

비즈니스

보안이 걱정돼 멈춘 AI 도입을 웨이스가 경영진의지의 문제로 보는 이유

걱정은 설계로 풀고, 실패해도 다시 하는 회사가 남습니다

방동걸 (주)웨이스 대표이사

2026년 9월 22일

제조 AI 운영체제 VEXPLOR를 만드는 웨이스에 한 제조사의 팀장이 찾아왔습니다. 현업은 AI를 쓰고 싶은데 임원진이 보안을 걱정해 검토가 멈춰 있다고 했습니다. 회사 자료가 외부 AI로 나가면 어떻게 하느냐는 질문에 답이 없어 회의가 멈춘다는 것이었고, 그 사이 AI를 안 써서 뒤처지는 비용은 누구도 세고 있지 않았습니다. 그때 웨이스가 답한 것은 셋이었습니다. 지금 필요한 것은 보안 대책이 아니라 경영진이 결정할 수 있는 설계안이라는 것, 보안이 필요한 자료는 나누어 설계하면 된다는 것, 그리고 웨이스가 그 설계를 어떻게 하는지였습니다.

이 글은 그 답을 그대로 적은 것입니다. 웨이스가 왜 이 문제를 경영진의 의지의 문제로 보는지, 제조사에 AI를 넣을 때 자료를 어떻게 나누고 언어 모델을 어디에 두며 왜 한 곳이 아니라 여러 곳에 섞어 두는지, 그리고 그 구조를 앞으로 어디까지 가져갈 것인지를 적습니다. 찾아온 회사가 어디인지는 적지 않습니다.

01

웨이스가 현장에서 보는 회사는 둘로 나뉩니다

웨이스가 제조사에 들어가서 보는 회사는 둘입니다. 한쪽은 경영진이 도입을 먼저 결정한 회사입니다. 첫 시도가 실패해도 — 현업이 안 쓰거나, 답이 틀리거나, 기존 시스템과 안 붙어도 — 그것을 도입 비용으로 보고 다음 시도를 지시하고, 두 번째나 세 번째 시도에서 AI가 업무 안에 자리 잡습니다. 다른 한쪽은 결정이 없는 회사입니다. 회의마다 보안, 비용, 인력, 시기, 검증 사례 부족이 차례로 검토 항목에 오르지만 결론은 매번 같습니다. 이번에는 안 한다는 것입니다.

둘을 가르는 것은 기술도 예산도 아니라 경영진의 의지입니다. 결정이 있으면 보안 걱정은 업체에 건넬 요건이 되고, 결정이 없으면 어떤 대책을 가져와도 다음 이유가 나옵니다. 웨이스가 보기에 과거 방식에 머무는 회사에 다음은 없습니다. 경쟁사가 두 번 실패하고 세 번째에 성공하는 동안 그 회사는 세 번째 이유를 찾고 있을 것이기 때문입니다. 두 회사가 어떻게 갈리는지는 구축 업체에 확인할 5가지에 조사 수치와 함께 적었습니다.

웨이스가 하는 일은 결정을 대신하는 것이 아니라, 결정한 경영진이 보안 걱정을 요건으로 바꿀 수 있게 설계를 가져가는 것입니다. 아래는 그 설계입니다.

02

걱정은 맞고, 멈춤은 답이 아닙니다

제조사 임원이 보안을 먼저 묻는 데는 근거가 있습니다. 도면은 대개 원청의 자산이라 밖으로 내보내려면 원청의 허가가 먼저이고, 공정 조건표와 레시피는 그 회사가 수십 년 쌓은 것입니다. 삼성SDS가 국내 기업·공공기관 재직자 1,200명을 조사한 2026년 기업용 클라우드 서비스 현황 보고서에서도 클라우드 사업자를 고르는 1순위 기준이 **조립·제조 업종만 데이터 보안**이었습니다. 웨이스가 만나는 제조사 경영진의 첫 질문이 대개 보안인 것과 같은 결과입니다.

