bitwarden | ヘルプセンターの記事

セキュリティ

セキュリティに関するFAQ

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

セキュリティに関するFAQ

この記事には、セキュリティに関するよくある質問（FAQ）が含まれています。

Q: なぜ私は自分のパスワードをBitwardenに信頼するべきなのですか？

A: 私たちを信頼できるいくつかの理由があります：

1. Bitwardenは**オープンソース**ソフトウェアです。私たちのすべてのソースコードはGitHubにホストされており、誰でも無料でレビューすることができます。
   数千のソフトウェア開発者がBitwardenのソースコードプロジェクトをフォローしています（そしてあなたもそうすべきです！）。

2. Bitwarden は、評判の高いサードパーティのセキュリティ会社および独立したセキュリティ研究者によって監査されている**ます**。

3. Bitwardenは**あなたのパスワードを保存しません**。Bitwardenはあなたのパスワードの暗号化されたバージョンを保存しますそれはあなただけがロック解除できます。
   あなたの機密情報は、私たちのクラウドサーバーに送信される前に、あなたの個人的なデバイス上でローカルに暗号化されます。

4. **Bitwardenは評判があります。**Bitwardenは何百万人もの個人とビジネスに使用されています。もし私たちが何か疑問のあることやリスクのあることをしたら、
   私たちはビジネスから手を引くことになるでしょう！

まだ私たちを信用していませんか？あなたはしなくてもいいです。オープンソースは美しいです。あなたは簡単に自分自身でBitwardenスタック全体をホストすることができます。
あなたは自分のデータを制御します。もっと詳しくはこちらをご覧ください。

Q: Bitwardenがハッキングされた場合、何が起こりますか？

A: Bitwardenは、そのウェブサイト、アプリケーション、クラウドサーバーが安全であることを確保するために、極端な措置を講じています。Bitwardenは、直接行うのではなく、
サーバーインフラストラクチャとセキュリティを管理するためにMicrosoft Azure管理サービスを使用しています。

何らかの理由でBitwardenがハッキングされ、あなたのデータが流出済みであっても、
あなたの情報は保管庫のデータとマスターパスワードに対して行われた強力な暗号化と一方向のソルト化ハッシュの措置により、依然として保護されています。

Q: Bitwardenは私のパスワードを見ることができますか？

A: いいえ。

データは**ローカル**デバイスから送信される前に完全に暗号化および/またはハッシュされるため、Bitwarden チームの誰も、実際のデータを参照したり、読み取ったり、リバース
エンジニアリングしたりすることはできません。Bitwardenのサーバーは暗号化され、ハッシュ化されたデータのみを保存します。
あなたのデータがどのように暗号化されているかについての詳細は、暗号化をご覧ください。

Q: 私のBitwardenマスターパスワードはローカルに保存されていますか？

A: いいえ。

私たちはマスターパスワードをローカルにもメモリにも保存していません。あなたの暗号化キー（マスターパスワードから派生）は、
アプリがロック解除済みである間だけメモリに保持され、これは保管庫内のデータを復号化するために必要です。保管庫がロックされると、
このデータはメモリからパージされます。

また、ロック画面での非活動状態が10秒続いた後に、アプリケーションのレンダラープロセスを再読み込みします。これにより、
まだガベージコレクションされていない管理されたメモリアドレスがすべてパージされることを確認します。私たちは、
アプリケーションが機能するためにメモリに保持される可能性のあるデータが、必要な期間だけメモリに保持され、
アプリケーションがロックされるたびにメモリがクリーンアップされるように最善を尽くしています。アプリケーションがロック状態にある間、
アプリケーションの暗号化されたデータは完全に安全であると考えています。

A: Bitwardenに新しいデバイスがログインしているのを認識しない場合、何をすればいいですか？

A:新しいデバイスの IP アドレスが既知の IP アドレス (ホーム ネットワーク、職場ネットワーク、モバイル ネットワークなど) と一致しない場合は、マスター パスワードを変更し、
アカウントで 2 段階ログインが有効になっていることを確認してください。すべてのデバイスでログアウトを強制するためには、
ウェブ保管庫の**アカウント設定**ページからセッションの認証を解除するべきです。あなたの保管庫のアイテムが危険にさらされていると思われる場合、
パスワードを変更すべきです。

Q: Bitwardenは何と互換性がありますか？あなたはどのような資格を持っていますか？

A: Bitwardenは以下のポリシーに準拠しています:

