bitwarden | ヘルプセンターの記事

Bitwarden用語集

ヘルプセンターで表示:
https://bitwarden.com/help/bitwarden-glossary/

Bitwarden用語集

全般

専門用語	定義
アカウント	Bitwardenアカウントは、あなただけが知っているユーザー名とマスターパスワードによって定義される記録です。あなたのBitwardenアカウントは、Bitwardenサービスにアクセスするために使用され、請求書、設定、言語の選択などの情報も含まれています。
アカウント切り替え	Bitwardenの機能は、デスクトップとモバイルのクライアントで、個人のアカウントや仕事のアカウントなど、複数のアカウント間を簡単に切り替えることができます。もっと詳しく知る。
個人アカウント	個人のBitwardenアカウントは、ユーザー名とマスターパスワード（これはあなただけが知っている）によって定義され、組織の保管庫や会社やビジネスエンティティに関連付けられていない記録です。個人アカウントは通常、個人のメールアドレスで設定され、あなただけが所有権と制御権を持つ保管庫のアイテムを含んでいます。
ビジネスアカウント	ビジネスBitwardenアカウントは、あなただけが知っているユーザー名とマスターパスワードで定義され、会社やビジネスエンティティに関連する組織に関連付けられている記録です。ビジネスアカウントは通常、ビジネス用のメールアドレスで設定されます。 ビジネスアカウントは、関連する組織によって管理されます。ビジネスアカウント内に含まれる保管庫のアイテムや秘密は、関連する会社やビジネスエンティティの専有物と考えるべきです。
API キー	アプリケーションプログラミングインターフェイス（API）キーは、ユーザーまたはプログラムを特定するための特定の識別コードです。APIキーは、自動化、監視などの用途で他のアプリケーションをBitwardenと統合するために使用できます。APIキーは機密性が高く、慎重に取り扱うべきです。
クライアント / Bitwardenクライアント	クライアント、またはクライアントアプリケーションは、Bitwardenにログインするアプリケーションです。これには、ウェブ、モバイル、デスクトップアプリ、Bitwarden CLI、およびブラウザの拡張機能が含まれます。クライアントはダウンロードページからダウンロードすることができます。
ディレクトリ-コネクタ	ディレクトリサービスからBitwarden組織へのユーザーとグループを同期するためのアプリケーション。Bitwardenディレクトリコネクタは、ソースディレクトリからユーザー、グループ、およびグループの関連付けを自動的にプロビジョニングおよびデプロビジョニングします。もっと学ぶ。
ドメイン確認	組織が特定のインターネットドメイン（例：mycompany.com）の所有権を証明するプロセス。ドメインの確認により、追加の機能が有効化されます。例えば、ユーザーがログインプロセス中にSSO識別子の入力をスキップできるようになるなどです。もっと学びましょう。
グループ	組織メンバーの設定。グループはユーザーをまとめ、権限を割り当てるスケーラブルな方法を提供します。これには、コレクション、プロジェクト、または秘密へのアクセス、および各別のコレクション内の権限が含まれます。新しいユーザーをプロビジョニングするときは、そのユーザーをグループに追加して、そのグループの設定された権限を自動的に継承させます。
マスターパスワード	Bitwardenパスワード、メインパスワード、アカウントパスワード、または保管庫パスワードとも呼ばれます。 あなたのBitwardenアカウントとデータにアクセスするための主要な方法（またはキー）、マスターパスワードは、Bitwardenサービスへの認証と、保管庫のアイテムや秘密などの機密データの復号化の両方に使用されます。Bitwardenは、ユーザーに対して、記憶に残る強力でユニークなものを設定することを奨励しています。それはBitwardenだけで使用されるものです。 *2021年に、Bitwardenはアカウント回復管理（以前は管理者パスワードリセット）を導入しました。これにより、エンタープライズユーザーや組織は、管理者や所有者が登録ユーザーのマスターパスワードをリセットできるポリシーを実装することが可能になりました。*もっと学びましょう。
組織	Bitwardenユーザーを組織のデータ（組織の保管庫内のログインや、シークレットマネージャープロジェクトなど）に関連付けるエンティティ（会社、機関、人々のグループ）。これにより、アイテムの安全な共有が可能になります。
プラン	プランは、利用可能な機能や製品を使用できるユーザーの数を含む、ライセンスを通じてBitwardenが提供するサービスを定義します。個人または組織が登録できる、複数のタイプの事前定義されたプランが利用可能です。
方針	ポリシーは、管理者が会社を安全に保つための組織全体のコントロールであり、メンバー（エンドユーザーとも呼ばれます）がBitwardenを使用する方法についての追加設定を有効にします。これらのポリシーは、統一されたセキュリティ基準を保証します。もっと学びなさい。

