サポート情報記事

Password Vault によるデータの保護: 暗号化、PIN コード、ストレージ

2026 © Vitextra SIA. All rights reserved.

免責事項

本免責事項の適用上、次のとおり定義します。

- **会社** (本免責事項では「当社」と表記します) とは、Vitextra SIA (Matīsa iela 61-25, Rīga, LV-1009, Latvia) を指します。
- **本ドキュメント**とは、ナレッジベースの記事を指します。
- **お客様**とは、本ドキュメントにアクセスする個人、または該当する場合は、その個人が本ドキュメントにアクセスまたは使用する際に代理となっている会社その他の法人を指します。
- **本 Web サイト**とは、https://vitextra.com からアクセスできる Vitextra を指します。

免責事項

本ドキュメントに記載されている情報は、一般的な情報提供のみを目的としています。

当社は、本ドキュメントの内容における誤りや脱漏について、一切責任を負いません。

いかなる場合も、契約上の訴訟、過失、その他の不法行為上の訴訟であるかを問わず、本ドキュメントの内容の使用に起因または関連して生じる、特別損害、直接損害、間接損害、結果的損害、付随的損害、またはその他一切の損害について、当社は責任を負いません。当社は、事前の通知なく、いつでも本ドキュメントの内容に追加、削除、または変更を行う権利を留保します。

誤りおよび脱漏に関する免責事項

本ドキュメントに記載されている情報は、関心のある事項に関する一般的な指針を示すことのみを目的としています。そのため、本ドキュメントの内容を最新かつ正確に保つために当社があらゆる予防措置を講じている場合でも、誤りが生じる可能性があります。また、法律、規則、規制は変化するため、本ドキュメントに記載されている情報に遅れ、脱漏、または不正確な点が含まれる場合があります。

当社は、誤りや脱漏、またはこの情報の使用によって得られた結果について、責任を負いません。

フェアユースに関する免責事項

当社は、著作権者から明示的な許可を得ていない著作物を使用する場合があります。当社は、批評、論評、ニュース報道、教育、学術研究、または調査の目的で、そのような資料を提供しています。

当社は、これが、米国著作権法第 107 条に規定されている、当該著作物の「フェアユース」にあたると考えています。

お客様が、フェアユースの範囲を超えて、ご自身の目的で本ドキュメントの著作物を使用することを希望される場合は、著作権者から許可を得る必要があります。

「自己責任での使用」に関する免責事項

本ドキュメントのすべての情報は、完全性、正確性、適時性、またはこの情報の使用によって得られる結果について何ら保証することなく、また、性能、商品性、特定目的への適合性に関する保証を含むがこれらに限定されない、明示または黙示を問わずいかなる種類の保証もなく、「現状のまま」提供されます。

当社は、本ドキュメントに記載されている情報に依拠して行われた判断や措置、または結果的損害、特別損害、もしくはこれらに類する損害について、たとえそのような損害の可能性について知らされていた場合でも、お客様またはその他の者に対して責任を負いません。

お問い合わせ

本免責事項についてご不明な点がある場合は、メール (support@vitextra.com) でお問い合わせください。

目次

概要 4

まとめ 4

第 **1** 層**: Microsoft 365** のサインインと **OneDrive** のアクセス制御 5

第 **2** 層**:** ブラウザー内でのエントリの暗号化 6

暗号化される情報とされない情報 6

既存の保管庫は自動的にアップグレードされます 7

第 **3** 層**: PIN** コードとロックされた保管庫 8

自動ロック 9

失敗した試行の上限 10

Vitextra にデータは保存されない 10

Password Vault の想定用途 10

推奨事項 11

概要

Password Vault は、SharePoint Online のページと Microsoft Teams で使用する個人用のパスワード　　マネージャーです。各ユーザーは、自分の資格情報を自分の OneDrive にある 1 つの暗号化されたファイルに保管します。この記事では、データがどのように保護されるかを層ごとに説明し、PIN　コードが果たす役割と果たさない役割、保管庫のどの部分が暗号化されるか、Password Vault がどのような資格情報を想定して設計されているかを説明します。製品を理解したいエンド　ユーザーと、製品を審査する管理者およびセキュリティ担当者を対象としています。

