

AI

AI 겨냥 사이트 3곳이 만든 21만 페이지, 퍼플렉시티가 인용했다

380개 소프트웨어 카테고리 조사에서 인용 6할이 무명 사이트였고, 그중 3곳은 AI만 겨냥해 만들어졌어요



AI · AI 겨냥 사이트 3곳이 만든 21만 페이지, 퍼플렉시티가 인용했다

트렌더 연구진은 2026년 9월 2일 퍼플렉시티의 두 모델 sonar와 sonar-pro에 OpenRouter를 통해 접근해, 'CRM 소프트웨어'부터 '박물관 소장품 관리 소프트웨어'까지 380개 구매 의도 카테고리를 각각 물었어요. 카테고리당 모델당 한 번씩 총 760번 호출했고, 모든 응답에서 추천 제품 다섯 개와 함께 실제로 검색해 가져온 URL을 받았어요. 카테고리 목록은 결과를 보기 전에 미리 정해 뒀고 이후 수정하지 않았다고 밝혔어요. 이렇게 모은 인용은 7,534건, 서로 다른 도메인은 2,055개였어요. 연구진은 이 도메인들을 웹사이트 방문량 순위인 Tranco 목록과 인터넷 아카이브 웨이백 머신에 대조했어요. 순위가 매겨진 도메인 중 인용의 중간값 순위는 71,611위였고, 전체 인용의 59.8%가 10만 위 밖, 23.4%는 아예 상위 100만 위 안에도 들지 못하는 도메인이었어요. 비교하자면 위키백과는 7,534건 중 단 3번 인용됐어요.

구글은 이번 조사 대상에서 빠졌어요. OpenRouter로 재미나이 계열 모델에 그래운딩을 붙이면 구글 자체 검색이 아니라 OpenRouter의 검색 플러그인을 거치게 되기 때문이라고 연구진은 설명했어요.



Inworld AI, 리얼타임 TTS-2 출시...음성합성 1위 경쟁 재점화
가장 눈에 띄는 사례는 guideflow.com이에요. 이 회사는 인터랙티브 제품 데모를 판매하는 곳이지 리뷰 사이트도 디렉터리도 아니고, 조사 대상 380개 카테고리 어디에도 직

접하진 않던 worldmetrics.org, gitnux.org, wifitalents.com 세 사이트예요. 각각 60회·50회·71회, 합쳐서 181번 인용되며 41개 카테고리에 등장했는데 전체 인용에서 차지하는 비중은 2.4%로 크지 않아요. 하지만 이 셋은 하나의 운영 주체가 만든 것으로 보인다고 연구진은 밝혔어요. 세 도메인 모두 2023년 12월과 2024년 5월 사이 네임칩(NameCheap)을 통해 등록됐고, DNS를 같은 클라우드플레어 네임서버 두 곳(pam.ns.cloudflare.com, sean.ns.cloudflare.com)에 위임했으며, 내비게이션 메뉴 구성까지 똑같은 템플릿을 쓰고 있어요. 각 사이트는 블로그 글을 정확히 6개씩만 갖고 있는데, 그 내용은 전부 서로의 브랜드와 zipdo.co라는 네 번째 브랜드를 다뤄요. zipdo.co 역시 같은 네임서버를 쓰고 자기 홈페이지에 똑같이 'Facts & Grounding Page'라는 제목을 붙여 뒀어요.



판그렘, AI 탐지로 출판업계 뒤편들었지만 신뢰성 도마에
이 세 사이트의 사이트맵에는 각각 103,578개, 107,083개, 105,541개의 URL이 있고, 이 중 '/best/(카테고리)-software/' 형식의 자동 생성 구매 가이드 페이지가 70,731개, 71,684개, 72,713개예요. 합치면 215,128개인데, 세상에 그만큼 많은 소프트웨어 카테고리가 존재하는 건 아니예요.

worldmetrics.org와 gitnux.org의 홈페이지 HTML
제목은 식제료 '(브래드먼)' — Facts & Grounding

정 서비스를 '2,500유로부터' 판매한다고 광고하고 있어요. AI가 인용하는 자동 생성 '베스트 리스트' 바로 위에 유료 서비스를 걸어 둔 구조예요.

연구진은 세 사이트에서 똑같이 '프로젝트 견적 소프트웨어(project estimation software)' 카테고리 페이지를 가져와 비교했어요. 각 페이지는 순위를 JSON-LD 형식으로 명시해 두어 해석 없이 그대로 읽을 수 있었어요.

같은 질문 하나에 서로 다른 담당 직원 9명이 등장한 셈이에요. 게다가 세 페이지 중 두 곳은 작성자 줄에 "Within the next 26 days", 나머지 한 곳은 "Within the next 40 days"라는 문구가 그대로 노출돼 있었는데, 렌더링되지 않은 템플릿 변수로 보여요.

