ManageEngine
Password Manager Pro

セキュリティ構成やデータ保管の仕様について

概要

Password Manager Proは、特権アカウントのパスワードを管理し、企業の機密情報やデバイスへの安全なアクセスを提供します。特権アカウントのパスワードのセキュリティが損なわれると、企業が深刻な危機に晒されます。Password Manager Proを利用することで、ユーザー認証、データ転送、ストレージ、ワークフロー利用に対して即座に最大限の安全性を確保することができます。

以下のセキュリティ対策に加えて、当社では、アプリケーションの安全性を高めるための努力を続けています。このドキュメントでは、製品のセキュリティ仕様の詳細を説明します。

様々なレベルのセキュリティ

Password Manager Proは、以下のカテゴリに分類される様々なレベルでデータを保護します。

セキュリティ仕様

保管メカニズム	• AES-256による暗号化 • 2重暗号化（アプリケーションレベルとデータベースレベル） • 暗号化キーと暗号データを別に保管 • FIPS 140-2準拠モード
本人確認と認証	強固なアプリケーションレベルでの認証 • Microsoft AD、LDAP、RADIUS等との連携 • SHA2（SHA-512）アルゴリズムのローカル認証 • スマートカード認証 • SAML 2.0シングルサインオン

データの整合性	**データ転送** • HTTPSによる暗号化 • SSLモードでのクライアント接続 • SSHによるパスワード変更 **データストレージ** • AES-256による2重暗号化 **安全なリモートアクセス** • HTML5に互換性のあるブラウザーからのWindows RDP、SSH、Telnetセッション • 追加のプラグインまたはエージェントソフトウェア不要 • Password Manager Proのサーバー経由でのリモート接続 • パスワード非表示でのリモート接続 • クライアント端末とリモートホスト間での直接接続なし **アプリケーション間のパスワード管理** • HTTPSによるアプリケーション間通信 • SSL証明書による認証 **Web入力画面に対する対策** SQLインジェクション、クロスサイトスクリプティング、バッファオーバーフロー、その他の攻撃に対する保護
アクセス制御	**データアクセスコントロール** • 詳細なアクセス制御設定 • 特権IDの申請/承認ワークフロー **監査証跡** • パスワード変更の定期自動化 • パスワードポリシー違反のレポート出力
監査、アカウンタビリティコントロール、リアルタイムアラート	**検出機能** • 特権IDに関連するアクションのリアルタイムアラート • SNMPトラップやSyslogメッセージの生成、特権セッション記録

可用性メカニズム	**高可用性** • PMPサーバーとデータベースの冗長化 • データベース複製のための待ち時間を含むTCP接続 • 直接到達不可能なネットワークセグメント用のPMPエージェント **オフラインアクセス** • 暗号化HTMLファイル • AES-256による暗号化のためのパスフレーズ設定 **モバイル接続** • iOSとAndroidプラットフォーム用のアプリ • 暗号化キーとしてのパスフレーズ • オフラインアクセス • モバイルデバイスとのデータ同期用の監査証跡
災害復旧	**バックアップ** • データベースの定期的なバックアップ • バックアップファイルの暗号化 **緊急アクセス** • 緊急警報や緊急アクセス用のスーパー管理者アカウント
Webサイトやアプリケーションへの自動アクセス	**ブラウザーの拡張機能** • FirefoxおよびGoogle Chrome、IEの拡張機能 • CSPのベストプラクティス • インラインJavaScriptの実行とAJAXリクエストの防止

