

# 챗봇을 넘어, 실행하는 AI 에이전트

묻는 말에 답하는 것은 출발점입니다. 지시를 받아 스스로 계획하고, 실행하고, 결과를 확인합니다. 되돌릴 수 없는 일은 사람의 승인을 받습니다.

대상  
기업·기관

발행  
화려한덕후들(주) · 2026

# 사람이 하지 않아도 되는 일에 사람이 묶여 있습니다

## 응대

같은 질문이 채널마다 반복됩니다. 답은 이미 사내 문서에 있는데, **찾아서 옮겨 적는** 일에 담당자 시간이 들어갑니다.

## 반복 업무

보고서 작성·일정 등록·연락처 정리처럼 정형화된 일이 사람 손에 남아 있습니다. **판단이 필요 없는** 일인데도 사람이 붙어야 합니다.

## 이관

담당자가 바뀔 때마다 맥락이 끊기고, 고객은 같은 말을 다시 합니다. 인수인계 문서를 만들어도 **대화의 맥락**까지는 남지 않습니다.

데모는 많고,  
업무에 넣은 사례는 드뭅니다.

- 대부분의 챗봇은 **«말하기»** 까지다 — 등록·수정·발송은 사람 몫으로 남는다
- 실행을 붙이면 이번엔 **통제**가 문제가 된다 — 누가 무엇을, 잘못되면 어떻게
- 그래서 **도입 결정이 멈춘다**

실행이 빠져  
도입이 멈춘다

02

# 답하는 AI 와 실행하는 AI는 다릅니다

| 구분         | 일반 챗봇      | GO-CHATBOT 에이전트    |
|------------|------------|--------------------|
| 할 수 있는 것   | 질문에 답한다    | 답하고, 실행한다          |
| 한 번의 지시    | 한 번의 응답    | 계획 → 실행 → 관찰 → 재계획 |
| 쓰기 작업      | 대부분 없음     | 96개 — 등록·수정·발송·배정  |
| 권한         | 대화 단위      | 기능 단위 역할 게이트       |
| 되돌릴 수 없는 일 | 막거나, 그냥 실행 | 사람 승인 후 실행 (HITL)  |
| 실행 기록      | 대화 로그      | 감사 로그 · 승인 이력      |
| 비용         | 토큰 총량      | 기능별 비용 등급 · 미터링    |

밝게 표시한 줄이 이 문서의 핵심입니다. 이 표에서 처음 나오는 말 셋 — **HITL** 은 Human-in-the-Loop, 「사람이 중간에 승인한다」는 뜻입니다. **역할 게이트**는 기능마다 실행할 수 있는 역할이 정해져 있다는 뜻이고, **미터링**은 누가 얼마나 썼는지 실행 단위로 기록·차감하는 것입니다.

「물어보면 답한다」가 아니라  
 「시키면 한다, 다만 위험한 것은 물어보고 한다」입니다.

시키면 한다,  
 위험한 건 묻고

03

## 등록된 165개의 실행 역량

에이전트가 호출할 수 있는 기능은 미리 등록된 목록 안에만 있습니다. LLM 이 임의의 명령을 지어내 실행할 수 없습니다.

# 96

쓰기 — 실제로 수행

# 69

읽기 — 조회·요약

# 29

LLM 사용 · 나머지 136는 정해진 코드가 처리

| 영역             | 역량 수 | 예                               |
|----------------|------|---------------------------------|
| 프로젝트 · 업무(PMO) | 83   | 과제 등록 · 담당 배정 · 진척 갱신 · 보고서 생성  |
| 운영 · 설정        | 21   | 상태 점검 · 통계 조회 · 위젯·크롤링 설정       |
| 지식 · 문서        | 15   | 문서 처리 · 지식 그래프 · FAQ · 유사 문의 검색 |
| 생성형            | 12   | 이미지 · 영상 · 프롬프트 제작              |
| 고객관리(CRM)      | 11   | 고객 등록 · 담당자 배정 · 이력 정리          |
| 일정 · 할일 · 예약   | 11   | 일정 등록 · 리마인드 · 예약 확인·변경         |
| 계정 · 멤버        | 7    | 초대 · 가입 요청 처리 · 권한 변경           |
| 상담 · 응대        | 5    | 대화 요약 · 답변 제안 · 상담원 이관          |

