OAuth

> Open Authorization

인터넷 사용자들이 비밀번호를 제공하지 않고, 다른 웹사이트 상의 자신들의 정보에 대해 웹사이트나 애플리케이션의 접근 권한을 부여할 수있는 개방형 표준 방법

이러한 매커니즘은 구글, 페이스북, 트위터 등이 사용하고 있으며 타사 애플리케이션 및 웹사이트의 계정에 대한 정보를 공유할 수 있도록 허용해준다.

사용 용어

- **사용자** : 계정을 가지고 있는 개인
- **소비자** : OAuth를 사용해 서비스 제공자에게 접근하는 웹사이트 or 애플리케이션
- **서비스 제공자** : OAuth를 통해 접근을 지원하는 웹 애플리케이션
- **소비자 비밀번호** : 서비스 제공자에서 소비자가 자신임을 인증하기 위한 키
- **요청 토큰** : 소비자가 사용자에게 접근권한을 인증받기 위해 필요한 정보가 담겨있음
- **접근 토큰** : 인증 후에 사용자가 서비스 제공자가 아닌 소비자를 통해 보호 자원에 접근하기 위한 키 값

토큰 종류로는 Access Token과 Refresh Token이 있다.

Access Token은 만료시간이 있고 끝나면 다시 요청해야 한다. Refresh Token은 만료되면 아예 처음부터 진행해야 한다.

인증 과정

> 소비자 <-> 서비스 제공자

1. 소비자가 서비스 제공자에게 요청토큰을 요청한다.
2. 서비스 제공자가 소비자에게 요청토큰을 발급해준다.
3. 소비자가 사용자를 서비스제공자로 이동시킨다. 여기서 사용자 인증이 수행된다.
4. 서비스 제공자가 사용자를 소비자로 이동시킨다.
5. 소비자가 접근토큰을 요청한다.
6. 서비스제공자가 접근토큰을 발급한다.
7. 발급된 접근토큰을 이용해서 소비자에서 사용자 정보에 접근한다.