bitwarden | ヘルプセンターの記事

セキュリティ

暗号化

ヘルプセンターで表示:
https://bitwarden.com/help/what-encryption-is-used/

暗号化

Bitwardenは、保管庫のデータに対してAES-CBC 256ビット暗号化を使用し、PBKDF2 SHA-256またはArgon2を使用して暗号化キーを導出します。

Bitwarden は、データをクラウド サーバーに送信して保存する前に、ローカル デバイス上のデータを**常に**暗号化および/またはハッシュします。**Bitwardenのサーバーは、暗号化されたデータを保存するためだけに使用されます。**詳細については、ストレージをご覧ください。

保管庫のデータは、マスターパスワードから派生したキーを使用してのみ復号化できます。
Bitwardenはゼロ知識暗号化ソリューションであり、
あなただけがキーへのアクセス権と保管庫データを復号化する能力を持つことを意味します。

> **Tip**
> 私たちはあなたに、Bitwardenがあなたのデータをどのように暗号化するかを自分で確認するために、
> 私たちのインタラクティブ暗号化ページを訪れることをお勧めします。
>
> これらの暗号化キーがどのようにしてあなたの保管庫を保護するのかを詳しく知りたい場合は、
> セキュリティホワイトペーパーもご覧いただけます。

AES-CBC

Vault データの暗号化に使用されるAES -CBC (暗号ブロック チェーン)は暗号化の標準であり、
米国政府および世界中のその他の政府機関によって極秘データを保護するために使用されています。適切な実装と強力な暗号化キー（あなたのマスターパスワード）があれば、AESは破られないと考えられています。

PBKDF2

PBKDF2 SHA-256は、マスターパスワードから暗号化キーを導き出すために使用されますが、代わりにArgon2を選択することもできます。
Bitwardenは、サーバーへの送信前に、あなたのマスターパスワードをあなたのメールアドレスでソルト化しハッシュ化します**ローカルで**。
一度Bitwardenサーバーがハッシュ化されたパスワードを受け取ると、それは暗号学的に安全なランダム値で再度塩漬けにされ、
再度ハッシュ化され、私たちのデータベースに保存されます。

PBKDF2で使用されるデフォルトの反復回数は、クライアント（クライアント側の反復回数はアカウント設定から設定可能）で600,001回、
そして当社のサーバーに保存される際に追加の100,000回（デフォルトでは合計700,001回）です。組織のキーはRSA-2048を介して共有されます。

> **Tip**
> Bitwardenがデフォルトで使用する反復の数値は、2023年2月に増加しました。
> その時間以降に作成されたアカウントは600,001を使用しますが、それ以前にアカウントを作成した場合は、
> イテレーションカウントを増やすべきです。その方法については、次のセクションで見つけることができます。

使用されるハッシュ関数は一方向ハッシュです。つまり、Bitwarden の誰も**リバース エンジニアリングしてマスターパスワードを明らかにすることはできません。**たとえBitwardenがハッキングされたとしても、
あなたのマスターパスワードを取得する方法はありません。

KDF 反復回数を変更する

上記のように、Bitwardenは安全なデフォルトを使用していますが、ウェブ保管庫の**設定→セキュリティ→キー**メニューからイテレーションカウントを変更することができます。

反復回数を変更することで、攻撃者によるマスターパスワードの強制的な解読から保護することができますが、
それは最初から強力なマスターパスワードを使用する代替手段とは見なされるべきではありません。反復回数を変更すると、

保護された対称キーが再暗号化され、認証ハッシュが更新されます。これは通常のマスターパスワードの変更と同様ですが、対称暗号化キーはロテートされず、保管庫のデータは再暗号化されません。あなたのデータを再暗号化する情報については、ここをご覧ください。

KDF反復回数を高く設定すると、CPUの遅いデバイスでBitwardenにログイン（およびロック解除）する際のパフォーマンスが低下する可能性があります。私たちは、値を100,000ずつ増やし、その後すべてのデバイスをテストすることをお勧めします。

イテレーションカウントを変更すると、すべてのクライアントからログアウトされます。あなたの暗号化キーをロテートする際のリスクは、KDF反復回数を変更するときには存在しませんが、それでも私たちは保管庫をエクスポートすることをお勧めします。

Argon2id

2015年のパスワードハッシュコンペティションの優勝者であるArgon2は、PBKDF2の代替として利用可能です（詳細を学ぶ）。アルゴリズムのバージョンは3つあり、BitwardenはOWASPの推奨に従ってArgon2idを実装しています。Argon2idは他のバージョンのハイブリッドで、データ依存型とデータ独立型のメモリアクセスを組み合わせて使用しています。これにより、Argon2iのサイドチャネルキャッシュタイミング攻撃への抵抗力の一部と、Argon2dのGPUクラッキング攻撃への抵抗力の大部分を持つことができます（ソース）。

デフォルトでは、Bitwardenは64 MiBのメモリを割り当て、それを3回繰り返し、4つのスレッドで行うように設定されています。これらのデフォルトは現在のOWASPの推奨事項よりも高いですが、設定を変更する場合のいくつかのヒントがあります：

- **KDF 反復回数**を増やすと、実行時間は直線的に増加します。
- あなたが使用できる**KDF 並列性**の量は、マシンのCPUに依存します。一般的に、マックス。並列性 = コア数 x 2.

> **Note**
> Argon2idのユーザーで、KDFメモリ値が48MBより高い場合、iOSの自動入力が開始されるたび、または新しいSendが共有シートを通じて作成されるたびに、警告ダイアログが表示されます。このメッセージを避けるためには、Argon2idの設定を調整するか、生体認証でのロック解除を有効にしてください。

呼び出された暗号化ライブラリ

Bitwardenは暗号化コードを一切書き込みません。Bitwardenは、暗号化の専門家によって書かれ、維持されている人気のある信頼性の高い暗号化ライブラリからのみ暗号化を呼び出します。次の暗号化ライブラリが使用されています:

- JavaScript（ウェブ保管庫、ブラウザ拡張機能、デスクトップ、CLI）
  - ウェブ暗号化
  - Node.jsクリプト
  - 鍛冶場
- C# (モバイル)
  - コモンクリプト（iOS、アップル）
  - Javax.Crypto (Android、Oracle)
  - バウンシーキャッスル (アンドロイド)