サポート情報記事

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

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

Password Vault の概要 4

比較の早見表 5

Password Vault が適している場合 6

ブラウザーのパスワード マネージャーが適している場合 7

エンタープライズ パスワード マネージャーが適している場合 7

ツールの併用 7

決定する前に確認すべき質問 8

概要

従業員にパスワードをスプレッドシートやメモに保存するのをやめさせたい組織は、通常、次の 3 種類のツールを検討します。

- **ブラウザーのパスワード マネージャー** – Web ブラウザーに組み込まれたパスワードの保存機能で、ユーザーが Web サイトにサインインするときに資格情報を保存します。
- **エンタープライズ パスワード マネージャー** – 通常、独自のサービス、クライアント アプリ、ブラウザー拡張機能を備えた専用製品で、組織全体の資格情報管理を目的としています。
- **Password Vault** – Vitextra の SharePoint Framework Web パーツで、Microsoft 365 (SharePoint Online と Microsoft Teams) の中ですべての従業員に軽量な個人用保管庫を提供します。

これらのツールが解決する課題はそれぞれ異なります。この記事では、各カテゴリの一般的な特徴を説明し、特定のニーズにどれが合うかを判断できるようにします。同じカテゴリ内でも製品ごとに違いがあるため、検討する製品の詳細は、自社の要件と照らし合わせて確認してください。

Password Vault の概要

Password Vault は、各ユーザーのエントリをそのユーザー自身の OneDrive 内のファイルに暗号化して保存し、SharePoint ページまたは Teams の Web パーツに表示します。Web パーツ内でのアクセスは 4 桁の PIN コードで保護され、暗号化キーはこの PIN コードから導出されます。保管庫がロックされている間はエントリが表示されず、操作がないまま 5 分経過すると自動的にロックされます。PIN コードは 4 桁しかないため、ファイルを守る最初の防御線は引き続き OneDrive へのアクセス制御です。パスワード ジェネレーター、強度メーター、フォルダー、タグ、お気に入り、検索を備えています。詳細については、KB10437. Password Vault. ソリューションの概要を参照してください。

同じくらい重要なのが、Password Vault にできないことです。

- サインイン フォームの自動入力やブラウザー拡張機能はありません。資格情報は **クリップボードにコピー** でコピーします。
- エントリの共有やチーム用の保管庫はありません。
- 管理コンソールや、忘れた PIN コードの回復機能はありません。誤った PIN コー

ドを 5 回入力した後に選べるのは保管庫のリセットだけで、リセットするとすべてのエントリが消去されます。
- エクスポートやインポートはできません。

比較の早見表

Password Vault の列は製品そのものについて、他の 2 列は各カテゴリで一般的な内容について説明しています。

観点	Password Vault	ブラウザーのパスワード マネージャー (一般的な例)	エンタープライズ パスワード マネージャー (一般的な例)
目的	Microsoft 365 内での従業員個人の資格情報	ブラウジング中の個人的な利便性	組織全体の資格情報管理
データの保存場所	ユーザー自身の OneDrive 内の暗号化されたファイル	ブラウザーのプロファイル内。ブラウザー ベンダーのアカウントを通じて同期されることが多い	製品独自のサービス、または組織が運用するインフラストラクチャ
アクセス方法	SharePoint ページまたは Microsoft Teams。職場のアカウントと 4 桁の PIN コードを使用	プロファイルにサインインしているブラウザー	製品のクライアント アプリ、ブラウザー拡張機能、Web アクセス
サインイン フォームの自動入力	なし	あり	通常はあり
同僚との共有	なし	業務上は限定的、またはなし	通常はあり (共有フォルダーや共有保管庫)
管理、ポリシー、	なし (展開と	ブラウザーの管理	通常は充実

観点	**Password Vault**	ブラウザーのパスワード マネージャー **(**一般的な例**)**	エンタープライズ パスワード マネージャー **(**一般的な例**)**
監査	Graph のアクセス許可のみ)	オプションによる	
アクセスを失った場合の回復	なし (リセットすると保管庫が消去される)	ブラウザーのアカウントによる	通常は管理者またはユーザー向けの回復手段がある
展開	SPFx パッケージ 1 つと Graph のアクセス許可 1 つ。追加のクライアント ソフトウェアは不要	ブラウザーにすでに搭載	別製品として展開、構成し、ユーザーごとにライセンスを付与する必要がある
一般的な料金体系	テナント単位のライセンス	ブラウザーに含まれる	通常はユーザー単位のサブスクリプション

