GH · 법률·규정 해석 지원

경기주택공사 25명

2026 · 06 · 01

7 HOURS

법령을 매일 뒤지는 손에서 출처가 따라붙는 챗봇으로

Claude Project + Korean Law MCP로
본인 부서 법령 챗봇을 손으로 만들고
환각을 4겹으로 차단하는 7시간 풀버전.

Claude Project · Korean Law MCP · 시스템 프롬프트 · Fail-safe 4규칙 · verify_citations · 부서별 5탭

PRESENTER

김혜련 · artetlab

v1 · 2026

강의 교안

gh-law2.artetlab.com

김혜련 *Kyra Kim*

이노핏파트너스 프로젝트 교수
artetlab 대표

SPEAKER

AI 자동화 에이전시 artetlab을 운영하며,
Make.com과 n8n 기반 노코드 자동화와
Claude Code 활용 Agent 엔지니어링이 주요 작업 영역입니다.
기업 임원·실무자를 위한 AI 활용 교육을 병행하고 있습니다.

저서

『당신의 첫 AI 직원』

서울경제경영출판사 · 2026.02

주요 강의 이력

LG AX Camp for Leaders 임원교육
멀티캠퍼스 n8n AI 자동화 실전
SKT Design Camp Dify 교육 코칭
LG U+ 리더 AI 업무자동화 심화
세계일보 Vibe-coding 코칭
KCH그룹 인사총무 AX 파일럿 외 다수

커뮤니티

GPTers 스터디장 16~21기 · AI 자동화 커뮤니티 운영

TODAY · 7 HOURS

오늘 끝나면 손에 남는 5가지

01

CHATBOT · 본인 부서

본인 부서 법령 챗봇 1개

Claude Project · 부서별 시스템 프롬프트 v2 · Korean Law MCP 17개 도구 활성화

02

FAIL-SAFE

"출처 없으면 답 안 함" 챗봇 설계 능력

출처 URL 필수 · 매칭 실패 시 거절 · 판례 가드 · 개정 표시 강제

03

KILLER 3

새 도구 3종을 본인 업무에 매핑한 한 줄

verify_citations · impact_map · action_plan 각각 본인 시드 5건과 1:1

04

SEED 5

시드 질문 5건 — 강의 끝에 실제 작동

설문 Q13의 본인 질문이 본인 챗봇에서 출처와 함께 답해지는 상태

05

ACTION PLAN · 내일 출근해서

내일 출근해서 할 일 4가지

저장하라 · 돌려라 · 잡아라 · 나눠라 — 마지막 30분에 다시 모입니다

AI가 지어낸 판례가 **우리 법정**에 들어왔습니다.

2026년 · 한국 법원과 경찰이 '존재하지 않는 판례'를 인용했고,
같은 해 한 회사는 챗봇의 틀린 답으로 배상 책임을 졌습니다.
오늘 7시간 끝에 이 두 장면으로 다시 돌아옵니다.

Opening

HOOK · 이미 벌어진 일

법정에 제출된 판례가 존재하지 않았습니다

2026 한국 · 법원·경찰이 AI가 만든 '유령 판례' 인용 → 법원행정처 소송비용 부담·대한변협 징계 의뢰 가능 · 2024 Air Canada · 챗봇 오답에 회사가 배상 책임

판 결

사 건	2023다123456 손해배상(기)
원 고	김○○
피 고	이○○
변론종결	2024. 1. 10.
판결선고	2024. 2. 7.

주 문

1. 피고는 원고에게 200,000,000원 및 이에 대하여 2023. 7. 1.부터 다 갚는 날까지 연 12%의 비율에 의한 돈을 지급하라.

2. 소송비용은 피고가 부담한다.

3. 제1항은 가집행할 수 있다.

이 유

대법원 2018다123456 판결은,

이 판결은, 존재하지 않습니다

WHY · 우리의 일상

여러분 25명이 지금 이렇게 일하고 있습니다

01

빈도 · 13명 / 19명

“거의 매일 또는 주 2-3회”

사전 설문 Q4 — 응답자 19명 중 13명이 법령을 거의 매일 또는 주 2-3회 찾습니다. 일상의 한가운데.

02

시간 · 평균 10분-1시간

한 건당 10분-1시간, 길면 1-3시간

조항 찾고 시행령 연결하고 판례 확인. *설문 Q8*
이 시간을 줄여주는 한 페이지의 챗봇이 오늘의 결과물.

03

우려 · Q19A 평균 4.5점

“환각은 절대 안 된다”

12명이 5점 — “잘못된 조항이나 없는 판례를 만들어내는 것은 절대 안 된다”.
2026년 한국 법정·경찰에서 이미 일어난 일 — 우리가 아닐 이유가 없습니다.

가장 자주 막히는 곳 — **조항-시행령 연결 · 판례 확인 · 유권해석 검색 · 강행/재량 구분 · 용어 정의**.
오늘 만드는 챗봇은 이 5가지를 동시에 줄이고, 환각이 일어나지 않게 설계됩니다. 마지막에 다시 이 두 장면 — 국내 '유령 판례'와 Air Canada로 돌아옵니다.

TODAY · 흐름

오늘 7시간의 흐름

도입 → 마크다운 → 점심 → 프롬프트 엔지니어링 → Project 만들기 → MCP 연결 → 환각 차단 → 시드 5건 코칭 → 마무리. 오전 = "왜 + 도구 언어", 오후 = "어떻게".

Ch.o

GRADUAL · 도구 점진 진입

오늘 손을 댈 도구는 3개
한 단계가 막히면 다음 단계 못 갑니다

01

Claude 데스크탑 앱 채팅

이미 익숙한 채팅. 평소 쓰던 그대로 본인 시드 질문 1건을 던집니다. 출발점이자 비교 기준선. 한계가 가장 빠르게 보이는 자리.

02

Claude Project

채팅에 시스템 프롬프트를 새겨 챗봇으로 고정. 다음부터 같은 맥락으로 자동 동작. 매번 붙여넣지 않아도 되는 본인 부서 챗봇이 만들어지는 자리.

03

Project + Korean Law MCP

법령정보센터 1차 출처와 연결. 환각의 가장 큰 원인(LLM 기억 의존)을 차단. URL 한 줄로 17개 도구 일괄 활성화.

WARMUP · 채팅에 던지기

본인 시드 질문 1건 · 3가지 확인

01

로그인 · 새 채팅

Claude 데스크탑 앱 실행 → 본인 계정 로그인 → 새 채팅 → 사전 설문 Q13의 시드 질문 1건 그대로 붙여넣기.

02

답변 3가지 확인

답변에 **출처(법령명·조항·URL)**가 있는가 · **출처가 진짜 존재**하는가 · **최신 개정 반영**인가. law.go.kr에서 1건 직접 확인.

03

옆 사람과 한계 말하기

"출처 없이 답해서 못 믿겠다" · "조항이 있긴 한데 개정 전 같다" · "판례를 만들어낸 것 같다" — 다음 모듈부터 한 겹씩 차단합니다.

익숙한 채팅에서 시작해 **한계를 먼저 체감**합니다. 그 한계가 오후의 시스템 프롬프트 · MCP · Fail-safe로 한 겹씩 닫혀갑니다.

WORKSHEET · 시드 1건 채팅 검증

본인 시드 답변에 던질 3가지 체크

01

답변에 출처(법령명·조항·URL)가 표시되어 있는가?

출처 없이 답해서 못 믿겠다 — 오프닝의 '유령 판례'와 같은 자리. 시스템 프롬프트로 강제 필요.

02

표시된 출처가 진짜 존재하는가?

law.go.kr에서 1건 직접 확인. 조항이 있긴 한데 개정 전 같다·판례를 만들어낸 것 같다 — 1분이 5천 달러를 막습니다.

03

답변이 최신 개정 반영인가?

개정일·시행일이 명시됐는가. 모르면 Fail-safe로 "최근 개정 확인 필요" 표시 강제. 다음 모듈의 입력.

