

DAY 36-45 · 4부 조심할 것

4부 총정리 — 조심할 것

내 정보 지키기부터 AI의 법까지 · 용어까지 · DAY 36-45

시험 없음 — 읽고 넘어가는 복습 자료

넣는 순간 내 손을 떠난다

- 1 AI에 넣은 말은 넣는 순간 내 손을 떠난다고 생각하는 게 안전해.
- 2 이름·주소·전화번호처럼 **나를 꼭 집어낼 것**만 빼면 답은 똑같이 나와.
- 3 친구 얼굴이나 친구 번호는 내가 올릴지 정할 수 있는 게 아니야.

조각은 합쳐질 때 나를 가리킨다

- 1 '중3 남학생' 하나로는 수십만 명이야.
- 2 학교와 반이 붙으면 서른 명이 되고, 학원 시간까지 붙으면 **한 명**이 돼.
- 3 개인정보보호법도 다른 정보와 쉽게 합쳐 알아볼 수 있으면 개인정보로 봐.

넣기 전에 파질 세 가지

- 1 첫째, 나를 집어낼 수 있냐. 둘째, 내 것인가. 셋째, 비밀번호인가.
- 2 비밀번호는 넣어서 얻을 게 아예 없고 잃을 것만 있어서 **어떤 경우에도 안 되는** 쪽이야.
- 3 만든 쪽이 넣은 말을 학습에 쓰는지, 어떻게 끄는지는 공식 안내에 적혀 있어.

'베꼈다'는 말에 칸이 하나 늘었다

- 1 예전에는 '베꼈다'를 결과물이 얼마나 닮았는지로만 따졌어.
- 2 이제는 **만들기 전에 무엇으로 배웠나**까지 쟁점이 돼.
- 3 나라마다 답이 다르고 재판도 진행 중이라, 외울 게 아니라 쟁점을 알아 뉘어야 해.

파질 칸이 하나 늘었을 뿐이야

1 왼쪽 기준이 사라진 건 아니야 — 닮은 결과물은 지금도 그대로 문제야.

2 오른쪽에 **배움에 쓴 자료**라는 칸이 새로 생긴 거야.

3 그래서 결과물이 안 닮았는데도 다투는 일이 생겼어.

나라마다 다르게 그은 선

- 1 유럽은 권리자가 미리 '학습에 쓰지 마'라고 표시해 둘 수 있게 했어.
- 2 일본 정부는 '학습은 자유'라는 조항에도 한계선이 있다고 직접 적어 뒀어.
- 3 미국 저작권청은 보고서를 내면서도 **결론을 못 박지 않았어** — 모르는 게 정상인 상태야.

눈으로는 못 가린다 — 출처로 가린다

1 눈으로 봐서는 못 가려 — 손가락 개수를 세라던 옛 요령은 거의 안 통해.

2 화면 속을 뜯어보는 대신 어디서 왔는지를 따라가.

3 원래 있어야 할 곳에 있나, 다른 사람이 찍은 것도 있나를 보면 돼.

안 통하는 단서와 지금 쓰는 단서

1 안 통하는 쪽은 다 화면 안을 보는 방법이야 — 손가락, 눈 깜빡임, 화질.

2 지금 쓰는 쪽은 다 **화면 밖**을 보는 방법이야 — 출처, 다른 각도, 급한 요구.

3 화면 안은 갈수록 완벽해지니까, 눈을 화면 밖으로 옮기는 게 맞아.

만드는 쪽에 표시를 붙이는 흐름

- 1 글에 눈에 안 보이는 표식을 심는 방법이 2024년에 학술지에 실렸어.
- 2 사진과 영상에 '어디서 어떻게 만들어졌나'를 적어 두자는 공개 규격도 생겼어.
- 3 유럽은 AI로 만든 것에 표시를 붙이고 딥페이크는 밝히게 하는 규칙을 **법에 넣었어**.