まとめ

質問	回答
保管庫はどこに保存されますか?	ユーザー自身の OneDrive のアプリ フォルダーにある 1 つのファイル *vitextra-password-vault.json*
ファイルを開けるのは誰ですか?	Microsoft 365 のアクセス許可に基づいてユーザーの OneDrive にアクセスできるすべての人 (既定ではユーザー本人のみ)
どの ID が使用されますか?	サインインしている Microsoft 365 ユーザー。委任されたアクセス許可 *Files.ReadWrite.AppFolder* を使用して Microsoft Graph 経由でアクセスします
何が暗号化されますか?	各エントリのテキスト フィールド: 名前、ユーザー名、パスワード、URL、メモ、フォルダー、タグ (AES、ブラウザー内、PIN コードから導出したキーを使用)
PIN コードの役割は何ですか?	暗号化キーは 4 桁の PIN コードから導出されます。PIN コードを入力するまで、Web パーツにはエントリが一切表示されません

質問	回答
PIN コードが再度求められるのはいつですか?	Web パーツで 5 分間操作がなかったとき、およびページを再読み込みしたとき
誤った PIN コードを入力するとどうなりますか?	誤った PIN コードを 5 回連続で入力すると保管庫はブロックされ、リセットすることしかできなくなります。リセットするとすべてのエントリが消去されます
Vitextra に何が送信されますか?	保管庫のデータは送信されません。ライセンス チェックと利用状況テレメトリの技術的な識別子のみが送信されます

第 1 層: Microsoft 365 のサインインと OneDrive のアクセス制御

Password Vault には、独自のアカウント、サーバー、データベースはありません。Web パーツはサインインしているユーザーのブラウザーで実行され、そのユーザーの ID で Microsoft Graph を通じて保管庫を読み書きします。ファイルはユーザー自身の OneDrive に保存されるため、そこにある他のファイルと同じ仕組みで保護されます。つまり、Microsoft 365 のサインイン (組織で使用している場合は多要素認証と条件付きアクセスを含む)、OneDrive のアクセス許可、組織の Microsoft 365 のポリシーです。

Web パーツが使用する委任されたアクセス許可は *Files.ReadWrite.AppFolder* の 1 つだけで、これによって Web パーツはサインインしているユーザーの OneDrive のアプリ フォルダー内でのみ動作できます。ユーザーの他のファイルを開くことも、別のユーザーの OneDrive を開くこともできません。詳細については、KB10454. Microsoft Graph のアクセス許可 Files.ReadWrite.AppFolder: Password Vault に必要な理由と承認方法を参照してください。

保管庫はページではなくユーザーの OneDrive に保管されるため、Web パーツのあるページや Teams タブを開いたユーザーには、それぞれ自分の保管庫だけが表示

されます。共有ページに Web パーツを配置しても、パスワードが共有されることはありません。

第 2 層: ブラウザー内でのエントリの暗号化

Password Vault は、保管庫を保存する前に、各エントリのテキスト フィールドを AES で暗号化します。暗号化と復号はユーザーのブラウザー内で行われ、ファイルは Microsoft Graph を通じてブラウザーとユーザーの OneDrive の間でのみ転送されます。そのため、値がプレーン テキストで保存または転送されることはありません。ファイルを開いた人には、名前、ユーザー名、パスワードの代わりに暗号化された文字列が表示されます。

暗号化キーは、ブラウザー内で PBKDF2-SHA256 (Web Crypto) を使用して PIN コードから導出されます。その際、ランダムな 16 バイトのソルトと 600,000 回の反復が使用されます。ソルトは、PIN コードを設定または変更するたびに新しく作成されます。キーはどこにも保存されません。保管庫ファイルにも、ブラウザーのストレージにも、Vitextra にも保存されません。キーは、保管庫のロックが解除されている間、開いているページのメモリ内にのみ存在します。PIN コードを確認する際、Web パーツは PIN コードからキーを導出し、確認値 (キーで暗号化された既知のテキスト) を復号します。確認値は、ソルトおよび反復回数と共にファイルに保存されています。PIN コードも PIN コードのハッシュも保存されません。そのため、保管庫ファイルだけではエントリを読み取ることはできず、PIN コードが必要です。

警告

PIN コードは 4 桁しかなく、組み合わせは 10,000 通りです。PBKDF2 によって推測のたびに意図的に時間がかかるようになっていますが、保管庫ファイルのコピーを入手した人は、Web パーツの外部でオフラインですべての PIN コードを試すことができます。5 回の試行制限が適用されるのは Web パーツ内だけです。したがって、OneDrive へのアクセス制御が引き続き第一の防御線です。Microsoft 365 アカウントを安全に保ち、保管庫ファイルやそれを含むフォルダーを共有しないでください。