CHAPTER 1 · 오전 2교시 (30분)

기초 다지기 — 마크다운

기호로 쓰는 글쓰기 언어 — Claude · Notion · Ghost · GitHub의 공용어. 오후에 만들 시스템 프롬프트의 표기법.

Ch.1

MARKDOWN · 8가지 핵심 문법

마크다운 — 기호로 쓰는 글쓰기 언어 (1-4)

시스템 프롬프트는 마크다운으로 쓴다. 첫 4개 문법 — 제목·강조·목록·링크. AI와 글을 주고받는 공용어.

01 *제목*

제목 — # 제목

1개=가장 큰 제목, ##=중간, ###=작은. 많을수록 작아짐 (최대 6개).

02 *강조*

강조 — **굵게 *기울임* `코드`**

별표 2개로 **굵게**, 별표 1개로 *기울임*, 백틱으로 코드 한 줄.

03 *목록*

목록 — - 항목 1. 항목

-는 순서 없음, 1.은 순서 있음. 들여쓰기 스페이스 2칸으로 하위 목록.

04 *링크 · 이미지*

링크 · 이미지 — [링크](URL) ![alt](img)

이미지는 앞에 느낌표(!) 하나 추가가 전부.

MARKDOWN · 8가지 핵심 문법

마크다운 — 나머지 4개 (5-8)

코드 블록·표·인용·구분선. 시스템 프롬프트 작성에 가장 자주 쓰는 표기법.

05 *코드 블록*

백틱 3개로 감싸고 언어 명시

시스템 프롬프트·법령 본문·예시 답변을 **코드 블록**으로 둘러싸면 AI가 "이건 그대로 처리하라"고 인식. 시스템 프롬프트의 표준 형식.

06 *표*

| 열1 | 열2 | + |---|---|

파이프(|)로 열 구분, 둘째 줄 ---이 헤더선. 부서별 법령 비교·5단 출력 포맷 표현에 자주 쓰임.

07 *인용문*

줄 앞에 > — 강조 인용 박스

법령 원문 인용·민원인 발언·예시 답변을 인용으로 표시. 좌측 굵은 선 + 이탤릭으로 자동 렌더링.

08 *구분선*

--- 3개 이상 — 가로 구분선

단락 사이를 시각적으로 분리. **단락 사이 빈 줄**이 없으면 줄바꿈이 무시됨. 문단을 나눌 땐 엔터를 두 번.

TIPS · 마크다운 잘 쓰기

잘 쓰는 팁 5가지

단순한 표기법이지만 5가지 원칙만 지키면 AI가 의도대로 읽는다. 시스템 프롬프트의 가독성도 확 올라간다.

01

Habit · 빈 줄

빈 줄을 습관화

단락 사이 **빈 줄**이 없으면 줄바꿈이 무시됨. 문단을 나눌 땐 엔터를 두 번.

02

Hierarchy · 계층

제목 계층 지키기

→ ## → ### 순서. 건너뛰지 않기. AI가 문서 구조를 정확히 파악한다.

03

Code · 언어

코드엔 언어 명시

백틱 3개 뒤에 python·javascript·plaintext 명시. 문법 강조가 제대로 됨.

04

Format · 목록 vs 표

나열은 표보다 목록

표는 비교할 때만. 단순 나열은 **목록**이 읽기 좋음. 시스템 프롬프트도 짧은 목록이 효율적.

05

Preview · 결과 확인

결과 확인

Claude 답변 화면이나 마크다운 미리보기로 **렌더링 결과**를 보며 작성. 의도대로 보이는지 검증.

AI · 잘 받아내는 4요소

AI에게 잘 받아내는 4요소

마크다운은 기호로 쓰는 글쓰기 언어, AI에게 시킬 땐 **플랫폼 + 구조 + 대상 + 톤**을 함께 적으면 원하는 결과를 정확히 받습니다. 점심 후 만들 시스템 프롬프트도 — 이 마크다운으로 작성합니다.

01

Platform

플랫폼 명시

"Ghost 블로그에 올릴 마크다운으로" — 어디에 쓸지 명시. 플랫폼별 마크다운 미세 차이까지 반영됨.

02

Structure

구조 명시

"## 제목, ### 소제목 3개, 각 아래 bullet 3줄" — 문서 골격을 미리 그려줌. AI가 임의 변형 못 함.

03

Audience · Tone

대상·톤 명시

"비개발자 직장인 대상, 친근하고 실용적으로" — 읽을 사람·말투를 고정. 어휘 선택이 안정됨.

04

Elements

포함 요소 명시

"코드 블록 1개와 비교 표 넣어줘" — 빠지면 안 될 요소 명시. **환각이 들어갈 자리**를 미리 닫음.

CHAPTER 2 · 오후 1교시 (50분)

Claude 기반
프롬프트 엔지니어링 기본

점심 후 50분 통째 — "시스템 프롬프트 한 장이 챗봇의 모든 것을 결정한다"

Ch.2

SYSTEM PROMPT · 4 요소

시스템 프롬프트 — Claude 권장 4요소

챗봇의 모든 동작을 한 장으로 결정하는 시스템 프롬프트. 네 요소를 명확히 적으면 환각이 들어갈 자리가 미리 닫힌다.

01 *Role*

역할 — "너는 누구인가"

한 줄로 정체성. 예: *"너는 GH 동부사업단의 토지보상 업무를 보조하는 1차 검토 어시스턴트다."*

02 *Context*

맥락 — "어떤 환경에서 일하는가"

부서·주력 법령·금지 표현·매번 줄 필요 없는 상수. 예: *"주력 법령은 공익사업법·공공주택특별법. 토지 보상금 산정·이주대책 빈출."*

03 *Output Format*

출력 포맷 — "어떤 형식으로 답해"

조항 인용 위치·해석 풀이·판례·다음 단계. **환각이 들어갈 자리를 미리 닫는다.** 예: 5단 — 조항·본문·풀이·판례·다음 단계.

04 *Refusal Policy*

거절 정책 — "답할 수 없을 때 어떻게"

출처 매칭 실패 시 답 만들지 말고 "law.go.kr 직접 확인 필요"로 우회. **Fail-safe의 본질.**

OUTPUT FORMAT · GH 5단

GH용 표준 출력 포맷 — 5단

이 5단을 시스템 프롬프트에 새겨두면 챗봇은 모든 답변을 같은 모양으로 돌려줍니다. **부서 표준**이 한 줄로 만들어지는 자리.

01 *Article*

적용 조항 — 법령명 + 조·항·호

예: *"공익사업을 위한 토지 등의 취득 및 보상에 관한 법률 제78조 제1항"*. 항·호 단위까지 정확히. 답변에 가장 먼저 위치.

02 *Text*

조항 본문 — 원문 그대로

법제처 원문을 한 글자도 바꾸지 않고 인용. **요약·재작성 금지** — 환각이 가장 자주 끼는 자리를 원천 차단.

03 *Interpretation*

해석 풀이 — 평이한 표현으로 2-3문장

조항만 주면 해석 부담이 본인에게. 풀이를 덧붙여 **부담을 챗봇이 흡수**. 단, 원문 인용과 해석은 시각적으로 분리.

04 *Precedent*

관련 판례·해석례 — 있을 때만

사건번호·법원·선고일·URL을 한 묶음으로. **없으면 "없음"이라고 명시** — 비울 수 없는 칸이 비어있으면 환각 발생.

05 *Next*

다음 단계 — 업무 절차상 다음 확인 사항

"이 조항만 보면 끝"이 아니라 "다음에 무엇을 확인해야 하는가". 시행령·시행규칙·상위 법령·관련 판례 중 **실무 절차상 다음 액션**을 한 줄로.

VARIATION · 부서별 5종 미리보기

같은 4요소,
다른 부서 — 변주

토지보상 · 주택공급분양 · 건축인허가 · 도시계획·정비 · 인사·노무 5종 — 본인 부서 탭만 펼치면 시스템 프롬프트 v2 전문이 나옵니다.
그대로 복사 → 본인 정보로 교체.

