

管理者コンソール > 詳細

# チームとエンタープライズ移行ガイド

ヘルプセンターで表示:

<https://bitwarden.com/help/teams-enterprise-migration-guide/>

## チームとエンタープライズ移行ガイド

Bitwardenを使用した組織の安全な移行は直接的で安全です。このガイドの手順に従って、既存のパスワードマネージャーからデータとユーザーを移行してください。

1. データをエクスポートします。
2. Bitwarden 組織を作成して構成します。
3. データを Bitwarden にインポートします。
4. ユーザーをオンボーディングします。
5. コレクションとボルト アイテムへのアクセスを構成します。

### 💡 Tip

If you need assistance during your migration, our [Customer Success team is here to help!](#)

## 範囲

この文書は、現在のパスワードマネージャーからBitwardenのチームまたはエンタープライズ組織への安全なデータの移行に関するベストプラクティスを説明しています。これは、シンプルでスケーラブルな方法に基づいたセキュリティのインフラストラクチャを構築するためのものです。

パスワードの管理は、組織のセキュリティと運用効率にとって重要です。最適な移行および設定方法についての洞察を提供することは、エンタープライズツールを交換する際にしばしば必要となる試行錯誤のアプローチを最小限に抑えるように設計されています。

このドキュメントの手順は、ユーザーの使いやすさとスムーズなオンボーディングのために、**推奨される順序でリストされています。**

## ステップ1: あなたのデータをエクスポートします

他のパスワードマネージャーからのデータエクスポートは、各ソリューションで異なり、場合によっては少し難しいかもしれません。私たちのインポート&エクスポートガイドの一つを使用して、例えばLastpassや1Passwordからのエクスポートに関するヘルプを得てください。

あなたのデータの完全なエクスポートを集めるためには、エクスポートのために共有フォルダーやアイテムを単一のユーザーに割り当てる、または適切な権限を持つユーザー間で複数のエクスポートを実行することが必要かもしれません。さらに、エクスポートされたデータには、共有/組織データと並んで個々に所有されたデータが含まれる可能性がありますので、Bitwardenにインポートする前に、エクスポートファイルから個々のアイテムを削除してください。

### 📌 Note

We recommend paying special attention to the location of the following types of data during export:

- Secure documents
- Secure file attachments
- Secure notes
- SSH / RSA key files
- Shared folders
- Nested shared items
- Any customized structures within your password management infrastructure

## ステップ2: あなたの組織を設定します

Bitwardenの組織は、ユーザーと保管庫のアイテムを関連付けて、ログイン、メモ、カード、およびIDの安全な共有を行います。

 **Tip**

It's important that you create your organization first and [import data to it directly](#), rather than importing the data to an individual account and then [moving items](#) to the organization secondarily.

1. **組織を作成します。**まず、あなたの組織を作成しましょう。方法を学ぶには、[この記事](#)をご覧ください。

 **Note**

To self-host Bitwarden, create an organization on the Bitwarden cloud, generate a [license key](#), and use the key to [unlock organizations](#) on your server.

2. **ボード上の管理ユーザー**あなたの組織が作成されたら、いくつかの**管理ユーザー**をオンボーディングすることで、さらなるセットアップ手順を簡単にすることができます。組織の準備にはまだいくつかの手順が残っているため、この時点では**エンドユーザーのオンボーディングを開始しないことが重要です**。ここで管理者を招待する方法を学びましょう。
3. **IDサービスを設定する。**エンタープライズ組織は、SAML 2.0またはOpenID Connect (OIDC)を使用して**シングルサインオン (SSO)**でログインすることをサポートしています。SSOを設定するには、**設定** → **シングルサインオン**画面を開き、**組織の所有者と管理者**がアクセスできる**管理者コンソール**で行います。
4. **エンタープライズ ポリシーを有効にします。****エンタープライズポリシー**は、組織がユーザーに対するルールを実施することを可能にします。例えば、二段階ログインの使用を要求するなどです。ユーザーをオンボーディングする前に、ポリシーを設定することを強く推奨します。

