**認証と認可**

**認証とは**

あらかじめ与えられたIDを使ってログインを行い、本人確認をする処理のこと

もともと認証の仕組みはサイトごとに実装されており、各サイトで利用者のアカウント情報を管理していたが、最近ではGoogleやTwitterなどの利用者が多いWebサービスが管理しているアカウント情報を利用して認証を行うようになり、ユーザが管理するアカウントの数を減らすことができるようになった

○一般的な認証の仕組み

○Webサービスを使った認証の仕組み



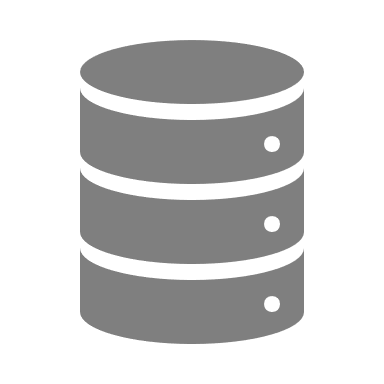
Webブラウザ

ユーザID、パスワード

ログイン成功

ユーザID、パスワード

ログイン許可



DBサーバ



Webサーバ

ログイン画面

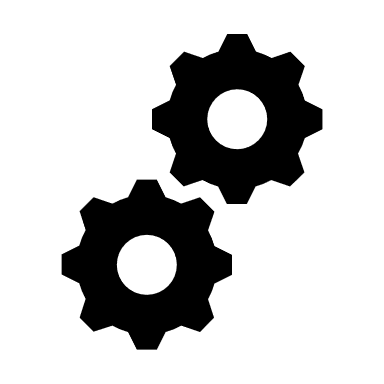
**認証APIとOpenIDの仕組み**

利用

Webサイトごとに認証が不要ログイン情報を扱う必要がない

認証

認証を代行する



GoogleのようなWebサービス



ログイン画面



ログイン画面



Webサーバ

ログイン画面



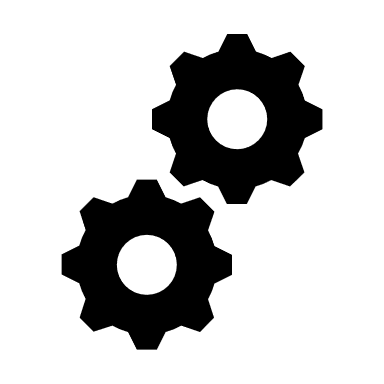
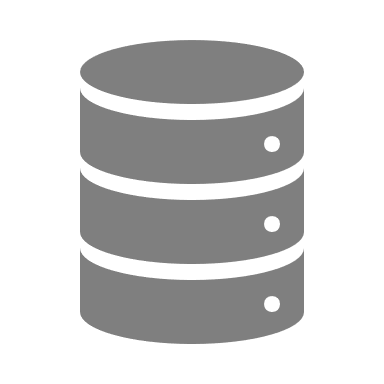
Webブラウザ

認証API

認証処理をする側は処理の仕組みをAPIとして提供し、認証APIを利用するサイトは認証を行うWebアプリケーションがユーザを認証APIに誘導し、認証APIから認証結果の通知をもらうことで、ユーザのログイン情報を扱うことなく認証処理を行うことができる

ただし、ユーザが対象の認証API側のアカウントを持っていないとこの方式でログインできない

また、各社ごとにAPIの仕様が統一されていないため、複数の認証APIを対応させるには時間がかかる



認証API

認証サイト

認証APIを提供するサイトに

アカウントがある必要がある

①ログインの要求

②認証APIへのログイン指示

④認証完了の通知

⑤ログイン成功通知

③ログイン



会員制サイト

ログイン画面



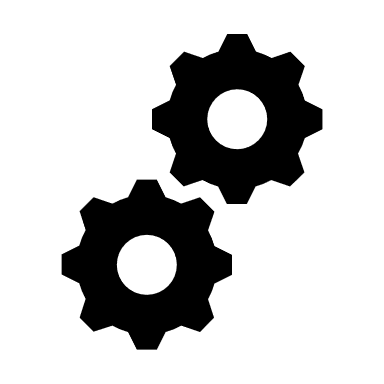
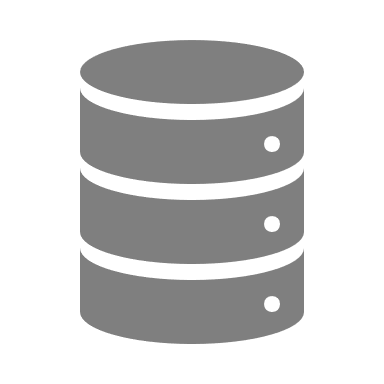
Webブラウザ

OpenID

認証APIの問題を解決するために認証処理を標準化したプロトコル

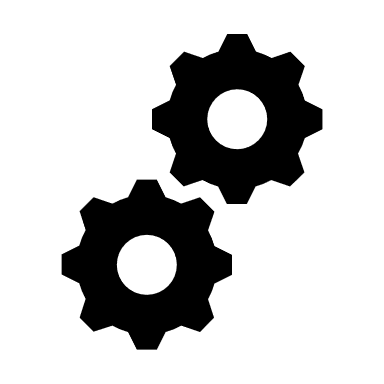
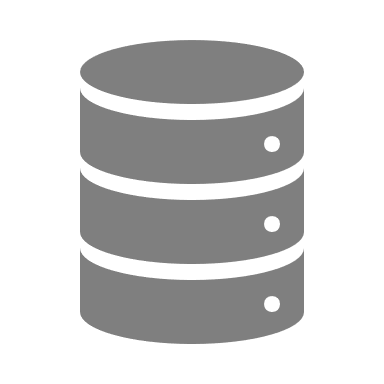
複数の企業が提供する認証サービスを同じ手順で利用することが可能になる

