bitwarden | ヘルプセンターの記事

PASSWORD MANAGER > 保管庫管理

保管庫健康レポート

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

保管庫健康レポート

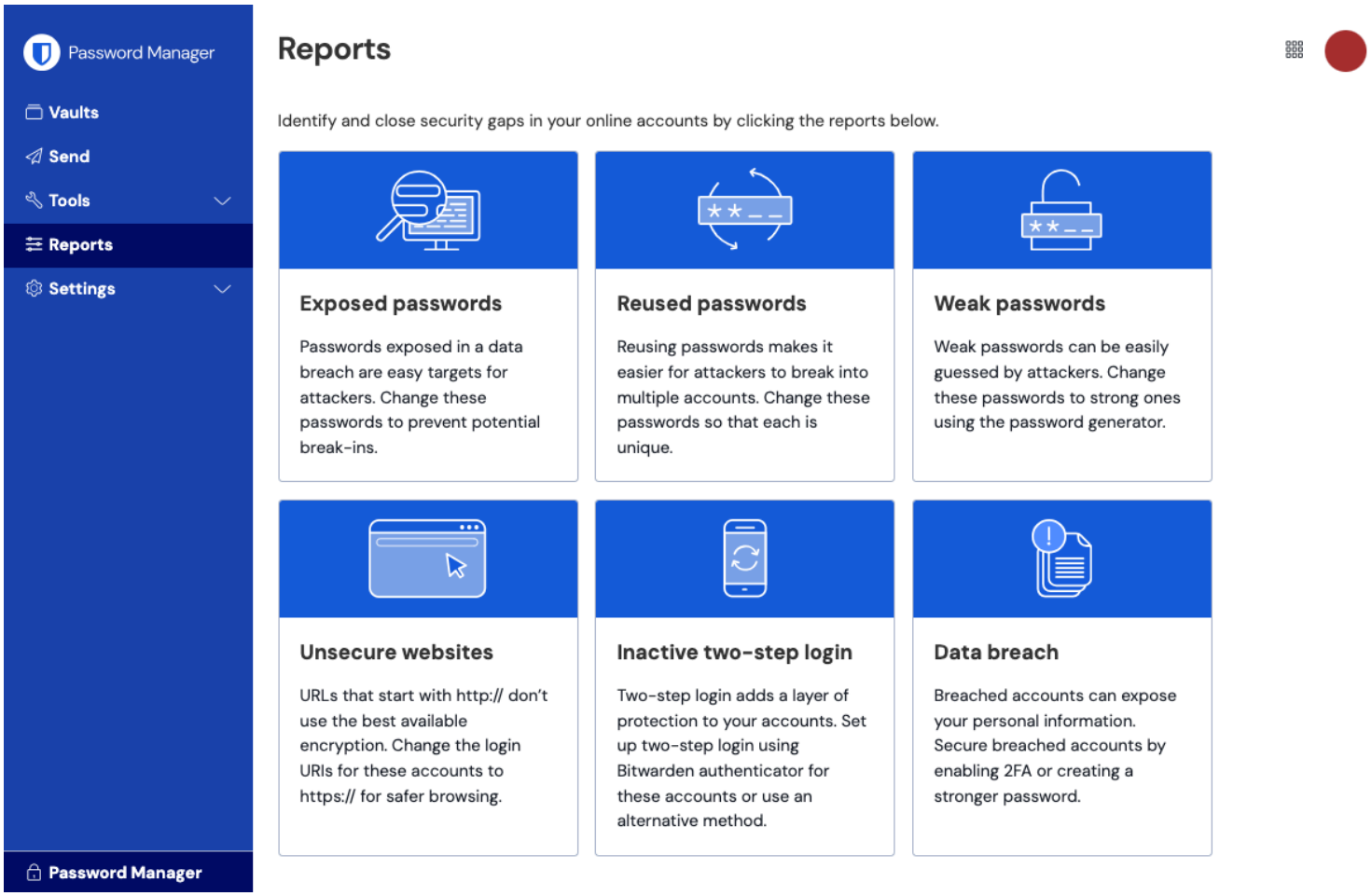
保管庫の健康レポートは、あなたのBitwarden個人または組織の保管庫のセキュリティを評価するために使用することができます。例えば、再利用されたパスワードと弱いパスワードのレポートなどのレポートは、あなたのクライアントでローカルに実行されます。これにより、Bitwardenがこのデータの暗号化されていないバージョンにアクセスすることなく、問題のあるアイテムを特定することができます。