2026-09-02 기준으로 시스템에서 **직접 집계**한 값이고, **여덟 줄을 더하면 165**이 됩니다 — 일부만 추린 표가 아닙니다. 도입 시 귀사 업무에 맞춰 추가 등록이 가능합니다.

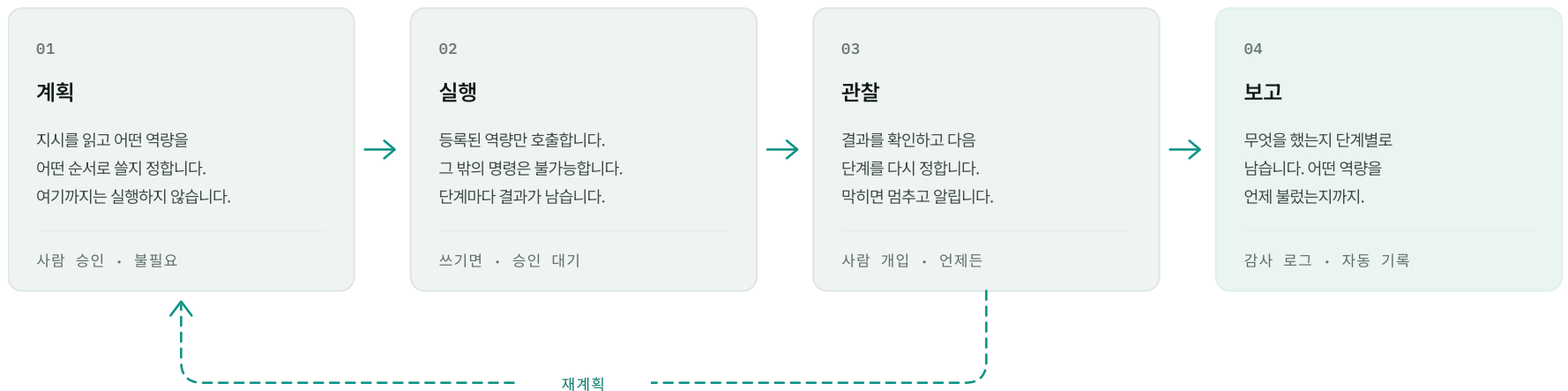
역량은 등록된  
목록 안에만

# 04

# 한 번 지시하면 여러 단계를 스스로

## 「이번 주 지연된 과제 정리해서 담당자별로 알려줘」

이 지시 하나가 부른 역량 — 지연 과제 조회 → 담당자별로 묶기 → 요약 작성 → 담당자에게 알림. 아래 순환을 네 바퀴 돈 결과입니다.



한 번 지시, 여러 단계 자율

05

막히면 멈추고 알립니다. 단계마다 결과가 표시되므로 중간에 사람이 개입할 수 있고, 단순한 한 가지 지시는 이 순환을 건너뛰고 바로 처리해 비용을 줄입니다.

쓰기 작업에 닿으면 이 순환이 멈추고 **사람의 승인을 요청합니다** — 다음 쪽.

# 되돌릴 수 없는 일은 승인을 받고 합니다

쓰기 작업은 실행 직전에 멈추고 승인을 요청합니다.



## 왜 이 경계인가

완전 자동은 편하지만 사고 시 되돌릴 수 없습니다. 완전 수동은 안전하지만 도입 효과가 없습니다. 읽기는 자동, 쓰기는 승인 — 실제 업무에 넣을 수 있는 경계였습니다.

