生体認証でロック解除

生体認証でロック解除

Bitwardenは、保管庫をロック解除する方法として生体認証を受け入れるように設定できます。

生体認証は、**保管庫をロック解除するためだけに使用**できます。マスターパスワードを使用するか、デバイスでログインする必要があります。また、有効にした2段階ログイン方法も**ログイン**時に使用する必要があります。生体認証でのロック解除は、
パスワードレスのログインを設計するための機能ではありません。違いがわからない場合は、ロック解除とログインの理解をご覧ください。

> **ⓘ Note**
>
> 生体認証の機能は、あなたのデバイスやオペレーティングシステムに組み込まれたセキュリティの一部です。
> Bitwardenはこの検証を行うためにネイティブAPIを活用しており、したがって**Bitwardenはデバイスから生体認証情報を受け取りません。**

生体認証でロック解除を有効にする

Bitwardenのモバイル、デスクトップ、およびブラウザ拡張機能で、生体認証によるロック解除を有効にすることができます:

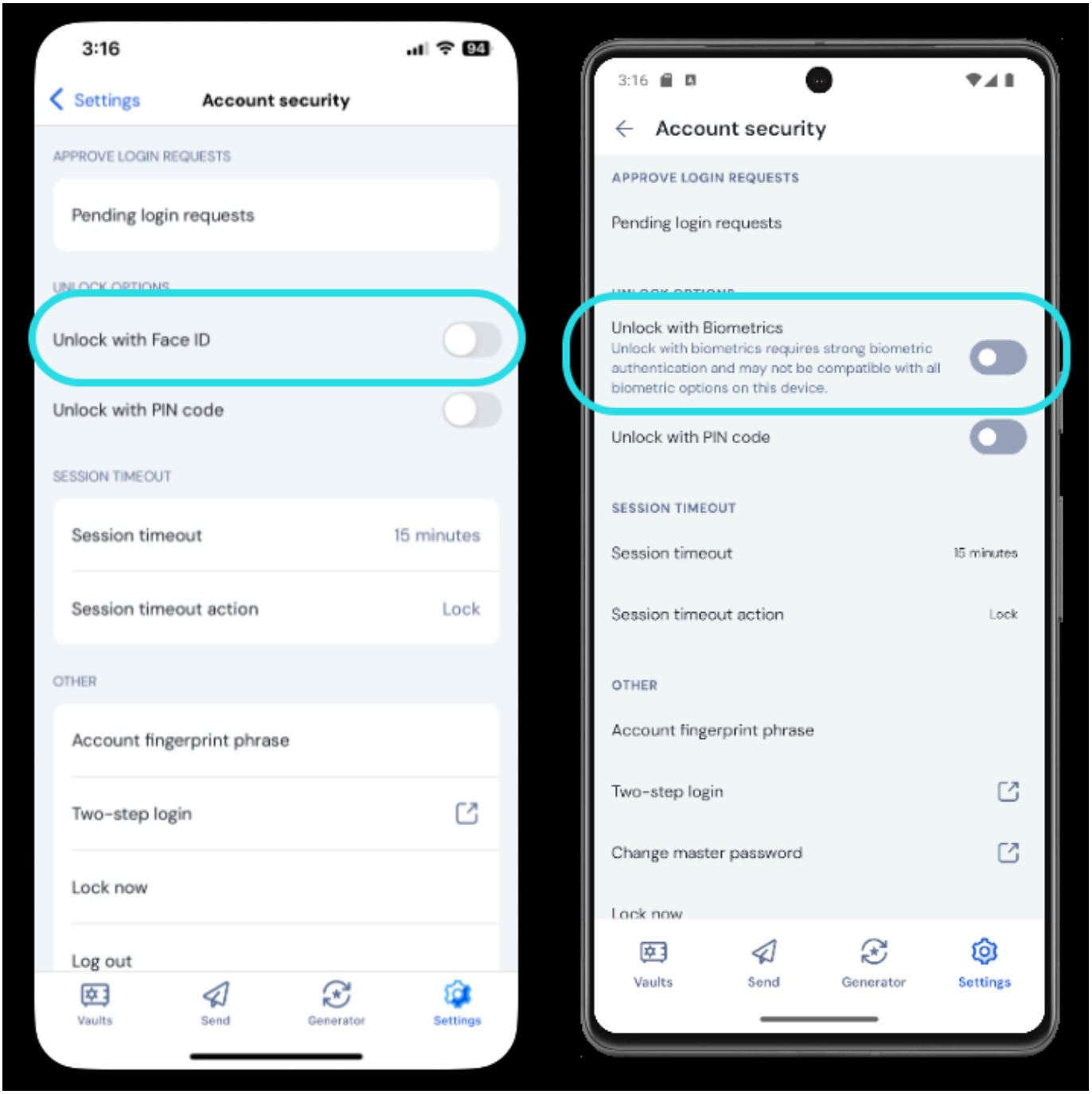
⇒モバイル

モバイル用に有効にする

生体認証によるロック解除は、Android（Google PlayまたはFDroid）では指紋認証によるロック解除または顔認証によるロック解除、iOSではTouch IDおよびFace IDを介してサポートされています。

モバイルデバイスで生体認証によるロック解除を有効にするには：

1. あなたのデバイスのネイティブ設定（例：iOSの⚙ **設定**アプリ）で、生体認証方法がオンになっていることを確認してください。
