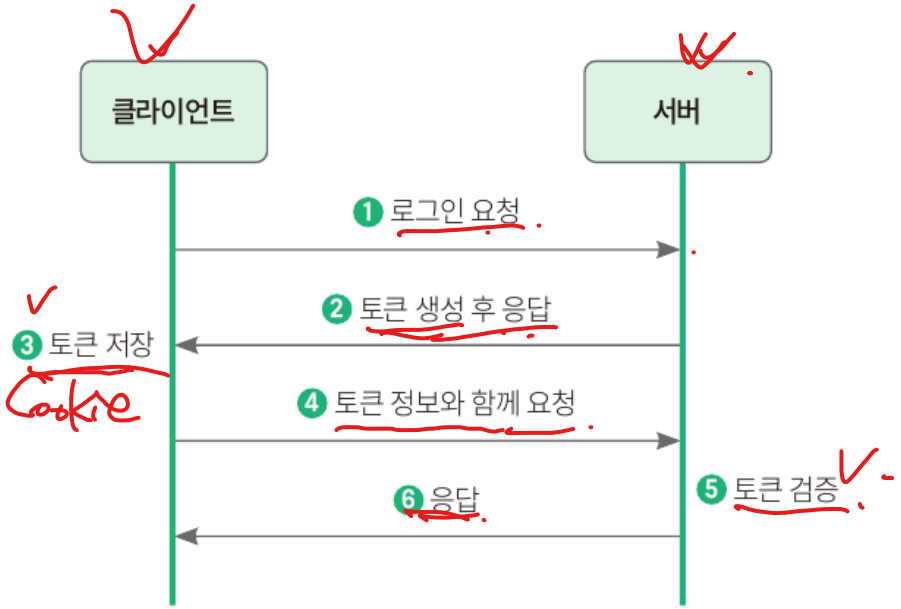
10장 JWT

목차

1. 토큰 기반 인증

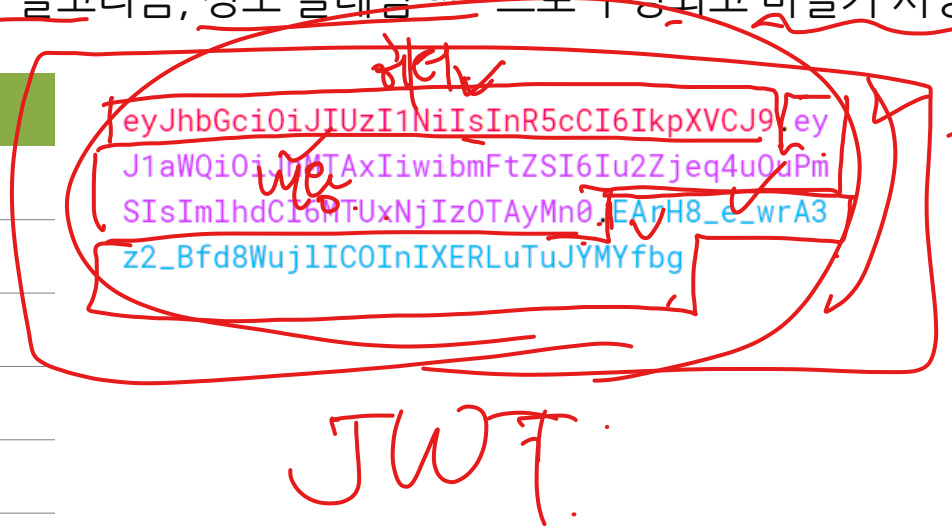
- 토큰 Token은 인증된 사용자를 식별하기 위해 서버에서 발급된 Base64 인코딩 문자열 데이터
- 사용자 인증 방식은 세션 기반 인증 방식과 토큰 기반 인증 방식
- 토큰 기반 인증 방식을 서버에서 토큰을 생성하고 사용자에게 토큰을 제공해 사용자를 인증하는 방식



