bitwarden | ヘルプセンターの記事

管理者コンソール > レポート

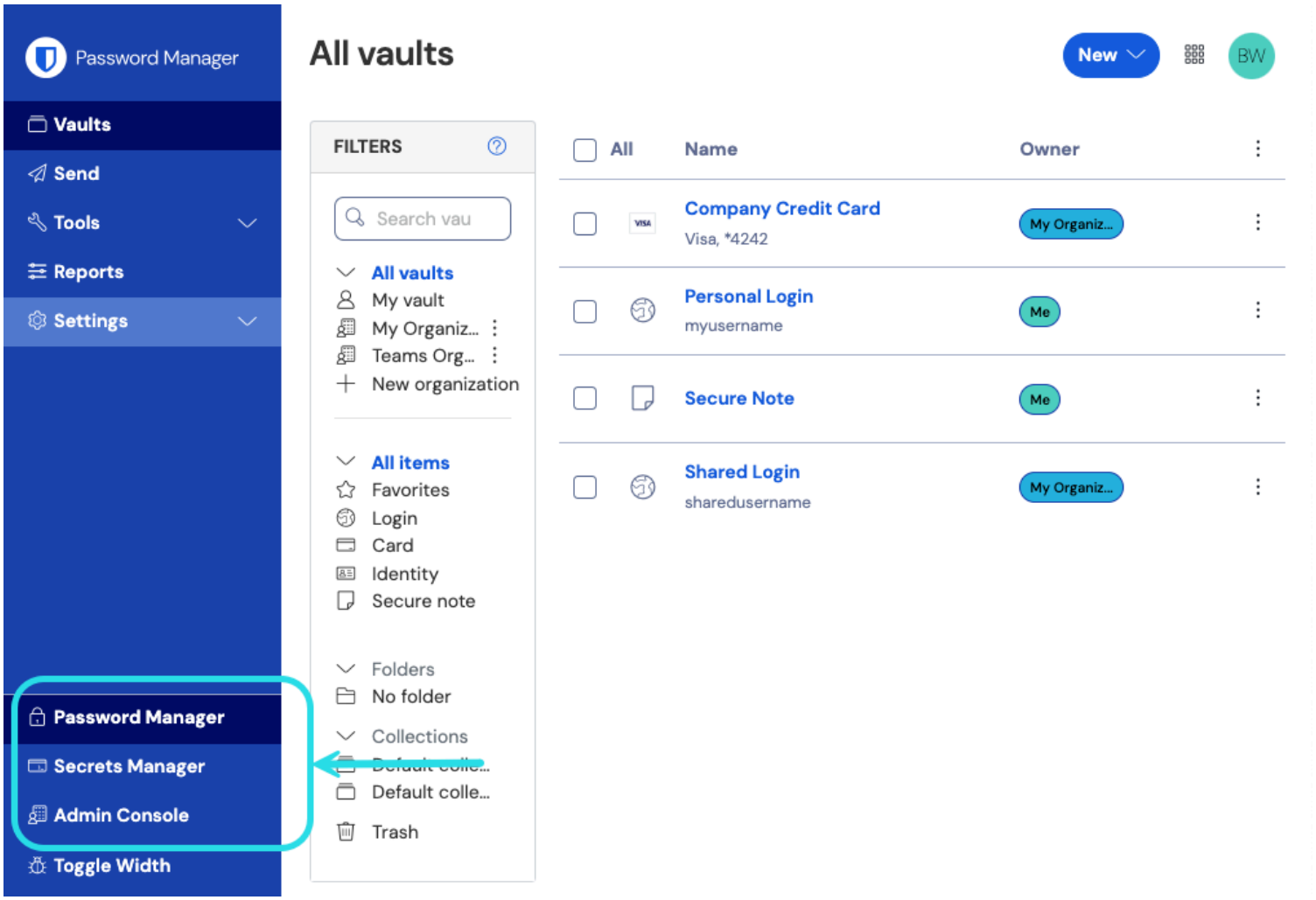
イベントログ

ヘルプセンターで表示:
https://bitwarden.com/help/event-logs/

イベントログ

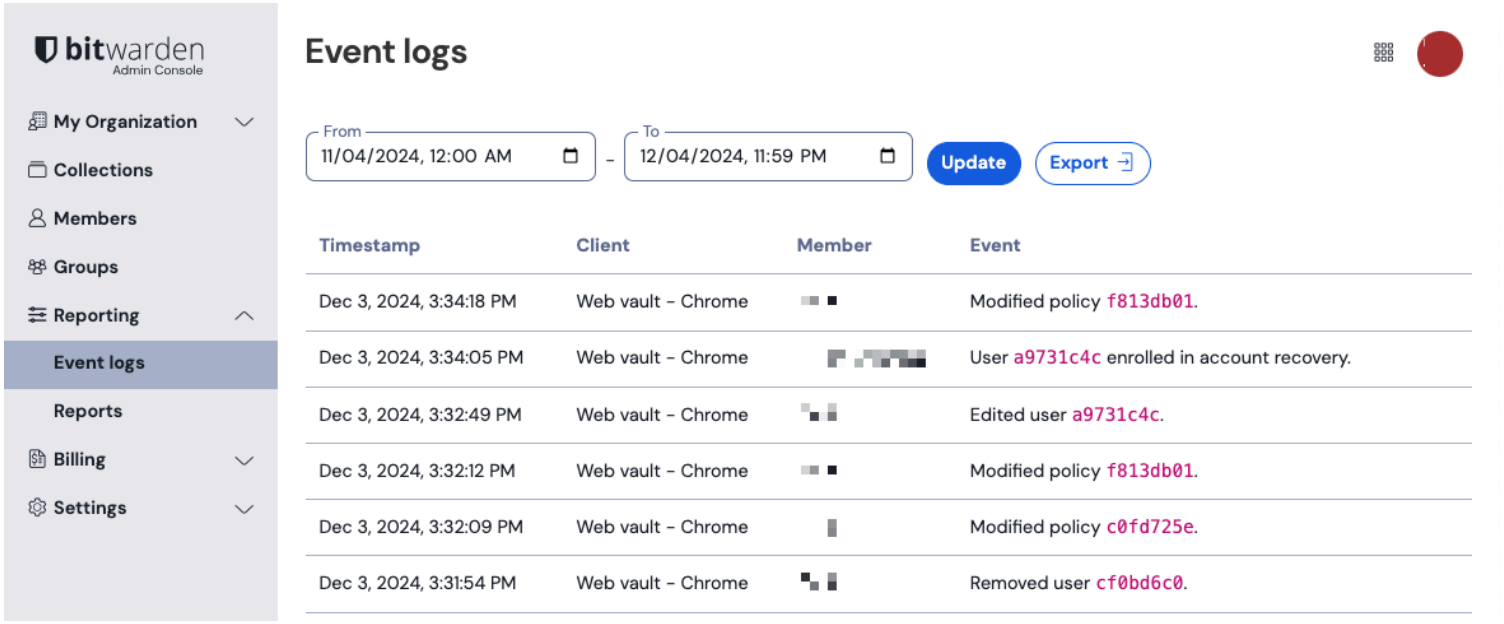
イベントログは、あなたのチームやエンタープライズ組織内で発生するイベントのタイムスタンプ付きレコードです。
イベントログにアクセスするには：

1. Bitwardenウェブアプリにログインし、製品スイッチャー（⊞）を使用して管理者コンソールを開きます。



製品-スイッチャー

2. ナビゲーションから**レポート** → **イベントログ**を選択してください。



イベントログ

イベントログはエクスポート可能で、Bitwarden公開APIの/eventsエンドポイントからアクセス可能であり、無期限に保持されますが、一度に表示できるデータは367日分まで（範囲セレクタによって決定されます）。

