

PASSWORD MANAGER > VAULT BASICS

Bitwarden 認証器 (TOTP)

ヘルプセンターで表示:

<https://bitwarden.com/help/integrated-authenticator/>

Bitwarden認証器 (TOTP)

Bitwarden認証機能は、Authyのような専用の認証アプリに代わるソリューションで、2段階ログインを使用するウェブサイトやアプリの本人確認に使用できます。Bitwarden認証機能は、SHA-1を使用して6桁の時間ベースのワンタイムパスワード (TOTP) を生成し、30秒ごとにローテーションする。

Note

認証キー (TOTP) ストレージは、すべてのアカウントで利用可能です。TOTPコード生成には、プレミアムまたは有料組織 (ファミリー、チーム、企業) のメンバーシップが必要です。

TOTPを使った2段階ログインが初めての場合は、[2段階ログインのフィールドガイド](#)を参照してください。

TOTPコードの生成

TOTPまたは認証機能付き二要素認証 (2FA) をサポートする各ウェブサイトは、それぞれ異なるコンフィギュレーションを扱います。アクセスする個々のウェブサイトやサービス (例えばgoogle.comやgithub.com) からセットアップを開始する。


Bitwarden では、2つの方法でTOTPを生成できます：

- Bitwardenのモバイルアプリまたはブラウザの拡張機能から、以下の方法で行います。 [QRコードをスキャンする](#)
- どのBitwardenアプリからでも [手動で秘密を入力する](#)

QRコードをスキャンする

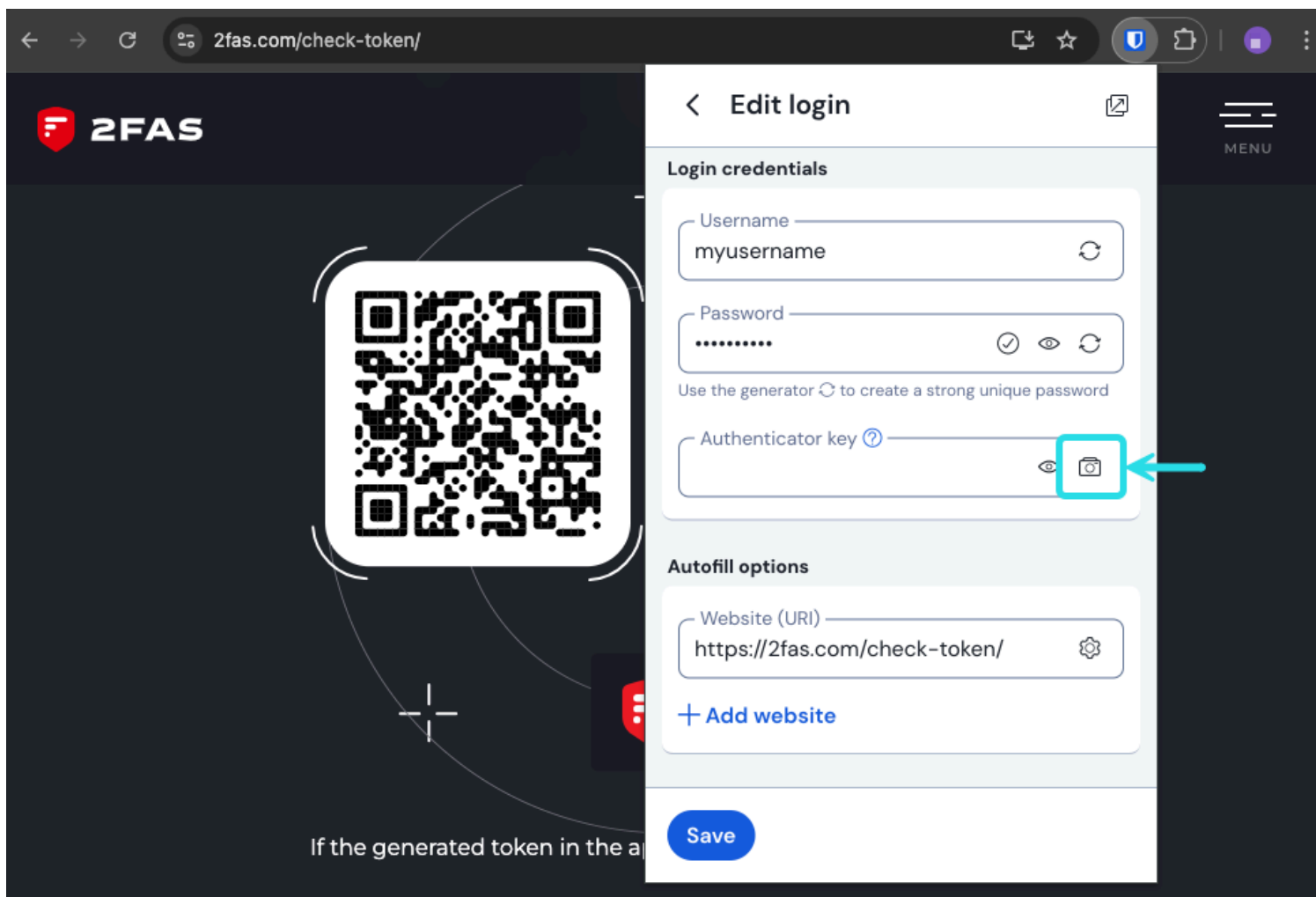
以下のステップを完了し、選択したアプリからBitwarden認証機能を設定します：

