

管理者コンソール > 組織の基本

エンタープライズポリシー

ヘルプセンターで表示:

<https://bitwarden.com/help/policies/>

エンタープライズポリシー

エンタープライズのポリシーは何ですか？

エンタープライズのポリシーは、エンタープライズ組織がすべてのユーザーに対してセキュリティルールを強制することを可能にします。例えば、二段階ログインの使用を義務付けることができます。

エンタープライズのポリシーは、組織の管理者または所有者によって設定することができます。

⚠ Warning

ユーザーを組織に招待する前に、エンタープライズのポリシーを設定することをお勧めします。一部のポリシーは、有効にすると非準拠のユーザーを削除しますが、一部は遡及的に適用できません。

エンタープライズのポリシーを設定する

ポリシーは、**設定** → **ポリシー**に移動して管理者コンソールから設定できます。

The screenshot shows the Bitwarden Admin Console interface. On the left is a sidebar with navigation options: My Organization, Collections, Members, Groups, Reporting, Billing, Settings, Organization info, Policies (highlighted), Two-step login, and Import data. The main content area is titled 'Policies' and lists several policy categories with their descriptions: 'Require two-step login' (Require members to set up two-step login), 'Master password requirements' (Set requirements for master password strength), 'Account recovery administration' (Based on the encryption method, recover accounts when master passwords or trusted devices are forgotten or lost), 'Password generator' (Set requirements for password generator), 'Single organization' (Restrict members from joining other organizations), and 'Require single sign-on authentication' (Require members to log in with the Enterprise single sign-on method). In the top right corner, there is a hamburger menu icon and a red circular button with 'FR' inside.

[ポリシーを設定する](#)

利用可能なポリシー

2段階認証が必要です

二段階ログインを必要とするポリシーをオンにすると、メンバーは保管庫にアクセスするために任意の二段階ログイン方法を使用する必要があります。SSOまたはIDプロバイダーの二要素認証機能を使用している場合、このポリシーを有効にする必要はありません。このポリシーは、あなたの組織への受け入れられた招待だけを持つユーザーに対しても適用されます。

⚠ Warning

所有者や管理者でなく、アカウントに二段階ログイン設定をしていない組織のメンバーは、このポリシーを有効にすると組織から削除されます。このポリシーの結果として削除されたユーザーは、メールアドレスで通知され、組織に再度招待されなければなりません。追加情報:

- 既存のユーザーは、保管庫の二段階ログインがオンになるまで、所有者や管理者への招待を含む招待を受け入れることができません。
- 新規ユーザーは自動的にメールアドレスを基にした二段階ログインが設定されますが、これはいつでも変更可能です。

マスターパスワードの要件

マスターパスワード要件ポリシーをオンにすると、ユーザーのマスターパスワードの強度に対する最小要件の設定可能なセットが強制されます。組織は以下を強制することができます:

- マスターパスワードの最小複雑性
- マスターパスワードの最小長さ
- 必要なキャラクターのタイプ

パスワードの複雑さは、0 (弱) から4 (強) のスケールで計算されます。Bitwardenはzxcvbnライブラリを使用してパスワードの複雑さを計算します。

既存のメンバーにパスワードの変更を要求するオプションを使用して、役割に関係なく、既存の非準拠組織メンバーに対して、次のログイン時にマスターパスワードを更新するよう要求します。組織からの招待で新しいアカウントを作成するユーザーは、あなたの要件を満たすマスターパスワードを作成するよう求められます。

アカウント回復の管理

アカウント回復管理ポリシーをオンにすると、所有者と管理者はパスワードリセットを使用して、登録ユーザーのマスターパスワードをリセットすることができます。デフォルトでは、ユーザーはパスワードリセットに自己登録する必要がありますが、自動登録オプションを使用して招待されたユーザーの自動登録を強制することができます。

あなたの組織が信頼できるデバイスでのSSOを使用するためには、アカウント回復管理ポリシーが必要です。

① Note

このポリシーを有効にする前に、単一組電のポリシーを有効にする必要があります。

その結果、アカウント回復管理ポリシーをオフにする前に、単一組織ポリシーをオフにする必要があります。

自動登録

自動登録オプションをオンにすると、新しいメンバーは役割に関係なく、パスワードリセットに自動的に登録され、組織への招待が承認されたときに退会することが防止されます。

① Note

組織内の既存のユーザーは、パスワードリセットには後から登録されず、自己登録が必要となります。

パスワード生成ツール

パスワードジェネレーターのポリシーをオンにすると、役割に関係なく、すべてのメンバーのユーザーが生成したパスワードに対して、設定可能な最小要件のセットが強制されます。組織は以下を強制することができます：

- パスワード、パスフレーズ、またはユーザーの設定

パスワードについて：

- パスワードの最低文字数
- 最小数値（0-9）の数
- 最小特殊文字（!@#\$\$%^&*）数
- 必要なキャラクターのタイプ

パスフレーズのために：

- 文字の最小数
- 大文字を使うかどうか
- 数値を含めるかどうか

⚠ Warning

このポリシーがオンになったとき、既存の非準拠パスワードは変更されませんし、アイテムも組織から削除されません。このポリシーがオンになった後でパスワードを変更または生成すると、設定されたポリシーのルールが適用されます。

