ビットワーデンのセキュリティとコンプライアンス

ビットワーデンは、誰もハッキングされない世界を構想している。これは、セキュリティ、プライバシー、国際基準の遵守に対するビットワーデンの確固たるコミットメントに反映されています。

Get the full interactive view at
https://bitwarden.com/ja-jp/compliance/

ビットワーデンのプライバシーと製品のセキュリティ

第三者監査
外部の専門家が定期的にBitwarden製品をレビューし、
強固で信頼できるセキュリティを確保しています。

ゼロ知識、エンドツーエンドの暗号化
強力な暗号化で保護されているため、Bitwardenでさえも、
誰もあなたの保管庫の情報にアクセスすることはできません！

プライバシーおよびセキュリティ基準に準拠
Bitwarden 製品は、業界のコンプライアンスに準拠し、社内の IT
チームとセキュリティチームによって迅速に承認されます。

オープンソースがもたらす信頼と透明性
オープンソースのコードベースにより、Bitwarden製品のセキュリティは、独立系セキュリティ研究者、著名なセキュリティ企業、Bitwardenコミュニティによって容易に監査されます。

信頼できるオープンソースアーキテクチャ
GitHub上のBitwardenコードベースは、
何百万人ものセキュリティ愛好家やアクティブなBitwardenコミュニティメンバーによって定期的にレビューされ、
監査されています。

ソースコード評価
Bitwardenは、コアアプリケーションとライブラリに加えて、ウェブ、ブラウザ拡張機能、
デスクトップを含む各クライアントのソースコード監査と侵入テストを毎年実施しています。

ネットワークセキュリティ評価
ビットワーデンでは、
信頼できるセキュリティ企業によるネットワークセキュリティ評価と侵入テストを毎年実施しています。

HackerOne バグ報奨金
独立したセキュリティ研究者は、
潜在的なセキュリティ問題を提出することで報酬を得ることができる。

データの保護
パスワードマネージャーおよびクレデンシャルセキュリティプロバイダーとして、Bitwardenは信頼できるセキュリティ対策と暗号化方法を利用してユーザーデータを保護します。

ゼロ知識、エンドツーエンドの暗号化
Bitwardenでは、
すべてのデータ保管庫のデータをエンドツーエンドで暗号化し、
マスターパスワードだけが解読できるようにしています。
ゼロナレッジアーキテクチャにより、
Bitwardenは保管庫内の暗号化されたデータを読み取る能力を持ちません。悪意

多要素暗号化
多要素暗号化は、
保存された情報を保護する追加の暗号化レイヤーです。
これにより、
たとえ暗号化されたデータ保管庫のデータにアクセスできたとしても顧客は保存された情報をより詳細に管理することができる。
ある行為者があなたのデータ保管庫に侵入することは事実上不可能となります。

セルフ・ホスティング・オプション
Bitwardenをお客様のプライベートネットワークまたはインフラ
管理するセルフホスティングオプションを選択できます。
セルフホスティングにより、

セキュリティ基準に準拠
Bitwardenは、SOC2およびSOC3の認証とHIPAAコンプライアンスにより、業界のセキュリティ基準を遵守しています。

SOC2とSOC3
システム・組織統制（SOC）は、組織のセキュリティ・
システムとポリシーを検証するために使用される一連の統制フレームワークです。
ビットワーデンはSOC2 Type
IIおよびSOC3の認証を受けています。

ご要望に応じてSOC2報告書をご提供いたします。

HIPAA
BitwardenはHIPAAに準拠しており、
HIPAAで構成されるルールに準拠するために第三者機関による監査を毎年受けています。

ISO 27001
BitwardenはISO 27001の認証を取得しており、
に関するISO
27001のコントロールセットを遵守しています。

個人情報保護コンプライアンス
Bitwardenは、ユーザーの個人データを保護し、世界中の主要なプライバシー基準に確実に準拠することを優先しています。

CCPA & CPRA
ビットワーデンは、カリフォルニア州消費者プライバシー法
（CCPA）およびカリフォルニア州プライバシー権法（CPRA）
に準拠しています。

一般データ保護規則
ビットワーデンは、GDPR、現行のEUデータ保護規則、
およびEU標準契約条項（SCC）に準拠しています。

Data Privacy Framework
ビットワーデンは、カリフォルニア州消費者プライバシー法
（CCPA）およびカリフォルニア州プライバシー権法（CPRA）
に準拠しています。

Bitwardenでセキュリティコンプライアンス基準を満たす
Bitwardenは単なるパスワード管理ツールではなく、主要なセキュリティ基準に対する業界のコンプライアンスを達成し、維持するための基盤となるツールです。安全な共有、監視機能、一元管理、
堅牢なデータ保護を通じて、Bitwardenはコンプライアンスニーズを満たすために組織のサイバーセキュリティ体制を強化します。

ISO 27001

国際規格であるISO27001は、データ管理を含む情報セキュリティマネジメントシステム（ISMS）を構築、維持、発展させるための基礎を定めたものです。

SOC 2

SOC 2（Service Organization Control 2）レポートは、アウトソーシング・ソリューション・プロバイダの顧客やビジネス・パートナーからしばしば要求されます。SOC 2準拠を目指す企業は、SOC 2準拠のパスワードマネージャを活用することで、要件を満たすことができます。

NERC

北米電気信頼性公社（NERC）は、米国、カナダ、メキシコの一部で何億人もの人々に電力を供給する電力網と電力系統に対するリスクを低減するための[redacted]