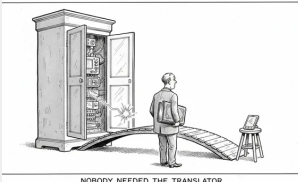
퍼플렉시티가 알려진 벤더 홈페이지 1,502개를 직접 접속과 로테이팅 프록시 접속 두 방식으로 각각 확인한 결과, 10개는 아예 주소가 연결되지 않았고(그중 8개는 네임서버조차 없었어요) 4개는 응답하지 않아 총 17개(1.1%)가 접속 불가 상태였어요. GraphiQL의 홈페이지로 제시된 graphiql.com, 마이크로소프트 투두용으로 제시된 todo.com, Trivy용으로 제시된 aquasecurity.io는 실제로는 그런 사이트가 존재하지 않았어요. 또 92개(6.1%)는 다른 등록 도메인으로 리다이렉트됐는데 대부분 혼한 인수·리브랜딩 사례였어요.

두 모델은 사실상 하나의 검색 엔진을 두 번 측정한 것에 가까워요. 380개 카테고리 중 289개에서 두 모델의 인용 목록이 완전히 동일했고, URL 집합의 자카드 유사도는 0.898에 달했어요. 1위 추천이 같았던 비율도 380개 중 290개였어요.

연구진은 스스로 한계를 분명히 뒀어요. 이번 측정은 퍼

오늘 지면

- 1 AI
AI 겨냥 사이트 3곳이 만든 21만 페이지, 퍼플렉시티가 인용했다
- 2 AI
앤스로픽, 커머스 에이전트 청사진 오픈소스 공개
- 3 AI
ATV 빅에어투어, 챗GPT 워크로 재고정리 사흘을 3시간에
- 4 AI
AI 설계 단백질, 예측과 실험이 갈렸다
- 5 AI
구글, 페어워드 프로그램으로 정부·기업에 사이버 방어 AI 공개
- 6 AI
Inworld AI, 리얼타임 TTS-2 출시...음성합성 1위 경쟁 재점화



AI끼리는 말로 하지 않는 편이 빠르다, 필즈상 수학자가 놓은 모델 사이의 다리



판그렘, AI 탐지로 출판업계 뒤편들었지만 신뢰성 도마에

이 지면은 2026년 9월 4일 금요일 아침 구독자 메일함으로 나간 레터를 신문 판형으로 다시 조판한 것입니다. 기사 전문은 metallab.ai 에서 읽을 수 있습니다.

AI



AI 설계 단백질, 예측과 실험이 갈렸다

AI가 설계한 단백질이 실험실에서 얼마나 붙는지, 그리고 만들기 전에 붙을 것을 골라낼 수 있는지 정면으로 재본 결과가 나왔어요. 앤스로픽이 공개한 자율 단백질 바인더 설계 캠페인과 그 데이터를 뜯어본 후속 분석이에요. 규모부터 보면 이래요. 클로드가 설계한 미니단백질 바인더 1,320개를 표적 15개에 대고 시험했고, 354개가 결합했어요. 적중률 26.8%예요.

▶ 2면에 계속

AI

앤스로픽, 커머스 에이전트 청사진 오픈소스 공개



앤스로픽이 9월 2일 커머스 에이전트를 만드는 청사진을 오픈소스로 공개했어요. 깃허브 저장소 anthropics/commerce-agents에 손님을 상대하는 쇼핑 에이전트와 가게를 운영하는 판매자 에이전트의 구현 코드, 그리고 리테일·여행·통신·엔터테인먼트 네 갈래 예제가 아파치 2.0 라이선스로 올라갔어요.

▶ 2면에 계속

AI

ATV 빅에어투어, 챗GPT 워크로 재고정리 사흘을 3시간에



ATV 빅에어투어는 미국 전역 26개 도시를 5월부터 11월까지 도는 모토크로스 공연팀이에요. 오픈시가 9월 2일 공개한 고객 사례에 따르면, 이 2인 팀은 챗GPT 워크로 이벤트 정보 점검, 재고관리, AI 검색 노출까지 자동화해 대형 경쟁사와 맞먹는 업무량을 소화하고 있어요.

▶ 2면에 계속

◀ 1면에서 계속

AI

앤스로픽, 커머스 에이전트 청사진 오픈소스 공개



- 1 앤스로픽이 9월 2일 쇼핑·판매자 에이전트를 만드는 청사진을 아파치 2.0 라이선스로 공개했어요.
- 2 리테일·여행·통신·엔터테인먼트 네 갈래 예제와 클로드 코드 플러그인이 저장소에 함께 들어 있어요.
- 3 결제와 가격 변경은 모델이 실행하지 못하고 사람 승인 대기로만 쌓이도록 설계했어요.

쇼핑 에이전트는 고객이 말로 물어보는 것을 받아요. 카탈로그를 검색하고 여러 상품을 비교해 화면에 띄우고, 장바구니를 채우고, 주문 상태나 반품 규정 같은 질문에 답해요. 여기에 다섯 개의 스킬이 붙어요. 검색·발견, 구매 조사, 계획 세우기, 고객 응대, 기억과 개인화예요.

