

Hermes Agent 로 이해하는 프로파일·에이전트·봇 — Agentic AI 멀티에이전트 입문

역할을 나눈 AI 에이전트 팀을 사람 팀처럼 이해하기

AI 에이전트 팀은 사람 팀과 같은 방식으로 이해하면 됩니다. 프로파일은 직원의 자리와 기록이고, 에이전트는 그 자리에서 지금 일하는 직원이며, 메신저 봇과 Bot Mode 봇은 그 직원을 부르는 창구입니다. 이 셋을 나누어 두었기 때문에 여러 에이전트가 기억과 비밀 정보를 서로 섞지 않고 한 팀으로 일합니다.

목차

Hermes Agent 로 이해하는 프로파일·에이전트·봇 — Agentic AI 멀티에이전트 입문

- 1장. 말하는 AI 에서 일하는 AI 로
 - 1.1 질문에 답하고 끝나는 챗봇과 일을 끝까지 맡는 AI 에이전트의 차이
 - 1.2 도구 사용과 예약 실행, 지난 일의 기억으로 챗봇과 구분되는 에이전트의 능력
 - 1.3 에이전트에 맡길 업무와 사람이 맡을 확인·판단의 경계
- 2장. 혼자 일하는 에이전트에서 에이전트 팀으로 — 역할을 나눌 때의 이점과 판단 기준
 - 2.1 에이전트 하나에 모든 업무를 맡길 때 섞이는 기억과 권한
 - 2.2 역할을 나눈 에이전트 여럿이 한 팀으로 일하는 멀티에이전트 방식
 - 2.3 에이전트 팀이 필요한 업무와 한 에이전트로 충분한 업무의 판단 기준
 - 2.4 역할 나누기를 프로파일 단위로 정리한 오픈소스 Hermes Agent
- 3장. 에이전트의 자리와 기록을 담는 프로파일
 - 3.1 사원증과 업무 노트처럼 대화가 끝나도 남는 프로파일의 정의
 - 3.2 프로파일 한 개에 담기는 여덟 가지 항목
 - 3.3 역할마다 프로파일을 따로 두는 칸막이 — 설정을 서로 물려받지 않는 독립 단위
 - 3.4 칸막이와 금고의 차이 — 프로파일이 보장하지 않는 운영 조건
- 4장. 지금 일하는 직원인 에이전트와 그 에이전트가 부르는 도우미 서브에이전트
 - 4.1 대화 한 건, 예약 작업 한 건마다 실행되고 끝나면 사라지는 에이전트
 - 4.2 프로파일 하나에 에이전트 여럿 — 1:N 관계와 저장되지 않는 에이전트
 - 4.3 큰 일을 나눠 맡기는 서브에이전트 — 기본 최대 10개의 도우미
- 5장. 에이전트를 부르는 두 가지 창구 — 메신저 봇과 Bot Mode 봇
 - 5.1 「봇」 한 낱말이 가리키는 두 대상 — 메신저 계정과 자리 배치도 이름표
 - 5.2 메신저 봇 하나는 프로파일 하나에만 연결되는 텔레그램·슬랙 계정
 - 5.3 Bot Mode 봇 — 데스크톱 명단에 오른 프로파일의 얼굴과 고정 대화방
 - 5.4 새 역할에는 새 프로파일, 같은 역할에는 창구 추가 — 두 봇을 함께 쓰는 판단
- 6장. 에이전트 팀이 함께 일하는 방식 — 업무 게시판으로 주고받는 일감
 - 6.1 모든 프로파일이 함께 보는 업무 게시판(칸반)
 - 6.2 도우미 부르기와 업무 게시판 사이의 선택 기준
 - 6.3 Bot 끼리 주고받는 직접 메시지와 다른 서버 Bot 과의 연결
 - 6.4 업무 역할 11개로 구성한 에이전트 팀 운영 사례
- 7장. 에이전트를 옮기고 나눠 줄 때 지키는 비밀 정보 — 내보내기 파일과 배포판의 차이
 - 7.1 직원 대신 책상과 업무 노트를 옮기는 세 가지 이전 방식
 - 7.2 다른 팀이 설치하고 업데이트하는 배포판
 - 7.3 내보내기 파일에 들어가는 것과 넘기기 전 비밀 정보 점검
 - 7.4 남에게 줄 때는 배포판, 서버를 옮길 때는 내보내기 — 방식 선택과 이전 전 점검표
- 8장. 우리 조직의 첫 에이전트 팀 — 반복 업무 3개로 꾸리는 시범 도입과 MSAP.ai AAS
 - 8.1 반복 업무 3개와 「업무 하나 = 프로파일 하나」로 그리는 종이 위의 시범 팀

8.2 부르는 창구 선택과 2주 시범 운영의 확인 항목

8.3 시범 도입 검토 목록에 올릴 1~7장의 의사결정 질문 묶음

8.4 명령줄 없이 화면에서 에이전트 팀을 쓰는 MSAP.ai AAS

부록: 참고문헌과 용어 정의

Appendix A — 참고문헌 (References)

Appendix B — 용어 정의 (Glossary)

