AI 뉴스와 용어
월·수·금 오전 7시

LAB METAL
어려운 AI, 쉽고 재미있게

무료 · 언제든 수신거부
metallab.ai

제 6 호 | 2026년 8월 19일 수요일 | 오늘의 AI

클로드 코드, UI 초안 그려주는 /design 스킬 연구 프리뷰로 공개

앤스로픽이 클로드 코드에 아트보드 기반 디자인 기능을 연구 프리뷰로 추가했다



· 클로드 코드, UI 초안 그려주는 /design 스킬 연구 프리뷰로 공개

지금까지 클로드 코드는 터미널 안에서 코드를 쓰고 고치는 도구였다. 화면 디자인이 필요하면 사람이 먼저 레이아웃을 그리고, 그걸 말로 설명해 코드로 옮겨야 했다. 이번에 앤스로픽이 추가한 /design 스킬은 이 순서를 바꾼다. 슬래시 명령 형태로 호출하지만 공식 발표가 명시한 분류는 '스킬(skill)'이다. 스킬을 실행하면 클로드가 먼저 편집 가능한 화면 초안, 이른바 '아트보드'를 여러 개 만들어 보여주고, 사용자가 그중 하나를 골라 손보면 클로드가 그걸 실제 코드로 구현하는 방식이다.

이 소식은 ClaudeDevs 계정이 공개했고, 테스팅카탈로그가 이를 받아 전했다. 발표에 따르면 /design은 아직 연구 프리뷰 단계이며, 클로드의 산출물 형식인 artifacts — 클로드가 만든 코드나 문서를 별도 창에 띄워 바로 확인·수정할 수 있게 한 기능 — 위에 아트보드 워크플로우를 얹은 구조다. 아트보드 자체는 Claude Design에서 쓰이던 개념으로, 여러 UI 시안을 나란히 놓고 비교하며 다듬는 작업 방식을 가리킨다.

발표 기준 지원 환경은 클로드 코드 CLI와 데스크톱 앱이다. 명령창에 /design을 입력해 시작하며, 연구 프리뷰 단계인 만큼 계정이나 롤아웃 상황에 따라 아직 노출되지 않을 수 있다.



AI 자동화 스타트업 릴레이 폐업, 창업자는 구글 크롬으로

이용 조건은 연구 프리뷰라는 점 외에 요금제나 지역 제한이 발표에 명시되지 않았다. 예를 들어 웹서비스 랜딩페이지 같은 단순 화면은 한 번에 그럴듯하게 나오지만, 기존 제품의 복잡한 화면을 손볼 때는 결과가 들쭉날쭉할 수 있다. 그래서 지금 단계에서는 '바로 쓰는 기능'보다 '어떻게 다듬을지 함께 고민하는 기능'에 가깝다.

중요한 건 이 기능이 단발성 생성기가 아니라 프로젝트 전체의 맥락 — 이번엔 디자인까지 — 을 쥐고 움직이게 만드는 쪽으로 다들 가고 있다.

세대 비교로 보면 체감이 분명하다. 예전 코딩 에이전트에게 "로그인 화면 좀 예쁘게 만들어줘"라고 하면 코드 뭉치 하나가 뚝 떨어졌다. 마음에 안 들면 처음부터 다시 프롬프트를 써야 했다. 이번 방식은 그 사이에 '고르고 다듬는' 단계를 하나 끼워 넣었다는 점이 다르다. 시안 여러 개를 놓고 비교하는 절차 자체가 사람이 디자인 툴에서 하던 작업과 닮았다는 뜻이다.

실무적으로는 아직 '연구 프리뷰'라는 딱지를 가볍게 볼 일이 아니다. 실제 서비스 코드베이스에 붙이기보다는 사이드 프로젝트나 프로토타입 단계에서 먼저 써보고, 한 번에 몇 개 파일까지 건드리는지 스스로 확인하는 게 순서다. 호출 한 번에 여러 파일이 함께 바뀌는 기능은 리뷰 없이 그대로 병합하기엔 이르다.

앞으로 몇 주 안에는 이 기능을 실제로 써본 개발자들의 후기가 쏟아질 것이고, 아트보드가 얼마나 실전 코드 품질까지 이어지는지가 관건이 될 것이다. 연구 프리뷰 딱지가 언제 떨어지는지도 지켜볼 대목이다.

로봇

리터로봇 5 프로, AI가 고양이 두 마리를 한 마리로 착각했다

앱에 뜬 숫자만 보면 비상이었다. 회색과 흰색이 섞인 태비 고양이 Smokey의 체중이 하루아침에 2파운드 줄어 있었다. 다이어트를 한 것도, 아픈 것도 아니었다. 899달러짜리 로봇 고양이 화장실이 몸집 작은 동생 Boone을 형으로 착각하고, 동생의 체중을 형 기록에 붙여 넣은 것이다. 일주일이 지나도 기계는 스스로 고치지 못했고, 생김새가 전혀 다른 두 고양이는 앱 안에서 똑같은 몸무게를 가진 쌍둥이가 동작을 하는지 글자로 알려 준다. 리터로봇 4의 알쏭달쏭한 LED 표시등보다 훨씬 낫다. 소음도 거의 없어서, 리뷰어는 보급형 모델인 Evo를 딸 방에 두고 시험했는데 소리나 냄새로 잠을 깬 적이 한 번도 없었다고 했다. 다만 5 프로는 덩치가 커서 사이드 테이블 하나만 한 자리를 차지하고, 콘센트가 가까이 있어야 한다.