2. あなたのBitwardenアプリで、⚙ **設定**タブを開きます。
3. アカウントのセキュリティセクションを開き、有効にしたい生体認証のオプションをタップしてください。この画面で利用できるものは、あなたのデバイスのハードウェア能力と、あなたが有効にしたもの（**ステップワン**）によって決まります。例えば：



Biometric unlock on mobile

このオプションをタップすると、生体認証（例えば、顔や親指のプリント）を入力するように求められます。トグルは、生体認証でロック解除が成功したときに入力されます。

マスターパスワードの確認待ちで無効化されました

あなたのマスターパスワードの確認待ちで自動入力のための生体認証ロック解除が無効化されているというレポートのメッセージを受け取った場合：

1. Bitwardenで一時的に自動入力をオフにします。
2. Bitwardenで生体認証を再度有効にします。

3. Bitwardenで自動入力を再度オンにしてください。

⇒デスクトップ

デスクトップで有効にする

生体認証によるロック解除は、PIN、顔認証、またはWindows Helloの生体認証要件を満たすその他のハードウェアを使用したWindows Hello経由のWindowsと、Touch ID経由のmacOSでサポートされています。

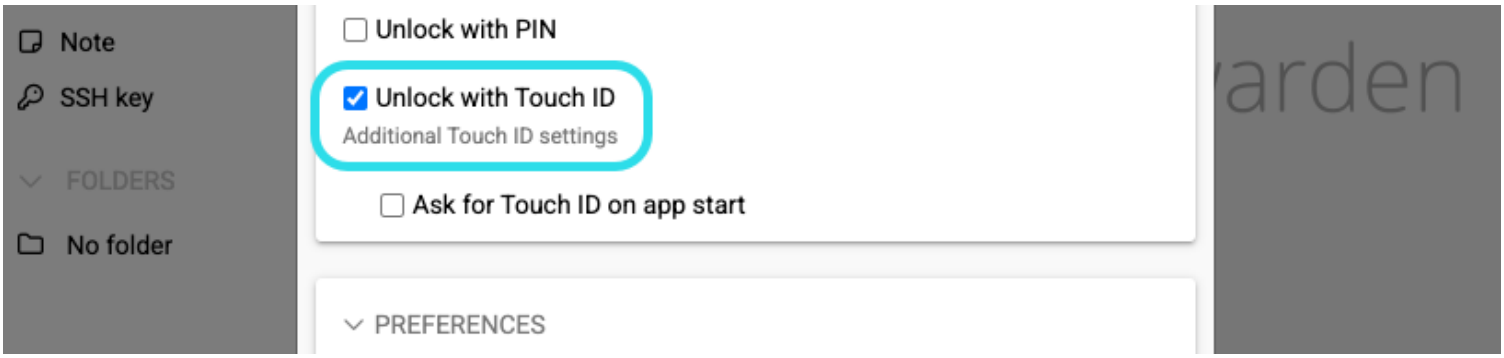
生体認証でのロック解除は、デスクトップアプリにログインしている各アカウントごとに別々に設定されます。
生体認証でロック解除を有効にするには：