읽기는 자동,  
쓰기는 승인

06

# 에이전트가 폭주하지 않도록



## 화이트리스트

등록된 165개 밖의 기능은 호출 자체가 불가능합니다. 모델이 명령을 지어내도 실행되지 않습니다.



## 역할 게이트

85개는 실행 역할이 지정돼 있습니다(관리자 22 · PMO 50 · 상담원 8 · 슈퍼관리자 5). 나머지 80개는 운영자 공통이고, 그중 쓰기 30개는 승인을 거칩니다.



## 비용 등급

저비용 104 · 보통 47 · **고비용 14**  
— 무거운 작업만 통제 대상입니다.



## 사용량 미터링

실행마다 사용량이 기록·차감됩니다.  
예상 밖의 소모를 조기에 확인합니다.

## ⚙ 기본 설정

### 업종 프리셋

프리셋 기본값 불러오기  
선택만으로 저장되지 않습니다. "불러오기"로 권장값을 채운 뒤 저장하세요.

### ☒ 에이전트 모드 활성화

끄면 기존 RAG 챗봇 그대로 동작합니다(의도 라우터·웹검색 비활성).

### 처리할 질문 갈래 (출처 의도)

체크한 갈래만 해당 도구가 노출·동작합니다. 예: 실시간 사실을 끄면 날씨·미세먼지·버스 도구가, 작업을 끄면 예약·안내(민원 가이드) 도구가 챗봇에서 비노출됩니다.  
상담원 연결·범위 밖 거절·본인확인 같은 안전 제어는 체크 여부와 무관하게 항상 동작합니다.

## 🛡 가드레일

### 거절(범위 밖) 주제

정치적 견해  
투자 권유  
의료 진단

한 줄에 하나. 이 주제 질문은 정중히 거절합니다.

### 면책 안내 문구

☒ 강한 불만 신호 시 상담원 연결 안내

- 165개 중 **29개만 LLM** 을 사용합니다 — 나머지는 같은 입력이면 같은 결과가 나오는 코드가 처리합니다
- 모델은 «무엇을 부를지» 를 고르고 **처리**는 코드가 **합니다** — 환각이 개입할 여지가 좁습니다

고르는 건 모델,  
하는 건 코드

07

실제 관리자 화면입니다. 거절할 주제와 면책 문구를 화면에서 직접 정합니다 — 프롬프트를 고치지 않습니다.

# 근거 없이는 답하지 않습니다

질문 하나에 네 곳을 동시에 조회하고, 재랭킹해 가장 관련 있는 근거로 답합니다.

## 01 실시간 페이지

사용자가 보고 있던 화면을 함께 읽습니다.

## 02 사내 문서

PDF·워드·엑셀을 잘라 «뜻» 기준으로 검색합니다.

## 03 홈페이지

매일 새벽 자동 재학습으로 최신 상태를 유지합니다.

## 04 지식 그래프

용어·제품·조직 관계를 2단계까지 탐색합니다.

### 크롤링 설정

#### 크롤링 대상 웹사이트 URL \*

https://example.com  
https://example.com/products  
https://example.com/about

① 귀사의 웹사이트 URL을 입력하세요. 여러 URL은 줄바꿈으로 구분합니다. (각 URL을 별도의 줄에 입력)

#### 크롤링 활성화

☒ 자동 크롤링 활성화 (매일 02:00 실행)

비활성화하면 자동 크롤링이 중지됩니다.

#### 최대 크롤링 페이지 수

50

한 번의 크롤링에서 수집할 최대 페이지 수 (10-1000)

- 근거를 못 찾으면 **답을 만들지 않고** 상담원에게 넘깁니다
- 답변마다 어떤 자료를 근거로 썼는지 남아 원인 추적이 됩니다

지어낸 답 하나가  
도입을 되돌립니다.

