KB금융그룹 | 국민의 평생 금융파트너

2025년 상반기 K-디지털 트레이닝

크로스 오리진 문제 해결 방법

[KB] IT's Your Life

웹 작업에서 신경써야하는 문제 항상
보안 문제.

js는 신뢰할 수 없어. 악의적인 애인지. 서버입장에서는
클라에서 주는 js를 어떻게 확인할 수 있을까?
통신을 허용해야 하는가?

기본적으로 코드를 못봐서 모름.
정책을 세움.

정책 : 서버 나 자신이 준 html에 들어있는 js내용은
안전하다.

그렇다면 다른 서버에서 받은 html에서 js내용은
서버에서 믿지 않음.

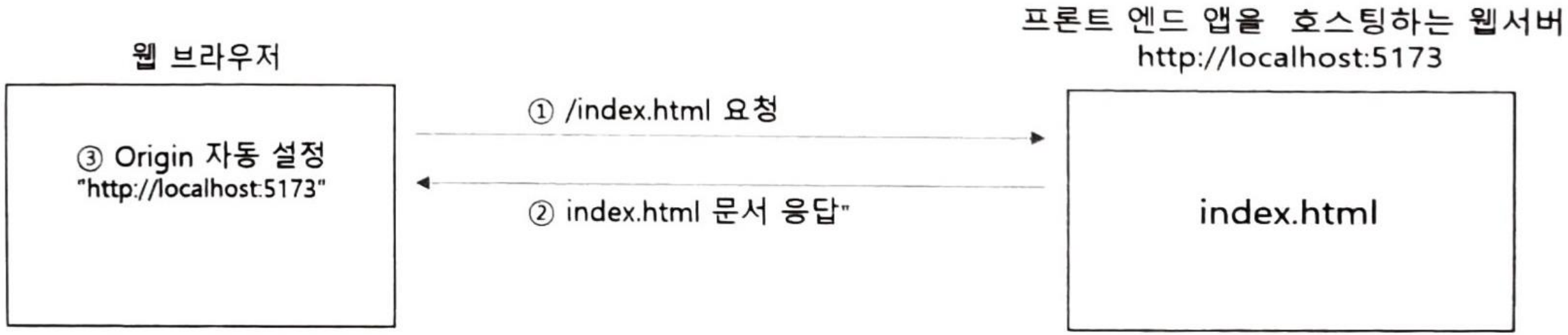
그렇다면 어느 서버에서 html이 왔는지 기록해야함.
어디서 왔냐를 식별하는 게 origin이라고 함.

html에는 오리진 표기가 주소와 포트번호로 이뤄짐.

KB 국민은행

크로스 오리진(Cross Origin) 문제

- 오리진(Origin)
  - 현재 요청 페이지를 받은 서버의 정보(주소와 포트번호)




```
> location.origin
< 'http://localhost:5173'
```

받으면 브라우저에
오리진이라는 정보가
세팅이 된다.
프로토콜 주소 포트번호.

