管理者コンソール > ユーザー管理

オンボーディングと後継者計画の概要

オンボーディングと後継者計画の概要

> **Tip**
> 以下で完全な論文を読むか、またはPDFをダウンロードしてください。

あなたのビジネスに合ったパスワード管理

新しい従業員を迅速に稼働させることが生産性を向上させます。同様に、適切に別れを告げることは、
ビジネスのシステムとアカウントのセキュリティに対する信頼を高めます。あなたのビジネスが統合と集中化に傾いているか、
柔軟でダイナミックな環境を好むかに関わらず、Bitwardenはあなたのニーズに適しています。

このガイドでは、組織のメンバー向けのBitwardenのオンボーディングと後継者計画について説明します。まず、
メンバーと組織との関係についての私たちのアプローチから始め、次にオンボーディングと後継者計画の最も簡単なユースケースをカバーし、
最後にあなたのニーズに合わせてBitwardenを調整するためのレバーとオプションに移ります。

Bitwardenのアプローチ

Bitwardenのビジョンは、誰もがハッキングされない世界を想像することです。私たちは、
個人や企業が自分たちの機密情報を簡単かつ安全に管理するのを助けるという使命を前進させています。Bitwardenは次のように考えています：

- 個人の基本的なパスワード管理は**無料に**することができ、またそうすべきです。私たちはまさにそれを提供しています、
  個人向けの基本的な無料アカウントを。
- 個々の人々とファミリーは、TOTP、緊急アクセス、およびその他のサポートセキュリティ機能を使用して、
  自分たちのセキュリティに積極的な役割を果たすべきです。
- 組織は、組織のパスワード管理と安全な共有を通じて、大幅にセキュリティプロファイルを改善することができます。

> **Tip**
> Bitwardenには、ハックフリーな世界を目指す私たちのビジョンから生まれた、
> さまざまなプランとオプションが連携し補完し合っています。職場**や**家庭の全員にパスワード管理を提供することで、
> その目標に一歩近づくことができます。

Bitwardenの重要な側面は、多くのソフトウェアアプリケーションとは異なり、
すべての保管庫の中のすべてがエンドツーエンドで暗号化されていることです。このセキュリティモデルを維持するために、
Bitwardenを使用するすべての人は、ユニークなマスターパスワードを持つユニークなアカウントを持つ必要があります。
マスターパスワードは**強力**であり、**記憶に残る**ものであるべきです。

各ユーザーは自分のマスターパスワードを管理しています。Bitwardenはゼロ知識暗号化ソリューションであり、つまり、
BitwardenのチームもBitwardenのシステム自体も、マスターパスワードの知識がなく、取得する方法もリセットする方法もありません。

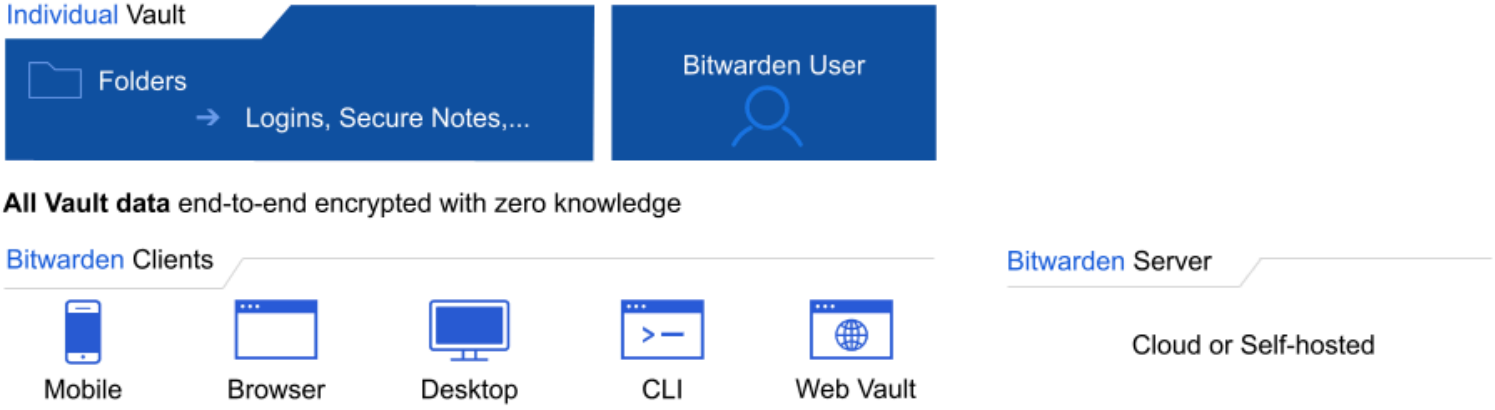
Bitwardenをどこでも使用してください

セキュリティはどこでもセキュリティを意味するので、最高のパスワードマネージャーはあなたのすべてのデバイスでアクセスを提供します。
Bitwardenは、さまざまなクライアントアプリケーションをサポートしており、
それらはいずれも私たちのクラウドホスト型サーバーまたはあなた自身の自己ホスト型サーバーに接続することができます:

