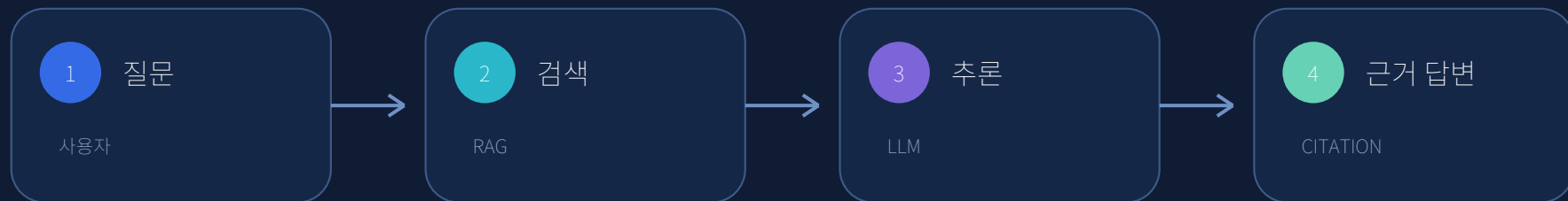


기업 지식을 이해하는 LLM · RAG 챗봇

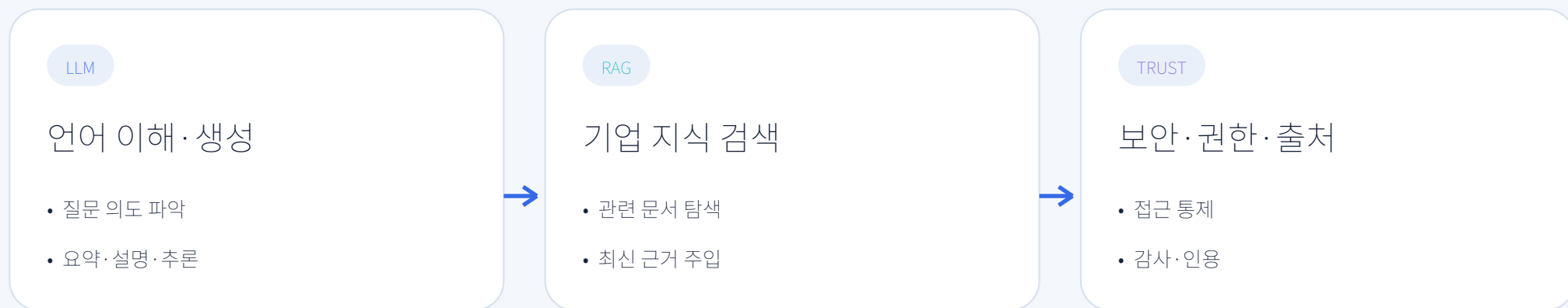
개념부터 구축·보안·활용까지 한눈에 보는 홈페이지/제안서용 가이드



일반 생성형 AI를 넘어, 사내 문서와 권한을 기반으로 신뢰 가능한 답변을 제공합니다.

한 장으로 보는 핵심 개념

기업용 AI 챗봇은 ‘말을 잘하는 모델’에 ‘찾아야 할 지식·지켜야 할 권한·확인 가능한 근거’를 결합한 업무 인터페이스입니다.