Hermes Agent 로 이해하는 프로파일·에이전트·봇 — Agentic AI 멀티에이전트 입문

AI 에이전트 팀은 사람 팀과 같은 방식으로 이해하면 됩니다. 프로파일은 직원의 자리와 기록이고, 에이전트는 그 자리에서 지금 일하는 직원이며, 메신저 봇과 Bot Mode 봇은 그 직원을 부르는 창구입니다. 이 셋을 나누어 두었기 때문에 여러 에이전트가 기억과 비밀 정보를 서로 섞지 않고 한 팀으로 일합니다. 1장은 답을 주는 AI와 일을 끝내는 AI를 가르고, 2장은 에이전트를 여럿으로 나눌지 판단하는 기준을 세운 뒤 이 백서의 기준 사례인 오픈소스 에이전트 제품을 소개합니다. 3장부터 7장까지는 그 제품을 따라 프로파일, 에이전트와 도우미, 부르는 창구, 업무 게시판, 이전과 배포를 차례로 회사 조직에 빚대어 설명합니다. 마지막 8장은 매일 되풀이되는 업무 3개로 시범 에이전트 팀을 종이에 그리고, 업무마다 부르는 창구와 결과 확인자를 정해 시범 도입 검토 목록에 올리는 방법을 정리합니다. 각 장 끝의 「8장으로 가져갈 질문」을 모으면 그 검토 목록의 빈칸이 채워집니다.

1장. 말하는 AI 에서 일하는 AI 로

Agentic AI(에이전틱 AI)는 AI 모델이 질문에 답하는 데서 멈추지 않고 검색·파일·메신저 같은 도구를 직접 써서 맡은 일을 끝내는 방식을 가리키며, 이렇게 일하는 프로그램을 AI 에이전트라고 부릅니다. Anthropic은 2024년 12월 공개한 글에서 에이전트를 LLM(Large Language Model, 대규모 언어 모델)이 일하는 순서와 쓸 도구를 스스로 정하고 도구를 쓴 결과를 보며 다음 행동을 고르는 시스템으로 정의했습니다[S7]. 반면 대부분의 조직이 지금 쓰는 대화형 AI, 즉 챗봇은 질문을 받으면 글로 된 답을 내놓고 대화를 마칩니다. 같은 「AI 도입」이라는 말 안에도 답을 받는 도구와 일을 맡기는 동료라는 성격이 다른 두 가지 선택지가 함께 들어 있습니다.

두 선택지를 지금 구분해야 하는 이유는 의사결정의 대상이 바뀌었기 때문입니다. 챗봇 도입은 직원이 질문할 도구를 하나 더 고르는 결정이었지만, 에이전트 도입은 어떤 업무를 AI에게 맡기고 그 결과를 누가 확인할지를 정하는 결정입니다. 에이전트는 사람의 지시 없이 정해진 시각에 일을 시작하고 지난 업무 내용을 기억해 다음 일에 이어 쓰므로, 맡긴 업무의 범위가 그대로 에이전트가 움직이는 범위입니다[S1][S5]. 에이전트 팀을 이루는 낱말들을 하나씩 나누어 보기 전에 답을 주는 AI와 일을 끝내는 AI를 먼저 구분해 두어야 이후의 설명을 자기 조직의 업무에 맞춰 읽을 수 있습니다.

첫 장에서 얻을 것은 챗봇과 에이전트를 가르는 세 가지 능력, 그리고 결과를 확인할 사람을 업무보다 먼저 정하는 원칙이며, 이 둘이 8장에서 시범 도입할 업무를 고르는 첫 기준이 됩니다.

한 줄 요약 챗봇은 묻는 말에 답하는 안내 데스크 직원이고, AI 에이전트는 일을 받아 도구를 써서 결과물까지 만들어 내는 업무 담당자입니다.

1.1 질문에 답하고 끝나는 챗봇과 일을 끝까지 맡는 AI 에이전트의 차이

챗봇과 AI 에이전트는 같은 AI 모델을 쓰더라도 일이 끝나는 시점이 서로 다릅니다. 챗봇은 답을 보여 준 순간 할 일이 끝나고 그 답을 실행하는 몫은 질문한 사람에게 남지만, 에이전트는 결과물을 내놓을 때까지 도구 사용과 결과 확인을 여러 번 되풀이합니다[S7]. 이 차이는 회사 업무에 견주어 보면 분명합니다. 회사 안에서도 질문에

답하는 안내 창구와 일을 맡아 처리하는 담당 부서는 하는 일이 다르고, 경영진이 일을 끝까지 맡길 때 찾는 상대는 담당 부서입니다.

1.1.1 안내 데스크 직원과 업무 담당자 비유로 본 챗봇과 에이전트

쉬운 비유 안내 데스크 직원은 「입찰 공고는 어디서 찾나요?」라는 물음에 정확한 방법을 알려 주지만 공고를 직접 찾아 주지는 않습니다. 업무 담당자는 같은 부탁을 받으면 공고를 찾고 표로 정리해 결과를 보고합니다.