Bitwarden クライアント/サーバー

ユーザーの個々の保管庫

Bitwardenアカウントを作成する人は誰でも、自分だけの個別の保管庫を持つことになります。
どのクライントアプリケーションからでもアクセス可能な個々の保管庫は、各ユーザーに固有のもので、
そのユーザーだけがメールアドレスとマスターパスワードの組み合わせを使用してアクセスするためのキーを保持しています。個人のアカウント、
そしてそこに保管されている個々に所有された保管庫のアイテムは、アカウントの所有者の責任です。組織の所有者、管理者、
およびマネージャーは、設計上他のユーザーの個人のボールトを表示できないため、誰かの個人のボールト
データが自分のものであることが保証されます。



個人の保管庫

ファミリー、チーム、エンタープライズ組織は、メンバーに自動的にプレミアム機能を個々に提供します。これには、
緊急アクセスや暗号化された添付ファイルのストレージなどが含まれ、メンバーはこれらを使用するかどうかを選択できます。
個々の保管庫のデータはユーザーに属します。個々の保管庫は共有を可能にしません、組織は可能にします。

Tip

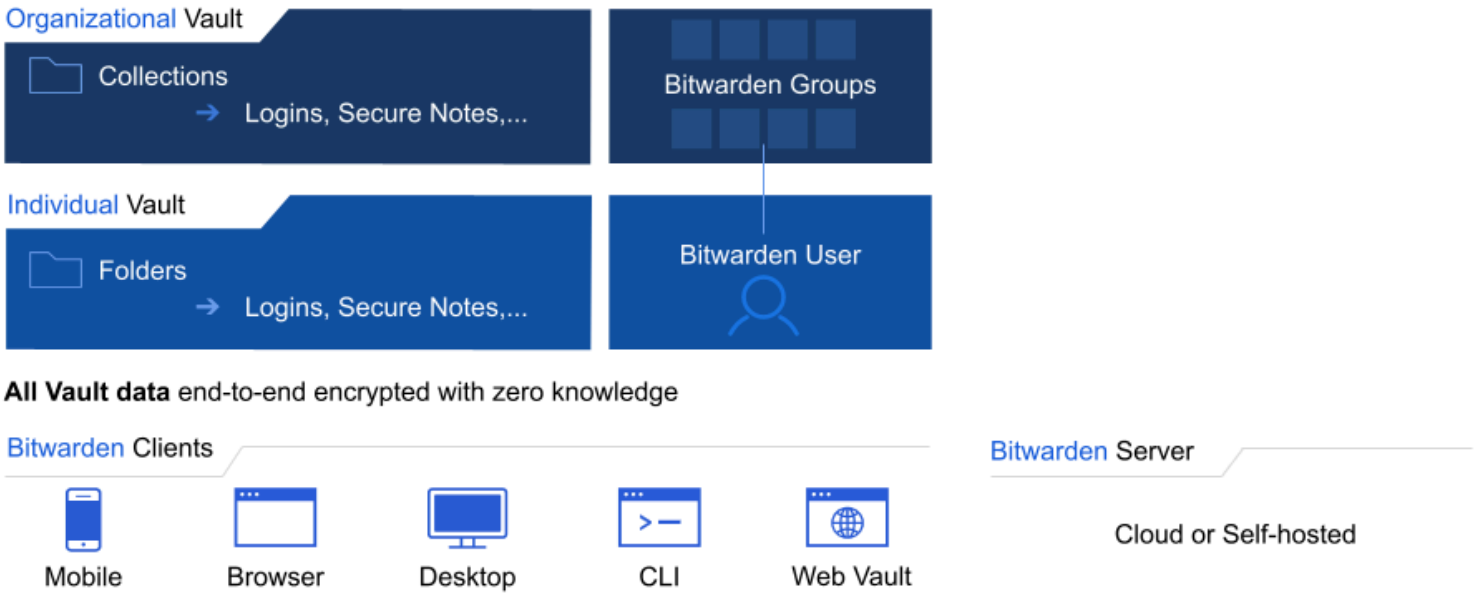
なぜデフォルトで個々の保管庫を提供するのですか？

個々の保管庫は、Bitwardenのアプローチの重要な要素です。従業員は毎日、個人的にも職業的にもさまざまな資格を使用しており、**一方の領域で形成された習慣は通常、他方の領域でも習慣となります。**私たちの表示では、
個人生活で適切なセキュリティ対策を使用する従業員は、その良い行動を職業生活にも持ち込むでしょう。
その過程で**あなたのビジネスを保護します。**