핵심 가치

정확성

문서 근거로 환각 감소

최신성

재학습 없이 지식 갱신

통제성

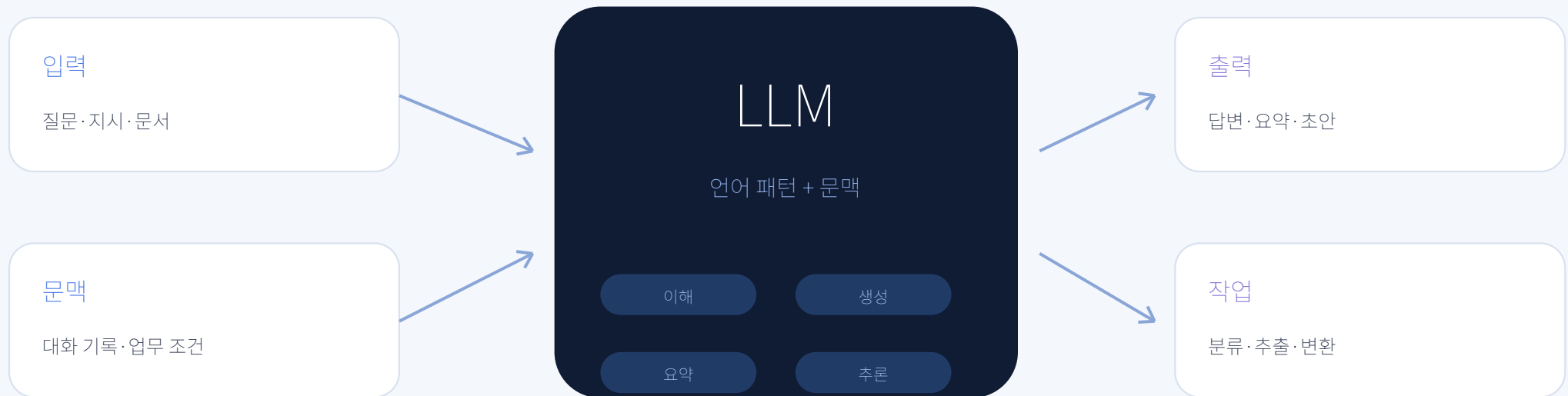
사용자별 권한 적용

생산성

검색·요약·작성 시간 단축

LLM은 무엇인가

대규모 언어 모델(LLM)은 방대한 텍스트에서 언어의 패턴을 학습해, 입력 문맥에 이어질 가능성이 높은 표현을 생성하는 기반 모델입니다.



중요

LLM의 답변은 확률적 생성 결과입니다. '그럴듯함'이 곧 '사실성'이나 '사내 기준 준수'를 의미하지는 않습니다.

일반 LLM만으로 부족한 이유

1

지식 시점

학습 이후의 최신 규정·프로젝트 현황을 모름

2

기업 맥락

사내 용어·제품 코드·업무 절차를 충분히 모름

3

환각

근거가 없을 때도 자연스러운 응답을 만들 수 있음

4

출처 부재

답변이 어느 문서와 조항에서 왔는지 확인이 어려움

5

권한 위험

민감 정보가 사용자 권한과 무관하게 노출될 수 있음

6

갱신 비용

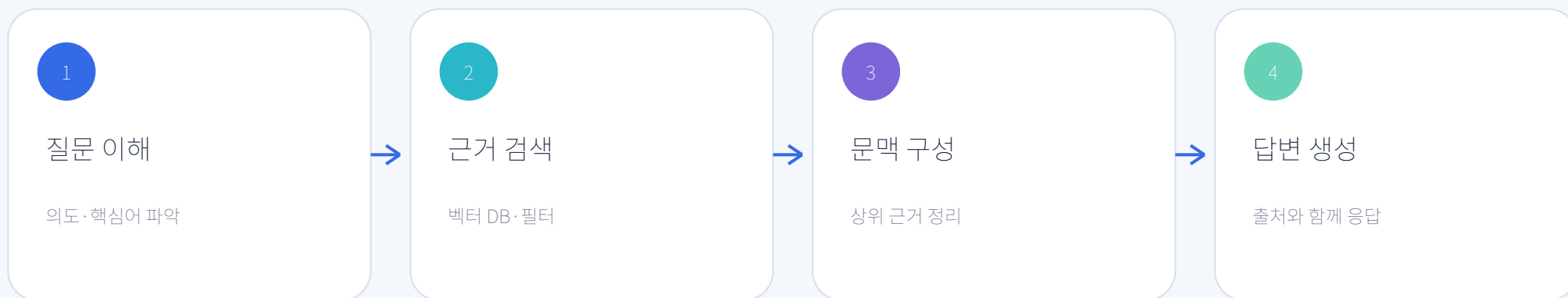
지식 변경 때마다 모델 재학습은 느리고 비효율적

해결 방향

모델을 다시 가르치기보다, 질문 시점에 필요한 기업 지식을 찾아 문맥으로 제공하는 RAG가 현실적인 해법입니다.