⇒iOSまたはAndroidアプリ

1. TOTP を生成する保管庫項目を [編集](#) します。
2.  **Set up TOTP** ボタンをタップします。
3. QRコードを読み取り、「**保存**」をタップしてTOTPの生成を開始します。

⇒ブラウザ拡張機能

1. TOTP を生成する保管庫項目を [編集](#) します。
2.  **TOTP** ボタンを選択すると、現在のウェブページから認証QRコードをスキャンします。完全なQRコードが画面に表示されていること。



ブラウザTOTPスキャン

3. コードが入力されたら「保存」をタップし、TOTPの生成を開始します。

一度セットアップすると、Bitwarden認証機能は30秒ごとに6桁のTOTPを継続的に生成し、接続されたウェブサイトやアプリへの2段階ログインのセカンダリー・ステップとして使用できる。アイテム編集画面の🔑アイコンを使って、いつでもTOTPシードを更新できます。

手動で秘密を入力する

iOSまたはAndroidアプリからシークレットキーを手動で入力するには、以下の手順に従います：

1. TOTPを生成する保管庫項目を編集します。
2. 📄 Set up TOTP ボタンをタップします。
3. 画面下部の「Enter Code Manually」リンクをタップします。
4. 秘密鍵をAuthenticator Key フィールドに貼り付け、Add TOTP をタップします。

一度セットアップすると、Bitwarden認証機能は30秒ごとに6桁のTOTPを継続的に生成し、接続されたウェブサイトやアプリへの2段階ログインのセカンダリー・ステップとして使用できる。項目編集画面の🔑アイコンを使って、

