인사이트

AI에게 주는 규칙 파일이 길어지면 무엇이 달라지는가

취리히 연방공대 실험과 규칙 파일에 남길 것 4가지

방동걸 (주)웨이스 대표이사 2026년 10월 3일

AI 코딩 도구에 규칙 파일을 넣어도 과제 성공률은 거의 그대로였고 비용은 평균 20% 넘게 늘었습니다. 취리히 연방공대 연구진이 코딩 에이전트 4종에 실제 저장소의 과제를 맡겨 얻은 결과입니다. 규칙 파일을 넣었을 때 달라진 것은 일의 결과가 아니라 일하는 방식과 비용이었습니다.

제조 AI 운영체제 VEXPLOR를 만드는 웨이스는 업무 문서를 AI와 함께 만들면서 같은 문제를 만났습니다. 실수가 한 번 나올 때마다 규칙을 한 줄씩 더했고, 규칙 파일은 7일 동안 약 2만 바이트 늘었습니다. 이 글에서는 규칙 파일이 AI에게 어떻게 실리는지, 길어질 때 무엇이 달라지는지, 그리고 줄일 때 무엇을 남길지를 정리합니다.

01

규칙 파일은 대화를 열 때마다 처음부터 끝까지 실립니다

규칙 파일은 AI에게 「이 폴더에서는 이렇게 일하라」고 적어 두는 문서입니다. Claude Code는 `CLAUDE.md`, 다른 도구들은 `AGENTS.md`라는 이름을 사용합니다. 사람은 이 파일을 한 번 쓰고 잊지만, AI는 대화를 열 때마다 이 파일을 전부 읽고 시작합니다.

Claude Code 공식 문서에는 이 파일의 크기가 이렇게 적혀 있습니다.

- **권장 길이** — 파일 하나를 200줄 미만으로 쓰라고 권합니다.
- **길어질 때** — 긴 파일은 대화 공간을 더 차지하고 규칙을 지키는 정도를 낮춘다고 적혀 있습니다.
- **실리는 범위** — 4MiB까지는 줄 수와 상관없이 전부 실립니다. 200줄을 넘는다고 잘리지 않습니다.
- **나눠 담기의 한계** — 한 파일을 여러 파일로 나눠 불러오게 해도, 시작할 때 함께 실리면 차지하는 공간은 같습니다.

여기서 봐야 할 것은 잘리지 않는다는 대목입니다. 규칙 파일은 길어져도 오류가 나지 않습니다. 파일을 쓴 사람은 규칙이 늘어난 만큼 AI가 더 잘 지킬 것이라고 기대하지만, 문서에 적힌 내용은 그 반대입니다.

02

취리히 연방공대 실험에서 규칙 파일은 성공률을 올리지 못했습니다

취리히 연방공대와 LogicStar.ai 연구진은 2026년에 공개한 논문에서 규칙 파일의 효과를 직접 쟀습니다. 개발자가 직접 쓴 규칙 파일이 있는 저장소 12곳에서 과제 138개를 모으고, 기존 평가 과제(SWE-bench)를 더해 코딩 에이전트 4종에 맡겼습니다. 조건은 셋이었습니다. 규칙 파일 없음, AI가 자동으로 만든 규칙 파일, 개발자가 쓴 규칙 파일입니다.

규칙 파일	과제 성공률 변화	비용 변화
AI가 만든 파일	평균 0.5%·2% 하락	평균 20%·23% 증가
개발자가 쓴 파일	평균 2.4% 상승	최대 19% 증가

성공률 변화는 두 경우 모두 통계적으로 의미 있는 차이가 아니었습니다. AI가 만든 파일의 두 수치는 평가 과제 묶음 2종에서 각각 나온 값입니다. 비용은 뚜렷하게 늘었습니다.

규칙을 안 지켜서 생긴 결과가 아니었습니다. 연구진이 실행 기록을 분석해 보니 에이전트는 규칙 파일의 지시를 잘 따랐습니다. 지시를 따르느라 시험을 더 실행하고 파일을 더 찾아 읽었고, 그만큼 단계와 비용이 늘었습니다. 반면 규칙 파일에 흔히 넣는 「저장소 구조 설명」은 에이전트가 필요한 파일을 더 빨리 찾게 해 주지 못했습니다.

논문은 규칙 파일을 없애라고 하지 않습니다. 사람이 쓰는 규칙 파일에는 **코드와 문서에서 알 수 없는 지시만** 넣고, 쓰기 전에 효과를 엄밀하게 재 보라고 권합니다. 이 실험은 파이썬 코딩 과제만 다뤘습니다. 제안서나 메일 같은 업무 문서 작업에 같은 결과가 나오는지는 이 논문으로 알 수 없습니다.