> **Note**
> ほとんどの保管庫健康レポートは、有料の組織（ファミリー、チーム、またはエンタープライズ）のメンバーを含むプレミアムユーザーのみが利用可能ですが、データ漏洩レポートはすべてのユーザーが無料で利用できます。

レポートを表示する

あなたの**個々の保管庫**の健康レポートを実行するには：

1. ウェブアプリにログインし、ナビゲーションから**レポート**を選択してください。



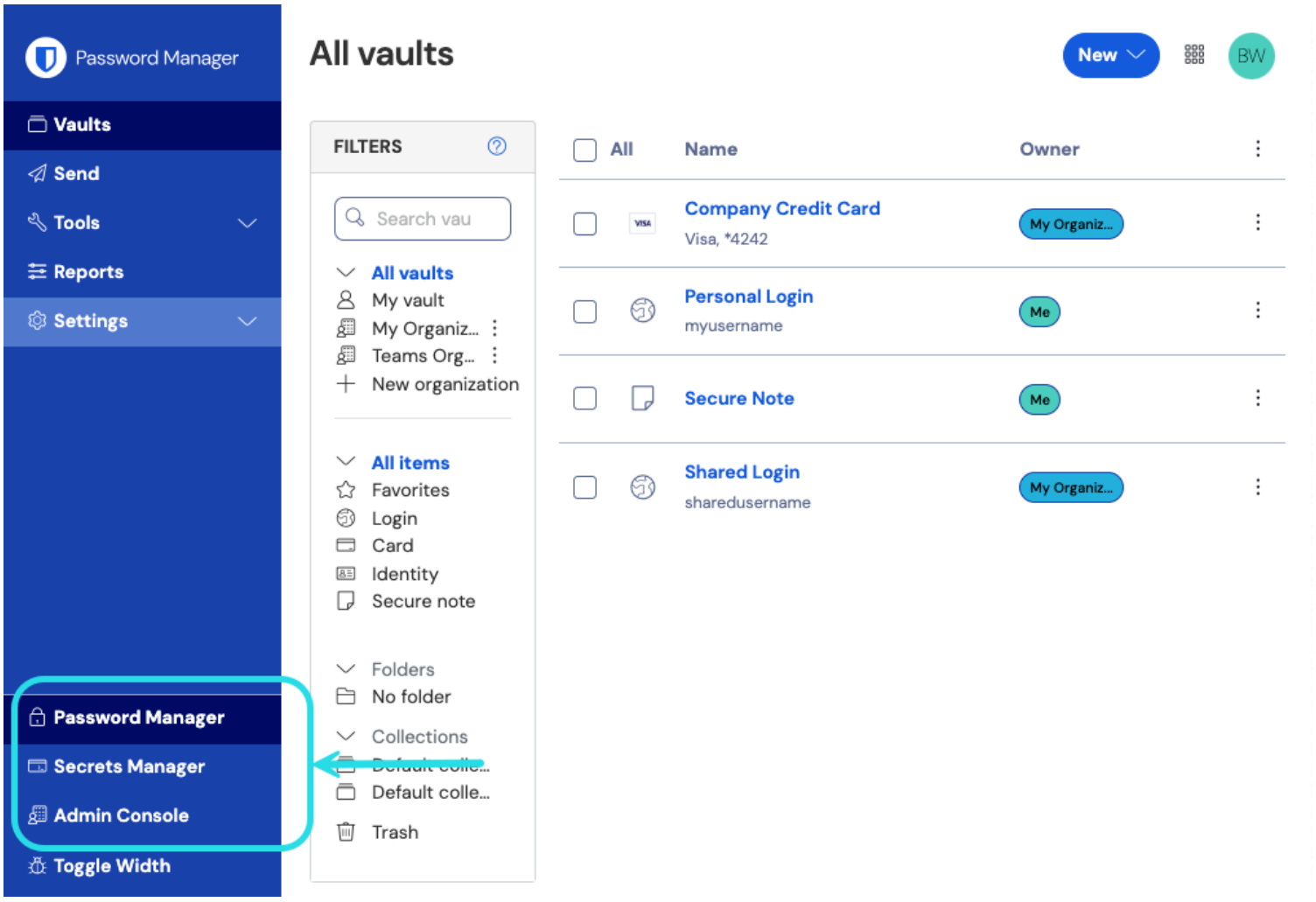
レポートページ

2. 実行するレポートを選択してください。

あなたの**組曳の保管庫**の任意の保管庫健康レポートを実行するには：

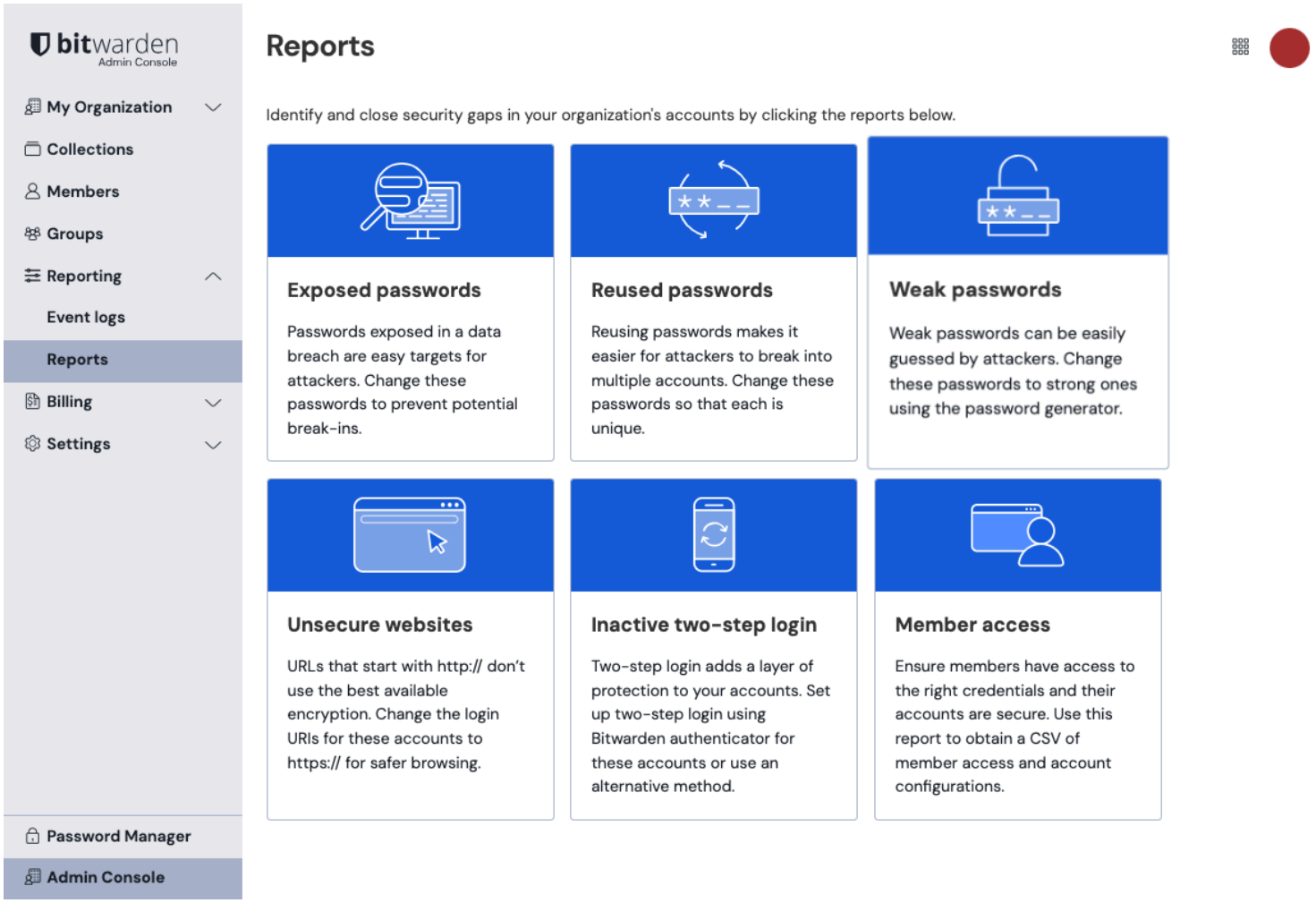
1. Bitwardenウェブアプリにログインしてください。

2. 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

3. あなたの組織で、ナビゲーションから**レポート** → **レポート**を選択してください。



組織のレポート

4. 実行するレポートを選択してください。

利用可能なレポート

パスワード流出済みレポート

流出済みパスワードレポートは、公にリリースされたり、
ハッカーによってダークウェブで販売されたりした既知のデータ漏洩で発見されたパスワードを特定します。

このレポートは、信頼性のあるウェブサービスを使用して、すべてのパスワードのハッシュの最初の5桁を、
既知の漏洩したパスワードのデータベースで検索します。返された一致するハッシュのリストは、
あなたのパスワードの完全なハッシュとローカルで比較されます。その比較は、あなたのk-匿名性を保持するために、
ローカルでのみ行われます。