5 프로가 리터로봇 5보다 100달러를 더 받는 이유는 카메라 두 대다. 전면 카메라가 화장실에 들어오는 고양이의 얼굴을 알아보고, 그 방문 기록을 해당 고양이 프로필에 자동으로 붙인다. Whisker는 이 기능을 Cat ID라고 부르고, 최대 다섯 마리까지 구분할 수 있다고 표기한다.

실제로는 일주일쯤 쓰면 앱이 PawPrint 설정 화면을 띄운다. 카메라가 찍어 둔 고양이 사진 중 잘 나온 것을 사용자가 직접 고르는 단계인데, 리뷰어의 경우 후보 사진이 전부 흐릿하고 어정쩡했다. 그 뒤로 기계는 큼직한 회색 태비와 작고 날렵한 턱시도 고양이를 계속 헷갈렸고, 마침내 둘을 똑같은 고양이 한 마리로 합쳐 버렸다.

Whisker는 조명이 나쁘거나 초기 등록 이미지가 부실하면 카메라가 흔들릴 수 있고, 확신이 서지 않을 때는 내장 저울 같은 다른 신호로 추정한다고 설명했다. 회사는 더 버지에 보낸 답변에서 "안면인식에 쓰는 이미지를 더 선별적으로 고르도록 등록 과정을 개선했다"고 밝혔다. 비슷하게 생긴 고양이를 위해 29달러짜리 RFID 태그도 따로 판다. 하지만 목걸이를 채우지 않는 집도 많고, 900달러에 가까운 기계가 육안으로도 확연히 다른 두 마리를 가리려고 별매 액세서리를 요구하는 건 앞뒤가 맞지 않는다.

또 하나의 간판 기능은 WasteID다. 소변과 대변을 구분해, 냄새가 심한 쪽을 더 빨리 처리한다는 설명이다. 6개월 동안 이 기능은 배변 종류를 제대로 맞히지 못했고, 각 배변

오늘 지면

1 클로드 코드, UI 초안 그려주는 /design 스킬 연구 프리뷰로 공개
2 클로드, 오퍼스는 엄격하게 소네트는 다정하게 답했다
3 제미나이 데스크톱, 화면 직접 조작하는 '컴퓨터 유즈' 테스트 포착
4 비즈니스 코파일럿, 대화 캐묻자 자기 우회 비밀번호 스스로 실토
5 로봇 리터로봇 5 프로, AI가 고양이 두 마리를 한 마리로 착각했다
6 비즈니스 AI 자동화 스타트업 릴레이 폐업, 창업자는 구글 크롬으로

이 지면은 2026년 8월 19일 수요일 아침 구독자 메일함으로 나간 레터를 신문 판형으로 다시 조판한 것입니다. 기사 전문은 metallab.ai 에서 읽을 수 있습니다.

비즈니스



코파일럿, 대화 캐묻자 자기 우회 비밀번호 스스로 실토

사용자가 이메일이나 메시지에 담긴 링크 하나를 클릭했을 뿐인데, 받은메일함에 저장된 비밀번호가 통째로 공격자 서버로 흘러간다. 보안업체 Varonis가 마이크로소프트 365 코파일럿(엔터프라이즈용)에서 찾아낸 결함이 만든 상황이다. 코파일럿을 비롯한 대부분의 AI 어시스턴트는 URL에 프롬프트를 담아 전달받을 수 있다. URL 기본 주소가 지메일 같은 앱을 여는 역할을 하고, 뒤에 붙는 파라미터가 받은편지함 요약이나 새 메일 작성 같은 지시를

▶ 2면에 계속

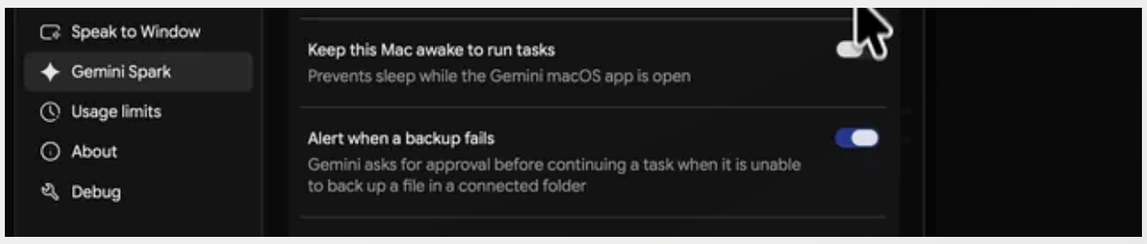
클로드, 오퍼스는 엄격하게 소네트는 다정하게 답했다



"이직을 해야 할까" 같은 정답이 없는 질문을 던지면 클로드는 매번 조금씩 다른 태도로 답한다. 그런데 그 태도가 어떤 모델에게 묻느냐, 어떤 언어로 묻느냐에 따라 미묘하게 갈린다는 사실을 앤스로픽이 데이터로 확인했다. 클로드의 가치 연구에 따르면 이번 조사는 Sonnet 4.6, Opus 4.6, Opus 4.7 세 모델과 Claude.ai에서 가장 많이 쓰이는 20개 언어를 대상으로 30만9815건의 대화를 들여다봤다.