両方の領域で同じツールを使用することで、その習慣はより早く、より簡単に形成されます。エンタープライズ組織は、
個々の保管庫を無効にするなど、ポリシーを設定するオプションを持っています。

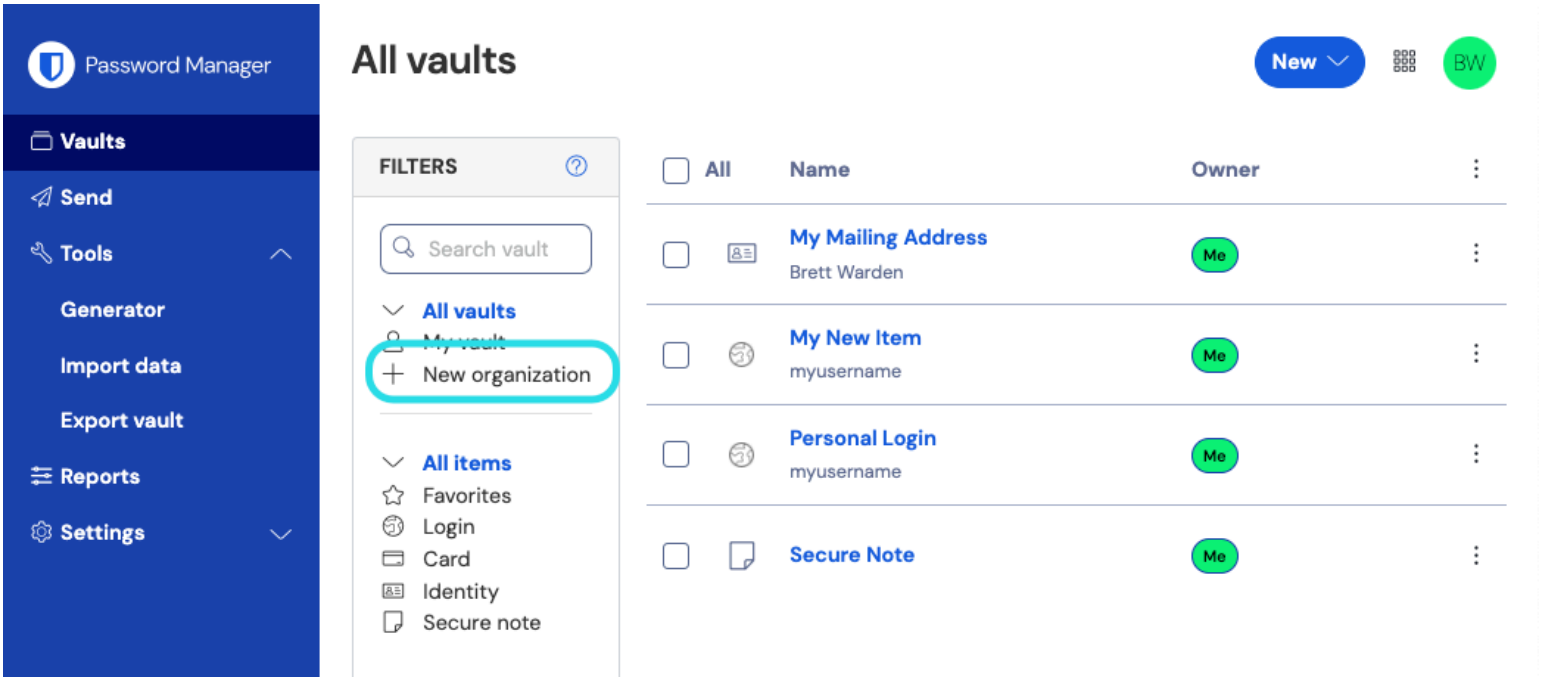
Bitwarden 組織

Bitwarden 組織は、チームや企業のパスワード管理にコラボレーションと共有のレイヤーを追加し、オフィスの Wi-Fi パスワード、
オンライン資格情報、会社の共有クレジット カードなどの共通情報を安全に共有できるようにします。組織を通じた安全な共有は安全で簡単です。



