

# OIDC連携実装ガイド

Digital Platformer 株式会社

2022/07/22 Ver0.2

# DP社OIDC連携実装ガイドについて

- DP社の提供するDIDサーバーサービス（MyDID）では認証にOpenIDConnect（OIDC）を利用してユーザーIDや個人情報などを一元管理することができます。
- ここではID連携を利用する場合に考慮しておくべきことを簡単に説明します。

① ユーザーIDを作成する

② 作成したユーザーIDをOpenID Connectを利用して認証する  
について案内いたします。

なお、ご自身のシステムに組み込むためには別途API資料と接続方式に関する資料をご覧ください。

\* \*開発途中のものであり、変更される場合があります。

# OpenID Connectで提供する機能一覧

- ・アカウント作成とverificationCodeをemailで送付する機能
- ・メールアドレスの検証を行いアカウントを作成する機能とパスワード初期化
- ・DIDサービスへのログインとAPI認証用トークンを取得機能
- ・API認証用トークンを更新する機能
- ・パスワードリセットおよびメールアドレスリセット機能
- ・認証されたユーザの個人情報を登録・更新する機能
- ・登録済みユーザの個人情報を取得する機能

# ユーザーIDの作成

- ユーザーIDを作成するには  
利用したいアプリケーションからOIDCエンドポイントに対して  
httpsによるPOST通信を行います。Content-typeは  
application/jsonとし、POST Bodyに
  - "devID": "string",
  - "versionOS": "string",
  - "publicKey": "string",
  - "emailAddress": "user@example.com",
  - "skipMFA": trueを指定します。  
ただしユーザーID作成処理に関しては当社が「ユーザーID作成用  
MyDIDクライアントアプリ（Android/iOS用）仮称」を用意いたしま  
すので、実際には組み込む必要はありません。

# ユーザーID作成リクエストAPIとレスポンス例

POST /did/v1/signup アカウント作成のためのverificationCodeをemailで送付する。

指定された情報でアカウントを作成するための検証コードを、指定されたメールアドレスに送信する。ただし、skipMFA=trueの場合には検証コードは送信しない。その場合にはverificationCodeは固定値になる。

Parameters

No parameters

Request body

application/json

Try it out

Examples:

example-1

Example Value | Schema

```
{ "devID": "d32c8d6f-9bf0-41d6-8e6e-999999999999", "versionOS": "Android 31", "publicKey": "dc841a25498e574e84d38d759b69714feb1c70954eaad740678d119999999999", "emailAddress": "example@digitalplatformer.co.jp", "skipMFA": true }
```

Responses

Code	Description	Links
200	登録結果。	No links

Media type

application/json

Controls Accept header.

Examples

example-1

Example Value | Schema

```
{ "status": { "code": 0, "errorCode": null, "error": null, "message": null, "warning": null }, "data": { "requestId": 144, "verifyIvl": 600, "retryTimeout": 60 } }
```

# 作成したユーザーIDをOpenID Connect利 用してアプリで認証する

- MyDIDから受け取ったトークンを利用して認証や個人情報の取得などを行います。
1. MyDID側で用意するログイン用のエンドポイント(Web URL)を利用したいアプリ・サービスで表示させて、ユーザーID作成時に登録したユーザーIDとパスワードの入力し実行してください
  2. ログイン失敗時は「ユーザーIDまたはパスワードが異なっている」旨の結果が得られますので、再入力などを促してください
    1. もしユーザー登録がまだの場合はユーザー登録用アプリのダウンロードと実行を促してください
  3. 成功すると①AccessToken（認証情報）、②IDToken（個人情報）、③RefreshToken（有効期限を超えた場合に利用する）を受け取ることができますので、①AccessToken（認証情報）を利用して認証処理を行います
  4. 受け取った①AccessToken（認証情報）をMyDIDで用意するエンドポイント（Web URL）に送信すれば、正しいAccessTokenでユーザーIDが正しい情報かを判別し認証を行います
  5. 認証の成功後は利用中のログインセッション管理機構を利用して有効なログイン中であるか検証の上アプリ上の処理を継続ください

# ログインリクエストAPIとレスポンス例

POST /did/v1/login DIDサービス用ログインAPI。

API認証用トークンを取得する。

Parameters

No parameters

Request body

application/json

ログイン用リクエストボディ。

Examples:

example-1

Example Value | Schema

```
{  
  "devID": "d32c8d6f-9bf0-41d6-8e6e-999999999999",  
  "publicKey": "dc841a254898e574e84d38d759b69714feb1c70954ead740678d199999999999",  
  "secret": "DkezVRa00XusFRiVyP5bHyRsTm5KgLI"  
}
```

POST /did/v1/login DIDサービス用ログインAPI。

API認証用トークンを取得する。

Parameters

No parameters

Request body

application/json

ログイン用リクエストボディ。

Examples:

example-1

Example Value | Schema

```
{  
  "devID": "d32c8d6f-9bf0-41d6-8e6e-999999999999",  
  "publicKey": "dc841a254898e574e84d38d759b69714feb1c70954ead740678d199999999999",  
  "secret": "DkezVRa00XusFRiVyP5bHyRsTm5KgLI"  
}
```

## その他API

- 本ドキュメントではMyDIDで用意しているOpenIDConnectでのユーザーIDの作成とログイン認証について簡単に記述しましたが、その他のAPIに関しては後日提供いたします。
- また本APIに関しては開発中のものとなっていますので変更が発生する場合があります。

# 追加参考情報

OIDCとは? ID Federation 2021/11/22

OpenID ConnectによるID連携

[https://www.alpha.co.jp/blog/202111\\_02](https://www.alpha.co.jp/blog/202111_02)

IDトークンとは？アクセストークンとは？どのタイミングでどのような内容のやり取りがされるか？

<https://qiita.com/TakahikoKawasaki/items/498ca08bbfcc341691fe>

リフレッシュトークンとは？御社の場合どのタイミングでどのような内容のやり取りがされるか？

<https://qiita.com/TakahikoKawasaki/items/185d34814eb9f7ac7ef3>

OIDC標準のユーザー属性クレーム群

<https://qiita.com/TakahikoKawasaki/items/8f0e422c7edd2d220e06>

- DP社オリジナルの拡張クレーム名に関しては最新情報をDP社へご確認ください。