### ステップ3：あなたの組織にインポートします

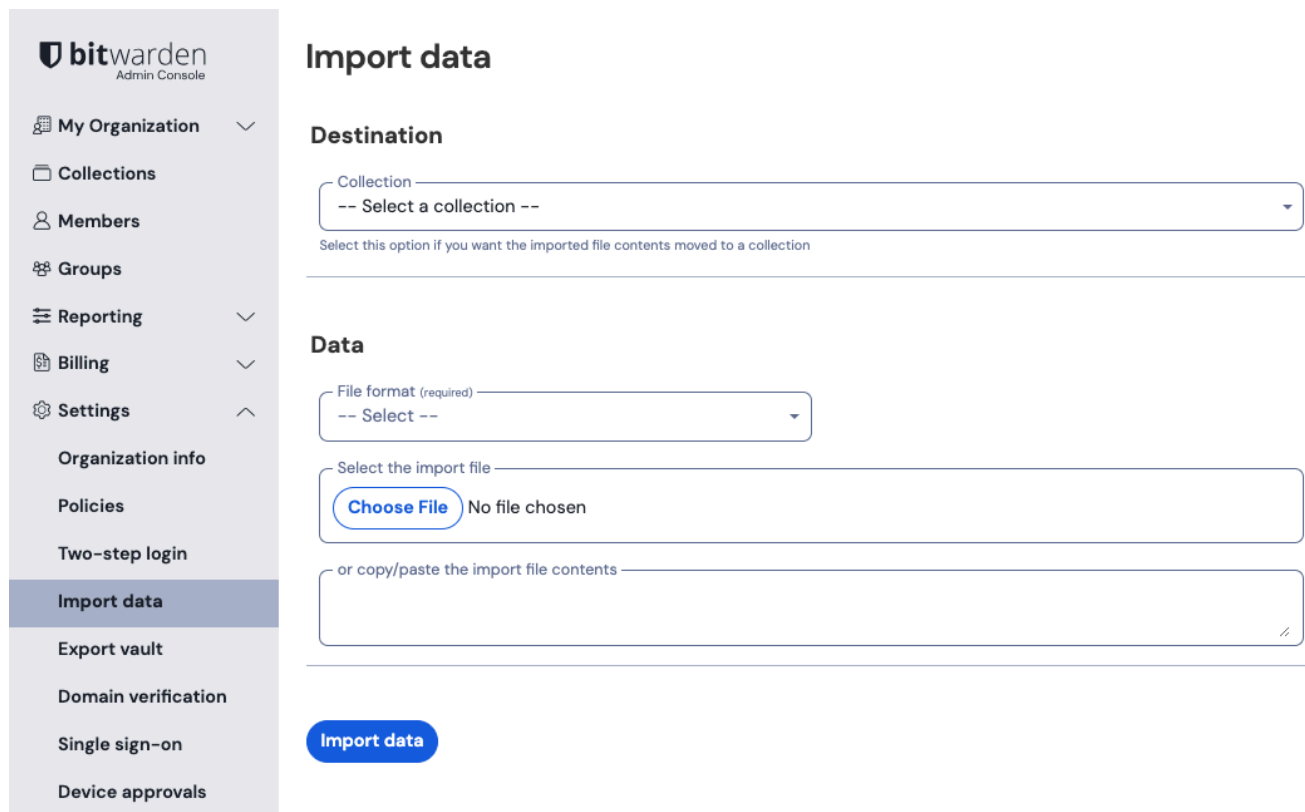
あなたの組織にデータをインポートするには：

1. Bitwardenウェブアプリにログインし、製品スイッチャー (☰) を使用して**管理者コンソール**を開きます。

The screenshot shows the Bitwarden web interface. On the left is a dark blue sidebar with navigation options: Password Manager, Vaults, Send, Tools, Reports, Settings, Password Manager (highlighted with a red box), Secrets Manager, Admin Console, and Toggle Width. The main content area is titled 'All vaults' and features a 'FILTERS' panel on the left with a search bar and a list of categories: All vaults, My vault, My Organiz..., Teams Org..., New organization, All items, Favorites, Login, Card, Identity, Secure note, Folders, No folder, Collections, Default colle..., Default colle..., and Trash. The main vault list on the right includes: All, Company Credit Card (Visa, \*4242), Personal Login (myusername), Secure Note, and Shared Login (sharedusername). Each vault entry has a checkbox, an icon, a name, a description, an owner (e.g., My Organiz... or Me), and a three-dot menu icon.

製品-スイッチャー

2. 設定 → データをインポートに移動します。



## 管理者コンソール インポート

3. フォーマットのドロップダウンから、**ファイル形式**を選択してください（下のインポートの推奨事項を参照してください）。
4. **ファイルを選択**ボタンを選択し、インポートするファイルを追加してください。

**Warning**

Import to Bitwarden can't check whether items in the file to import are duplicative of items in your vault. This means that **importing multiple files will create duplicative** vault items if an item is already in the vault and in the file to import.

5. あなたのインポートを完了するために、**データをインポート**ボタンを選択してください。

現在、添付ファイルはBitwardenのインポート操作に含まれておらず、手動で保管庫にアップロードする必要があります。詳細については、[添付ファイル](#)をご覧ください。

**Tip**

You should also recommend to employees that they export their individually-owned data from your existing password manager and prepare it for import into Bitwarden. Learn more [here](#).

**インポートの推奨事項**

あなたの組織にデータをインポートするとき、あなたには2つの選択肢があります：

1. あなたの以前のパスワードマネージャーからデフォルトのファイル形式をインポートします。
2. インポートのためにBitwarden特有の**.CSV**を条件付けする。

最適な結果を得るためには、インポート用のファイルをBitwarden **.CSV** ファイル形式にすることをお勧めします。また、上級ユーザーの方は、Bitwarden **.JSON** ファイル形式を使用することもできます。Bitwarden特有のインポートファイルの作成方法については、[このインポートガイド](#)を参照してください。

## ステップ4：ユーザーのオンボーディング

Bitwardenは、ウェブ保管庫を通じた手動のオンボーディングと、SCIM統合または既存のディレクトリサービスからの同期を通じた自動オンボーディングをサポートしています。