- **一般データ保護規則**もっと読む ここ。
- **CCPA.**もっと読む ここ。
- **HIPAA.**もっと読む ここ。
- **SOC 2 タイプ 2.**もっと読む ここ。
- **SOC 3.**もっと読む ここ。

詳細については、セキュリティとコンプライアンスのページをご覧ください。

Q: Bitwardenはどのようにしてヨーロッパのコンプライアンス要件を満たしていますか？

A: BitwardenはGDPRに準拠しており、EU標準契約条項（SCC）を含む承認された情報転送メカニズムを使用しています。これは、欧州議会と理事会が欧州委員会の実施決定（EU）2021/914（2021年6月4日）により承認した規則（EU）2016/679に基づいています。現在、https://eur-lex.europa.eu/eli/dec_impl/2021/914/ojで詳細を確認できます。ビジネスおよびエンタープライズのお客様に対して、BitwardenはBitwardenデータ保護契約を実行することができます。

Bitwardenのクラウドサーバーは現在、アメリカ合衆国と欧州連合内のMicrosoft Azure上にホストされています。今日、Bitwardenはこのインフラストラクチャを通じて、ヨーロッパや世界中の政府やエンタープライズの顧客を含む何百万人ものユーザーにサービスを提供しています。

データの居住地に対する完全なコントロールが必要なお客様のために、Bitwardenは代わりにあなた自身のインフラストラクチャーでプライベートにホストすることができます。

Bitwardenに保存されているすべての保管庫データ、クラウド上であろうと自己ホスト型であろうと、エンドツーエンドで暗号化されており、Bitwardenユーザー以外の誰もアクセスできません。このエンドツーエンド、ゼロ知識暗号化アーキテクチャでは、Bitwardenでさえもあなたのデータにアクセスすることはできません。

Bitwardenのセキュリティとコンプライアンス認証の完全なリストについては、https://bitwarden.com/compliance/をご覧ください。

Q: 私のBitwardenアカウントでどのようなサードパーティーサービス、ライブラリ、または識別子が使用されていますか？

A: モバイルアプリでは、Firebase Cloud Messaging（しばしばトラッカーと間違えられます）は、同期に関連するプッシュ通知のためだけに使用され、追跡機能は一切実行しません。Microsoft Visual Studio App Centerは、さまざまなモバイルデバイスでのクラッシュレポートに使用されます。ウェブ保管庫では、StripeとPayPalのスクリプトは支払いページでのみ支払い処理に使用されます。

3rdパーティのコミュニケーションをすべて除外したい方のために、FirebaseとMicrosoft Visual Studio App CenterはF-Droidビルドから完全に削除されています。さらに、自己ホスト型のBitwardenサーバーでプッシュ通知をオフにすると、プッシュリレーサーバーの使用が無効になります。

BitwardenのAndroidアプリケーションには、設定の下でクラッシュレポートを無効にする機能も含まれています。

Bitwardenはユーザーのセキュリティとプライバシーを真剣に考えています。Bitwardenは、あなたの暗号化キーについての知識がゼロで、安全なエンドツーエンドの暗号化を維持します。私たちはオープンソースに注力している会社として、誰でもいつでもGitHubで私たちのライブラリ実装をレビューするように招待します。

Q: 私のBitwarden組織で二段階ログインを要求するにはどうすればいいですか？

A: Enterprise 組織のサブスクリプションに含まれるエンタープライズ ポリシーを使用します。あなたの組織の2FA/MFAを強制するために、Duo MFA統合を有効にすることもできます。詳細については、Duoを介した二段階ログインをご覧ください。

Q: 自己ホスト型のBitwardenインスタンスの証明書オプションは何ですか？

A: 完全なリストと指示については、証明書オプションをご覧ください。

Q: Bitwardenはコードの変更をどのように審査しますか？

A: Bitwarden にとって、システムのセキュリティに対する信頼は最も重要です。すべての提案されたコードの変更は、それがどのコードベースにもマージされる前に、チームの非著者メンバー1人以上によってレビューされます。すべてのコードは、本番環境に移行する前に複数のテスト環境とQA環境を経ています。Bitwardenは、私たちの内部手続きを監査し、検証するためのSOC2レポートを実装しました。レポートで述べられているように、私たちのチームは厳格な背景調査と徹底的な面接プロセスの対象となっています。Bitwardenはオープンソース製品であるため、いつでもコードのピアレビューを歓迎しています。Bitwardenのチームは、ユーザーが快適に感じるために可能な限り全力を尽くし、そのデータを安全に保つことを目指しています。