안내 데스크 직원에 해당하는 챗봇

챗봇은 회사 로비의 안내 데스크 직원과 같은 일을 합니다. 묻는 말에는 막힘없이 답하고 설명도 친절하며 필요하면 문서 초안까지 써 주지만, 대화 창 밖으로 나가 다른 시스템을 직접 다루지는 않습니다. 챗봇이 내놓는 것은 언제나 글로 된 답이고, 그 답을 업무 시스템에 옮기거나 메일로 보내는 일은 질문한 사람이 직접 처리합니다. 대화가 끝나면 다음 대화에서 같은 배경을 처음부터 다시 설명해야 하는 경우가 많아, 반복되는 업무일수록 사람의 수고가 줄지 않습니다. 챗봇과 에이전트를 자율성·도구 사용·기억 같은 기준으로 나누어 보는 방식은 공개된 비교 글에서도 같은 틀로 정리되어 있습니다[R1].

업무 담당자에 해당하는 AI 에이전트

AI 에이전트는 일을 받아 끝까지 처리하는 업무 담당자에 해당합니다. 담당자는 요청을 받으면 필요한 자료를 찾고, 사내 시스템에 접속해 내용을 확인하고, 결과를 정리해 보고하는 순서를 스스로 정합니다. 에이전트도 같은 방식으로 검색, 파일 읽기와 쓰기, 메신저 전송 같은 도구를 골라 쓰고 도구를 쓴 결과를 보고 다음 행동을 고릅니다[S7]. 에이전트에게는 질문 한 줄보다 업무 한 건을 통째로 건네고, 그 대가로 받는 것도 설명이 담긴 답보다 바로 쓸 수 있는 결과물입니다.

회사 비유로 이어지는 에이전트 팀의 구성 요소

이 회사 비유는 에이전트 한 명을 넘어 에이전트 팀 전체로 이어집니다. 회사의 담당자에게는 일하는 책상과 지난 업무 기록, 익힌 업무 방식이 있고, 동료들은 사내 메신저로 그 담당자를 부르며, 부서끼리는 업무 게시판에 일감을 올려 넘깁니다. 2장 끝에서 소개할 에이전트 제품도 설정·기록·익힌 기술·예약 작업을 에이전트마다 따로 보관하고, 메신저 계정으로 에이전트를 부르며, 일감을 넘길 때마다 기록이 한 줄씩 남는 게시판을 둡니다[S1][S3][S6]. 3장 이후의 프로파일은 담당자의 자리와 기록, 에이전트는 지금 일하는 직원, 메신저 봇은 그 직원을 부르는 창구에 각각 대응합니다.