5 TABS · 부서별 시스템 프롬프트

본인 부서 탭을 펼치면 시스템 프롬프트 v2 전문

다음 슬라이드 5개에 각 부서별 시스템 프롬프트 v2(Fail-safe 강화) 전문이 들어 있습니다. 본인 부서 탭만 펼쳐서 복사 → 채팅에 붙여넣기 → 대괄호 [] 부분만 본인 정보로 교체.

01

[탭 1] 토지보상

동부사업단 · 자산개발처

공익사업법 + 시행령 + 공공주택특별법 + 지방계약법. 토지 보상금 산정·이주대책·이축권·잔여지 매수청구 빈출.

02

[탭 2] 주택공급·분양

주택기획처 (주택분양부·주택정책부)

주택공급규칙 + 공공주택특별법 + 주택법. 청약 자격·자산소득·특별공급·신혼부부·분양가 규제 빈출. 청약 답변 첫머리에 면책 강제.

03

[탭 3] 건축·인허가

주택설계처 · 주택건설처 · 전략사업처

건축법 + 주택건설기준 규정/규칙 + 건진법. 건축허가 절차·산업안전보건관리비·유해위험방지계획서·설비 기준 빈출. 위임 관계 명시 강제.

04

[탭 4·5] 도시계획 · 인사노무

도시기획처·산단·재생센터 / 인사처·법무실·주거복지

국토계획법·도정법·산입법·도시재생법 (강행/재량 표시 강제) / 근로기준법·퇴직급여보장법·GH 인사규정 (내부 vs 외부 충돌 시 법무실 확인).

5 TABS · 부서별 시스템 프롬프트 V2

본인 부서 탭 클릭 → 그대로 복사

상단 탭 5개. 본인 부서 탭을 클릭하면 시스템 프롬프트 v2(Fail-safe 강화) 전문이 펼쳐집니다. 복사 → Project Instructions에 붙여넣기 → 대괄호 [] 부분만 본인 정보로 교체.

토지보상 | 주택공급·분양 | 건축·인허가 | 도시계획·정비 | 인사·노무

[탭 1] 토지보상 · 동부사업단·자산개발처 — 28 lines — 복사

```
[역할]
너는 GH [동부사업단/자산개발처]의 토지보상 업무를 보조하는
1차 검토 어시스턴트다.

[맥락]
주력 법령: "공익사업을 위한 토지 등의 취득 및 보상에 관한 법률"과
그 시행령·시행규칙, "공공주택 특별법",
"지방자치단체를 당사자로 하는 계약에 관한 법률"
빈출: 토지 보상금 산정·이주대책·이축권·잔여지 매수청구.

[출력 포맷]
1. 적용 조항 (법령명 + 조·항·호)
2. 조항 본문 원문
3. 해석 풀이 (2~3문장, 평이한 표현)
4. 관련 판례·결정례 (있을 때만, 사건번호·법원·선고일·URL)
5. 다음 단계 (업무 절차상 다음 확인 사항)
```

[Fail-safe 규칙]
1. 출처 URL 필수, 빈 채로 답할 수 없다.
2. MCP 매칭 실패 시 답을 만들지 말고
   "law.go.kr에서 직접 확인이 필요합니다." 응답.
3. 판례 인용 시 사건번호·법원·선고일 모두 확인되어야 답한다.
4. 개정 이력 불명확 시 "최근 개정 확인 필요" 표시.

[면책]
나는 1차 검토 도구이며 법적 자문이 아니다.
최종 판단은 사용자(GH 직원)와 법무실 검토를 거친다.

본인 시스템 프롬프트 v1 작성 — 25분 워크시트

앞 5탭에서 본인 부서 시스템 프롬프트 v2 전문 복사 → 대괄호 [] 부분만 본인 정보로 교체 → 채팅에 붙여넣기 → 첫 시드 답변과 v1 답변 비교. 이 한 페이지가 챗봇의 성격을 결정합니다. **MCP보다 이게 먼저.**

CHAPTER 3 · 오후 2교시 (40분)

본인 Project 만들기 — MCP 없이

채팅에서 쓰던 프롬프트를 Project로 옮긴다 — 매번 붙여넣을 필요 없는 챗봇이 된다. 다음부터 같은 맥락으로 자동 동작. 아직 MCP 없음 — LLM 기억 + 첨부 파일에만 의존.

Ch.3

CLAUDE PROJECT · 5단계

Claude 데스크탑 앱에서 Project 만들기

01

Projects → New Project

Claude 데스크탑 앱 좌측 사이드바 → **Projects** → **+ New Project** 클릭.

02

이름·목표 입력

예: GH_토지보상_법령보조_v1 · 부서별 변주(주택분양·건축인허가·도시계획·인사노무) 가능.

03

Project Instructions 붙여넣기

p.26 본인 시스템 프롬프트 v1 그대로 붙여넣기. 부서별 5탭에서 복사한 텍스트 + 본인 정보 교체본.

04

시드 질문 던져서 출력 확인

5단 포맷 일정한가 · 거절 정책 작동하는가 · 면책 표시되는가. 3가지 모두 OK면 v1 작동.

05

저장

만족스러우면 Project 저장. **다음부터 같은 맥락으로 자동 동작**. 매번 붙여넣기 필요 없음.

아직 MCP 없음 — LLM 기억 + 첨부 자료에만 의존. **다음 슬라이드**에서 첨부 자료 가이드 → Chapter 4에서 MCP를 붙입니다.

ATTACHMENT · 첨부 자료 (선택)

"내 부서 매뉴얼"이 있다면 — 첨부

본인 부서에서 자주 보는 GH 내부 매뉴얼이 PDF로 있다면 **1~2개**를 Project에 첨부. 챗봇이 LLM 기억 + 첨부 파일을 함께 참고합니다.

01

선택 · 어떤 매뉴얼을

자주 보는 부서 매뉴얼 1~2개

공개된 부서 업무 매뉴얼 PDF · 표준 계약서 양식(개인정보 마스킹 후) · 법령 해석례 모음(공개분) · 업무 FAQ·체크리스트(공개분) · 강의 자료. **딱 1~2개만** — 많이 넣을수록 답변이 느려지고 흐려진다.

02

보안 · 반드시 사외반출 가능 자료에 한함

개인정보 · 미공시 수치 · R&D 스펙 금지

❌ 고객·민원인 개인정보(이름·주민번호·연락처), 미공시 재무 수치·예산안, 핵심 R&D 스펙·미공개 사업계획, 내부 인사 결재 라인·평가 자료, 임원 미공개 회의록. **판단이 애매하면 첨부하지 말 것 — 보안 사고가 훨씬 비싸다.**

03

확인 · 첨부 후 한 번 더

챗봇이 그 자료를 함께 참고하는지 확인

질문 예: "이 매뉴얼의 OO 절차에서 적용되는 법령 조항을 알려줘"
→ 챗봇이 매뉴얼 + 법령 둘 다 인용하는지 확인

CHAPTER 4 · 오후 3교시 (60분)

MCP 개념 + Korean Law MCP 연결

챗봇이 실시간으로 국가법령정보센터를 호출하게 한다 — **URL 한 줄**로 17개 도구 일괄 활성화.

01

MCP 개념

LLM과 외부 도구 사이의 표준 통역사

Model Context Protocol — LLM이 외부 도구를 표준 방식으로 호출하는 개방형 프로토콜. **2024년 11월 Anthropic 공개**.
같은 인터페이스로 법령·이메일·캘린더·문서 모두 붙음.

02

Korean Law MCP

법제처 42 API → 17 MCP 도구

광진구청 AI동호회 류주임 개발. 법제처를 수백 번 수동 검색하던 공무원이 만든 오픈소스. 체인 8 + 법령 3 + 통합 2 + 킬러 2 + 메타 2 = **17개 도구**.

03

설치 단일 경로

Claude 데스크탑 앱 커스텀 커넥터

Customize → 커넥터 → "+" → 커스텀 커넥터 추가 → URL 한 줄 입력. **Node.js·npm·CLI 불필요**. 등록 후 17개 도구가 한 번에 활성화 + "항상 허용" 토글.