ほとんどのイベントは、各種Bitwardenクライアントで行われたアクションをキャプチャし、
イベントデータを60秒ごとにサーバーにプッシュしますので、最近のイベントのレポートにはわずかな遅延が生じることがあります。

イベントを調査する

ウェブアプリの**イベントログ**表示で、ピンクのリソース識別子（例：`1e685004`）を選択すると、2つのことが行われます：

1. そのリソースに関連するイベントのリストを含むダイアログボックスを開きます。例えば、アイテムの識別子を選択すると、そのアイテムが編集された回数、表示された回数など、各アクションを実行したメンバーを含むリストが開きます。

2. リソースにアクセスする表示に移動します。例えば、**イベントログ**からメンバーの識別子を選択すると、自動的にそのメンバーに絞り込まれたリストを**メンバー**表示で見ることができます。

イベントリスト

イベントログは50以上の異なるタイプのイベントを記録します。イベントログ画面は、イベントの**タイムスタンプ**、クライアントアプリの情報（アプリケーションタイプとIP（🌐地球のアイコンにカーソルを合わせることでアクセス可能））、イベントに接続した**ユーザー**、そして**イベント**の説明をキャプチャします。

> **ⓘ Note**
>
> 各**イベント**は、イベントがキャプチャしたアクションを識別するタイプコード（`1000`、`1001`など）と関連付けられています。タイプコードは、イベントによって文書化されたアクションを識別するために、Bitwarden公開APIによって使用されます。

すべてのイベントタイプが以下にリストされており、それぞれのタイプコードとともに表示されています：

ユーザーイベント

- ログインしました。(`1000`)

- アカウントのパスワードを変更しました。(1001)
- 二段階ログインを有効化/更新しました。(1002)
- 二段階ログインを無効にしました。(1003)
- 二段階ログインからアカウントを回復しました。(1004)
- パスワードが間違っているため、ログインの試みが失敗しました。(1005)
- 二段階ログインが間違っているため、ログイン試行が失敗しました。(1006)
- ユーザーは個々の保管庫アイテムをエクスポートしました。(1007)
- ユーザーは、アカウント回復を通じて発行されたパスワードを更新しました。(1008)
- ユーザーは、キーコネクターを使用して復号化キーを移行しました。(1009)
- ユーザーはデバイスの承認を要求しました。(1010)

アイテムイベント

- 作成されたアイテム *item-identifier*。(1100)
- 編集されたアイテム *item-identifier*。(1101)
- 永久に削除されたアイテム*item-identifier*。(1102)
- アイテム*item-identifier*の添付ファイルを作成しました。(1103)
- アイテム*item-identifier*の添付ファイルを削除しました。(1104)
- アイテム*item-identifier* を組織に移動しました。(1105)
- アイテム*item-identifier*（1106）のコレクションを編集しました。
- 表示されたアイテム *item-identifier*。(1107)
- アイテム*item-identifier*のパスワードを表示しました。(1108)
- アイテム*item-identifier*の隠されたフィールドを表示しました。(1109)
- アイテム*item-identifier*のセキュリティコードを表示しました。(1110)
- アイテム*item-identifier*のパスワードをコピーしました。(1111)
- アイテム*item-identifier*のための隠されたフィールドをコピーしました。(1112)
- アイテム*item-identifier*のセキュリティコードをコピーしました。(1113)
- 自動入力されたアイテム *item-identifier*。(1114)
- アイテム*item-identifier*をゴミ箱に送りました。(1115)

- 復元されたアイテム *item-identifier*。(1116)
- アイテム*item-identifier*のカード数値を表示しました。(1117)

コレクションイベント

- コレクション*collection-identifier*を作成しました。(1300)
- 編集コレクション *collection-identifier*. (1301)
- 削除されたコレクション *collection-identifier*。(1302)

グループイベント

- グループ*group-identifier*を作成しました。(1400)
- 編集されたグループ *group-identifier*。(1401)
- 削除されたグループ *group-identifier*。(1402)

