セキュリティ

Bitwardenセキュリティホワイトペーパー

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

Bitwardenセキュリティホワイトペーパー

Bitwardenセキュリティとコンプライアンスプログラムの概要

リモートワークの増加とインターネットの使用率がこれまで以上に高まる中、ログインとパスワードを持つオンラインアカウントを何十個も（場合によっては何百個も）作成し、維持する需要は驚くほどです。

セキュリティ専門家は、作成するすべてのアカウントに対して異なるランダムに生成されたパスワードを使用することを推奨しています。でも、どうやってすべてのパスワードを管理しますか？そして、組电全体で良好なパスワード衛生を維持するにはどうすればよいですか？

効果的なパスワード管理は、エンタープライズで大いに活用されていないリソースです。Rapid7による2020年版Under the Hoodieレポートでは、パスワード管理と二要素認証のような二次コントロールが「深刻な不足」であり、「簡単な」妥協を引き起こしているとメモしています。パスワードを安全でない方法で再利用したり共有したりすると、エンタープライズは脆弱になります。

組甒に変化をもたらすためには、セキュリティチームとITチームが最善の方法について従業員に教育を行う必要があります。パスワードの管理に関して、良好なパスワード衛生を奨励しサポートする最も簡単な方法の一つは、職場全体にパスワード管理ソリューションを展開することです。

Bitwardenは、すべてのログイン、パスワード、その他の機密情報を保存する最も簡単で安全な方法であり、便利にすべてのデバイス間で同期を保つことができます。

Bitwardenは、最高レベルのセキュリティを維持しながら、パスワードを作成、保存、共有するためのツールを提供します。

Bitwardenのソリューション、ソフトウェア、インフラストラクチャ、およびセキュリティプロセスは、多層的で防御深度のアプローチを基に、最初から設計されています。Bitwardenのセキュリティとコンプライアンスプログラムは、ISO27001情報セキュリティ管理システム（ISMS）に基づいています。私たちは、セキュリティポリシーとプロセスを管理するポリシーを定義し、私たちがあなたに提供するサービスの適用可能な法的、業界、規制要件に一致するように、セキュリティプログラムを継続的に更新します。これは私たちのサービス利用規約の下で行われます。

Bitwardenは、専用のセキュリティエンジニアリングチームを含む業界標準のアプリケーションセキュリティガイドラインに準拠しています。これには、アプリケーションのソースコードとITインフラストラクチャの定期的なレビューが含まれ、セキュリティの脆弱性を検出、検証、修復します。

このホワイトペーパーは、Bitwardenのセキュリティ原則の概要と、特定の領域でより詳細な情報を提供する追加のドキュメントへのリンクを提供します。

Bitwardenセキュリティ原則

ユーザーデータ保護

Bitwardenは、ユーザーデータを保護するために以下のキーセキュリティ対策を利用しています。

エンドツーエンドの暗号化:エンドツーエンドの AES-CBC 256 ビット暗号化、ソルテッド ハッシュ、および PBKDF2 SHA-256 を使用して、パスワードと個人情報をロックします。すべての暗号化キーは、デバイス上のクライアントによって生成され、管理され、すべての暗号化はローカルで行われます。パスワードハッシュ化導出セクションで詳細をご覧ください。

知識ゼロの暗号化: Bitwarden チーム メンバーはパスワードを見ることができません。あなたのデータは、個々のメールアドレスとマスターパスワードでエンドツーエンドに暗号化されたままです。私たちは決してあなたのマスターパスワードや暗号化キーを保存せず、アクセスすることもできません。

> ⓘ **Note**
>
> 2021年の中頃にリリースされたアカウント回復は、すべての組織に新しいRSA公開/秘密キーペアを導入しました。プライベートキーは、保存する前に組織の既存の対称キーでさらに暗号化されます。新しい組織の作成時、または既存の組織に対しては、キーペアが生成され、クライアント側で暗号化されます。
>
> - 管理 → 人々 画面へのナビゲーション。
> - 設定→私の組織画面で何でも更新します。
> - 一つの組織タイプから別の組織タイプへのアップグレード。

セキュアなパスワード共有: Bitwardenは、組織全体のユーザーとのセンシティブなデータの安全な共有と管理を可能にします。非対称および対称暗号化の組み合わせは、共有される敏感な情報を保護します。

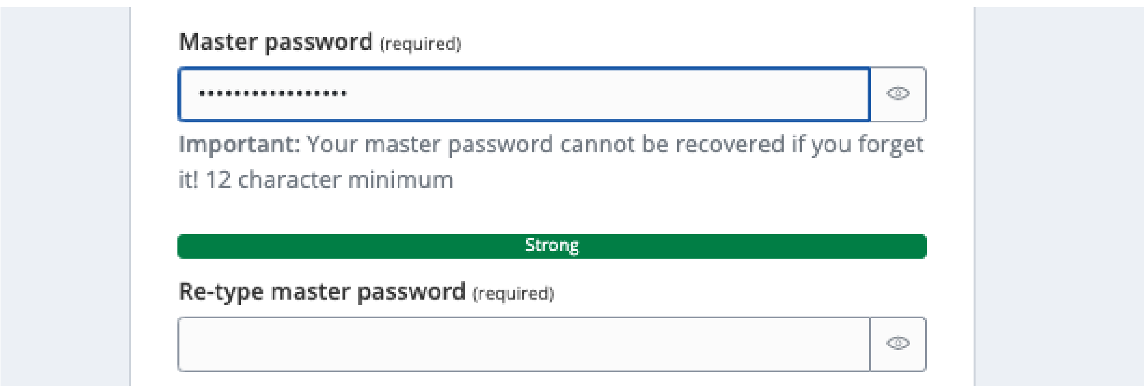
オープンソースとソース利用可能なコード:
すべてのBitwardenソフトウェア製品のソースコードはGitHubにホストされており、誰でもBitwardenのコードベースのレビュー、監査、貢献を歓迎します。Bitwardenのソースコードは、評判の良いサードパーティーのセキュリティ監査会社や独立したセキュリティ研究者によって監査されています。さらに、Bitwardenの脆弱性開示プログラムは、HackerOneのハッカーコミュニティの協力を得て、Bitwardenをより安全にするためのものです。

設計によるプライバシー: Bitwarden は、すべてのログインを暗号化された保管庫に保存し、すべてのデバイス間で同期します。それがあなたのデバイスを離れる前に完全に暗号化されているため、あなただけがあなたのデータにアクセスできます。たとえ私たちが望んでも、Bitwardenのチームでさえあなたのデータを読むことはできません。あなたのデータはAES-CBC 256ビット暗号化、ソルティングハッシング、およびPBKDF2 SHA-256で封印されています。

セキュリティ監査＆コンプライアンス： オープンソースで、サードパーティーによる監査を受けているBitwardenは、AICPA SOC2 タイプ2 / プライバシーシールド、GDPR、およびCCPAの規制に準拠しています。

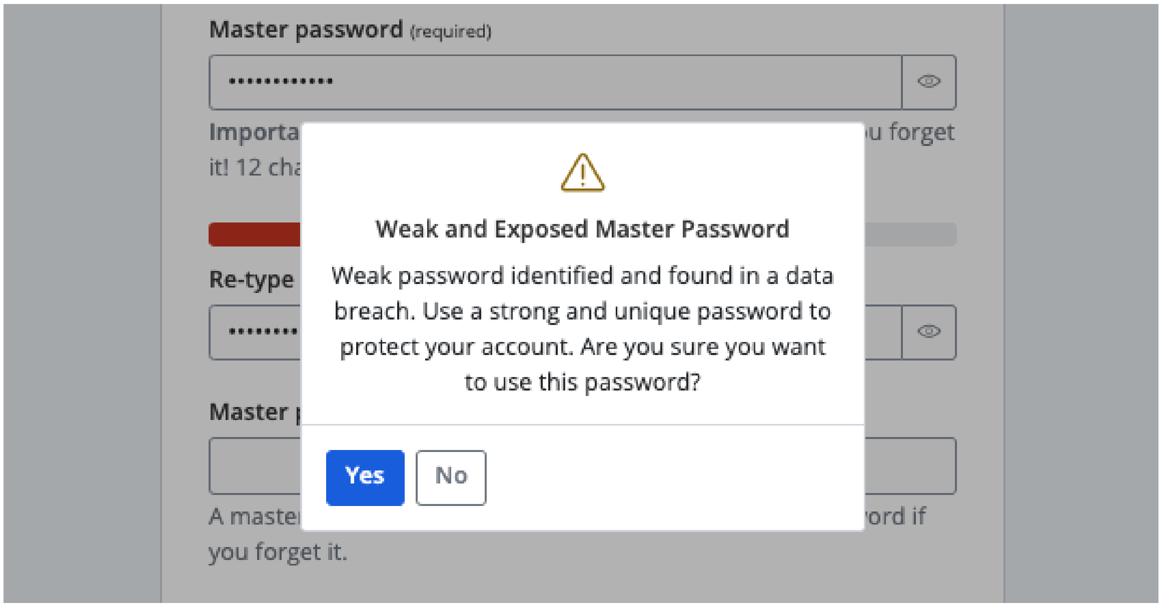
マスターパスワード

Bitwardenでのユーザーデータ保護は、ユーザーがアカウントとマスターパスワードを作成する瞬間から始まります。オンボーディングプロセス中に強力なマスターパスワードを使用することを強くお勧めします。Bitwardenには、強力なマスターパスワードを奨励するために入力されるマスターパスワードの全体的な強度を評価し表示するパスワード強度メーターが含まれています。