目次

セキュリティ仕様 2
1. 保管メカニズム 6
1.1. インストールマスターキー 6
1.2. データベースキー 6
1.3. FIPS準拠モード 6
2. 本人確認と認証 7
2.1. 強固なアプリケーションレベルの認証 - 様々なオプション 7
2.2. 2段階認証 8
3. データの完全性 9
3.1. データ転送 9
3.2. 2重暗号化によるデータストレージ 10
3.3. 安全なリモートアクセス 10
4. アクセス制御 11
4.1. データのアクセス制御 11
5. 監査、アカウンタビリティコントロール、リアルタイムアラート 11
5.1. 検出機能 11
5.2. 監査情報 12
6. Webサイトやアプリケーションへの自動ログイン 12
6.1. ブラウザー拡張機能 12
7. 可用性 13
7.1. 高可用性 13
7.2. オフラインアクセス 13
7.3. モバイル・アクセス 13
8. 災害復旧 14
8.1. バックアップ対策 14
8.2. システム障害と復旧 14
8.3. 緊急アクセス 14
9. 製品のご購入検討に際して 15
9.1. 訪問／製品デモの依頼 15
9.2. セミナーへの参加 15

セキュリティ機能

1.保管メカニズム

1.1. インストールマスターキー

- Password Manager Proは、AES-256暗号化（合衆国政府が承認した強固な暗号化）を使用しています。暗号化キーは各サーバーにインストールしたPassword Manager Proごとに自動生成されます。
- インストールマスターキーをPassword Manager Proのインストールフォルダーと一緒に保管することはできません。暗号化キーと暗号化されたデータを別々に管理することで、安全性が向上します。
- Password Manager Proは、暗号化キーの定期変更もサポートしており、古い暗号化キーを破棄し、新しい暗号化キーを定期的に生成して既存のデータに適用できます。詳細はこちらをご参照ください。

1.2. データベースキー

- Password Manager Proのデータベースは、各デバイスにPMPのインストールごとに生成される個別のキーにより保護されます。
- データベース用のキーはPassword Manager Pro内で安全に保管することができます。
- Password Manager Proでは、安全な場所にデータベース用のキーを保管して、キーへのアクセスをサーバーに限定することができます。
- RDBMSは、常に安全な接続（クライアント接続にSSLモードを強制）のみを受諾しており、クライアントは同じローカルホスト（クライアントが現在操作している手元の端末）からのみ接続することができます。WebサーバーとRDBMSが別のサーバーに存在する場合、設定されたIPアドレスからのみ接続できるように強制できます。

1.3. FIPS準拠モード

- Password Manager Proは、FIPS 140-2準拠モードで動作するように設定できます。

2. 本人確認と認証

2.1. 強固なアプリケーションレベルの認証 - 様々なオプション

Password Manager Proには、アクセスするユーザーを一意に識別するための4種類のオプションを提供しており、セキュリティの向上に繋げることができます。

1. **アイデンティティストアとの連携**：Password Manager Proは、Microsoft Active DirectoryやLDAPディレクトリサービス（Novell eDirectoryやOracle OID）、RADIUSと簡単に連携することができます。ユーザーをアイデンティティストアからインポートし、個別の認証メカニズムを利用して、ユーザーを認証できます。詳細はこちらをご参照ください。

2. **固有のアカウントと強固なローカル認証**：Password Manager Proには、ユーザー用に作成された固有のアカウントによるローカル認証機能が備わっています。ユーザーは、自身の証明書を用いてアクセスすることができます。また、パスワードはSHA2アルゴリズムに従って生成するため、各ログインのパスワードは固有の値となり安全性が確保されます。

3. **共通アクセスカード**：Password Manager Proはスマートカード認証をサポートしています。ユーザーはスマートカードを所持し、本人確認番号（PIN）を覚えておく必要があります。詳細はこちらをご参照ください。

4. **SAML準拠サービス**：Password Manager Proは、SAML 2.0をサポートしており、シングルサインオンに対するフェデレーションID管理ソリューションと連携することができます。サービスプロバイダー（SP）として機能し、 SAML 2.0を使用してアイデンティティプロバイダー（IdP）と連携します。また本連携は、SPに関する詳細内容がIdPに提供され、またその逆も同様に行われます。Password Manager ProをIdPと連携させると、ログインユーザーは、各アイデンティティプロバイダーのGUIに対して、証明書を再提出することなく自動的にログインできるようになります。詳細はこちらをご参照ください。