いつでも TOTP シードを編集できます。

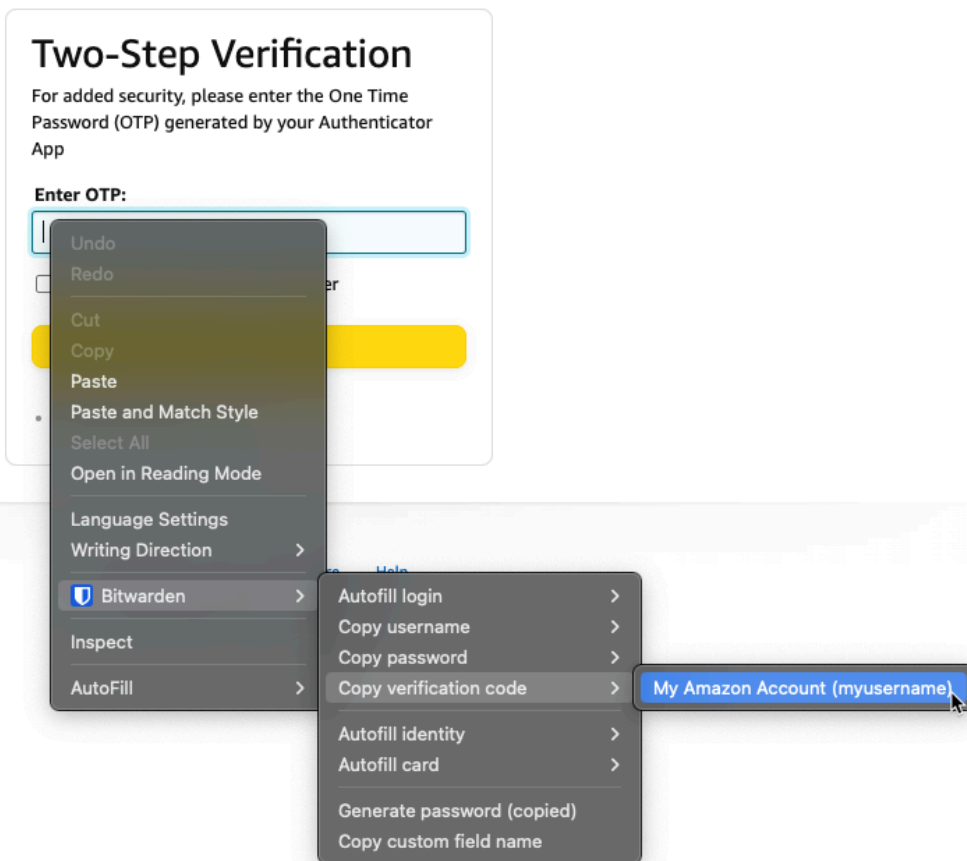
生成されたコードを使用する

💡 Tip

TOTPは時間ベースのコード生成に依存している。あなたのデバイスがサーバーと比較して誤った時刻を持っている場合、動作しないコードが生成されます。TOTPコードに問題がある場合は、デバイスの時刻とタイムゾーンを「自動」に設定してください。

Bitwarden ブラウザ拡張機能は、**Auto-fill on Page Load** オプションがアクティブでない限り、TOTP コードを自動入力します。その場合、ブラウザの拡張機能はTOTPコードをクリップボードにコピーし、フォームに簡単に貼り付けることができる。モバイル・アプリケーションは、自動入力後、TOTPコードをデバイスのクリップボードにのみ自動的にコピーします。