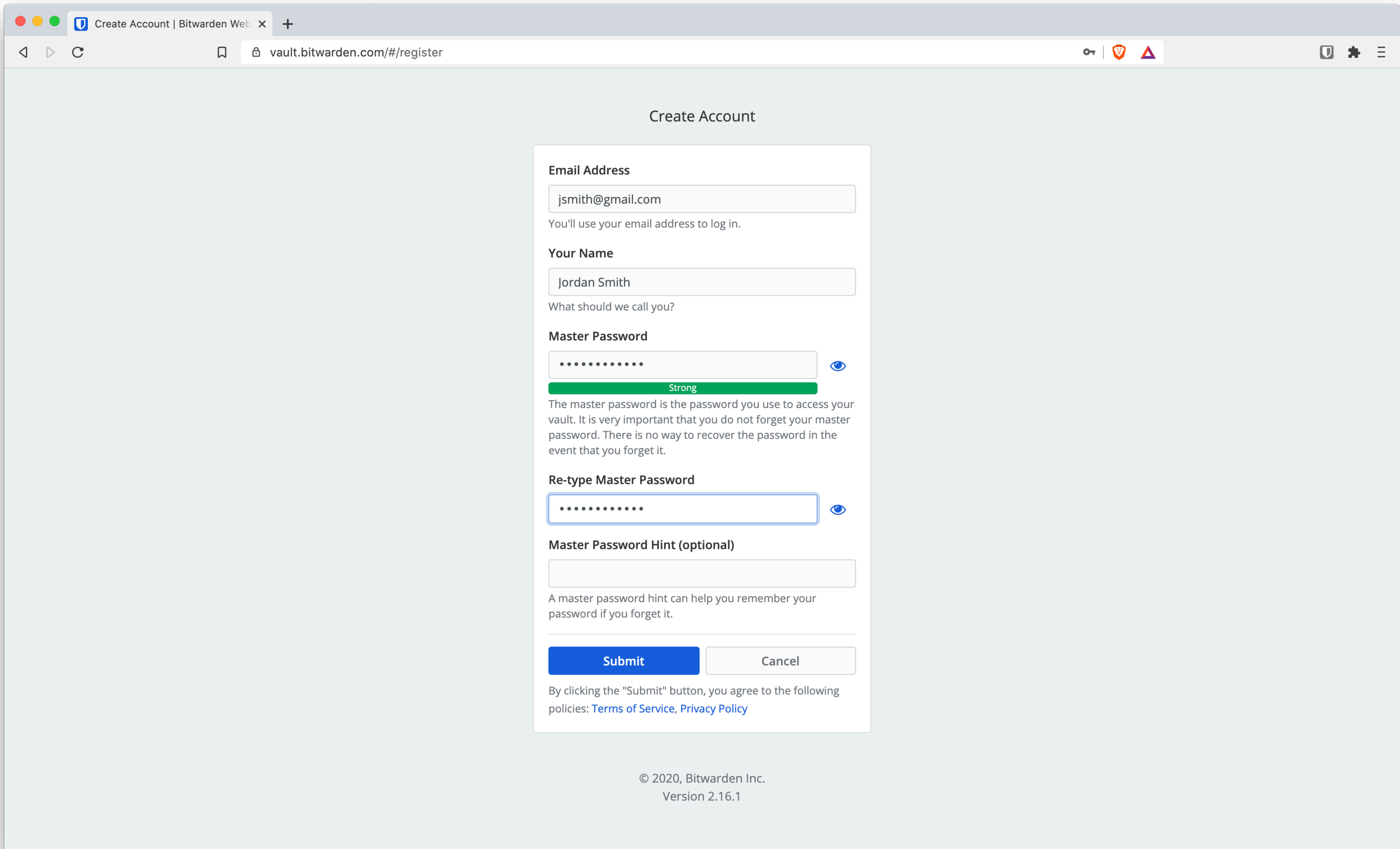
Bitwardenアカウントを作成する

弱いパスワードでサインアップしようとすると、Bitwardenは選択したマスターパスワードが弱いと通知します。Bitwardenアカウントを作成するとき、HIBPを使用してマスターパスワードの既知のデータ漏洩をチェックするオプションもあります。



弱いマスターパスワードの警告

強力なマスターパスワードを使用することは、あなた自身のセキュリティ上の利益のためです。なぜなら、
それはあなたがセキュアな保管庫にアクセスするために使用するトークンであり、そこにはあなたの機密アイテムが保管されているからです。
Bitwardenサービスを使用する間、あなたのアカウントのセキュリティを保つ責任があります。私たちは、
二段階ログインなどの追加的な対策を提供していますが、アカウントの内容とそのセキュリティはあなた次第です。



強力なマスターパスワードを選んでください。

詳細はこちら：パスワード管理のための最良の5つの実践 と NISTからのパスワードを安全に保つための3つのヒント

便利なツール: Bitwarden パスワード強度テストツール と Bitwarden パスワードジェネレーター

あなたがマスターパスワードを決して忘れないことが非常に重要です。マスターパスワードは使用後にメモリから消去され、Bitwardenのサーバーには一切送信されません。したがって、それを忘れた場合にパスワードを回復する方法はありません。

これは、Bitwardenチームの誰もがあなたの実際のデータを見たり、読んだり、逆にエンジニアリングして取得することはできないということも意味します。あなたのデータは、ローカルデバイスを離れる前に完全に暗号化および/またはハッシュ化されます。これはBitwardenがあなたとあなたのデータを保護するために取る重要なステップです。

あなたのアカウントを作成し、マスターパスワードを指定した後、Bitwardenは次に、アカウントのデータを保護するために使用されるいくつかのキーを生成します。

> **ⓘ Note**
>
> 2021年半ばに、Bitwardenはエンタープライズプランのためのアカウント回復を導入しました。このオプションを使用すると、ユーザーと組織は、管理者と所有者がユーザーのパスワードをリセットできる新しいポリシーを実装する機会を得ることができます。

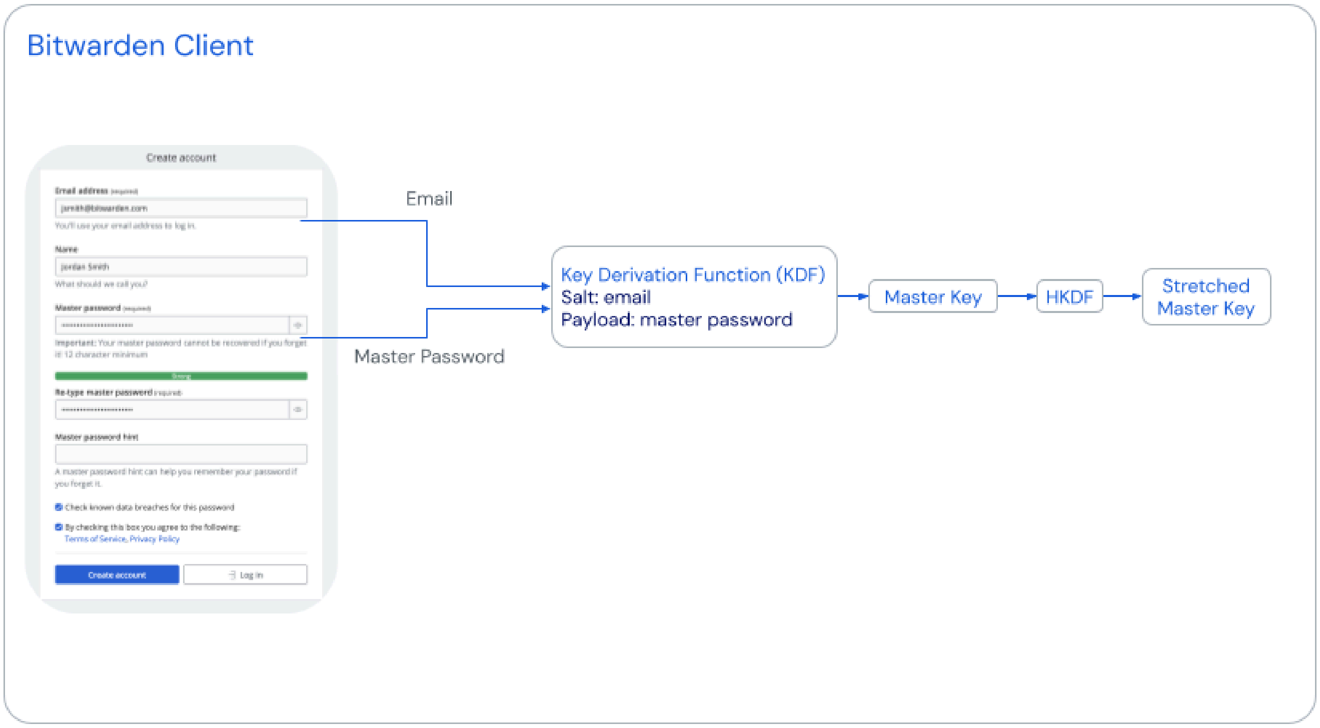
マスターパスワードのハッシュ化、キー導出、および暗号化プロセスの概要

ユーザーアカウントの作成

アカウント作成フォームが送信されると、BitwardenはPassword-Based Key Derivation Function 2（PBKDF2）を使用して、600,000回の反復ラウンドでユーザーのマスターパスワードを伸ばし、ユーザーのメールアドレスの塩を使用します。