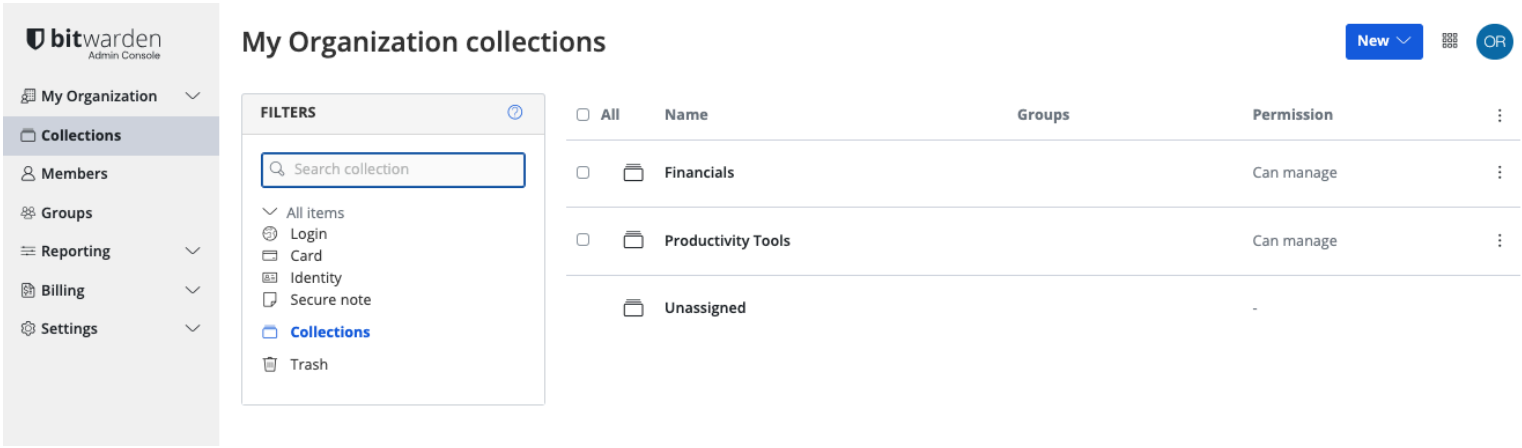
組織の保管庫

誰でもウェブアプリから直接組電を始めることができます:



新しい組織

作成されると、あなたは管理者コンソールに移動します。これは、共有と組織管理のすべての事柄の中心的なハブです。組織を立ち上げる人が所有者となり、保管庫の監督、アイテム、メンバー、コレクション、グループの管理、レポートの実行、ポリシーのような設定の設定など、全てを完全に制御することができます。



管理者コンソール

コレクション

Bitwarden組織は、スケーラブルで安全な方法でメンバーとデータを管理します。大規模なビジネスでは、メンバーやデータを個々に管理することは非効率的で、エラーの余地を残すことがあります。これを解決するために、組織はコレクションとグループを提供します。

コレクションは、ログイン、メモ、カード、およびIDを集め、安全な共有のために組織内で使用します。

コレクションを使用する

メンバーのオンボーディング

あなたの組織が設立され、データを保存するためのコレクションが設定されたら、所有者と管理者は新しいメンバーを招待するべきです。
あなたの組織のセキュリティを確保するために、Bitwardenは新しいメンバーをオンボーディングするための3ステッププロセスを適用します、招待 → 受け入れる → 確認する。

メンバーは、ウェブ保管庫から直接、Directory Connectorアプリケーションを使用して個々のユーザーとグループを同期、
またはSSOでのログインを使用したJust in Time（JIT）プロビジョニングを通じてオンボーディングできます。

メンバーを追加する

最も簡単なケースでは、ユーザーはウェブアプリから直接あなたの組織に追加することができます。ユーザーを追加するとき、
どのコレクションにアクセス権を付与するか、どの役割を与えるかなどを指定できます。

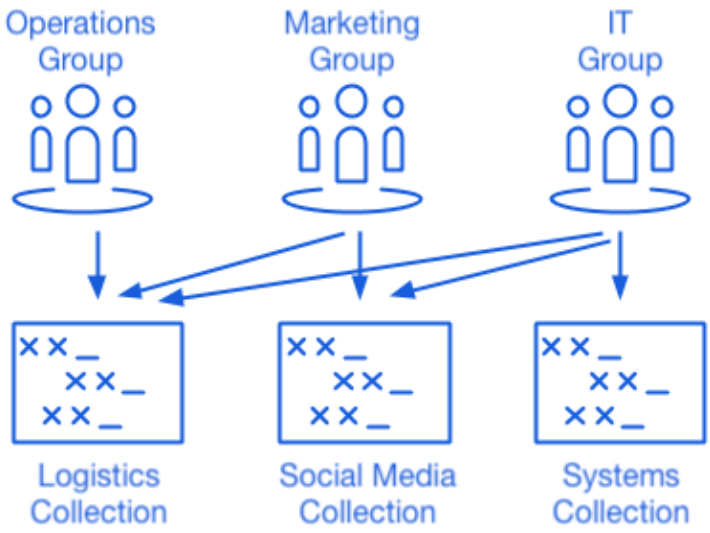
あなたの組織にユーザーを追加する方法をステップバイステップで学びましょう。

ユーザーがあなたの組織に完全にオンボーディングされると、コレクションに割り当てることで、
組織の保管庫データへのアクセスを割り当てることができます。チームとエンタープライズ組織は、
スケーラブルな権限割り当てのためにユーザーをグループに割り当て、個々のレベルでのアクセス割り当ての代わりにグループ-コレクションの関連付けを構築することができます。