미워하는 게 아니라 기울어 있는 것

1 AI는 마음먹고 누구를 미워하는 게 아니야.

2 배운 자료가 한쪽으로 치우쳐 있으면 **답도 그쪽으로 기울** 뿐이야.

3 그러니 사람을 나누거나 고르는 질문엔 '다른 경우는?'을 한 번 더 붙여.

2018년에 실제로 재 본 결과

1 얼굴 사진으로 남녀를 맞히는 프로그램들을 피부색과 성별로 나눠 검사했어.

2 틀리는 비율이 가장 높았던 건 **피부색이 어두운 여성 얼굴**이었어.

3 가장 낮았던 건 피부색이 밝은 남성 얼굴이었어.

치우침은 앞에서부터 흘러온다

1 모은 자료가 기울면 학습은 많은 쪽을 기본으로 삼고, 답은 적은 쪽에서 자주 틀려.

2 미국 표준기관도 얼굴 인식의 집단별 차이를 대규모로 측정해 보고서를 냈어.

3 AI를 고치는 건 어렵지만, 맨 끝에서 한 번 되묻는 건 오늘 당장 할 수 있어.

밝히는 한 줄은 내 몫을 지키는 울타리

1 AI를 썼다고 밝히는 건 자수가 아니라 이름표야.

2 안 밝히면 **내가 잘한 부분까지** 같이 의심받거든.

3 과제를 조각으로 쪼개고, 조각마다 누가 했는지 한 줄만 적으면 끝이야.

한 줄을 쓰는 법

1 과제를 주제 정하기·자료 찾기·초안 쓰기·다듬기·사실 확인으로 쪼개.

2 조각마다 내가 했는지 AI가 했는지 표시해.

3 '어느 조각을, 어떻게 썼고, 내가 뭘 고쳤는지' **이 세 가지**면 한 줄이 완성돼.

기계가 읽는 표시도 생겼어

- 1 구글은 자기 모델이 만든 결과물에 보이지 않는 워터마크를 넣어.
- 2 유럽연합은 AI가 만든 것에 **기계가 읽을 수 있는 표시**를 붙이게 하는 규칙을 법에 넣었어.
- 3 언제부터 적용할지는 아직 조정 중이야.

끝났을 때 내 머리에 뭐가 남았나

1 기준은 긴 규칙집이 아니라 한 문장이야 — 끝났을 때 내 머리에 뭐가 남았나.

2 통째로 시키면 **결과물만 남고** 나는 그 내용을 설명하지 못해.

3 막힌 데만 물어보고 내가 다시 쓰면 결과물도 남고 실력도 남아.

숙제 앞에서 밟는 네 걸음

1 숙제를 받으면 먼저 '뭘 배우라는 걸까'를 생각해.

2 그다음 5분이라도 내 머리로 해 봐.

3 막히면 **답 말고 실마리로** 묻고, 마지막은 내 말로 다시 써.

같은 도구, 다른 자리

- 1 통째로 시킨 티는 발표 자리나 시험지 앞에서 바로 나 — 내용을 설명하지 못하니까.
- 2 유네스코도 학교에서 AI를 어떻게 쓰면 좋을지 공식 안내서를 냈어.
- 3 같은 조사에서 **지침이 있는 학교는 10%도 안 됐어** — 기준을 스스로 세워야 하는 이유야.

가려내는 건 눈썰미가 아니라 순서

- 1 가짜뉴스를 가려내는 건 눈썰미가 아니라 순서야.
- 2 누가 처음 말했나, 언제 일인가, 다른 곳에도 있나 — **이 셋만** 차례로 보.
- 3 셋 중 하나라도 비어 있으면 거기서 멈추면 돼. 멈추는 것도 판단이야.

세 칸을 지나가는 데 1분

- 1 첫 칸은 출처 — 처음 말한 곳까지 거슬러 올라가.
- 2 둘째 칸은 날짜 — 옛 일이 지금 일처럼 돌아다닐 때가 많아.
- 3 제일 힘이 센 건 셋째 칸 — 다른 곳이 따로 취재해 같은 말을 하나.