結果として得られる塩化された値は、256ビットのマスターキーです。マスターキーは、HMACベースの抽出拡張キー導出関数（HKDF）を使用して512ビットの長さに拡張されます。マスターキーとストレッチされたマスターキーは、Bitwardenのサーバーに保存されたり、送信されたりすることはありません。

> **Note**
> 2023.2.0リリースで、BitwardenはPBKDF2の代替オプションとしてArgon2idを追加しました。もっと学ぶ

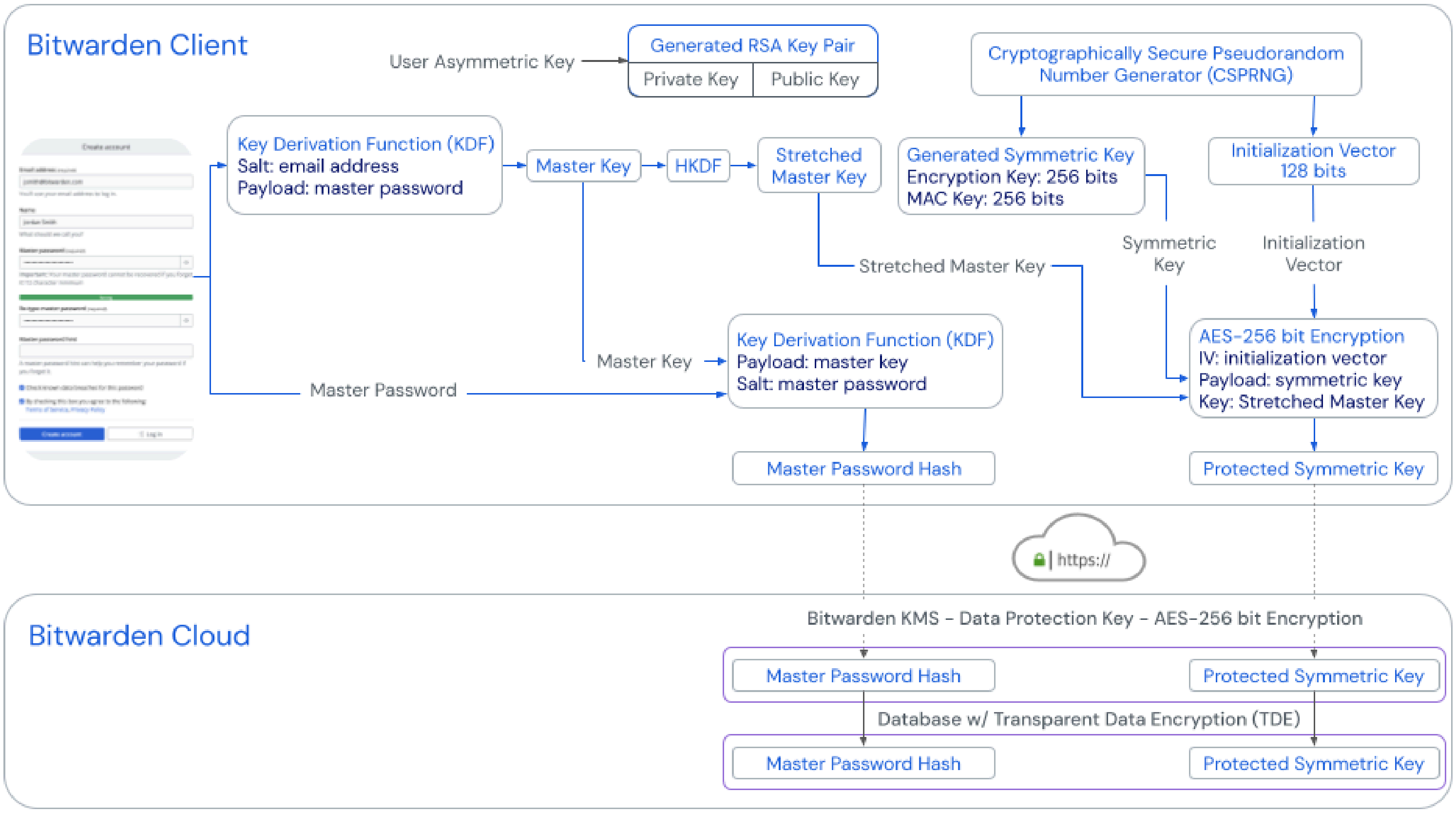


パスワードベースのキー導出

さらに、512ビットの対称キーと初期化ベクトルは、暗号学的に安全な疑似ランダム数値ジェネレーター（CSPRNG）を使用して生成されます。対称キーは、ストレッチされたマスターキーと初期化ベクトルを使用してAES-256ビット暗号化で暗号化されます。結果として得られるキーは、保護された対称キーと呼ばれます。保護された対称キーは、ユーザーに関連付けられた主要なキーで、アカウント作成時にサーバーに送信され、同期時にBitwardenクライアントアプリに送り返されます。

ユーザーがアカウントを登録するとき、非対称キー（RSAキーペア）も生成されます。生成されたRSAキーペアは、ユーザーが組織を作成する場合、または作成した場合に使用されます。これは、ユーザー間でデータを共有するために作成および使用することができます。詳細については、ユーザー間でデータを共有するを参照してください。

マスターキーとマスターパスワードの塩をペイロードとして、PBKDF-SHA256を使用してマスターパスワードのハッシュも生成されます。マスターパスワードのハッシュは、アカウント作成とログイン時にサーバーに送信され、ユーザーアカウントの認証に使用されます。サーバーに到達すると、マスターパスワードのハッシュはランダムなソルトと600,000回の反復を使用してPBKDF2-SHA256で再度ハッシュ化されます。以下に、パスワードのハッシュ化、キー導出、および暗号化プロセスの概要を示します。



