シークレットマネージャー › 始めましょう

# シークレットマネージャーにログインします

# シークレットマネージャーにログインします

エンドツーエンドのゼロ知識暗号化されたBitwardenアカウントを使用してパスワードマネージャーにログインすると、
シークレットマネージャーにログインするのと同じになります。

> **Tip**
> この記事は、シークレットマネージャーのウェブ保管庫にログインすることに関連しています。
> 主にアプリケーションやインフラストラクチャにシークレットを注入するスクリプトを作成するために使用されるシークレットマネージャーCLIは、アクセストークンでログインする必要があります。

## マスターパスワード

あなたのマスターパスワードは、あなたのBitwardenアカウントにアクセスするための主要な方法です。あなたのマスターパスワードが重要です：

- **記憶に残る**: Bitwarden の従業員とシステムには、マスター パスワードに関する知識も、取得方法も、リセット方法もありません。
  **あなたのマスターパスワードを忘れないでください！**
- **強力**: 長く、より複雑で、あまり一般的ではないマスター パスワードが、アカウントを保護する最良の方法です。Bitwardenは、
  検討中のいくつかの記憶に残るパスワードの強度をテストするための無料のパスワード強度テストツールを提供しています。

> **Tip**
> マスターパスワードを忘れることを心配していますか？これがやるべきことです:
>
> - **ヒントを設定する**。必要であれば、ログイン画面でマスターパスワードのヒントをリクエストするメールアドレスを設定できます。
>   あなただけが理解できるヒントを使用するように確認してください。
> - **指定する** 信頼できる緊急連絡先。プレミアムアクセスを持つユーザーは、
>   緊急時に友人や家族にアカウントアクセスを許可することができます。

あなたのマスターパスワードを変更する方法を学びましょう、またはマスターパスワードを忘れた場合に何をすべきかを学びましょう。

## 2段階認証

あなたのBitwardenアカウントを保護するために二段階ログイン（二要素認証または2FAとも呼ばれます）を使用すると、
マスターパスワードが悪意のある行為者に発見されたとしても、ログイン時に二次デバイスからの認証を必要とすることで、
あなたのデータへのアクセスを防ぎます。

二段階ログインの方法はさまざまで、専用の認証アプリからハードウェアのセキュリティキーまであります。あなたが選んだものに関係なく、
Bitwardenは強くあなたの保管庫を二段階ログインを使用して保護することをお勧めします。

### 無料の方法

Bitwardenは、以下を含むいくつかの二段階ログイン方法を無料で提供しています：

| 方法 | 設定手順 |
| --- | --- |
| 認証アプリを通じて（例えば、AuthyまたはGoogle 認証システム） | クリックしてください ここ。 |

| 方法 | 設定手順 |
| --- | --- |
| メールアドレス経由で | クリックしてください ここ。 |
| FIDO WebAuthn認証器を介して | クリックしてください ここ。 |

## プレミアムな方法

プレミアムユーザー（有料組織のメンバーを含む）向けに、Bitwardenはいくつかの高度な二段階ログイン方法を提供しています：

| 方法 | 設定手順 |
| --- | --- |
| Duoセキュリティを使用して、Duo Push、SMS、電話、およびセキュリティキーを通じて | クリック ここ。 |
| YubiKey経由（任意の4/5シリーズデバイスまたはYubiKey NEO/NFC） | クリック ここ。 |

## デバイスでログイン

あなたは、マスターパスワードの代わりにセカンダリデバイスを使用してBitwardenウェブアプリにログインできることを知っていましたか？
デバイスでログインすることは、認証へのパスワードレスのアプローチであり、
現在ログインしている特定のデバイスに認証リクエストをSendすることで、マスターパスワードを入力する必要をなくします。もっと学ぶ

## シングルサインオン(SSO)

あなたの組織がSSOでログインを使用している場合、あなたはあなたの連携SSO資格情報を使用してBitwardenウェブアプリにアクセスできます。