NIS2

NIS2は、EU全域のネットワークと情報システムを保護するための一連の要件である。この指令は、必要基準を設定する[redacted]に対し、サイバーセキュリティを強化し、法的義務を遵守するための適切な対策を実施することを義務付けている。

NIST サイバーセキュリティフレームワーク

米国国立標準技術研究所（NIST）は、企業、非営利団体、その他の民間機関がサイバーセキュリティのリスク管理を改善するのを支援するために、組織が従うべきガイダンスとベストプラクティスを提供している。

ソックス

サーベンス・オクスリー法（SOX法）のコンプライアンスには、財務報告の完全性を確保するために設計された一連のセキュリティ要件の遵守が含まれる。

パスワード管理成熟度モデル

このフレームワークは、組織が現在の業務に基づくパスワード・マネージャーの成熟度レベルを理解し、セキュリティを強化し、既存の分類を改善するために必要なステップを特定するのに役立ちます。

よくある質問

- **Bitwarden チームは私のパスワードを見ることができますか？**

  いや。

  お客様のデータは、**お客様の**ローカルデバイスを離れる前に完全に暗号化またはハッシュ化されるため、Bitwardenチームの誰もお客様の本当のデータを見たり、読んだり、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。データがどのように暗号化されるかについては、暗号化をご覧ください。

  さらに詳しく >

- **クラウドサーバーの安全性はどのように確保されていますか？**

  ビットワーデンは、ウェブサイト、アプリケーション、クラウドサーバーの安全性を確保するため、細心の注意を払っています。ビットワーデンは、サーバーのインフラとセキュリティを直接管理するのではなく、Microsoft Azureのマネージドサービスを使用しています。

  さらに詳しく >

- **ビットワルデンは監査を受けていますか？**

  ビットワーデンは、著名なセキュリティ会社と定期的に包括的な第三者セキュリティ監査を実施しています。これらの年次監査には、BitwardenのIP、サーバー、およびウェブアプリケーションにわたるソースコード評価と侵入テストが含まれます。

  さらに詳しく >

- **Bitwardenがハッキングされたらどうなりますか？**

  もし何らかの理由でBitwardenがハッキングされ、あなたのデータが流出してしまったとしても、あなたの保管データおよびマスターパスワードには強力な暗号化と一方向塩漬けハッシュ処理が施されているため、あなたの情報は保護されています。

  さらに詳しく >

- **私のデータはクラウドのどこに保存されていますか？**

  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、米国またはEUの Microsoft Azure Cloudですべての保管データを安全に処理し、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、サーバーインフラを管理・維持する必要がありません。すべてのアップタイム、スケーラビリティ、セキュリティアップデート、保証は、マイクロソフト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る。詳細については、Microsoft Azure Compliance Offeringsのドキュメントを参照してください。

  さらに詳しく >

- **なぜBitwardenにパスワードを任せる必要があるのですか？**

  私たちを信頼していただける理由はいくつかあります：

  1. Bitwardenは**オープンソースソフトウェア**です。私たちのソースコードはすべてGitHubにホストされており、誰でも自由に閲覧することができます。
     何千人も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。

  2. Bitwardenは、信頼できるサードパーティのセキュリティ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。

  3. **Bitwardenはお客様のパスワードを保存**しません。Bitwardenは、あなただけが解除できるパスワードの暗号化バージョンを保存します。お客様の機密情報は、
     当社のクラウドサーバーに送信される前に、お客様の個人デバイス上でローカルに暗号化されます。

  4. **ビットウォーデンには定評がある。**Bitwardenは何百万もの個人や企業に利用されています。疑わしいことや危険なことをすれば、私たちは廃業してしまうだろう！

  まだ我々を信用していないのか？その必要はない。オープンソースは美しい。Bitwardenスタック全体を自分で簡単にホストすることができます。自分のデータは自分で管理する。

  さらに詳しく >

- **Bitwardenはパスワードに塩漬けハッシュを使用しますか？**

  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、代替手段としてArgon2を選択することもできます。Bitwardenは、サーバーに送信する前に、
  お客様のマスターパスワードをお客様のEメールアドレスと一緒にローカルで **塩付けし、ハッシュ化** します。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、
  暗号的に安全なランダム値で再度塩付けされ、再度ハッシュ化され、データベースに保存されます。

  さらに詳しく >

- **Bitwardenのサーバーで、私のデータはどのように安全に送信され、保存されるのですか？**

  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、**常に**お客様のローカルデバイス上でデータを暗号化またはハッシュ化します。**Bitwardenのサーバーは、
  暗号化されたデータの保存にのみ使用されます。**詳細はストレージを参照。

  さらに詳しく >

- **どのような暗号化が使われているのか？**

  Bitwarden では、データ保管庫のデータをAES-CBC256 ビットで暗号化し、PBKDF2SHA-256 またはArgon2を使用して暗号鍵を導出します。

  さらに詳しく >

- **どのような情報が暗号化されるのか？**

  すべてのデータ保管庫のデータは、Bitwardenによって暗号化されて保存されます。その方法については、暗号化を参照。

  さらに詳しく >

- **私のデータは私のコンピュータ/デバイスのどこに保存されていますか？**

  あなたのコンピュータやデバイスに保存されているデータは暗号化され、あなたが保管庫のロックを解除したときにのみ復号化されます。復号化されたデータは**メモリーにのみ**保存され、
  永続記憶装置に書き込まれることはない。

  さらに詳しく >