판매자 에이전트는 가게 쪽 화면에서 돌아요. 매출을 분석하고 재고를 추적하고 가격과 프로모션을 제안하고 마케팅 캠페인 초안을 써요. 이쪽 스킬도 다섯 개로 성과 분석, 카탈로그 관리, 재고 운영, 가격·프로모션, 마케팅 캠페인이예요.

무엇을 시스템 프롬프트에 넣고 무엇을 스킬로 뺄지는 규칙이 하나예요. 전체 대화의 3분의 1쯤에 해당하는 일은 프롬프트에 상주시키고, 나머지 긴 꼬리는 스킬로 내려요.

◀ 1면에서 계속

AI

ATV 빅에어투어, 챗GPT 워크로 재고정리 사흘을 3시간에



- 1 ATV 빅에어투어 공동창업자 2인이 챗GPT 워크로 이벤트 정보 오류 점검 시간을 주 8시간에서 1시간으로 줄였어요.
- 2 상품 사진을 올리면 15분 만에 재고 웹사이트와 발주안이 나와, 사흘 걸리던 재고정리가 2~3시간으로 줄었어요.

챗GPT 워크에 매일 아침 브리핑을 예약해 두자, 라리사가 몰랐던 행사 목록까지 포함해 사이트 전반의 오류를 찾아내는 보고서가 자동으로 도착하게 됐어요. 챗GPT는 오류를 찾는 데서 멈추지 않고 해당 매체의 담당자 연락처와 일정 요청 이메일 초안까지 만들어 줘요. 그 결과 점검 시간은 주 8시간에서 1시간으로, 7시간이 줄었어요.

굿즈 재고 정리와 재주문도 손이 많이 가는 일이었어요. 라리사는 상품 사진을 찍어 챗GPT 워크에 올렸고, 챗GPT는 15분도 안 돼 재고 목록과 스프레드시트, 눈으로 확인할 수 있는 재고 웹사이트, 재주문 추천안까지 만들어냈어요. 라리사가 추천안을 검토하고 조정한 뒤 공급업체에 최종 주문을 넘기면 끝이예요. "여러 팀원의 몫까지 대신 해줘요"라고 라리사 게터(ATV 빅에어투어 공동창업자)는 말했어요. 예전엔 2~3일이 꼬박 걸리던 이 작업이 이제 2~3시간이면 끝난다고 회사 측은 밝혔어요.

가족 단위 관객이 구글이든 챗GPT든 어떤 창구로 행사를 찾든 잡혀야 한다는 게 라리사의 목표예요. 2인 회사라 별도 마케팅팀을 둘 수 없으니, 그 역할도 챗GPT 워크가 맡았어요. 매일 자동으로 웹사이트를 감사해 날짜·장소·티켓 정보가 AI 검색 도구가 읽어낼 수 있는 구조로 돼 있는지 확인하는 방식인데요, 여기서 말하는 AEO(Answer Engine Optimization)는 검색엔진이 아니라 챗GPT 같은 AI 답변 도구에 잘 노출되도록 사이트 구조를 다듬는 작업을 뜻해요. 이 감사에서 챗GPT가 사이트 FAQ의 약 90%를 아예 읽어내지 못한다는 사실이 드러났고, 챗GPT는 문제를 지적하는 데 그치지 않고 해결 방향까지 제안했어요.

◀ 1면에서 계속

AI

AI 설계 단백질, 예측과 실험이 같았다



- 1 클로드가 자율 설계한 미니단백질 바인더 1,320개 중 354개가 결합해 적중률 26.8%를 냈고, 통상 캠페인은 10~15%예요.
- 2 후속 분석에서는 구조 예측기 10종의 AUC가 0.55에서 0.75에 그쳤고, 결합 실패로 기록된 상당수가 사실 발현 실패였어요.

앤스로픽은 오늘날 단백질 설계 캠페인에서 통상 10\~15%가 나온다고 밝혔어요. 두 배 안팎이에요.

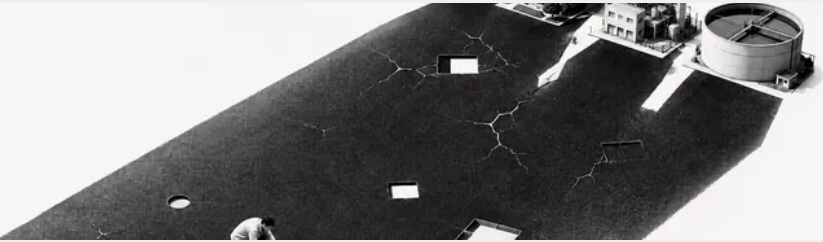
바인더는 표적 단백질에 달라붙도록 설계한 작은 단백질이에요. 항체보다 훨씬 작아서 미니바인더라고 불러요.