一度特定されたら、問題のあるアカウントやサービスに対して新しいパスワードを作成するべきです。

> **Tip**
> なぜパスワードのハッシュの最初の5桁を使用するのですか？
>
> もし、あなたの実際のパスワードを使ってレポートが行われたのであれば、それが流出したかどうかは問題ではなく、
> あなたは自発的にそれをサービスに漏らしたことになる。このレポートの結果は、
> あなたのアカウントが侵害されたことを意味するのではなく、
> 暴露されたパスワードのこれらのデータベースで見つかったパスワードを使用していることを意味する可能性があります。

再利用されたパスワードのレポート

再利用されたパスワードのレポートは、保管庫内の非ユニークなパスワードを識別します。同じパスワードを複数のサービスで再利用すると、1つのサービスが侵害されたときに、ハッカーがあなたのオンラインアカウントにより簡単にアクセスできるようになります。

一度特定されたら、問題のアカウントやサービスに対してユニークなパスワードを作成すべきです。

弱いパスワードのレポート

弱いパスワードレポートは、ハッカーやパスワードを解読するための自動化ツールによって簡単に推測される弱いパスワードを特定し、その弱さの重大性によって並べ替えます。このレポートは、パスワードの強度分析にzxcvbnを使用しています。

一度特定されたら、問題のあるアカウントやサービスに対して強力なパスワードを生成するために、Bitwardenパスワードジェネレーターを使用すべきです。

保護されていないウェブサイトのレポート

保護されていないウェブサイトのレポートは、保護されていない（`http://`）スキームをURIで使用するログインアイテムを識別します。TLS/SSLを使用して通信を暗号化するためには、`https://`を使用する方がはるかに安全です。詳しくは、URIの使用をご覧ください。

一度特定されたら、問題のあるURIを`http://`から`https://`に変更すべきです。

非活動二要素認証レポート

非アクティブな二要素認証レポートは、以下の場合にログインアイテムを特定します：

- このサービスでは、TOTPを介した二要素認証（2FA）が利用可能です。
- あなたはTOTP認証キーを保存していません

二要素認証（2FA）は、あなたのアカウントを保護するための重要なセキュリティ手順です。どのウェブサイトでも提供している場合は、常に二要素認証を有効にすべきです。不適切なアイテムは、URI-データとhttps://2fa.directory/からのデータを相互参照することで特定されます。

一度特定されたら、各違反アイテムに対して指示ハイパーリンクを使用して二要素認証を設定してください：

レポートの指示

データ漏洩レポート（個々の保管庫のみ）

データ漏洩レポートは、Have I Been Pwned（HIBP）というサービスを使用して、既知の漏洩で侵害されたデータ（メールアドレス、パスワード、クレジットカード、生年月日など）を特定します。

Bitwardenアカウントを作成するとき、それを使用する前にマスターパスワードに対してこのレポートを実行するオプションがあります。
このレポートを実行するには、マスターパスワードのハッシュがHIBPに送信され、流出済みのハッシュと比較されます。
あなたのマスターパスワード自体は、Bitwardenによって決して流出済みになりません。

HIBPによれば、「ブリーチ」は「データが脆弱なシステムで不注意に流出済みの事故、通常はアクセス制御が不十分であるか、
ソフトウェアのセキュリティが弱いため」と定義されています。詳細については、HIBPのFAQsドキュメンテーションを参照してください。

ⓘ Note

Bitwardenをセルフホストしている場合、インスタンスでデータ侵害レポートを実行するには、
APIへの呼び出しを許可するHIBPサブスクリプションキーを購入する必要があります。

キーを手に入れたら、`./bwdata/env/global.override.env`を開き、`globalSettings__hibpApiKey`
のプレースホルダーの値を購入したAPIキーに置き換えてください:

```Bash
globalSettings__hibpApiKey=REPLACE
```

詳細については、環境変数の設定をご覧ください。