ブラウザの拡張機能では、コンテキストメニューからTOTPコードをコピーすることもできます：



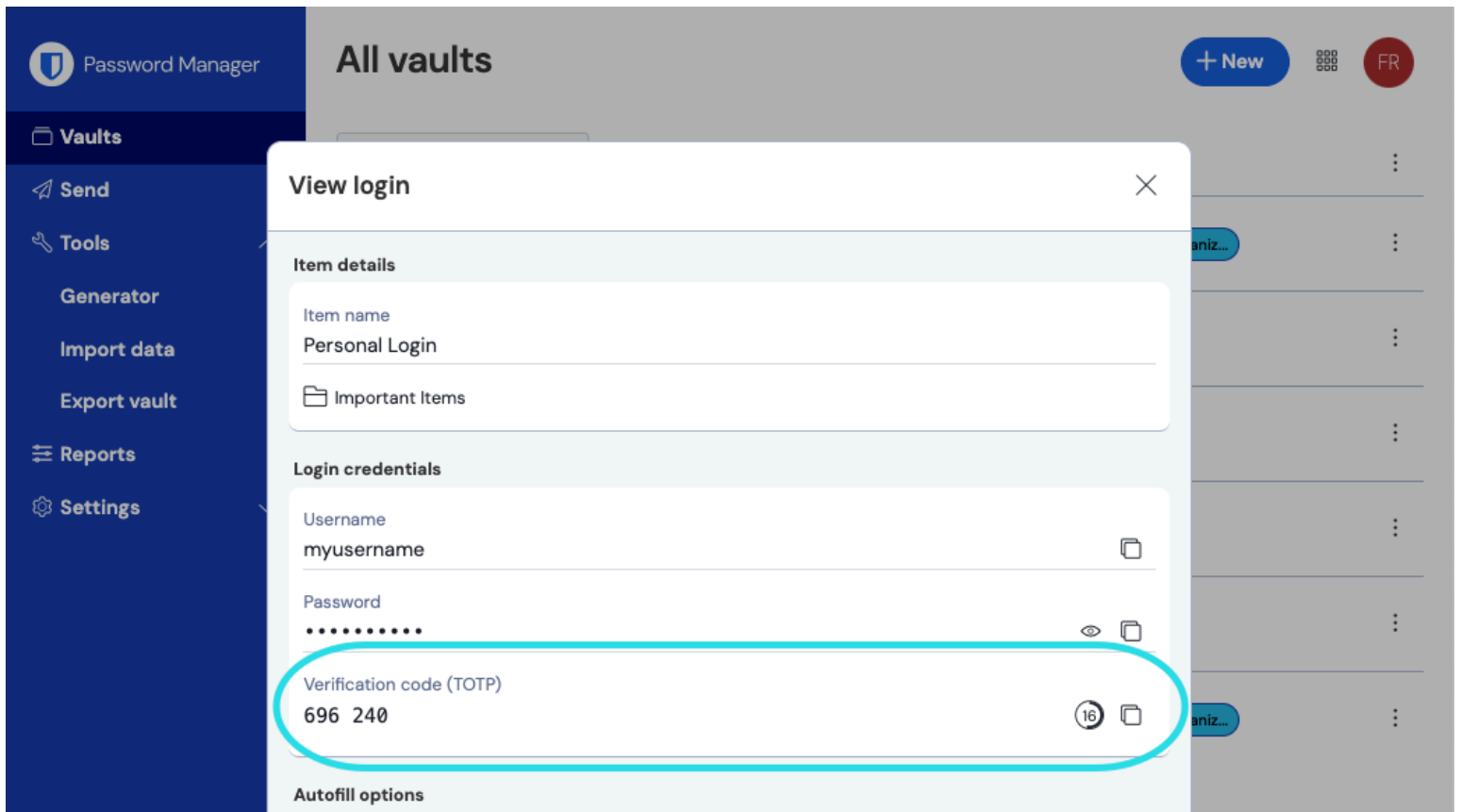
ブラウザ拡張機能のコンテキストメニュー

💡 Tip

TOTPの自動コピーは、**設定→オプション→TOTPの自動コピー**でオフにすることができますが、デフォルトではオンになっています。さらに、近くにある**クリップボードのクリア** オプションを使用して、コピーした値をクリアする間隔を設定します。