### 手動オンボーディング

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。新しいユーザーを招待する方法を[ここで](#)学びましょう。

### 自動オンボーディング

自動化されたユーザーオンボーディングは、Azure AD、Okta、OneLogin、およびJumpCloudとのSCIM統合を通じて、またはDirectory Connectorを使用して利用可能です。これは、既存のディレクトリサービスからユーザーとグループを同期するデスクトップアプリおよびCLIツールとして利用可能なスタンドアロンのアプリケーションです。

どちらを使用しても、ユーザーは自動的に組織に招待され、Bitwarden CLIツールを使用して手動または自動で確認できます。

## ステップ5：コレクションとアイテムへのアクセスを設定する

コレクション、グループ、およびグループレベルまたはユーザーレベルの権限を通じてアクセスを設定することにより、エンドユーザーと保管庫のアイテムを共有します。

### コレクション

Bitwardenは、組織がデータを簡単に、安全に、そしてスケーラブルな方法で共有することを可能にします。これは、共有された秘密やアイテム、ログインなどをコレクションに分割することで達成されます。

コレクションは、ビジネス機能、グループ割り当て、アプリケーションアクセスレベル、またはセキュリティプロトコルによるなど、さまざまな方法でセキュアなアイテムを組織化することができます。コレクションは共有フォルダーとして機能し、ユーザーグループ間で一貫したアクセス制御と共有を可能にします。

他のパスワードマネージャーからの共有フォルダーは、タイプ: アセットハイパーリンク id:

4DdJLAtEuHMYIE581pPErFで見つけられる組織インポートテンプレートを使用して、Bitwardenにコレクションとしてインポートすることができます。これは、[コレクション](#)列に共有フォルダーの名前を配置することで行います。例えば、次のように変換します：

url	username	password	extra	name	grouping	fav
https://azure.microsoft.com/en-us/	AzureUser	5HDXWtuAAK3SX8		Azure Login	Shared-Systems	0
https://github.com/login	GitHubUser	P4JUghjRfhKrDJ		Github	Shared-Systems	0
https://adobe.com	AdobeUser	T6RYSbD5mn78ab		Adobe Login	Shared-Design	0
https://shutterstock.com	ShutterStock	749bs2saWb3bxH		Shutterstock	Shared-Design	0
https://usps.com	USPSUser	6UmtWlKgydBmAZ		USPS Shipping	Shared-Shipping	0
https://ups.com	UPSUser	YBD7ftBZbosS9u		UPS Login	Shared-Shipping	0
https://fedex.com	FedexUser	y44xgs5fiyYZNU		FedExUser	Shared-Shipping	0

Migration Export Example

に

collections	type	name	notes	fields	login_uri	login_username	login_password	login_totp
Shared-Systems	login	Azure Login			https://azure.microsoft.com/en-us/	AzureUser	5HDXWtuAAK3SX8	
Shared-Systems	login	Github			https://github.com/login	GitHubUser	P4JUghjRfhKrDJ	
Shared-Design	login	Adobe Login			https://adobe.com	AdobeUser	T6RYSbD5mn78ab	
Shared-Design	login	Shutterstock			https://shutterstock.com	ShutterStock	749bs2saWb3bxH	
Shared-Shipping	login	USPS Shipping			https://usps.com	USPSUser	6UmtWlKgydBmAZ	
Shared-Shipping	login	UPS Login			https://ups.com	UPSUser	YBD7ftBZbosS9u	
Shared-Shipping	login	FedExUser			https://fedex.com	FedexUser	y44xgs5fiyYZNU	

Migration Import Example

コレクションは、グループと個々のユーザーの両方と共有することができます。コレクションにアクセスできる個々のユーザーの数値を制限することで、管理者の管理がより効率的になります。もっと詳しくは[こちら](#)をご覧ください。

## グループ

グループを使用して共有することは、資格情報と秘密のアクセスを提供する最も効果的な方法です。ユーザーと同様に、グループもSCIMまたはDirectory Connectorを使用して組専に同期することができます。

## 権限

Bitwardenのコレクションの権限は、グループまたはユーザーレベルで割り当てることができます。これは、各グループまたはユーザーが同じコレクションに対する権限を設定できることを意味します。コレクションの権限には、**読み取り専用とパスワードを隠す**のオプションが含まれています。

Bitwardenは、ユーザーとコレクションアイテムの最終的なアクセス権限を決定するために、権限の組み合わせを使用します（[詳細はこちら](#)）。例えば：

- ユーザーAはTier 1サポートグループの一部であり、サポートコレクションへのアクセス権限がありますが、読み取り専用の権限です。
- ユーザーAはまた、サポートコレクションへの読み書きアクセス権を持つサポート管理グループのメンバーでもあります。
- このシナリオでは、ユーザーAはコレクションに読み書き（読み-書き込み）ができます。

## 移民支援

Bitwardenのカスタマーサクセスチームは、あなたの組織のための優先サポートで24/7利用可能です。ご不明な点やお手伝いが必要な場合は、遠慮なくお問い合わせください。