組織のイベント

- 招待されたユーザー *user-identifier*。(1500)
- 確認されたユーザー *user-identifier*。(1501)
- 編集されたユーザー *user-identifier*。(1502)
- ユーザー*user-identifier*を削除しました。(1503)
- ユーザー*user-identifier*のための編集されたグループ。(1504)
- ユーザー*user-identifier*のSSOリンクを解除しました。(1505)
- *ユーザー識別子*はアカウントの回復に登録しました。(1506)
- *ユーザー識別子*はアカウントの回復から撤退しました。(1507)
- *user-identifier*のマスターパスワードリセット。(1508)
- ユーザー*user-identifier*のSSOリンクをリセットします。(1509)
- *ユーザー識別子*は、初めてSSOを使用してログインしました。(1510)
- *ユーザー識別子*(1511)の組織アクセスを取り消しました
- *ユーザー識別子*（1512）の組織アクセスを復元します
- *ユーザー識別子*のための承認済みデバイス。(1513)
- *ユーザー識別子*のデバイスが拒否されました。(1514)
- 組織の設定を編集しました。(1600)

- 組織の保管庫をパージしました。(1601)
- エクスポートされた組織の保管庫。(1602)
- 管理プロバイダーによる組織の保管庫へのアクセス。(1603)
- 組織はSSOを有効にしました。(1604)
- 組織はSSOを無効にしました。(1605)
- 組織が有効にしたキー コネクタ。 (1606)
- 組織はキーコネクターを無効にしました。(1607)
- ファミリースポンサーシップが同期されました。(1608)
- 修正されたポリシー *policy-identifier*。(1700)
- ドメイン *ドメイン名*を追加しました。(2000)
- ドメイン *ドメイン名*を削除しました。(2001)
- *ドメイン名*が確認されました。(2002年)
- *ドメイン名*が確認されていません。(2003)