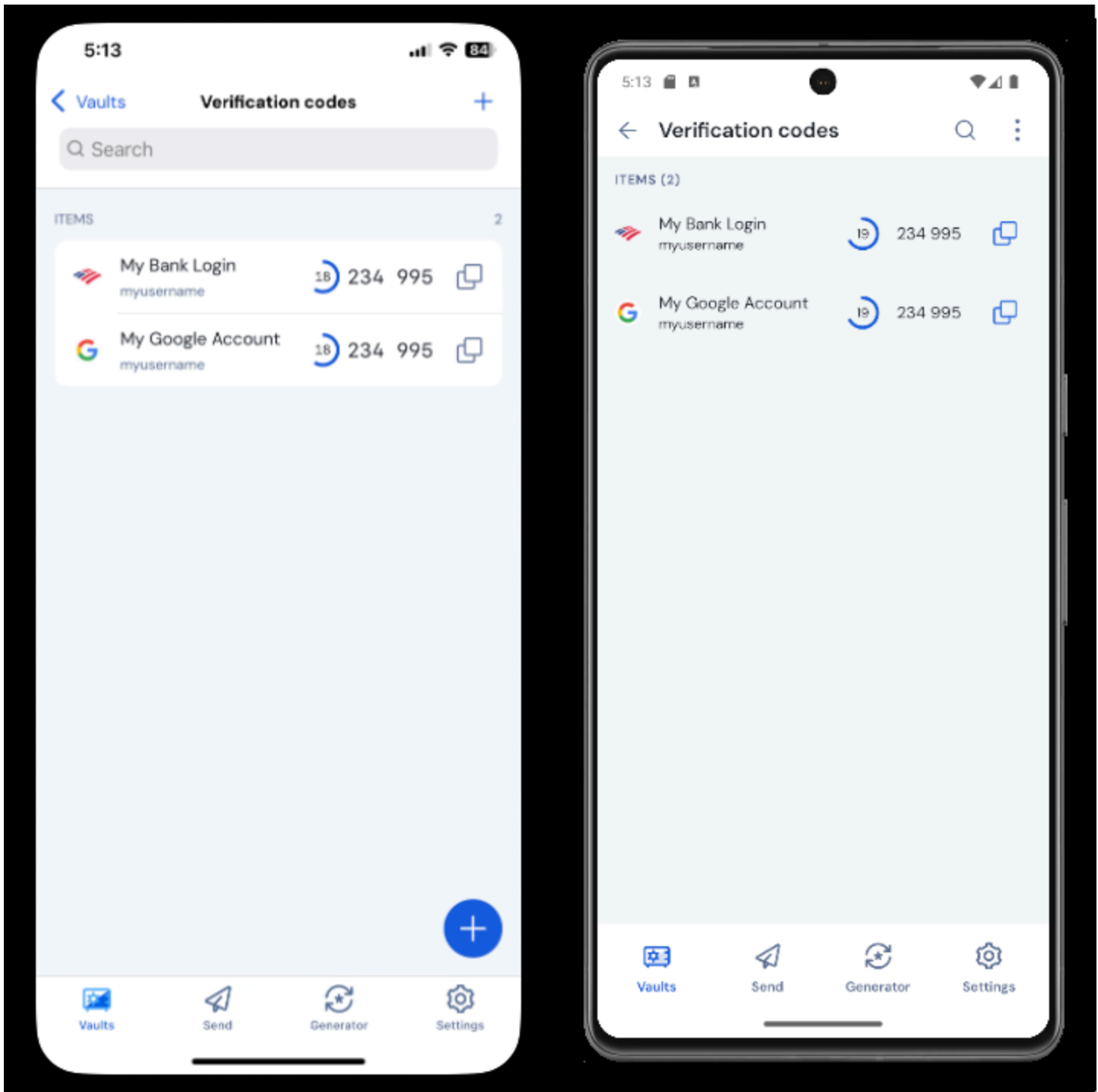
TOTPコードを見る

すべてのBitwardenアプリは、ユーザー名やパスワードと同じようにコピー＆ペーストすることができます：



TOTPコードをコピーする

また、モバイルアプリには専用の検証コード画面があり、有効なTOTPを一覧表示して素早くコピーできる：



モバイル認証コード画面

トラブルシューティング

TOTPコードはデバイスのシステムクロックに基づいて生成されます。生成されたコードが機能しない場合、最も考えられる原因は、デバイスの時計がBitwardenサーバーとずれていることです。デバイスの時計を再同期するには：

⇒ウィンドウズ

スタート → 「設定」 → 「時間と言語」 → 「日付と時刻」の順に選択し、「自動的に時刻を設定する」オプションをオフにし、オンに戻します。

これがうまくいかない場合は、以下のPowerShellコマンドを使ってタイムゾーンを設定し、タイムゾーン名をこのリストから正しいものに置き換えてから、コンピュータを再起動してください：

Plain Text

```
Set-TimeZone -Id "Central Standard Time"
```

Plain Text

```
Restart-Computer
```

⇒マックオス

システム設定 → 「一般」 → 「日付と時刻」を開き、「自動的に時刻と日付を設定する」と「現在地を使用して自動的にタイムゾーンを設定する」のオプションをオフにしてからオンに戻します。

⇒アンドロイド

設定] → [システム] → [日付と時刻]を開き、[自動的に時刻を設定] オプションをオフにし、オンに戻します。

⇒iOS

設定] → [一般] → [日付と時刻]を開き、[自動的に設定] オプションをオフにしてオンに戻します。

より多くのパラメータをサポート

デフォルトでは、BitwardenはSHA-1を使用して6桁のTOTPを生成し、30秒ごとにローテーションしますが、一部のウェブサイトやサービスは異なるパラメータを要求します。Bitwardenでは、保管庫アイテムの`otpauth://totp/` URIを手動で編集することで、パラメータをカスタマイズできます。