Bitwardenのパスワードハッシング、キー導出、および暗号化

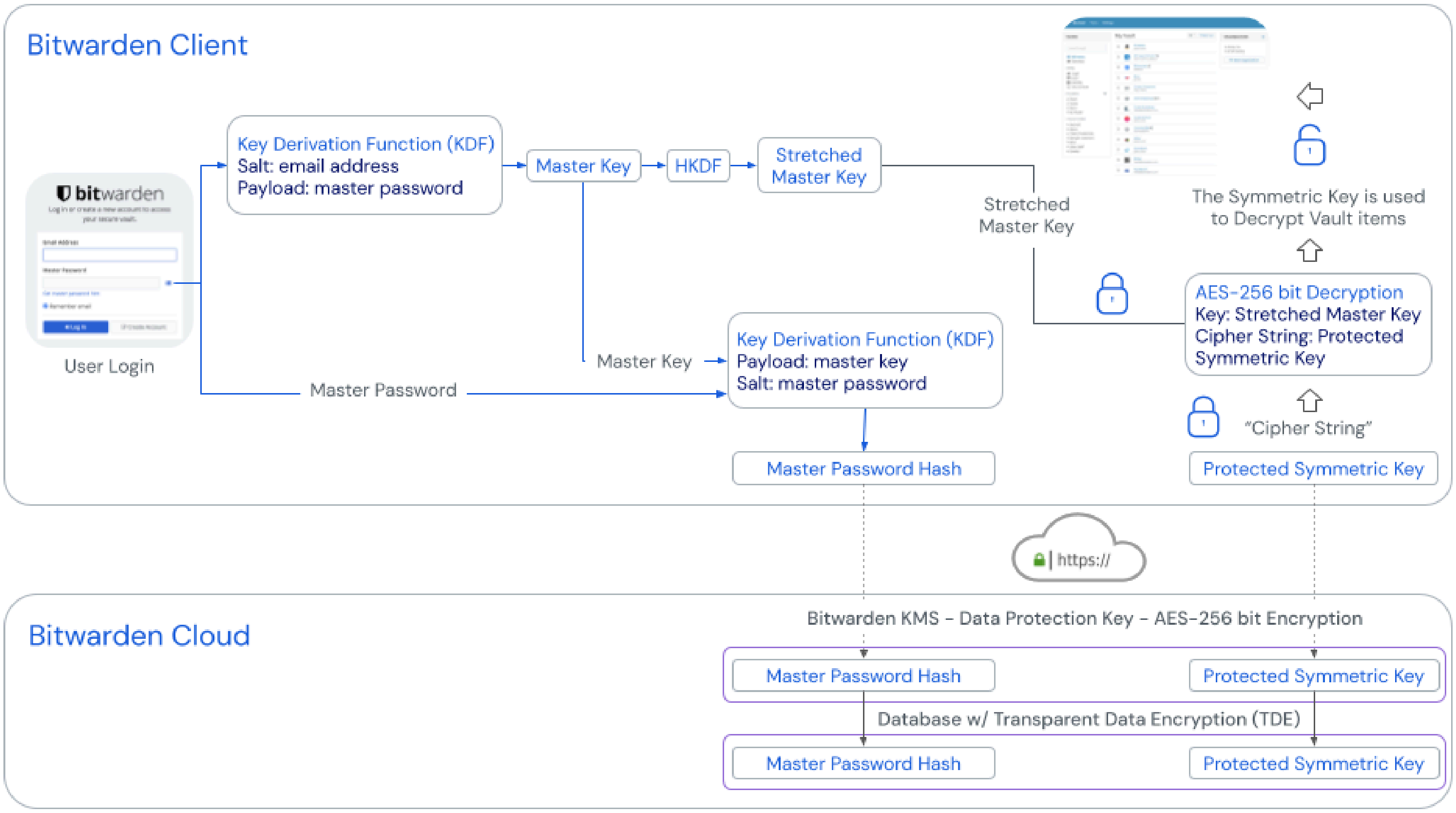
ユーザーログイン | ユーザー認証 | ユーザー保管庫データへのアクセス

まず、Bitwardenアカウントにログインするためには、メールアドレスとマスターパスワードを入力する必要があります。

次に、Bitwardenは、デフォルトで600,000回の反復ラウンドを使用して、Password-Based Key Derivation Function 2（PBKDF2）を使用して、メールアドレスの塩を使用してマスターパスワードを伸ばします。結果として得られる塩化された値は、256ビットのマスターキーです。アカウント作成とログイン時にマスターキーのハッシュがサーバーに送信され、ユーザーアカウントの認証に使用されます。

> ⓘ **Note**
> 2023.2.0リリースで、BitwardenはPBKDF2の代替オプションとしてArgon2idを追加しました。もっと学ぶ

マスターキーは、HMACベースの抽出拡張キー導出関数（HKDF）を使用して512ビットの長さに拡張されます。保護された対称キーは、ストレッチされたマスターキーを使用して復号化されます。対称キーは保管庫のアイテムを復号化するために使用されます。復号化はBitwardenクライアント上で完全に行われます。なぜなら、あなたのマスターパスワードまたはストレッチされたマスターキーは、Bitwardenのサーバーに保存されたり、送信されたりすることはありません。



ユーザーログインの概要

私たちはマスターパスワードをローカルにもBitwardenクライアントのメモリにも保存していません。あなたの暗号化キー（対称キー）は、アプリがロック解除済みの間、メモリに保持されています。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消去されます。ロック画面で一定時間の非活動状態が続いた後、残存する管理されたメモリアドレスもすべてパージされるように、アプリケーションのプロセスを再読み込みします。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。私たちは、ロック状態の間、アプリケーションが完全に安全であると考えています。

追加ユーザーデータ保護：二段階ログインを有効にする時

2 段階ログイン (2 要素認証または 2FA とも呼ばれます) は、アカウントの追加のセキュリティ層であり、たとえ誰かがマスターパスワードを発見したとしても、自分**だけ**がアカウントにアクセスできるように設計されています。

ベストプラクティスとして、すべてのユーザーにBitwardenアカウント内で二段階ログインを有効にし、使用することをお勧めします。2ステップログインが有効化されていると、Bitwardenにログインする際に（マスターパスワードに加えて）二次的なステップを完了する必要があります。デフォルトでは、この二次ステップを毎回完了するように求められますが、「私を覚えておいて」というプロンプトがあり、二要素認証のステータスを保存することができます。そのため、特定のデバイスで次回ログインする際には、最大30日間二要素認証なしでログインすることができます。

メモ：マスターパスワードを変更したり、セッションの認証を解除したりすると、以前に「私を覚えておいて」と選択したかどうかに関係なく、二要素認証を再度認証する必要があります。

Bitwardenは、以下の方法を使用した二段階ログインをサポートしています：

無料プラン

- 認証アプリ（例えば、2FAS、Ravio、またはAegis）を使用する

- FIDO2 WebAuthn（任意のFIDO2 WebAuthn認定キー）
- Eメール

プレミアム機能 - ファミリー、チーム、エンタープライズプランの一部として含まれています

- Duoセキュリティ、Duo Push、SMS、電話、およびU2Fセキュリティキー
- YubiKey（任意の4/5シリーズデバイスまたはYubiKey NEO/NFC）

あなたは複数の二段階ログイン方法を有効にすることができます。複数の2段階ログイン方法が有効になっている場合、ログイン時に表示されるデフォルト方法の優先順位は次の通りです：FIDO U2F > YubiKey > Duo > 認証アプリ > メールアドレス。ただし、ログイン中に任意の方法に手動で切り替えて使用することもできます。

あなたの二段階ログインリカバリーコードを絶対に失わないことが非常に重要です。Bitwardenは、マスターパスワードや二段階ログインのリカバリーコードを失ったユーザーをサポートしないアカウント保護セキュリティモデルを提供しています。あなたのアカウントで二段階ログインが有効になっていて、二段階ログインのリカバリーコードへのアクセスを失った場合、あなたのBitwardenアカウントにログインすることはできません。

> **Note**
> 2021年の中頃、Bitwardenはエンタープライズプランのためのアカウント回復を導入しました。このオプションを使用すると、ユーザーと組織は、管理者と所有者がユーザーのパスワードをリセットできる新しいポリシーを実装する機会を得ることができます。

ユーザーパスワードの変更

あなたのマスターパスワードは、ウェブ保管庫からのみ変更できます。ユーザーパスワードの変更方法についての具体的な手順は、このBitwardenヘルプ記事をご覧ください。

あなたのアカウントの暗号化キーをロテートする

パスワードの変更操作中に、アカウントの暗号化キーをロテート（変更）するオプションもあります。以前のマスターパスワードが侵害されたと思われる場合や、あなたのデバイスの一つからBitwarden保管庫のデータが盗まれたと思われる場合、暗号化キーをロテートすることは良い考えです。

> **Warning**
> あなたのアカウントの暗号化キーをロテートすることは、敏感な操作であり、それがデフォルトのオプションではない理由です。キーのローテーションは、アカウントの新しいランダムな暗号化キーを生成し、この新しいキーを使用して**すべての保管庫データを再暗号化する**ことを含みます。この記事で追加の詳細をご覧ください。

トランジット中のデータ保護

Bitwardenは、あなたの機密データを取り扱う際に、非常に真剣にセキュリティを重視します。あなたのデータは、ローカルデバイスで最初に暗号化されない限り、Bitwardenクラウドに送信されることはありません。

さらに、BitwardenはTLS/SSLを使用して、Bitwardenクライアントとユーザーデバイスからのサーバーへの通信を保護します。BitwardenのTLS実装は、サーバー認証とキー交換のために2048ビットのX.509証明書を使用し、一括暗号化のための強力な暗号スイートを使用します。私たちのサーバーは、弱い暗号とプロトコルを拒否するように設定されています。

Bitwardenは、HTTP Strict Transport Security（HSTS）などのHTTPセキュリティヘッダーも実装しており、すべての接続がTLSを使用するように強制します。この追加の保護層であるHSTSは、ダウングレード攻撃や誤設定のリスクを軽減します。

レスト時のデータ保護

Bitwardenは、クラウドサーバーに同期する前に、ローカルデバイス上のデータを常に暗号化および/またはハッシュ化します。Bitwardenのサーバーは、暗号化された保管庫データの保存と同期にのみ使用されます。Bitwardenクラウドサーバーから暗号化されていないデータを取得することはできません。具体的には、BitwardenはAES 256ビット暗号化およびPBKDF-SHA256を使用して、あなたのデータを保護します。

AESは暗号化の標準であり、アメリカ政府や世界中の他の政府機関が最高機密のデータを保護するために使用しています。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）を使用すると、AESは破られないと考えられています。

PBKDF-SHA256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。その後、このキーはBitwardenサーバーでの認証のためにソルト化され、ハッシュ化されます。PBKDF2で使用されるデフォルトの反復回数は、クライアント上で600,001回（このクライアント側の反復回数はあなたのアカウント設定から設定可能）、そして当社のサーバー上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。

> **Note**
>
> 2023.2.0リリースで、BitwardenはPBKDF2の代替オプションとしてArgon2idを追加しました。もっと学ぶ

一部の暗号化されたデータ、ユーザーの保護された対称キーとマスターパスワードのハッシュも、アプリケーションによって透明に休止状態で暗号化され、Bitwardenデータベースへの出入り時に再度暗号化および復号化されます。