지어낸 답 하나가  
도입을 되돌린다

08

위 03 홈페이지 경로의 실제 설정 화면입니다. 매일 02시 자동 재학습을 여기서 켭니다.

## 문서에 쓰여 있지 않은 것까지

문서 검색만으로는 「A 제품 담당 부서의 연락처」 같은 질문에 답하기 어렵습니다. 용어·조직·제품을 관계로 정리해 두면 여러 문서에 흩어진 사실을 이어 답할 수 있습니다.

### 자동 추출

문서를 올리면 인물·조직·제품·개념과 그 관계를 자동으로 뽑습니다.

### 2단계 탐색

질문에 등장한 대상에서 두 단계까지 따라가 근거를 모읍니다.

### 지속 정제

운영하며 쌓인 대화로 관계를 보강하고, 승인 후 반영합니다.

- 「A 제품 담당 부서 연락처」 — 제품 → 부서 → 담당자 를 이어 답합니다
- 세 정보가 서로 다른 문서에 있어도 관계를 따라가면 하나로 모입니다

검색은 문서를 찾고,  
그래프는 사실을 잇습니다.

문서에 없는  
연결까지

09

지식 그래프는 Pro 플랜 이상에서 제공합니다.

# AI가 못 풀면 맥락째 넘깁니다

## 이관 판단

근거 부족·감정 신호·명시적 요청을  
기준으로 스스로 판단합니다.

## 맥락 인계

오간 대화와 참조 근거가 함께  
넘어갑니다. 고객이 같은 말을 반복하지  
않습니다.

## 상담원 화면

대기 중인 상담을 한 화면에서 확인하고  
응대합니다.

## 운영자 모바일 앱

이동 중에도 상담 확인·지시·승인이  
가능합니다.

→ 함께 넘어가는 것 — 오간 대화 전문 · 답변에 쓴 근거 문서 · 이관을 판단한 이유 · 이전 상담 이력

## 위기 신호는 과금보다 먼저

위험 신호가 감지되면 구독·잔여 횟수와 무관하게 지원 안내가 먼저 나갑니다. 설계상 그렇게 고정돼 있습니다.

# 고객이 있는 창구에서 **같은 엔진이**

## 카카오톡 채널

오픈빌더 스킴으로 연결. 관리자에서 웹훅 주소를 발급합니다.

**필요:** 채널 + 오픈빌더 계정

## 네이버 톡톡

스마트플레이스·쇼핑 문의를 그대로 받습니다.

**필요:** 톡톡 파트너 계정

## 인스타그램 DM

브랜드 계정 문의를 자동 응대합니다.

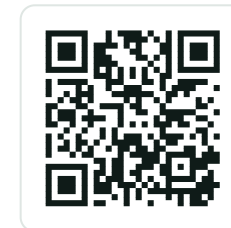
**필요:** 비즈니스 계정 연결

## 텔레그램

사내 봇으로도 활용할 수 있습니다.

**필요:** 봇 토큰 하나

- 채널별로 답변을 따로 만들 필요가 없습니다 — **지식과 정책이 하나입니다**
- 채널 문의도 **상담원 이관·감사 로그**가 동일하게 적용됩니다
- 고객이 어디로 물었든 **응대 이력이 한 화면에** 이어집니다



실제 채널을 지금 확인하실 수 있습니다

창구는 넷, 엔진은 하나

# 11

# 민감한 자료는 회사 밖으로 보내지지 않습니다

## GO-Chatbot 엔진 · 공통

모든 조회에 «소속 조건» 이 강제됩니다. 조건이 빠진 질의는 실행되지 않습니다.

격리 경계



고객사가 늘어도 저장소는 계속 나옵니다. 조회·실행·설정 변경은 감사 로그에 남아 «누가 언제 무엇을» 했는지 추적됩니다.



### 자체 서버 모델

사내 설치 모델(vLLM)로 처리하도록 전환할 수 있습니다. 외부 API 로 전송되지 않습니다.