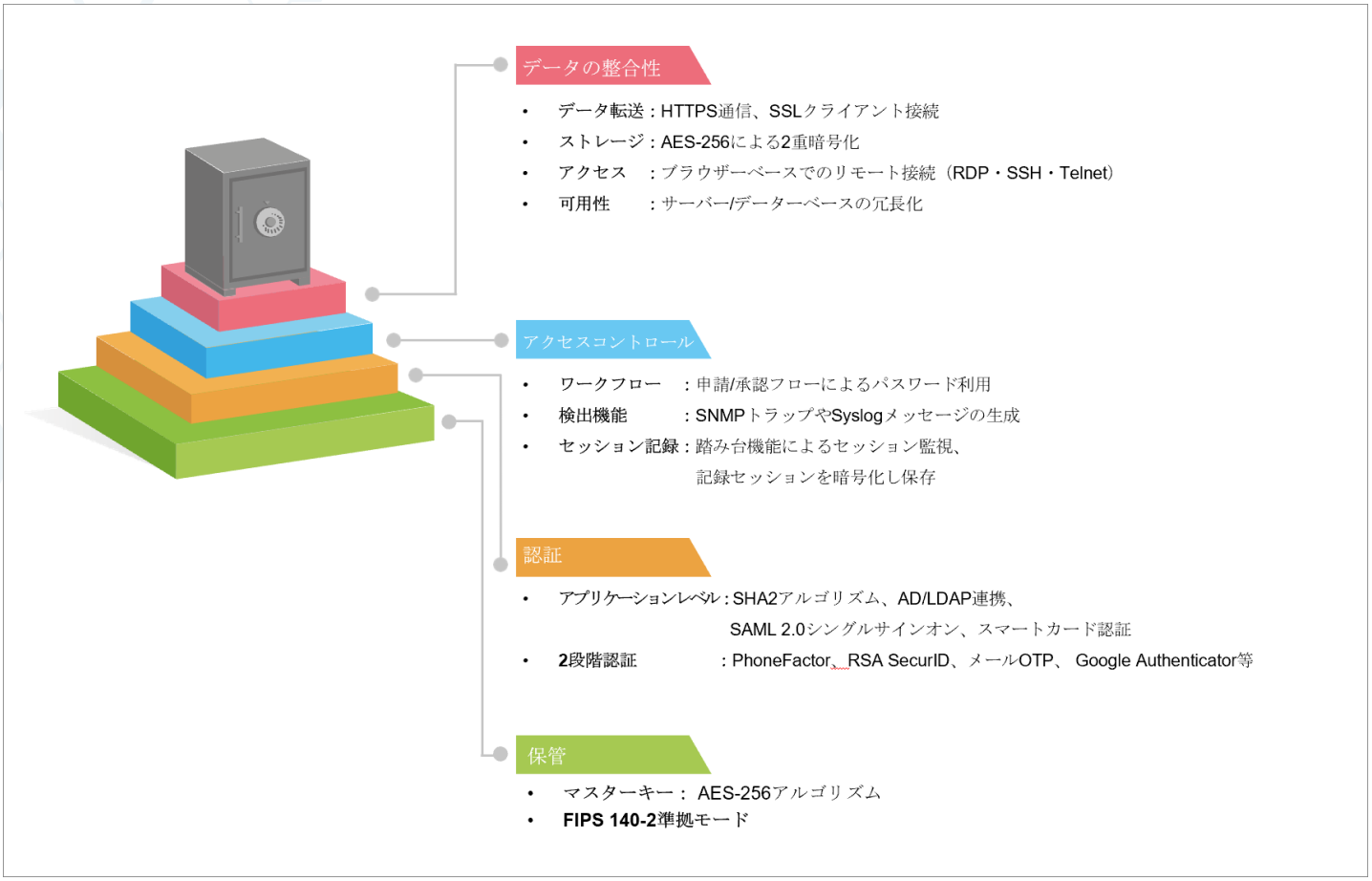

図1. 製品セキュリティ アーキテクチャー

2.2. 2段階認証

Password Manager Proは、セキュリティを補強するために、2段階認証機能を提供しています。2段階認証を設定すると、ユーザーは、Password Manager Proの操作画面にアクセスするために、認証を2回行う必要があります。第2段階の認証は、以下の方法で行います。

