管理者コンソール > 詳細

LastPassエンタープライズ移行ガイド

LastPass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、LastPassからデータとユーザーを移行してください:

1. Bitwarden 組織を作成して構成します。
2. データを Bitwarden にインポートします。
3. ユーザーをオンボーディングします。
4. コレクションとボールト 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、LastpassからBitwarden
チームまたはエンタープライズ組織へのデータを安全に移行するための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ためのインフラストラクチャを構築します。

パスワード管理は、組織のセキュリティと業務効率にとって非常に重要です。最適な移行や設定を行う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ことを目指しています。

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てください。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**あなたの組電が作成されたら、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、管理者コンソールで組織の**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2：データをインポートする

LastPassからのエクスポート

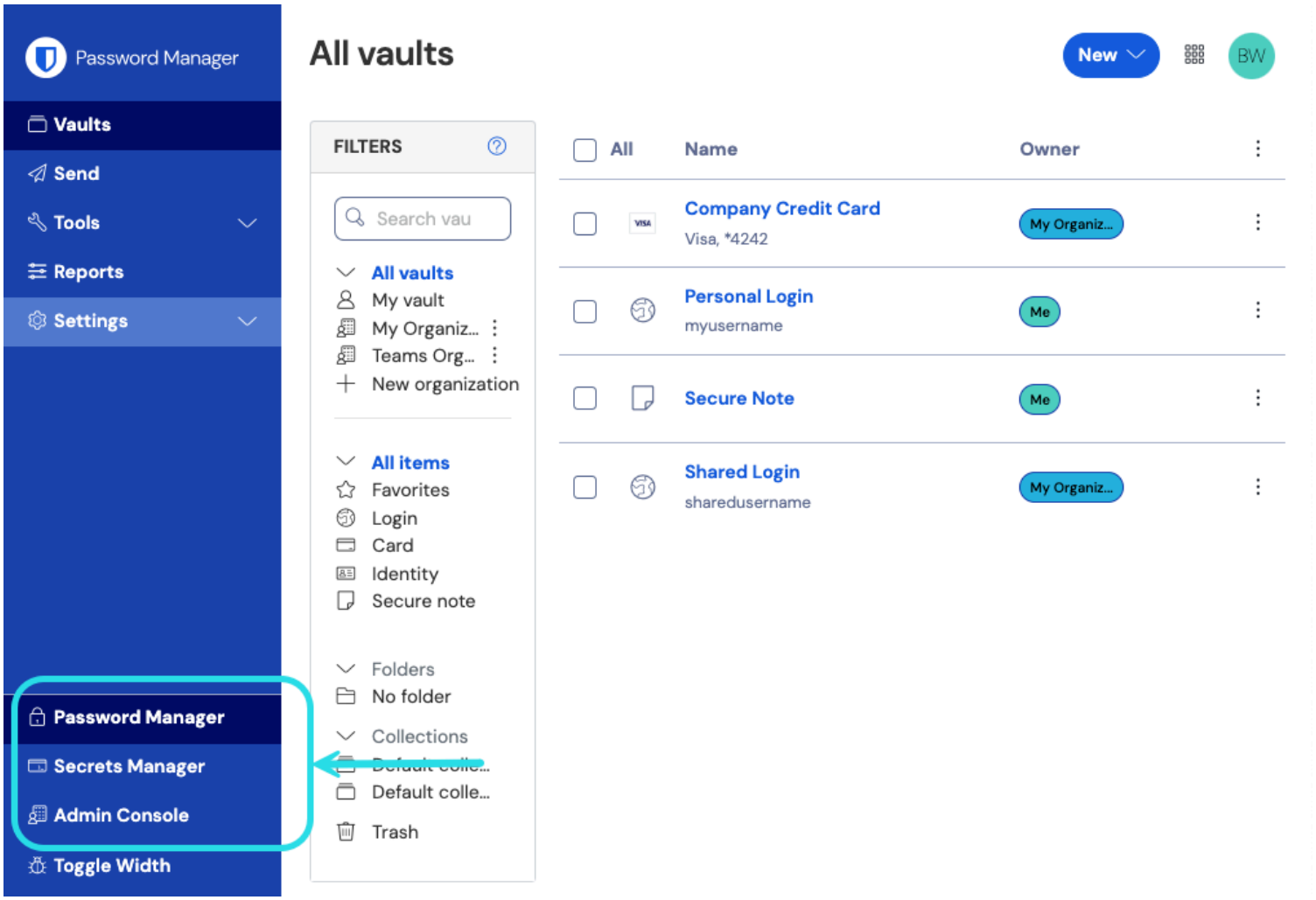
LastPassウェブ保管庫から共有データの全エクスポートを`.csv`ファイルとして作成してください（方法の学習）。
完全なエクスポートを集めるためには、エクスポートを作成する前に、
すべての共有フォルダーをエクスポートするユーザーに割り当てることが必要かもしれません。