RAG란 무엇인가

RAG는 질문과 관련된 기업 문서를 먼저 검색(Retrieval)하고, 찾은 근거를 LLM에 보강(Augmented)해 답변(Generation)을 생성하는 방식입니다.



사용자 질문

“A라인 설비 점검 주기와 최근 변경 근거를 알려줘.”

근거 기반 답변

점검 주기 + 적용 조건 + 개정일 + 원문 링크

정책 문서 4.2절 · 개정 2026-07-15

실제 챗봇 사용 화면: 질문에서 근거 확인까지

The screenshot shows a web-based chatbot interface. On the left is a dark blue sidebar with the text 'KNOWLEDGE AI' at the top. Below it are four menu items: '새 대화', '제조 지식' (highlighted with a dark blue background), '프로젝트', and '경영지원'. At the bottom of the sidebar is the text '홍길동 · 생산기술'. The main area has a title '사내 지식 챗봇 · A라인 설비 점검'. Below the title is a light blue rounded rectangle containing the question 'A라인 프레스 설비의 정기 점검 주기와 근거는?'. Below that is a larger light gray rounded rectangle containing the answer: '정기 점검은 월 1회이며, 가동 500시간 도달 시 추가 점검이 필요합니다. 안전 센서 항목은 매주 확인합니다.' Below the answer is a green button with the text '답변 근거 3건'. To the right of the main area is a light gray sidebar titled '참조 문서'. It contains three items: '설비 예방정비 기준' (with subtext '4.2절 · p.18'), 'A라인 작업표준서' (with subtext '개정 2026-07'), and '안전 센서 점검표' (with subtext '항목 3~8'). At the bottom of the main area is a white input field with the placeholder text '후속 질문을 입력하세요...' and a blue circular button with an upward arrow on the right.

KNOWLEDGE AI

새 대화

제조 지식

프로젝트

경영지원

홍길동 · 생산기술

사내 지식 챗봇 · A라인 설비 점검

A라인 프레스 설비의 정기 점검 주기와 근거는?

정기 점검은 월 1회이며, 가동 500시간 도달 시
추가 점검이 필요합니다. 안전 센서 항목은 매주 확인합니다.

답변 근거 3건

참조 문서

설비 예방정비 기준
4.2절 · p.18

A라인 작업표준서
개정 2026-07

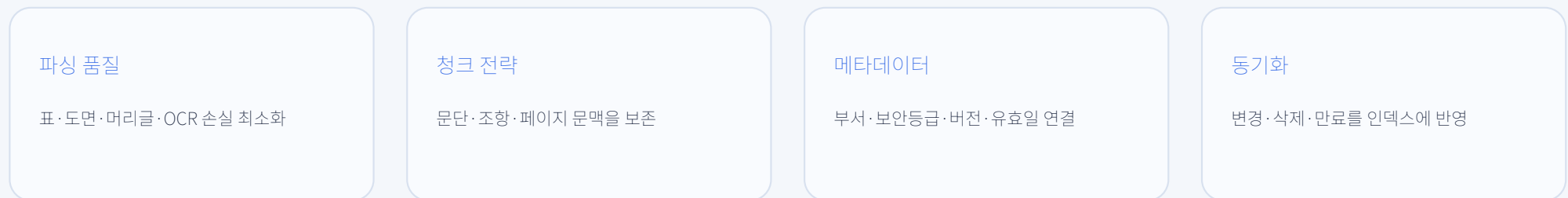
안전 센서 점검표
항목 3~8

후속 질문을 입력하세요...