Bitwardenはさらに、Azureの透過的データ暗号化（TDE）を使用して、データベース、関連するバックアップ、および休止中のトランザクションログファイルのリアルタイム暗号化と復号化を実行することで、悪意のあるオフライン活動の脅威から保護します。

詳しく学ぶ：エンドツーエンドの暗号化がゼロ知識を可能にする方法 と どの暗号化が使用されているか

パスキーでログインし、エンドツーエンドの暗号化を維持してください。

マスターパスワードに加えて、ユーザーはパスキーを使って保管庫をロック解除することを選択できます。このプロセスは、認証器からキー素材を取得する擬似ランダム関数またはPRFと呼ばれるWebAuthnの先端的な標準と拡張機能を利用します。PRFを使用して、Bitwardenパスワードマネージャーの保管庫とBitwardenシークレットマネージャーに保存されたデータの暗号化と復号化に派生キーが使用され、エンドツーエンドのゼロ知識暗号化が維持されます。

パスキーがBitwardenへのログインに登録されたとき：

1. 認証者はWebAuth APIを介して**パスキーの公開鍵と秘密鍵のペア**を生成します。このキーペアは、定義により、あなたのパスキーを構成するものです。

2. **PRF対称キー**は、WebAuthn APIのPRF拡張機能を介して認証器によって生成されます。このキーは、あなたのパスキーに固有の**内部秘密**とBitwardenから提供される**ソルト**から派生しています。

3. Bitwardenクライアントによって、**PRFの公開鍵と秘密鍵のペア**が生成されます。PRF公開鍵はあなたの**アカウント暗号化キー**を暗号化し、クライアントはログインしてロック解除することでこれにアクセスでき、結果として得られる**PRFで暗号化されたアカウント暗号化キー**がサーバーに送信されます。

4. **PRFプライベートキー**は**PRF対称キー**（ステップ2参照）で暗号化され、結果として得られる**PRFで暗号化されたプライベートキー**がサーバーに送信されます。

5. あなたのクライアントはデータをBitwardenサーバーにSendし、あなたのアカウントの新しいパスキー資格レコードを作成します。あなたのパスキーが保管庫の暗号化と復号化のためにサポートに登録されている場合、この記録には以下が含まれます：

   - パスキーの名前
   - パスキー公開鍵
   - PRF公開鍵
   - PRF暗号化されたアカウント暗号化キー
   - PRFで暗号化されたプライベートキー

認証を達成するために必要なパスキープライベートキーは、暗号化された形式でのみクライアントから出ます。

パスキーがログインに使用され、特に、保管庫のデータを復号化するために使用される場合:

1. WebAuthn APIの公開鍵暗号を使用して、あなたの認証リクエストが主張され、確認されます。

2. あなたの**PRFで暗号化されたアカウントの暗号化キー**と**PRFで暗号化されたプライベートキー**は、
サーバーからあなたのクライアントに送信されます。

3. Bitwardenが提供する同じ**ソルト**と、あなたのパスキーに固有の**内部秘密**を使用して、**PRF対称キー**がローカルで再作成されます。

4. **PRF対称キー**は、あなたの**PRFで暗号化されたプライベートキー**を復号化するために使用され、あなたの**PRFプライベートキー**が得られます。

5. **PRFプライベートキー**は、あなたの**PRFで暗号化されたアカウント暗号化キー**を復号化するために使用され、
あなたの**アカウント暗号化キー**を得る結果となります。あなたのアカウントの暗号化キーは、保管庫のデータを復号化するために使用されます。

保管庫のアイテムがどのように保護されているか

あなたの保管庫データに関連するすべての情報（ログイン、カード、ID、メモ）は、エンドツーエンドの暗号化で保護されています。
あなたがBitwarden保管庫に保存することを選んだアイテムは、まずCipherオブジェクトと呼ばれるアイテムで保存されます。暗号化オブジェクトは、生成された対称キーで暗号化され、
これはあなたの保護された対称キーをあなたの伸ばされたマスターキーを使用して復号化することでのみ知ることができます。この暗号化と復号化は、マスターパスワードまたはストレッチされたマスターキーがBitwardenのサーバーに保存されたり送信されたりしないため、
完全にBitwardenクライアント上で行われます。

保管庫健康レポート

すべてのBitwarden有料プランには、個人と組織の両方のための保管庫健康レポートが付属しています。

個々の保管庫について、個々の人々は以下のものにアクセスできます：

- 流出済みパスワードレポート
- 再利用されたパスワードのレポート
- 弱いパスワードのレポート
- 保護されていないウェブサイトのレポート
- 非活動二要素認証レポート
- データ漏洩レポート

ビジネスユーザーのために、組甎の保管庫アイテムに対する同様のレポートセットが存在します。

詳細を読む：Vault Healthのレポート

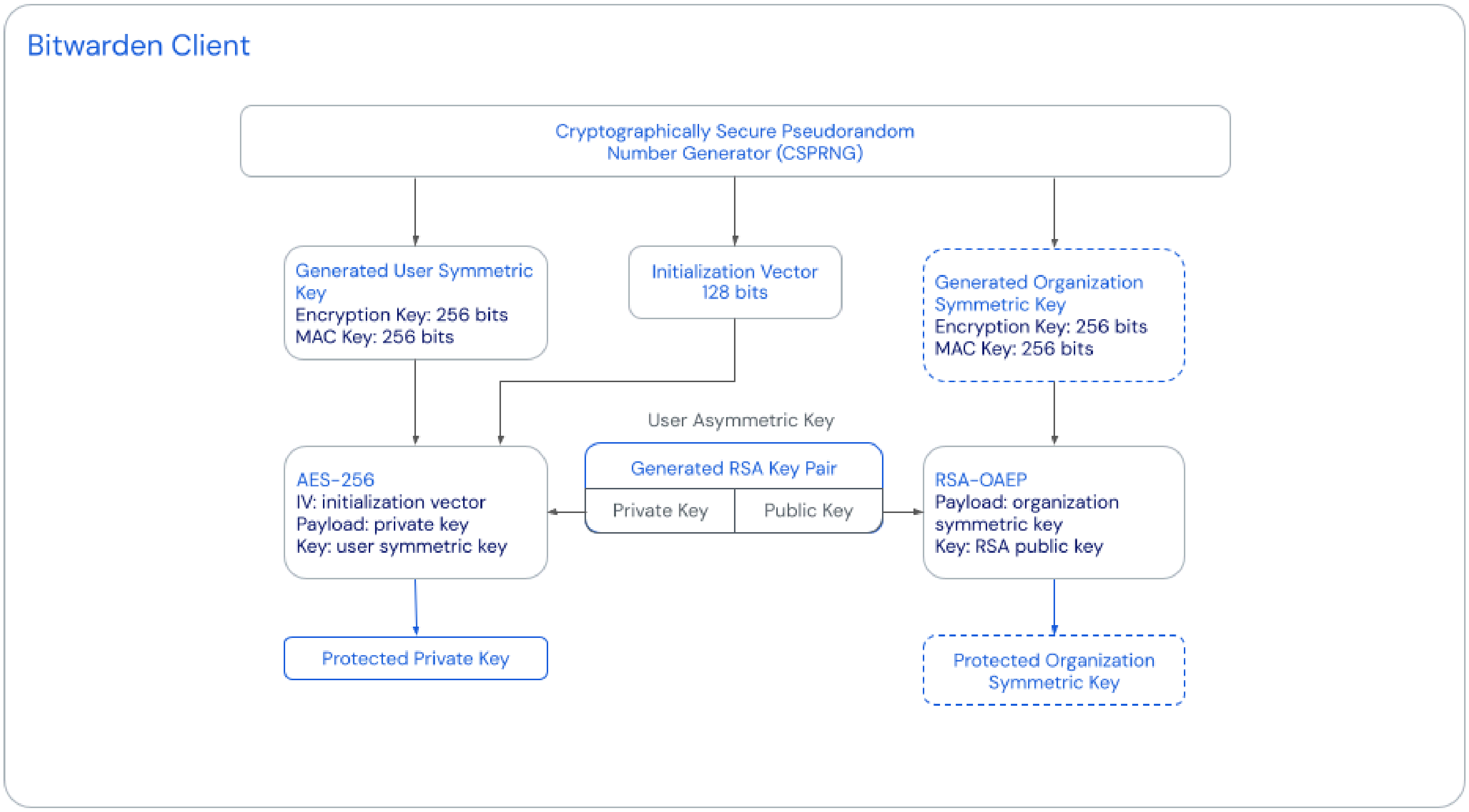
Bitwardenイベントログと外部レポートについての詳細は、イベントログをご覧ください。

