bitwarden | ヘルプセンターの記事

新しいデバイスのログイン保護（2025年2月/3月）

ヘルプセンターで表示:
https://bitwarden.com/help/new-device-verification/

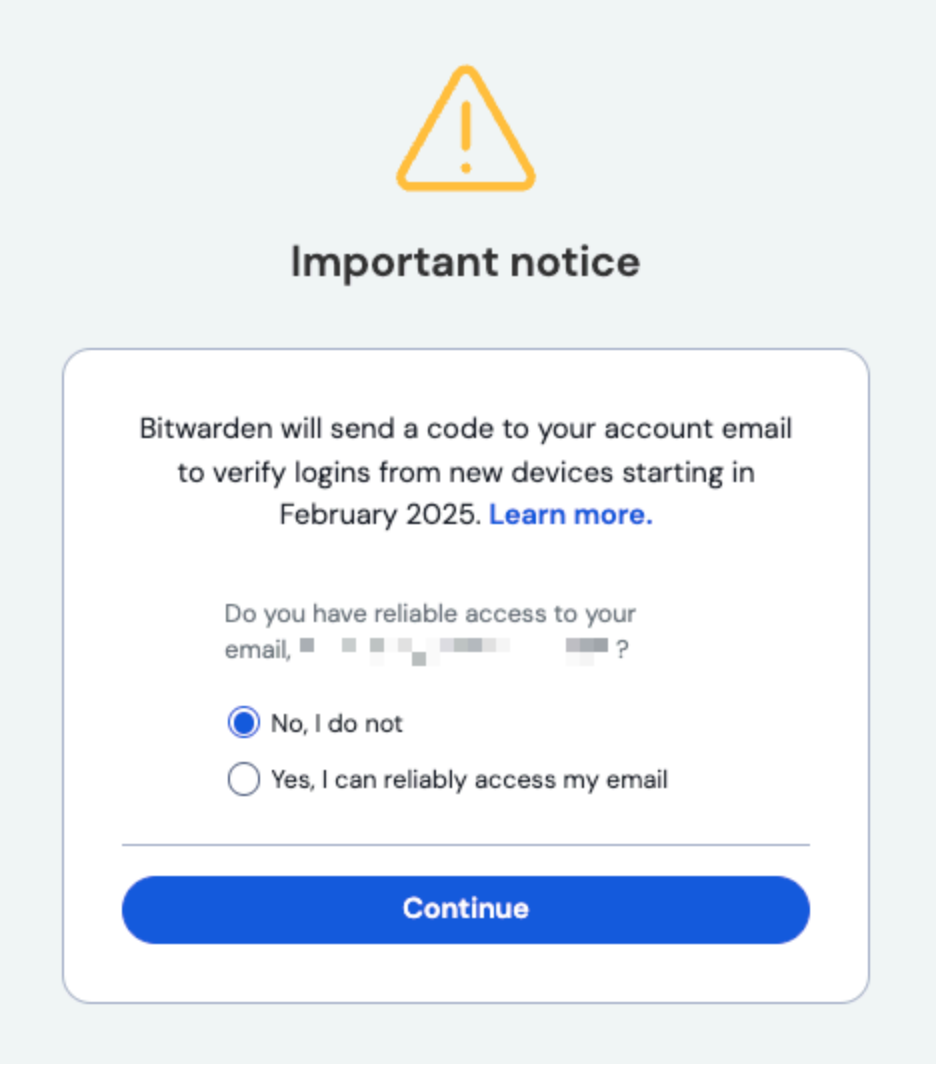
新しいデバイスのログイン保護（2025年2月/3月）

お客様のアカウントを安全かつセキュアに保つため、2025年2月から3月にかけて、Bitwardenは、
二段階**ログインを使用しないユーザーに対して** 追加の認証を要求します。 二段階ログイン.Bitwardenのマスターパスワードを入力した後、
以前にログインしたことの**ないデバイスからログインする場合**、ログインプロセスを完了するために、
アカウントの電子メールに送信される1回限りの認証コードを入力するよう求められます。たとえば、
以前に使用したことのあるモバイルアプリやブラウザ拡張機能にログインする場合は、このプロンプトは表示されません。