1. **PhoneFactor** - 電話を利用した認証サービスで、ログイン処理中に、使用中の端末にかかった電話にでることで、ログインができます。
2. **RSA SecurID** - RSA SecurIDと連携して、60秒ごとに生成されるワンタイム認証トークンを利用します。
3. **固有のパスワードをメール送信** - ユーザーに固有のパスワードを送信して認証に利用します。パスワードは一度、ログインセッションで使用されると失効します。
4. **Google Authenticator** - Googleが開発した時間ベースの数字トークンで、Google Authenticatorのアプリをスマートフォンやタブレットデバイスにインストールして利用します。
5. **RADIUS Authenticator** – VASCO DIGIPASSなどのRADIUS準拠システムを活用して、ワンタイムパスワードを作成します。

6. **Duo Security** - Duo securityの認証を第2段階の認証として活用します。
7. **YubiKey** - YubiKeyを第2段階の認証として、ワンタイムパスワードを生成します。

詳細はこちらをご参照ください。

3. データの完全性

3.1. データ転送

- Password Manager Proのユーザーインターフェイスとサーバー間のすべての通信は、暗号化されたHTTPSで行われます。

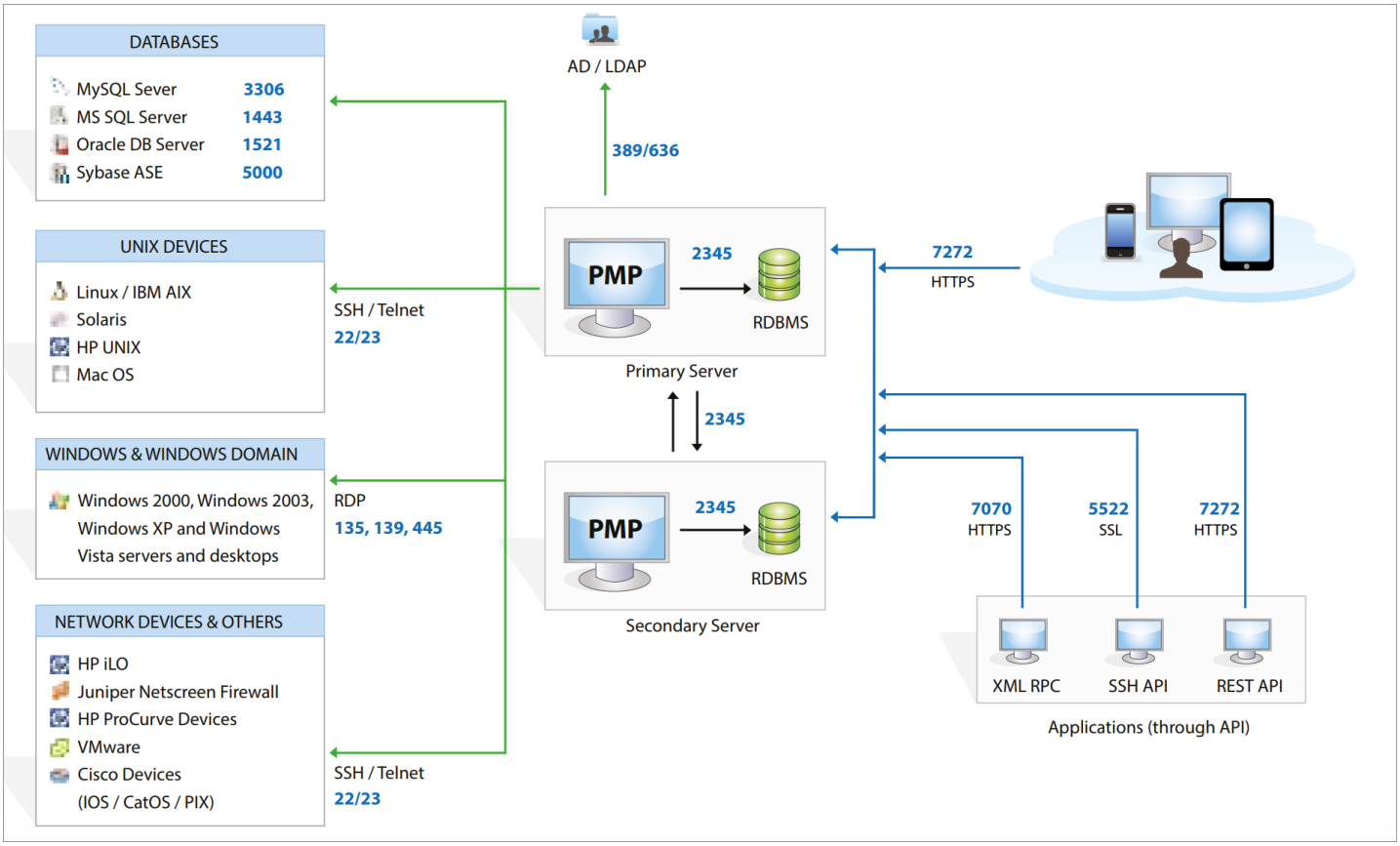

図2. データフローダイアグラム

- Password Manager Proサーバーとデータベース間のすべてのデータ転送はSSLで行われます。
- リモートパスワード変更時は、セキュアなSSHを使用することもできます。
- **Password Manager Proとエージェント間での通信**：Password Manager Proでは、サーバーに接続できるエージェントを提供できます。通信は常に一方向であり、エージェントが接続を開始します。そのため、ファイアウォールのポートを開放したり、VPNの設定を行う必要はありません。エージェントは定期的に、操作（パスワード変更やパスワード認証）の状況を確認します。詳細はこちらをご参照ください。

- **プライマリサーバーとセカンダリサーバー間での通信：**HTTPSを利用した通信で行われます。

3.2. 2重暗号化によるデータストレージ

- Password Manager Proは、WebサーバーとRDBMSがバンドルしたWebアプリケーションとして設計されています。