표적은 원래 16개를 골랐는데 하나는 표적 자체가 뭉쳐 버려 판정이 안 나와 빠졌어요. 남은 15개 중 14개에서 결합체가 나왔어요.

AI

구글, 페어윈드 프로그램으로 정부·기업에 사이버방어 AI 공개

제미니이 3.8 플래시 사이버와 코드멘터를 묶어 650여 파트너에 취약점 자동 수정을 제공해요



- 1 사이버 전용 모델 제미니이 3.8 플래시 사이버와 코드멘더 하네스를 결합해 취약점을 자동으로 찾고 고쳐요.
- 2 전 세계 650여개 파트너가 참여하며, 내부 보안팀 한정·다중인증 같은 이용 조건을 지켜야 해요.

구글 딥마인드가 정부기관과 기업 보안팀에 자사의 가장 앞선 사이버 방어 AI를 먼저 여는 프로그램을 시작했어요. 이름은 페어윈드(Fairwind) 프로그램이고, 정부·Google Cloud 고객·사이버보안 파트너 가운데 신뢰할 수 있는 조직에 한해 접근을 허용하는 방식이에요. 특히 병원, 통신망처럼 사회 기반을 떠받치는 조직을 우선순위에 뒀다고 밝혔어요.

풀어서 설명하면, 페어윈드는 접근을 허가하는 프로그램 이름이고 제미니이 3.8 플래시 사이버는 그 안에서 쓰이는 실제 AI 모델이에요. 코드멘더는 그 모델이 찾아낸 취약점을 실제 코드로 고쳐주는 도구고요. 세 가지가 하나로 묶여야 방어팀이 문제를 발견하고 검증된 패치까지 몇 분 만에 만들 수 있어요.

지금까지 보안팀은 두 가지 선택지 사이에서 골라야 했어요. 거대한 프린터 모델에 쓰면 배포 비용이 크고 기업 코드베이스 전체를 통제하기 어려웠고, 반대로 작은 오픈웨이트 모델을 쓰면 복잡한 취약점 수정에서 힘이 부치는 데다 도구와 인프라를 팀이 직접 만들어야 했어요. 페어윈드는 이 둘 사이의 틈을 메우려는 시도예요.

AI

Inworld AI, 리얼타임 TTS-2 출시...음성합성 1위 경쟁 재점화

카르테시아가 2주 전 차지한 아티피셜 애널리시스 1위를 Inworld AI가 다시 가져갔다고 밝혔어요



- 1 Inworld AI가 실시간 음성합성 모델 Realtime TTS-2를 정식 출시(GA)하며 아티피셜 애널리시스 리더보드 1위를 자체 주장했어요
- 2 지연시간 150밀리초 미만, 자연어로 톤을 조정하는 보이스 스티어링, 같은 화자로 500개 이상 방언을 오가는 기능을 갖췄어요
- 3 불과 2주 전인 8월 19일에는 카르테시아 Sonic-3.6이 같은 리더보드 1위였어서, 선두 자리가 다시 흔들렸어요

Inworld AI가 9월 2일(현지시간) 자사 X 계정에 올린 발표 영상에서 실시간 음성합성 모델 "Realtime TTS-2"를 정식 출시(GA-General Availability)했다고 밝혔어요. 회사는 이 모델이 아티피셜 애널리시스 리더보드에서 1위를 차지했고, 같은 체급 안에서 가장 빠른 TTS라고 자체 소개했어요. TTS(Text-to-Speech)는 글을 사람 목소리처럼 읽어주는 음성합성 기술로, 콜센터 상담봇부터 오디오북 내레이션까지 두루 쓰이는 기반 기술이에요.

풀어서 설명하면, 아티피셜 애널리시스는 여러 AI 모델의 성능·속도·가격을 직접 측정해 순위를 매기는 독립 평가 기관이에요. 이 회사가 모델을 만드는 게 아니라 채점만 한다는 점에서, 여기서 나온 「1위」는 업계가 성능을 증명할 때 흔히 인용하는 지표예요.

회사는 리서치 프리뷰 단계에서 예상보다 훨씬 많은 사용량이 몰렸고, 그 경험을 다시 연구에 반영해 이번 GA 모델을 내놴다고 설명했어요. 이번 출시를 두고는 "Inworld 역사상 가장 큰 도약"이라고 자평했어요.

연구 실

AI끼리는 말로 하지 않는 편이 빠르다, 필즈상 수학자가 놓은 모델 사이의 다리

모델 두 개를 이어 붙일 때 우리는 늘 한쪽이 쓴 글을 다른 쪽이 읽게 해 왔어요.