1. あなたのデバイスのネイティブ設定（例えば、macOSの⚙ **システム環境設定**アプリ）で、
   生体認証方法がオンになっていることを確認してください。

> **Tip**
> Windowsユーザーは、デスクトップの設定でWindows Helloをオンにする前に、Microsoft Visual C++ Redistributableをインストールする必要があるかもしれません。

2. Bitwardenアプリで、設定を開きます（Windowsでは、**ファイル → 設定**）（macOSでは、**Bitwarden → 環境設定**）。

3. セキュリティセクションで、有効にしたい生体認証オプションを選択してください。この画面で利用できるものは、
   あなたのデバイスのハードウェア能力と、あなたがオンにしたもの（**ステップ1**）によって決まります。例えば：

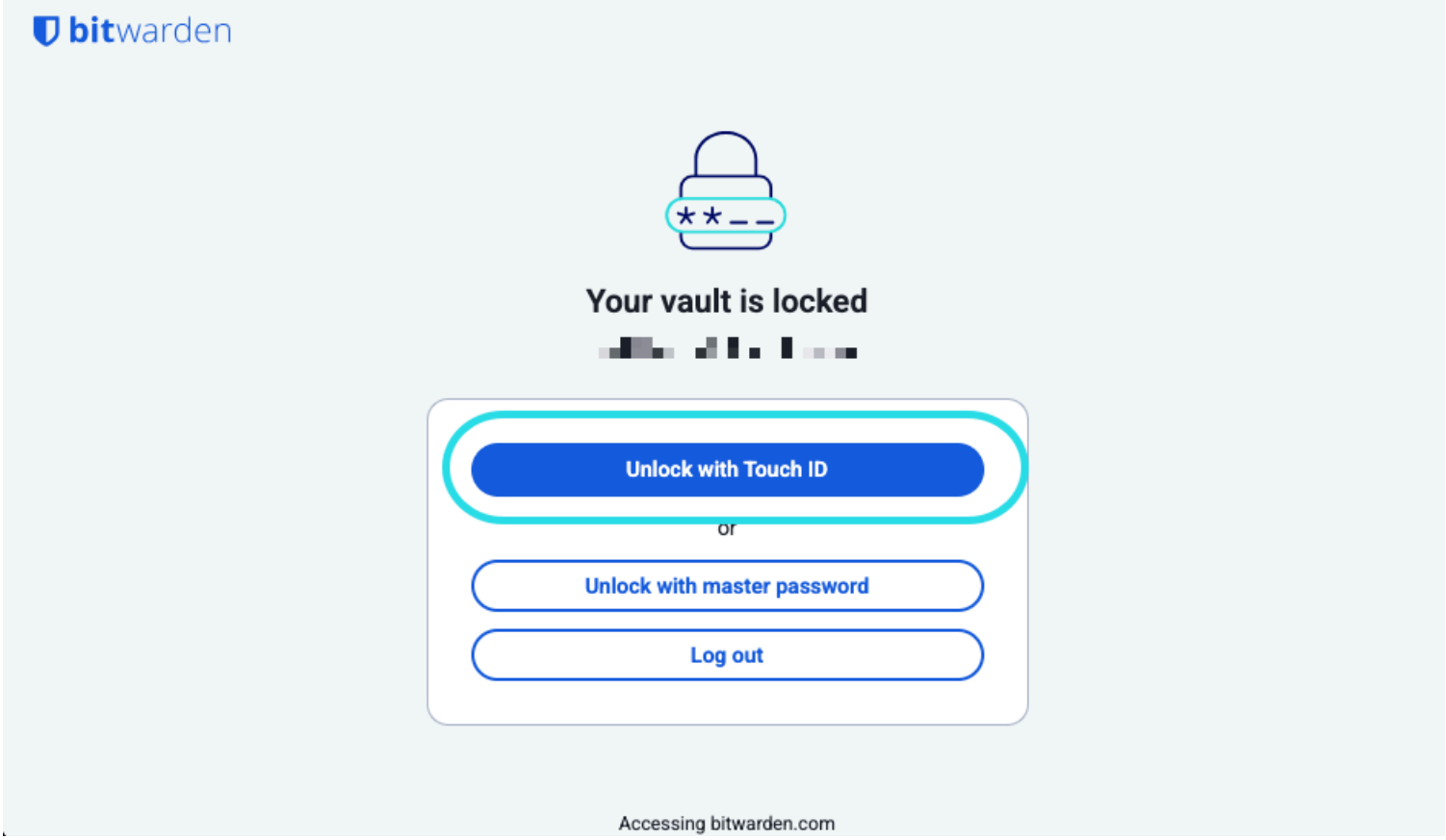


Unlock with biometrics toggle

4. 必要に応じて、**アプリ起動時にパスワード（またはPIN）を要求する**または**アプリ起動時に生体認証を求める**オプションを選択して、
   デスクトップアプリが起動時にどのように動作するかを設定します。

> **Tip**
> Windowsを使用している場合、Bitwardenは、セキュリティを最大化するために、**最初のログイン後にパスワード（またはPIN）を要求する**を使用することをお勧めします。

どちらのオプションも選ばない場合、ログイン画面で「**生体認証で**ロック解除ボタンを選択するだけで、生体認証オプションが求められます。



Unlock desktop with biometric

⇒ブラウザ拡張機能

ブラウザ拡張機能における生体認証について

生体認証によるロック解除は、Bitwardenデスクトップアプリとの統合を通じて拡張機能でサポートされています。これは実際的には次の意味です:

1. **すべてのブラウザ拡張機能については**、進行する前にデスクトップで生体認証によるロック解除を有効にする必要があります。
   Safariを除くすべてのブラウザでは、Bitwardenのデスクトップアプリがログインし、実行中でなければ、
   ブラウザの拡張機能で生体認証を使用してロック解除することはできません。

