

GARMIN インターナショナル

# Garmin Connect 開発者プログラム ム スタートガイド

---

バージョン 1.0.0

---

社外秘

## 内容

1	改訂履歴	1
2	はじめに	2
2.1	Garmin 開発者プログラムの目的	2
2.2	コンシューマー・キーとシークレット	2
2.3	ユーザー登録	3
2.4	API ツールを使用したコンシューマーキーのセットアップ	3
2.4.1	コンシューマーAPI	3
2.4.2	エンドポイント構成	3
2.4.3	ユーザーの承認	3
2.4.4	署名の要求	3
2.5	プロダクション・キーの要求	4
2.6	エンドポイント構成	5
2.6.1	エンドポイントのデレジストレーション	5
3	ユーザーのエンドポイント	7
3.1	ユーザー・アクセストークンの削除	7
3.2	ユーザーID の取得	7

## 1 改訂履歴

バージョン	日付	改訂
1.0.0	日付	初版

## 2 はじめに

### 2.1 Garmin 開発者プログラムの目的

Garmin Connect 開発者プログラムは、Garmin のユーザーが、アクティビティトラッカーやフィットネス機器で生成したデータを、Garmin 以外のコーポレートパートナーと共有し、コーポレートパートナーから自身のデバイスへワークアウトのプランやコースをダウンロードできるようにする仕組みです。

Garmin Connect 開発者プログラムは 5 つの API で構成されます。

- トレーニング API (ワークアウトを Garmin Connect へアップロード)
- コース API (コースを Garmin Connect へアップロード)
- ヘルス API (ウェルネスデータを Garmin Connect からインポート)
- アクティビティ API (アクティビティを Garmin Connect からインポート)
- ウィメンズヘルス API (女性のヘルスデータをインポート)

各 API は該当する仕様ドキュメントで詳細に解説されています。

### 2.2 コンシューマー・キーとシークレット

API へアクセスするには、コンシューマー・キーとシークレットを作成する必要があります。コンシューマー・キーはパートナーを一意に識別するために使用され、コンシューマー・シークレットは、コンシューマー・キーへの不正アクセスを取得した第三者ではなく、そのパートナーから要求されたことの検証に使用されます。

コンシューマー・キーは公開情報と見なすことができますが、コンシューマー・シークレットはプライベートとして扱われます。 ユーザーのセキュリティのために、コンシューマー・シークレットはセキュアにする必要があります、ネットワーク経由でプレーンテキストを送信すべきではありません。モバイルアプリのような消費者向け製品にコンシューマー・シークレットを埋め込むことは許可されていません。

コンシューマー・キーの認証情報は、開発者ポータルを使用して、アプリを作成して作成します (<https://developerportal.garmin.com/user/me/apps?program=829>)。各アプリは一意的コンシューマー・キーを表します。

キーの作成時、API を選択することもできます。

ユーザーの最初のアプリは、レート制限された評価レベルのコンシューマー・キーを生成します。製品に対しユーザーの統合が確認されると、後続のアプリは生産レベルのアクセスでコンシューマー・キーを作成します。詳細については、以下の「プロダクション・キーの要求」を参照してください。

#### メモ：

ユーザーベースが論理的に分離されたプロジェクトや実装に対応するために、複数のコンシューマー・キーを作成する必要があります。一般的なシナリオでは、単一のパートナーが複数の他社からのユーザーデータを管理します。Garmin のユーザーが当該の会社との間でデータを共有することに合意するかについて、詳細な情報を得た上で決断できるよう、各管理会社に新しい管理キーを作成して関連付ける必要があります。

## 2.3 ユーザー登録

パートナーがユーザーのデータにアクセスするには、ユーザーがパートナーのアクセスを許可しなければなりません。（<https://developerportal.garmin.com/developer-programs/content/829/programs-docs>）を参照してください。開発者プログラムウェブツール（以下の Web Tools を参照）には、ユーザー認証と要求署名のデモンストレーションも含まれています。

## 2.4 API ツールを使用したコンシューマーキーのセットアップ

エンドポイント構成ツールに加えて、統合する際のパートナーを支援するいくつかのウェブベースのツールが用意されています。これらのツールは、構成するプログラムに適用できるコンシューマー・キーとシークレット情報を使用して <https://apis.garmin.com/tools/login> にログインすることで利用できます。

### 2.4.1 コンシューマーAPI

必要に応じて、コンシューマーキーに選択した API を編集できます。

### 2.4.2 エンドポイント構成

デフォルトで、API はすべて 2 つのエンドポイントが利用できます

- デレジストレーション（ユーザーとパートナーアプリとの接続が解除された場合、このエンドポイントを通じてパートナーへ通知します）
  - ユーザー権限（ユーザーがデータ共有の権限を削除した場合、このエンドポイントを通じて通知されます）
- 選択した API に応じて、その他のエンドポイントが利用できます

### 2.4.3 ユーザーの承認

このツールは、3-legged OAuth プロセス全体を記述して実行します。このツールを使用して、ユーザーアクセストークンを手動で生成し、パートナーの OAuth インフラストラクチャが書き込まれる前に、現在使用しているコンシューマー・キーに対し、それを認可することができます。

### 2.4.4 署名の要求

このツールは、OAuth 1.0a の要求署名を実行する方法について説明およびデモンストレーションを行います。サードパーティのライブラリを使用することをお勧めしますが、手作業による署名は初期の統合とデバッグの目的に役立ちます。OAuth 1.0a 要求の署名の詳細については、OAuth 仕様のドキュメントを参照してください。