暗号化される情報とされない情報

保管庫ファイル内のデータ	暗号化
エントリの名前	はい
ユーザー名	はい
パスワード	はい
URL	はい
メモ	はい
フォルダー	はい
タグ	はい
お気に入りフラグ (星)	いいえ
エントリの識別子、作成日時と更新日時	いいえ
ソルト、反復回数、確認値 (PIN コードの確認に使用)	ソルトと反復回数: いいえ。確認値は、キーで暗号化された既知のテキストです。PIN コード、そのハッシュ、キーは保存されません
ユーザーの Microsoft Entra ID オブジェクト ID	いいえ
PIN コードの失敗した試行のカウンター	いいえ

SharePoint リスト、Web パーツのプロパティ、ブラウザーのストレージには何も書き込まれません。キーと復号された値は、保管庫のロックが解除されている間、開いているページのメモリ内にのみ存在します。

既存の保管庫は自動的にアップグレードされます

以前のバージョンの Password Vault で作成された保管庫は、以前のファイル形式を使用しています。この形式では、キーはファイルに保存された PIN コードの SHA-256 ハッシュとユーザーの Microsoft Entra ID オブジェクト ID から導出されて

いました。新しいバージョンで初めて正しい PIN コードを入力すると、Web パーツは PBKDF2 で導出した新しいキーですべてのエントリを再暗号化し、保管庫を新しい形式で保存します。エントリとその更新日時は保持され、失敗した試行のカウンターはリセットされます。ユーザーが何かを行う必要はありません。アップグレード後のファイルには、PIN コードのハッシュは含まれなくなります。

メモ

アップグレードによって変更されるのは、現在の保管庫ファイルだけです。OneDrive のバージョン履歴やごみ箱に保持されている以前のバージョンのファイル、およびバックアップ内のコピーは以前の形式のままです。以前の形式では、PIN コードがなくてもファイル自体からエントリを復号できました。それらを開くことができる人は、OneDrive のアクセス制御と、組織の保持およびバックアップの設定によって決まります。

第 3 層: PIN コードとロックされた保管庫

PIN コードは、保管庫の作成時にユーザーが設定する 4 桁のコードです (KB10442. Password Vault で PIN コードを設定する方法を参照)。PIN コードが必要なのは、保管庫を開くときの 1 回だけです。Web パーツは、4 桁目の数字が入力された時点で PIN コードを確認します。それまでは保管庫はロックされており、Web パーツにはエントリが一切表示されません。エントリの名前さえ表示されません。一覧の代わりに、「続行するには PINコードを入力してください」と 4 つの数字入力ボックスを含む **PINコードの入力** プロンプトが表示され、ツール バーには**更新**ボタンしかありません。

操作	保管庫がロックされている間に利用可能
エントリの名前、ユーザー名、URL、フォルダー、タグ、メモを含む一覧の表示	いいえ (一覧は非表示)
パスワードの表示 (目のボタン)、またはパスワードやユーザー名の**クリップボードにコピー**	いいえ

操作	保管庫がロックされている間に利用可能
新しいアイテム、編集、削除	いいえ
PINコードの変更 (構成の歯車)	いいえ
お気に入りに追加 / お気に入りから削除	いいえ
検索とフィルター	いいえ
更新	はい

正しい PIN コードを入力すると保管庫のロックが解除され、保管庫が再びロックされるまで、これらの操作はすべて PIN コードを再度求められることなく直接実行できます。

警告

保管庫のロックが解除されている間は、保管庫が再びロックされるまで、あなたのコンピューターを使用する人は誰でも、パスワードを含む保管庫内のすべての情報を表示およびコピーできます。コンピューターから離れるときは必ずロックしてください。

PINコードの入力 プロンプトでは、入力中の数字はマスクされます。**PIN**コードの設定 画面と **PIN**コードの変更 画面では数字が表示されるため、PIN コードの設定や変更は、画面を誰にも見られない場所で行ってください。

