

OAuth

By CommentLee

Remind: 인증과 인가

인증 (Authentication)

사용자의 신원을 확인하는 과정

- "누구인가?"를 검증
- 아이디/비밀번호, 지문, OTP 등
- 실패 시 401 Unauthorized

인가 (Authorization)

인증된 사용자의 접근 권한을 결정

- "무엇을 할 수 있는가?"를 결정
- 자원에 대한 권한 체크
- 실패 시 403 Forbidden



Login with Facebook



Sign in with Google+

Oauth는 인가를 위한 프로토콜이지만..

Remind: 토큰 기반 인증

토큰 기반 인증이란?

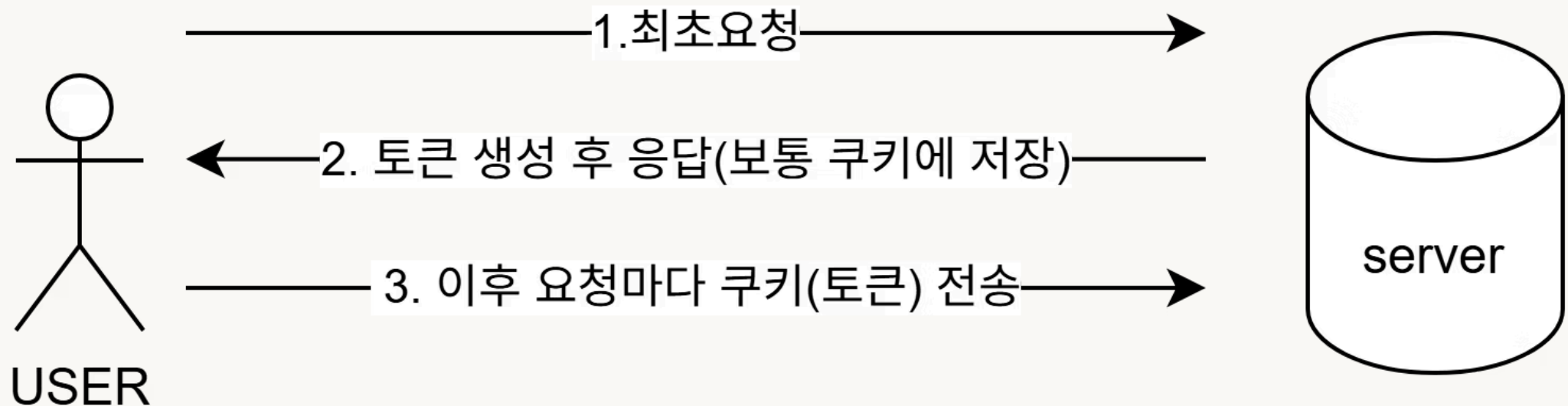
토큰은 서버가 발급한 인증 정보를 담은 문자열입니다. 사용자는 로그인 후 Access Token을 받아, 이후 모든 요청 시 아이디/비밀번호 대신 토큰을 사용합니다. (Refresh token도 사용 가능)

장점

- 높은 확장성 (분산 시스템에 적합)
- 서버는 세션 저장 불필요 (Stateless)
- 다양한 플랫폼 간 공유 가능

단점

- 토큰 탈취 시 보안 위험
- 토큰 갱신과 무효화 관리
- 유효기간 관리 필요



OAuth의 등장 배경

기존 방식의 문제점

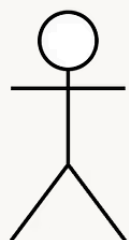
사용자가 비밀번호를 제3자 앱에 직접 제공

보안 위험 발생

"깃허브 계정으로 로그인" 기능 구현 시 → 깃허브 비밀번호를 다른 앱에 입력 → 비밀번호 노출 위험

OAuth 표준 등장

비밀번호 공유 없이 권한만 위임하는 안전한 프로토콜 **OAuth (Open Authorization)** 탄생



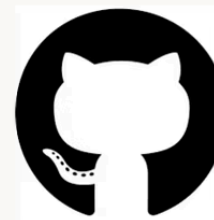
유저

깃허브 ID,PASSWORD



서버

유저 정보로 서비스 요청



OAuth란

OAuth 정의

제3자 애플리케이션이 사용자 자원에 접근할 수 있도록 허용하는 **표준 프로토콜**.