パラメータ	説明	価値観	サンプル クエリー
アルゴリズム	TOTP の生成に使用される暗号アルゴリズム。	-シャ1 -シャ256 -シャ512 -otpauth	アルゴリズム=sha256
数字	生成されたTOTPの桁数。	1-10	桁=8
期間	TOTPを回転させる秒数。	0 以上でなければならない	period=60

例えば、こうだ：

Bash

```
otpauth://totp/Test:me?secret=JBSWY3DPEHPK3PXP&algorithm=sha256&digits=8&period=60
```

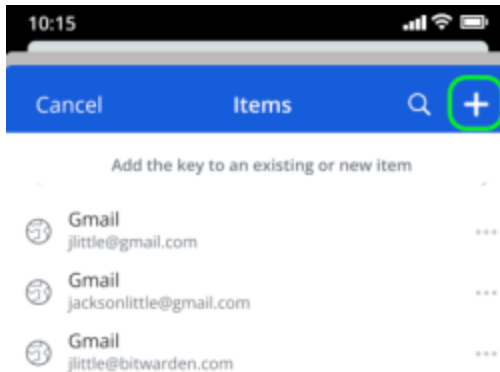
otpauth://URIの使い方については[こちら](#)をご覧ください。

iOSのBitwarden認証機能

iOS16以上のiOSユーザーは、カメラアプリから直接コードをスキャンする際に、認証コードを保存するデフォルトのアプリケーションとしてBitwardenを設定することもできます。これを設定する：

1. デバイスのiOS設定 アプリを開く。
2. 「パスワード」をタップします。
3. 「パスワードオプション」をタップします。
4. **Set up verification codes using:** リストから、**Bitwarden** を選択します。

有効にすると、カメラアプリのQRコードに「**Bitwardenで開く**」ボタンが追加されます。タップすると、認証キーを新しい保管庫アイテムに追加するか、既存の保管庫アイテムに追加するかを選択できます。アイテムを作成または編集したら、閉じる前に必ず**保存**してください。