그런데 같은 조사에서 프라이빗 환경을 검토하는 기업이 가장 중요하다고 꼽은 것은 보안이 아니라 기존 시스템과의 연동이었고, 검토를 중단한 이유 1위는 비용이었습니다. 걱정의 이름은 보안이지만 실제로 도입이 막히는 지점은 연동과 비용이라는 뜻이고, 그래서 「안전합니다」라고 말하는 것으로는 도입이 움직이지 않습니다. 어느 자료가 어디로 가는지, 기존 시스템과 어떻게 붙는지, 비용이 얼마인지가 표로 나와야 임원의 질문이 다음 질문으로 넘어갑니다. 웨이스가 가져가는 것은 그 표입니다.

03

웨이스는 자료를 먼저 나눕니다

웨이스가 제조사에 들어가면 모델 데모보다 먼저 하는 일이 있습니다. 진단 단계에서 그 회사의 망 분리 정책·보안 규정과 데이터 등급을 실사해 **자료 등급표**를 만드는 것입니다. 어느 자료가 대외비이고, 어느 자료가 내부용이며, 어느 자료는 공개돼도 되는지를 회사와 함께 정합니다. 어느 방식으로 갈지는 이 실사에서 확정합니다.

이 표가 있으면 「AI를 쓸 것인가」라는 질문이 「이 등급의 자료는 어디까지 갈 수 있는가」로 바뀝니다. 대외비 등급은 밖으로 나가지 않는 것이 원칙이고, 그 등급의 자료를 다루는 모델은 회사 안에 둡니다. 나머지 등급은 계약으로 학습 미사용을 확인한 외부 모델로 처리합니다.

도면과 BOM을 관리하는 웨이스의 PLM이 이 방식의 예입니다. 부품 제조사의 도면은 대외비이자 대개 원청의 자산이라 웨이스 클라우드나 외부 AI로 보내려면 원청의 반출 허가가 먼저입니다. 그래서 PLM의 배치를 3가지로 나눠 제안합니다. 전부 회사 서버에 두는 방식, 전부 웨이스 서버에 두는 방식, 그리고 **도면 파일은 회사 서버에 두고 도면 번호·개정·품목 같은 메타 정보와 BOM과 검색만 클라우드에서 처리하는** 방식입니다. 셋째 방식이면 도면 원본은 회사 밖으로 나가지 않으면서 검색과 BOM 연결은 클라우드로 됩니다. 자료를 나누면 「전부 막거나 전부 열거나」가 아니라 이런 중간이 생깁니다.



회사 자료를 대외비·내부·일반 3등급으로 나눈 세 장소 — 잠긴 서버실, 사무실 책상, 창밖이 보이는 회의실. 대외비 자료는 회사 안 서버에서만 다룹니다

04

모델은 3곳 가운데 고르고, 섞습니다

자료를 나눴으면 언어 모델을 둘 곳도 나눌 수 있습니다. 웨이스는 3가지를 제시하고, 어느 하나를 고르는 것이 아니라 등급에 따라 섞는 혼합 구성을 기본으로 권합니다.

방식	무엇	누구에게	지금 상태
고객 직접 계약	회사 명의로 외부 모델 계약	클라우드 계정이 있는 곳	원칙 · 웨이스도 직접 계약
클라우드 경유	웨이스가 계약 창구를 맡음	계정이 없는 중소·중견	계약 조건 확인 후
회사 안 서버	GPU 서버 + 공개 모델 + 조정	폐쇄망·원청 보안 규정	선택 시 구축, 좁은 일부터

세 방식의 지금 상태는 이렇습니다. **고객 직접 계약**이 원칙이고, 웨이스 안에서도 직접 계약 방식으로 사용합니다. 고객사는 자기 명의로 계약하고 직원용 접속 키를 나눠 주며, 기업용 계약 조건에서 입력 자료를 학습에 쓰지 않는다는 것을 문서로 확인합니다. **클라우드 경유**는 클라우드 계정과 구매 절차가 없는 중소 제조사를 위한 것인데, 모델 사업자의 약관과 맞물리는 조건이 있어 변호사와 사업자 확인을 거친 뒤에 표준으로 삼습니다. **회사 안 서버**는 자료가 밖으로 나가면 안 되는 등급을 위한 것으로, 회사가 산 GPU 서버에 자유 라이선스가 확정된 공개 모델을 올리고 그 회사 업무에 맞게 조정합니다. 공개 모델의 품질은 조정 전후를 실측해야 알 수 있어, 대외비 문서의 검색·분류·요약처럼 좁은 일부터 시작합니다.