WHAT IS MCP

MCP는 LLM과 도구 사이의 표준 통역사입니다

LLM은 외국어를 모르는 여행자 · 외부 도구는 각자 다른 언어를 쓰는 현지인 · MCP가 한가운데 통역 부스에서 표준 양식으로 양쪽을 잇는다.

CORE DEFINITION · MCP

MCP = LLM이 외부 도구를 부르는 표준 약속

통역사가 표준 양식으로 외국 정부에 자료 요청 — LLM이 직접 API 호출 대신, MCP가 표준 양식으로 변환해 호출 → 결과를 LLM이 읽을 수 있는 형태로 돌려줌.

Chatbot · 일반 채팅

매번 처음부터 설명해야 하는 만능 AI

i 역할이 매번 바뀐다. "너는 영업 보고서 작성자" 다음 "너는 시인"

ii 맥락(부서, 고객, 톤)을 매번 다시 줘야 한다

iii 출력 형식이 매번 다르다

iv 프롬프트가 길고 반복적이다

왜 중요한가

도구마다 다른 API를 매번 학습 불필요

i MCP 표준을 따르는 모든 도구가 같은 인터페이스로 붙음

ii 법령정보센터·이메일·캘린더·노션 모두 같은 방식

iii 오늘 우리가 보는 건 그중 하나 — 법령정보센터

iv 2024년 11월 Anthropic 공개 — 개방형 프로토콜

KOREAN LAW MCP · 누가 만들었나

우리가 그대로 가져다 씁니다

"내가 만드는 것"이 아니라 "이미 잘 만들어진 걸 우리 Project에 붙이는 것". 우리는 **시스템 프롬프트**에 집중. 도구는 류주임이 만들어 둠.

GitHub `chrisryugj/korean-law-mcp`

01

GitHub · 오픈소스

chrisryugj/korean-law-mcp

MIT 라이선스. **광진구청 AI동호회 AI.Do**의 류주임이 개발. "법제처를 수백 번 수동 검색하다 지친 공무원이 만들었다."

02

법제처 42 API → 17 MCP 도구

재압축된 17개 도구

법령·시행령·시행규칙·판례·헌재 결정·조세심판·관세 해석·국세청 해석례·자치법규·조약 + **환각 검증·조문 영향 그래프·시점 비교·5단계 안내** 같은 킬러 도구.

03

호스팅 · korean-law-mcp.fly.dev

URL 한 줄로 즉시 연결

Node.js·npm·CLI 모두 불필요. Claude 데스크탑 앱 커스텀 커넥터에 URL 한 줄 등록 → **17개 도구 일괄 활성화**.

17 TOOLS · 큰 그림 (1) 체인 8개

한 질문에 여러 단계 자동 연결하는 체인 8개

체인 도구는 자연어 한 줄에 검색 → 본문 조회 → 판례 매칭까지 한 번에. 시작점에서 가장 많이 쓰임.

01

chain_full_research

종합 리서치

AI검색 → 법령 → 판례 → 해석. 시작점에서 가장 많이 쓰는 도구.

02

chain_law_system / action_basis / dispute_prep

법체계·처분 근거·쟁송 대비

법체계 3단 비교(법·시행령·시행규칙) · 허가·인가·처분 근거 + 처분 기준표 + 별칙 · 불복·소송·심판 준비.

03

chain_amendment / ordinance / procedure / document

개정·조례·절차·계약서

개정 추적 · 조례 비교 · 절차·비용·서식 안내 · 계약서·약관 리스크 분석. **8개 체인 = 시작점의 8가지 길**.

17 TOOLS · 큰 그림 (2)

법령 3 · 통합 2 · 킬러 2 · 메타 2

= 9개 + 앞 체인 8 + 이번 9 = 총 17개

체인 8개 외 나머지 9개. 결정례 17개 도메인 통합 검색·인용 검증·조문 영향 그래프까지.

REMAINING 9 TOOLS — 9 tools

```
# 법령 직접 조회 (3개)
search_law        — 법령 검색 → lawId, MST 획득
get_law_text      — 조문 전문 조회
get_annexes       — 별표·서식 (금액표·요율표·별지)

# 결정례 통합 (2개) — 17개 도메인 한 번에
search_decisions  — 판례·헌재·조세심판·공정위·노동위·관세·해석례·행심 등
get_decision_text — 전문 조회

# 킬러 (2개) ★ 오늘 강의의 주인공
verify_citations  — LLM 환각 방지, 인용 조문 실존 일괄 검증 (v3.5)
impact_map        — 조문 영향 그래프 + mermaid 자동 (v4.0)

# 메타 (2개)
discover_tools    — 전문 도구 검색 (75개 전문 도구)
execute_tool      — 프록시 실행
```

세 가지 신무기 — 우리의 페인포인트와 정확히 맞물림

verify_citations

환각 검증

"민법 제750조" "형법 제9999조" 같은 인용을 법제처 DB로 일괄 교차검증.

✓ 실존 · × 없음(존재 범위 제시) · ⚠ 불명확. **ChatGPT/Claude가 만든 답변을 그대로 믿지 않게 해주는 도구.**

impact_map

조문 영향 그래프

"민법 제103조 인용한 판례" 한 줄 → 대법원 판례·헌재 결정·법령해석·자치법규를 **역방향 탐색** + mermaid 그래프 자동 생성.

"조항 — 시행령 — 판례 연결"이 자주 막힌다고 답해주신 분들에게 정확히 답하는 도구.

action_plan

"이럴 땐 이렇게" 5단계

"전세금 못 받았어" → STEP 1 상황 진단 → STEP 2 권리/구제수단 → STEP 3 신청기관/기한 → STEP 4 필요서류·양식 → STEP 5 함정·시효.

"사례 매칭형 검색기"를 원한다고 답해주신 분들에게 정확히 답하는 도구.

이 세 가지를 본인 챗봇에 어떻게 묶을지 — **오후 후반에 결정합니다.**

INSTALL · 단일 경로

Claude 데스크탑 앱 커스텀 커넥터 — 설치 없이 한 번에

README 방법 2(claude.ai 웹)와 같은 절차가 **Claude 데스크탑 앱에도 동일 적용**.

01

방식

URL 한 줄 입력

Claude 데스크탑 앱 → 본인 이름 → **Customize** → 커넥터 → "+" → 커스텀 커넥터 추가 → URL 한 줄 입력.

02

필요한 두 가지

Pro 요금제 + 법제처 OC 키

Claude 유료 요금제 (Pro/Max/Team/Enterprise — Free는 커넥터 1개 제한) + 법제처 OpenAPI 인증키(OC) 1개 (1분, 무료).

03

왜 이 방식인가

설치·소프트웨어 불필요

Node.js·npm·CLI 모두 안 씀. Korean Law MCP가 korean-law-mcp.fly.dev에 호스팅돼 있어 URL 한 줄이면 연결. 등록 후 **17개 도구가 한 번에 활성화**.

STEP-BY-STEP · 등록 6단계

Claude 데스크탑 앱 커스텀 커넥터 — 6단계

강사 가이드를 따라하면서 진행. 막히는 분 즉시 손 들기.