같은 부탁, 끝나는 자리가 다르다 — 챗봇과 AI 에이전트

부탁 한 건: 「지난달 입찰 공고를 정리해 주세요」

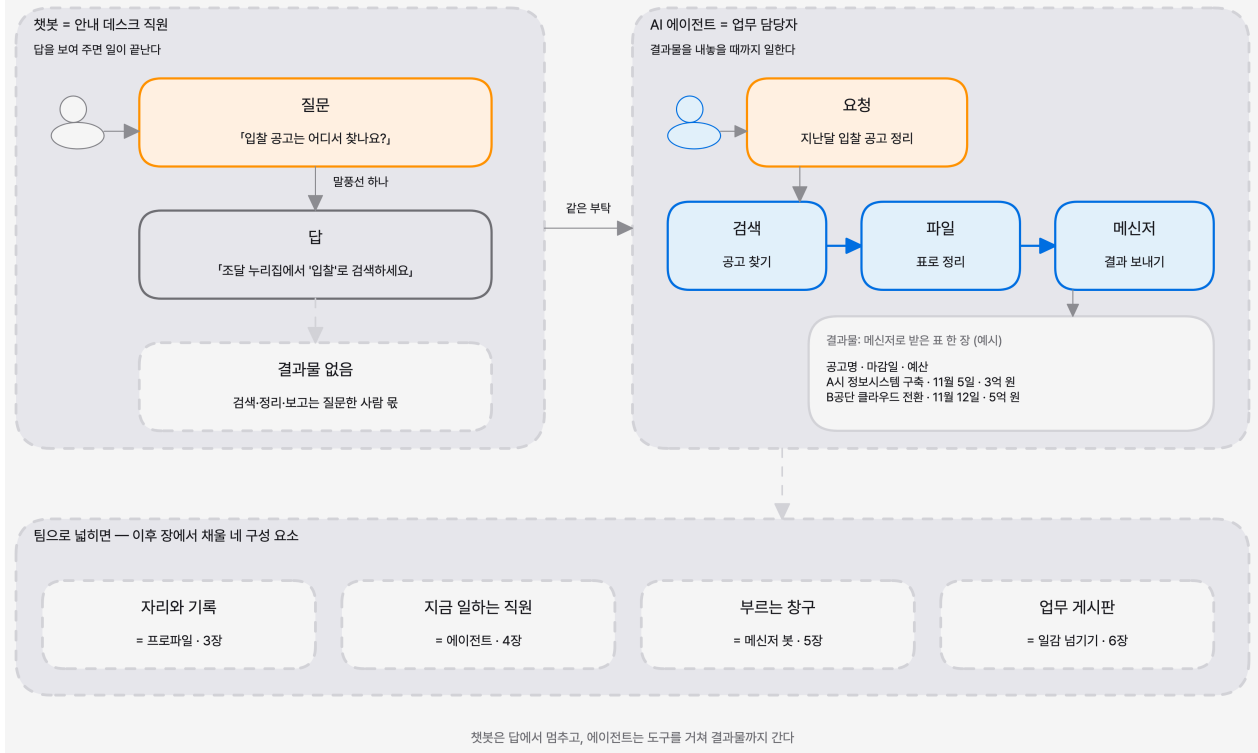


그림. 회사 비유로 본 챗봇과 AI 에이전트의 차이, 그리고 에이전트 팀의 네 구성 요소

1.1.2 입찰 공고 정리 요청 하나로 비교한 챗봇의 답과 에이전트의 결과물

예를 들면 영업 부서가 「지난달 입찰 공고 정리해 줘」라고 요청합니다. 챗봇은 나라장터(조달청 국가종합전자조달시스템)에서 기간과 분야를 지정해 검색하고 엑셀로 내려받아 정리하는 방법을 단계별로 알려 줍니다. 에이전트는 공고를 직접 검색해 공고명·발주 기관·예산·마감일을 표로 만들고, 그 표를 영업팀 메신저 방에 올린 뒤 처리 결과를 보고합니다.

같은 요청 뒤에 남는 일의 양

두 결과의 차이는 요청을 마친 뒤 사람에게 남는 일의 양에서 드러납니다. 챗봇의 답을 받은 영업 담당자는 여전히 검색하고 내려받고 표를 만드는 작업을 직접 해야 하므로 업무 시간이 거의 줄지 않습니다. 반면 에이전트의 결과물을 받은 영업 담당자는 표의 내용이 맞는지 확인하고 참여할 공고를 고르는 판단에만 시간을 씁니다. 다시 말해 답은 사람이 실행해야 쓸모가 생기지만 결과물은 사람이 확인하면 곧바로 업무에 쓸 수 있으며, 이 차이가 곧 AI에게 맡길 수 있는 일의 차이입니다.

챗봇과 AI 에이전트의 일곱 가지 비교 항목

같은 요청에 대한 두 AI의 결과를 항목별로 나란히 놓으면 다음과 같습니다. 일곱 개 항목 가운데 도구 사용, 예약 실행, 기억 세 가지가 두 AI를 가르는 능력이고 나머지 항목은 그 능력에서 나오는 결과입니다.

비교 항목	챗봇	AI 에이전트
받은 요청	「지난달 입찰 공고 정리해 줘」	같은 요청
답의 형태	검색·정리 방법을 설명한 글	공고 목록 표와 처리 보고
도구 사용	대화 창 안에서 글만 작성	검색, 파일 작성, 메신저 전송을 직접 실행
예약 실행	사람이 물어야 시작	정해진 시각에 같은 작업을 스스로 시작
기억	대화가 끝나면 배경을 다시 설명	지난번 기준(분야·예산 범위)을 이어서 사용
결과물	사람이 직접 만들어야 함	메신저로 받은 공고 목록 표
결과 확인 주체	질문한 사람이 작업까지 수행	요청한 사람이 표를 확인하고 판단

출처: 에이전트 정의는 Anthropic(2024-12)[S7], 예약 실행과 기억은 2장에서 소개할 에이전트 제품의 공식 문서[S1][S5]를 바탕으로 정리했습니다.

입찰 공고 정리를 매일 맡기는 운영 방식

같은 요청을 매일 받는 영업 부서라면 에이전트에게 「입찰 공고 정리」라는 업무 하나를 통째로 맡기고, 정해진 시각마다 결과를 받는 방식으로 운영할 수 있습니다. 이때 에이전트는 영업 부서가 정한 검색 기준과 지난 정리 결과를 계속 가지고 있어야 하므로, 그 기준과 기록을 담아 두는 단위가 필요합니다. 「영업 담당」이라는 이름으로 이 기준과 기록을 묶어 두면 다음 달 정리에서도 같은 기준으로 일하며, 이 묶음을 프로파일이라고 부릅니다(3장)[S1].

1.2 도구 사용과 예약 실행, 지난 일의 기억으로 챗봇과 구분되는 에이전트의 능력

AI 에이전트를 챗봇과 구분하는 능력은 도구 사용, 예약 실행, 기억 세 가지입니다. 도구를 쓸 수 있어야 글 대신 결과물을 만들고, 예약 실행이 있어야 사람이 부르지 않아도 반복 업무를 처리하며, 기억이 있어야 같은 배경을 매번 다시 설명하지 않고 일을 이어 갑니다[S1][S7]. 세 능력은 에이전트의 기술 사양이면서 동시에 에이전트에게 어떤 업무를 맡길 수 있는지 판단하는 기준입니다. 결과물이 필요 없는 일에는 도구가, 시작 시각이 정해지지 않은 일에는 예약 실행이 쓸모없습니다.

챗봇과 에이전트를 가르는 기준은 대화 창의 모양이나 AI 모델의 크기가 아니라 일을 처리하는 방식에 있습니다. 같은 모델을 쓰더라도 사람이 답을 읽고 다음 지시를 내리면 챗봇처럼 쓰는 것이고, 목표를 받은 뒤 어떤 도구를 부르고 어떤 파일을 열고 언제 멈출지를 스스로 정해 여러 단계를 이어 가면 에이전트로 쓰는 것입니다. 예를 들어 「지난주 장애 접수 건을 정리해 보고서 초안을 만들어 달라」는 요청 하나에 에이전트는 접수 시스템 조회, 관련 파일 읽기, 문서 작성까지를 한 흐름으로 이어서 처리합니다. 에이전트의 정의와 구성 요소, 기업이 도입할 때 살펴볼 기준은 공개된 해설 글[R2]에서도 함께 정리되어 있습니다.