웨이스에 중견 제조사가 요청해 오는 것은 대부분 이 셋째 방식입니다. 공개 모델(오픈소스)을 회사 안 서버에 올리고 그 회사의 문서와 업무에 맞게 조정(파인튜닝)해 달라는 요청입니다. 원청 보안 규정과 대외비 비중 때문에 외부 모델로는 시작조차 못 하는 회사가 그만큼 많다는 뜻이고, 그래서 아래 「앞으로 웨이스가 내놓을 것」의 첫 항목이 이 방식의 품질 실측입니다.

이 셋을 섞으면 임원의 걱정과 현업의 속도가 같은 설계 안에 들어갑니다. 대외비는 회사 안 서버로, 나머지는 외부 모델로 나누는 것이 기본 권고입니다.



언어 모델을 두는 곳 3가지 — 회사 명의 계약서(고객 직접 계약), 사업자의 데이터센터(클라우드 경우), 회사가 산 서버(회사 안 서버). 셋 가운데 고르고, 자료 등급에 따라 섞습니다

05

특정 모델에 묶이지 않는 구조로 만듭니다

웨이스가 고객에게 쓰는 문장이 하나 있습니다. 「특정 모델에 묶이지 않습니다. 업무별로 고르고 바꿀 수 있는 구조로 구축합니다.」 「모든 모델을 지원합니다」와 다른 점은, 어느 업무에 어느 모델을 붙였고 무엇으로 바꿀 수 있는지가 표로 나온다는 것입니다.

구조는 이렇습니다. 요약·분류·추출·번역 같은 개별 업무 단계마다 다른 사업자의 모델이나 회사 안 서버의 모델을 도구로 붙일 수 있게 두고, 자료 등급표와 연동해 대외비 등급은 회사 안 모델로 가게 합니다. 이 배분은 진단 뒤에 그 회사에 맞게 구축하는 것이지 제품에 완성돼 들어 있는 기능이 아닙니다.

06

AI가 실행하는 행위 앞에는 사람이 승인합니다

보안 걱정은 자료 유출에서 시작하지만, 웨이스가 더 크게 보는 위험은 AI가 무엇을 실행하느냐입니다. 발주를 내거나 설비에 명령을 보내는 일은 되돌리기 어렵습니다.

그래서 VEXPLOR의 AI 에이전트는 근거 있는 판단까지는 스스로 하고, **발주 같은 실행 행위는 사람 승인 단계를 지나야** 넘어갑니다. 설비 제어 쪽도 같습니다. AI가 낸 명령이 실제 설비에 닿기 전에 그 공장의 제어 로직으로 먼저 실행해 보고 권한 단계와 물리 제약을 검증해 위반 명령을 설비 앞에서 막는 구조입니다(특허 출원 중). 사내 시험에서 동작을 확인했고 실제 제어기와 대조한 수치는 그 뒤에 공개합니다.

자료가 안 나간다는 것과 AI가 사고를 내지 않는다는 것은 다른 문제이고, 둘 다 설계에 들어 있어야 합니다.

07

회사 안 서버를 「더 싸다」로 팔지 않습니다

회사 안 서버 방식은 「더 싸다」로 요약되지 않습니다. 자료가 나가지 않는 대신 GPU 서버 구매와 운영 부담이 붙고, 공개 모델의 품질은 조정과 실측 없이는 보장되지 않기 때문입니다. 앞서 본 조사에서 프라이빗 도입을 중단한 이유 1위가 비용이었던 것과 같은 지점입니다.