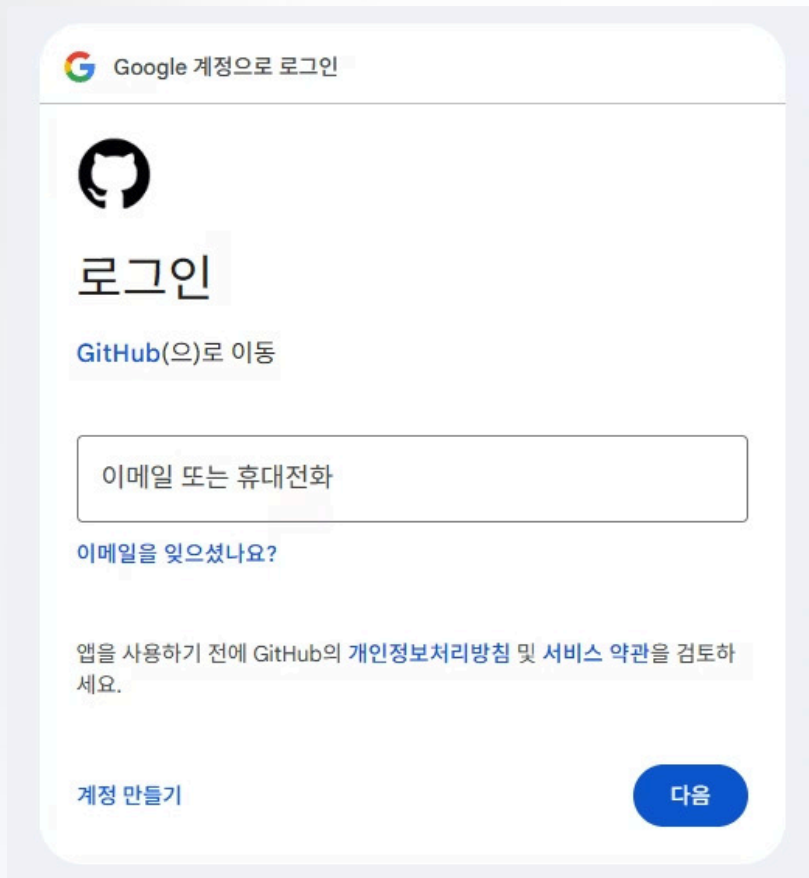
핵심 개념

비밀번호를 주지 않고, **접근 권한만 위임**.

→인가를 위한 프로토콜

실제 사용 예시

"구글 계정으로 로그인" 시 → 사용자가 구글에 로그인 후 → 해당 앱에 필요한 접근 권한만 허락



The screenshot shows a GitHub login interface. At the top, there is a button labeled "Google 계정으로 로그인" (Login with Google account). Below it is the GitHub logo and the word "로그인" (Login). A link "GitHub(으)로 이동" (Go to GitHub) is visible. There is a text input field for "이메일 또는 휴대전화" (Email or phone number). Below the input field is a link "이메일을 잊으셨나요?" (Forgot your email?). A note states "앱을 사용하기 전에 GitHub의 개인정보처리방침 및 서비스 약관을 검토하세요." (Review GitHub's privacy policy and service terms before using the app.). At the bottom left is a link "계정 만들기" (Create account) and at the bottom right is a blue button labeled "다음" (Next).

OAuth 구성요소

OAuth 시스템을 구성하는 4가지(서버 개발자 입장)

비슷한 용어의 헷갈림 주의!



Resource Owner = 사용자 = 내 유저

사용자 - 데이터의 주인이자 권한을 위임하는 주체



Client = 내 서버

제3자 애플리케이션 - 사용자 자원에 접근하려는 앱



Resource Server

API 서버 - 보호된 리소스를 가진 서버 (예: Google API)



Authorization Server

인증 서버 - 사용자를 인증하고 **토큰을 발급**하는 서버

OAuth 구조 개요



OAuth 사전작업

Register a new OAuth app

Application name *

Something users will recognize and trust.

Homepage URL *

The full URL to your application homepage.

Application description

This is displayed to all users of your application.

Authorization callback URL *

Your application's callback URL. Read our [OAuth documentation](#) for more information.

☐ **Enable Device Flow**

Allow this OAuth App to authorize users via the Device Flow.
Read the [Device Flow documentation](#) for more information.


Register application Cancel

Client ID

Ov231ijp8hMwghEcDs1D

Client secrets [Generate a new client secret](#)

Make sure to copy your new client secret now. You won't be able to see it again.