기업 지식이 검색 가능한 형태가 되기까지

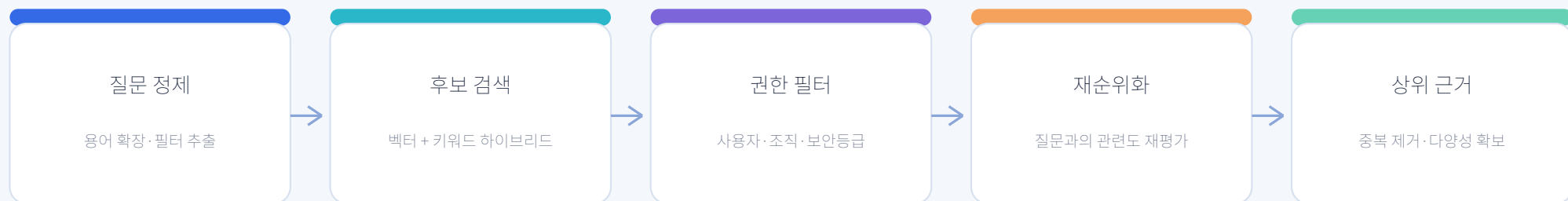


품질을 좌우하는 설계 포인트



질문에서 근거를 찾는 검색 파이프라인

검색은 ‘가장 비슷한 문서’를 찾는 일이 아니라, 답변에 필요한 ‘가장 유효한 근거’를 고르는 과정입니다.