自動ロック

ページが読み込まれた後、保管庫はロックされた状態です。エントリは表示されず、**PIN**コードの入力 プロンプトだけが表示されます。正しい PIN コードを入力すると保管庫が開き、作業している間はロック解除されたままになります。Web パーツ内で **5 分間**クリックもキー入力もなかった場合 (**PIN**コードの変更 画面での操作も対象になります)、保管庫は再びロックされます。一覧は消え、表示されていたパスワードは非表示になり、キーはメモリから削除され、開いているすべてのダイアログ (新しいアイテム、プロパティの編集、削除の確認) は保存されずに

閉じられます。ロック解除の状態は開いているページの中にしか存在しないため、ページを再読み込みしても保管庫はロックされます。KB10451. 自動ロック: Password Vault が PIN コードを再度要求するタイミングを参照してください。

失敗した試行の上限

誤った PIN コードを入力するたびに、「PINコードが正しくありません」と **残りの試行回数** が表示されます。カウンターは保管庫ファイルに保存され、常に最新バージョンのファイルを基に増やされるため、異なるデバイスやページでの試行は確実に合算されます。以前に誤った試行がある場合は、ページを再読み込みした後や別のデバイスでも、**PINコードの入力** プロンプトに **残りの試行回数** の行が表示されます。カウンターは時間が経ってもリセットされません。カウンターをリセットできるのは正しい PIN コードだけです。誤った PIN コードを **5** 回連続で入力すると保管庫はブロックされ、Web パーツには **リセット**画面だけが表示されます。リセットすると、すべてのエントリと PIN コードが消去されます。KB10455. Password Vault で PIN コードを誤って入力した場合: 5 回失敗するとどうなるかを参照してください。

警告

忘れた PIN コードは、あなた自身も、管理者も、Vitextra も、回復またはリセットすることはできません。PIN コードは安全な場所に控えておき、重要な資格情報は組織が承認した別の場所にも保管してください。KB10460. Password Vault の PIN コードを忘れた場合の対処方法を参照してください。

Vitextra にデータは保存されない

Vitextra は、保管庫のデータを受信、保存、バックアップしません。Web パーツから Vitextra のサービスへの要求は、ライセンス チェックと、技術的な識別子を含む利用状況テレメトリのみです。詳細な一覧については、KB10363. Vitextra 製品がデータを保存する場所: プライバシー、データ所在地、GDPRを参照してください。

Password Vault の想定用途

Password Vault は、日常的に使用する資格情報 (Web ポータルや取引先のシステム

へのサインイン情報、テスト　アカウントなど、ユーザーがこれまでノートやテキスト ファイルに記録していたようなエントリ) を保管する、便利な個人用の場所として設計されています。その保護は、Microsoft 365 のアクセス制御と、4 桁の PIN コードから導出したキーによる保存された値の暗号化を組み合わせたものです。

Password Vault は特権アクセス管理システムではありません。ユーザー間の共有、管理者による回復、独自の監査ログ、強度の高いマスター　パスワードはいずれも備えていません。管理者アカウント、サービス　アカウント、チームで共有する資格情報、その他の高い特権を持つ秘密情報については、組織のポリシーに従い、組織が指定するツールを使用してください。他の方法との比較については、KB10440. Password Vault とブラウザーのパスワード マネージャー、エンタープライズ パスワード マネージャーの比較: どれを選ぶべきかを参照してください。

推奨事項

- Microsoft 365 アカウントを保護してください。保管庫の安全性は、OneDrive を所有するアカウントの安全性を超えることはありません。
- 推測されにくい PIN コードを選び (*0000*、*1234*、生まれ年などは避けてください)、安全な場所に控えておいてください。
- 保管庫ファイルを共有したりコピーしたりしないでください。コピーを持つ人は、10,000 通りの PIN コードすべてをオフラインで試すことができます。
- 短時間であっても、コンピューターから離れるときはロックしてください。
- コピーしたパスワードは、別のものをコピーするまでクリップボードに残ります。共有コンピューターでは、使用後にクリップボードをクリアしてください。
- 複数のデバイスやタブで保管庫を使用する場合、変更は自動的に統合されます。他の場所で行われた変更を表示するには、更新を押してください (KB10453. Password Vault がパスワードを保存する場所: OneDrive のアプリ フォルダーを参照)。
- 個人用のパスワード　マネージャーに保管することを組織が許可している資格情報だけを保存してください。

ヒント

エントリを見ることができる人とできない人を正確に確認するには、KB10456. Password Vault のパスワードを見ることができるのは誰かを参照してください。