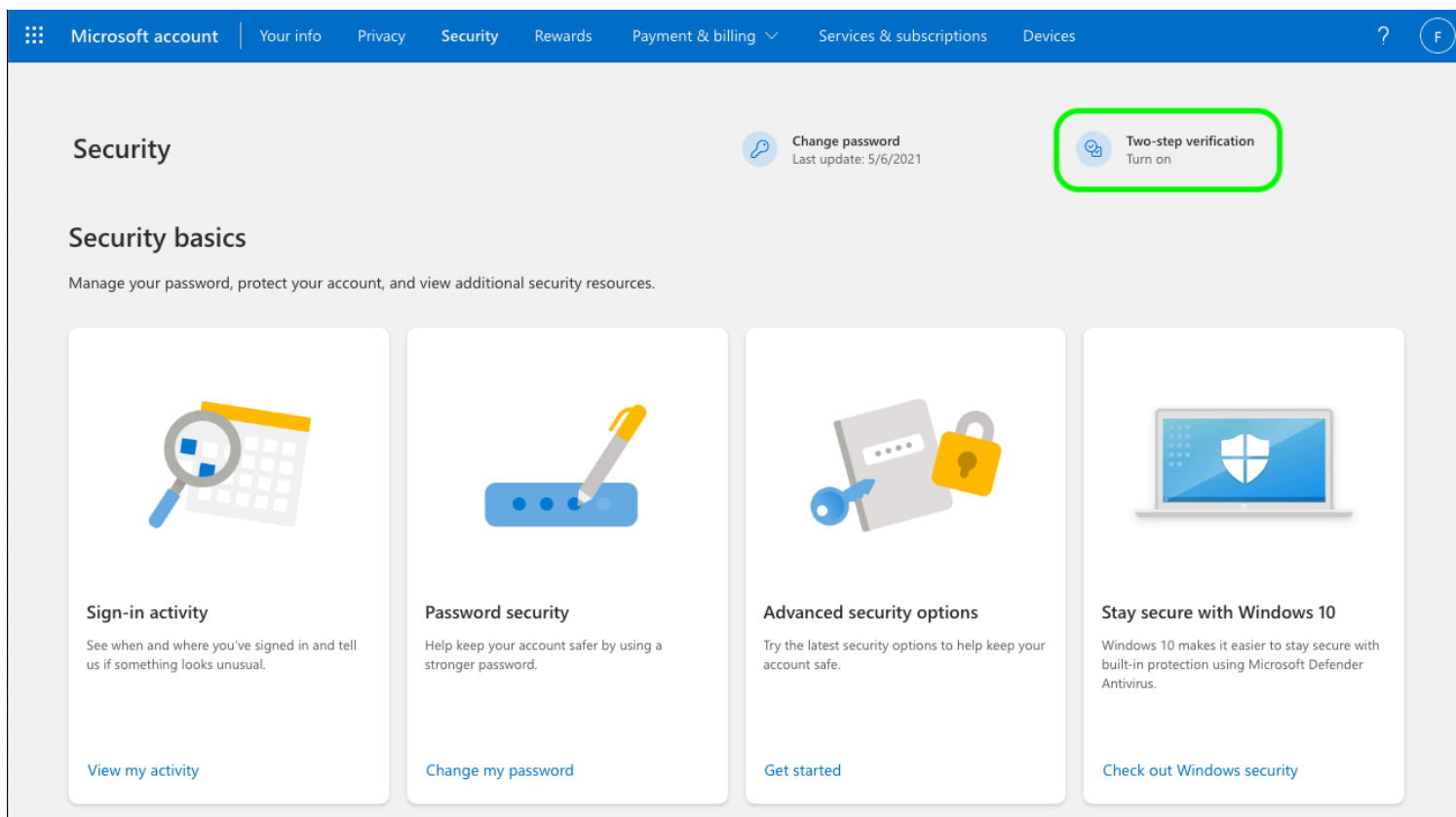
新規または既存の検証コードを追加する

iOSで自動入力ログインすると、TOTPコードが自動的にクリップボードにコピーされます。
 認証コードフィールドにTOTPコードを入力してログインを完了します。

AzureとOffice 365

既定では、Microsoft Azure および Office 365 アカウントでは、TOTP に Microsoft Authenticator が使用されます。Bitwarden Authenticator を使用して Microsoft Azure または Office 365 アカウントの TOTP を生成する場合は、次の手順を実行する必要があります：

1. マイクロソフトのアカウント設定ページに移動します。個人アカウントかビジネスアカウントかによって、account.microsoft.com または myaccount.microsoft.com となります。
2. 個人アカウントかビジネスアカウントかに応じて、**セキュリティ・ダッシュボード**を開くか、**セキュリティ情報**を選択します。**セキュリティ・ダッシュボード**を経由する場合は、その画面から**2段階認証も**選択する必要があります。



2FAをオンにする

3. 二段階認証を **オンにする** ボタンまたは **[サインイン方法を追加する]** ボタンのいずれかを選択し、ドロップダウンから Authenticator アプリを選択します。
4. セットアップ中に、検証方法のドロップダウンメニューが表示されます。**Authenticator App** または **An app** を選択します。
5. 青い「別の認証アプリ」のハイパーリンクが表示されるまで進む。ハイパーリンクが表示されたら選択してください。
6. QRコードが表示されるまで続けてください。その時点で、[こちらの通常の指示](#)に従ってください。

スチームガードTOTP

Bitwarden Authenticator (TOTP) は、[steam://](#)プレフィックスと秘密キーを使用して、Steam の TOTP 生成の代替手段として使用できます：

EDIT ITEM

Name	Steam	Folder	No Folder
Username	my_steam_username	Password
Authenticator Key (TOTP)	steam://secret		

[New URI](#)

スチームTOTP世代

生成されるsteam://TOTPは、デフォルトで英数字5桁であり、従来の数字6桁のTOTPとは異なる。

⚠ Warning

この機能を使用するには、サードパーティ製のツールを使ってSteamアカウントの秘密を手動で抽出する必要があります。
SteamTimeldlerや Steam Desktop Authenticatorなどのツールがありますが、
このような抽出ツールはBitwardenやSteamによって公式にサポートされていません。これらのツールは自己責任で使用する事。