ほとんどのユーザーは、新しいデバイスに頻繁にログインしない限り、このプロンプトを経験することはない。この認証は、
新しいデバイスまたはブラウザのクッキーをクリアした後にのみ必要です。

定期的にEメールにアクセスしていれば、認証コードの取得は簡単なはずだ。認証に Bitwarden
アカウントの電子メールを使用したくない場合は、Authenticator アプリ、ハードウェア キー、または別の電子メールを使用した2
段階ログインを設定できます。

この変更の影響を受けるユーザーには、次のような製品内コミュニケーションが表示され、変更を通知する電子メールが届いているはずです：



新デバイス検証の発表

よくあるご質問

いつになるのだろうか？

この変更は2025年2月から3月にかけて実施される。リリースの日程が決まり次第、このページは更新される。

なぜビットワルデンはこれを導入するのか？

Bitwardenは、2段階ログインを有効にしていないユーザーのセキュリティを強化するために、この変更を実施しています。
誰かがあなたのパスワードにアクセスしたとしても、二次認証（あなたのEメールに送られるコード）がなければ、
あなたのアカウントにログインすることはできません。この追加レイヤーは、
不正アクセスを得るために弱いパスワードや露出したパスワードを狙うハッカーからデータを保護するのに役立つ。

この確認はいつ行われますか？

この認証を求められるのは、新しいデバイスからログインするときだけです。以前に使用したことのあるデバイスにログインする場合は、
プロンプトは表示されません。

新機種とは？

新しいデバイスとは、Bitwardenアカウントへのログインに使用したことのないデバイスのことです。これには、
これまで一度もログインしたことのない新しい携帯電話、タブレット、コンピューター、ブラウザーの拡張機能などが含まれる。
新しいデバイスからログインすると、Eメールに送信されるワンタイムコードで本人確認を求められます。

新しいデバイスが起動するその他のシナリオは以下の通り：

- モバイル、デスクトップアプリ、またはブラウザの拡張機能をアンインストールして再インストールすると、
  新しいデバイスが起動します。
- ブラウザのクッキーをクリアすると、ウェブアプリの新しいデバイスが起動しますが、ブラウザの拡張機能は起動しません。

私の電子メール認証情報はBitwardenに保存されています。Bitwardenからロックアウトされますか？

電子メール認証コードは、2段階ログインを有効にしていないユーザーの新しいデバイスでのみ必要となります。
以前にログインしたデバイスではこのプロンプトは表示されず、
アカウントの電子メールとマスターパスワードを使って通常通りログインします。

新しいデバイスにログインする場合、BitwardenアカウントのEメールに1回限りの認証コードが送信されます。もし、あなたのEメール、
つまり携帯電話でログインしたままのEメールにアクセスできるのであれば、
ログインするためのワンタイムベリフィケーションコードを入手することができる。新しいデバイスにログインすると、
認証コードの入力を求められることはありません。

Bitwardenに保存された認証情報を使用して定期的に電子メールにログインする場合や、認証のために電子メールに依存したくない場合は、
Bitwardenアカウントの電子メールとは独立した2段階ログインを設定する必要があります。これには、認証アプリ、セキュリティ・キー、
または別の電子メールによる電子メール・ベースの2段階ログインが含まれる。どの2FAメソッドもアクティブにしておくと、
電子メールベースの新しいデバイス認証からユーザーをオプトアウトする。2FAを有効にしているユーザーは、
Bitwardenの回復コードも安全な場所に保存してください。

このアカウント・メール・ベースの新規デバイス認証から除外されるのは誰ですか？

以下のカテゴリーのログインは除外されます：

- 二段階ログインを設定しているユーザーは除外されます。
- SSO、パスキー、またはAPIキーでログインするユーザーは除外されます。
- セルフホスト・ユーザーは除く。

- 過去にログインしたことのあるデバイスからログインしたユーザーは除外されます。
- **設定→マイアカウント**画面からオプトアウトしたユーザーは除外されます（**推奨されません**）。

私の組織はSSOを使用していますが、ユーザーは新しいデバイスの認証を完了する必要がありますか？

いいえ。SSOでログインするユーザーは免除され、新しいデバイスでのログインの確認は求められません。しかし、
2段階ログインを有効にしていないユーザーが、SSOを通さずにユーザー名とパスワードでログインすると、
新しいデバイスを確認するよう求められる。