Q: Bitwardenはどのくらいの期間、セッション情報をキャッシュしますか？

A: 素晴らしい質問ですね！答えは特定の情報とクライアントアプリケーションによります：

- オフラインの保管庫セッションは30日後に期限切れになります。
  - **ただし**、モバイル クライアント アプリケーションは 90 日後に期限切れになります。
- 二段階ログイン **私を覚えて**の選択は30日後に期限切れになります。
- ディレクトリコネクター同期キャッシュは30日後にクリアされます。
- 組織の招待は5日後に期限切れになります。自己ホスト型の顧客は、これを環境変数を使用して設定できます。

Q: Bitwardenアプリのチェックサムをどのように検証しますか？

A: まず、関連するリリースの最新のyamlファイル（例えば、`latest-linux.yml`）と対応するリリースパッケージ（例えば、`Bitwarden-1.33.0-amd64.deb`）を取得します。ダウンロードしたリリースパッケージ（例えば、`sha512sum Bitwarden-1.33.0-amd64.deb`）のSHA512ハッシュを生成し、生成されたHex値をBase64に変換します。計算されたBase64の値をyamlファイルからの`sha512:`の値と比較して検証してください。

Q: Bitwardenにセキュリティ開示またはレポートをどのように作成しますか？

A : Bitwarden は、ユーザーの安全を守るためには世界中のセキュリティ研究者と協力することが重要であると考えています。もし、私たちの製品やサービスでセキュリティ上の問題を見つけたと思われる場合は、HackerOneプログラムを通じてレポートを提出していただくことをお勧めします。

問題を迅速に解決するために、あなたと協力することを歓迎します。当社の開示ポリシーについて詳しくは、こちらをご覧ください。

Q: なぜ私のウェブ保管庫がweb-vault.pages.devに移動しているのですか？

A: `web-vault.pages.dev`は、Cloudflare Pagesで使用されるBitwarden専用のサブドメインです。このURLは、
CloudflareがDNSの問題を経験しているときにユーザーに表示されることがあります。常にフィッシング試みに警戒し、
ユーザー名とマスターパスワードを入力する前にURLを確認するべきですが、`web-vault.pages.dev`はログインするのに安全と考えられます。

A: Bitwardenアカウントをブルートフォース攻撃から保護するにはどうすればよいですか？

A:ブルート フォース攻撃とは、悪意のある攻撃者が、脆弱なパスワードと短いパスワードの組み合わせを繰り返し使用して、アカウントにアクセスしようとすることです。
Bitwardenは、これらの潜在的な攻撃から自分自身を守るためのいくつかの方法を提供しています:

- 長くてユニークなマスターパスワードを持ってください。Bitwardenは、アカウントのセキュリティを強化するために、最低12文字が必要です。
- すべてのBitwardenアカウントに二要素認証を設定し、セキュリティを一層強化します。
- Bitwardenは、未知のデバイスからのログイン試行が9回失敗した後、CAPTCHAの確認を要求します。

特定のクライアントアプリに関する質問

A: Bitwardenはクライアントアプリケーションからどのようなデータを使用しますか？

A: Bitwardenは、あなたにBitwardenサービスを提供するために管理データを使用します。いくつかの**App Privacy**レポートによれば、
ユーザーはアカウント作成時に以下の情報を提供します：

- あなたの名前（任意）。
- あなたのメールアドレス（メール確認、アカウント管理、そしてあなたとBitwardenとのコミュニケーションのために使用されます）。

さらに、**Bitwardenが生成した**デバイス固有のGUID（時々デバイスIDと呼ばれる）があなたのデバイスに割り当てられます。このGUIDは、
新しいデバイスがあなたの保管庫にログインしたときに警告するために使用されます。

Q: エレクトロンアプリのセキュリティについて説明できますか？

A: よく共有される記事では、エレクトロンアプリに欠陥があると示唆されていますが、参照されている攻撃は、ユーザーが侵害されたマシンを持っていることを必要とします。
もちろん、これにより悪意のある攻撃者がそのマシン上のデータを侵害することが可能になります。あなたが使用しているデバイスが侵害されたと考える理由がない限り、
あなたのデータは安全です。

