

인사이트

경영진이 AI 도입을 결정하면 보안 걱정은 설계 요건이 됩니다

구축 업체에 확인할 5가지

방동걸 (주)웨이스 대표이사

2026년 9월 22일

제조 AI 운영체제 VEXPLOR를 만드는 웨이스에 한 제조사의 팀장이 찾아와 이런 이야기를 꺼냈습니다. 현업은 AI를 쓰고 싶은데 임원진이 보안을 걱정해 검토가 멈춰 있다는 것입니다. 회사 자료가 밖으로 나가면 어떻게 하느냐, 그 답이 없으니 다음 회의로 넘어가고, 다음 회의에서도 같은 질문이 나온다고 했습니다. 웨이스가 제조사 경영진을 만나면 가장 자주 듣는 말이 이것입니다.

이 글은 그 걱정이 틀렸다는 글이 아닙니다. 걱정은 맞습니다. 다만 도입이 멈춘 이유는 보안이 아니라 **경영진의 의지**입니다. 의지가 있는 경영진에게 보안 걱정은 멈출 이유가 아니라 구축 업체에 요구할 설계 요건이 되고, 의지가 없으면 어떤 설계를 가져와도 다음 이유가 나옵니다. 보안이 필요한 자료와 그렇지 않은 자료를 나누어 설계하면 되는 일인데, AI를 구축해 준다는 업체는 많아졌어도 그 회사에 맞게 그 설계를 해 주는 업체는 드뭅니다. 그래서 결정한 경영진에게 필요한 것은 기술 지식이 아니라 업체를 가려내는 질문입니다. 아래에 그 질문 5가지를 적습니다.

01

결국 갈리는 것은 경영진의 의지입니다

같은 업종, 비슷한 규모의 제조사가 지금 둘로 나뉘고 있습니다. 한쪽은 AI를 빠르게 들여왔습니다. 첫 시도는 대개 실패합니다. 현업이 안 쓰거나, 답이 틀리거나, 기존 시스템과 안 붙습니다. 그런데 그 회사는 실패한 그 지점에서 다음 시도를 합니다. 두 번째, 세 번째 시도 끝에 AI가 업무 안에 자리 잡습니다. 다른 한쪽은 보안, 비용, 인력, 시기, 검증 사례 부족까지 갖가지 이유를 들어 과거 방식에 머물러 있습니다. 이유는 매번 다르지만 결론은 같습니다. 이번에는 안 한다는 것입니다.

두 회사의 차이는 기술도 예산도 아닙니다. 첫 실패를 도입 비용으로 보는지, 멈출 이유로 보는지의 차이입니다. 그 판단은 실무자가 아니라 경영진이 합니다. 그래서 보안 걱정으로 멈춘 회사에서 실제로 없는 것은 보안 대책이 아니라 결정입니다. 결정이 있으면 보안 걱정은 업체에 건넬 요건이 되고, 결정이 없으면 대책을 가져와도 다음 이유가 나옵니다. 과거 방식에 머무는 회사가 앞으로 어디에 있을지는 어렵지 않게 그려집니다. 경쟁사가 두 번 실패하고 세 번째에 성공하는 동안 그 회사는 세 번째 이유를 찾고 있을 것이기 때문입니다.

아래는 결정한 뒤에 무엇을 하면 되는지입니다. 보안 걱정을 요건으로 바꾸는 설계가 무엇이고, 그 설계를 할 줄 아는 업체를 어떻게 가려내는지를 적습니다.

02

임원의 보안 걱정은 제조업에서 특히 근거가 있습니다

제조사의 자료는 다른 업종과 다릅니다. 도면은 대개 원청의 자산이고, 공정 조건표와 레시피는 그 회사가 수십 년 쌓은 것이며, 불량 이미지 한 장에도 어느 고객의 어느 부품인지가 들어 있습니다. 그 자료가 외부 AI 서비스로 나간다는 말을 들으면 임원이 멈추는 것은 당연합니다.