2. JWT

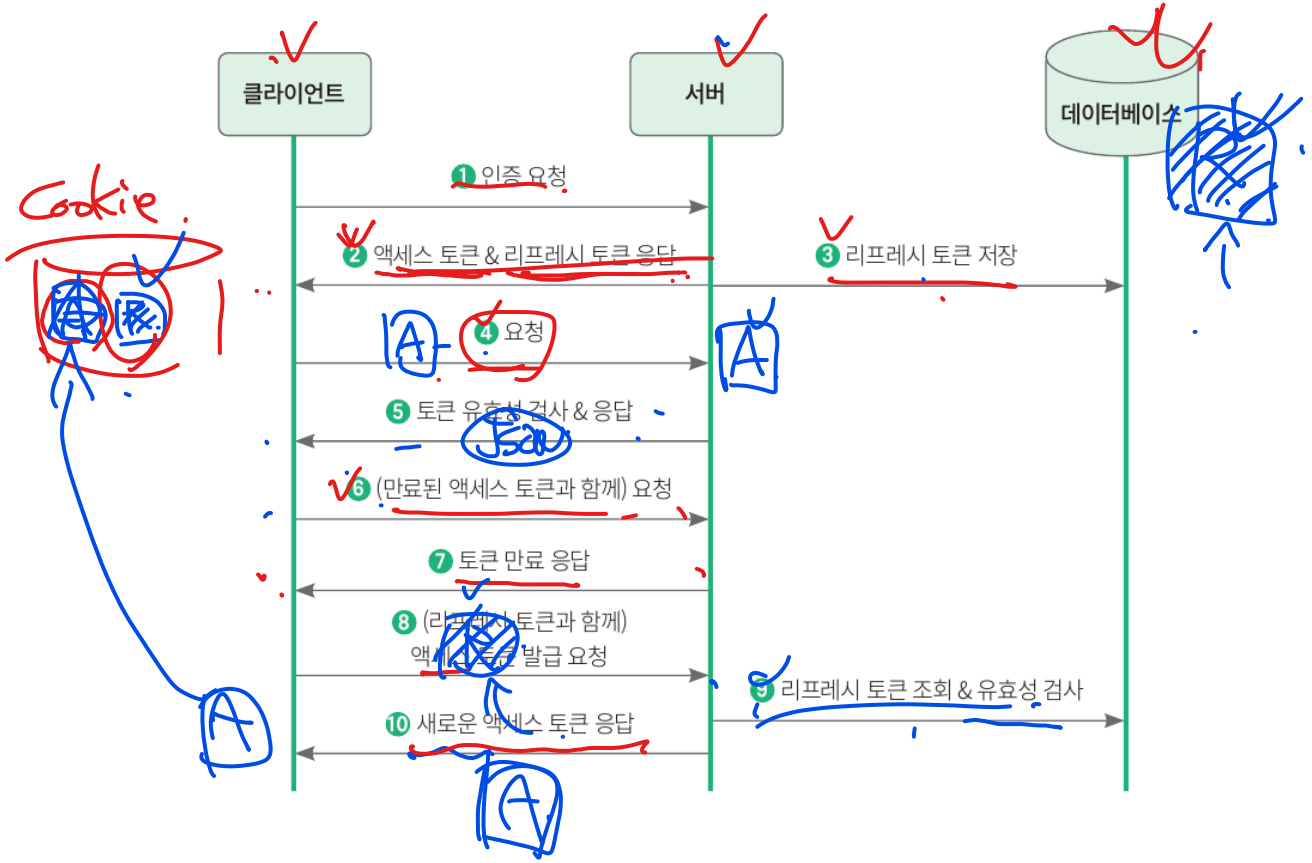
- JWT Json Web Token는 사용자를 인증하고 식별하기 위한 토큰 기반 인증 기술
- JWT는 사용자의 인증 정보와 서버에서 발급되었음을 증명하는 서명이 포함된 암호문을 클라이언트에서 저장 관리
- JWT는 헤더 Header, 내용 Payload, 서명 Signature으로 토큰 타입과 해싱 알고리즘, 정보 클레임 Claim으로 구성되고 비밀키 서명

구분	클레임	설명
Header	typ	토큰 타입
	alg	해싱 알고리즘
Payload	iss	토큰 발급자
	sub	토큰 제목
	exp	토큰 만료 시간
	iat	토큰 발급 시간
	aud	토큰 대상
	nbf	토큰 활성 시간
	jti	토큰 고유 식별자
Signature		Header 인코딩 + Payload 인코딩 + 비밀키 서명



3. Access/Refresh Token

- JWT는 보안성을 향상하기 위해 Access 토큰과 Refresh 토큰을 운영
- Access 토큰은 짧은 유효기간을 갖고 API에 대한 인증 및 권한 검증에 사용
- Refresh 토큰은 만료된 Access 토큰을 갱신하는 목적으로 긴 유효기간을 갖음



4. OAuth2

- Oauth2는 토큰방식으로 제 3의 플랫폼 업체의 사용자 정보를 통해 사용자를 인증하는 표준 위임 인증 기술
- 대다수의 서비스 업체에서 표준으로 OAuth2 방식으로 인증 서비스 제공