Client secret

✓ 886c256393009ec64662abe60afa152cee7f0e57 [Copy](#)

Added now by commentLee

Never used

[Delete](#)

You cannot delete the only client secret. Generate a new client secret first.

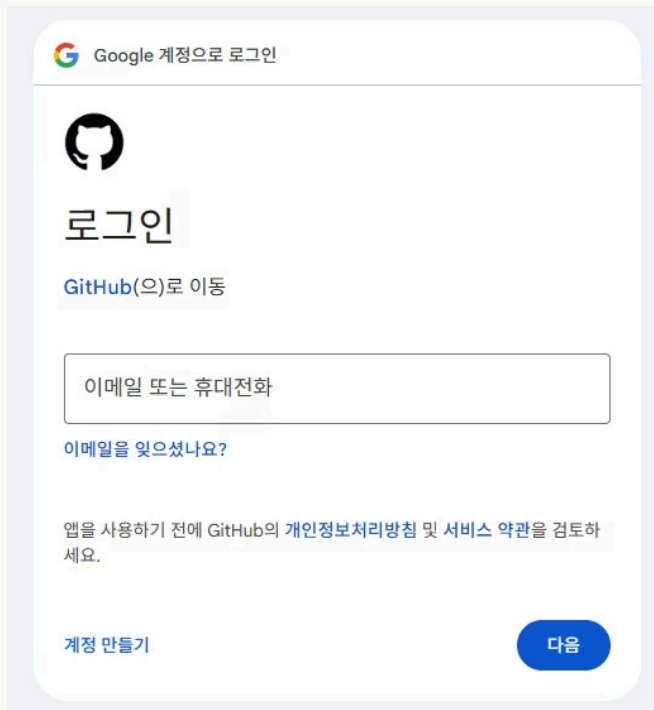
client id와 secrets을 받는다

미리 Authorization Server에 url과 callback 주소를 등록해야한다.


OAuth 사전작업(2)

[https://github.com/login/oauth/authorize?](https://github.com/login/oauth/authorize?client_id=Ov23lijp8hMwghEcds1D&redirect_uri=https://localhost:8080/callback)

[client_id=Ov23lijp8hMwghEcds1D](https://github.com/login/oauth/authorize?client_id=Ov23lijp8hMwghEcds1D&redirect_uri=https://localhost:8080/callback)
[&redirect_uri=https://localhost:8080](https://github.com/login/oauth/authorize?client_id=Ov23lijp8hMwghEcds1D&redirect_uri=https://localhost:8080/callback)
[/callback](https://github.com/login/oauth/authorize?client_id=Ov23lijp8hMwghEcds1D&redirect_uri=https://localhost:8080/callback)



Google 계정으로 로그인



로그인

GitHub(으)로 이동

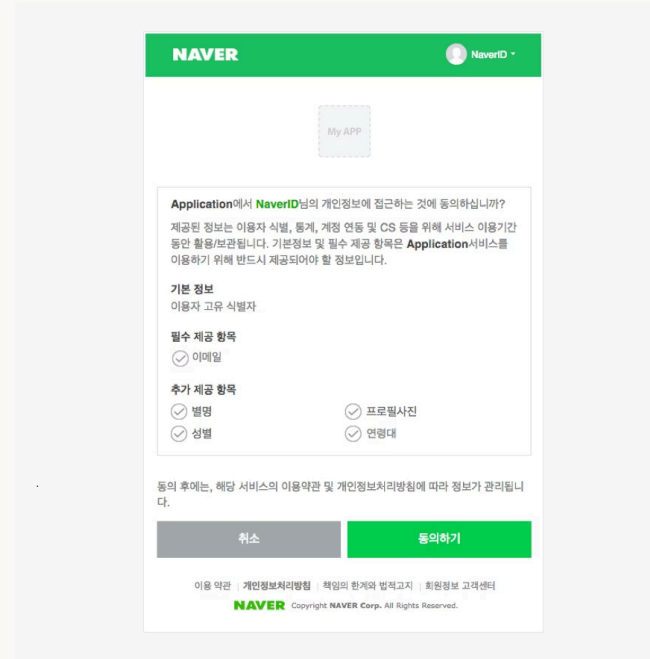
이메일 또는 휴대전화

이메일을 잊으셨나요?

앱을 사용하기 전에 GitHub의 개인정보처리방침 및 서비스 약관을 검토하세요.