パスワードや他の秘密情報をBitwardenにインポートする

あなたは簡単にデータを40以上の異なるサービスからBitwardenにインポートできます。これには、
すべての人気のあるパスワードマネージャーアプリケーションが含まれます。サポートされているアプリケーションの完全なリストと、
Bitwardenにデータをインポートするための追加情報、トラブルシューティング手順を含む情報は、Bitwardenヘルプセンターで文書化されています。

LastPass.comのWeb保管庫からサイトをエクスポートする場合は、
このヘルプメモLastPassからデータをインポートするの特定の情報を参照してください。

ユーザー間でデータを共有する



組織のキー保護と交換

コラボレーションは、パスワードマネージャーを使用する最大の利点の一つです。共有を有効にするためには、まず組織を作成する必要があります。Bitwarden組織は、アイテムを共有したいユーザーを関連付けるエンティティです。組織は、ファミリー、チーム、会社、またはデータを共有したいと願う他のタイプのグループである可能性があります。

個々のユーザーアカウントは、多くの異なる組織を作成したり、所属したりすることができ、あなたは一つのアカウントからアイテムを管理することができます。

Web保管庫から新しいBitwarden組織を作成するか、既存の組織の管理者に招待をSendするように要求することができます。

組織を作成するとき

組織を作成すると、組織の対称キーが暗号学的に安全な疑似ランダム数値ジェネレーター（CSPRNG）を使用して生成されます。この組織の対称キーは、組織が所有する保管庫のデータを復号化するために使用されます。したがって、組織のメンバーとデータを共有するには、それへのアクセスを安全に提供する必要があります。生の組甑対称キーは、Bitwardenサーバーには一切保存されません。

組織の対称キーが生成されるとすぐに、RSA-OAEPが使用されて組織の対称キーを組織の作成者のRSA公開キーで暗号化します。アカウント作成時には、組織のメンバーであるかどうかに関係なく、すべてのユーザーに対してRSAキーペアが生成されます。したがって、このキーは組織作成前にすでに存在します。

> ⓘ **Note**
> 以下に説明されている用途のRSAプライベートキーは、ユーザーのアカウント暗号化キーで暗号化されて保存されているため、ユーザーはそれにアクセスするために完全にログインしなければなりません。

この操作の結果得られる値は、保護された組織の対称キーと呼ばれ、Bitwardenのサーバーに送信されます。

組織の作成者、または組織のメンバーのいずれかがアカウントにログインすると、
クライアントアプリケーションは復号化されたRSA秘密鍵を使用して保護された組織の対称鍵を復号化し、結果として組織の対称鍵が得られます。
組織の対称キーを使用して、組电が所有する保管庫のデータはローカルで復号化されます。

ユーザーが組粤に参加するとき

後続のユーザーが組粤に参加するプロセスはかなり似ていますが、いくつかの違いはメモする価値があります。

まず、組織の確立されたメンバー、特に他のユーザーをオンボードする権限を持つ人が、ユーザーを組織に確認します。この確立されたメンバーは、
既にアカウントにログインし、前のセクションで説明された組粤データの復号化プロセスを経て、復号化された組織の対称キーにアクセスできます。

新しいユーザーが確認されると、既存のメンバーのクライアントはBitwardenサーバーに接続し、
アカウント作成時にBitwardenサーバーに保存されている新しいユーザーのRSA公開鍵を取得し、
それを使って復号化された組織の対称キーを暗号化します。これにより、新しい保護された組織の対称キーが生成され、
新しいメンバーのためにBitwardenサーバーに送信され、保存されます。

> **Note**
>
> 保護された各組織の対称キーはユーザーごとにユニークですが、特定のユーザーのRSA秘密キーで復号化すると、
> すべてが必要な組織の対称キーに復号化されます。

新しいユーザーがアカウントにログインすると、
クライアントアプリケーションは復号化されたRSA秘密鍵を使用して新しい保護された組織対称鍵を復号化し、結果として組織対称鍵が得られます。
組織の対称キーを使用して、組織が所有する保管庫のデータはローカルで復号化されます。

詳細を読む: 組織とは何ですか？

アクセスコントロールとBitwardenコレクションの管理

あなたの組織がBitwardenをより多く使用するにつれて、組織の保管庫内のすべてにアクセスすることなく、
コレクションを独立して管理できるユーザーがいると便利です。

コレクションとグループの管理は、Bitwardenの保管庫アイテムへのアクセスを分けたり、許可したり、制限したりする簡単な方法であり、
リソースのユーザー可視性を制御します。

Bitwardenヘルプセンターのユーザータイプとアクセス制御セクションに、役割とアクセス制御の完全なリストが記載されています。

詳細を読む: コレクションについて

イベントログ

イベントログには、組甑内で何が行われたか、または何が変更されたかについての時間印付きの詳細な情報が含まれています。これらのログは、
資格情報や設定の変更を調査するのに役立ち、監査証跡の調査やトラブルシューティングに非常に有用です。

イベントログに関する追加情報はBitwardenヘルプセンターに記載されています。イベントログは、チームとビジネスプランのみで利用可能です。

より多くのデータを収集するために、APIアクセスを持つプランはBitwarden APIを使用できます。APIのレスポンスには、
イベントのタイプと関連データが含まれます。

SIEM統合と外部システム

Splunkのようなセキュリティ情報およびイベント管理（SIEM）システムでは、Bitwardenからデータをエクスポートする際に、
APIとCLIからのデータの組み合わせがデータ収集に使用されるかもしれません。

このプロセスは、ヘルプセンターのメモで説明されています。**組織のイベントログ**という項目の下のSIEMと外部システムの統合にあります。

アカウント保護とロックアウトの回避

今日、基本、プレミアム、ファミリー、チームプランのために、
Bitwardenはパスワードや二段階ログインリカバリーコードを失うユーザーをサポートしないセキュリティモデルでアカウント保護を提供しています。

Bitwardenはユーザーのパスワードをリセットすることも、アカウントで有効にされている二段階ログインを無効にすることもできません。
ファミリーとチームのアカウントの所有者または管理者は、ユーザーのパスワードをリセットすることはできません。
エンタープライズプランに関する詳細は次のセクションをご覧ください。

> ⚠ **Warning**
> マスターパスワードを紛失したユーザーや、2ステップログインのリカバリーコードを紛失したユーザーは、
> アカウントを削除してからやり直す必要があります。

これらの潜在的な問題を軽減するために、Bitwardenはアカウント保護とロックアウト回避のための以下の推奨事項を提案します。

マスターパスワード
あなたがマスターパスワードを忘れた場合に保持し、回復できる方法を特定してください。これには、それを書き込み、
金庫や安全な場所に置くことが含まれるかもしれません。

マスターパスワードのヒントを使用してください。
役立つ場合は、サインアップ時にBitwardenから提供されたマスターパスワードのヒントを使用してください。
Web保管庫の設定でいつでもヒントを設定できます。

組織管理
組織には、組織にアクセスして管理できる複数の管理者が必要です。

2ステップログインリカバリーコード
あなたが二段階ログインを設定することを選択するか、または組織からそれを要求される場合、必ずリカバリーコードにアクセスし、
それをマスターパスワードと同じくらい安全な場所に保管してください。

エンタープライズプランにおけるアカウントの回復

2021年の中頃、Bitwardenはエンタープライズプランのためのアカウント回復を導入しました。このオプションを使用すると、
ユーザーと組織は新しいポリシーを実装する機会を持つことができ、
これにより管理者と所有者がユーザーのパスワードをリセットすることができます。