ビットワルデンに自分の本当のEメールを教えたくありません。

匿名を希望するユーザーには、いくつかのオプションが用意されている：

- 認証アプリ、セキュリティキー、別のEメールを使ったEメールベースの2段階ログインなど、
  Eメールを必要としない2段階ログインオプションを使用する。
- メールエイリアス転送サービスを利用する。
- ビットワルデンのセルフホスト。

Bitwardenは、ログインに失敗した場合などの重要なセキュリティアラートを送信するため、
ユーザーにはアクティブなEメールを持つことを推奨しています。

2FAアクセス権を失ったため、新しいデバイスで2FA回復コードを使用する場合、この新しいデバイス認証の対象となりますか？

Bitwardenは、パスワードとリカバリーコードを送信すると、ウェブアプリにログインし、2FA設定に移動するように、
リカバリーコードフローを更新する予定です。ロックアウトされる心配がある場合は、
シークレットブラウザやインターネット接続が不安定なデバイスでこのフローを実行することは**避け**、
ログインセッションで必要なセットアップ手順を完了できるようにしてください。

オプトアウトしたい！オプションはありますか？

これは、2段階ログインを有効にしていないユーザーのための追加セキュリティです。二段階ログインを有効にしていないユーザーは、
パスワードが強固で一意であったとしても、複数の方法で漏洩する可能性があるため、攻撃者による不正アクセスに対してより脆弱である。
例えば、一般的な方法には以下のようなものがある：

- **フィッシング攻撃**：サイバー犯罪者は、人を騙す電子メールやウェブサイトを使い、パスワードの漏えいをだます。
- **ソーシャル・エンジニアリング**：攻撃者は、電話、メール、その他の手段で、あなたを操ったり、
  騙してパスワードを明かそうとするかもしれません。
- **ブルートフォース攻撃によるパスワードクラッキング**：攻撃者は自動化されたツールを使って、パスワードの推測を繰り返し試みる。
- **キーロギングやマルウェア**：お使いのデバイスがマルウェアやキーロガーに感染している場合、攻撃者はあなたの知らないうちに、
  パスワードを含むすべてのキー入力を記録する可能性があります。

新しいデバイス認証では、上記のいずれかの方法でパスワードが漏えいした場合でも、
攻撃者は電子メールに記載されたワンタイムコードである2つ目の認証を取得する必要があります。これにより、
不正アクセスの可能性を大幅に減らすことができる。

新しいデバイス認証は、従来の2段階ログインよりも侵入しにくいように設計されている。これは、
これまで使用したことのないデバイスやクライアントからログインする場合にのみ適用されるため、

ほとんどのユーザーは日常的に使用しているデバイスでログインしているため、この余分なステップを経験することはない。
認証プロセスでは、多くの人が携帯電話やコンピューターで開いているEメールを使用するため、コードの取得は素早く簡単だ。

このような場合、以下のような問題が発生する可能性があります：

- 二段階ログインを有効にしない。
- EメールのパスワードをBitwardenに保存する。
- Bitwardenのアンインストールと再インストールを繰り返す。
- どこでもEメールを**ログアウト**する。

これらのことをすべて実行し、上記の条件に一致するユーザーだけが、このセキュリティ・アップデートで摩擦を経験することになります。
ユーザーがアカウントからロックアウトされた場合は、Bitwardenのカスタマーサクセスに連絡することができます。

ユーザーが新しいデバイス認証を望まない場合は、アカウントを保護するために、別の2段階ログイン方法（認証アプリ、ハードウェアキー、または別のメールのいずれか）をオンにすることを強くお勧めします。

ユーザーが新しいデバイス認証を望まず、代替の2段階ログイン方法を設定せず、**アカウントにセキュリティをかけたくない場合は**、**「設定」**→**「マイアカウント」**画面に移動し、「危険地帯」セクションまでスクロールすることで、オプトアウトするオプションがあります。これは、あなたのアカウントが様々な攻撃に対して無防備になるため、**強くお勧めできない**ことを強調しておかなければならない。