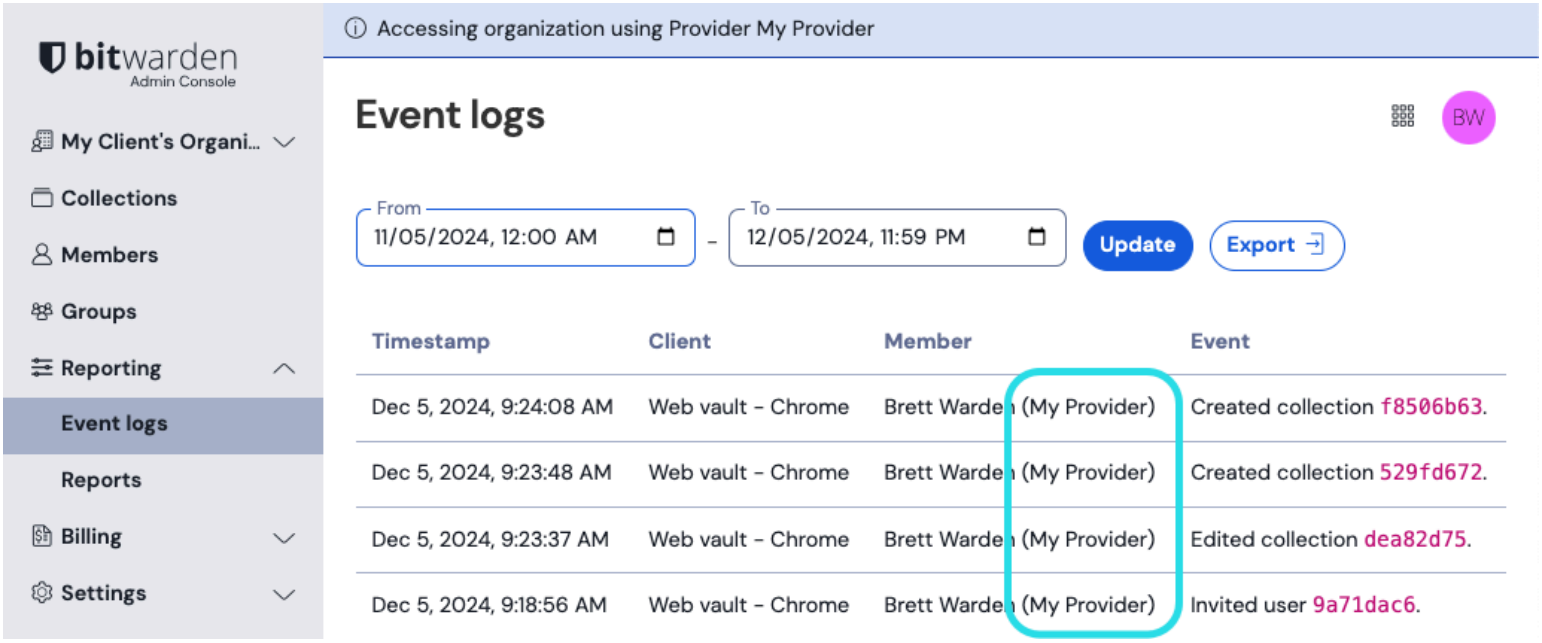
シークレットマネージャーのイベント

シークレットマネージャーのイベントは、組織の保管庫の**レポート**タブと、
サービスアカウントのイベントログページの両方から利用できます。次のシークレットマネージャーのイベントがキャプチャされます：

- シークレット*secret-identifier*にアクセスしました。(2100)

プロバイダーイベント

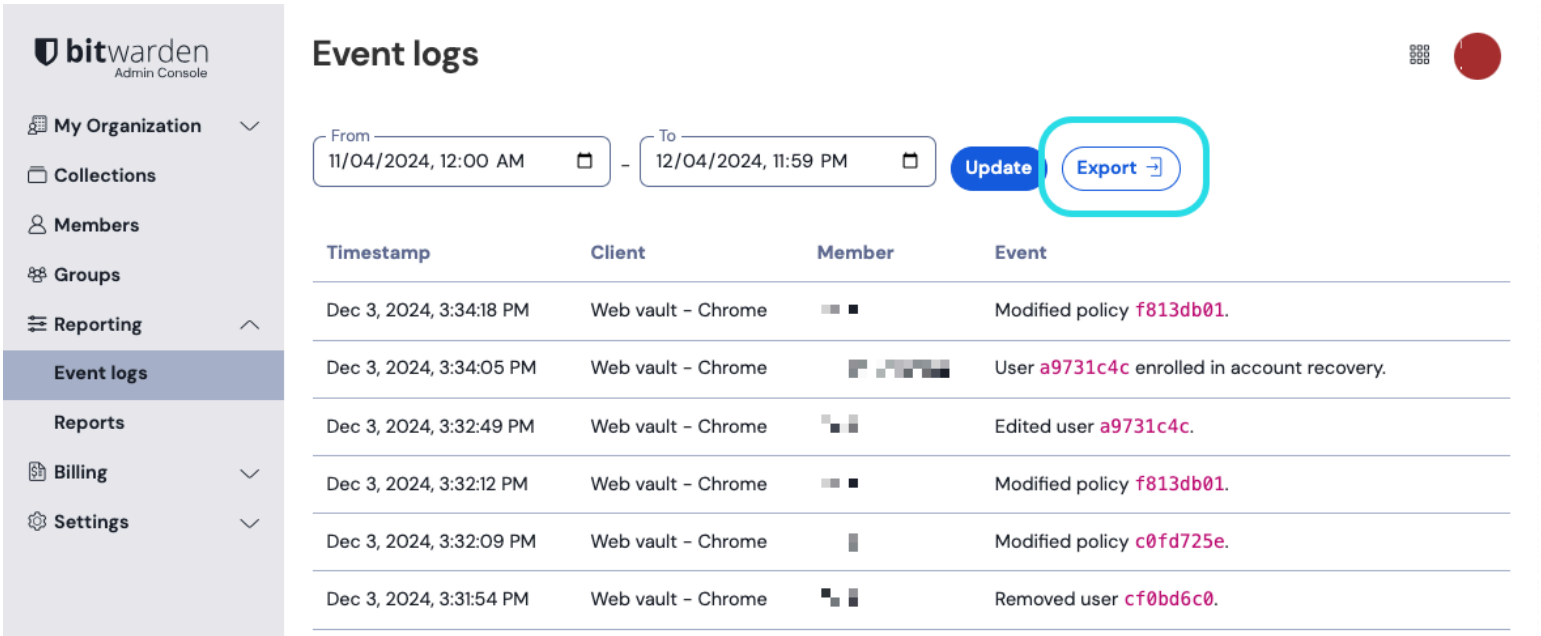
上記のイベントが管理プロバイダーのメンバーによって実行されると、**ユーザー**列にはプロバイダーの名前が記録されます。さらに、
管理プロバイダーのメンバーがあなたの組織の保管庫にアクセスするたびに、プロバイダー固有のイベントが記録されます。