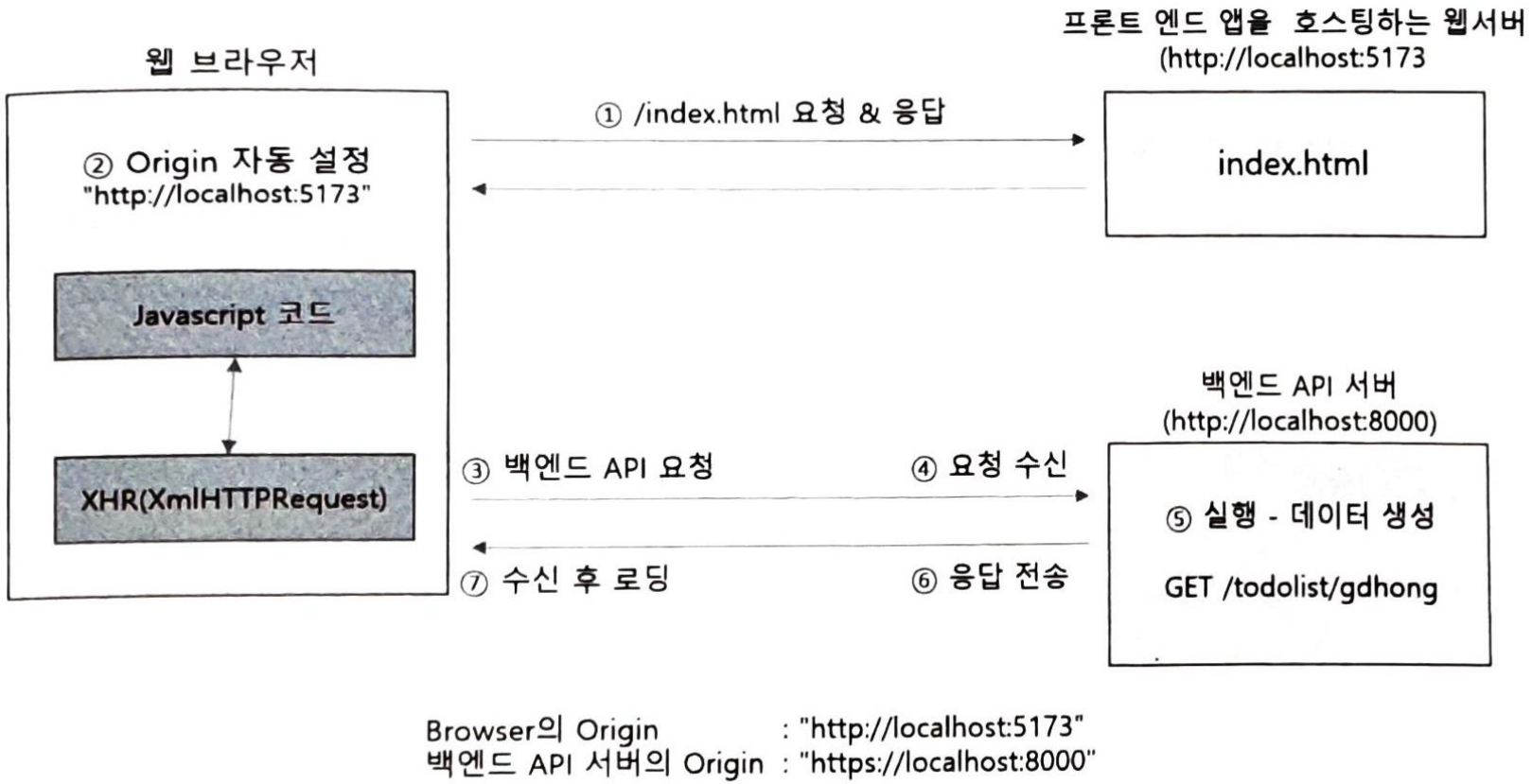
향후에 이 페이지 안에 들
어있는 js코드는 준 서버와
만 통신할 수 있다.

그렇다면 html을 준 서버와
js코드가 영향을 미치는 db서버와 다르다면
어덯게 될까? 에러가 발생됨. 보안 정책 때문에
데이터 정상이어도 에러.

크로스 오리진(Cross Origin) 문제

브라우저의 기본 보안 정책

- 동일 근원 정책: SOP(Same Origin Policy)
- 브라우저의 오리진과 동일한 오리진을 가진 서버일 때만 통신 가능
- 다른 오리진의 서버와 통신을 허용하지 하지 않음



Browser의 Origin : "http://localhost:5173"
백엔드 API 서버의 Origin : "https://localhost:8000"

3 크로스 오리진 문제 해결 방법

해결 방법 2개. 영구/임시 방법

- 백엔드 API 서버측에서 CORS(Cross Origin Resource Sharing)라는 기능을 제공
  - Origin이 달라도 통신을 허용해 줌

서버에서 허용하는 영구적인 방법.
open api를 제공하는 서버들이 반드시 해야함. open api는 특정 클라이언트에 종속되지 않잖아.