A: Bitwardenはどのようにブラウザの拡張機能を保護しますか？

A: 拡張機能は正しく開発されていれば、安全に使用することができます。ブラウザの拡張機能の動作の性質上、常にバグが発生する可能性があります。私たちは、
拡張機能やアドオンを開発する際には極度の注意と慎重さを持って取り組んでいます。業界で何が起こっているかを常に見聞きし、
セキュリティ監査を実施して全てを多くの目で見守っています。

A: ブラウザの拡張機能は何の権限を求めていますか？

A:インストール時に、ブラウザ拡張機能は、スケジュールされたクリップボード クリア機能 (**[オプション]**メニューからアクセス) を使用するために、
クリップボードへのアクセス許可を求めます。

この**オプションの機能**が有効になっていると、クリップボードのクリアは、設定可能な間隔で作成または入力されたBitwardenのエントリをクリアします。
クリップボードへのアクセスにより、Bitwardenは、最後にコピーしたアイテムをあなたの保管庫から最後にコピーしたアイテムと照らし合わせることで、
Bitwardenアプリケーションと関連のないクリップボードアイテムを削除せずにこれを行うことができます。この機能は**デフォルトではオフ**になっていることにメモしてください。

A: そのモバイルアプリはどのようなアプリの権限を求めていますか？

A: BitwardenのAndroidおよびiOSアプリは、アプリを使用している間に次の権限を要求する場合があります：

権限	理由
Bitwardenに写真を撮影し、ビデオを録画する許可を与えますか？	二段階ログインまたはBitwarden認証器のQRコードをスキャンする。
あなたのデバイス上の写真やメディアにBitwardenがアクセスすることを許可しますか？	あなたのデバイスに保存されたファイルから添付ファイルやSendsを作成する。

Bitwardenに必要な追加の基本的な権限は、Google Playストアに記載されています。

A: ブラウザの拡張機能がnativeMessagingの権限を必要とする理由は何ですか？

A:ブラウザ拡張機能のバージョン 1.48.0では、ブラウザ拡張機能の生体認証によるロック解除が可能です。

この権限は、`nativeMessaging`とも呼ばれ、安全に受け入れることができます。これにより、ブラウザの拡張機能がBitwardenデスクトップアプリと通信できるようになり、生体認証でのロック解除を有効にするために必要です。

あなたのブラウザがこのバージョンに更新されると、「協力するネイティブアプリケーションと通信する」という新しい権限を受け入れるよう求められるかもしれません（Chromiumベースのブラウザで）、または「Firefox以外のプログラムとメッセージを交換する」。これについてはメモしておいてください。この権限を受け入れないと、拡張機能は無効のままになります。

Q: BitwardenはFIPS準拠ですか？

A: BitwardenはFIPS 140準拠のライブラリと暗号化を使用し、ほとんどのFIPS 140インストールのBitwardenは評価（例えば、サイバー成熟度モデル認証）を容易にするために自己ホスト型のオプションを活用しています。この時点で、Bitwardenプラットフォームは FIPS認証を実施していません。お問い合わせページからお気軽にお問い合わせください。

Q: Bitwardenへのアクセスを特定のデバイスに制限することはできますか？

A: 自己ホスト型を使用すると、カスタムファイアウォールやNGINXの設定、さらにはVPN/VLANアクセス制御を使用して、Bitwardenインスタンスのデバイスタイプやネットワークレイヤーアクセスを決定することができます。Bitwardenインスタンスへの特定のデバイスアクセスを制御するために、デバイスレベルの証明書などの他のツールも使用することができます。

Q: Bitwardenにはポータブルアプリケーションがありますか？

A: はい！Bitwardenデスクトップアプリは、ダウンロード可能なポータブル`.exe`としてWindowsで利用できます。ここからダウンロードできます。ポータブルアプリは、**常にオフライン**の環境や、アプリの自動更新が望ましくないシナリオに適しています。ポータブルアプリ**は自動的に更新されません**。

A: サイトアクセスオプションはBitwardenブラウザ拡張機能に干渉しますか？

A:ブラウザ拡張機能が適切に動作するには、Bitwarden ブラウザ拡張機能のサイト アクセス設定を **[すべてのサイト上] に設定するか、Bitwarden サーバーがリストに追加された特定のサイト上に**設定する必要があります。**クリック時**にサイトアクセスを設定すると、Bitwardenのサーバーからデータを取得するBitwardenの能力が制限され、これは基本的に資格情報を保存または更新するために必要です。