2. ブラウザの拡張機能は、デスクトップと同じ生体認証オプションをサポートしています。Windowsの場合は、Windows Helloを使用してPIN、顔認証、またはWindows Helloの生体認証要件を満たすその他のハードウェア、macOSの場合はTouch IDを使用します。

統合を有効にする前に心に留めておくべき2つのことは、以下に記載されている**権限**と**サポート可能性**です。

権限

この統合を容易にするために、ブラウザの拡張機能**Safariを除く**は、
Bitwardenが協力するネイティブアプリケーションと通信するための新しい権限を受け入れるように求めます。この権限は安全で、**オプション**ですが、生体認証でロック解除を有効にするために必要な統合を有効にします。

この権限を拒否すると、生体認証でロック解除する機能なしで、通常通りブラウザの拡張機能を使用することができます。

サポータビリティ

生体認証でのロック解除は、**Chromiumベースの**ブラウザ（Chrome、Edge、Opera、Braveなど）、Firefox 87+、およびSafari 14+の拡張機能でサポートされています。生体認証でのロック解除は**現在以下ではサポートされていません**:

- Firefox ESR (Firefox v87+は動作します)。
- Microsoft App Storeデスクトップアプリ（bitwarden.com/ja-jp/ダウンロードで利用可能なサイドロードされたWindowsデスクトップアプリは問題なく動作します）。
- サイドロードされたMacOSデスクトップアプリ（App Storeのデスクトップアプリは問題なく動作します）。

ブラウザ拡張機能を有効にする

あなたのブラウザ拡張機能で生体認証によるロック解除を有効にするには：

> **Tip**
>
> デスクトップアプリで生体認証（Windows HelloまたはTouch ID）を有効にする必要があります。デスクトップアプリでWindows Helloオプションが表示されない場合は、Microsoft Visual C++ Redistributableをインストールする必要があるかもしれません。さらに、**Safariを使用している場合**は、**ステップ4**に直接進むことができます。

1. Bitwardenのデスクトップアプリで、設定に移動します（Windowsでは、**ファイル → 設定**）（macOSでは、**Bitwarden → 環境設定**）。
2. オプションセクションまでスクロールダウンし、**ブラウザ統合を許可する**ボックスをチェックしてください。