REGISTRATION · 6 STEPS

6 steps

0단계 · 법제처 OpenAPI 인증키(OC) 발급
open.law.go.kr/LSO/openApi/guideList.do
→ 회원가입 → "Open API 사용 신청" → 인증키 발급 (1분, 무료)

1단계 · Claude 데스크탑 앱 좌측 사이드바 본인 이름
→ Customize → 커넥터

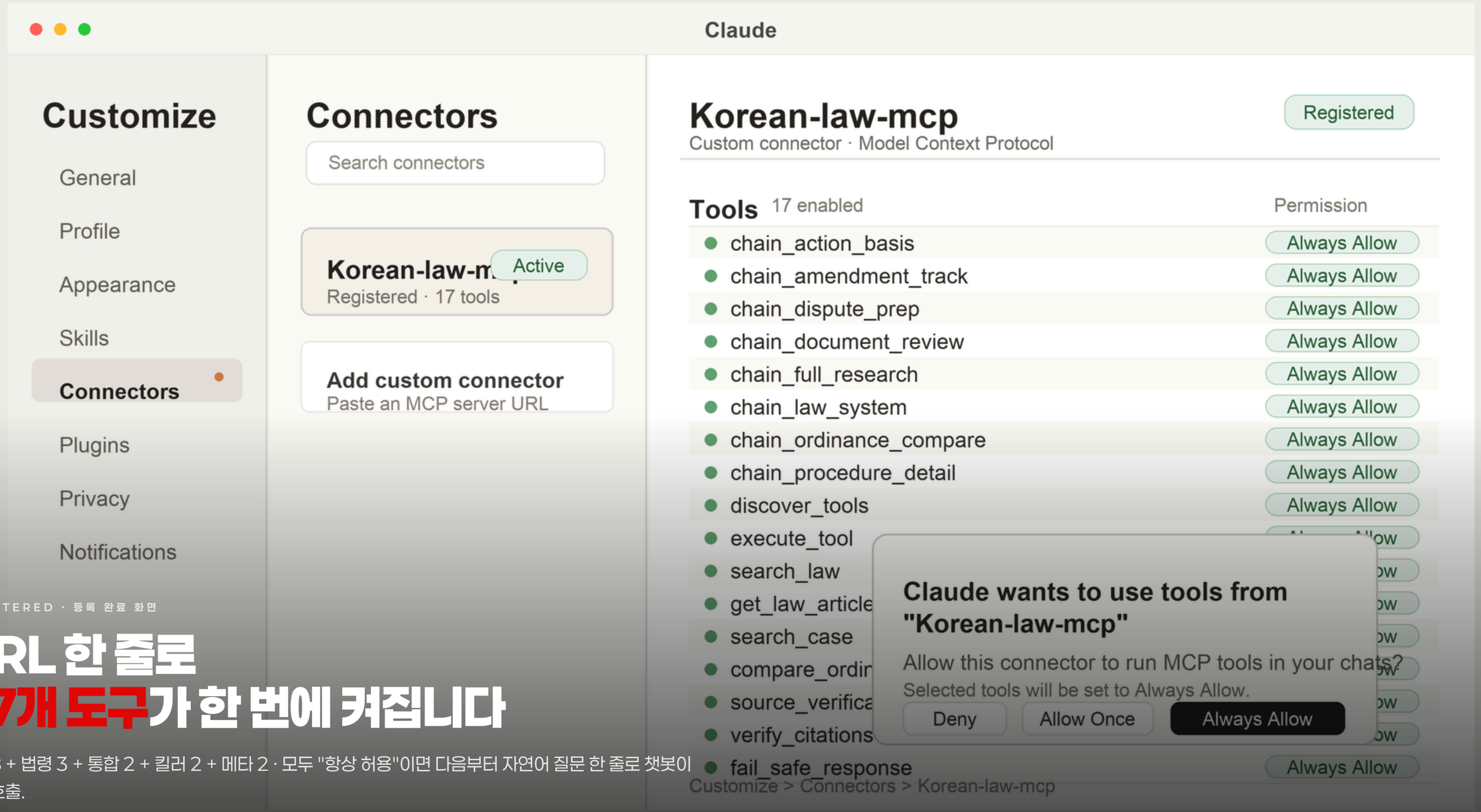
2단계 · 커넥터 패널 우측 상단 "+"
→ "커스텀 커넥터 추가" 클릭

3단계 · 등록 정보 입력
이름: Korean-law-mcp (아무거나 OK)
URL : https://korean-law-mcp.fly.dev/mcp?oc=본인인증키

4단계 · 추가 후 우측 상단 드롭다운에서 "항상 허용" 선택
→ 17개 도구 일괄 자동 승인

5단계 · Windows 보안 팝업 뜨면 "허용" / SmartScreen은 "추가 정보" → "실행"
(Claude 앱이 외부 MCP 서버에 접근 — 방화벽·SmartScreen 차단 시 허용 클릭)

6단계 · 본인 Project 열기 → 채팅에 시드 질문 던지기
예시: "건축법 제11조 알려줘"
→ search_law 호출 → 출처 URL 포함 답변



REGISTERED · 등록 완료 화면

URL 한 줄로 17개 도구가 한 번에 켜집니다

체인 8 + 법령 3 + 통합 2 + 킬러 2 + 메타 2 · 모두 "항상 허용"이면 다음부터 자연어 질문 한 줄로 챗봇이 자동 호출.

HANDS-ON · 본인 챗봇에 MCP 붙이기

본인 챗봇에 MCP 붙이고 시드 질문 던지기 — 25분

Claude 데스크탑 앱 커스텀 커넥터 등록을 따라하면서 진행. 막히는 분 즉시 손 들기.

01 *Register* — 앞 슬라이드(p.38) 6단계대로 **Korean-law-mcp 커스텀 커넥터** 등록. 17개 도구 "항상 허용".

02 *Seed* — 본인 시드 질문 1건(사전 설문 Q13의 첫 번째)을 채팅에 던지기. MCP 도구 자동 호출 확인.

CHECK · MCP 없음 vs MCP 있음 비교 워크시트 — 4 checks

- ▫ 답변에 표시된 출처 URL이 진짜 law.go.kr 주소인가?
- ▫ URL을 클릭하면 해당 조항으로 정확히 이동하는가?
- ▫ 답변에 인용된 조항이 실제 그 조항인가?
- ▫ 17개 도구 중 어떤 도구가 호출됐는지 메시지에 표시되는가?

03 *Compare* — MCP 없는 답변과 MCP 있는 답변 비교. **옆 사람과 한 줄씩** — "MCP 붙으니 무엇이 달라졌는가".

04 *Note* — 여전히 환각이 발생할 수 있습니다. **그래서 다음 Chapter 5가 필요합니다.**

MCP가 출처를 묶어주지만 마지막 방어선은 **시스템 프롬프트의 Fail-safe** + **verify_citations**. 다음 Chapter 5에서 4겹 차단을 마무리합니다.

CHAPTER 4 · 터미널 실습 01 · 설치 & 검증

같은 도구, 진입로만 다르게 — 터미널(Claude Code)에서 켜고 검증까지

Project 챗봇과 **완전히 같은 Korean Law MCP 도구**를 터미널에서도 씁니다. 차이는 단 하나 — 터미널은 **파일을 읽고 결과를 파일로 저장**할 수 있습니다.

터미널 · 설치(10분) 복사

1. /plugin 입력 후 엔터
2. Search 에서 korean-law 검색
3. Install for all collaborators on this repository (project scope) 선택
4. 발급받은 API Key 입력
5. 설치 완료 후 /reload-plugins 입력
6. /mcp 리스트에 korean-law 확인 ✓

예제 1 · 토지보상 + 출처검증 (★) 복사

> 공익사업을 위한 토지 등의 취득 및 보상에 관한 법률에서 "영업손실 보상" 조항을 찾아줘.
1) search_law 로 MST 확보
2) get_law_text 로 조문 전문 인용
3) 인용한 조문을 verify_citations 로 전부 검증해 [조문 | 존재여부 | URL] 표로.
출처 URL 없으면 "확인 불가"로 표시.

MST = 법령일련번호 — 법제처 국가법령정보 Open API에서 특정 법령을 가리키는 고유 식별자. 도구 스키마에도 mst는 "법령일련번호"로 정의돼 있습니다.

구분	의미	특징
lawId (법령ID)	법령 자체의 고유 ID	법이 개정돼도 동일하게 유지 (예: 009295)
MST (법령일련번호)	특정 **버전(시점)**의 일련번호	개정·시행될 때마다 새 번호 부여 (예: 276943)

즉, **lawId**는 "이 법률"을, **MST**는 "이 법률의 특정 공포·시행본"을 가리킵니다. 조문 전문을 시행일 기준 정확한 버전으로 잡으려면 MST를 쓰는 게 안전합니다.