어느 방식이든 사용료 구조를 도입 전에 문서로 고지하고, 월 상한과 경보를 붙이고 사용량 증빙을 남깁니다. 임원이 보안 다음으로 물을 것이 비용이고, 그 답이 도입 전에 표로 있어야 검토가 다음 단계로 갑니다.

08

설계는 업체가 가져오고, 결정은 경영진이 합니다

업체의 차이는 데모가 아니라 자료를 나누고 모델을 배치하고 승인 단계를 두는 설계에 있고, 그 설계는 고객이 물어야 드러납니다. 그래서 구축 업체에 확인할 5가지를 따로 적었습니다. 자료 등급표를 먼저 요구하는가, 모델을 둘 곳을 회사가 고를 수 있는가, 특정 모델에 묶이는가, 실행 앞에 승인이 있는가, 회사 안 서버를 더 싸다고만 파는가. 이 5가지는 웨이스에게 물어도 됩니다. 답은 위에 적은 등급표, 3곳 배치표, 승인 단계, 비용 고지입니다. 다만 질문을 던지는 것 자체가 결정 뒤에 오는 일입니다. 경영진이 도입을 결정해야 업체를 가리는 질문이 나오고, 그 질문이 나와야 설계가 회사 안으로 들어옵니다.

09

앞으로 웨이스가 내놓을 것

이 구조에서 아직 다 되지 않은 것이 있고, 순서를 정해 두었습니다.

- **회사 안 서버 모델의 품질 실측 공개.** 중견 제조사 요청의 대부분이 이 방식이므로 먼저 합니다. 대외비 문서의 검색·분류·요약에서 조정 전과 조정 뒤의 품질을 실측해 수치로 내놓습니다. 지금은 실측 전이라 수치를 내지 않습니다. 그 결과가 나오면 「어느 업무까지 회사 안 서버로 되는지」를 수치와 함께 적습니다.
- **클라우드 경유 방식의 표준화.** 모델 사업자 약관과 클라우드 파트너 조건을 변호사·사업자 확인으로 정리한 뒤, 클라우드 계정이 없는 중소 제조사에 기본 제안으로 내놓습니다.
- **자료 등급에 따른 자동 배분.** 등급표에 따라 업무 단계마다 모델이 자동으로 나뉘는 배분을 진단 뒤 구축 항목으로 표준화합니다. 첫 구축 현장이 생기면 그 현장의 결과를 적습니다.



이 글을 한 장으로 요약하면 이렇습니다 — AI 도입은 경영진의 결정에서 갈리고, 웨이스는 자료를 3등급으로 나누고 모델을 3곳에 섞어 두며 실행 앞에 사람을 두는 설계로 결정한 회사와 함께 갑니다

설계는 웨이스가 가져가고 결정은 경영진이 합니다. 결정한 회사와 함께 웨이스는 자료를 나누고 모델을 섞고 실행 앞에 사람을 두는 설계를 현장에 올리고, 위에 적은 순서대로 그 설계를 현장의 결과로 채워 갑니다.

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

10

함께 읽어보세요

- [경영진이 AI 도입을 결정하면 보안 걱정은 설계 요건이 됩니다 — 구축 업체에 확인할 5가지](#)
- [AI 도입 3개월 뒤 아무도 안 쓰는 6가지 형태, 90일 계획으로 막기 \(30분\)](#)
- [왜 AI 도입 검토는 전산실에서 멈출까](#)
- [우리는 왜 사업자등록번호를 저장하지 않기로 했을까](#)



원문 blog.vexplor.com/post/split-data-mix-models
발행 2026년 9월 22일 · 방동걸 (주)웨이스 대표이사

회사 주식회사 웨이스 (WACE Inc.) · 대표이사 방동걸 ·
사업자등록번호 439-87-02852
주소 (18462) 경기 화성시 동탄구 동탄영천로 150, 에이동(A동)
1702·1706호 (영천동, 실리콘밸리동탄)
연락처 전화 070-4730-0629 · contact@wace.me
홈페이지 wace.me · linkedin.com/company/wace-inc



원문



홈페이지



링크드인