### 감사 로그

실행·승인·설정 변경이 기록됩니다. 누가 언제 무엇을 했는지 추적됩니다.



### 권한 분리

관리자·상담원·영업·PMO 역할이 분리되고, 기능 단위로 접근이 제한됩니다.

고객사별로  
저장소가 나뉜다

12

- 개인정보는 **최소 수집** 원칙으로 설계했습니다
- 보안 검토 자료와 구성도는 **도입 검토 단계에서 별도** 제공합니다

# 검토·실사에서 먼저 묻는 것들

도입 검토와 보안 실사에서 반복해서 요구된 항목입니다. 표시 없는 항목은 협의 대상으로 적었습니다.

| 구분  | 항목              | 현재 제공                                   | 확인 방법  |
|-----|-----------------|-----------------------------------------|--------|
| 보안  | 클라우드 보안인증(CSAP) | 간편등급 요건 기준으로 통제 항목 정비 — 인증은 취득 전        | 일정 협의  |
| 보안  | 관리자 인증          | 2차 인증(TOTP) · 공공 설정 시 콘솔 접근 IP 제한       | 데모     |
| 보안  | 암호화             | 연동 자격증명 · 결제수단 · 2차 인증 비밀을 암호화 저장       | 구성도    |
| 데이터 | 저장 위치           | 국내 서버 · 사내 설치 모델을 고르면 외부로 전송되지 않음       | 구성도    |
| 데이터 | 개인정보            | 최소 수집 설계 — 식별자는 해시로 두고 민감 항목을 두지 않음     | 스키마 열람 |
| 데이터 | 고객사 격리          | DB · 벡터 저장소를 고객사별로 분리 (12쪽 구성도)         | PoC    |
| 운영  | 백업              | 매일 자동 백업 · 무결성 해시 검증 · 보관 기간 정책         | 운영 문서  |
| 운영  | 감사 · 파기         | 실행 · 승인 · 설정 변경 기록 · 계정 삭제 30일 후 완전 삭제  | 로그 열람  |
| 운영  | 성능 · 가용성        | 응답 시간 · 동시 처리량은 PoC 에서 귀사 환경으로 실측해 드립니다 | PoC    |
| 조달  | 계약 방식           | 디지털서비스물 등록 준비 중 — 계약 형태는 협의             | 협의     |

인증 취득 여부를 부풀리지 않았습니다. 확인하시면 드러날 항목이고, 그 한 줄 때문에 검토가 멈추는 편이 도입 후에 문제가 되는 것보다 낫다고 봅니다.

요건은 갖췄고  
인증은 진행 중

13

## 작게 검증하고 확산합니다

| 단계      | 기간 | 하는 일                                 | 확인 기준       |
|---------|----|--------------------------------------|-------------|
| 1 · 준비  | 1주 | 대상 업무 선정 · 문서 수집 · 계정 개설             | 범위 합의       |
| 2 · PoC | 2주 | 문서 학습 · 답변 품질 점검 · 질문 세트 검증          | 정답률 · 근거 표시 |
| 3 · 파일럿 | 4주 | 한 부서 적용 · 상담원 이관 운영 · 에이전트 «읽기» 역량부터 | 처리 시간 · 이관율 |
| 4 · 확산  | 협의 | 쓰기 역량 승인 정책 수립 · 채널 연동 · 부서 확대       | 업무 절감       |

단계마다 **손에 남는 것** — 1 범위 합의서 · 2 질문 세트별 정답률 결과 · 3 부서 운영 리포트와 이관율 · 4 승인 정책과 확산 계획. 다음 단계로 갈지는 이 산출물을 보고 정합니다.