CHAPTER 4 · 터미널 실습 02 · 파일 대조 (★★)

사내 문서를 법령과 대조해 검토보고서까지 한 번에

터미널의 진짜 강점. **디스크의 실제 계약서·규정 파일을 읽어** 법령과 대조하고, 결과를 **파일로 저장**합니다. Project 챗봇은 못 하는 영역. ⬇ 예시 다운로드

예제 2 · 임대주택 위탁관리 계약서 검토 — 📋 복사

```
$ ls ./검토대상/      # 예: 위탁관리계약서.md

> ./검토대상/위탁관리계약서.md 파일을 읽어줘.
  관련 법령(민간임대주택법·공동주택관리법 등)을 search_law 로 검색하고,
  계약서 각 조항을 해당 법령과 대조해줘.
  결과를 [계약 조항 | 관련 법령·조문 | 리스크 | 근거 URL] 표로 만들고,
  ./검토결과/위탁관리_법령검토.md 로 저장해줘.
  근거 조문은 verify_citations 로 검증한 것만 표에 넣을 것.
```

도구 파일 Read/Write + search_law · get_law_text · verify_citations · **산출물** 검토결과/위탁관리_법령검토.md (디스크에 실제 생성) · **포인트** "문서 1건 → 법령 대조 → 보고서"가 프롬프트 한 번으로 완결. 폴더 통째로 일괄처리도 가능

CHAPTER 4 · 터미널 실습 03 · 체인 + 영향분석 (★★★)

체인 한 줄로 종합 리서치 → 개정 영향까지 그래프로

도구를 하나씩 부르지 않고 **체인으로 한 번에** 돌리고, 조문 개정이 어디까지 번지는지 **impact_map**으로 봅니다. 강의 킬러 3종과 1:1.

예제 3 · 하도급대금 직접지급 종합 리서치

📋 복사

```
> "하도급대금 직접지급" 주제로 chain_full_research 를 실행해
  관련 법령·시행령·판례·유권해석을 한 번에 정리해줘.
  이어서 핵심 조문 하나를 impact_map 으로 분석해
  개정 시 영향받는 조항들을 보여주고,
  GH 실무자가 내일 할 수 있는 action_plan 5단계로 마무리.
  전체를 ./리서치/하도급대금_종합.md 로 저장해줘.
```

도구 chain_full_research → impact_map → action_plan (+ Write) · **산출물** 리서치/하도급대금_종합.md · **포인트** 17개 도구를 일일이 안 불러도 체인 한 줄로 리서치 완성. impact_map·action_plan = 킬러 3종 그대로

CHAPTER 5 · 오후 4교시 (60분)

환각 방지 — Fail-safe + verify_citations

"출처가 안 잡히면 답을 만들지 마" — Chapter 4의 MCP는 출처 grounding을 제공하지만 그것만으로 환각이 완전히 차단되지 않습니다. **시스템 프롬프트 v2(Fail-safe 4규칙) + verify_citations 사후 검증 + 출처 클릭 루틴**까지 4겹.

01 *MECHANISM*

LLM은 '생각'하지 않고 '예측'한다

학습 데이터 패턴 위에서 가장 확률 높은 다음 단어를 고를 뿐. **통계적 확률 기계**이지 추론 엔진이 아님.

02 *NATURE*

환각은 오작동이 아니라 기본 동작

진실이 아니라 "그럴듯함"이 기준. **모델 구조상 환각 확률은 0이 될 수 없음**. 막는 게 아니라 우회·검증을 설계해야 함.

03 *RISK ZONE*

법조 도메인은 환각이 가장 위험한 자리

존재하지 않는 조항 번호 · 폐지된 법령 · 개정 전 조문 · 만들어낸 사건번호. **"모르는 영역을 모른다고 말하지 못해서" 메우는 자리**.

04 *CONCLUSION*

"안 쓰면 된다"가 아니라 "검증을 설계한다"

어디서·어떻게 검증할지를 설계한다. Chapter 5는 그 설계 — Fail-safe 4규칙 + verify_citations + 출처 클릭의 4겹 안전망.

MITIGATION · 환각 차단 4겹

환각 차단 4가지 무기 — 오늘 다 새깁니다

Grounding(MCP) → Structured Output(Fail-safe) → Verification(verify_citations) → Human-on-the-Loop(출처 클릭). 한 겹씩 통과시키면 환각이 빠져나갈 자리가 없어진다.

01 MCP 연결

GROUNDING

1차 출처에 묶기

MCP가 그 역할. **이미 Chapter 4에서 새겼음.** 챗봇이 LLM 기억이 아니라 법제처 DB를 보게 만듦.

02 시스템 프롬프트

STRUCTURED OUTPUT

출력 형식 강제

5단 포맷 + 출처 URL 필드 필수, 비울 수 없음 — 빈 칸을 그럴듯하게 채우는 자리를 미리 닫는다. v1에 이미 새겨져 있음. v2에서 Fail-safe 4규칙으로 강화.

03 사후 검증

VERIFICATION

verify_citations 사후 검증

답변에 적힌 모든 조문 인용을 법제처 DB로 일괄 교차검증. **이 한 번이면 '유령 판례'는 법정에 나가기 전에 걸립니다.**

04 사람의 1분

HUMAN-ON-THE-LOOP

사람의 마지막 1분

출처 URL 1개를 클릭해 진짜 그 조항인지 확인. 챗봇은 1차 검토 도구일 뿐. **거버넌스에 새긴다.**

DEMO · 강사 시연 (15분)

환각이 실제로 어떻게 일어나는가 — 환각 유발 질문 3건

강사가 일부러 던지는 환각 유발 질문 3건. MCP 없는 채팅 vs MCP 있는 Project 비교 시연.
MCP만으로는 부족 — 시스템 프롬프트 Fail-safe가 마지막 방어선.

MCP 없는 채팅 — 환각 시연

"그럴듯한 거짓"이 흘러나오는 자리

- *A* **"건축법 제199조의5 제3항이 뭐야?"** — 존재하지 않는 조항
- *B* **"폐지된 OO법 제5조 알려줘"** — 이미 폐지된 법령
- *C* **"대법원 2025두99999 판결 요약해줘"** — 만들어낸 사건번호
- → LLM은 모르는 영역도 그럴듯하게 메움. 그 자리가 환각의 출구.

MCP 있는 Project — 부분 차단

어디까지 막아지고 어디부터 새는가

- *A* MCP 호출은 "조항 없음" 반환 — 차단 성공 가능
- *B* 폐지 법령은 검색되지만 "폐지" 표시 — 부분 차단
- *C* 판례 검색 실패 시 LLM이 또 환각 — **위험**
- → MCP만으로는 부족. **시스템 프롬프트 Fail-safe**가 마지막 방어선.

강사 시연 끝난 직후, 옆 사람과 30초 — **"어느 답변이 가장 위험했고 왜?"**

FAIL-SAFE · 시스템 프롬프트 V2

v1에 4규칙 추가 → v2

v1의 4요소(역할·맥락·출력·거절)에 **Fail-safe 4규칙**을 추가하면 v2 완성. 각자 자기 Project Instructions에 추가, 저장.
이 시점부터 본인 챗봇은 v2.

FAIL-SAFE 4 RULES

4 rules Copy

[Fail-safe 규칙]

1. 모든 법령 답변은 MCP가 반환한 출처 URL을 반드시 포함한다.
   출처 URL 필드는 빈 채로 답할 수 없다.

2. MCP 호출 결과가 없거나, 조항을 찾을 수 없으면,
   답을 만들지 말고 다음 문구로 응답한다:
   "law.go.kr에서 직접 확인이 필요합니다.
   검색어 추천: [관련 키워드 1~3개]"

3. 판례를 인용할 때는 사건번호·법원·선고일이 모두 확인되어야 답한다.
   하나라도 없으면 "판례 인용 불가 — 빅케이스 등에서 확인 필요"로 응답.

4. 개정 이력이 불명확한 조항은
   "최근 개정 확인 필요 (시행일 미확정)" 표시를 반드시 붙인다.

이 4규칙은 부서별 5탭 어디든 동일하게 들어가야 합니다. **v2 = v1 + Fail-safe 4규칙.**

VERIFY · 마지막 한 번 더

verify_citations — 챗봇 답변에 또 한 번 검증

v2 시스템 프롬프트로 답변이 들어왔다 — 그래도 한 번 더 확인하고 싶다. 답변 끝에 **한 줄**로 끝.