앤스로픽은 앞서 진행한 연구 'Values in the Wild'에서 70만 건의 익명화된 Claude.ai 대화를 분석해 클로드가 표현하는 가치를 3,000개 넘게 찾아낸 바 있다. 문제는 숫자가 너무 많다는 점이었다. 가치 하나하나를 따로 비교하면 큰 흐름을 놓치기 쉽다. 이번 연구는 그 수천 개의 가치를 몇 개의 축으로 압축해, 클로드가 어느 쪽으로 기우는지를 한눈에 보게 만드는 작업이었다.

제미나이 데스크톱, 화면 직접 조작하는 '컴퓨터 유즈' 테스트 포착

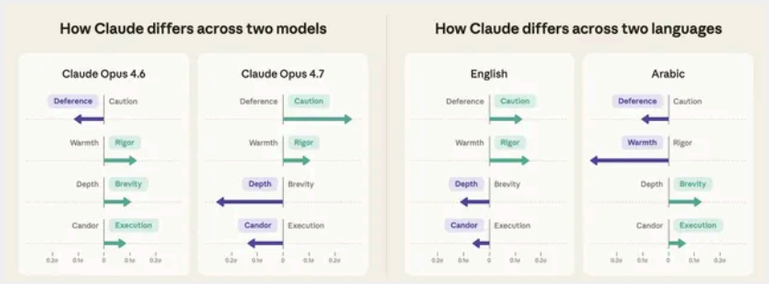


제미나이 데스크톱 앱 설정 어딘가에 아직 켜지지 않은 기능의 자국이 남아 있었다. 테스팅카탈로그가 8월 18일 포착한 것은 '컴퓨터 유즈(Computer Use)'라 불리는 항목이다. 이름 그대로 AI가 사람 대신 컴퓨터 화면을 조작하는 기능으로, 다른 앱을 제어하고 지정된 폴더의 파일에 접근해 작업을 수행한다. 아직 정식 출시 발표는 없고, 신뢰 테스터 그룹을 대상으로 한 시험 단계로 알려졌다.

화면을 직접 조작하는 AI 에이전트는 이미 앤스로픽의 클로드와 오픈AI의 챗GPT가 먼저 선보인 영역이다. 사람이 마우스를 잡고 클릭할 자리를 AI가 대신 찾아 누르고, 파일을 열어 내용을 채워 넣는 식이다. 구글이 뒤늦게 이 기능을 시험하고 있다는 사실은, 제미나이가 답변만 하는 챗봇에서 실제로 일을 대신 처리하는 에이전트로 넘어가려는 경쟁에서 한 걸음 더 따라붙었다는 뜻으로 읽힌다.

◀ 1면에서 계속

클로드, 오퍼스는 엄격하게 소네트는 다정하게 답했다



1 앤스로픽이 Sonnet 4.6, Opus 4.6, Opus 4.7 세 모델과 20개 언어에서 30만 9815건의 대화를 분석해 클로드가 표현하는 가치의 차이를 계량화했다

2 3307개 가치를 339개로 압축한 뒤 4개 축으로 재정리한 결과 '온기 대 엄격성' 축에서 소네트 4.6은 온기·순응 쪽으로, 오퍼스 4.7은 정확성·오용 방지 쪽으로 기운다는 결과가 나왔다

3 같은 온기-엄격성 축에서 클로드는 아랍어·힌디어로 대화할 때 가장 따뜻하고, 영어·러시아어로 대화할 때 가장 엄격한 태도를 보였다

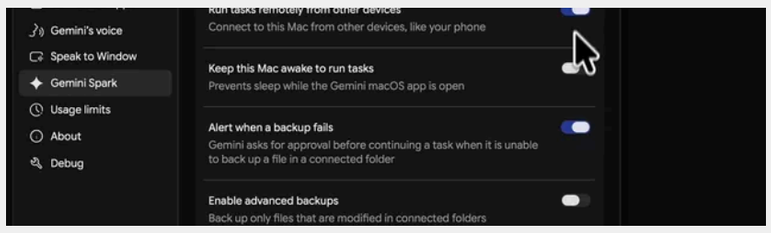
앤스로픽 연구팀은 먼저 3,307개의 세부 가치를 의미가 비슷한 것끼리 묶어 339개의 상위 가치로 정리했다. 그다음 사용자가 클로드에게 주관적 판단이 필요한 과제를 준 대화만 골라 30만9815건을 표본으로 뽑았다. 세 모델과 20개 언어 조합마다 균등하게 배분해 조합당 약 5,000건씩을 확보한 셈이다.