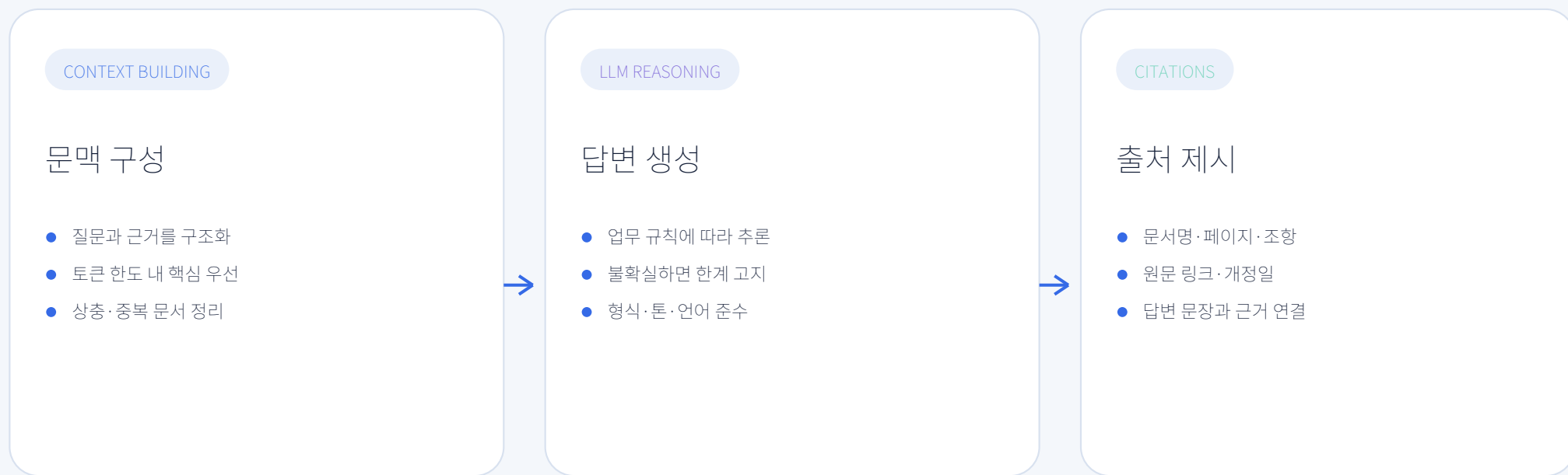
벡터 검색

표현이 달라도 의미가 유사한 문서를 탐색

키워드 검색

제품 코드·규정 번호처럼 정확한 문자열에 강점

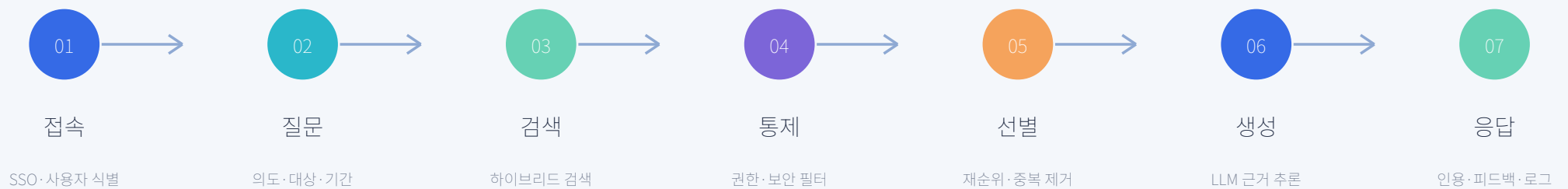
근거가 답변으로 바뀌는 과정



신뢰 원칙

답을 만들 수 없을 때 ‘모른다’고 말하고, 사용자가 원문을 직접 확인할 수 있어야 합니다.