1.2.1 검색·파일·메신저·업무 시스템을 쓰고 결과를 보며 다음 행동을 고르는 반복 구조

에이전트가 쓰는 도구 네 종류

에이전트가 쓰는 도구는 쓰임새에 따라 네 종류로 나눌 수 있으며, 어떤 도구를 쓸 수 있는지는 에이전트마다 따로 정합니다.

- 검색 — 웹이나 사내 문서에서 필요한 자료를 찾습니다.
- 파일 — 문서와 표를 읽고 새 문서나 표를 만들어 저장합니다.
- 메신저 — 텔레그램(Telegram)·슬랙(Slack) 같은 메신저 방으로 결과를 보내고 질문을 받습니다 [S6].
- 업무 시스템 — 고객 관리 시스템(CRM, Customer Relationship Management)이나 모니터링 화면처럼 이미 쓰는 시스템에서 값을 조회하거나 기록합니다.

쓸 수 있는 도구 묶음이 넓을수록 에이전트가 끝낼 수 있는 일의 범위도 넓지만, 그만큼 사람이 확인해야 할 동작도 많습니다. 처음에는 업무 하나에 필요한 도구만 열어 두고, 결과가 안정적으로 나오는 것을 확인한 뒤 범위를 늘리는 편이 관리하기 쉽습니다.

요청에서 완료 보고까지 이어지는 반복 구조

에이전트의 일은 요청, 계획, 도구 실행, 결과 확인, 다음 행동, 완료 보고의 순서로 이어지고 결과 확인과 다음 행동 사이를 여러 번 오갑니다. 예를 들어 입찰 공고를 찾던 에이전트가 검색 결과에 지난달 이전 공고가 섞인 것을 보면 날짜 조건을 고쳐 다시 검색하고, 예산 항목이 빠진 공고는 상세 페이지를 한 번 더 열어 값을 채웁니다. Anthropic은 에이전트를 결과를 보며 반복해서 도구를 쓰는 LLM으로 설명하고, 사람이 미리 정한 순서대로 도구를 부르는 자동화 흐름인 워크플로(workflow)와 구분했습니다[S7]. 에이전트의 핵심은 도구의 개수보다 결과를 보고 다음 행동을 스스로 고르는 반복 구조에 있습니다.

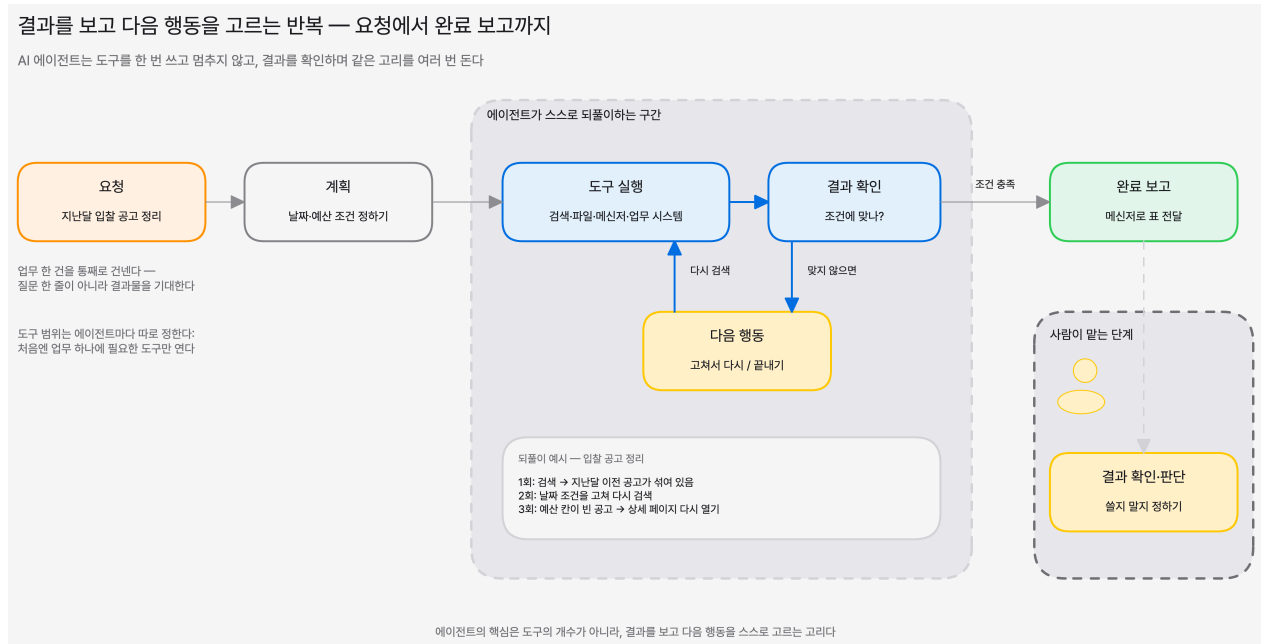


그림. 요청에서 완료 보고까지 AI 에이전트가 도구를 쓰며 일하는 반복 구조

스스로 고르는 도구 실행의 이득과 사람 확인의 필요

에이전트가 스스로 판단해 도구를 실행한다는 점은 업무를 빨리 끝내게 하는 이득이면서 동시에 사람의 확인이 필요한 이유입니다. 단계마다 사람에게 묻지 않으므로 처리 속도는 빠르지만, 첫 단계에서 잘못 고른 조건이 이