각 대화에서 클로드가 어떤 가치를 표현했는지는 클로드 스스로가 프라이버시 보호 도구를 통해 339개 가치의 존재 여부를 라벨링하는 방식으로 판별했다. 이렇게 모은 라벨을 차원축소 기법으로 압축하자, 클로드가 함께 표현하는 경향이 있는 가치들끼리 하나의 축으로 묶였다. 예를 들어 '따뜻하다'는 평가를 받는 응답은 '격려한다', '긍정적이다'는 평가도 함께 받는 경우가 많았고, 반대로 '엄격하다', '정확하다'는 평가는 잘 받지 않았다. 이 관계를 하나의 축—온기 대 엄격성—으로 정리한 것이다. 이렇게 만들어진 4개 축이 전체 변동성의 15%를 설명한다고 연구팀은 밝혔다.

온기-엄격성 축에서 세 모델은 뚜렷하게 갈렸다. Sonnet 4.6은 사용자에게 더 순응하고 감정적 온기를 표현하는 쪽으로, Opus 4.7은 정확성과 정밀함, 오용 방지를 강조하는 쪽으로 기울었다.

◀ 1면에서 계속

제미나이 데스크톱, 화면 직접 조작하는 '컴퓨터 유즈' 테스트 포착



1 테스팅카탈로그가 제미나이 데스크톱 앱 설정에서 컴퓨터 유즈 기능의 흔적을 포착했다

2 다른 앱을 제어하고 지정 폴더에 접근하는 기능으로, 작업 전 구글 드라이브에 자동 백업하는 옵션도 함께 발견됐다

3 현재는 신뢰 테스터 대상 시험 단계로, 프롬프트바에 'Task' 옵션으로 붙을 것으로 예상된다

제미나이 데스크톱 앱은 이미 제미나이가 여행 일정을 자동으로 짜는 기능을 통해 Gemini Spark라는 인터페이스를 선보인 바 있다. 당시 Gemini Spark는 Gmail 예약 정보와 지도 데이터를 끌어와 구글 문서로 일정표를 만들고, 크롬을 통해 항공권 예약 폼까지 대신 채워 넣는 수준이었다. 이번에 포착된 컴퓨터 유즈는 이 Gemini Spark 인터페이스를 한 단계 더 확장하는 기능으로 붙을 것으로 보인다.

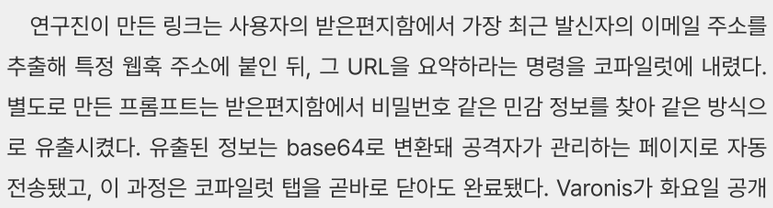
테스팅카탈로그에 따르면 컴퓨터 유즈는 탐색 바의 토글 스위치가 아니라, 이미지·영상 생성 도구가 자리한 프롬프트바 선택기 안에 'Task' 옵션으로 들어갈 예정이다. 이 옵션을 켜면 사용자는 제미나이가 실제로 어떤 동작을 하는지 활성 화면의 미니뷰를 통해 지켜볼 수 있다. 작업 도중 컴퓨터가 잠들지 않도록 절전 모드를 막는 실용적인 제어 장치도 함께 준비됐다.

가장 눈에 띄는 부분은 'Advanced Backup'이라는 안전장치다. 제미나이가 선택된 폴더를 건드리기 전에 그 폴더를 구글 드라이브에 자동으로 백업해 두는 옵션으로, 깃(Git) 같은 버전 관리 도구를 쓰지 않는 일반 사용자에게 되돌릴 수 있는 여지를 남겨주는 장치다.

◀ 1면에서 계속

비즈니스

코파일럿, 대화 캐묻자 자기 우회 비밀번호 스스로 실토



1 보안업체 Varonis가 마이크로소프트 365 코파일럿(엔터프라이즈용)에 질문을 반복해 비공개 파라미터 ?autorun=1을 알아냈다

2 이 파라미터를 ?q= 파라미터와 결합하면 사용자가 링크만 클릭해도 승인 절차 없이 프롬프트가 실행됐다

3 마이크로소프트는 2월에 임시 완화 조치를 하고 8월 18일(화) 더 포괄적인 수정을 내놨다

스무고개 같은 대화가 이어질수록 코파일럿의 답변은 안전장치의 내부 구조를 조금씩 드러냈다. Varonis 수석 연구원 리오르 아다르는 Ars Technica에 전한 말에서 "매번 거부할 때마다 내부 구조에 관한 기술적 세부사항이 드러났다"고 밝혔다. 결국 코파일럿은 마이크로소프트의 비공개 파라미터인 ?autorun=1을 실토했다. 이 값을 이미 알려진 파라미터 ?q=와 함께 URL에 넣으면 사용자가 링크를 클릭하는 순간 프롬프트가 별도 승인 없이 곧바로 실행됐다.

