bitwarden | ヘルプセンターの記事

セキュリティ

KDFアルゴリズム

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

KDFアルゴリズム

Bitwardenは、アカウント作成時に最初にKey Derivation Functions (KDFs)を使用して、
入力されたマスターパスワードからアカウントのマスターキーを導き出し、
それがアカウントのマスターパスワードハッシュの入力として機能します（詳細を学ぶ）。ユーザーが認証されるたび、
例えば保管庫のロック解除やマスターパスワードの再提示を満たすと、新たに導出されたハッシュを元のハッシュと比較できるように、
プロセスが繰り返されます。それらが一致する場合、ユーザーは認証されます。

KDFは、マスターパスワードに対するブルートフォース攻撃や辞書攻撃を防ぐためにこのような能力で使用されます。KDFは、
攻撃者のマシンに対して、各パスワードの推測ごとに非自明な数値のハッシュを計算させ、攻撃者のコストを増加させます。

現在、Bitwardenで使用できるKDFアルゴリズムは2つあります。それらは**PBKDF2**と**Argon2**です。各アルゴリズムには、
攻撃者に対して時間と費用、または「作業要因」を増加させるために使用できるオプションの選択肢があります。

PBKDF2

パスワードベースのキー導出関数2（PBKDF2）はNISTによって推奨されています。また、Bitwardenによって実装されたものは、
デフォルト値が変更されない限り、FIPS-140の要件を満たします。

Bitwardenによって実装されたPBKDF2は、マスターパスワードをユーザー名で塩漬けにし、その結果の値を一方向ハッシュアルゴリズム
（HMAC-SHA-256）を通して固定長のハッシュを作成する方法で動作します。この値は再度、ユーザー名で塩漬けにされ、設定可能な数値
（**KDF 反復回数**）でハッシュ化されます。すべての反復後の結果値があなたのマスターキーであり、
それはユーザーがログインするたびにそのユーザーを認証するために使用されるマスターパスワードハッシュの入力として機能します
（詳細を学ぶ）。

デフォルトでは、BitwardenはHMAC-SHA-256の実装に対してOWASPが推奨する通り、600,000回反復するように設定されています。
ユーザーがこの値を低く設定しない限り、実装はFIPS-140に準拠していますが、
設定を変更することを選択した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、攻撃者がパスワードをクラックするのにかかる時間**とともに**、
  正当なユーザーがログインするのにかかる時間**も**増加します。

- 私たちは、値を100,000単位で増やし、すべてのデバイスをテストすることをお勧めします。

Argon2id

Argon2は2015年のパスワードハッシュ化コンペティションの優勝者です。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）。

Bitwardenによって実装されたArgon2は、マスターパスワードをユーザー名で塩漬けにし、その結果の値を一方向ハッシュアルゴリズム
（BLAKE2b）を通して固定長のハッシュを作成する方法で動作します。

Argon2は次に、一部のメモリ（**KDFメモリ**）を割り当て、計算されたハッシュでそれを満たすまで埋めます。これは、
最初に終了したメモリの次の部分から始まり、反復的に（**KDF 反復回数**）数値の回数、スレッドの数値（**KDF 並列性**）で繰り返されます。
すべての反復後の結果値が、マスターキーとなり、
それはユーザーがログインするたびにそのユーザーを認証するために使用されるマスターパスワードのハッシュの入力として機能します
（詳細を学ぶ）。

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.

- iOSはオートフィルのためのアプリメモリを制限します。デフォルトの64 MBからイテレーションを増やすと、
自動入力で保管庫をロック解除する際にエラーが発生する可能性があります。

KDFアルゴリズムを変更する

> **Note**
>
> **2023-02-14**:Argon2はBitwardenクライアントのバージョン2023.2.0以降でサポートされており、
> ウェブ保管庫経由でArgon2に切り替えると、他のクライアントが更新されるまで、
> 通常リリース後1週間以内に保管庫をロードできなくなる可能性があります。

KDFアルゴリズムを変更するには、ウェブ保管庫の**設定→セキュリティ→キー**ページに移動します。アルゴリズムを変更すると、
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。

アルゴリズムを変更すると、すべてのクライアントからログアウトされます。
アルゴリズムを変更するときに存在しない暗号化キーをロテートするリスクがありますが、
それでも私たちはまず保管庫をエクスポートすることをお勧めします。

低い KDF 反復回数

2023.2.0リリースで、Bitwardenは、更新されたOWASPガイドラインに従って、
PBKDF2アルゴリズムを使用するアカウントのデフォルトのKDF反復回数を600,000に増やしました。これは、
ますます強力なデバイスを装備したハッカーに対する保管庫の暗号化を強化します。PBKDF2アルゴリズムを使用していて、
KDF反復回数が600,000未満に設定されている場合、KDF設定を増やすように促す警告メッセージが表示されます。

> **⚠ Warning**
>
> 暗号化設定に何か変更を加える前に、個々の保管庫のデータをまずバックアップすることをお勧めします。詳細については、
> 保管庫データをエクスポートをご覧ください。

ゼロ知識暗号化を維持するために、
Bitwardenも管理者もあなたのアカウントのセキュリティや保管庫の暗号化設定を変更することはできません。
このメッセージが表示された場合、**KDF設定を更新**ボタンを選択し、PBKDF2の反復を少なくとも600,000回に増やすか、
KDFアルゴリズムをデフォルト設定のArgon2idに変更してください。これらの変更を保存すると、
すべてのクライアントからログアウトされますので、マスターパスワードを覚えており、
二段階ログイン方法が利用可能であることを確認してください。

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。強力なマスターパスワードは、
常にあなたのBitwardenアカウントの最初で最良の防衛線です。