または削除することはできません。再インストールする場合は、インストールフォルダ全体を削除するだけになります。

注意：インストールが正常に機能することを確認するまで、Password Manager Proの既存インストールを削除しないでください。これにより、移動中に災害やデータ破損を克服する必要がある場合に備えて、有効なバックアップを準備できます。

16.0 緊急アクセス規定

16.1 緊急時に備えPassword Manager Proのローカルアカウントを使用

まれにActive Directoryサーバーがダウンすると、ユーザーがロックアウトされる場合があります。これに対処するには、Password Manager Proでローカルアカウントを持つことをお勧めします。

16.2 暗号化HTMLファイルとしてパスワードをエクスポートし、オフラインからアクセス

通常、データセンターなどの制御された環境では、インターネット接続は他のデバイスでは許可されていません。そのような場所でパスワードへのアクセスを確保するために、Password Manager Proはオフラインアクセスを提供します。この機能により、必要に応じてすべてのパスワードを暗号化されたHTMLファイルとして定期的にエクスポートし、ファイルを安全な場所に保存できます。ファイルは、提供された16桁のパスフレーズで暗号化されます。パスフレーズを知っているユーザーのみがオフラインファイルのロックを解除できます。時間間隔（15分など）を指定して、ファイルの自動ログアウトを構成することもできます。これらの設定は、**[管理者] >> [設定] >> [エクスポート/オフラインアクセス]**に移動して構成できます。オンデマンドエクスポートとは別に、**グループ**に移動し、**[アクション]**のドロップダウンメニューから**[定期的なパスワードのエクスポート]**を選択して、リソースグループのパスワードのエクスポート操作をスケジュールすることもできます。毎日、毎週、または毎月など指定した間隔で、エクスポートをスケジュールできます。

17.0 管理者が不在の場合

管理者が不在の場合があるかもしれません。このような場合に備える必要があります。

17.1 イグジットレポートを準備

管理者が組織を離れるとき、最初に組織内での管理者の特権レベルを確認し、関連する脆弱性に対処する必要があります。管理者はIT資産への無制限のアクセスがあるため、このプラクティスは重要です。このような場合、特定のユーザーがアクセスしたパスワードの完全なリストを含むカスタムレポートをPassword Manager Proで生成することをお勧めします。**ユーザー**固有のカスタムレポートを生成するには、**[ユーザー]**に移動し、特定のユーザーを選択して、[レポート]列の下にある**[ユーザーレポート]**アイコンをクリックします。

17.2 リソースの所有権の譲渡

退任する管理者が作成したリソースのリストを取得したら、それらすべてのリソースの所有権を自分またはPassword Manager Proの別の管理者に譲渡します。これを行うまで、アプリケーションで管理者アカウントを削除することはできません。
リソースの所有権を譲渡するには、**ユーザー**に移動し、退任する管理者を選択してから、**[ユーザーアクション]**のドロップダウンメニューから**[所有権を譲渡]**を選択します。

17.3 承認者権限を譲渡

アクセス制御を設定している場合、退職する管理者は特定のリソースの承認者である可能性があります（つまり、Password Manager Proで他のユーザーからのパスワードアクセス要求を処理した可能性があります）。彼らが去るとき、その承認者権限を他の管理者に移すことをお勧めします。承認者権限は以下の方法で譲渡できます：**[ユーザー]**をクリックし、退任する管理者を選択し、**[ユーザーアクション]**の下のドロップダウンメニューから**[承認者権限の譲渡]**をクリックします。

17.4 直ちにパスワードをリセット

セキュリティ違反や不正アクセスの試みを排除するために、これらのリソースの所有権が管理者レベルの権限を持つ別のユーザーに移された直後に、退任する管理者が所有するすべてのリソースのパスワードをリセットすることを強くお勧めします。