専門用語	定義
SCIM	クロスドメインID管理（SCIM）システムは、Bitwarden組織内のメンバーやグループを自動的にプロビジョニングするために使用できます。 Bitwardenサーバーは、有効なSCIM APIキーを持つと、ユーザーとグループのプロビジョニングとデプロビジョニングのためのあなたのIDプロバイダー（IdP）からのリクエストを受け入れるSCIMエンドポイントを提供します。もっと学びましょう。
シングルサインオン	従業員やユーザーが自身のIDと権限に基づいた一組のログイン認証情報でアプリケーションにアクセスできるようにするセッションおよびユーザー認証サービス。シングルサインオンには複数の実装オプションがあり、IDプロバイダ（IdPs）と広く互換性があり、顧客が既存のソリューションを活用できるようになっています。もっと学びなさい。
SSOでログインする	シングルサインオンの実装この方法では、ユーザーはIDプロバイダーによって認証され、その後ユーザーは自分のBitwardenパスワードを入力して自分のデータを復号化します。もっと学ぶ。
信頼できるデバイスとのSSO	パスワードレスのシングルサインオンの実装。この方法では、ユーザーはIDプロバイダーによって認証され、指定された信頼できるデバイスに保存されたデバイス暗号化キーを利用するプロセスを通じて、ユーザーのデータが復号化されます。もっと学びましょう。
顧客管理暗号化を使用したSSO	自己ホスト型の組織向けに利用可能な、高度なパスワードレスのシングルサインオンの実装。この方法では、ユーザーはIDプロバイダーによって認証され、その後、ユーザーの暗号化キーは自己ホスト型のキーサーバーからキーコネクターを利用して自動的に取得され、ユーザーデータの復号化が可能になります。もっと学びましょう。
契約	サブスクリプションは、ライセンスの発行の一部として、顧客とBitwardenとの間の取引合意です。所有者は、プランで概説されたBitwardenによって提供されるサービスのために、合意した料金で定期的に（月額または年額）プランに加入します。

Bitwarden パスワードマネージャー

用語学	定義
オートフィル	以前に保存された情報をフォームフィールドに自動的に入力するソフトウェア機能。Bitwardenを使用すると、ブラウザの拡張機能やモバイルデバイスを通じてログイン情報を自動入力でき、またブラウザの拡張機能を通じてカードやIDを自動入力することができます。もっと学びなさい。
コレクション	ビジネスがBitwarden組織内で安全に共有するための一つ以上の保管庫アイテム（ログイン、メモ、カード、ID）を一緒に保存するユニット。もっと学ぶ。
個人の保管庫	個々の保管庫は、すべてのユーザーが無制限にログイン、メモ、カード、およびIDを保存できる保護されたエリアです。ユーザーは、任意のデバイスやプラットフォームで自分のBitwarden個人保管庫にアクセスできます。 **ビジネスの文脈内で** Bitwardenのチームまたはエンタープライズプランの一部であるユーザーの場合、個々の保管庫は彼らの仕事用メールアドレスに接続されています。個々の保管庫は、しばしば組織の保管庫と関連付けられていますが、それとは別のものです。 **個人的な文脈で** Bitwardenの個人プランまたはファミリープランの一部であるユーザーにとって、個々の保管庫は彼らの個人的なメールアドレスに接続されています。ファミリープランの一部であるか、無料の二人組織の一部である場合でも、個々の保管庫は組織の保管庫から別々に保持されますが、ユーザーは両方にアクセスできます。 Bitwardenは、仕事用のメールアドレスをチームとエンタープライズ組織に、個人用のメールアドレスをファミリー組織に関連付けることを推奨します。 メモ：エンタープライズポリシーを通じて、エンタープライズ組織のメンバーのために個々の保管庫をオフにすることができます。
アイテム / 保管庫のアイテム	アイテムは、ログイン、メモ、カード、IDなど、Bitwardenパスワードマネージャーで保存および共有できる個々のエントリーです。