> **Tip**
> 大規模な組織にとって、SCIMとディレクトリコネクタは、
> スケールでユーザーをオンボーディングおよびオフボーディングする最良の方法です。

グループ

グループは個々のユーザーを関連付け、コレクションへのアクセスや他のアクセス制御を含む権限を割り当てるスケーラブルな方法を提供します。
新規ユーザーをオンボーディングする際には、彼ら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。



コレクションをグループと一緒に使用する

包括的な役割ベースのアクセス制御

Bitwardenは、スケールでの共有に対してエンタープライズフレンドリーなアプローチを取ります。メンバーは、
さまざまな役割の数値で組織に追加することができ、異なるグループに所属し、
それらのグループをさまざまなコレクションに割り当ててアクセスを制御することができます。利用可能な役割の中には、
管理権限の詳細な設定のためのカスタム役割があります。

ユーザーの削除

Bitwardenでは、資格情報の共有を効率的かつ安全に仕事を進めるための重要な側面と捉えています。また、資格情報が共有されると、
受け取った人がそれを保持することが技術的に可能であることも認識しています。そのため、
適切な役割ベースのアクセス制御を使用した安全なオンボーディングとポリシーの実施は、安全な後継を促進する重要な役割を果たします。

Bitwardenは、ワークフローのカスタマイズや継承に対するコントロールを強化するためのさまざまなツールを提供しています。
次のセクションでは、これらのツールを一切使用しない基本的な後継者ワークフローと、
組織が頻繁に使用する高度な後継者戦略について説明します。

基本的なデプロビジョニング

Bitwardenからユーザーを削除するということは、あなたの組織からユーザーを削除することを意味し、オンボーディングと同様に、
直接ウェブ保管庫から行うことも、SCIMやディレクトリコネクタを使用して自動的に行うこともできます。

Aliceはあなたの組甑の**ユーザー**で、Bitwardenクラウドでホストされ、会社のメールアドレス（例：`first-last@company.com`）
を使用しています。現在、アリスがBitwardenを使う方法は次の通りです：

製品エリア	説明
クライアントアプリケーション	個人的にも専門的にもモバイルとブラウザの拡張機能でBitwardenを使用し、 組織関連の仕事にはたまにウェブ保管庫を使用します。

製品エリア	説明
メールアドレス & マスターパスワード	`alice@company.com` と `p@ssw0rD` を使用してBitwardenにログインします。
個人的なアイテム	彼女の個人的な保管庫には、ログインやクレジットカードなど、さまざまな個人的なアイテムを保管しています。
2段階認証	組織全体でDuo 二要素認証を使用します。
コレクション	アリスは「マーケティング資格」コレクションの管理権限を持っており、そのコレクションの多くの側面を管理する能力を授与されています。
共有アイテム	彼女のチームのコレクションに所在し、組畀に所有されているいくつかの保管庫アイテムを作成し、共有しました。

アリスがあなたの組織から削除されると：

製品エリア	説明
クライアントアプリケーション	彼女は個々の保管庫にアクセスするために任意のBitwardenアプリケーションを引き続き使用できますが、**すぐにすべての組織の保管庫、すべてのコレクション、および共有されたすべてのアイテムへのアクセスを失います。**
メールアドレス & マスターパスワード	`alice@company.com` と `p@ssw0rD` を使用してログインを続けることができますが、彼女は `@company.com` の受信箱にアクセスできなくなるため、彼女のBitwardenアカウントに関連付けられたメールアドレスを変更するように助言するべきです。
個々のアイテム	彼女はまだ個人の保管庫を使用し、そこに保管されているアイテムにアクセスすることができます。
組織内の権限	**直ちに組織に関連する全てのものに対する全ての権限とアクセスを失います。**

製品エリア	説明
2段階認証	彼女は組織のDuo二要素認証を使用して保管庫にアクセスすることはできませんが、 私たちの無料の二段階ログインオプションの1つを設定するか、 より多くのためにプレミアムにアップグレードすることができます。
作成したコレクション	アリスの「マーケティングチーム」コレクションは、組織の所有者と管理者が保持し、 新しいユーザーに管理権限を割り当てることができます。
共有アイテム	コレクションと共有アイテムの所有権は**組専に属しています**、したがって、 それらを作成したにもかかわらず、アリスはこれらすべてのアイテムへのアクセスを失います。

> **Tip**
> オフラインのデバイスは、組織の保管庫データを含む保管庫データの読み取り専用コピーをキャッシュします。
> これを悪意ある利用が予想される場合、メンバーがアクセスしていた資格情報は、彼らを組織から削除するときに更新するべきです。