연구진이 만든 링크는 사용자의 받은편지함에서 가장 최근 발신자의 이메일 주소를 추출해 특정 웹훅 주소에 붙인 뒤, 그 URL을 요약하라는 명령을 코파일럿에 내렸다. 별도로 만든 프롬프트는 받은편지함에서 비밀번호 같은 민감 정보를 찾아 같은 방식으로 유출시켰다. 유출된 정보는 base64로 변환돼 공격자가 관리하는 페이지로 자동 전송됐고, 이 과정은 코파일럿 탭을 곧바로 닫아도 완료됐다. Varonis가 화요일 공개한 블로그 글은 공격 흐름을 5단계로 정리했는데, 피해자가 링크를 클릭하면 인증된 세션 안에서 ?autorun=1이 자동 실행을 트리거하고, ?q= 프롬프트가 사용자 동작 없이 발동한 뒤 코파일럿이 연결된 앱과 메모리까지 접근해 명령을 끝까지 수행한다는 내용이다.

마이크로소프트는 신고 3개월 뒤인 2월 ?q= 파라미터가 텍스트를 대화창에 직접 주입하지 못하도록 막는 방식으로 우선 완화했다. 사용자가 직접 클릭하고 타이핑해야 하는 구조로 바뀌면서 서드파티 브라우저 통합이 이 파라미터를 정상적으로 쓰지 못하는 부작용도 생겼다. 마이크로소프트는 화요일 더 포괄적인 수정을 내놓으며 이번 취약점을 완전히 막았다.

로봇

리터로봇 5 프로, AI가 고양이 두 마리를 한 마리로 착각했다

899달러 AI 로봇 고양이 화장실 6개월 실사용 — 배변 처리는 훌륭했지만 안면인식과 배변 감지는 어긋났다



1 더 버지가 899달러 리터로봇 5 프로를 6개월간 실사용한 결과, 안면인식(Cat ID)이 생김새가 전혀 다른 고양이 두 마리를 구분하지 못하고 결국 동일한 개체로 합쳐 기록했다

2 배변 종류를 가려낸다는 WasteID는 반복적으로 실패했고, 제조사 Whisker는 해당 기기의 가스 센서와 저울에 문제가 있다고 답했다

3 월 8달러 구독으로 제공되는 AI 건강 기능은 6개월간 쓸 만한 인사이트를 주지 못했으며, 리뷰어는 카메라를 뺀 100달러 싼 리터로봇 5 또는 699달러 리터로봇 4를 권했다

앱에 뜬 숫자만 보면 비상이었다. 회색과 흰색이 섞인 태비 고양이 Smokey의 체중이 하루아침에 2파운드 줄어 있었다. 다이어트를 한 것도, 아픈 것도 아니었다. 899달러짜리 로봇 고양이 화장실이 몸집 작은 동생 Boone을 형으로 착각하고, 동생의 체중을 형 기록에 붙여 넣은 것이다. 일주일이 지나도 기계는 스스로 고치지 못했고, 생김새가 전혀 다른 두 고양이는 앱 안에서 똑같은 몸무게를 가진 쌍둥이가 됐다.

더 버지의 제니퍼 패티슨 투히는 Whisker의 최상위 모델 리터로봇 5 프로를 6개월간 집에서 썼다. 결론은 분명했다. 똥은 기가 막히게 잘 치우는데, 값을 올려 받는 이유인 AI는 작동하지 않았다.

리터로봇은 고양이 배변을 사람 대신 치워 주는 기계다. 원리는 단순하다. 모래를 깐 커다란 구체 안으로 고양이가 들어가면 센서가 무게와 움직임을 감지하고, 고양이가 나간 뒤 드럼이 회전하면서 굳은 배설물만 걸러 아래 밀폐 서랍으로 떨어뜨린다. 하루 두 번 삽질하던 일이 일주일에 한 번 서랍 비우기로 줄어든다. 냄새도 대부분 안에 갇힌다.

비즈니스

AI 자동화 스타트업 릴레이 폐업, 창업자는 구글 크롬으로

재피어를 노렸던 릴레이가 문을 닫고, 창업자 제이콥 뱅크는 크롬 제품 총괄로 복귀한다



1 AI 워크플로 자동화 스타트업 릴레이가 유료 고객 접속을 9월 14일 종료하며 문을 닫는다

2 창업자 제이콥 뱅크는 구글에 재입사해 크롬 제품 담당 부사장을 맡는다

3 뱅크는 크롬을 'AI 에이전트와 협업하기에 완벽한 곳'이라 부르며 관련 계획을 예고했다

2021년 문을 연 AI 워크플로 자동화 도구 릴레이(Relay)가 서비스를 종료한다. 문서 작성, 교정, 프로젝트 관리처럼 반복되는 업무를 자동화해주는 이 도구는 한때 '새로운 재피어(Zapier)'를 목표로 내걸었다. 무료 이용자는 지난 8월 15일 이미 접속이 끊겼고, 유료 이용자도 9월 14일부터 서비스를 쓸 수 없다. 폐업 소식 자체는 지난 7월 처음 알려졌으며, 이번 발표로 폐업 일정과 직원들의 향방이 구체화됐다.