- 暗号化されたデータは、RDBMSにSQLクエリを使用して保管され、その後、Password Manager ProがRDBMSの組み込みAES機能を使用して、データを2重に暗号化します。
- 特権IDの操作内容は、保管される前に暗号化され、独自の形式で保存されるため、再生するには専用のプレイヤーが必要です。

3.3. 安全なリモートアクセス

- Password Manager Proでは、サーバーにプラグインまたはエージェントソフトウェアを導入しなくても、HTML5対応のブラウザーからWindows RDP、SSH、Telnetセッションを開始することができます。
- ITリソースへのリモート接続は、Password Manager Proを経由するため、クライアント端末とリモート接続先のホスト間での直接接続はしません。
- Password Manager Pro経由でITリソースに接続する場合、パスワードを知ることなくリモート接続が可能です。そのため、安全なリソースセッションを確立できます。詳細はこちらをご参照ください。

4. アクセス制御

4.1. データのアクセス制御

- Password Manager Proにおけるすべてのデータのアクセスは、アクセス制御機能によりコントロールされます。パスワード所有者と共有者を明確にし、ユーザーは利用を許可されたパスワードにのみアクセスができます。
- 機密性の高いITリソースに関しては、管理者からの承認を必須にすることで、セキュリティを強化します。ITリソースのパスワードを使用しなければならない場合は、利用要望を送信して、管理者（要望を承認する担当者）の承認を受けて、一定期間、利用が許可される必要があります。詳細はこちらをご参照ください。
- ユーザーによるパスワードに対するアクション（いつ、誰が、何のパスワードを使用したか）やITリソースに対する操作は、証跡として把握され、すべてのユーザーの操作の説明責任を明確化することができます。
- さらに、ポリシー強制の一環として、ITリソースのパスワードを定期的にランダムで生成されたパスワードに変更することができます。Password Manager Proは、強固な固有のパスワードをITリソースに割り当てることができ、予め設定したポリシーに違反したパスワードをレポート化することも可能です。パスワードポリシー設定により、脆弱なパスワードによって生じるサーバーやアプリケーションへの不正アクセスの防止に役立ちます。詳細はこちらをご参照ください。