- 1 모스틱(Mostik)은 러시아어로 작은 다리라는 뜻이에요. 서로 다른 AI 모델을 가중치 속 수학적 값으로 연결해, 텍스트를 만들지 않고도 한 모델의 능력을 다른 모델에 넘기는 방식을 만들었어요.
- 2 시연으로 매개변수 7,530억 개짜리 GLM-5.2 최대 버전과 휴대폰에서 도는 40억 개짜리 Qwen-3.5를 이어 붙였더니, 비용은 큰 모델의 20분의 1인데 성능은 두 모델의 정확히 중간이 나왔어요.
- 3 회사 대표는 AI의 다음 단계가 하나의 거대한 모델이 아니라 여러 모델의 조합에 있다고 봐요. 다만 아직 논문도 공개 벤치마크도 없어서, 지금 우리가 켜 온 것은 결과 발표가 아니라 시연이에요.

모스틱(Mostik)은 러시아어로 작은 다리를 뜻해요. 러시아 수학자들이 세운 이 스타트업의 이름은 회사가 하는 일을 그대로 옮긴 거예요. 서로 다른 AI 모델 사이에 다리를 놓아, 사람이 읽을 수 있는 글자를 단 한 자도 만들지 않고 능력을 주고받게 하는 일이에요. 회사 사람들은 이걸 기계끼리의 텔레파시에 가깝다고 설명해요.

다리의 재료는 모델의 가중치예요. 가중치는 프롬프트가 출력으로 바뀌는 방식을 결정하는 숫자 덩어리인데, 모스틱은 그 숫자 안에서 두 모델이 공유할 수 있는 값을 찾아 서로를 이어요. 그러면 큰 모델이 가진 능력을 작은 모델 쪽으로 훨씬 적은 비용에 흘려보낼 수 있어요.

이 방식으로 만든 모델이 AI에게 가장 어려운 시험 가운데 하나로 꼽히는 ARC-AGI 3 정상에 올랐다고 회사는 말해요. 다만 그 대회에서 우승하고 싶다면 어떤 모델을 어떻게 이었는지는 알려 주지 않았어요.

AI

판그램, AI 탐지로 출판업계 뒤흔들었지만 신뢰성 도마에

직원 24명 스타트업이 매긴 AI 점수가 대형 출판사의 책 계약을 취소시켰고, 연구 협력자의 이해관계도 논란이 됐어요



- 1 브루클린 파피이스 매장 위층에 있는 24명 규모 스타트업 판그램이 1월 소셜 Shy Girl에 78% AI 판정을 내리면서 아셰트가 출간을 취소했어요
- 2 뉴욕타임스 모던러브 칼럼, 커먼웰스 단편소설상 수상작이 각각 100%, 240만 달러 계약 스릴러가 97% 판정을 받는 등 유사 사례가 이어졌어요
- 3 판그램이 확보한 원고가 불법 복제 사이트 출처였다는 지적과, 연구 협력자가 창업자와 가까운 사이로 API 크레딧을 지원받아 온 사실이 신뢰성 논란을 키우고 있어요

직원 24명짜리 스타트업이 매긴 점수 하나가 대형 출판사의 책 계약을 무너뜨렸어요. 위어드(Wired) 취재에 따르면 이 회사, 판그램(Pangram)은 브루클린의 한 파피이스

오늘 나온 어려운 말 풀이 전문은 metallab.ai/glossary

코폴딩 모델 cofolding model 두 분자가 서로 붙었을 때 만들어지는 입체 구조를 미리 계산해서 예측하는 AI 모델.	표면 플라스몬 공명 surface plasmon resonance 빛을 금속 표면에 쏘아 두 분자가 얼마나 단단히 결합하는지 측정하는 물리 현상이자 측정 기법이다.	구조 예측기 structure predictor 아미노산 서열처럼 한 줄로 된 정보만 보고 분자가 실제로 어떤 입체 모양으로 접히는지 계산하는 AI 도구예요.	소나 프로 sonar-pro 퍼플렉시티가 실시간 웹 검색 결과를 근거로 답변을 만들 때 쓰이는 AI 모델.
---	--	---	--

오늘 해볼 것

오늘 지면에 나온 것 중 지금 바로 해볼 수 있는 6가지

1 소나 프로

sonar-pro

퍼플렉시티가 실시간 웹 검색 결과를 근거로 답변을 만들 때 쓰는 AI 모델.

이 게 뭔데

소나 프로는 퍼플렉시티라는 AI 검색 서비스가 질문에 답할 때 쓰는 모델이다. 일반 챗봇이 미리 배운 지식만으로 답하는 도서관 사서라면, 소나 프로는 질문을 받자마자 직접 인터넷을 뒤져 관련 페이지를 찾아온 다음 그 내용을 요약해 답하는 심부름꾼에 가깝다.

문제는 이 심부름꾼이 어떤 자료를 가져오는지다. 심부름꾼이 아무 가게에서나 전단지를 주워 오면, 그 전단지가 실제로 믿을 만한지와 상관없이 답변에 그대로 섞여 들어간다. 최근 조사에서는 소나와 소나 프로가 소프트웨어 추천 질문에 답하며 방문자가 거의 없는 무명 사이트, 심지어 그 시장과 관련 없는 회사의 블로그 글을 근거 자료로 자주 가져온 사실이 드러났다.