이것은 감이 아니라 조사에도 나옵니다. 삼성SDS가 국내 기업·공공기관 재직자 1,200명을 조사한 2026년 기업용 클라우드 서비스 현황 보고서에서, 클라우드 사업자를 고르는 1순위 기준이 대부분 업종에서는 가격이었는데 **조립·제조 업종만 데이터 보안**이었습니다. 조립·제조 업종에서는 임원의 보안 걱정이 개인의 성향이 아니라 업종의 특성으로 나타난다는 뜻입니다.

같은 조사에서 눈여겨볼 것이 하나 더 있습니다. 프라이빗 환경을 쓰거나 검토하는 644명에게 무엇이 가장 중요한지 물었더니 1위가 보안(41%)이 아니라 기존 시스템·네트워크와의 연동 용이성(42%)이었고, 검토하다 중단한 이유 1위는 운영·구축 비용이었습니다. **걱정의 이름은 보안이지만, 실제로 막히는 지점은 연동과 비용**이라는 뜻입니다. 이 차이는 뒤에서 다시 나옵니다.

03

안 쓰는 비용은 청구서로 오지 않습니다

임원이 보안 사고를 걱정하는 만큼 AI를 안 써서 생기는 손해를 걱정하지 않는 데는 이유가 있습니다. 쓰는 비용은 보입니다. 구독료가 청구서로 오고, 사고가 나면 보고서가 올라옵니다. 안 쓰는 비용은 아무 데도 찍히지 않습니다. 견적서 하나를 만나질 걸려 쓰는 동안 경쟁사가 한 시간에 쓸 수 있어도, 그 차이는 이번 달 결산에 나오지 않습니다.

그래서 보안 걱정으로 도입을 멈추면 회사는 안전해진 것처럼 보입니다. 실제로는 한쪽 비용만 세고 있는 것입니다. 이때 필요한 것은 「그래도 도입하자」는 설득이 아니라, 걱정하는 자료를 밖으로 내보내지 않으면서 나머지 일에는 AI를 쓰는 **설계**입니다. 설계가 있으면 임원의 걱정과 현업의 요구가 한 설계 안에 같이 들어가고, 설계가 없으면 한쪽만 이깁니다.

04

자료를 나누면 걱정은 요건이 됩니다

설계의 출발점은 단순합니다. 회사 자료를 등급으로 나누고, 등급마다 어디까지 갈 수 있는지를 정합니다. 「AI를 쓴다·안 쓴다」 양자택일이 아니라, 자료별로 어느 모델을 어디에 두고 쓰는지가 정해집니다.

자료 등급	예시	어디에서 처리하는가
대외비	도면·레시피·원청 자료	회사 안 서버의 모델만
내부	회의록·품질 기록·건적 초안	계약으로 학습 미사용 확인된 모델
일반	공개 자료·교육 자료	외부 모델

이 표가 나오면 임원의 질문은 「자료가 나가면 어떻게 하느냐」에서 「대외비 등급에 무엇을 넣을 것이냐」로 바뀝니다. 앞의 질문은 답이 없어 회의가 멈추고, 뒤의 질문은 답이 있어 회의가 진행됩니다. 이 표를 먼저 내놓는지, 「저희는 다 안전합니다」로 답하는지가 업체의 수준을 가르는 첫 기준입니다.



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

05

모델은 한 곳에 두지 않아도 됩니다

자료를 나눴으면 모델을 둘 곳도 나눌 수 있습니다. 크게 3가지입니다.

- **회사가 외부 사업자와 직접 계약** — 회사 명의로 계약하고 직원용 접속 키를 나눠 줍니다. 기업용 계약이면 입력 자료를 학습에 쓰지 않는 조건을 문서로 확인할 수 있습니다. 내부 등급 자료까지 여기서 처리합니다.
- **클라우드 사업자 경유** — 회사가 클라우드 계정을 따로 만들지 않고 구축 업체가 계약 창구를 맡는 형태입니다. 계약 상대가 누구인지, 자료가 어느 지역 서버에 남는지를 구축 업체가 대신 확인해 문서로 줘야 합니다.
- **회사 안 서버의 공개 모델** — 자료가 밖으로 나가면 안 되는 등급을 위한 것입니다. 회사가 산 GPU 서버에 자유 라이선스 공개 모델을 올리고 그 회사 업무에 맞게 조정(파인튜닝)합니다. 폐쇄망에서도 됩니다. 웨이스에 중견 제조사가 요청해 오는 것도 대부분 이 방식입니다.