후 단계에 그대로 이어질 수 있습니다. Anthropic도 에이전트는 자율적으로 움직이는 만큼 비용이 늘고 오류가 쌓일 수 있으므로 격리된 환경에서 충분히 시험하고 알맞은 안전장치를 두라고 권했습니다[S7]. 비용 면에서도 도구 실행을 되풀이하는 만큼 AI 모델이 읽고 쓰는 글의 양, 즉 토큰 사용량이 늘어납니다. Anthropic이 2025년 6월 자사 다중 에이전트 조사 시스템을 만들며 조사 업무의 사용량을 켜 결과, 에이전트 하나는 일반 채팅보다 토큰을 약 4배 썼습니다[S8]. 여러 에이전트가 함께 일할 때 사용량이 얼마나 더 늘어나는지는 2장(2.2.2)에서 같은 측정으로 이어 봅니다. 에이전트에게 일을 맡길 때는 쓸 수 있는 도구의 범위와 결과를 확인할 사람을 함께 정합니다.

1.2.2 사람의 지시 없이 정해진 시각에 실행되는 예약 작업과 지난 일을 이어 쓰는 기억

정해진 시각에 시작하는 예약 작업

예약 작업은 에이전트가 사람의 지시 없이 정해진 시각에 정해진 일을 시작하게 하는 기능입니다. 서버에서 정해진 시각에 명령을 실행하는 예약 기능과 원리가 같으며, 2장 끝에서 소개할 에이전트 제품도 에이전트의 반복 업무(루틴)를 일반 예약 작업으로 등록해 실행합니다[S5]. 예를 들어 「매주 월요일 오전 9시에 지난주 입찰 공고를 정리해 영업팀 메신저 방에 올린다」는 업무를 한 번 등록하면, 에이전트는 그 시각마다 검색부터 보고까지를 스스로 처리합니다. 사람이 대화 창을 열어 물어야 시작하는 챗봇과 비교하면 예약 작업은 반복 업무의 시작을 사람의 기억과 일정표에서 떼어 내는 기능입니다.

예약 작업으로 맡기기 좋은 첫 업무로는 아침 소식 정리가 자주 꼽힙니다. 매일 오전 8시에 에이전트가 새 대화로 시작해 관심 분야의 최신 자료를 찾고, 가장 중요한 소식 세 건을 골라 제목·세 문장 요약·중요한 이유·원문 링크로 정리한 뒤 팀 메신저 방에 보내는 방식입니다. 같은 소식을 여러 매체가 다루면 하나로 합치고 전날 보낸 소식과 겹치는 항목은 빼도록 정해 두면, 받는 사람이 같은 내용을 두 번 읽지 않습니다. 이런 업무는 한 번에 찾을 자료 수와 쓸 수 있는 비용의 상한을 함께 정해 두는 편이 안전하며, 주중과 주말의 실행 시각을 다르게 두거나 주제마다 도우미를 나눠 동시에 조사하게 하는 식으로 넓혀 갈 수 있습니다(4장).

지난 업무를 이어 쓰는 기억

기억은 지난 대화와 업무 내용을 다음 일에 이어 쓰는 능력입니다. 에이전트는 사용자가 알려 준 조건과 지난 업무 내용을 에이전트마다 따로 두는 기억에 남기고, 다음 대화나 다음 예약 작업에서 다시 읽습니다[S1]. 예를 들어 「건설 분야는 빠고 예산 1억 원 이상만」이라는 조건을 한 번 알려 두면, 에이전트는 다음 주 정리에서도 같은 조건으로 공고를 고릅니다. 반면 기억이 없는 챗봇에서는 같은 조건을 대화를 열 때마다 다시 입력해야 하고, 입력을 빠뜨리면 결과도 달라집니다.

예약 작업과 기억이 함께 만드는 업무 연속성

예약 작업과 기억이 함께 있어야 에이전트는 매번 처음부터 설명하지 않아도 일을 이어 가는 동료가 됩니다. 예약 작업은 일을 시작하는 시각을, 기억은 일을 처리하는 기준을 맡기 때문에 둘 중 하나만 있으면 반복 업무를 온전히 맡기기 어렵습니다. 에이전트의 기억, 예약 작업, 익힌 기술은 에이전트마다 따로 보관하는 묶음에 함께 담기며, 이 묶음이 3장의 프로파일입니다[S1]. 어떤 반복 업무를 맡길 수 있는지 판단할 때는 그 업무에 정해진 시작 시각이 있는지, 그리고 지난 결과를 이어 써야 하는지를 먼저 확인합니다.

