Bitwardenのセルフホストパスワードマネージャー

Bitwarden Password Managerをセルフホストすることで、ビジネス認証情報とカスタムセキュリティポリシーを独自のサーバーで安全に管理できます。

完全なインタラクティブ表示をご覧ください
https://bitwarden.com/ja-jp/self-hosted-password-manager-on-premises/

bitwarden

独自のセキュリティ・モデルを適用する

Bitwardenのインストールをプロキシ、
ファイアウォール、
その他のセーフガードの背後に置き、
データのセキュリティを強化します。

バックアップと可用性の管理

DockerまたはKubernetesのコンテナベースのソリューション
既存の高可用性とリカバリ戦略に適合し、
確立された手順の範囲内に収まる。

ニーズに合わせてカスタマイズ

進化するニーズに対応する柔軟な環境変数で、
特定のコンプライアンス要件や内部データ残留ポリシーを

自宅、職場、外出先で信頼されるパスワード・マネージャー

クロスプラットフォームのアクセシビリティ＆無制限のデバイス

あなたの保管庫の重要なデータに、どの場所からでも、
どのブラウザからでも、
そして無制限のデバイスを通じてアクセスしてください。

Bitwardenをシームレスに統合

シングルサインオン（SSO）
IDプロバイダーやSCIMを含むディレクトリサービスなどの柔軟な統合オプションにより、
Bitwardenを既存の技術スタックにシームレスにプラグインします。

セキュリティ-監査-コンプライアンス

オープンソース、サードパーティーによる監査、
ゼロ知識、GDPR、プライバシーシールド、HIPAA、
およびCCPA規制に準拠しています

ディレクトリ同期

SCIMサポートまたはDirectory Connectorを使用して、
ユーザーとグループのプロビジョニングを効率化し、
ディレクトリサービスとの同期を維持します。

保管庫健康レポート

弱い、
再利用されたパスワードやその他の有用なセキュリティメトリクスを報告する洞察に富んだレポートにアクセスし

常時対応サポート

カスタマーサクセスエージェントは、
あなたを24時間体制でご

セルフ・ホスト型パスワード・マネージャーの利点

真のデータ主権

取締役会からの懸念であれ、顧客からの懸念であれ、
セルフホスティングでは真のデータ主権が現実のものとなる。

規制遵守

あなたの業界、サービス、製品に厳格なデータコンプライアンス要件がある場合、
セルフホスティングのBitwarden Password
Managerは大きなコンプライアンスボックスをチェックします。

カスタマイズ可能なセキュリティ

ニーズに合わせてセキュリティ設定を調整してください。
セルフホスト環境変数から製品内ポリシーまで、
組織のセキュリティのあらゆる側面をカスタマイズできます。

シームレスな統合

Windows、Linux、Docker、
またはKubernetesのインストールをサポートし、
既存のITインフラストラクチャと統合します。
セルフホスティングのBitwardenサーバーは、
モバイルやデスクトップアプリ、
ブラウザの拡張機能など、
すべてのエンドクライアントと互換性があります。
製品内で、アイデンティティ・プロバイダ、
ディレクトリ・サービスなどと統合できます！

監査およびコンプライアンス対応

詳細なイベントログは、
統合やAPIを通じてSIEMツールに取り込まれ、
ユーザーの行動を追跡し、
社内ポリシーや外部規制へのコンプライアンスを確保する
第三者監査結果、SOC2報告書、
およびアプリケーションに関するその他のコンプライアン
毎年公表され、更新される。

業界をリードするセキュリティとデータの完全管理を実現

Bitwarden Password Managerをセルフホストすることで、オンライン体験をより安全に、より速く、より楽しくすることができます。

よくあるご質問

その他のセルフホスティングに関するFAQはこちら

- セルフホスト型パスワード・マネージャーを使うメリットは何ですか？

  1. **真のデータ主権**：パスワードマネージャーをセルフホスティングすることで、データを完全に管理することができます。お客様はご自身のサーバーを管理し、機密性の高いパスワードや認証情報がお客様が管理するインフラに保存されるようにします。