여기서 중요한 것은 셋 가운데 하나만 고르는 것이 아니라 **섞는 것**입니다. 대외비 자료는 회사 안 서버의 모델로, 나머지는 외부 모델로 나누어 구성하면 임원의 걱정과 현업의 속도를 둘 다 얻습니다. 이런 혼합 구성을 처음부터 제안하는 업체인지, 아니면 한 가지 방식만 제안하는 업체인지를 보면 됩니다.

06

구축 업체가 늘었지만 조직에 맞게 설계하는 업체는 드뭅니다

AI를 구축해 준다는 업체가 많아졌습니다. 그런데 데모 화면은 서로 비슷합니다. 어느 업체든 문서를 넣으면 요약이 나오고 질문하면 답이 나옵니다. 모델 자체는 사서 쓰는 것이라 업체마다 크게 다를 수가 없습니다.

차이는 데모 뒤에 있습니다. 그 회사의 자료를 등급으로 나누는 일, 등급마다 모델을 어디에 둘지 정하는 일, MES·ERP 같은 기존 업무 시스템과 연결하는 일, AI가 낸 결과가 실행으로 넘어가기 전에 누가 승인하는지 정하는 일입니다. 앞서 본 조사에서 검토 기업이 1순위로 꼽은 요구사항이 보안이 아니라 연동이었던 이유가 여기 있습니다. 이 일은 데모로 보여 줄 수 없고, 그래서 업체 소개 자료에도 잘 나오지 않습니다.

그래서 고객이 판단해야 합니다. 판단에 필요한 것은 모델의 원리를 아는 것이 아니라, 업체가 이 일을 할 줄 아는지 드러나게 하는 질문입니다.