End-to-End: 질문 한 번이 답변이 되기까지



전 구간 가드레일

프롬프트 정책

개인정보 마스킹

권한 검사

유해성 · 기밀 검사

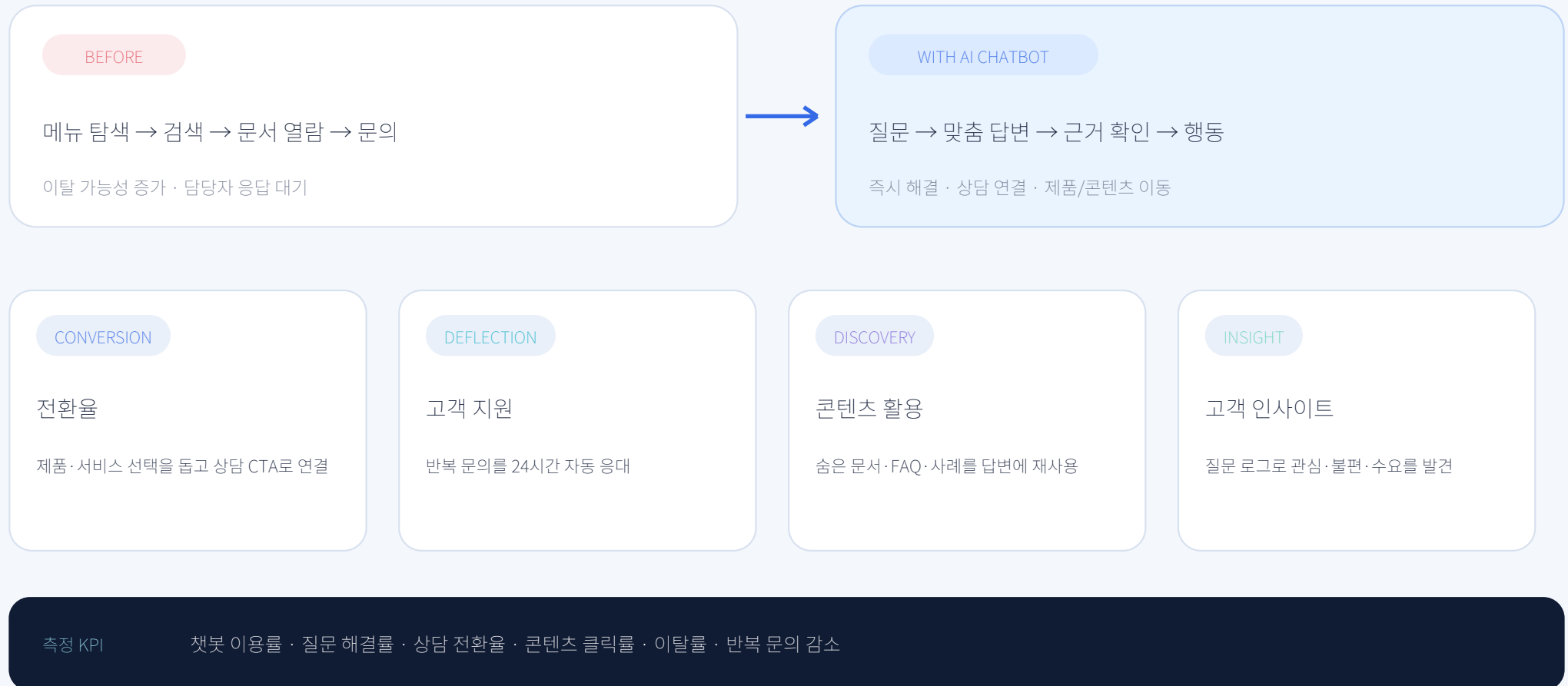
감사 로그

운영 루프

사용자 평가 → 실패 질문 분석 → 검색/프롬프트 개선 → 지식 최신화 → 품질 재검증

웹사이트에 적용하면 무엇이 달라지는가

방문자가 메뉴와 긴 문서를 직접 탐색하는 대신, 자연어로 묻고 즉시 근거 있는 답을 얻습니다. 웹사이트가 '정보 저장소'에서 '상담·전환 인터페이스'로 바뀝니다.



보안과 배포: 기업 환경에 맞는 Private AI

ON-PREMISE

온프레미스

적합성

최고 수준의 통제·망분리

고려사항

운영 복잡도와 인프라 비용 큼

PRIVATE CLOUD

프라이빗 클라우드

적합성

전용 네트워크·관리형 확장

고려사항

클라우드 정책·리전 검토 필요

HYBRID

하이브리드

적합성

민감 데이터는 내부, 모델은 선택적 외부

고려사항

데이터 경계와 라우팅 설계가 핵심

공통 보안 통제

전송·저장 암호화

키·비밀정보 관리

DLP·개인정보 마스킹

모델 입력·출력 정책

감사·이상행위 탐지

권한은 검색 전에, 출처는 답변 뒤에

문서 접근 권한 매트릭스

사용자	공개 지침	부서 문서	프로젝트 기밀
현장 작업자	✓	✓	-
프로젝트 PM	✓	✓	✓
경영지원	✓	✓	-

권한 적용 순서

- 1 SSO/IdP에서 사용자 속성 확인
- 2 문서 ACL · 조직 · 보안등급 필터
- 3 허용된 문서만 검색 · 재순위
- 4 근거 인용 및 접근 로그 기록

금지 패턴

검색 후 답변 단계에서만 숨기는 방식은 위험합니다. 검색 후보 생성 전부터 권한을 적용해야 합니다.

