AI 에이전트 권한 점검표 · 10분

메일·카드 연결한 AI, 돈·정보 안 새는 설정 5개

유튜브 「인공지능 한이룸」 영상의 무료 점검표입니다. 사고 5건마다 바꿀 설정 1개씩, 메뉴 위치 그대로 적었어요. 위에서부터 칸을 체크하세요.

1 기본값을 「항상 묻기」로

「항상 허용」은 그 종류의 행동 전부를 허락하는 버튼입니다. (집 주소가 나간 사고)

- ☐ 챗GPT **설정 › 클라우드 컴퓨터 › 웹사이트 승인** 을 **항상 묻기**로 (칸: 항상 묻기 · 자동 승인 · 항상 허용)
- ☐ 판매자센터와 메일은 허용 목록에 넣지 않기
- ☐ 허락 창이 뜨면 **「한 번만 허용」** 선택

2 한도를 걸고, 「강제로 멈춤」까지 켜기

알림만 오는 한도는 멈추지 않습니다. 저는 5달러 한도를 걸고 하루 7.53달러가 나갔어요. (자고 일어나니 230만 원 청구된 사고)

- ☐ 오픈AI 프로젝트 설정 **Limits** → 월 한도 입력 → **Enforce a hard limit** 켜기
- ☐ 구글 AI 스튜디오 **Spend** 메뉴에서 월 한도
- ☐ 앤스로픽 콘솔은 워크스페이스마다 월 지출 한도 따로 설정
- ☐ API 키를 붙여 둔 도구(상품설명 자동화, n8n 등) 목록 적어 보기

3 안 쓰는 연결은 양쪽에서 끊기

한쪽만 끊으면 반만 끊긴 겁니다. (연결된 메일이 남의 계정으로 건너간 연구진 시연)

- ☐ 챗GPT **설정 › 플러그인** 에서 안 쓰는 연결 해제
- ☐ 구글 계정 **타사 앱 및 서비스** 에서 챗GPT 권한 삭제
- ☐ 챗GPT **설정 › 데이터 관리 › 공유 링크** 에서 예전 대화 링크 삭제

4 AI에게는 좁은 권한의 계정을 따로

본계정으로 로그인한 AI는 대표님이 하는 일을 전부 할 수 있습니다. (거절을 피해 비공개 파일까지 연 내부 시험)

- ☐ 스마트스토어센터 **판매자 정보 › 매니저 관리** 에서 맡길 일에 맞는 **좁은 권한**의 매니저 초대 (주매니저 말고)
- ☐ AI는 그 계정으로만 로그인
- ☐ 일이 끝나면 챗GPT **설정 › 클라우드 컴퓨터 › 쿠키 › 모두 지우기** (모든 사이트에서 로그아웃)

5 끄는 곳 세 군데를 미리 열어 보기

일시정지는 지금 하는 일 하나만 멈춥니다. 예약 작업은 그대로 돌고, 이미 나간 메일은 회수가 안 됩니다.

- ☐ 닷츠의 **일시 중지 버튼** 위치 확인
- ☐ **최근 활동** 화면 열어 보기
- ☐ **예약** 화면 열어 보기 (다른 에이전트는 예약 목록이 어디 있는지 먼저 찾아 두기)

에이전트 지침에 붙여 넣는 한 줄

「보내기, 결제, 개인정보는 하기 전에 나에게 먼저 물어볼 것.」

메뉴 이름은 2026년 11월 화면 기준이라 서비스가 바뀌면 달라질 수 있어요. 오픈AI·구글·앤스로픽 한도 메뉴와 스마트스토어센터 화면은 각 서비스 안내를 함께 확인하세요. © 인공지능 한이룸 · irumhahn.com