プロバイダーがイベントにアクセスする

エクスポートイベント

指定された日付範囲内のすべてのイベントを含む`.csv`を作成するためにイベントログをエクスポートします。



イベントログのエクスポート

例えば：

```Bash
message,appIcon,appName,userId,userName,userEmail,date,ip,type
Logged in.,fa-globe,Web Vault - Chrome,1234abcd-56de-78ef-91gh-abcdef123456,Alice,alice@bitwarden.com,2021-06-14T14:22:23.331751Z,111.11.111.111,User_LoggedIn
Invited user zyxw9876.,fa-globe,Unknown,1234abcd-56de-78ef-91gh-abcdef123456,Alice,alice@bitwarden.com,2021-06-14T14:14:44.7566667Z,111.11.111.111,OrganizationUser_Invited
Edited organization settings.,fa-globe,Web Vault - Chrome,9876dcba-65ed-87fe-19hg-654321fedcba,Bob,bob@bitwarden.com,2021-06-07T17:57:08.1866667Z,222.22.222.222,Organization_Updated
```

APIのレスポンス

/eventsエンドポイントからBitwarden公開APIのイベントログにアクセスすると、次のようなJSONレスポンスが返されます：

```Bash
{
  "object": "list",
  "data": [
    {
      "object": "event",
      "type": 1000,
      "itemId": "string",
      "collectionId": "string",
      "groupId": "string",
      "policyId": "string",
      "memberId": "string",
      "actingUserId": "string",
      "date": "2020-11-04T15:01:21.698Z",
      "device": 0,
      "ipAddress": "xxx.xx.xxx.x"
    }
  ],
  "continuationToken": "string"
}
```

SIEMおよび外部システムの統合

Bitwardenから他のシステムにデータをエクスポートする際には、エクスポート、API、
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場合があります。例えば、組織の構造に関するデータを収集するためにBitwarden

RESTful APIを使用すること：

- GET /public/membersは、メンバー、ID、および割り当てられたgroupidを返します。
- GET /public/groupsは、すべてのグループ、ID、割り当てられたコレクション、およびそれらの権限を返します。
- GET /public/collectionsはすべてのコレクションと、それらに割り当てられたグループを返します。

各メンバー、グループ、コレクションの一意のIDを取得したら、CLIツールを使用してCLIコマンド`bw-list`を使用して、
次のアイテムをJSON形式で取得することができます。

- 組織のメンバー
- アイテム
- コレクション
- グループ

このデータを収集した後、ユニークIDで行を結合して、Bitwarden組織のすべての部分を参照するための基準を作成することができます。
Bitwarden CLIの使用に関する詳細は、Bitwardenコマンドラインツール（CLI）をご覧ください。