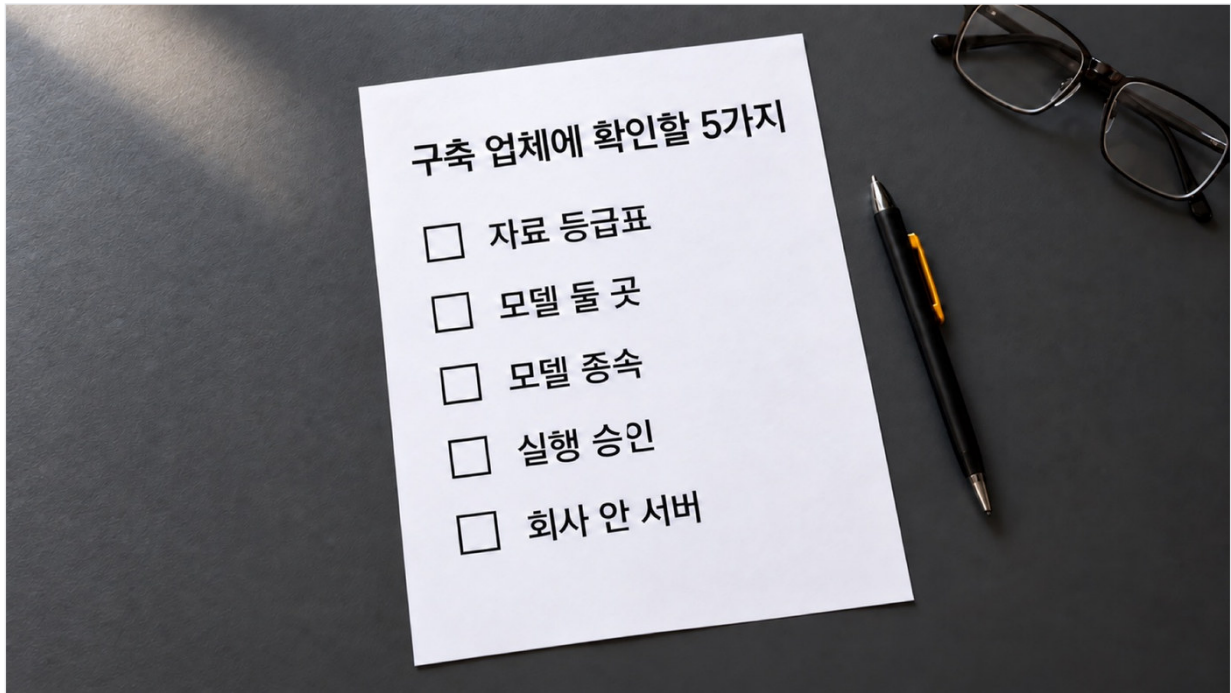
07

구축 업체에 확인할 5가지

아래 5가지를 첫 미팅에서 물으면 됩니다. 통과 답과 탈락 답을 함께 적었습니다.

- **1. 자료 등급표를 먼저 요구하는가.** 통과 답은 「먼저 귀사 자료를 등급으로 나누는 실사부터 하겠습니다」입니다. 탈락 답은 「저희 서비스는 다 안전합니다」입니다. 등급표 없이 안전하다는 말은 근거가 없는 말입니다.
- **2. 모델을 둘 곳을 회사가 고를 수 있는가.** 직접 계약·클라우드 경유·회사 안 서버 가운데 회사 상황에 맞게 고르고 섞을 수 있어야 합니다. 한 가지 방식만 있으면 등급표에 맞춘 배치가 나올 수 없습니다.
- **3. 특정 모델이나 사업자에 묶이는가.** 업무별로 모델을 고르고 나중에 바꿀 수 있는 구조인지, 회사가 이미 쓰거나 직접 만든 모델을 연결할 수 있는지 묻습니다. 「저희는 모든 모델을 지원합니다」는 탈락 답입니다. 바꾸는 절차를 설명하는 것이 통과 답입니다.
- **4. AI가 실행하는 행위 앞에 사람의 승인이 있는가.** 보안은 자료 유출만이 아닙니다. AI가 발주를 내거나 설비에 명령을 보내는 순간이 더 큰 위험입니다. 그 앞에 사람이 승인하는 단계가 설계에 들어 있는지 봅니다.
- **5. 회사 안 서버 방식을 「더 싸다·더 안전하다」로만 파는가.** 회사 안 서버는 자료가 안 나가는 대신 서버 비용과 운영 부담이 붙고, 공개 모델의 품질은 조정 전후를 실측해 봐야 합니다. 이 한계를 도입 전에 문서로 주고 월 사용료 상한과 경보를 붙이는 업체가 통과입니다.

확인 항목	통과 답	탈락 답
1 자료 등급표	실사부터 하겠다	다 안전하다
2 모델 둘 곳	고르고 섞을 수 있다	한 가지뿐이다
3 모델 종속	바꾸는 절차가 있다	모든 모델을 지원한다
4 실행 승인	승인 단계가 있다	AI가 알아서 한다
5 회사 안 서버	한계·비용을 문서로	더 싸고 안전하다



첫 미팅에 가져갈 확인 목록 5가지 — 자료 등급표·모델 둘 곳·모델 종속·실행 승인·회사 안 서버. 통과 답과 탈락 답은 위 표에 있습니다

08

임원 회의에 가져갈 한 장은 현업이 먼저 만들 수 있습니다

업체를 부르기 전에 회사가 먼저 할 수 있는 일이 하나 있습니다. 자료 등급표의 초안을 현업이 만드는 것입니다. 30분이면 됩니다.

- **1단계 — 자료 10종을 적습니다.** 도면, 공정 조건표, 견적서, 회의록, 품질 기록, 설비 매뉴얼, 거래처 목록, 급여·인사 자료, 교육 자료, 공개된 회사 소개. 실제로 AI에 넣고 싶은 것부터 적습니다.
- **2단계 — 자료마다 3가지를 묻습니다.** 원청이나 고객의 자산인가, 법으로 보호 의무가 있는가, 밖으로 나가면 회사가 손해를 보는가. 앞의 둘 가운데 하나라도 「예」면 대외비, 셋째만 「예」면 내부, 셋 다 「아니오」면 일반입니다.
- **3단계 — 등급 옆에 쓰고 싶은 업무를 붙입니다.** 「견적서 초안 작성」, 「회의록 정리」, 「설비 매뉴얼 검색」처럼 업무 이름으로 적습니다. 이 열이 채워지면 AI를 어디에 쓰려는지가 자료 등급과 함께 보입니다.