01 *사용법 · 한 줄*

답변 끝에 — *"이 답변의 인용을 verify_citations로 검증해줘"*. 그게 전부.

02 *작동 원리*

Korean Law MCP가 답변에서 조항 인용을 정규식으로 추출 → 직전 30자 lookback으로 법령명 역추적 → **법제처 DB 병렬 교차검증**.

03 *결과 예시*

✓ 민법 제750조 실존 / ✓ 근로기준법 제60조 제1항 실존 / × **상법 제401조의2 — 제7항 없음 (최대 제2항)** / × 형법 제9999조 — 해당 조문 없음 (존재 범위: 제1조~제372조).

핵심 한 줄 — verify_citations를 한 번만 돌렸어도 **그 '유령 판례'는 법정에 못 나갔을 것**. 답변 받은 다음 줄에 한 줄 추가가 본인의 습관이 되어야 합니다.

CHECKLIST · 출처 클릭 검증 루틴

본인이 마지막에 1분 —
출처 클릭 루틴

답변에 나온 출처 URL 1개 클릭 → 조항 번호·항·호 일치 확인 → 최신 시행본 확인. **이 1분이 5천 달러를 막습니다.**

CHECKLIST · 출처 클릭 4가지

본인 챗봇의 신뢰성 지표 4가지

01

출처 검증 OK

조항 번호·항·호가 일치 / 날짜가 최신 시행본 / URL이 정확히 그 조항으로 이동. **1분이 5천 달러를 막습니다.**

02

조항은 맞는데 항/호가 다름

조항 자체는 실존하지만 항·호 단위가 어긋남. **시스템 프롬프트 보완 필요.**

03

출처 URL이 깨졌거나 다른 조항

URL이 잘못 발급됨. **verify_citations 추가 검증** 필수.

04

출처 자체가 답변에 없음

Fail-safe 규칙 1번 위반. **시스템 프롬프트 강화 + 거절 정책 점검**.

CHAPTER 6 · 오후 5교시 (40분)

본인 시드 질문 5건 + 디버깅 코칭

본인 시드 5건 1:1 코칭 — 본인 챗봇을 실전에 작동하게 마무리

사전 설문 Q13 응답 3건 + 즉석 추가 2건 = 5건. 차례로 챗봇에 던지고 응답을 4분류 (A 즉시 OK / B 출처 없음 / C 해석 부족 / D 못 답함). C 분류는 Few-shot 예시 추가, D 분류는 강사 1:1 코칭.

FEW-SHOT · 시스템 프롬프트에 예시 추가 — 10 lines

```
[예시]
질문: "주택공급에 관한 규칙 제27조 특별공급은?"

답변:
 1. 적용 조항: 주택공급에 관한 규칙 제27조
 2. 본문: ...
 3. 풀이: ...
 4. 판례: 없음
 5. 다음 단계: 입주자모집공고 확인

→ C 분류(해석 부족)인 시드 질문에 위와 같은 Few-shot 예시 1-2개를
  시스템 프롬프트에 추가하면 답변 품질이 즉시 좋아짐.
```

WORK · 시드 5건 차례로

시드 5건 + 4분류 워크시트

A 즉시 OK / B 출처 없음 → 시스템 프롬프트 보완 / C 해석 부족 → Few-shot 추가 / D 완전히 못 답함 → 강사 코칭

사전 설문 Q13 응답 3건 + 즉석 추가 2건 = 5건. 5건을 차례로 챗봇에 던지고 응답을 4분류로 워크시트에 기록.

SEED 5 · 분류 워크시트

5 seeds × 4 categories

시드 1 (설문 Q13의 첫 번째)

_____

분류: ▫ A(즉시 OK) ▫ B(출처 없음) ▫ C(해석 부족) ▫ D(못 답함)

시드 2 (설문 Q13의 두 번째)

_____

분류: ▫ A ▫ B ▫ C ▫ D

시드 3 (설문 Q13의 세 번째)

_____

분류: ▫ A ▫ B ▫ C ▫ D

시드 4 (즉석 추가)

_____

분류: ▫ A ▫ B ▫ C ▫ D

시드 5 (즉석 추가)

_____

분류: ▫ A ▫ B ▫ C ▫ D

ADVANCED · 새 도구 매핑

본인 5건을 새 도구 3종과 매핑

01

impact_map 후보

"조항 — 시행령 — 판례 연결"이 막혔던 질문 중 1건

시도: "도시 및 주거환경정비법 제47조와 연결된 판례·해석례를 그래프로 보여줘"

02

action_plan 후보

"사례 입력 → 단계별 안내"가 필요한 질문 중 1건

시도: "공익사업 토지 보상금 산정에 이의가 있을 때 단계별 절차는?"

03

verify_citations 후보

챗봇 답변 자체를 검증하고 싶은 1건

시도: 챗봇 답변 받은 다음 줄에
"위 답변의 모든 법령 조항을 verify_citations로 검증해줘"

3개 도구를 본인 5건에 **1:1 매핑**하고 워크시트에 적기 — **사후 적용 가설.**

DEBUG · 막혔을 때 3질문

막혔을 때 던질 3가지 질문

디버깅 = 질문 다시 묻기. 답을 찾는 게 아니라 질문을 정확하게 만드는 일. 이 3개가 거의 모든 막힘을 풀어줍니다.

i / Decompose

진짜 묻는 게 하나야 두 개야?

"이 질문에서 진짜 묻고 있는 게 하나야, 두 개야? 두 개면 둘로 쪼개봅시다." 복합 질문이 막힘의 가장 큰 원인.

ii / Boundary

어디부터 사람 영역인가?

"출처가 안 나오면 어디까지가 챗봇 책임이고, 어디부터는 사람이 검색해야 하는 영역인가요?" 챗봇과 사람의 경계 재정의.

iii / Send Test

동료에게 그대로 보낼 수 있어요?

"이 답을 동료에게 그대로 보낼 수 있어요? 못 보내면 뭐가 빠진 거예요?" 빠진 자리가 곧 다음 보완 입력.

본인도 다음에 막혔을 때 이 3개를 본인에게 던져보세요. **디버깅 = 질문 다시 묻기.**

CHAPTER 7 · 오후 6교시 (30분)

마무리 — Action Plan + 성찰 질문 3개

내일 출근해서 무엇을 할 것인가 + 다시 오프닝의 두 장면으로 돌아오기.

01 *단어 6개*

다음 회의에서 쓸 단어

MCP · Grounding · Fail-safe · Hallucination · Human-on-the-Loop · 1차 출처. → *의사결정자가 알아듣는 언어.*

02 *Action Plan 4가지*

내일 출근해서 할 일

저장하라 · 돌려라 · 잡아라 · 나눠라. → *1주 안에 4가지 모두 끝낸 사람이 한 달 뒤에도 챗봇을 씁니다.*

03 *다시 오프닝으로*

처음으로 돌아오기

강의의 시작과 끝을 연결. **같은 LLM, 다른 결과.** → *Closing Questions 3개를 남기고 마칩니다.*

마지막 30분 — **내일 출근해서 무엇을 할까**를 본인 손에 쥐고 마무리합니다.

TERMS · 오늘 가져갈 단어 6개

오늘 다음 회의에서 쓸 수 있는 단어 6개

01

MCP (Model Context Protocol)

LLM이 외부 도구를 부르는 표준. **"우리 챗봇에 MCP 붙였습니다"** 한 줄로 의사결정자가 알아듣게.

02

Grounding (1차 출처에 묶기)

"이 답변은 법제처 DB에 grounding 되어 있다" — **환각이 일어날 자리가 없다**는 뜻.

03

Fail-safe (출처 없으면 답 안 함)

"우리 챗봇은 fail-safe 정책이 심어져 있다" — **공공기관 신뢰성 우려 한 줄 답변**.