5. 監査、アカウンタビリティコントロール、リアルタイムアラート

5.1. 検出機能

- Password Manager Proは、リモート接続、パスワード取得・変更、共有設定の変更、など様々なアクションをリアルタイムで通知することができます。詳細はこちらをご参照ください。
- ユーザーやシステムの操作を記録する監査モジュールでは、SIEMツールに送信する必要のあるイベントを設定できる機能を提供しています。SyslogメッセージまたはSNMPトラップとして送信することが可能です。詳細はこちらをご参照ください。
- 特権IDセッションにおけるユーザーの操作は、Windowsの場合には動画で、他のシステムの場合にはテキストベースで記録され、フォレンジック調査用のため安全に保存されます。
- セッション記録に加えて、管理者には、特権セッションをリアルタイムで監視する機能を提供します。疑わしい操作を確認したら、即座にセッションを中断させることができます。詳細はこちらをご参照ください。

5.2. 監査情報

- Password Manager Pro上で実行したすべての操作やスケジュールで設定した操作タスク設定タスクは監査されます。
- 「誰が」「どんな操作を」「いつ」「どこから行ったか」などの詳細な情報を証跡として取得し、データベースに保存されます。監査ログは改ざん不可能であり、データの完全性が証明されます。
- RDBMSは、常に安全な接続（クライアント接続にSSLモードを強制）のみを受諾するように設定されており、クライアントは現在操作しているデバイスからのみ接続することができます。RDBMSがWebサーバーと別に存在する場合、特定のIPアドレスからのみ接続できるように強制します。

6. Webサイトやアプリケーションへの自動ログイン

6.1. ブラウザー拡張機能

- Password Manager Proは、Firefox、Google Chrome、IE向けに拡張機能を提供します。拡張機能はセキュリティとプライバシーを確保することを念頭に置いて設計されています。
- コンテンツセキュリティポリシー（CSP）のベストプラクティスに則り、コンテンツインジェクション攻撃に対処します。
- XSS攻撃を防止するため、他のサイトへのJavaScriptの実行やAjaxリクエストは無効化されています。
- 以下の状況下では、セキュリティを確保したデータの取得・転送を実行しています。

  1. パスフレーズの検証
  2. サーバーからの暗号化データ取得
  3. パスワードおよびJavaScript変数（外部アプリケーションまたはその他の拡張機能からはアクセス不可能）のようなその他の機密データを保持
  4. その他のデータをバックグラウンドでローカルレコードとして保存
  5. 証明書情報のWebサイトへの提出

- ユーザーがログアウトするか、または一定期間使用されていない場合、ローカルデータは完全に消去されます。

7. 可用性

7.1. 高可用性

- Password Manager Proは、サーバーとデータベースの冗長化により、支障のないパスワードアクセスを実現します。
- 通常はプライマリサーバーにすべてのユーザーが接続し、セカンダリサーバーはスタンバイ状態になります。管理者やユーザーはブラウザー、スマートフォン、タブレットから各サーバーにGUIでアクセスできます。
- プライマリサーバーとセカンダリサーバーは、十分にデータベースを複製することのできる待ち時間を含んだTCP接続があれば、地理的に離れた場所、例えば別の大陸にインストールすることもできます。
- サーバーは、直接TCP接続を確立しているエンドポイントを管理できます。DMZ内やサーバーから直接到達できないネットワークセグメントにある管理対象のシステムについては、エージェントを利用することで管理できます。
- プライマリサーバーとセカンダリサーバー内にあるデータは、同期することができます。データ複製は、暗号化された方法で行われます。