さらに、LastPassで作成されたエクスポートには、
個人の保管庫からのデータと割り当てられた共有フォルダーからのデータの両方が含まれます。この段階では、
作成したエクスポートが共有データをすべて含み、個人データが含まれていないことを確認するために、監査を推奨します。

Bitwarden にインポート

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。



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。

3. 申し訳ありませんが、あなたの要求を理解するのが難しいです。
   具体的なフィールドやドロップダウンメニューの項目を提供していただけますか？

   - **コレクション:**インポートされたコンテンツを既存のコレクションに移動するかどうかを選択します。ほとんどの場合、インポートがあなたの代わりにそれを行うため、Bitwardenでコレクションを作成する必要はありませんので、このオプションは空白のままにしておいてください。

   - ファイル形式: **Lastpass (csv)**を選択します。

4. 「ファイルを選択」をクリックし、インポートするファイルを追加するか、ファイルの内容を入力ボックスにコピー＋ペーストしてください。

> **⚠ 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. **データをインポート**を選択して、インポートをトリガーします。

添付ファイルは手動でボールトにアップロードする必要があります。LastPassにネストされた共有フォルダーは、Bitwarden組織内でネストされたコレクションとして再作成されることにメモしてください。ただし、「親」コレクションにデータがない場合、一致する名前で親コレクションを手動で作成する必要があります。

> **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.

ステップ3：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をサポートし、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。

> **Tip**
> Once users are onboarded, instruct them to import their personal data to Bitwarden using an exported file or, if their LastPass accounts are still active, using the **Direct import** method described here.

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、JumpCloudとのSCIM統合を通じて、またはDirectory Connectorというスタンドアロンのアプリケーションを使用して利用可能です。これはデスクトップアプリとCLIツールで、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します。

どちらを使用しても、ユーザーは自動的に組織への参加を招待され、Bitwarden CLIツールを使用して手動または自動で確認することができます。

> **Tip**
> Once users are onboarded, instruct them to import their personal data to Bitwarden using an exported file or, if their LastPass accounts are still active, using the **Direct import** method described here.

ステップ4：コレクションとアイテムへのアクセスを設定します

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、組織が敏感なデータを簡単に、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ものなど、
多くの方法で組織がアイテムを保護することができます。コレクションは共有フォルダーのように機能し、
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。

LastPass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:
4DdJLATeuhMYlE581pPErF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。共有フォルダーの名前を`コレクション`の列に配置します。

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。

> **Note**
> Nested collections do not inherit the permissions of the top level collection. See using groups to designate permissions.

グループ

資格情報や秘密のアクセスを提供するための最も効果的な方法は、グループを使用して共有することです。グループは、ユーザーと同様に、
SCIMまたはディレクトリコネクタを使用して組織と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して異なる権限で設定できることを意味します。
コレクション権限のオプションには以下のオプションが含まれます:

- 閲覧可能

- パスワード以外は閲覧可能
- 編集可能
- パスワード以外は編集可能
- すべての現在および将来のコレクションへのアクセスを許可します

権限についてもっと学ぶここ。Bitwardenは、ユーザーとコレクション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。例えば：

- ユーザーAはTier 1サポートグループの一部で、サポートコレクションへのアクセス権限があり、表示権限があります。
- ユーザーAはまた、サポートコレクションへの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、編集アクセスが可能です。
- このシナリオでは、ユーザーAはコレクションを編集することができます。

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。