계정 만들기

다음



NAVER

My APP

Application에서 NaverID님의 개인정보에 접근하는 것에 동의하십니까?
제공된 정보는 사용자 식별, 통계, 계정 연동 및 CS 등을 위해 서비스 이용기간 동안 활용/보관됩니다. 기본정보 및 필수 제공 항목은 Application서비스를 이용하기 위해 반드시 제공되어야 할 정보입니다.

기본 정보
사용자 고유 식별자

필수 제공 항목
☒ 이메일

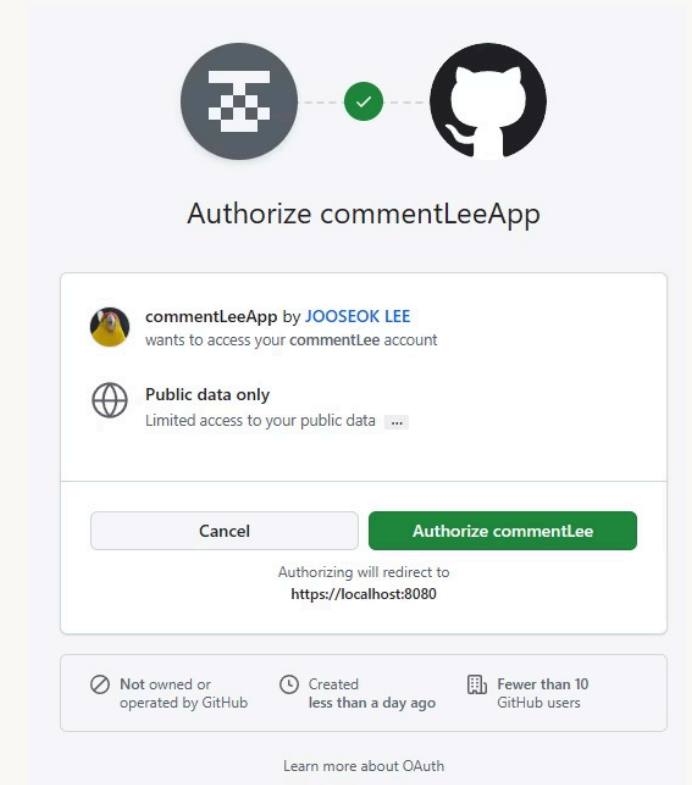
추가 제공 항목
☒ 별명 ☒ 프로필사진
☒ 성별 ☒ 연령대



동의 후에는, 해당 서비스의 이용약관 및 개인정보처리방침에 따라 정보가 관리됩니다.

취소 동의하기


이용 약관 : 개인정보처리방침 : 책임의 한계와 법적고지 : 회원정보 고객센터


NAVER Copyright NAVER Corp. All Rights Reserved.






Authorize commentLeeApp

 commentLeeApp by JOOSEOK LEE
wants to access your commentLee account

 Public data only
Limited access to your public data ...

Cancel Authorize commentLee

Authorizing will redirect to
<https://localhost:8080>

 Not owned or operated by GitHub  Created less than a day ago  Fewer than 10 GitHub users

