

管理者コンソール > SSOでログイン

# メンバー復号化オプション

ヘルプセンターで表示:

<https://bitwarden.com/help/sso-decryption-options/>

## メンバー復号化オプション

SSOでのログインがユニークなのは、私たちのゼロ知識暗号化モデルを保持しているからです。

Bitwardenの誰もがあなたの保管庫データにアクセスすることはできませんし、同様に、

**あなたのIDプロバイダーもそうすべきではありません。** だからこそ、SSOでのログインは**認証と復号化を分離**します。

すべてのSSOでのログイン実装において、

あなたのIDプロバイダーは保管庫のデータを復号化するために必要な復号化キーにアクセスすることはできませんし、そうすることはありません。

**メンバー復号化オプションは**、SSOが認証を処理するシナリオでボールド

データの復号化にどの復号化キーが使用されるかを決定するために使用されます。オプションには以下のものがあります：

- **マスターパスワード**: 認証されると、組織メンバーは**マスターパスワード**を使用してボールドデータを復号化します。
- **信頼できるデバイス**：ユーザーがSSOで認証し、デバイスに保存された暗号化キーを使用して保管庫を復号化することを可能にします。これにより、マスターパスワードを入力する必要がなくなります。[もっと学ぶ](#)
- **キーコネクタ**: SSOを使用してログインをセルフホスト型の復号キーサーバーに接続します。このオプションを使用すると、組織のメンバーは保管庫のデータを復号化するためにマスターパスワードを使用する必要がありません。代わりに、**キーコネクタ**は、あなたが所有し管理しているデータベースに安全に保存された復号化キーを取得します。

### Tip

Due to the sensitivity of storing decryption keys, the **Key Connector** option is disabled by default and currently only available to organizations self-hosting Bitwarden.

If you're interesting in using Key Connector, check out the [About Key Connector](#) and [Deploy Key Connector](#) articles and [contact us](#) to setup a time for us to help you get started.