高度なデプロビジョニング

> **Warning**
> マスターパスワードがない結果としての信頼できるデバイスとのSSOを持つアカウントについては、
> 組織からの削除またはアクセス権の取り消しにより、以下の場合を除き、そのBitwardenアカウントへのすべてのアクセスが遮断されます：
>
> 1. あらかじめアカウント回復を使用して、マスターパスワードを割り当てます。
> 2. ユーザーは、アカウント回復ワークフローを完全に完了するために、アカウント回復後に少なくとも一度ログインします。

管理権の移譲

マスターパスワードリセットポリシーを使用して、組織の所有者と管理者は、
後継時にユーザーのマスターパスワードをリセットすることができます。

ユーザーのマスターパスワードをリセットすると、ユーザーはすべてのアクティブなBitwardenセッションからログアウトされ、
ログイン認証情報が管理者によって指定されたものにリセットされます。つまり、その管理者（そしてその管理者だけ）
がユーザーの保管庫データ、個々の保管庫内のアイテムを含む、鍵を持つことになります。この保管庫の乗っ取り戦術は、

従業員が職場関連の個々の保管庫アイテムへのアクセスを保持しないように、組織が一般的に使用します。これは、
従業員が使用していた可能性のあるすべての資格情報の監査を容易にするために使用することができます。

> **ⓘ Note**
>
> **管理者パスワードのリセットは、二段階ログインをバイパスしません。**多くの場合、
> 一部のIdPではユーザーのために二要素認証と二要素認証バイパスのポリシーを設定できるため、SSOの使用をお勧めします。

個々の保管庫を取り除く

あなたの組粦が保管庫の全てのアイテムをリアルタイムで制御することを必要とする場合、個々の保管庫ポリシーを削除するを使用して、
ユーザーに組織にすべての保管庫アイテムを保存することを要求することができます。これは、後継時にユーザーのアカウントを引き継ぎ、
監査する必要を回避します。なぜなら、組織から削除された後、アカウントはデータが完全に空になるからです。

ログインなしでアカウントを削除

前述の通り、ユーザーをあなたの組織から削除しても、そのユーザーのBitwardenアカウントは自動的に削除されません。
基本的な後継ワークフローでは、ユーザーが削除されると、組織や共有されたアイテムとコレクションにはアクセスできなくなりますが、
既存のマスターパスワードを使用してBitwardenにログインし、個々の保管庫アイテムには引き続きアクセスできます。

組織がアカウントを完全に削除し、すべての個々の保管庫アイテムを含む場合、後継時に以下の方法のいずれかを使用して可能かもしれません：

1. 自己ホスト型のBitwardenを使用している場合、認証済みの管理者はシステム管理者ポータルからアカウントを削除できます。
2. あなたの会社が管理する@yourcompany.comのメールアドレスを持つアカウントの場合、ログインせずに削除のワークフローを使用して、
   @yourcompany.comの受信トレイ内で削除を確認できます。

あなたのビジネスのための組織設計

Bitwardenでは、パスワード管理は人々の管理であるとよく言います、
そして私たちはあなたの組織に適したワークフローを適応させることができます。
私たちのオープンソースのアプローチを通じて提供する幅広い選択肢により、
お客様は自身の個々のニーズを満たすことができると確信していただけます。

