

업무 생산성 개선

AI 개발 오류 조사에 구조화 응답 대체 경로와 인용 검증을 적용한 사례

AI 요약이 없으면 멈추고, 안전한 요약과 HTTPS 인용을 확보한 경우에만 결과를 보여주도록 개발 오류 조사 흐름을 개선했다.

활용한 AI 도구

Google AI Mode(SerpApi Google AI Mode API로 호출)

1. 어떤 상황에서 AI를 활용했나

개발 오류 조사에 AI를 활용할 때 문제는 답변 구조가 예상과 다를 수 있다는 점이다. 요약이나 출처가 비어 있는 데도 그럴듯한 답변 남을 수 있다. 나는 Google AI Mode를 호출하는 작은 조사 도구 PatchSignal을 직접 만들고, 안전한 요약과 HTTPS 인용을 함께 확보한 경우에만 결과를 보여주도록 고쳤다.

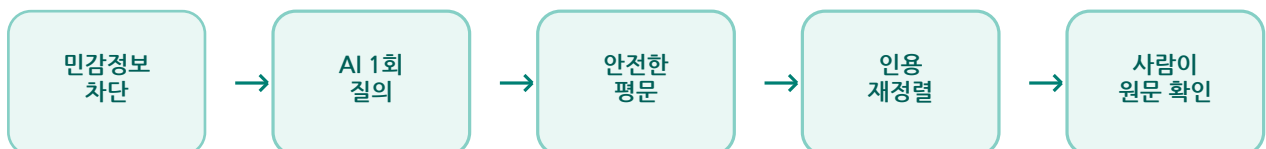
첫 실사용은 Node.js 22 관련 오류였다. 라이브 호출은 1회 성공했지만 쓸 수 있는 요약 필드가 없었다. 안전한 요약과 인용은 모두 0건이었다. 재시도 없이 멈췄다. 이 실패로 하나의 응답 형식만 믿는 방식은 실제 조사에서 깨질 수 있다는 점을 확인했다.

2. 어떤 AI를 어떻게 활용했나

PatchSignal은 오류 설명, 기술 생태계, 버전을 받아 Google AI Mode에 한 번 묻는다. 질문에는 가능한 원인과 안전한 확인 절차를 설명하되 공식 문서와 릴리스 노트를 인용하고, 근거 없이 확정하거나 실행 명령을 주지 말라는 조건을 넣었다.

응답은 곧바로 답으로 쓰지 않는다. 먼저 reconstructed_markdown을 확인하고, 이 값이 없으면 공식 문서에 나온 text_blocks에서 허용한 제목, 문단, 목록 등의 구조만 읽는다. 코드 블록, 링크, 서식은 제거하며 최대 900자의 평문만 남긴다. 이어서 AI가 돌려준 인용 중 HTTPS 주소만 받는다. 공식 문서인지, 입력 버전과 맞는지, 오류 용어가 들어 있는지, 날짜가 있는지, 같은 도메인에 치우치지 않았는지를 따로 계산해 순서를 다시 매긴다. 안전한 요약이나 인용이 없으면 결과를 내지 않는다.

처리 순서



3. 활용 결과 어떤 변화가 있었나

구조화 텍스트 대체 경로를 추가한 뒤, 다른 사전등록 사례인 Java 21 오류로 라이브 호출을 1회 진행했다. 안전한 요약 1건과 HTTPS 인용 8건을 확보했고, 상위 3개 안에 공식 문서 1건이 들었다. 독립 순위 계산에서는 Oracle 공식 문서가 첫 번째였다. 테스트는 20개에서 24개로 늘었고, 입력 차단과 요약 추출, HTTPS 인용, 공식 문서 순위, 출력 누락 시 중단을 함께 확인했다.

검증	라이브 호출	안전한 요약	HTTPS 인용	공식 문서 상위 3개	테스트	판정
첫 확인 Node.js 22	1회	0건	0건	-	20개	중단
대체 경로 후 Java 21	1회	1건	8건	1건	24개	통과

주의: 두 행은 서로 다른 사전등록 사례다. 동일 입력 A/B 비교나 정확도 향상 수치가 아니다.

첫 확인과 두 번째 확인은 서로 다른 사전등록 사례다. 따라서 같은 입력을 전후로 비교한 A/B 결과나 정확도 향상 수치로 해석하지 않는다. 확인된 변화는 유효한 다른 응답 형식을 받아들이면서도 안전 조건을 유지했고, 새 사례에서 끝까지 결과를 만들었다는 점이다.

4. 나만의 방식과 개선 포인트

가장 큰 차이는 AI 답변과 출처 감사를 분리한 것이다. AI가 만든 요약은 참고용 평문으로만 다루고, 인용 주소의 공식성, 버전 일치, 문제 관련성, 날짜, 도메인 다양성은 별도 규칙으로 계산한다. 답변이 자연스러워 보여도 출처가 없으면 멈춘다.

개인정보와 실행 위험도 입력부터 줄였다. 이메일, 로컬 기기 경로, 자격증명 표기, 긴 토큰 형태의 문자열은 검색 전에 차단한다. AI가 돌려준 코드 블록과 원시 링크는 요약에서 뺀다. 후보 페이지를 자동으로 방문하거나 명령을 실행하지 않으며, API 키는 브라우저로 보내지 않는다. 마지막 판단은 사람이 원문을 읽은 뒤 내린다.

5. 다른 사람도 따라 할 수 있나

- 1 오류 메시지에서 이메일, 사용자 경로, 토큰을 지우고 문제 설명과 버전을 짧게 정리한다.
- 2 AI에 가능한 원인과 확인 절차를 묻되 공식 문서와 릴리스 노트를 함께 요구한다.
- 3 응답을 평문으로 바꾸고 코드, 링크, 서식을 제거한다. 안전한 요약이 없으면 여기서 멈춘다.
- 4 AI가 반환한 HTTPS 인용만 모아 공식성, 버전, 오류 용어, 날짜, 도메인 다양성을 확인한다.
- 5 상위 출처의 원문을 사람이 읽고 실제 조치 여부를 정한다.

네트워크 없이 실행하는 24개 테스트에는 중복 JSON 키, 이메일과 로컬 경로 차단, 자격증명 형태 차단, 평문 요약 길이, 코드 블록 제거, HTTPS 인용, 공식 문서와 버전 순위, 도메인 다양성, 요약 또는 인용 누락 시 중단이 포함돼 있다. 출처를 돌려주는 다른 AI 서비스에도 같은 점검 순서를 적용할 수 있지만, 응답 구조에 맞춘 별도 검증은 필요하다.

책임 있는 활용과 한계

이 사례에서 AI는 결론을 내리지 않고 조사 초안을 만든다. 인용이 있다는 사실만으로 답이 맞다고 보지 않으며, 공식 문서도 현재 환경과 버전에 맞는지 다시 읽는다. 라이브 검증은 서로 다른 사전등록 사례에서 각 1회 진행했으므로 일반적인 정확도나 처리시간 개선을 주장하지 않는다. 적용의 중심은 실패 시 멈추고, 출처를 다시 확인한 뒤 사람이 결정할 수 있게 한 업무 흐름이다.