18.0 セキュリティ

18.1 常時、すべての通信でSSLを選択

Password Manager Proは、パスワードリセットやリソース追加やインポートなどの機密操作のためにSSLモードと非SSLモードの両方を提供します。セキュリティ上の利点のために、常にSSL通信を選択することをお勧めします。

18.2 スクリプトを安全に実行し、悪意のある入力を防止

Password Manager Proは有害なスクリプトまたはコードを識別し、それらの実行を防止するように構成されます。さらに、HTMLタグと属性を含むスクリプトの実行も禁止します。このオプションは、セキュリティを強化するためのベストプラクティスとして強く推奨されているため、無効にしないでください。正規のスクリプトを実行する必要がある場合は、このオプションを一時的に無効にし、タスクの完了後直ちに有効にしてください。

18.3 無活動タイムアウトを構成

ユーザーがワークステーションから離れたときにウェブインターフェースが継続的に接続していることは、セキュリティの観点から危険です。デフォルトでは、Password Manager Proのウェブセッション自動ログアウトは30分に設定されます。安全のために、15分以下に設定することをお勧めします。無活動タイムアウトを構成するには、**管理者>>設定>>一般設定>>ユーザー管理に移動します。**

18.4 ブラウザ拡張機能の自動ログアウトを構成

ブラウザ拡張セッションをアクティブのままにする期間を選択できます。セキュリティを最大限に高めるために、15〜30分後に自動ログアウトを設定することをお勧めします。ログアウト期間は、ブラウザ拡張機能の**[設定]**で構成できます。

18.5 オフラインアクセス：パスワードのエクスポートを無効化

Password Manager Proは、プレーンテキストのスプレッドシートファイルや暗号化されたHTMLファイルなど、安全なオフラインアクセスのための複数エクスポートオプションを提供します。ユーザーがパスワードを暗号化されたHTMLファイルとしてのみエクスポートできるようにすることを常にお勧めします。ユーザーがパスワード情報をCSVファイルでエクスポートできるようにした場合は、パスワードがプレーンテキストとしてエクスポートされないようにします。これは、**[管理者] >> [設定] >> [エクスポート/オフラインアクセス]**に移動して実行できます。

18.6 IPアドレスのブラックリストまたはホワイトリストによるAPI呼び出しとエージェントアクセスの制限

Password Manager Proを使用すると、API呼び出し、ネイティブモバイルアプリとブラウザー拡張機能からの通信、およびターゲットマシンからPassword Manager Proサーバーへのエージェント通信に対するIPベースの制限を有効にできます。Password Manager Proにアクセスできるクライアントシステムの数を制限してプロビジョニングすることをお勧めします。IPベースの制限を構成するには、**[管理者] >> [構成] >> [IP制限] >> [APIアクセス**（または）**エージェントアクセス]に移動します。**IP制限は、定義済みのIP範囲や個々のIPアドレスなど、さまざまなレベルと組み合わせで設定できます。

19.0 プライバシー

19.1 プライバシー制御

製品内のプライバシーを強化するために、Password Manager Proは、定型レポートの生成プロセスへの個人データの組み込みをカスタマイズおよび制御するのに役立ちます。Password Manager Proで入力した各個人データをレポートのマスクエントリとして使用するか、**管理者>>設定>>プライバシー設定>>プライバシー制御**に移動して完全に削除するかを決定できます。レポートの生成中は、機密性の高いデータをマスクまたは削除することをお勧めします。

19.2 暗号化エクスポート

Password Manager Pro全体のエクスポート操作に追加のセキュリティレイヤーを持たせるには、**[管理者] >> [設定] >> [プライバシー設定] >> [暗号化エクスポート]に移動して、エクスポートファイルの暗号化を有効にすることをお勧めします。**すべてのエクスポート操作で均一に使用されるグローバルパスフレーズを設定するか、ユーザーがエクスポートされたファイルに対して独自のパスフレーズを定義できるようにすることができます。ユーザーは、エクスポートされたファイルを表示するためのパスフレーズを提供する必要があります。