

refresh 및 access token의 처리 방식에 대해


▼ 팀명

1. client가 웹 사이트에 접속해서 login을 수행한다.
2. 인증 서버에서 login 한 client에게 access token과 refresh token을 지급한다.
3. client는 refresh token을 cookie에 저장하고 access token은 메모리에 저장한다.(같은 곳에 저장하지 않기 위함)
4. client는 인증이 필요한 service에 access token을 넣어서 보낸다.
5. 서버는 client가 제시한 access token이 유효한지 확인하고 유효하지 않다면 refresh token을 요구한다.
6. client는 refresh token을 서버에 보내 refresh token이 유효하다면 새로운 access token을 발급 받는다.
7. 서버에서 refresh token이 유효하지 않다고 판단한 경우 재 로그인을 요구한다.

클라이언트는 재발급 요청을 보낼 때 access token과 refresh token 모두를 헤더에 담아서 보낸다.

[WEB] Access Token & Refresh Token 원리 (feat. JWT)

Access Token과 Refresh Token 이번 포스팅에서는 기본 JWT 방식의 인증(보안) 강화 방식인 Access Token & Refresh Token 인증 방식에 대해 알아보겠다. 먼저 JWT(Json Web Token)에 대해 잘 모르는 독자

 <https://inpa.tistory.com/entry/WEB-%F0%9F%93%9A-Access-Token-Refresh-Token-%EC%9B%90%EB%A6%AC-feat-JWT>

ACCESS TOKEN