1.3 에이전트에 맡길 업무와 사람이 맡을 확인·판단의 경계

AI 에이전트를 도입해도 기존 업무 시스템과 사람의 역할은 그대로 남고, 바뀌는 것은 반복 업무를 처리하는 주체입니다. 에이전트는 메신저·고객 관리 시스템·모니터링·문서 저장소를 그대로 둔 채 그 옆에 연결하는 AI 동료

이고, 사람은 에이전트가 만든 결과를 확인하고 판단합니다. Anthropic도 에이전트가 정해 둔 확인 단계에 이르기나 진행이 막히면 사람의 판단을 받도록 설계할 수 있다고 설명했습니다[S7]. 따라서 에이전트에게 맡길 업무를 고를 때는 그 업무의 결과를 누가 확인할지를 처음부터 함께 적어 둡니다.

1.3.1 기존 메신저·업무 시스템을 그대로 두고 그 옆에 붙는 AI 동료의 자리

이렇게 쓴다 같은 일이 매일 되풀이되는 부서 업무 하나를 골라 에이전트에게 맡기고, 결과는 그 업무를 원래 맡던 사람이 확인합니다. 메신저와 업무 시스템은 지금 쓰는 것을 그대로 씁니다.

기존 메신저를 그대로 쓰는 연결 방식

에이전트 도입은 기존 시스템을 교체하는 결정보다 기존 시스템 옆에 AI 동료를 추가하는 결정에 가깝습니다. 에이전트는 사내에서 이미 쓰는 메신저로 결과를 보내고, 고객 관리 시스템과 문서 저장소에서는 필요한 값을 조회하거나 기록합니다. 메신저 쪽에서는 에이전트마다 메신저 봇 계정을 하나씩 따로 두며, 개인 비서 에이전트와 개발 지원 에이전트를 서로 다른 텔레그램 메신저 봇으로 운영하거나 슬랙 작업 공간마다 에이전트를 하나씩 두는 쓰임새가 같은 제품의 공식 문서에 예시로 실려 있습니다[S6]. 사용자는 새 화면을 익히지 않고 평소 쓰던 메신저 방에서 에이전트에게 일을 맡기고 결과를 받습니다.

부서별 반복 업무와 결과 확인자

에이전트를 연결하기에 알맞은 업무는 영업·재무·인사·마케팅·IT 운영처럼 같은 일이 매일 또는 매주 되풀이되는 부서 업무입니다. 다음 표는 부서마다 에이전트에게 맡길 수 있는 반복 업무와 그 결과를 확인할 사람을 짝지은 예시이며, 8장에서 시범 업무 후보를 고를 때도 같은 틀을 씁니다.

부서	반복 업무 예시	결과 확인자
영업	입찰 공고 수집과 정리, 경쟁사 소식 요약	영업 담당자
재무	비용 증빙 대조, 월말 정산 자료 취합	재무 담당자
인사	지원서 1차 분류, 입사 서류 누락 점검	채용 담당자
마케팅	발행 콘텐츠 반응 집계, 주간 성과 정리	마케팅 담당자
IT 운영	서버 경보 1차 분류, 장애 경위서 초안 작성	운영 당번 엔지니어

표의 다섯 업무는 모두 결과물이 표나 짧은 문서로 나오고, 그 업무를 원래 맡던 사람이 몇 분 안에 맞고 틀림을 가릴 수 있다는 공통점이 있습니다. 반면 계약 조건 협상이나 인사 평가처럼 판단 자체가 업무의 핵심인 일은 에이전트가 자료를 모아 주더라도 결정은 사람이 내립니다.

사람이 맡는 확인과 판단

에이전트가 반복 업무를 맡으면 사람의 일은 결과를 확인하고 판단하는 쪽으로 옮겨 갑니다. 예를 들어 영업 담당자는 공고 표를 만드는 데 쓰던 시간을 참여할 공고를 고르고 제안 방향을 정하는 데 쓰고, 재무 담당자는 대조 표에서 어긋난 항목의 원인을 확인하는 데 씁니다. Anthropic은 에이전트 시스템을 만들 때 가장 단순한 방법으

로 시작하고 필요할 때만 복잡도를 늘리라고 권했으며[S7], 같은 원칙에 따라 첫 에이전트에게는 결과 확인이 쉬운 업무 하나를 맡기는 편이 안전합니다. 에이전트 도입의 범위는 기술이 할 수 있는 일보다 사람이 확인할 수 있는 결과물의 범위에 맞춰 정합니다.

1.3.2 결과 확인자를 먼저 정하는 원칙과 8장으로 가져갈 첫 질문

결과 확인자를 업무보다 먼저 정하는 원칙

에이전트에게 맡길 업무를 고를 때는 결과를 누가 확인할지를 업무보다 먼저 정합니다. 확인자가 정해지지 않은 업무에서는 에이전트가 잘못 고른 조건이 그대로 다음 업무로 넘어가고, 문제가 생겼을 때 바로잡을 사람을 찾기 어렵습니다. 반대로 확인자가 정해져 있으면 에이전트의 결과물이 그 사람의 검토를 거쳐 업무에 쓰이므로, 에이전트의 판단이 틀려도 그 영향이 확인 단계 안에서 멈춥니다. 같은 제품의 공식 문서도 사람 확인이 필요하거나 중간에 멈췄다 다시 시작해도 이어져야 하는 일은 일감을 넘길 때마다 기록이 한 줄씩 남는 업무 게시판으로 관리하도록 권합니다[S3].