OpenIDサイトのいずれかにアカウントがあればOK

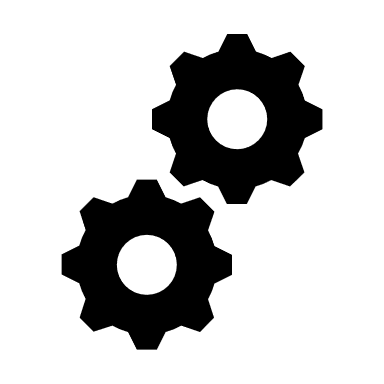
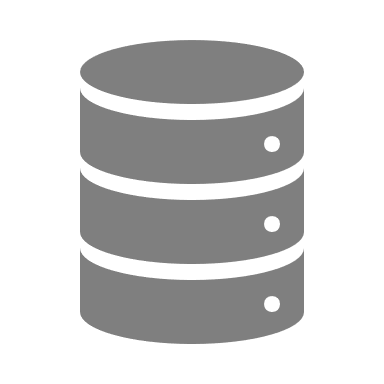


OpenID

OpenIDサイト



OpenID



OpenID

①OpenIDアカウント

③OpenIDへのログイン指示

⑥ログイン成功通知

⑤認証完了の通知

②アカウントを持つサイトを検索し暗号化鍵を交換

④ログイン



Webブラウザ



会員制サイト

ログイン画面

**認可とは**

認証によって確認した結果によりユーザごとの権限にしたがって利用できるサービスの許可を行うこと

○一般的な認可の仕組み



Webサーバ

ログイン画面

管理

画面

閲覧→許可

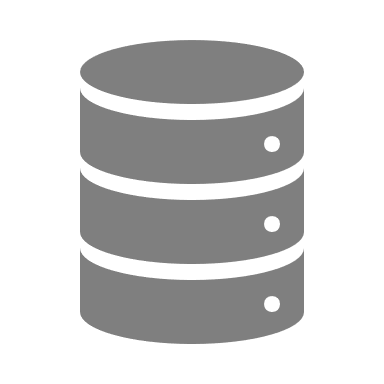
編集→不許可

ユーザID、パスワード

ログイン許可・権限情報



Webブラウザ



DBサーバ

ユーザID、パスワード

ログイン成功

○サイトをまたいだ認可の仕組み

同じ内容をTwitterに投稿

Facebookに投稿

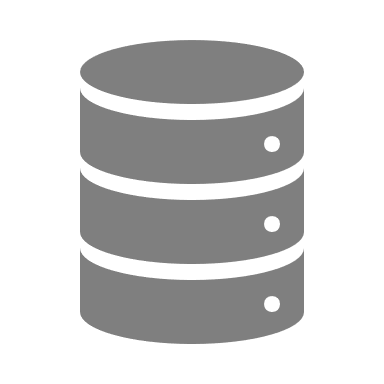


Facebook

管理

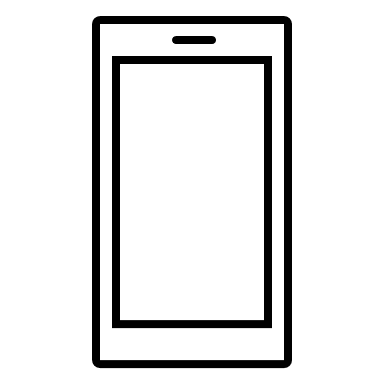
画面

ニュースアプリに表示されたニュースの内容を投稿(シェア)



Twitter

API



ニュースアプリ



Webブラウザ

**OAuthとOpenID Connect**

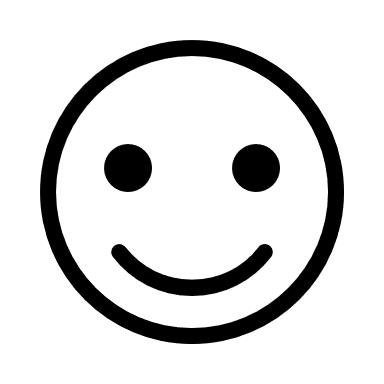
OAuth

サイトをまたいだ認可を実現するために標準化されたプロトコル、認証は行わない

利用したいサービスはリソースと呼ばれ、サービスを提供するサーバがリソースサーバ、そのユーザがリソースオーナー、認可を受けてリソースを提供するWebサイトやアプリをクライアントと呼ぶ

OpenID Connect

Facebookにアカウントの利用を許可しますか？



ユーザ

リソースユーザ



Webブラウザ



Facebook

クライアント

管理

画面

③トークンの要求

④トークンの発行

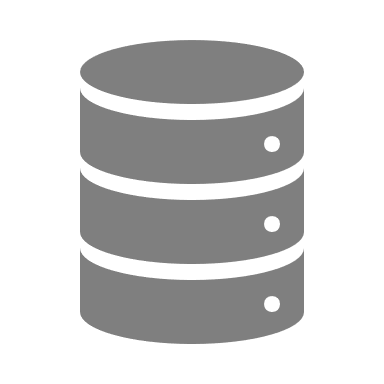
⑤トークンを提示し投稿

API

OAuth

①許可要求

②許可



Twitter

リソースサーバ

OAuth2.0をベースに認証機能が追加されたプロトコル

認証と認可が実現できるためOAuthのように別途認証の方法を用意する必要がない