7.2. オフラインアクセス

- Password Manager Proは、オフラインアクセス用に暗号化されたHTMLファイルでパスワードをエクスポートできます。さらに、エクスポートしたファイルをモバイルデバイスに同期することも可能です。
- エクスポート前に、ユーザーがAES-256暗号化データを保護するためのパスフレーズを求められます。オフラインコピーは、パスフレーズを入力することでアクセスすることができます。さらに、このパスフレーズはサーバーのどこにも保存することができません。
- ユーザーが共有されたITリソースや特権IDの情報（パスワードやFQDNなどの機密情報）をコピーした場合も監査ログとして記録されます。

7.3. モバイル・アクセス

- Password Manager Proは、iOSとAndroid用のモバイルアプリを提供しています。モバイルアプリは、データのセキュリティを損なうことなく簡単に使用できるように最適化されています。さらに、モバイルアプリにおいてもAES-256で暗号化されます。
- アプリは、暗号化キーとして使用される、ユーザーが最初に登録したパスフレーズによって保護されます。そのため、モバイルデバイスが盗まれた場合でも、管理している特権IDは解読することができません。
- 二段階認証を設定している場合、同じ認証方法をモバイルアプリにも適用することができます。

- ユーザーのログイン状態を保持させず、アプリにアクセスしたときに毎回認証するよう強制します。
- データのオフラインコピーが作成されるたびに、そのデータをユーザーのデバイスに同期します。さらに、同期処理が行われたことも監査証跡に反映させることができます。ユーザーがHTMLファイルを削除すると、同期の一環としてユーザーのデバイスからも削除されます。

8. 災害復旧

8.1. バックアップ対策

- Password Manager Proは、定期的にデータベースのバックアップを取得する機能を提供します。
- バックアップファイル内のすべての機密データは、.ezipファイル形式で暗号化保存され、**<PMP_Home/backUp>**ディレクトリまたは管理者が設定したディレクトリに配置されます。
- Password Manager Proは、バックアップファイルの暗号データと暗号化キーが同じ場所に存在しないよう、バックアップファイルには暗号化マスターキーがありません。暗号化キーがない限り、バックアップファイルから機密データを復号化することができません。
- データベースのバックアップ操作を進行している間、Password Manager Proの設定を変更することはできません。

8.2. システム障害と復旧

- 障害またはデータ損失時には、同じバージョンのPassword Manager Proをインストールし直して、即座にバックアップデータをデータベースにリストアし、復旧することができます。
- バックエンドデータベースとしてのMS SQLサーバー付きのPassword Manager Proにおける障害は、インストール時に最初に使用した暗号化マスターキーでのみ復旧できます。詳細はこちらをご参照ください。

8.3. 緊急アクセス

- 緊急時は、管理者にスーパー管理者権限を与えることで、システム内のすべての情報に無条件でアクセスすることができます。
- 管理者は、自分をスーパー管理者に変更することはできませんが、他の管理者の要望により権限を与えることができます。
- Password Manager Proインターフェースからスーパー管理者を把握できます。

9. 製品のご購入検討に際して

9.1. 訪問／製品デモの依頼

Password Manager Proにご関心を持って頂き、誠にありがとうございます。
ご購入前の設定／評価中に、個別のご相談や提案のご依頼がございましたら次の窓口をご利用ください。首都圏外でも、オンラインで対応が可能です。

■特権ID管理　課題相談　お申込みページ
https://www.manageengine.jp/products/Password_Manager_Pro/consultation.html?security_wp

9.2. セミナーへの参加

Password Manager Pro について、定期的に各種セミナーを開催しております。

セッション後に個別相談会を開催している「対面形式セミナー」の他、忙しい方でもインターネット上でご参加頂ける「Web セミナー」がございます。ぜひお申込み下さい。

■Password Manager Proの関連セミナー 一覧
https://www.manageengine.jp/products/Password_Manager_Pro/seminars.html?security_wp

お問い合わせ先

ゾーホージャパン株式会社
〒220-0012　神奈川県横浜市西区みなとみらい三丁目6 番1 号
みなとみらいセンタービル13 階

ManageEngine　営業担当宛
Phone: 045-319-4612
E-mail : jp-mesales@zohocorp.com

ManageEngine