업무별 활용 시나리오

제조 현장

설비·품질·안전

- SOP/매뉴얼 즉시 질의
- 고장 코드 원인·조치 탐색
- 품질 이슈 유사 사례 검색

근거 문서 연결

프로젝트

계약·설계·일정

- 회의록·설계 변경 요약
- 리스크·의사결정 이력 추적
- 계약 조항·산출물 검색

근거 문서 연결

경영지원

인사·재무·구매

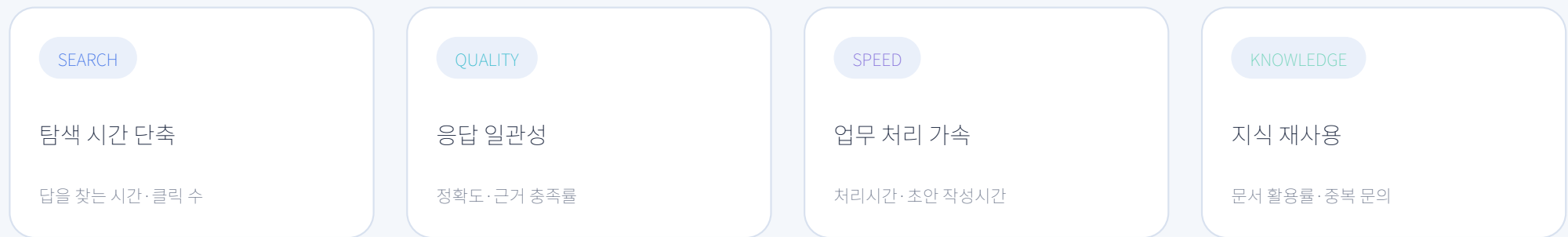
- 규정·복지·정산 안내
- 구매 기준·승인 절차 질의
- 보고서·시장자료 초안

근거 문서 연결

확장 원칙

처음부터 모든 업무를 다루기보다, 문서가 준비되어 있고 반복 질문이 많은 영역에서 시작합니다.

기대 효과와 성과 측정



균형 잡힌 KPI

답변 품질	정확성 · 완전성 · 근거 일치
검색 품질	Recall@K · 재순위 적합도
사용 경험	해결률 · 만족도 · 재질문률
운영 건전성	응답시간 · 비용 · 오류율
안전성	권한 위반 · 민감정보 노출 0건

ROI 관점

절감 시간 × 인건비

+

오류·재작업·교육비 절감

구현 로드맵: 작게 시작하고 검증하며 확장



권장 게이트

각 단계는 '품질·보안·운영 비용' 기준을 충족한 뒤 다음 범위로 확장합니다. 모델 성능보다 데이터 준비와 평가 체계가 먼저입니다.

관리자 화면: 품질과 운영 상태를 지속 개선

주간 질문

12,480

+18%

근거 포함률

96.4%

+2.1%

평균 응답

2.8초

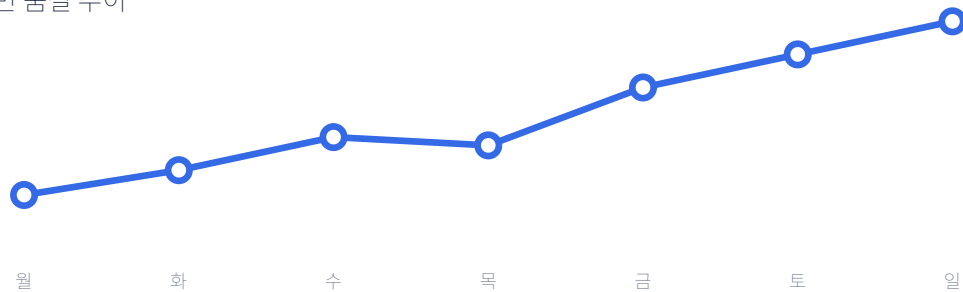
-0.4초

미해결 질문

214

분석 필요

답변 품질 추이



운영 알림

● 권한 필터

정상

● 문서 동기화

3건 지연

● 품질 평가

목표 이상

NEXT STEP

대표 업무 1개 · 핵심 문서 100~500건 · 평가 질문 50개로 4~8주 파일럿을 설계하세요.

그래서, 적용하면 우리 제품이 더 좋아집니다

단순히 답을 생성하는 챗봇이 아니라, 기업 지식을 고객과 임직원의 행동으로 연결하는 신뢰 가능한 AI 제품입니다.

01

정확한 답변

사내 문서와 최신 근거를 바탕으로 답변합니다.

02

안전한 활용

사용자 권한과 데이터 경계를 지킵니다.

03

웹 성과 연결

답변을 상담·구매·콘텐츠 행동으로 연결합니다.

04

지속적 개선

질문·평가·운영 데이터로 품질을 높입니다.

제품 메시지

“찾게 하는 웹사이트”를 넘어, 고객의 질문을 이해하고 근거로 설득하는 AI 경험을 제공합니다.