用語学	定義
組織メンバー	従業員やファミリーメンバーのようなエンドユーザーは、彼らの保管庫内の共有組織アイテムに加えて、個々の保管庫内の個々のアイテムにもアクセスできます。
組織の保管庫	共有アイテムのための保護されたエリア。組織の一部であるすべてのユーザー（「メンバー」とも呼ばれます）は、保管庫の表示で共有アイテムを見つけることができ、個々に所有しているアイテムと並んでいます。組織の保管庫は、管理者と所有者が組織のアイテム、ユーザー、および設定を管理することを可能にします。
保管庫 / 保管庫の表示	任意のアイテムへの厳格なアクセス制御と統一されたインターフェースを提供する安全な保管エリア。

Bitwarden シークレットマネージャー

用語学	定義
アクセストークン	あなたの保管庫に保存された秘密を解読し、サービスアカウントへのアクセスを容易にするキー。もっと学びなさい。
お名前	特定の秘密のためのユーザー定義ラベル。
プロジェクト	あなたのDevOpsとサイバーセキュリティチームによる管理アクセスのために、論理的にグループ化された秘密のコレクション。もっと学びなさい。
シークレット	あなたの組織が安全に保存する必要があるAPIキーのような敏感なキー値ペアは、決して平文のコードで流出済みになったり、暗号化されていないチャネルで送信されるべきではありません。
サービスアカウント	アプリケーションやデプロイメントパイプラインのような、非人間のマシンユーザーは、プログラムによるアクセスが必要な一連の秘密にアクセスする必要があります。
値	ソフトウェアや機械のプロセスで使用される、保存された秘密のユーザー定義フィールド。これは、Bitwardenシークレットマネージャーによって管理される機密情報で、APIキー、アプリケーションの設定、データベース接続文字列、環境変数を含むことができます。

Bitwarden Passwordless.dev

用語学	定義
FIDO	FIDOはFast Identity Onlineの頭文字を取ったものです。それは、フィッシング防止の安全でオープンなパスワードレス認証標準を開発するコンソーシアムを表しています。FIDO Allianceによって開発されたFIDOプロトコルには以下のものが含まれます： UAF: ユニバーサル認証フレームワーク U2F：ユニバーサルセカンドファクター FIDO2：新しいパスワードレスの認証プロトコルで、コア仕様にはWebAuthn（クライアントAPI）とCTAP（認証API）が含まれます詳細を学ぶ。
パスキー	パスキー - ユーザーが登録する各ウェブサイトのFIDO2標準から派生した認証情報 - は、ユーザーが伝統的なパスワードの代わりに暗号化トークンを作成し保存することを可能にします。今日では、パスキーが使用されて、事前に認証されたデバイス固有のトークンを使用してユーザーをアプリやウェブサイトにログインさせます。将来的には、このプロセスは共有可能または転送可能な暗号化トークンと共に使用することができます。もっと学びましょう。
パスワードレス	パスワードレスは、パスワードに依存しないさまざまな認証技術を説明するために使用される包括的な用語であり、ユーザーが持っているもの（セキュリティキー、トークン、またはデバイス）、ユーザー自身であるもの（生体認証）、そしてパスキーを含みます。