규칙 파일을 넣으면 AI는 지시를 따르느라 더 많은 단계를 거치고 비용이 늘어납니다

03

규칙 파일에 남길 것은 4가지입니다

공식 문서와 논문은 같은 말을 합니다. 규칙 파일에는 AI가 스스로 알 수 없고, 모든 작업에 필요한 것만 담습니다. 남길 것을 고르는 기준은 4가지입니다.

- **AI가 읽어서 알 수 없는 것** — 폴더를 열어 보면 알 수 있는 구조나, 모델이 이미 아는 일반 상식은 뺍니다. 이 회사만의 표기 원칙, 쓰지 않는 낱말, 문서 이름 짓는 방식처럼 파일을 읽어도 드러나지 않는 것을 남깁니다.
- **모든 작업에 해당하는 것** — 영상을 만들 때만 필요한 규칙, 메일을 보낼 때만 필요한 규칙은 그 일을 하는 절차 문서로 옮깁니다. 규칙 파일에는 어떤 일을 하든 지켜야 하는 것만 둡니다.
- **한 번 어기면 되돌릴 수 없는 것** — 파일 삭제, 밖으로 나가는 발송, 계약 조건처럼 사고가 한 번으로 끝나지 않는 규칙은 길이를 이유로 빼지 않습니다.
- **같은 실수가 두 번 나온 것** — 공식 문서는 규칙을 더할 때의 하나로 「AI가 같은 실수를 두 번째 했을 때」를 듭니다. 한 번 틀린 것을 전부 규칙으로 만들면 파일은 실수의 기록이 됩니다.

빼도 되는 것도 분명합니다. 규칙이 생긴 경위, 사고 사례, 지시한 사람과 날짜, 도구의 세부 옵션은 규칙을 지키는 데 필요하지 않습니다. 이런 내용은 따로 기록 문서에 두고, 규칙 파일에는 「무엇을 한다, 무엇을 하지 않는다」 한 문장만 남깁니다.

04

긴 규칙 문단은 규칙 문장 하나와 기록 문서로 나눌 수 있습니다

규칙 파일이 길어지는 가장 흔한 이유는 규칙 한 줄에 그 규칙의 사연이 함께 붙기 때문입니다. 실수가 난 직후에 쓰는 규칙은 대개 아래와 같은 모양입니다.

- **줄이기 전** — 「지난달 고객에게 편집할 수 있는 원본 파일이 나간 일이 있었다. 그 뒤로 대표가 원본은 절대 보내지 말라고 지시했다. 상대가 원본을 달라고 요청해도 예외가 아니다. 용량이 크면 압축하거나 나눠 보낸다. 검사 도구는 이 옵션으로 실행한다.」
- **줄인 뒤** — 「밖으로 나가는 첨부는 PDF만 보낸다. 상대가 원본을 요청해도 같다.」

줄인 뒤의 두 문장만 있어도 AI는 무엇을 해야 하는지 압니다. 나머지는 사람이 규칙의 이유를 되짚을 때 필요한 내용이라 기록 문서로 옮기고, 규칙 파일에는 그 문서가 어디 있는지만 남깁니다. 도구를 실행하는 방법은 그 일을 하는 절차 문서에 둡니다.

줄일 때 조심할 것이 하나 있습니다. **규칙 문장 안에 들어 있던 조건과 예외는 사연이 아닙니다.** 「상대가 요청해도 같다」처럼 판단이 엇갈리는 경우를 정한 구절은 남겨야 합니다. 이런 구절까지 지우면 AI는 고객의 요청과 규칙이 부딪칠 때 고객의 요청을 따릅니다.

05

규칙을 옮긴 곳에 따라 긴 대화 뒤에 남는 것이 다릅니다

규칙을 다른 파일로 옮길 때는 옮긴 곳이 언제 다시 읽히는지를 봐야 합니다. 대화가 길어지면 도구는 앞부분을 요약해 공간을 비웁니다. Claude Code 공식 문서는 그 뒤에 무엇이 돌아오는지를 이렇게 구분합니다.