> **Tip**
>
> 必要に応じて、**ブラウザ統合に対する確認を必要とする**オプションをチェックして、統合を有効にするときにユニークな指紋確認ステップを必要とします。

3. あなたのブラウザで、拡張機能管理者に移動します（例：`chrome://extensions`または`brave://extensions`）、Bitwardenを開き、**ファイルURLへのアクセスを許可する**オプションを切り替えます。

   すべてのブラウザでこれをオンにする必要はありませんので、このステップをスキップして、残りの手順が機能しない場合にのみ戻ってきてください。

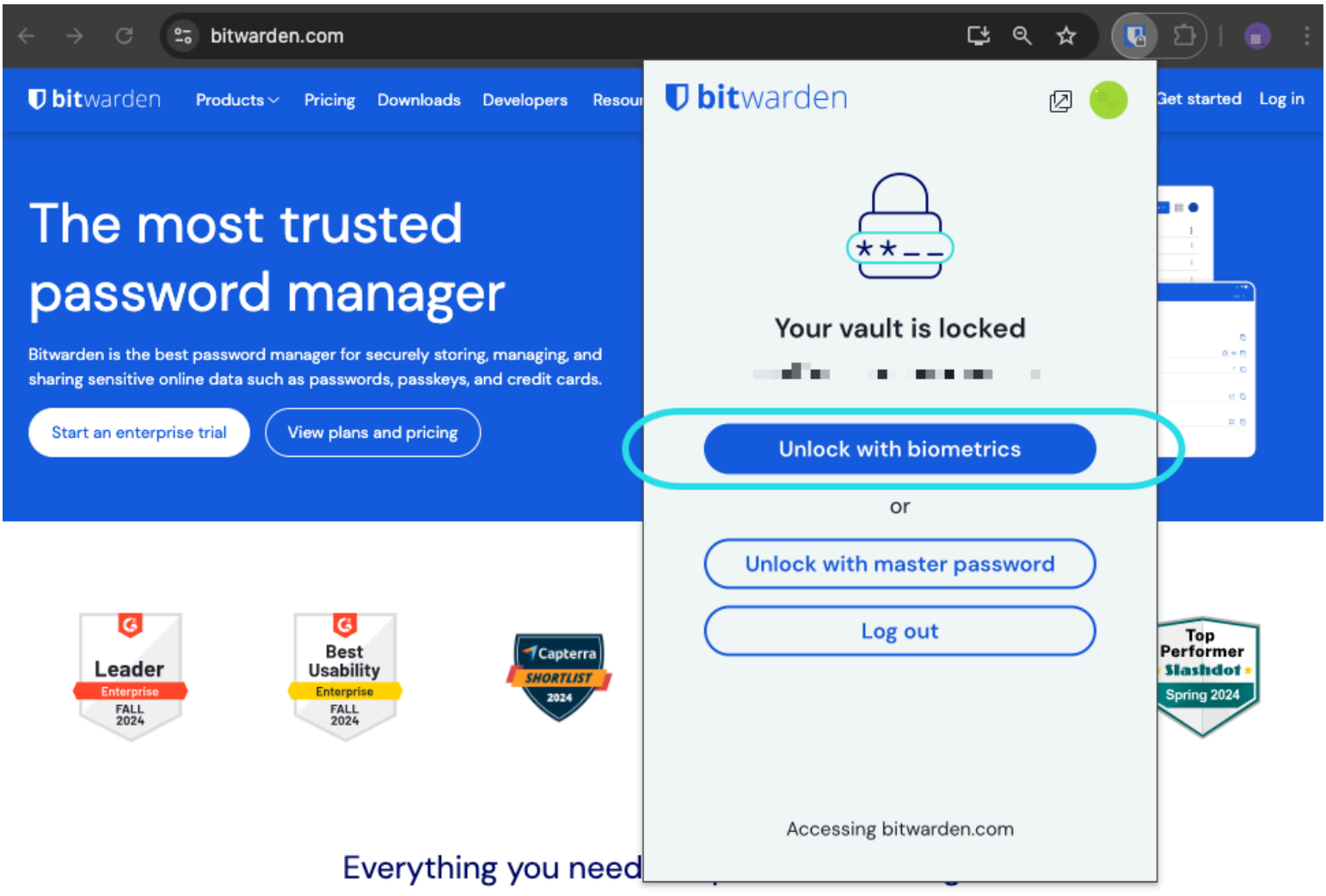
4. あなたのブラウザ拡張機能で、⚙ **設定**タブを開きます。
5. セキュリティセクションまでスクロールダウンし、**生体認証でロック解除**のボックスをチェックしてください。