Bitwardenクラウドプラットフォームとウェブアプリケーションセキュリティ

Bitwardenアーキテクチャ概要

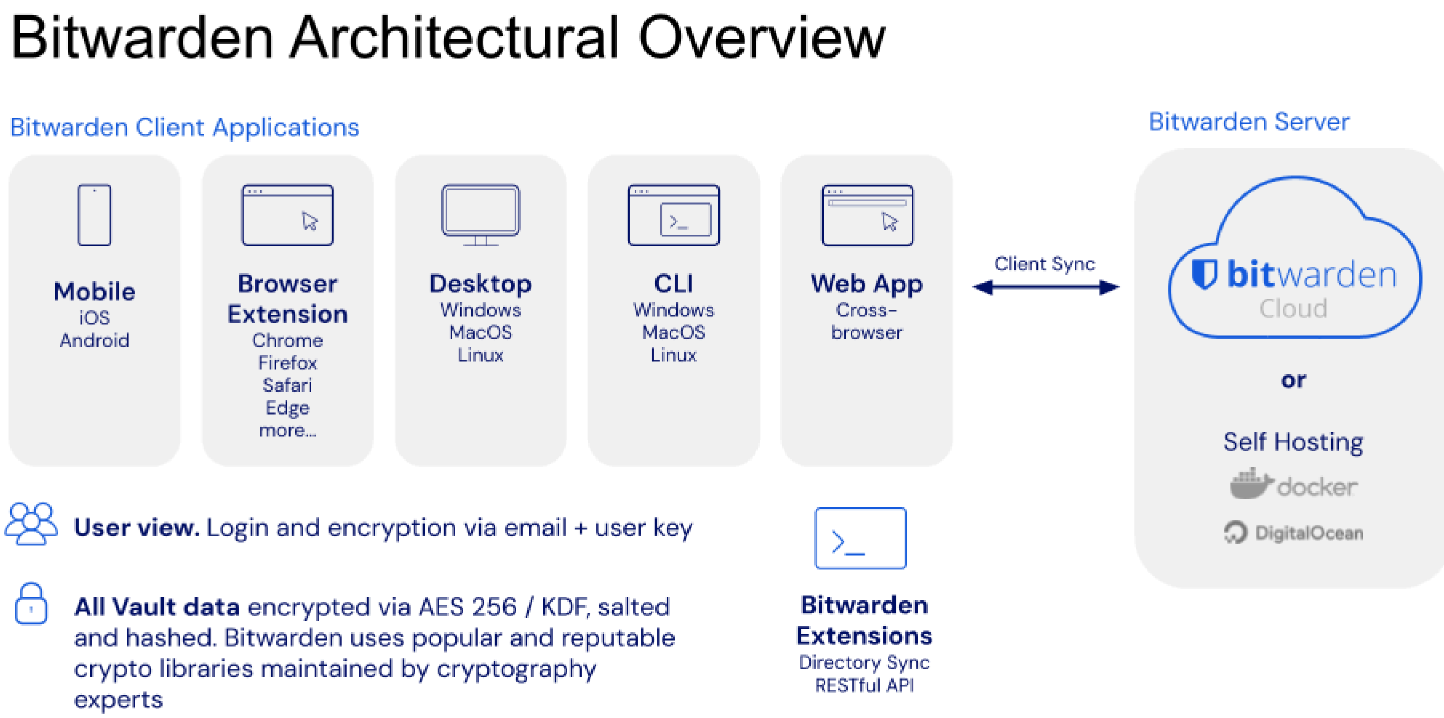
Bitwardenは、Microsoftのチームによって管理されているサービスを使用して、すべてのデータをMicrosoft
Azureクラウドで安全に処理および保存します。BitwardenはAzureが提供するサービスのみを使用しているため、
管理や維持を必要とするサーバーインフラストラクチャはありません。すべての稼働時間、スケーラビリティ、セキュリティの更新、パッチ、
および保証は、Microsoftとそのクラウドインフラストラクチャによってサポートされています。

セキュリティ更新とパッチ適用

Microsoftのチームは、物理サーバーとAzure App Serviceリソースを実行するゲスト仮想マシン（VM）の2つのレベルでOSパッチを管理します。
両方とも月に一度更新され、これは月に一度のMicrosoftのパッチ火曜日のスケジュールに合わせています。これらの更新は自動的に適用され、
Azureサービスの高可用性SLAを保証する方法で行われます。

詳細を読む: Azureアプリサービスのパッチ適用 または アプリサービスのSLA

更新がどのように適用されるかについての詳細な情報は、ここを読んでください



図：Bitwardenのアーキテクチャの概要

Bitwardenアクセスコントロール

Bitwardenの従業員は、彼らが設計、設計、実装、管理、サポート、そして対話するデータ、システム、情報資産のタイプに対して、顕著な訓練と専門知識を持っています。

Bitwardenは、適切なアクセスレベルが割り当てられ、維持されることを確認するために、確立されたオンボーディングプロセスに従います。Bitwardenは、各役割に適したアクセスレベルを設定しています。すべてのリクエスト、アクセス変更リクエストを含むものは、管理者によってレビューおよび承認される必要があります。Bitwardenは、従業員が職務を完了するために必要な最小限のアクセス権限を付与する最小特権ポリシーを採用しています。Bitwardenは、終了時にすべてのアクセス権を取り消すBitwarden人事を通じて確立されたオフボーディングプロセスに従います。

ソフトウェアライフサイクルと変更管理

Bitwardenは、リスクを最小限に抑えるためにプラットフォーム、アプリケーション、および生産インフラストラクチャへの変更を評価し、そのような変更はBitwardenの標準的な運用手順に従って実装されます。

変更リクエストのアイテムはロードマップに基づいて計画され、この時点でエンジニアリングに提出されます。エンジニアリングは、彼らの能力をレビューし評価し、各変更要求アイテムに対する努力のレベルを評価します。レビューと評価の後、彼らは特定のリリースのために何に取り組むかを策定します。CTOはコミュニケーションチャネルと管理会議を通じてリリースの詳細を提供し、そのリリースのための開発ライフサイクルが始まります。

高度な開発、リリース、テスト、承認プロセス：

- GitHubでプルリクエストを使用して開発、構築、反復処理を行う
- 機能をテスト可能な状態にまで進めてください。
- エンジニアリングは、開発や構築中の機能や製品の機能テストを実施します。

- ユニットテストビルドはBitwardenの継続的インテグレーション（CI）パイプラインの一部として自動化されています。
- 一部のテストもカスタマーサクセスチームによって実施されます
- エンジニアリング部門のディレクターはレビューを支援し、ドキュメンテーションの更新を含むプロセスの正式化を支援します。
- CTOが最終的な進行/中止の承認を提供します

会議出席：変更要求の成功的なレビュー、承認、実装、およびクロージャを確実にするために、
各コアオペレーションおよびITサービススタッフが変更要求をレビューし、議論するための会議に出席するべきです。

緊急デプロイメント/ホットフィックスは優先順位が上昇し、変更が行われる前にマネージャーやディレクターから変更のレビューと承認が得られ、
次に予定されている変更会議でレビュー、伝達、閉鎖が行われます。これは通常、サービス停止、システムダウン、
または緊急な停止防止の状況で発生します。

生産システムの制御

Bitwardenは、すべてのプロダクションシステムについて、デプロイメント、更新、
およびトラブルシューティングプロセスをカバーする文書化されたランブックを維持しています。問題が発生した場合に通知し、
エスカレートするために、広範なアラートが設定されています。

ベースライン設定

Bitwardenは、Microsoftのチームによって管理されているサービスを使用して、すべてのデータをMicrosoft
Azureクラウドで安全に処理および保存します。BitwardenはAzureが提供するサービスのみを使用しているため、
管理や維持が必要なサーバーインフラストラクチャはありません。すべての稼働時間、スケーラビリティ、およびセキュリティの更新と保証は、
Microsoftとそのクラウドインフラストラクチャによって支えられています。

Azureサービスの設定は、
Bitwardenによってアプリケーションが繰り返し一貫した方法で設定およびデプロイされることを保証するために利用されます。

Bitwardenプラットフォームキー管理手順

Bitwardenプラットフォーム自体が使用するキーとその他の秘密情報には、Bitwardenクラウドプロバイダーのアカウントの資格情報が含まれています。
すべてのそのようなキーは、業界標準の慣行に従って、生成され、安全に保管され、必要に応じてロテートされます。Bitwardenは、
Bitwardenプラットフォームで使用される敏感なキーまたは他の秘密の安全な保管とバックアップのために、内部のBitwarden保管庫を使用します。
Bitwardenの保管庫へのアクセス制御は、ユーザータイプとアクセス制御を活用します。

データタイプとデータ保持

Bitwardenは、Bitwardenサービスを提供するために2種類のユーザーデータを処理します：(i) 保管庫データ および (ii) 管理データ。

(i) 保管庫データ

保管庫のデータには、Bitwardenサービスへのアカウント内に保存されたすべての情報が含まれ、個人情報が含まれる場合があります。
もし私たちがあなたのためにBitwardenサービスをホストするなら、私たちは保管庫のデータをホストします。保管庫のデータは、
あなたの管理下にある安全な暗号化キーを使用して暗号化されています。Bitwardenは保管庫のデータにアクセスできません。

保管庫データのデータ保持：あなたはいつでも保管庫データを追加、修正、削除することができます。

(ii) 管理データ

Bitwardenは、アカウントの作成、Bitwardenサービスの使用とサポート、およびBitwardenサービスの支払いに関連して個人情報を取得します。
これには、Bitwardenサービスのユーザーの名前、メールアドレス、電話番号、その他の連絡先情報、
およびBitwardenサービスアカウント内のアイテムの数値（「管理データ」）が含まれます。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。あなたがBitwardenの顧客である限り、また法律で必要とされる限り、
私たちは管理データを保持します。Bitwardenとの関係を終了する場合、私たちはデータ保持ポリシーに従って、あなたの個人情報を削除します。

サイトを使用したり、私たちと（例えば、メールアドレスを通じて）コミュニケーションを取ったりすると、あなたは特定の個人情報を提供し、
Bitwardenはそれをコレクションします。