해 보려면

퍼플렉시티에서 소프트웨어나 제품 추천을 물어본 뒤, 답변 아래 표시되는 출처 링크를 하나씩 눌러 확인해 보자.

예시 프롬프트: "가장 좋은 [분야] 소프트웨어 5개를 추천하고 각 추천의 근거가 된 출처를 알려줘"

출처로 뜬 사이트가 이름을 들어본 적 있는 곳인지, 그 분야와 실제로 관련 있는 곳인지 스스로 판단해 보면 AI 검색 결과를 어떻게 걸러 읽어야 할지 감이 잡힌다.

오늘 지면에서 — AI 겨냥 사이트 3곳이 만든 21만 페이지, 퍼플렉시티가 인용했다

2 JSON-LD 형식

JSON-LD

웹페이지 속 정보를 기계가 알아보도록 붙이는 표준화된 이름표 같은 데이터 표기 방식

이 게 뭔데

JSON-LD 형식은 웹페이지 안에 숨겨서 넣는 '이 페이지 내용이 정확히 무엇인지?' 알려주는 명찰 같은 표기 방식이다. 사람이 눈으로 글을 읽고 '아, 이건 상품 리뷰구나' '이건 회사 소개구나'라고 파악하는 것과 달리, 컴퓨터 프로그램은 글을 통째로 읽고 의미를 파악하기 어렵다. 그래서 페이지를 만든 사람이 미리 '이 페이지는 상품이고, 이름은 이것, 가격은 이만큼, 별점은 이만큼'이라고 정해진 형식으로 적어두면, 기계가 본문을 다시 해석할 필요 없이 그 명찰만 읽고 바로 이해할 수 있다.

이 명찰은 사람 눈에는 보이지 않고 페이지 코드 안에 숨어 있어서, 겉모습을 해치지 않으면서도 검색엔진이나 AI 서비스가 페이지 성격을 빠르게 파악하는 데 쓰인다. 예를 들어 온라인 쇼핑몰이 상품 페이지마다 이 명찰을 붙여두면, 검색 결과에 별점이나 가격이 바로 뜨거나 질문에 답하는 AI가 그 페이지를 근거 자료로 더 쉽게 찾아 쓸 수 있게 된다.

다만 이 명찰은 페이지를 만든 쪽이 스스로 적어 넣는 것이라, 내용이 실제 페이지와 다르거나 부풀려져 있어도 겉으로는 구분하기 어렵다는 한계가 있다.

해 보려면

1 자주 쓰는 챗봇에 다음처럼 복붙해 실험해 본다.

다음 정보로 상품 페이지에 넣을 JSON-LD 구조화 데이터를 만들어줘: 상품명 '무선 이어폰', 가격 79000원, 평균 별점 4.5, 리뷰 수 120개.

2 결과로 나온 코드를 보면 상품명, 가격, 별점이 사람이 읽는 문장이 아니라 정해진 항목과 값으로 정리되어 있는 것을 확인할 수 있다. 바로 이런 형태가 웹페이지 안에 숨어서 기계에게 정보를 전달하는 방식이다.

오늘 지면에서 — AI 겨냥 사이트 3곳이 만든 21만 페이지, 퍼플렉시티가 인용했다

3 소나

Sonar

퍼플렉시티가 만든 검색 연동형 AI 모델로, 웹을 검색해 찾아온 문서를 근거로 답을 만든다

이 게 뭔데

소나는 퍼플렉시티가 만든 AI 모델로, 질문을 받으면 그냥 아는 척 답하는 게 아니라 인터넷을 검색해서 실제 웹페이지를 찾아온 뒤 그 내용을 근거로 답을 짜 맞춘다. 일반 언어모델이 미리 학습된 지식만으로 답한다면, 소나는 도서관에서 참고 자료 몇 편을 뽑아와 읽고 요약해주는 조사원처럼 움직인다.

이름 뒤에 붙는 sonar와 sonar-pro는 같은 계열의 서로 다른 버전으로, 속도나 답변 품질 수준이 다르다. 다른 회사나 개발자들도 자기 서비스에 이 검색 기능을 붙이고 싶을 때 오픈라우터 같은 중개 서비스를 통해 소나를 불러다 쓸 수 있다.

문제는 소나가 답을 만들 때 어떤 웹페이지를 근거로 골라오느냐가 곧 그 답의 신뢰도를 좌우한다는 점이다. 방문자가 거의 없는 무명 사이트를 근거로 삼으면, 사용자는 그 사실을 모른 채 부실한 정보를 진짜처럼 받아들이게 된다.

해 보려면

퍼플렉시티에서 특정 소프트웨어 카테고리를 물어보자. 예를 들어 '가장 좋은 프로젝트 관리 소프트웨어 추천해줘'라고 입력한 뒤, 답변에 달린 출처 링크를 하나씩 눌러 그 사이트가 실제로 이름이 알려진 곳인지, 방문자가 많은 곳인지 확인해보자. 답의 근거가 얼마나 믿을 만한지 스스로 판단하는 연습이 된다.