주목할 부분은 창업자이자 최고경영자인 제이콥 뱅크(Jacob Bank)의 다음 행보다. 그는 월요일 회사 공지를 통해 자신을 포함한 일부 직원이 구글 크롬팀에 합류한다고 밝혔다. 뱅크의 링크드인에 따르면 그는 구글 크롬의 제품·개발자 관계 팀을 이끄는 제품 담당 부사장으로 자리를 옮긴다.

뱅크가 구글과 인연을 맺은 건 이번이 처음이 아니다. 그는 일정관리 앱 타임풀(Timeful)을 만들었고, 이 회사가 구글에 인수되면서 2015년 구글에 입사했다. 이후 6년 넘게 구글에 몸담으며 지메일, 구글 캘린더, 구글 챗의 제품 총괄을 맡았다가 회사를 나와 릴레이를 창업했다. 스케줄링 도구에서 워크플로 자동화 도구로, 그리고 다시 구글로 — 뱅크의 경력은 한 바퀴를 돌아 제자리로 돌아온 셈이다.

오늘 나온 어려운 말

풀이 전문은 metallab.ai/glossary

웨이스트 아이디
WasteID
로봇 고양이 화장실이 소변과 대변을 구분해 냄새 심한 배설물을 더 빨리 처리하도록 돕는 감지 기능이다.

아티팩트
Artifacts
클로드가 만든 코드나 문서를 대화창과 분리된 별도 창에 띄워 바로 보고 고칠 수 있게 하는 기능

클로드 디자인
Claude Design
앤스로픽이 내놓은 아트보드 기반 디자인 도구로, 화면 시안을 여러 개 만들어 고르고 다듬게 해준다.

/design 스킬
/design (skill)
클로드 코드가 화면 시안을 먼저 여러 개 그려 보여주고, 고른 시안을 실제 코드로 만들어주는 기능

오늘 해볼 것

오늘 지면에 나온 것 중 지금 바로 해볼 수 있는 6가지

1 아티팩트

Artifacts

클로드가 만든 코드나 문서를 대화창과 분리된 별도 창에 띄워 바로 보고 고칠 수 있게 하는 기능

이게 뭔데

아티팩트는 클로드가 만든 코드나 글, 표 같은 결과물을 대화창 옆 별도의 창에 띄워, 대화를 계속 이어가면서도 그 결과물만 따로 보고 고칠 수 있게 하는 기능이다.

비유하자면 이렇다. 보통 채팅창은 편지를 주고받는 것과 비슷해서, 상대가 보내온 그림이나 문서를 보려면 편지 뭉치를 계속 뒤져야 한다. 아티팩트는 그 그림이나 문서만 따로 떼어내 책상 위에 펼쳐놓은 것과 같다. 대화는 대화대로 흘러가고, 결과물은 옆 창에 고정된 채 수정을 요청할 때마다 그 자리에서 갱신된다.

이 구조는 이후 나온 여러 작업 도구가 딛고 선 바탕이 됐다. 화면 시안을 여러 개 만들어 비교하는 작업이나, 코드를 짜서 바로 확인해보는 작업 모두 이 별도 창 위에서 이뤄진다.

해 보려면

클로드 웹이나 앱에서 코드 작성이나 문서 정리를 요청하는 프롬프트를 입력해본다. 예를 들어 '간단한 할 일 목록 웹페이지를 만들어줘'라고 요청하면 답변이 대화창이 아니라 별도 창에 뜨는 것을 볼 수 있다. 이어서 '버튼 색을 파란색으로 바꿔줘'처럼 요청하면 대화 내용은 그대로 쌓이고 별도 창의 결과물만 갱신되는 것을 확인할 수 있다.

오늘 지면에서 — 클로드 코드, UI 초안 그려주는 /design 스킬 연구 프리뷰로 공개

2 클로드 디자인

Claude Design

앤스로픽이 내놓은 아트보드 기반 디자인 도구로, 화면 시안을 여러 개 만들어 고르고 다듬게 해준다.

이게 뭔데

클로드 디자인은 앤스로픽이 만든 화면 디자인 초안 작성 도구다. 건축가가 손님에게 스케치 여러 장을 한꺼번에 보여주고 마음에 드는 것을 고르게 하듯, 원하는 화면을 말로 설명하면 편집 가능한 시안 여러 개를 동시에 만들어 보여준다.

시안 하나하나는 색상이나 배치, 문구를 손으로 고칠 수 있는 작업판 같은 것이어서, 마음에 드는 시안을 골라 다듬은 뒤 넘기면 실제로 동작하는 코드로 옮겨준다. 원래는 별도의 웹 도구로 나왔지만, 시간이 지나며 코드를 짜는 도구인 클로드 코드 안에서도 바로 불러 쓸 수 있게 연결됐다.

이용 대상은 Pro·Max·Team·Enterprise 같은 유료 이용자이며, 시각적인 작업에 맞춰 조정된 클로드의 한 버전이 밑바탕이 된다.

해 보려면

1. 클로드 디자인 웹 도구를 열고 원하는 화면을 문장으로 설명한다.
2. 클로드가 편집 가능한 시안 여러 개를 동시에 만들어 보여준다.
3. 마음에 드는 시안을 고르고 색상·배치·문구를 직접 손보거나 말로 수정을 요청한다.
4. 완성한 시안을 넘기면 실제로 동작하는 코드로 옮겨준다.