Learn more about OAuth

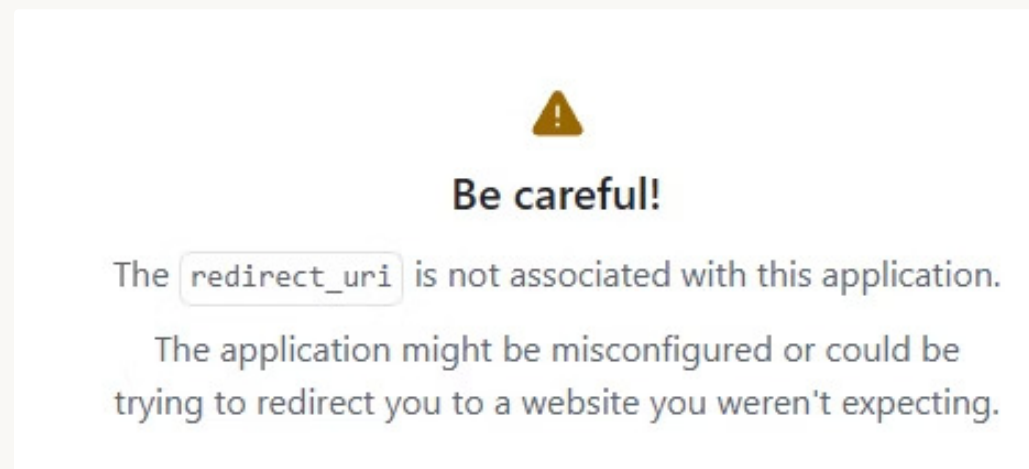
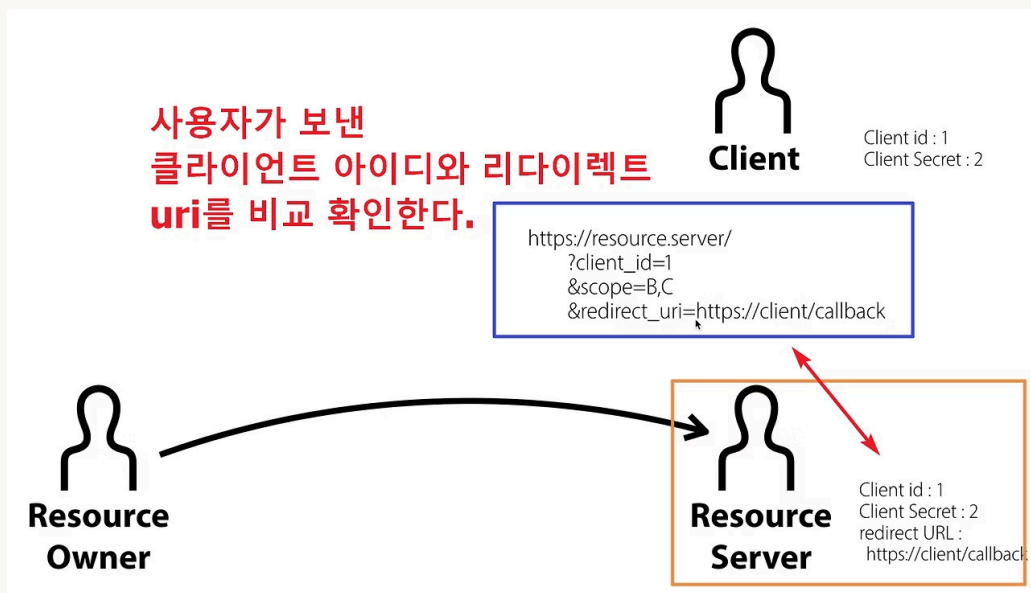
OAuth 흐름 (1)



3. client id와 리다이렉트 주소가 포함된 URL

접속시 해당 서버에서 인증(로그인) 후 권한 동의화면(이전슬라이드)

client ID와 redirect URL 검증



맞다면 code 발급 다르다면 404 또는 동작안함

여기까지 진행했을때 Resource Server가 알고있는 것

1. Client Id : Resource Owner와 연결된 client가 누구지
2. Client Secret: Resource Owner와 연결된 client의 비밀번호
3. Redirect URL : client와 통신할 통로
4. user id : client와 연결된 Resource Owner의 id
5. **Authorization code**: Resource Owner에게 준 인가 코드.

client는 인가 코드 뿐만 아니라 1~4를 같이 보내서 토큰을 받아와야한다.

OAuth 흐름 (2)