오늘 지면에서 — AI 겨냥 사이트 3곳이 만든 21만 페이지, 퍼플렉시티가 인용했다

4 오탐지

false positive

실제로는 문제가 없는데 있다고 잘못 판정하는 오류, AI 탐지 도구가 사람이 쓴 글을 AI가 썼다고 잘못 판단하는 경우가 대표적이다.

이 게 뭔데

오탐지는 실제로는 아무 문제가 없는데 검사기가 문제가 있다고 잘못 알리는 것을 말해요. 연기가 없는데 화재경보기가 울리거나, 스팸이 아닌 메일이 스팸함으로 걸러지는 것과 같은 경우예요. AI가 쓴 글을 찾아내는 서비스에서도 똑같은 일이 생길 수 있어요. 사람이 직접 쓴 문장을 두고 도구가 「AI가 78% 관여했다」는 식으로 점수를 매기면, 그 점수가 틀렸을 가능성이 오탐지예요.

비유하자면 이런 거예요. 가게 진열장을 사람이 지나가며 보기 좋게 꾸미는 게 예전 방식이었다면, 이제는 로봇 점원이 창고 안까지 들어와서 물건 위치와 가격표를 정확히 찾아낼 수 있도록 선반을 정돈해주는 작업에 가까워요. 사람 눈에는 예뻐 보여도 로봇이 글자를 못 읽는 구조라면 소용이 없거든요.

실제로 낱자·장소·가격 같은 핵심 정보가 웹사이트 어딘가에 있긴 해도, AI 도구가 그 페이지 구조를 이해하지 못해 통째로 놓치는 경우가 흔해요. 그래서 AEO 작업은 정보를 새로 만드는 게 아니라, 이미 있는 정보를 AI가 인식하기 쉬운 형태로 다시 배치하는 데 가깝습니다.

해 보려면

우리 회사(또는 개인) 웹사이트 주소를 알려주고 이렇게 물어보세요. "이 사이트에서 낱자·장소·가격처럼 사람들이 자주 찾는 핵심 정보를 AI 검색 도구가 얼마나 잘 읽어낼 수 있는지 점검해줘. 못 읽는 부분이 있다면 이유와 개선 방법도 알려줘." 결과로 나온 제안은 바로 적용하지 말고, 실제로 페이지 구조를 바꿔도 되는지 검토한 뒤 반영하는 게 안전해요.

오늘 지면에서 — ATV 빅어투어, 챗GPT 워크로 재고정리 사흘을 3시간에

오늘 나온 말, 조금 더

풀이 전문은 metallab.ai/glossary

코폴딩 모델

cofolding model

코폴딩 모델은 두 개의 분자가 실제로 만나 붙었을 때 어떤 3차원 모양으로 맞물릴지 컴퓨터 안에서 미리 그려보는 AI 모델이다. 퍼즐 조각 두 개를 직접 깎아서 맞춰보기 전에, 컴퓨터 화면에서 회전시켜 보며 이가 맞는지 가능해보는 것과 비슷하다.

단백질 설계에서는 이 모델이 특히 중요하다. 표적 단백질에 붙도록 새로 만든 작은 단백질(바인더)이 실제로 표적과 어떤 모양으로 결합할지, 그리고 얼마나 단단히 붙을지를 실험실에서 직접 합성하기 전에 코폴딩 모델로 먼저 걸러낸다. 수백, 수천 개의 설계안 중 붙을 가능성이 높은 후보만 골라 실험으로 넘기면 시간과 비용을 크게 줄일 수 있다.

다만 코폴딩 모델의 예측은 최종 답이 아니다. 컴퓨터 안에서 그린 구조가 실제 유리 바이알 속 단백질의 행동과 항상 일치하지는 않기 때문에, 예측이 맞았는지는 결국 실험실에서 직접 붙여보는 검증을 거쳐야 확인된다.

표면 플라스몬 공명

surface plasmon resonance

표면 플라스몬 공명은 아주 얇은 금속 막 표면에 빛을 쏘아, 그 표면에 분자가 붙었다 떨어지는 것을 실시간으로 읽어내는 측정 방법이다. 비유하자면 저울에 아무것도 안 올렸을 때와 원가를 올렸을 때 바늘이 움직이는 것처럼, 금속 표면에 분자 하나가 달라붙기만 해도 그 표면에서 반사되는 빛의 각도나 세기가 살짝 바뀐다. 이 변화를 정밀하게 읽으면 두 분자가 서로 얼마나 세게 붙잡고 있는지, 붙는 데 시간이 얼마나 걸리는지, 떨어지는 데는 얼마나 걸리는지를 숫자로 뽑아낼 수 있다.

신약이나 새 단백질을 설계할 때 이 결합 세기(KD 값으로 표시된다)를 재는 표준적인 방법 중 하나가 바로 이 기술이다. 컴퓨터로 아무리 정교하게 결합을 예측해도, 실제로 두 분자를 실험실에서 붙여보고 그 세기를 재는 검증 단계가 따로 필요한데, 이때 흔히 쓰이는 도구다.