## 2.5 プロダクション・キーの要求

開発者ポータルを通して生成される最初のコンシューマー・キーは評価キーです。このキーはレート制限されているため、テスト、評価、および開発にのみ使用する必要があります。プロダクションレベルの認証を取得するには、評価キーと使用する API プラヤーのリストを添えて、[connect-support@developer.garmin.com](mailto:connect-support@developer.garmin.com) へまずメールしてください。

個別の API 要求については、対応する仕様文書を参照してください。

## 2.6 エンドポイント構成

Ping サービス同様に、プッシュサービスを使用することで、パートナーは、Garmin ユーザーデータのほぼリアルタイムの更新を、定期的にスケジュールされている更新ジョブに生じる遅延や重複なく受信できます。Ping サービスのコールバック URL とは異なり、プッシュサービスでは、更新されたデータが JSON として POST 内に直接含まれている HTTPS POST が生成されます。このデータは、Ping 通知が生成され、コールバック URL が呼び出された時に返されるデータとまったく同一のものです。Ping サービスとプッシュサービスのどちらを使用するかは、お客様の好みと統合のやりやすさのみによって決まります。

### メモ：

プッシュ通知では、Ping サービスと同じ失敗通知に対する定義を使用した同一の再試行ロジックを採用しており、Ping サービスと同じ保留機能に対応しています。

### 2.6.1 エンドポイントのデレジストレーション

JSON 要素	説明
サマリータイプ（リストキー）	この ping リストの概要タイプ
userId	下層にあるユーザーの Garmin アカунトに対応した一意のユーザー識別子。この userId は API の呼び出しのパラメーターとしては一切使用されません。しかしながら、ユーザーが新しい UAT を生成するために再登録した場合、userAccessTokens の全体で存続します。
userAccessToken	UAT は新しいデータを生成したユーザーに対応します。

例：

```
{
  "deregistrations": [
    {
      "userId": "4aaca8e82427c251df9c9592d0c06768",
      "userAccessToken": "8f57a6f1-26ba-4b05-a7cd-c6b525a4c7a2"
    }
  ]
}
```

```
{
  "userPermissions": [
    {
      "userId": "4aaca8e82427c251df9c9592d0c06768",
      "userAccessToken": "8f57a6f1-26ba-4b05-a7cd-c6b525a4c7a2",
      "Courses_import",
      "Wellness_export"
    }
  ]
}
```

```
}  
]  
}
```



## 3 ユーザーのエンドポイント

ユーザーデータを取得するサマリーエンドポイントとは異なり、ユーザーエンドポイントはユーザーのアカウント自身で操作を実行します。操作の可用性と範囲は、ユーザーのプライバシーを保護するために意図的に制限されています。

### 3.1 ユーザー・アクセストークンの削除

このサービスは、UAT を削除することにより、使用されているコンシューマー・キーに固有のあなたのプログラムからユーザーを削除する機能を提供します。呼び出された後、Garmin Connect（有効になっている場合）を通してユーザーがアクセスを辞退したかのように、最終ユーザーの登録解除通知が送信されます。

登録解除の後すぐに、そのユーザーのためのすべての通知が直ちに停止し、その UAT でデータを要求しようとする試みは、許可されていないものとして拒否されます。削除された UAT は復元できません。同じユーザー（同じ Garmin Connect アカウントを持つユーザー）が OAuth を 2 回目に通過すると、全く異なる UAT が生成されます。

パートナーウェブサイトまたはアプリケーションが、通常の Garmin Connect 同意削除処理の外、またはユーザーがパートナープログラムを合理的に信じる他の場合に、「マイアカウントの削除」または「オプトアウト」メカニズムを提供している場合は、このエンドポイントをすべて終了する必要があります。Garmin データを共有するための同意を取り除く機会を与えています。

ユーザー登録を削除するための URL

**DELETE** : <https://apis.garmin.com/wellness-api/rest/user/registration>

この要求にパラメータは必要ありません。ユーザー・アクセストークンは OAuth ヘッダーから取得されます。

応答：要求が成功すると、このサービスは応答本文がない HTTP 204（内容なし）を返します。考えられるエラー応答については、付録 E を参照してください。

### 3.2 ユーザー ID の取得

Garmin Connect の各ユーザーには、固有の API ID が関連付けられ、複数の UAT にわたって存続します。例えば、ユーザーが Garmin Connect を通じて関連付けを削除した後、OAuth プロセスを完了して同じ Garmin Connect アカウントで新しいユーザー・アクセストークンを生成した場合、2 番目のトークンには依然として最初のトークンと同じ API ユーザー ID が含まれます。同様に、パートナーが複数のプログラムを管理しており、ユーザーがそれぞれに登録すると、各 UAT に対して返された API ユーザー ID が一致します。

API ID は識別情報を提供せず、他の Garmin API、ウェブサービス、またはシステムでは使用されません。Authorization ヘッダーのユーザー・アクセストークンを使用してユーザールックアップが常に実行されるため、API ユーザー ID をヘルス API に渡す理由はありません。

API のユーザー ID を取得するための URL

**GET** <https://apis.garmin.com/wellness-api/rest/user/id>

この要求にパラメータは必要ありません。

応答: {"userId": "d3315b1072421d0dd7c8f6b8e1de4df8"}