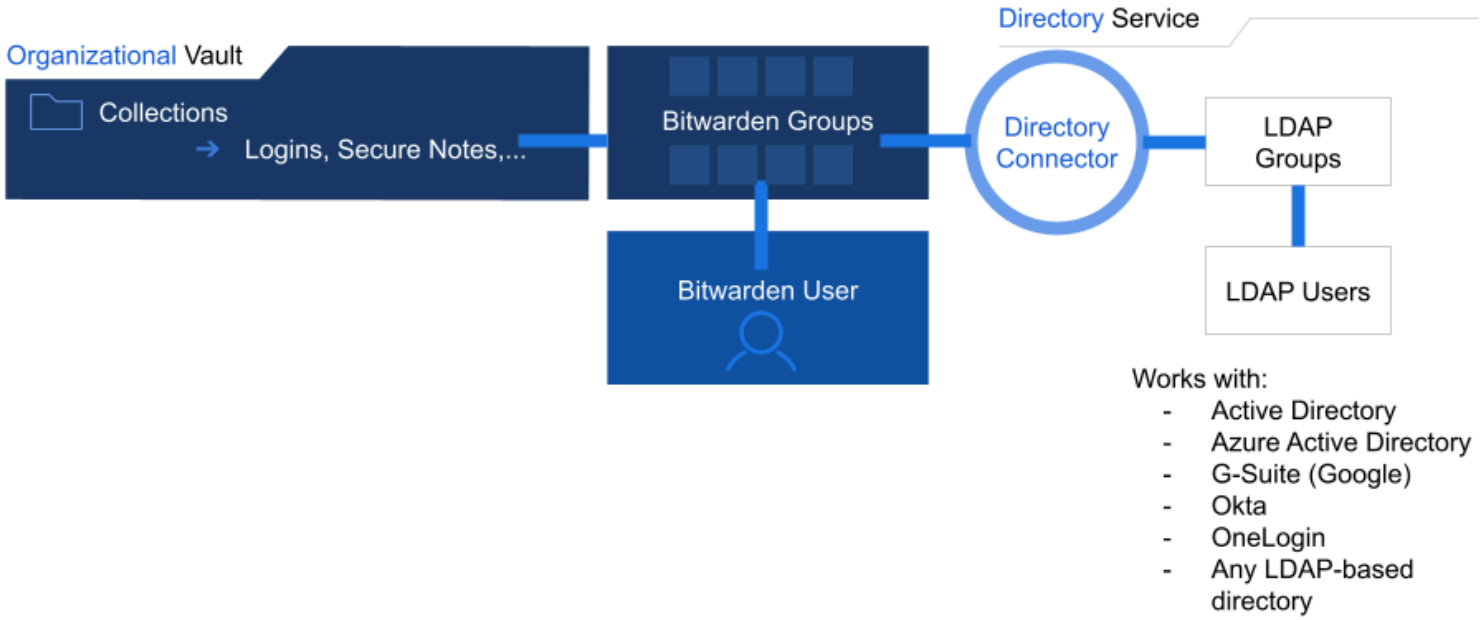
Enterprise または Teams の無料トライアルを今すぐ始めましょう。

SCIM

大規模なユーザーベースを持つエンタープライズ組織で、サポートされているID（現在はAzure AD、Okta、OneLogin、JumpCloud）
を使用して運用している場合、SCIMインテグレーションを使用して、
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ことができます。もっと学ぶ

ディレクトリ-コネクタ

大規模なユーザーベースを持つ会社がディレクトリサービス（LDAP、AD、Oktaなど）を使用して運営している場合、Directory
Connectorはディレクトリからユーザーとグループを Bitwarden組織に同期することができます。ディレクトリコネクタは、
あなたのディレクトリとBitwardenにアクセスできるどこでも実行できるスタンドアロンのアプリケーションです。



ディレクトリ-コネクタ

多くのBitwardenチームとエンタープライズ組織は、オンボーディングの努力をディレクトリコネクタに集中し、組織の保管庫管理エリアを使用してグループ-コレクションの関係を管理します。

ディレクトリコネクタは次のことを行います：

- LDAPベースのディレクトリグループをBitwardenグループと同期します
- 各グループ内のユーザーを同期させる
- 新しいユーザーを組織に招待します。
- 組織から削除されたユーザーを削除します

SSOでログイン

Bitwardenエンタープライズ組織は、SAML 2.0またはOIDCを使用して既存のIDプロバイダー（IdP）と統合することができ、組織のメンバーがSSOを使用してBitwardenにログインすることを許可します。SSOでログインすると、ユーザーの認証と保管庫の復号化が分離されます。

選択したIdPを通じて**認証**が完了し、そのIdPに接続された二要素認証プロセスが保持されます。ボールト データの**復号化には、**ユーザーの個別のキーが必要です。このキーの一部はマスター パスワードから派生します。2つの復号化オプションがあり、どちらもユーザーが通常のSSO資格情報を使用して認証します。

- **マスター パスワード**: 認証されると、組織メンバーはマスター パスワードを使用してボールト データを復号化します。
- **顧客管理の暗号化**：SSOを使用してログインし、自己ホスト型の復号化キーサーバーに接続します。このオプションを使用すると、組織のメンバーは保管庫のデータを復号化するためにマスターパスワードを使用する必要がありません。代わりに、キーコネクターは、あなたが所有し管理しているデータベースに安全に保存された復号化キーを取得します。
  - 既存のIDプロバイダーを活用してください。

- あなたのデータのエンドツーエンド暗号化を保護してください。
- ユーザーを自動的に提供します。
- SSOを使用するかしないかでアクセスを設定します。
- あなたの会社のセキュリティニーズに従って、保管庫のデータを復号化してください。

容易なオンボーディング

エンタープライズ組織は、あらゆるビジネスのための安全な基盤を築くために、さまざまなポリシーを実装することができます。
ポリシーには以下のものが含まれます：

- **二段階ログインを必要とします：**ユーザーに個人アカウントで二段階ログインを設定するように要求します。
- **マスターパスワードの要件：** マスターパスワードの強度の最小要件を設定します。
- **パスワード ジェネレーター:**パスワード ジェネレーター構成の最小要件を設定します。
- **単一組織:** ユーザーが他の組織に参加することを制限します。
- **個別の Vault を削除する:**個人所有権オプションを削除して、ユーザーに Vault アイテムを組織に保存するよう要求します。