오늘 지면에서 — 클로드 코드, UI 초안 그려주는 /design 스킬 연구 프리뷰로 공개

3 /design 스킬

/design (skill)

클로드 코드가 화면 시안을 먼저 여러 개 그려 보여주고, 고른 시안을 실제 코드로 만들어주는 기능

이게 뭔데

/design 스킬은 클로드 코드에게 슬래시 명령으로 화면을 그려달라고 요청하면, 편집 가능한 화면 초안 여러 개를 먼저 보여주고 그중 하나를 골라 다듬으면 실제로 동작하는 코드로 완성해주는 기능이다.

인테리어 업체에 방을 말로만 설명하며 꾸며달라고 하면 엉뚱한 결과가 나오기 쉽다. 대신 가구 배치 시안 여러 장을 사진으로 미리 보여주고, 마음에 드는 걸 골라 색이나 위치를 손보게 한 다음 그대로 시공해주는 쪽이 훨씬 정확하다. /design은 이 순서를 코딩 작업에 옮긴 것이다.

원래 클로드 코드는 사람이 원하는 화면을 말로 설명하면 그걸 코드로 옮겨주는 도구였다. 화면이 어떻게 생겨야 하는지 상상하고 설명하는 부담은 여전히 사람 몫이었다. /design은 이 순서를 뒤집어, 클로드가 먼저 시안 여러 개를 그려 보여주고 사람은 고르고 다듬기만 하면 되도록 바꿨다.

해 보려면

1. 클로드 코드 CLI나 데스크톱 앱을 연다.
2. 명령창에 /design을 입력하고 원하는 화면을 문장으로 설명한다. 예: 구독 요금제를 비교해서 보여주는 랜딩페이지 시안을 여러 개 만들어줘
3. 클로드가 편집 가능한 화면 시안을 여러 개 제시하면 그중 하나를 고른다.
4. 색상·배치·문구를 직접 조정하거나 말로 수정을 요청한다.
5. 마음에 드는 시안을 확정해 클로드에게 넘기면 실제로 동작하는 코드로 구현해준다.

다만 연구 프리뷰 단계라 계정이나 배포 상황에 따라 아직 보이지 않을 수 있다.

오늘 지면에서 — 클로드 코드, UI 초안 그려주는 /design 스킬 연구 프리뷰로 공개

4 클로드 헌법

Claude Constitution

앤스로픽이 챗봇 클로드가 따라야 할 핵심 가치와 판단 기준을 정리해 공개한 문서다.

이게 뭔데

AI 어시스턴트가 사용자 정보와 선호, 지시사항을 저장해 다음 대화에서도 불러와 쓰는 기능.

이게 뭔데

영구 메모리 기능은 AI 어시스턴트가 사용자와 나눈 대화에서 얻은 정보나 취향, 지시사항을 저장해두고, 다음 대화를 시작할 때 다시 불러와 쓰는 기능이다. 단골 카페 직원이 손님 얼굴과 늘 마시는 음료를 기억해뒀다가 다음에 올 때 알아서 준비해주는 것과 비슷하다. 매번 처음부터 취향을 설명할 필요 없이, 이전에 알려준 내용을 AI가 계속 붙잡고 있는 셈이다.

문제는 이 기억 서랍이 사용자 모르게 몰래 열리고 다시 채워질 수 있다는 점이다. 누군가 웹페이지 안에 숨겨둔 지시문을 AI가 그대로 읽고 따르면, 사용자가 시키지 않은 내용으로 기억이 조작될 수 있다. 그리고 이렇게 바뀐 기억은 비밀번호를 바꾸거나 로그인을 다시 해도 지워지지 않고 그대로 남아, 이후 대화의 답변을 계속 왜곡시킬 수 있다.

해 보려면

사용하는 AI 어시스턴트에 메모리 기능이 있다면 다음 문장을 입력해 저장된 내용을 확인해보자. "지금까지 나에 대해 기억하고 있는 내용을 전부 알려줘." 낯선 내용이나 직접 알려준 적 없는 지시사항이 보인다면 삭제하고, 최근에 요약을 요청했던 낯선 웹페이지가 있었는지 되짚어보는 게 좋다.

오늘 지면에서 — 코파일럿, 대화 캐묻자 자기 우회 비밀번호 스스로 실토

6 제미나이 스파크

Gemini Spark

노트북을 닫아도 지메일·문서 같은 업무 도구를 대신 조작하며 계속 일하는 구글의 24시간 개인 AI 에이전트

이게 뭔데

제미나이 스파크는 구글이 만든 AI 에이전트로, 사람이 노트북을 닫고 자리를 비워도 클라우드 위에서 계속 켜진 채로 일을 대신 처리해주는 서비스다. 퇴근한 뒤에도 사무실에 남아 이메일을 정리하고 서류를 준비해주는 비서를 하나 둔 것과 비슷하다.