バナーがパスワードジェネレーター画面に表示され、ポリシーがユーザーのジェネレーター設定に影響を与えていることを示します。

単一組織

単一組織ポリシーをオンにすると、組織の非所有者/非管理者メンバーは他の組織に参加したり、他の組織を作成したりすることが制限されます。このポリシーは、あなたの組織への招待を受け入れたユーザーに対しても適用されますが、所有者と管理者に対してはこのポリシーは適用されません。

⚠ Warning

このポリシーをオンにすると、複数の組織のメンバーである組織のユーザーは、あなたの組織から削除されます。

このポリシーの結果として削除されたユーザーは、メールアドレスで通知され、組織に再度招待されなければなりません。ユーザーは、他のすべての組織から自分自身を削除するまで、組織への招待を受け入れることができません。

シングルサインオン認証

シングルサインオン認証を必要とするポリシーをオンにすると、所有者/管理者でないユーザーはSSOでログインする必要があります。自己ホスト型である場合、環境変数を使用して、所有者と管理者に対してこのポリシーを強制することができます。詳細については、SSOを使用したログインの使用をご覧ください。このポリシーは、所有者と管理者には適用されません。

このポリシーを使用している組織のメンバーは、パスキーでログインすることができません。

① Note

この**単一の組織**のポリシーは、このポリシーを有効にする前にオンにしなければなりません。

その結果、**単一組織**のポリシーをオフにする前に、**シングルサインオン認証を必要とする**ポリシーをオフにする必要があります。

個別の保管庫を削除

個々の保管庫を削除ポリシーをオンにすると、非所有者/非管理者ユーザーは、組織のメンバーに対する保管庫アイテムの所有権を防ぐことで、保管庫アイテムを組織に保存する必要があります。

ユーザーには、**アイテムを追加**画面にバナーが表示され、ポリシーが所有権オプションに影響を与えていることを示しています。

このポリシーは、あなたの組織への招待を受け入れたユーザーに対しても適用されますが、所有者と管理者に対してはこのポリシーは適用されません。

① Note

このポリシーの実施前または組織への参加前に作成された保管庫のアイテムは、ユーザーの個々の保管庫に残ります。

Send を無効化

Sendの削除ポリシーをオンにすると、所有者/管理者でないメンバーはBitwarden **Send**を使用してSendを作成または編集することができなくなります。このポリシーの対象となるメンバーは、まだ削除日に達していない既存のSendを削除することができます。このポリシーは、所有者と管理者には適用されません。

ユーザーには、ポリシーがSendの削除のみに制限していることを示すために、**Send**表示および既存のSendを開く際にバナーが表示されます。

送信オプション

Sendオプションポリシーをオンにすると、所有者と管理者はSendの作成と編集のオプションを指定できます。このポリシーは、所有者と管理者には適用されません。オプションには以下のものがあります：

オプション

ユーザーがメールアドレスを隠すのを許可しないでください。

説明

このオプションをオンにすると、**メールアドレスを隠すオプション**が削除され、すべての受信したSendが誰から送られたかが含まれます。

保管庫のタイムアウト

保管庫のタイムアウトポリシーを設定することで、以下のことが可能になります：

- あなたの組織の全メンバーに対して最大の**保管庫タイムアウト**期間を実装してください**所有者を除く**。このオプションは、すべてのクライアントアプリケーション（モバイル、デスクトップ、ブラウザの拡張機能など）にタイムアウト制限を適用します。

- あなたの組の全メンバーに対して保管庫タイムアウトアクションを設定してください**所有者を除く**。このオプションは、保管庫のタイムアウトが発生したときに、**ユーザー設定**、**ロック**、または**ログアウト**に設定することができます。

ログアウトオプションは、例えば、ユーザーが保管庫にアクセスするたびに二要素認証を使用するように促すためや、定期的にユーザーのマシンからローカルデータをクリアしてオフライン使用を防ぐために使用できます。

ユーザーが保管庫のタイムアウト設定中に、ポリシーが彼らのオプションに影響を与えていることを示すバナーが表示されます。このポリシーが有効化されると、**ブラウザの再起動時や決して**などの一部の保管庫タイムアウトオプションはユーザーに利用できなくなります。このポリシーは、所有者と管理者には適用されません。

① Note

このポリシーを有効にする前に、**単一組電**のポリシーを有効にする必要があります。

その結果、**単一組織**のポリシーをオフにする前に、**保管庫タイムアウト**のポリシーをオフにする必要があります。

個別の保管庫のエクスポートを削除

個々の保管庫エクスポートを削除するポリシーをオンにすると、組織の非所有者/非管理者メンバーは**自分の個々の保管庫データをエクスポート**することが禁止されます。このポリシーは、所有者と管理者には適用されません。

ウェブ保管庫とCLIでは、ポリシーがユーザーのオプションに影響を与えていることを示すメッセージがユーザーに表示されます。他のクライアントでは、そのオプションは単純に無効になります。

自動入力を有効にする

自動入力を有効にするポリシーをオンにすると、組織のすべての既存のメンバーと新しいメンバーに対して、ブラウザの拡張機能上で**ページ読み込み時の自動入力機能**が自動的にオンになります。メンバーは、自分のブラウザ拡張機能のページロード時の自動入力をオフにしたり、変更したりすることができます。