'그럴듯함'이 증거를 못 하게 된 이유

- 1 AI가 글도 사진도 순식간에 만들 수 있게 됐어.
- 2 그래서 **그럴듯해 보인다**는 더 이상 근거가 못 돼.
- 3 눈으로 믿지 말고 단서로 믿는 습관이 그래서 필요해진 거야.

끊고, 내가 아는 번호로 내가 다시 건다

1 AI를 쓴 사기는 늘 같은 순서야 — 훔내 내고, 아는 척하고, 급하게 몰아치고, 요구해.

2 막는 법은 싱거울 만큼 간단해 — 일단 끊고, 내가 아는 번호로 내가 다시 걸기.

3 진짜 가족이면 다시 걸어도 아무 일 안 생겨.

사기가 노리는 셋, 그걸 깨는 셋

1 사기는 아는 목소리, '지금 당장'이라는 급함, 혼자 결정하게 만들기를 노려.

2 셋을 하나씩 뒤집으면 돼 — 끊고 다시 걸기, 한 박자 쉬기, 옆의 어른에게 말하기.

3 진짜인지 귀로 가려내려 하지 마 — **연락하는 방향을 내가 바꾸는** 게 쉬워.

수사기관이 직접 낸 경고

1 미국 수사기관은 AI로 만든 목소리·사진·영상이 사기에 쓰인다는 공식 경고를 냈어.

2 짧은 음성만 있어도 비슷하게 흉내 낼 수 있어서야.

3 급할수록 한 박자 쉬는 게 제일 빠른 길이야 — 진짜 급한 일은 5분 뒤에도 급하거든.

말기는 비율을 내가 정하고 있나

1 쓰지 말라는 얘기가 아니야 — 말기는 비율을 내가 정하고 있느냐가 전부야.

2 0도 100도 아니고, 남는 게 제일 많은 자리는 가운데야.

3 먼저 5분은 내 머리로 해 보고, 그다음에 말기면 돼.

2025년에 실제로 재 본 것

- 1 글쓰기로 실험한 연구팀이 AI에 많이 맡긴 쪽을 살펴봤어.
- 2 그쪽은 **자기가 방금 쓴 문장을 잘 기억하지 못했다**고 보고했어 — 글은 멀쩡했는데.
- 3 아직 검토 중인 예비 연구니까 결론처럼 외우진 말고.

비율보다 순서

- 1 0%는 느리지만 남고, 100%는 끝나지만 안 남아.
- 2 가운데가 제일 긴 이유는 하나야 — **결과물과 실력을 같이 남기니까.**
- 3 얼마나 기대고 있는지 스스로 점검해 볼 수 있는 공공기관 누리집도 있어.

위험한 정도에 따라 칸을 나눈다

1 AI에도 법이 있어. 그런데 모든 AI를 똑같이 다루지는 않아.

2 쓰임이 위험한 정도에 따라 칸을 나눠 규칙을 다르게 걸어.

3 우리나라 AI 기본법도 2026년 1월에 시행됐어.

네 칸으로 갈라 놓은 유럽연합 AI 법

1 아예 금지 · 고위험 · 알림 필요 · 최소, 이렇게 네 칸이야.

2 금지 칸은 쓰는 것 자체가 막히고, 고위험 칸은 검사를 통과하고 사람이 감독해야 해.

3 알림 필요 칸은 **AI라고 밝히기**, 최소 칸은 특별한 규칙이 없어.

법이 보는 건 기술이 아니라 쓰임

- 1 같은 얼굴 인식이라도 폰 잠금을 푸는 데 쓰면 아래 칸이야.
- 2 사람을 몰래 가려내는 데 쓰면 위 칸으로 올라가.
- 3 우리나라 AI 기본법에서 눈에 띄는 규칙은, AI가 만든 내용은 AI가 만들었다고 표시하라는 거야.

**규칙을 외우는 게 아니라,
확인하는 칸을 내 쪽에 두는 일이야.**



5부에서는 안을 들여다본다.