> **Tip**
> 例えば、**個々の保管庫を削除する**ポリシーは、個々の保管庫と組織の保管庫間の相互作用に関する以前の議論に適合します。
> 一部の企業は、すべての資格情報が組織の保管庫に保持されているという保証を望むかもしれません。可能な実装方法としては、
> 各個々のユーザーが自分自身のコレクションを持つことを許可し、それは個々の保管庫とは異なり、
> 組織の所有者と管理者によって監督されることができます。

イベントログ

Bitwardenの組織には、ウェブ保管庫から直接イベントログを表示したり、Splunkのようなセキュリティ情報およびイベント管理（SIEM）
システム内で分析するためにエクスポートすることができます。イベントログには以下の情報が含まれます：

- ユーザー-アイテムの相互作用
- 保管庫のアイテムに対する変更
- オンボーディングイベント
- 組織の設定変更
- はるかに、はるかに多く

> **Tip**
> これらの利点に加えて、顧客は既存のシステムにBitwardenを密接に統合する能力を高く評価しています。Bitwarden は、既存の組織のワークフローにさらに統合するための、堅牢なパブリックAPIと完全な機能を備えたコマンド ライン インターフェイス (CLI) を提供します。

セルフホスティング

Bitwardenがどこでもパスワード管理を提供するというアプローチに従い、Bitwardenは自己ホスト型のオプションを提供して、エンタープライズのさらに広範な使用事例に対応します。企業が自己ホスト型を選択する理由は多々あります。具体的には、オンボーディング、後継、および強化された機能に関して、企業がそれを選択するいくつかの理由は次のとおりです：

- **ユーザーアカウントの即時削除：** サーバーを制御しているため、ユーザーは完全に削除することができます (彼らの個々の保管庫を含む) 。
- **ネットワークアクセス制御**：組織の所有者は、従業員がBitwardenサーバーにアクセスするために使用しなければならないネットワークアクセスを決定することができます。
- **高度なプロキシ設定：** 管理者は、特定のタイプのデバイスがBitwardenサーバーにアクセスするのを有効にするか無効にするかを選択できます。
- **既存のデータベースクラスタを使用する：**既存のMicrosoft SQL Serverデータベースに接続します。将来、追加のデータベースがサポートされる予定です。
- **添付ファイルとBitwarden Sendのストレージを増やす：** BitwardenのアイテムやBitwarden Sendのための添付ファイルは、ユーザーが提供するストレージに保管されます。

ピースを組み合わせてください

ディレクトリコネクタ、SSOでのログイン、エンタープライズポリシー、そしてあなたの保管庫は、個々にまたは調和して、あなたのオンボーディング、後継、および組織管理の経験を最適化するためにうまく機能します。次の表は、これらのピースを一つのスムーズなプロセスにまとめる方法を詳しく説明しています:

ステップ	説明
同期する	既存のディレクトリサービスからBitwardenへグループとユーザーを同期するために、Directory Connectorを使用してください。
招待	ディレクトリコネクタは、同期されたユーザーに自動的に招待を発行します。
認証する	あなたのログインをSSO実装とペアリングし、ユーザーが招待を受け入れるときにSSOでサインアップすることを要求するSSOポリシーと一緒に使用してください。

ステップ	説明
管理する	ウェブ保管庫を使用して、一部のユーザーを異なる役割に昇格させ、グループ- コレクションの関係が正しく設定されていることを確認し、適切なアクセスを適切なユーザーに付与します。
再同期する	定期的にDirectory Connectorを再実行して、 ディレクトリサービスでアクティブでなくなったユーザーをBitwardenから削除し、 新規採用者のオンボーディングを開始します。

よくある質問

Q: 従業員がすでにBitwardenアカウントを持っている場合、それを組織に紐付けて、別のBitwardenアカウントを必要としないようにすることは可能ですか？

A: はい！あなたはできます。一部のお客様は、ユーザーを組織に追加する前に、
そのユーザーが会社のメールアドレスにBitwarden保管庫を関連付けておくことを推奨しています。この選択は会社特有のもので、
どちらのアプローチも機能します。

Q: 従業員が退職した場合、彼らが会社の資格情報にアクセスできなくなるように、また彼らが個々に所有する資格情報を失わないように、彼らのアカウントを組織から切り離すことはできますか？

A: はい！それがまさにデプロビジョニングが含むものです。

Q: 私たちは、社員が会社の組織から自分の個人の保管庫に資格情報を複製するのを防ぐことができますか？

A：はい！私たちの役割ベースのアクセス制御の包括的なスイートを使用すると、資格情報を**読み取り専用**にして複製を防ぐことができます。