구조 예측기

structure predictor

구조 예측기는 서열이라는 한 줄짜리 설계도만 보고, 그 분자가 공간에서 어떤 입체 모양으로 접힐지 미리 계산해 내는 프로그램이다. 종이접기 도안만 보고 완성됐을 때 모양을 머릿속으로 그려보는 것과 비슷하다고 생각하면 된다. 단백질은 아미노산이 실처럼 길게 이어진 물질인데, 그 실이 어떻게 구불구불 접히느냐에 따라 하는 일이 완전히 달라진다.

이 예측이 중요한 이유는, 두 분자가 서로 딱 붙게 만들려면 먼저 각자의 모양을 알아야 하기 때문이다. 모양을 잘못 짚으면 아무리 서열을 정교하게 설계해도 실제 실험실에서는 붙지 않는 결과물이 나온다. 그래서 새로운 단백질을 설계하는 작업에서는 구조 예측기가 서열을 고르는 작업과 짝을 이뤄 함께 쓰인다.

최근에는 이 예측기가 혼자 쓰이기보다, 표적과 새 단백질이 만났을 때 함께 어떤 모양으로 붙는지까지 계산하는 방식으로 발전하고 있다. 이렇게 두 구조를 동시에 접어보는 계산은 따로 이름이 붙어 있는데, 관련 항목에서 더 볼 수 있다.

제미나이 엔터프라이즈 에이전트 플랫폼

Gemini Enterprise Agent Platform

제미나이 엔터프라이즈 에이전트 플랫폼은 회사가 자기 업무에 맞는 AI 도우미를 조립할 수 있도록 구글이 여러 모델을 진열해 둔 매장 같은 곳이에요. 개인이 쓰는 채팅 앱과 달리, 기업 고객이 자기 시스템에 붙여 쓸 모델을 고르고 연결하는 용도로 만들어졌어요.

예를 들어 사이버 보안 쪽에서는 이 플랫폼에 올라온 모델을 취약점을 실제로 고쳐주는 도구와 엮어서 쓸 수 있어요. 특별히 승인 받은 일부 기관만 쓸 수 있는 전용 최고급 모델과는 달리, 이 플랫폼은 구글 클라우드를 쓰는 기업이라면 더 폭넓게 접근할 수 있는 통로예요.

즉 같은 회사 안에서도 접근 문이 두 개인 셸이에요. 하나는 특별 승인이 필요한 좁은 문, 다른 하나는 일반 기업 고객도 지나갈 수 있는 넓은 문인데, 제미나이 엔터프라이즈 에이전트 플랫폼은 후자에 해당해요.

페어윈드 프로그램

Fairwind Program

페어윈드 프로그램은 구글 딥마인드가 만든 강력한 사이버 방어용 인공지능을, 아무나 살 수 있는 물건이 아니라 자격을 갖춘 곳에만 내주는 초대장 같은 제도다.

비유하자면 처방이 까다로운 약을 아무 약국에서나 팔지 않고, 정해진 병원과 인증된 의료진에게만 먼저 공급하는 것과 비슷하다. 여기서 약에 해당하는 건 보안 취약점을 찾아내고 고치는 AI 모델이고, 페어윈드는 그 약을 누구에게 어떤 조건으로 줄지 정하는 프로그램의 이름이다. 병원이나 통신망처럼 사회 기반이 되는 조직이 우선 대상이고, 신성한 조직은 접근 권한을 보안·사고대응 담당 인력으로 제한하고 추가 보안 장치를 갖추는 데 동의해야 한다.

페어윈드에 들어가지 못한 일반 고객이 완전히 배제되는 건 아니다. 다른 경로로 비슷한 기능을 쓸 수는 있지만, 가장 앞선 사이버 전용 모델 자체는 페어윈드 참여 조직에게 먼저 열린다.

합성 미러링

synthetic mirroring

합성 미러링은 AI가 만든 글의 버릇을 먼저 익힌 다음, 그 버릇을 거울처럼 되비추어 비슷한 글을 알아보는 방식이다. 위조지폐 감별사가 진짜 위조지폐를 직접 만들어 보면서 그 특유의 질감과 잉크 냄새를 익히고, 나중에 다른 지폐를 보자마자 「이거 낯익다」고 잡아내는 것과 비슷하다. 즉 AI를 잡아내는 도구 안에도 AI가 들어 있는 셈이다.

이 방식은 확률로 결과를 준다는 점이 핵심이다. 어떤 글을 넣으면 「몇 퍼센트가 AI로 생성된 것 같다」는 점수가 나오는데, 이 점수는 그 글을 직접 쓴 사람의 진술이나 원고 작성 기록 같은 확실한 증거가 아니라 패턴이 얼마나 비슷한지를 어림한 값이다. 그래서 문