Password Vault が適している場合

- 従業員が業務に関わる**自分自身の**資格情報 (仕入先ポータル、パートナー エクストラネット、テスト システム、デバイス コンソールなど) を保管する場所を必要としており、組織がその場所を個人用のツールやファイルではなく Microsoft 365 内に置きたいと考えている場合。
- 組織が、データを追加のサードパーティ　サービスではなく**自社のテナント**　(各ユーザーの OneDrive) 内に保持したいと考えている場合。
- 自動入力よりも、拡張機能やクライアント　ソフトウェアをインストールせずに SharePoint ページや Teams で使えるシンプルなツールのほうが重要な場合。
- 資格情報が共有されず、PIN　コードを忘れた場合に失っても許容できる場合。資格情報は提供元から復元できるためです　(たとえば、そのサービス独自の「パスワードを忘れた場合」の手続きを利用します)。

ブラウザーのパスワード マネージャーが適している場合

- 主なニーズが利便性、つまりブラウジング中に Web サイトのパスワードを保存して自動入力することである場合。
- ユーザーが主に 1 つのブラウザーで作業し、組織のポリシーで業務用の資格情報をブラウザーに保存することが認められている場合。

ブラウザーのパスワード マネージャーは資格情報をブラウザーのプロファイルに保存するため、利用できる内容は、ブラウザーやユーザーがサインインしているアカウント、そして組織によるブラウザーの管理方法に左右されることに注意してください。

エンタープライズ パスワード マネージャーが適している場合

- サービス アカウントや共有メールボックスなど、資格情報をチーム内で**共有**する必要がある場合。
- 組織が、一元的な**ポリシー、監査証跡、アクセス レビュー、回復**の手順を必要としている場合。
- **高い特権を持つ**管理者アカウントを管理する必要がある場合 (多くの場合、特権アクセス管理と組み合わせて使用します)。
- ブラウザー、デスクトップ アプリ、モバイル アプリをまたいだ自動入力が必要な場合。

こうした機能を利用するには、別製品の展開、構成、ユーザー トレーニング、ライセンス (通常はユーザー単位) が必要になります。

警告

Password Vault は個人の資格情報向けに設計されています。共有アカウントや高い特権を持つアカウントを管理するソリューションの代わりにはなりません。そのようなアカウントについては、組織のセキュリティ ポリシーに従ってください。

ツールの併用

これらのカテゴリは互いに排他的ではありません。たとえば、IT 部門と共有アカ

ウントにはエンタープライズ パスワード マネージャーを運用し、それ以外の業務用資格情報を保管する手軽な個人用の場所として全従業員に Password Vault を提供する、あるいはリスクの低い Web サイトについてはブラウザーへの保存を認める、といった運用が可能です。重要なのは、どの種類の資格情報をどこに保管するかを定めた明確なポリシーです。

メモ

Password Vault にはインポートもエクスポートもないため、エントリを移行するには 1 件ずつ追加する必要があります。従業員が保管庫にエントリを蓄積し始める前に、どのツールを選ぶかを計画してください。

決定する前に確認すべき質問

1 資格情報を共有する必要がありますか、それとも完全に個人用ですか?
2 サインイン フォームの自動入力は必要ですか?
3 暗号化されたデータをどこに保存してよいですか? Microsoft 365 テナント内、ブラウザー ベンダーのアカウント、サードパーティのサービスのいずれですか?
4 管理者による回復、ポリシー、監査は必要ですか?
5 何を展開できますか? SPFx Web パーツですか、それともすべてのデバイスへのクライアント ソフトウェアと拡張機能ですか?
6 ユーザーがアクセスを失った場合、資格情報はどうなりますか? 元のシステムから復元できますか?

ヒント

Password Vault がデータをどのように保護し、誰がアクセスできるかについては、KB10452. Password Vault によるデータの保護: 暗号化、PIN コード、ストレージと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。試してみるには、KB10438. Password Vault Web パーツをページに追加して保管庫を作成する方法を参照してください。