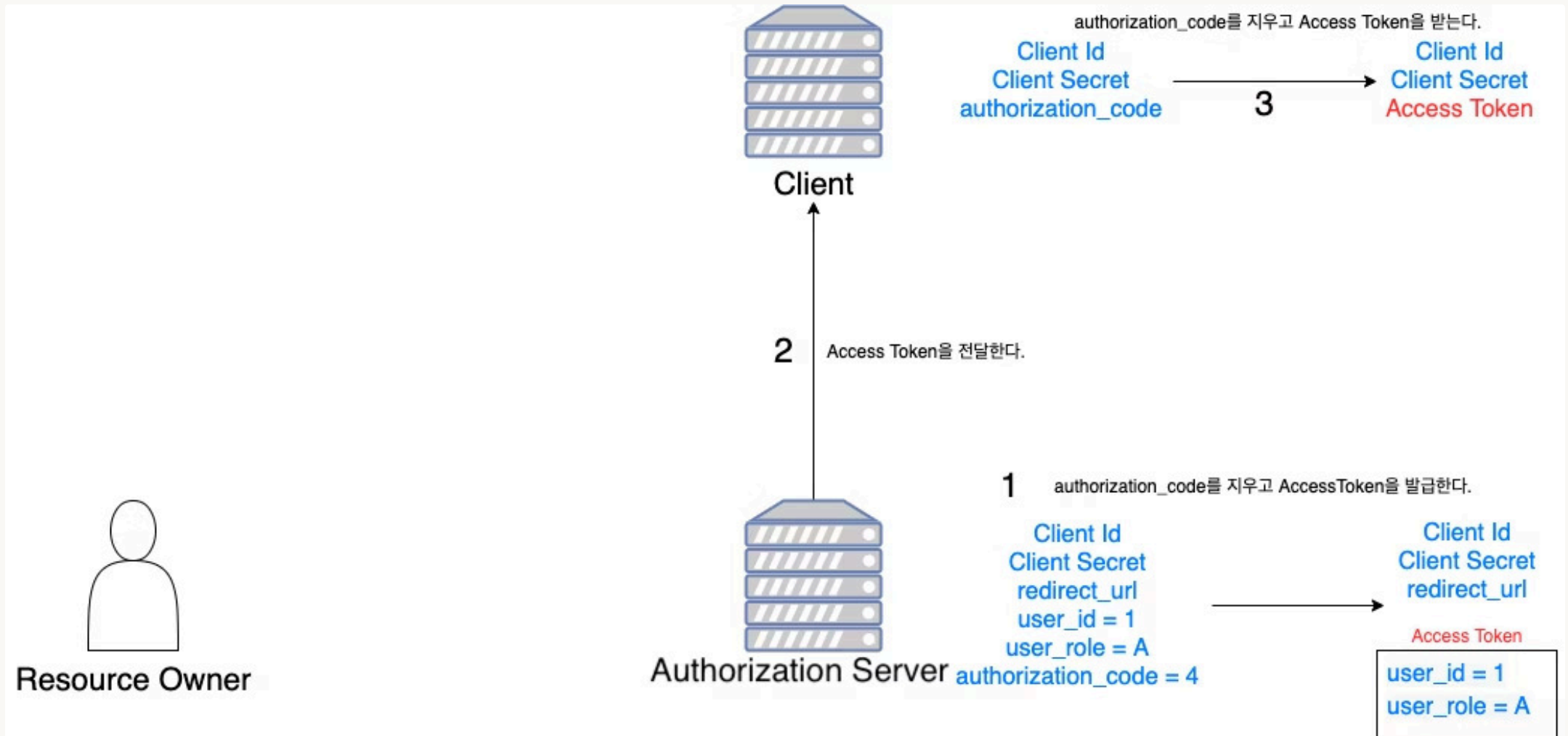


5 사용자가 확인했다면 인가코드를 받게된다.

6. 리다이렉트로 등록한 나의 서버의 callback주소로 전송한다

7. 받은 인가코드를 client의 정보와 함께 Authorization Server로 보내서 토큰을 받아온다.

끝: 발급 받은 Access 토큰으로 리소스에 접근 가능!



Refresh 토큰도 같이 주는경우(발급 여부, 기간 등은 Resource Server의 docs를 봐야..):

- Access Token이 기간이 만료될 때, Refresh Token을 통해 Access Token을 재발급 한다.

OAuth 2.0 의 특징

1. Scope 설정 가능
2. Bearer Token (=Access Token): 해당 토큰을 갖고 있으면 권한 존재. 따라서 TLS 강제됨.
3. 다양한 권한 부여 방식(Grant Types) : 브라우저가 아닌 다른 기기 배려. 하지만 대부분 Authorization code 사용
4. 역할의 분리 : 인가는 Authorization Server, 서비스 호출은 Resource Server
5. Refresh 토큰: Access Token 탈취 개선

선택하세요. ▼ ✓

네이버 로그인

제공 정보 선택(이용자 식별자는 기본 정보로 제공) ⓘ

권한	필수	추가
회원이름	<input type="checkbox"/>	<input type="checkbox"/>
이메일	<input type="checkbox"/>	<input type="checkbox"/>
별명	<input type="checkbox"/>	<input type="checkbox"/>
프로필 사진	<input type="checkbox"/>	<input type="checkbox"/>
성별	<input type="checkbox"/>	<input type="checkbox"/>
생일	<input type="checkbox"/>	<input type="checkbox"/>
연령대	<input type="checkbox"/>	<input type="checkbox"/>
출생연도	<input type="checkbox"/>	<input type="checkbox"/>
휴대전화번호	<input type="checkbox"/>	<input type="checkbox"/>

[알림] 추가권한에 대한 네이버 로그인 공지사항을 확인하세요.