- お名前
- ビジネス名と住所
- ビジネス電話数値
- メールアドレス
- IPアドレスおよび他のオンライン識別子
- あなたが私たちに共有する許可を与えた任意の顧客の証言。
- あなたがサイトのインタラクティブエリアに提供する情報、例えば記入可能なフォームやテキストボックス、トレーニング、ウェビナーやイベントの登録など。
- あなたが使用しているデバイスに関する情報、それはハードウェアモデル、オペレーティングシステムとバージョン、ユニークなデバイス識別子、ネットワーク情報、IPアドレス、および/またはサイトとのやり取り時のBitwardenサービス情報を含みます。
- Bitwardenコミュニティやトレーニングと交流したり、試験やイベントに登録した場合、私たちはあなたの人物情報と共有した内容をコレクションすることがあります。
- クッキー、ピクセルタグ、ログ、またはその他の類似の技術を通じて収集された情報。

追加情報については、Bitwardenプライバシーポリシーをご参照ください。

ログ記録、監視、およびアラート通知

Bitwardenは、デプロイメント、更新、
およびトラブルシューティングのプロセスをカバーするすべてのプロダクションシステムのための文書化されたランブックを維持しています。
問題が発生した場合に通知し、エスカレートするために、広範なアラートが設定されています。
Bitwardenクラウドインフラストラクチャの手動および自動監視の組み合わせにより、システムの健康状態についての包括的で詳細な表示を提供し、
懸念のある領域に対する積極的なアラートを提供します。問題は迅速に浮上し、インフラストラクチャーチームが効果的に対応し、
最小限の混乱で問題を軽減できるようにします。

ビジネス継続性 / 災害復旧

Bitwardenは、Bitwardenクラウドに組み込まれたMicrosoft Azureからの完全な範囲の災害復旧とビジネス継続の実践を採用しています。これには、
アプリケーション層とデータベース層の高可用性とバックアップサービスが含まれます。

脅威防止と対応

Bitwardenは定期的に脆弱性評価を行います。私たちは、OWASP ZAP、Mozilla Observatory、
OpenVASなどのサードパーティーのツールや外部サービスを活用し、内部評価を行っています。

Bitwardenは、エッジでのWAFを提供し、より良いDDoS保護、分散を提供するためにCloudflareを使用します。
利用可能性とキャッシング。Bitwardenは、ネットワークセキュリティを向上させるために、Cloudflare内のプロキシも使用します。
そのサービスとサイトのパフォーマンス。

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。Bitwardenのソースコードは、
評判の良いサードパーティーのセキュリティ監査会社や独立したセキュリティ研究者によって監査されています。さらに、
Bitwardenの脆弱性開示プログラムは、HackerOneのハッカーコミュニティの協力を得て、Bitwardenをより安全にするためのものです。

監査可能性とコンプライアンス

Bitwardenのセキュリティとコンプライアンスプログラムは、ISO27001情報セキュリティ管理システム（ISMS）に基づいています。私たちは、
セキュリティポリシーとプロセスを管理するポリシーを定義し、提供するサービスに対する適用可能な法的、業界、規制要件に一致するように、
セキュリティプログラムを継続的に更新します。これらのサービスは、私たちのサービス利用規約の下で提供されます。

Bitwardenは、専用のセキュリティエンジニアリングチームを含む業界標準のアプリケーションセキュリティガイドラインに準拠しています。これには、
アプリケーションのソースコードとITインフラストラクチャの定期的なレビューが含まれ、セキュリティの脆弱性を検出、検証、修復します。

外部セキュリティレビュー
アプリケーションおよび/またはプラットフォームのサードパーティーによるセキュリティレビューと評価は、少なくとも年に一度実施されます。

認定資格
Bitwardenの認定には以下のものが含まれます：

- SOC2タイプII（毎年更新）
- SOC3（毎年更新）

AICPAによれば、SOC 2タイプIIレポートの使用は制限されています。SOC 2レポートのお問い合わせは、こちらからお問い合わせください。

詳細はこちら: BitwardenはSOC2認証を取得

SOC 3レポートは、公に配布できるSOC 2レポートの要約を提供します。AICPAによれば、SOC 3は一般使用のための信頼サービス基準に関するサービス組織のレポートのためのSOCです。Bitwardenは、私たちのSOC 3レポートのコピーをここで利用可能にしています。

これらのSOC認証は、お客様のセキュリティとプライバシーを保護し、厳格な基準を遵守するという私たちのコミットメントの一面を表しています。Bitwardenは、ネットワークセキュリティとコードの完全性に対する監査を定期的に実施しています。

詳細はこちら：Bitwarden 2020年のセキュリティ監査が完了しましたそしてBitwardenはサードパーティーのセキュリティ監査を完了しました

HTTPセキュリティヘッダー

Bitwardenは、Bitwardenウェブアプリケーションと通信の追加の保護レベルとしてHTTPセキュリティヘッダーを活用します。例えば、HTTP Strict Transport Security（HSTS）は、すべての接続がTLSを使用するように強制し、ダウングレード攻撃や誤設定のリスクを軽減します。コンテンツセキュリティポリシーヘッダーは、クロスサイトスクリプティング（XSS）などのインジェクション攻撃からさらなる保護を提供します。さらに、BitwardenはクリックジャッキングにX対抗するためにX-Frame-Options: SAMEORIGINを実装しています。

脅威モデルと攻撃面分析の概要

Bitwardenは、脅威モデリングと攻撃面分析を含むリスクベースのアプローチを採用して、安全なサービスとシステムを設計しています。これにより、脅威を特定し、それらに対する緩和策を開発します。リスクと脅威モデリング分析は、Bitwardenクラウドサーバーアプリケーションのコアから、モバイル、デスクトップ、ウェブアプリケーション、ブラウザ、および/またはコマンドラインインターフェイスなどのBitwardenクライアントまで、Bitwardenプラットフォームのすべての領域に広がります。

Bitwardenクライアント

ユーザーは主にモバイル、デスクトップ、ウェブアプリケーション、ブラウザ、および/またはコマンドラインインターフェイスなどのクライアントアプリケーションを通じてBitwardenと対話します。これらのデバイス、ワークステーション、およびウェブブラウザのセキュリティは重要です。なぜなら、これらのデバイスの1つ以上が侵害されると、攻撃者はキーロガーなどのマルウェアをインストールでき、これらのデバイスに入力されたすべての情報、パスワードや秘密を含む、をキャプチャする可能性があるからです。エンドユーザーおよび/またはデバイス所有者として、あなたのデバイスが安全で、不正なアクセスから保護されていることを確認する責任があります。

HTTPS TLSおよびWebブラウザのエンドツーエンド暗号化

BitwardenのWebクライアントはあなたのウェブブラウザで動作します。Bitwarden Webクライアントの認証性と完全性は、それが提供されるHTTPS TLS接続の完全性に依存しています。ウェブクライアントを配信するトラフィックを改ざんできる攻撃者は、ユーザーに悪意のあるクライアントを配信することができます。

ウェブブラウザの攻撃は、攻撃者やサイバー犯罪者がマルウェアを注入したり、ダメージを与えるための最も一般的な方法の一つです。ウェブブラウザに対する攻撃ベクトルには以下のものが含まれるかもしれません：

- **ソーシャルエンジニアリングの要素、例えばフィッシングなど、**
  被害者が自分のユーザーシークレットやアカウントのセキュリティを危険にさらす行動をとるようにだます、説得すること。
- **ウェブブラウザの攻撃とブラウザ拡張機能/アドオンのエクスプロイト：**
  キーボードでタイプされるユーザーの秘密をキャプチャできるように設計された悪意のある拡張機能。

- **ブラウザを介した Web アプリケーションへの攻撃:**クリックジャッキング、クロスサイト スクリプティング (XSS)、クロスサイト リクエスト フォージェリ (CSRF)。

Bitwardenは、Bitwardenウェブアプリケーションと通信の追加の保護レベルとしてHTTPセキュリティヘッダーを活用します。

コード評価

Bitwardenはオープンソースのパスワードマネージャーです。私たちの全ソースコードはGitHubにホストされ、公開されており、レビューのために利用可能です。Bitwardenのソースコードは、評判の良いサードパーティーのセキュリティ監査会社や独立したセキュリティ研究者によって、毎年監査されてきましたし、今後も監査が続けられます。さらに、Bitwardenの脆弱性開示プログラムは、HackerOneのハッカーコミュニティの協力を得て、Bitwardenをより安全にするためのものです。

もっと読む:

- BitwardenセキュリティFAQs
- Bitwarden 脅威防止と対応
- Bitwardenセキュリティとコンプライアンス評価、レビュー、脆弱性スキャン、ペンテスティング

結論

このBitwardenセキュリティとコンプライアンスプログラムの概要は、あなたのレビューのために提供されます。Bitwardenのソリューション、ソフトウェア、インフラストラクチャ、およびセキュリティプロセスは、多層的で防御的な深度アプローチを基に、最初から設計されています。

Bitwardenのセキュリティとコンプライアンスプログラムは、ISO27001情報セキュリティ管理システム（ISMS）に基づいています。私たちは、セキュリティポリシーとプロセスを管理するポリシーを定義し、提供するサービスに対する適用可能な法的、業界、規制要件に一致するように、セキュリティプログラムを継続的に更新します。これらのサービスは、私たちのサービス利用規約に基づいて提供されます。

何か質問があれば、どうぞお問い合わせください。