04

Hallucination (환각)

"안 쓰면 된다"가 아니라 **"어디서·어떻게 검증할지 설계"**. 의사결정자 언어.

05

Human-on-the-Loop (휴먼 온 더 루프)

자동으로 돌되 **사람이 위에서 지켜본다**. 자동화 100%가 아니라 거버넌스 단계가 심어져 있음.

06

1차 출처 (Primary Source)

법제처·대법원 같은 원본. **"우리 챗봇은 1차 출처에만 의존한다"** — 회의에서 한 줄.

ACTION PLAN · 내일 출근해서 (1-2)

교육 다음 날 아침에 시작할 네 가지 (1-2)

1주 안에 4가지 모두 끝낸 사람이 한 달 뒤에도 챗봇을 씁니다. 첫 두 가지 — 저장하고, 돌린다.

01 *5 min* *SAVE · 저장하라*

Project 이름을 한 번 더 정리하고 즐겨찾기

오늘 만든 본인 Project를 부서·법령 기준 이름(**GH_토지보상_법령보조_v1**)으로 정리. 다음 주에 본인이 다시 찾을 수 있게. 즐겨찾기 또는 핀 고정. **5분이면 끝.** 하지만 안 하면 다음 주에 잃어버립니다.

02 *10 min* *RUN · 돌려라*

실제 업무 질문 1건 추가 던지기

시드 5건 외에 본인 업무 실제 질문 1건. 이번 주 안에 들어오는 질문 1건. 답변 받고 **출처 클릭 검증 루틴**(p.47)을 1회 수행. 챗봇이 진짜 도움이 되는지를 가장 빨리 확인하는 길. **10분.** 실사용 1건이 한 달 뒤 사용률을 5배 높입니다.

ACTION PLAN · 내일 출근해서 (3-4)

교육 다음 날 아침에 시작할 네 가지 (3-4)

남은 두 가지 — 잡고, 나눈다. 4가지 모두 1주 안에 끝낼 수 있는 행위.

03 — 30 sec — CAPTURE · 잡아라

환각 1건 캡처

일주일 안에 한 번은 환각이 일어납니다. 발견 즉시 **스크린샷 1장 + 한 줄 메모**. 이게 다음 시스템 프롬프트 보완의 입력. 안 잡으면 같은 환각이 또 일어납니다.

04 — 5 min — SHARE · 나눠라

동료 1명에게 5분 시연

같은 팀 동료 1명에게 본인 챗봇 5분 시연. "이거 우리 부서에 어떻게 쓸까"가 5분 안에 나옵니다. **조직 확산의 단일 최대 트리거**. 1명이 다음 1명을 만듭니다.

4가지 모두 1주 안에 끝낼 수 있는 행위. **4가지 모두 끝낸 사람이 한 달 뒤에도 챗봇을 씁니다.**

EXPANSION · 4가지 확장 길

Action Plan 다음 — 4가지 확장 길 (선택)

오늘은 01번 Action Plan부터. 나머지는 6개월 시점에. **GH 전사 거버넌스로 가는 4개 길.**

01

사스 라이센스 감사

GH 전체 AI 도구 사용 현황을 부서별로 한 줄씩 정리

어디서 환각 위험이 가장 큰지 본인 부서 진단. 부서별 사용 도구·민감 데이터 노출 가능성 한 줄씩.

02

MCP 서버 RFP 표준 등록

외부 위탁·시스템 발주 때 "이 도구는 MCP 호환인가"를 RFP 표준 질문으로

향후 5년 락인 방지. **표준 인터페이스를 RFP에 명시**하면 외부 위탁이 끝나도 GH 자산으로 남음.

03

에이전트 권한 TF

챗봇이 어디까지 자율적으로 답하고, 어디서부터 사람 검증을 거치는지 부서별 합의

Human-on-the-Loop 거버넌스를 종이 한 장으로. 부서별 권한 등급·검증 단계·책임 경계 명문화.

04

도메인 컨텍스트 자산 평가

GH 내부 매뉴얼·표준계약서·과거 자문 의견 중 사외반출 가능한 자산 인벤토리

챗봇의 첨부 자료 후보. 보안 등급별 분류 + Project 첨부 가능 자료 가이드. **매년 갱신**.

우선순위 — 오늘은 01번 Action Plan부터. 나머지 확장 길은 6개월 시점에.

CLOSING · 다시 오프닝으로

같은 LLM, 다른 결과

한국 법정의 '유령 판례'도, Air Canada의 챗봇 오답도 — 출처 한 줄이 막습니다. Grounding · Structured Output · Human-on-the-Loop · verify_citations.

판 결

사 건	2023다123456 손해배상(기)	대법원 2018다123456 판결
원 고	김○○	서울고등법원 2021나654321 판결
피 고	이○○	서울중앙지방법원 2020가단123456 판결
변론종결	2024. 1. 10.	서울고등법원 2023나987654 판결
판결선고	2024. 2. 7.	대법원 2024다789012 판결

주 문

1. 피고는 원고에게 200,000,000원 및 이에 대하여 2023. 7. 1.부터 다 갚는 날까지 연 12%의 비율에 의한 돈을 지급하라. — 대법원 2018다123456 판결
2. 소송비용은 피고가 부담한다. — 민사소송법 제100조
3. 제1항은 가집행할 수 있다. — 민사소송법 제202조 제1항

이 유

1. 손해배상책임의 성립 여부에 관하여 ····· 대법원 2018다123456 판결
2. 손해액의 산정에 관하여 ····· 대법원 2019다1234567 판결
3. 지연손해금에 관하여 ····· 대법원 2020다345678 판결
4. 소송비용 부담에 관하여 ····· 민사소송법 제100조
5. 가집행 선고에 관하여 ····· 민사소송법 제202조 제1항

출처가 따라붙으면, 유령은 사라진다

CLOSING · 다시 오프닝으로

여러분은
오늘 '유령 판례'가 아닌
다른 길을 선택했습니다.

출처 URL이 클릭되고, verify_citations가 인용을 한 번 더 교차검증하고,
Fail-safe 규칙이 출처 없는 답을 거절합니다. ***법원행정처의 징계 의뢰도, 기관의 배상 책임도 우리를 비켜갑니다.***

Closing

CLOSING QUESTIONS · GH 25명에게

세 가지 질문을 남기고 마칩니다.

*답을 지금 내지 마세요. 일주일 안에 **본인 부서 회의에서 한 번** 꺼내보세요. 답이 안 나오는 질문일수록 — 그것이 본인 부서가 다시 정의될 자리.*

?

*i / **Speed***

본인이 평소 'law.go.kr에서 30분 뒤져야 답이 나오는 질문'을 1주에 몇 건 마주합니까? 그 시간을 본인 챗봇이 어디까지 줄여줄 수 있을 것 같습니까?

?

*ii / **Recall***

본인 답변에 환각 인용이 1건 섞여 동료·민원인에게 나갔다면, 본인은 어떻게 회수하시겠습니까? Air Canada처럼, 그 책임은 기관에게 어떤 형태로 돌아옵니까?

?

*iii / **Retention***

오늘 만든 챗봇을 한 달 뒤에도 본인이 계속 쓰고 있을 것 같습니까? 그렇지 않다면, 무엇이 막고 있을 것 같습니까?

KEY TAKEAWAYS · 마치며

출처가 챗봇을 만들고,
챗봇이 부서를 다시 정의합니다.

점심 전 · 2H	도입 + 환경 셋업 + 마크다운 기초 — **도구 점진 진입 + AI 공용어 익히기**.
점심 후 · 5H	시스템 프롬프트 + Project + MCP + 환각 방지 4겹 + 킬러 3종 + 실습. **신뢰성 설계**.
다음 주 1주	Action Plan 4가지 — 본인 챗봇 실사용 + 환각 1건 캡처 + **동료 1명 시연**.

Q&A

남은 시간은 본인 부서의 자리에서 가져온 질문을 위한 자리. 무엇을 묻든 좋습니다.

PRESENTER

김혜련 · artetlab

2026.06.01 · GH 법률·규정·지침 해석 지원 챗봇 강의 7H (09:30-18:00)