> **Tip**
> この段階で、Bitwardenが 協力するネイティブアプリケーションと通信する ことを許可するように求められる場合があります。
> この権限は安全ですが、**オプション**であり、上記のようにデスクトップとブラウザ拡張機能との通信を可能にするだけです。

デスクトップアプリがあなたに生体認証の入力を促します。これにより、初期設定手順が完了します。
検証を必要とするオプションを選択した場合（**ステップ二**）、指紋検証チェックを承認する必要があります。

6. ブラウザの拡張機能が起動時に自動的に生体認証の入力を求めるようにするには、
   起動時に生体認証を求めるオプションがオンになっていることを確認してください。

ブラウザの拡張機能を開くと、自動的に生体認証が求められます。プロンプトオプションをオンにする場合（**ステップ六**）、
ロック解除画面で**生体認証でロック解除**ボタンを使用します：



Browser extension unlock with biometrics

> **Tip**
> デスクトップアプリはログインする必要がありますが、
> 生体認証でブラウザの拡張機能をロック解除するためにはロック解除済みである必要はありません。

マスターパスワードの確認待ちで無効化されました

あなたがメッセージを受け取り、生体認証によるロック解除がマスターパスワードの確認待ちで自動入力が無効になっているとレポートされた場合：

1. Bitwardenで一時的に自動入力をオフにします。
2. Bitwardenで生体認証を再度有効にします。
3. Bitwardenで自動入力を再度オンにしてください。

ロック解除とログインの理解

ロック解除とログインが同じではない理由を理解するためには、
Bitwardenが暗号化されていないデータをサーバーに保存しないことを覚えておくことが重要です。
あなたの保管庫がロック解除済みでもログインしていない場合、保管庫のデータはサーバー上に暗号化された形式でしか存在しません。

ログイン

ログインしてBitwardenにアクセスすると、暗号化された保管庫のデータが取得され、
そのデータはあなたのデバイス上でローカルに復号化されます。実際には、それは2つのことを意味します:

1. ログインするには常に、デバイスでログインするかマスターパスワードを使用して、
   保管庫のデータを復号化するために必要なアカウント暗号化キーにアクセスする必要があります。

   この段階では、有効化された二段階ログイン方法も必要となります。

2. ログインするには常にインターネットに接続する必要があります（または、自己ホスト型の場合はサーバーに接続する必要があります）。
   これにより、暗号化された保管庫がディスクにダウンロードされ、その後、デバイスのメモリで復号化されます。

ロック解除

ロック解除は、すでにログインしているときにのみ行うことができます。これは、上記のセクションによれば、
あなたのデバイスにはディスク上に**暗号化された**保管庫データが保存されていることを意味します。実際には、これは2つのことを意味します:

1. あなたは特にマスターパスワードを必要としません。あなたのマスターパスワードは保管庫をロック解除するために使用できますが、
   PINコードや生体認証のような他の方法も使用できます。

> **Note**
>
> PINまたは生体認証を設定すると、PINまたは生体認証要素から派生した新しい暗号化キーが使用されて、アカウント暗号化キーを暗号化し、ログインしているためにアクセスでき、ディスク上に[a]保存されます。
>
> **ロック解除**すると、保管庫はメモリ内のアカウント暗号化キーをPINまたは生体認証キーで復号化します。復号化されたアカウント暗号化キーは、メモリ内のすべての保管庫データを復号化するために使用されます。
>
> **ロック** すると、復号化された保管庫のデータ全体、復号化されたアカウントの暗号化キーを含む、が削除されます。
>
> [a] - **再起動時にマスターパスワードでロック**オプションを使用すると、このキーはディスクではなくメモリにのみ保存されます。

2. インターネットに接続する必要はありません（または、自己ホスト型の場合、サーバーに接続する必要はありません）。