이 한 장을 임원 회의에 올리면 「자료가 나가면 어떻게 하느냐」는 질문이 「대외비 3종은 회사 안에서만 처리하고, 나머지 7종에 AI를 쓰자」로 바뀝니다. 업체에는 이 표를 건네고 「이 등급표대로 설계해 달라」고 요구하면 됩니다. 등급표를 받아 설계로 답하는지, 등급표와 무관한 데모로 답하는지가 첫 미팅에서 드러납니다.

09

결정한 경영진은 첫 미팅에서 업체를 가립니다

업체를 고르는 데 모델의 구조를 알 필요는 없습니다. 위 5가지를 물었을 때 표와 절차로 답하는 업체와 「안전합니다.다 됩니다」로 답하는 업체가 가립니다. 앞의 답에서는 그 회사에 맞춘 등급표와 배치가 나오고, 뒤의 답에서는 나오지 않습니다.

임원이 보안을 걱정하는 회사는 오히려 좋은 출발점에 있습니다. 걱정이 분명하면 요건도 분명해지고, 요건이 분명하면 업체의 수준이 첫 미팅에서 드러나기 때문입니다. 다만 그 출발점에서 먼저 필요한 것은 설계가 아니라 결정입니다. 경영진이 도입을 결정하면 보안 걱정은 설계 요건이 되고, 첫 실패는 다음 시도의 재료가 됩니다. 결정하지 않으면 걱정은 이유로 남고, 그다음 이유가 그것을 대신합니다.

경영진이 AI 도입을 결정하면 보안 걱정은 설계 요건이 됩니다

구축 업체에 확인할 5가지

자료를 나누면 걱정은 요건이 됩니다

자료 등급	예시	어디에서 처리하는가
 대외비	도면·레시피·원청 자료	회사 안 서버의 모델만
 내부	회의록·품질 기록·견적 초안	계약으로 학습 미사용 확인된 모델
 일반	공개 자료·교육 자료	외부 모델

구축 업체에 확인할 5가지

확인 항목	통과 답	탈락 답
 1 자료 등급표	✓ 실사부터 하겠다	✗ 다 안전하다
 2 모델 둘 곳	✓ 고르고 쉼을 수 있다	✗ 한 가지뿐이다
 3 모델 종속	✓ 바꾸는 절차가 있다	✗ 모든 모델을 지원한다
 4 실행 승인	✓ 승인 단계가 있다	✗ AI가 알아서 한다
 5 회사 안 서버	✓ 한계·비용을 문서로	✗ 더 싸고 안전하다

이 글을 한 장으로 요약하면 이렇습니다 — AI 도입은 경영진의 결정에서 갈리고, 결정하면 보안 걱정은 설계 요건이 되며, 구축 업체에 확인할 5가지로 업체의 수준이 드러납니다

보안 걱정은 맞는 걱정이고, 그 걱정에 답하는 것은 설득이 아니라 설계입니다. 결정했다면 위 5가지를 첫 미팅에 가져가면 되고, 등급표 초안은 현업이 30분이면 만듭니다. 실패해도 다시 시도하는 회사와 이유를 찾아 머무는 회사는 그 결정에서 가립니다.

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

10

함께 읽어보세요

- [AI 도입 3개월 뒤 아무도 안 쓰는 6가지 형태, 90일 계획으로 막기 \(30분\)](#)
- [왜 AI 도입 검토는 전산실에서 멈출까](#)
- [「AI가 유지보수까지 해 드립니다」라는 업체, 계약 전에 무엇을 확인해야 할까요](#)
- [공급사 제안서, AI로 질문 20개 만들고 내 데이터로 검증하기 \(50분\)](#)



원문 blog.vexplor.com/post/five-checks-when-security-stops-ai

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, 실리콘엘리동탄)

연락처 전화 070-4730-0629 · contact@wace.me

홈페이지 wace.me · linkedin.com/company/wace-inc



원문



홈페이지



링크드인