- 프론트 엔드 애플리케이션을 호스팅하는 웹서버에 프록시(Proxy)를 설치 또는 설정
  - 개발 단계에서 주로 사용

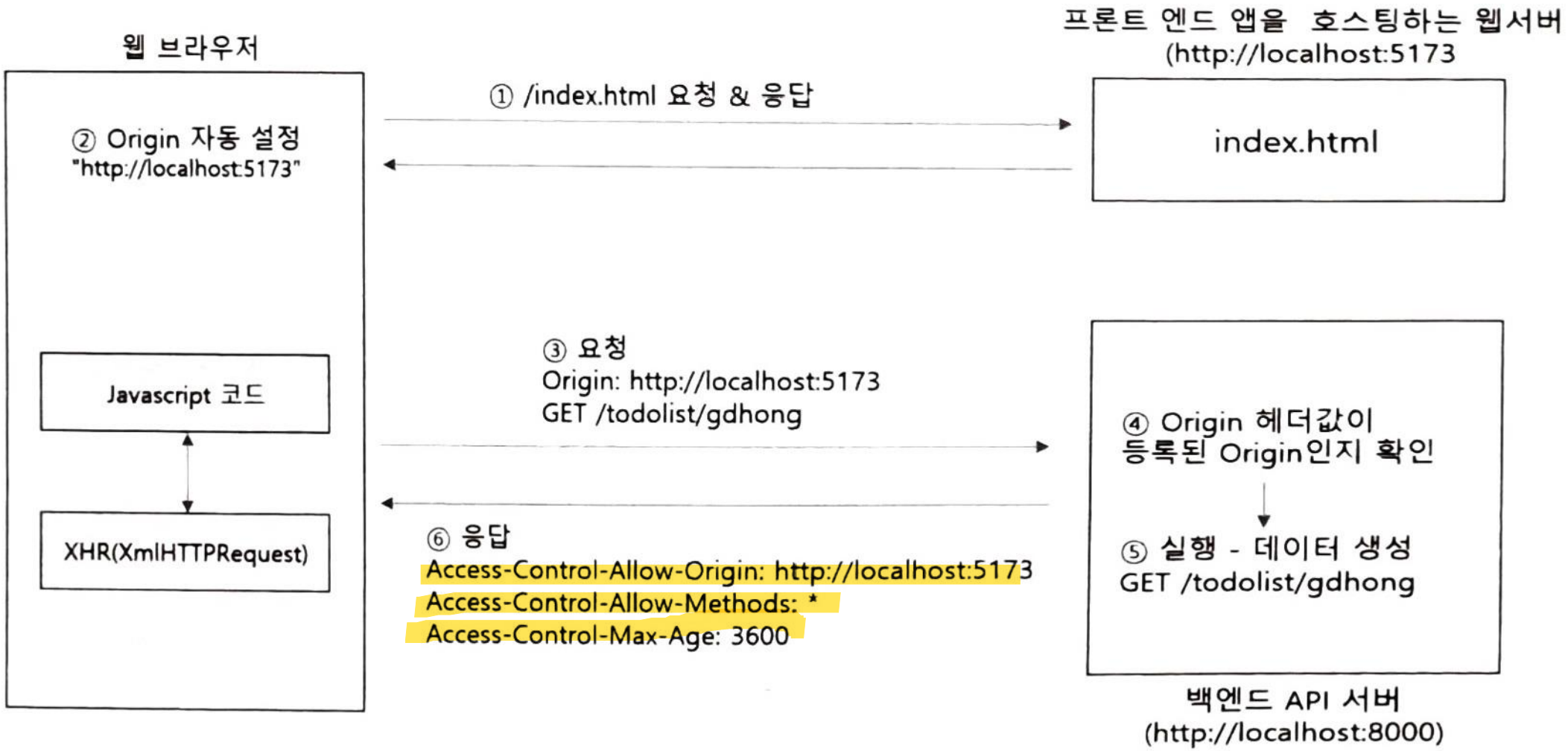
임시적인 방법.
개인 백엔드가 없을 때
프론트에 남의 서버(json-sever)
임시 개발서버를 활용할때
외부니까 크로스 오리진 문제가
발생함.

json-server와 프론트 사이에
우리만의 개발서버를 생성하고
개발서버에 프록시를 활용하여
vue프론트->개발서버(프록시)->json-server
json-server->개발서버(포트포워딩)->vue프론트

이렇게 하면 크로스 오리진 문제 해결~

CORS(Cross Origin Resource Sharing)

- 서버가 응답할 때 Access-Control-Allow-Origin HTTP 헤더로 Origin이 달라도 통신을 허용



프록시를 이용한 우회

- 프론트엔드 앱의 입장에서는 동일한 Origin으로 통신
- 개발용 웹 서버가 대신 통신을 중개해 줌