  2. **セキュリティの強化**：セルフホスト・ソリューションでは、独自のセキュリティ・モデルを適用できる。パスワード管理のインストールをプロキシやファイアウォールの背後に置き、さらに保護する。

  3. **カスタマイズ**：セルフホスティングのパスワードマネージャは、柔軟な環境変数を提供することが多く、特定のニーズやコンプライアンス要件に合わせて設定をカスタマイズすることができます。

  4. **オープンソースの利点**：信頼性と透明性は、どのパスワード・マネージャーをセルフ・ホストするか選択する際に不可欠である。Bitwardenはオープンソースのパスワードマネージャーであるため、セキュリティ対策は自己検証可能であり、コードのすべての行は、世界中の何千人ものセキュリティ専門家や愛好家によって定期的に検査されています。

  5. **規制コンプライアンス**：セルフホスティングは、データレジデンシーとアクセスを完全にコントロールできるため、さまざまな業界の厳しいデータコンプライアンス要件を満たすのに役立ちます。

  6. **既存システムとの統合**：セルフホスト・ソリューションは、多くの場合、ディレクトリ・サービスやIDプロバイダーなど、現在のITインフラとのシームレスな統合をサポートしています。

  7. **監査準備**：内部監査やコンプライアンス維持のために重要な、ユーザーアクティビティ追跡のための詳細なイベントログにアクセスできます。

- どのプラットフォームでホスティングできますか？

  Bitwardenクライアントはクロスプラットフォームであり、サーバーはWindows、Linux上のDockerコンテナ、またはHelmチャートを使用してKubernetesにデプロイできる。

  Windows上のDocker Desktopは、あなたの会社がDockerのライセンス要件を満たしているかどうかによってライセンスが必要になる場合があるが、Linux上のDockerは無料である。

  Dockerとコンテナ技術の詳細については、Dockerのウェブサイトで読むことができる。

- BitwardenをAWS、Azure、GCP、またはVMware vCenterにデプロイするにはどうすればよいですか？

  Bitwardenのヘルプドキュメントには、Dockerインストールをデプロイするための詳細なガイドがあります。AWSのEKS、OpenShift、AzureのAKSにHelmを使ってインストールする手順もあります。以下は、あなたが始めるのに役立つお勧めのリソースです：

  - Dockerデプロイメントガイド
  - Helm 配備ガイド
  - Bitwarden組織をセルフホストする方法

- **自分のサーバーにオープンソースのパスワード・マネージャーをセットアップするには？**

  自分のサーバーにオープンソースのパスワード・マネージャーをセットアップするには、通常、次の手順を踏む。

  1. **サーバーの準備**サーバーまたは仮想マシンを用意してください。これはオンプレミスのハードウェアであったり、クラウドベースのサーバーであったりする。
  2. **導入方法を選択する**：多くのセルフホストパスワードマネージャーは、複数のインストールオプションを提供しています。一般的なものは以下の通り：
     - Dockerコンテナ
     - Kubernetesのデプロイメント
  3. **インストール**様々なデプロイメントタイプのBitwardenセルフホストに関する詳細なドキュメントをご覧ください。
  4. **設定**：環境変数を設定し、セキュリティ要件や組織のニーズに合わせて設定を調整する。
  5. **ユーザー管理**：管理者アカウントを設定し、ユーザーのアクセス権を設定します。
  6. **クライアントのセットアップ**：ブラウザー拡張機能、デスクトップアプリ、モバイルアプリをユーザーにインストールし、セルフホスティングサーバーに接続できるように設定します。
  7. **テスト**：パスワードジェネレーター、安全な共有、多要素認証などの機能を含め、インストールを徹底的にテストする。
  8. **メンテナンス計画**：定期的なバックアップ、アップデート、セキュリティ監査の手順を確立し、セルフホスト型パスワード・マネージャを安全かつ最新の状態に保ちましょう。

  セルフホスティングには多くの利点がある一方で、継続的なメンテナンスとセキュリティへの警戒も必要であることを忘れてはならない。セルフホスト・ソリューションを効果的に管理するためのリソースと専門知識を確保してください。