- 에이전트는 **읽기 역량부터** 켜고, 쓰기는 승인 정책을 정한 뒤 단계적으로 엽니다
- 각 단계에서 **되돌릴 수 있는 상태**로 유지합니다
- 다음 단계로 넘어가기 전에 **앞 단계 산출물**을 함께 확인합니다 — 기준에 못 미치면 그 자리에서 멈춥니다

작게 검증하고  
확산한다

14

# 업종은 달라도 자리 잡는 방식은 같습니다

특정 고객사의 실적이 아니라, 운영에서 반복해서 나타난 유형입니다.

| 업종 유형    | 반복되는 문의            | AI 가 처리               | 사람이 판단      |
|----------|--------------------|-----------------------|-------------|
| 법무·세무    | 상담 절차·필요 서류·비용 기준  | 절차와 서류 목록 안내·상담 예약 접수 | 사건 판단·수임 결정 |
| 의료·병원    | 진료 시간·오시는 길·검사 준비물 | 안내 회신·예약 접수           | 진단·처방       |
| 제조·부품    | 규격·호환·납기·견적 요청     | 규격 자료 회신·견적 요청 접수     | 단가·납기 약속    |
| 이커머스     | 배송·교환·환불·재고        | 정책 안내·처리 절차 회신        | 예외 보상 판단    |
| SW·기술 지원 | 설치·오류 코드·버전 호환     | 매뉴얼을 근거로 회신·재현 정보 수집  | 원인 규명·패치    |

반복 문의는 자동,  
판단은 사람

15

- 들어오는 문의의 상당수는 이미 문서에 답이 있는 반복 질문입니다
- AI 는 근거를 들어 답하고, 판단이 필요한 건은 맥락째 사람에게 넘깁니다
- 홈페이지·문서가 갱신되면 답변도 함께 최신화됩니다

도입 기업의 실사례와 수치는 해당 고객사의 사용 동의를 받은 범위에서 별도 자료로 제공합니다. 귀사 문의 30건으로 2주 PoC를 돌리면 같은 표를 귀사 데이터로 채워드립니다.

## 규모에 맞춰 단계적으로

| 플랜     | 월          | 대화      | 문서   | 주요 대상             |
|--------|------------|---------|------|-------------------|
| 스탠다드   | 239,000원   | 2,500회  | 25건  | 부서 단위 도입          |
| 프로     | 500,000원   | 6,000회  | 50건  | 지식 그래프·음성이 필요한 조직 |
| 비즈니스   | 1,200,000원 | 15,000회 | 150건 | 다중 사이트 · API 확장   |
| 엔터프라이즈 | 별도 견적      | 협의      | 협의   | 보안 요건 · 전용 인프라    |

어느 플랜이든 포함 — 문서 학습 · 채널 연동 · 상담원 이관 · 감사 로그. **사용량이 넘치면** 플랜 변경 없이 30일 이용권으로 보완합니다. **별도 협의**는 전용 인프라 · 사내 설치 · 응답·복구 기준(SLA)입니다.

- **14일 무료 체험** — 카드 등록이 필요 없습니다. 먼저 써 보고 정하십시오
- 부가세 별도 · 연간 결제 시 할인 적용
- 사용량이 물리는 시기는 **30일 이용권**으로 보완합니다
- 엔터프라이즈는 전용 인프라 · 사내 설치(온프레미스) · 응답·복구 기준(SLA) 을 협의합니다

밝게 표시한 줄은 **권장 플랜**이라는 뜻입니다 — 나머지도 모두 제공합니다. 금액과 한도는 시스템에 등록된 값을 그대로 옮긴 것입니다.

### 2주면 우리 문서로 검증됩니다.

대표 문의 **30건**과 관련 문서를 주시면 격리된 환경에 학습해 실제 답변을 보여 드립니다. 정답률·근거 표시·이관 판단을 함께 확인합니다 — 절차와 확인 기준은 **14쪽 표**와 같습니다.



지금 답하는 AI 를 직접 확인하실 수 있습니다

연락처

go-chatbot.ai.kr · 070-4455-0099 · help@g-oduk.com

규모에 맞추고,  
2주면 검증

16