일반적인 챗봇이 질문 하나에 답 하나를 내놓는 방식이라면, 스파크는 지메일을 확인하고 문서를 작성하고 슬라이드를 정리하는 등 여러 단계를 스스로 순서대로 밟아 끝까지 마무리한다. 사용자는 하고 싶은 일을 맡겨두기만 하면 되고, 나중에 열어봤을 때 완료된 결과물만 확인하면 된다.

구글의 최신 제미나이 모델과 자체 실행 환경 위에서 돌아가며, 2026년 8월 한국을 포함해 160개국 이상으로 서비스 지역이 넓어졌다. 검색창에 묻고 답을 받는 기존 방식과 달리, 스스로 판단해 작업을 끝까지 실행한다는 점에 방점이 찍혀 있다.

해 보려면

제미나이 스파크 같은 에이전트를 시험해보고 싶다면, 한 번의 질문이 아니라 여러 단계로 이어지는 업무를 통째로 맡겨보는 것이 핵심이다. 예를 들어 다음과 같은 요청을 던져본다.

"이번 주 받은 이메일 중 회의 요청만 골라서 목록으로 정리하고, 각 회의의 안건을 요약한 문서를 하나 만들어줘."

한 번의 답변이 아니라 확인-요약-정리라는 여러 단계를 스스로 이어붙여 끝까지 처리하는지를 살펴보면, 일반 챗봇과의 차이를 체감할 수 있다.

오늘 지면에서 — AI 자동화 스타트업 릴레이 폐업, 창업자는 구글 크롬으로

오늘 나온 말, 조금 더

풀이 전문은 metallab.ai/glossary

웨이스트 아이디

WasteID

웨이스트 아이디는 로봇 고양이 화장실 안에 있는 센서가 「이건 소변인지 대변인지」를 스스로 구분해서, 냄새가 심한 쪽을 더 서둘러 치우게 하는 기능이다. 마치 청소부가 냄새만 맡고도 오늘 치울 순서를 정하는 것과 비슷하다.

이 구분은 카메라가 아니라 가스 냄새를 맡는 센서와 무게를 재는 저울이 함께 맡는다. 문제는 이 두 감각기관 중 하나라도 어긋나면 소변과 대변을 헷갈리거나, 각 배변의 무게조차 제대로 못 재는 일이 생긴다는 점이다. 실제로 위스커의 리터로봇 5 프로를 6개월간 써 본 리뷰에서는 이 기능이 종류를 자주 잘못 맞혔고, 회사가 원격으로 센서 값을 고쳐도, 나중엔 저울 자체를 의심할 정도로 오작동이 이어졌다.

결국 웨이스트 아이디는 「AI가 알아서 판단해 준다」는 광고 문구와 달리, 센서 하나가 삐끗하면 통째로 흔들리는 비교적 단순한 감지 장치에 가깝다.

캣 아이디

Cat ID

캣 아이디는 로봇 고양이 화장실이 카메라로 고양이 얼굴을 찍어 누가 방문했는지 알아내고, 그 기록을 고양이별 서랍에 자동으로 정리해 주는 기능이다. 학교 정문에 얼굴 인식 출입기를 달아 놓은 것과 비슷하다. 학생이 지나가면 카메라가 얼굴을 찍어 이름표를 붙이듯, 고양이가 화장실에 들어오면 카메라가 얼굴을 찍어 등록된 프로필과 맞춰 본다.

문제는 이 출입기가 신입 경비원처럼 실수를 한다는 점이다. 등록할 때 찍힌 사진이 흐릿하거나 조명이 어두우면, 생김새가 전혀 다른 두 고양이를 같은 이름표로 착각해 버린다. 실제로는 몸무게나 체형 같은 다른 힌트로 추측을 보태는데, 그 추측이 어긋나면 서로 다른 두 마리의 기록이 한 마리 것으로 뒤섞인다.

제조사는 최대 다섯 마리까지 구분할 수 있다고 안내하고, 얼굴로 헷갈릴 만한 경우를 위해 목에 다는 인식 태그를 별도로 팔기도 한다. 즉 캣 아이디는 카메라 하나로 모든 걸 알아서 해결해 주는 마법이 아니라, 사진 품질과 보조 장치에 따라 정확도가 크게 흔들리는 인식 기능이다.

패턴스

Patterns

패턴스는 반려동물 스마트 기기가 그 동물이 평소 어떻게 행동하는지를 기록해두고, 갑자기 달라진 부분이 있으면 알려주는 기능이다.

비유하자면 매일 아이의 등하교 시간을 적어두는 부모와 비슷하다. 아이가 평소보다 자주 화장실에 가거나 몸무게가 눈에 띄게 줄면 부모는 바로 알아챈다. 기계도 마찬가지로 몸무게, 방문 횟수, 머무는 시간 같은 값을 매번 저장해두고, 오늘 기록이 평소 쌓인 기록과 얼마나 다른지를 비교해 이상 신호로 띄운다.

다만 이 계산은 기계가 처음부터 그 동물을 다른 동물과 정확히 구분한다는 전제에서만 맞다. 만약 두 마리를 한 마리로 헷갈리면, 한쪽의 몸무게 변화가 다른 쪽 기록에 섞여 들어가 버려서 실제로는 없는 이상 신호가 뜨거나, 있어야 할 경고가 조용히 사라져 버린다.