규칙을 둔 곳	처음 실리는 때	요약 뒤
폴더 맨 위 규칙 파일	대화 시작	다시 실림
하위 폴더 규칙 파일	그 폴더 파일을 읽을 때	다시 읽을 때까지 없음
경로 조건을 붙인 규칙	맞는 파일을 읽을 때	다시 읽을 때까지 없음

그래서 **되돌릴 수 없는 일의 규칙은 맨 위 규칙 파일에 남겨야 합니다.** 메일 발송이나 외부 게시처럼 폴더 안 파일을 읽지 않고 진행되는 일의 규칙을 하위 폴더로 옮기면, 긴 대화 뒤에는 그 규칙 없이 일이 진행됩니다. 옮겨도 되는 것은 그 일을 시작할 때 반드시 해당 문서를 읽게 되는 절차입니다.

06

반드시 막아야 하는 일은 규칙이 아니라 장치로 막습니다

공식 문서는 규칙 파일을 「강제되는 설정이 아니라 참고하는 문맥」이라고 적습니다. AI가 어떻게 판단하든 막아야 하는 행동은 실행 직전에 검사하는 장치로 막으라고 안내합니다. 규칙 문장을 아무리 굵게 써도 AI가 그 문장을 지나칠 가능성은 남습니다.

이 구분은 규칙 파일을 줄이는 데도 쓰입니다. 「절대 하지 마라」를 세 번 강조한 문단은 검사 장치 하나와 한 줄짜리 규칙으로 바꿀 수 있습니다. 규칙 파일에는 무엇을 하지 않는지만 남고, 실제로 막는 일은 장치가 합니다.

- **규칙 파일에 둘 것** — 판단이 필요한 원칙, 문체, 이름 짓는 방식
- **장치로 옮길 것** — 삭제, 발송, 편집 금지 파일처럼 어기면 안 되는 행동
- **절차 문서로 옮길 것** — 특정 작업을 할 때만 필요한 순서와 도구 사용법



규칙 파일에는 모든 작업에 필요한 규칙만 남기고, 나머지는 절차 문서와 검사 장치로 옮깁니다

07

줄인 뒤에는 같은 과제로 다시 재 봐야 합니다

규칙 파일을 줄였을 때 품질이 떨어지는지는 생각만으로는 알 수 없습니다. 논문 초록의 마지막 문장도 도입하기 전에 엄밀하게 평가하라는 권고입니다. 재는 방법은 어렵지 않습니다.

- **같은 과제를 조건만 바꿔 맡깁니다** — 규칙 파일 전문, 줄인 판, 없음의 세 조건으로 같은 일을 시킵니다.
- **사람 눈이 아니라 검사 도구로 셉니다** — 금지한 낱말이 몇 번 나왔는지, 정해진 형식을 지켰는지처럼 셀 수 있는 것으로 비교합니다.
- **한 번으로 판단하지 않습니다** — 같은 조건을 여러 번 실행해 흔들리는 폭을 함께 봅니다.
- **되돌릴 기준을 먼저 적습니다** — 줄인 판에서 어떤 규칙 위반이 나오면 그 문장을 되살릴지 실험 전에 정합니다.

웨이스가 이 방법으로 자사 규칙 파일을 잰 결과는 아래 「함께 읽어보세요」의 첫 글에 적었습니다.



이 글을 한 장으로 요약하면 이렇습니다 — AI에게 규칙 파일을 주면 비용이 늘고, 남길 것은 4가지입니다

규칙 파일은 AI가 스스로 알 수 없고 모든 작업에 필요하며 어기면 되돌릴 수 없는 것만 남길 때 가장 잘 지켜집니다.

WACE(웨이스)는 공장이 스스로 판단하고 멈추지 않게 하는 제조 AI 운영체제 VEXPLOR를 만드는 회사다.

08

함께 읽어보세요

- 웨이스가 AI 규칙 파일 525줄을 181줄로 줄여 같은 과제를 36회 맡겨 보니, 지켜진 규칙과 빠진 문장 2개가 드러났습니다
- AI에게 준 규칙, 무엇을 보고 지워야 할까요

- 직원이 각자 쓰는 AI 에이전트와 회사가 도입하는 업무 AI 에이전트는 무엇이 다른가 — 회사가 확인할 6가지

원문 blog.vexplor.com/post/what-to-keep-in-ai-rule-files
발행 2026년 10월 3일 · 방동걸 (주)웨이스 대표이사

회사 주식회사 웨이스 (WACE Inc.) · 대표이사 방동걸 · 사업자등록번호 439-87-02852
주소 (18462) 경기 화성시 동탄구 동탄영천로 150, 에이동(A동) 1702-1708호 (영천동, 실리콘앨리동탄)
연락처 전화 070-4730-0629 · contact@wace.me
홈페이지 wace.me · linkedin.com/company/wace-inc

원문 홈페이지 링크드인