업무 선정의 첫 기준인 확인 가능성

확인 가능성은 시범 도입할 업무를 고르는 첫 기준이기도 합니다. 공고 목록, 정산 대조표, 경보 분류 결과처럼 사람이 짧은 시간에 맞고 틀림을 가릴 수 있는 결과물은 에이전트에게 맡기기 좋고, 매일 되풀이되는 업무라면 예약 작업과 기억의 효과도 함께 드러납니다. 1장의 질문은 「매일 되풀이되는가」와 「결과를 사람이 확인할 수 있는가」라는 두 조건을 한 문장에 담고 있으며, 이 질문이 8장 의사결정 질문 묶음표의 첫 행입니다.

기억할 것

1. AI 에이전트는 검색·파일·메신저 같은 도구를 직접 써서 맡은 일을 결과물까지 끝내는 AI입니다.
2. 정해진 시각에 일을 시작하는 예약 작업과 지난 일을 이어 쓰는 기억이 있어 반복 업무를 맡을 수 있습니다.
3. 에이전트가 만든 결과는 그 업무를 아는 사람이 확인하고 판단하며, 확인자는 업무보다 먼저 정합니다.

8장으로 가져갈 질문 우리 조직에서 매일 되풀이되고 결과를 사람이 확인할 수 있는 업무는 무엇인가?

2장. 혼자 일하는 에이전트에서 에이전트 팀으로 — 역할을 나눌 때의 이점과 판단 기준

1장 끝의 질문으로 매일 되풀이되는 업무를 몇 개 골랐다면, 다음에 부딪히는 질문은 그 업무를 모두 에이전트 하나에 맡길지입니다. 멀티에이전트(multi-agent) 방식은 역할을 나눈 AI 에이전트 여럿이 한 팀처럼 일하도록 구성하는 방법입니다. 1장에서 살펴본 AI 에이전트는 검색·파일·메신저 같은 도구를 쓰고, 정해진 시각에 예약 작업을 실행하며, 지난 대화를 기억해 다음 일에 이어 씁니다. 이런 에이전트 하나에 영업 업무와 재무 업무를 함께 맡기면 두 업무에 필요한 접속 정보와 대화 기록이 한 에이전트 안에 쌓이고, 에이전트가 다른 업무의 맥락으로 답하거나 맡은 일에 필요 없는 비밀 정보까지 갖게 됩니다. 그래서 조직이 사람의 일을 부서와 담당자로 나누듯 이 에이전트도 역할마다 따로 두는 구성이 쓰이기 시작했습니다. 2장은 역할을 나눴을 때 얻는 칸막이와 일 나누기의 이점, 그 대가인 AI 사용량 증가를 함께 놓고, 의사결정권자가 「한 에이전트로 충분한가, 여러 에이전트가 필요한가」를 자기 업무에 대입해 판정할 기준을 제시합니다. 끝으로 이 역할 나누기를 프로파일이라는 단위로 제품 안에 정리한 오픈소스 에이전트를 이 백서의 기준 사례로 소개합니다.

2.1 에이전트 하나에 모든 업무를 맡길 때 섞이는 기억과 권한

에이전트를 처음 도입하는 조직은 대개 이미 만든 에이전트 하나에 업무를 하나씩 더 맡기는 방식을 먼저 떠올립니다. 설정을 한 번만 하면 되고 담당자도 한 곳에만 물으면 되므로 처음에는 이 방식이 가장 간단해 보입니다. 하지만 업무가 늘어날수록 한 에이전트 안에 서로 다른 업무의 기억과 권한이 함께 쌓이고, 그 결과는 두 갈래로 나타납니다. 첫째는 기억이 섞여 다른 업무의 맥락으로 답하는 문제이고, 둘째는 권한이 섞여 맡은 일에 필요 없는 비밀 정보까지 갖게 되는 문제입니다. 두 문제 모두 AI 모델의 성능과 무관하게 업무를 한 에이전트에 몰아 둔 구성에서 생기므로, 모델을 바꾸는 것으로는 줄지 않습니다.

2.1.1 만능 비서 한 명과 부서별 담당자 팀의 비유

한 줄 요약 에이전트 하나에 모든 업무를 맡기면 기억과 권한이 한곳에 섞이므로, 사람 조직처럼 역할마다 에이전트를 나눠 둡니다.

쉬운 비유 만능 비서 한 명은 모든 부서의 서류와 열쇠를 한 책상에 두고 일하고, 부서별 담당자 팀은 각자 자기 책상과 자기 열쇠만 가지고 일합니다.

만능 비서 한 명에게 모든 부서의 일을 맡긴 회사를 생각해 보면 섞임이 어디서 생기는지 쉽게 드러납니다. 이 비서의 책상에는 영업 제안서, 재무 장부, 인사 기록이 함께 쌓이고, 서랍에는 재무 시스템 열쇠와 인사 시스템 열쇠가 나란히 들어 있습니다. 처음에는 누구든 비서 한 명에게만 부탁하면 되므로 편리하지만, 영업 담당자의 부탁을 처리하던 비서가 재무 장부 내용을 섞어 답하거나 영업 담당자가 비서를 거쳐 인사 기록을 받아 보는 일이 구조적으로 가능해집니다. 만능 비서 구성에서는 업무 사이의 경계가 비서 한 사람의 주의력에만 달려 있습니다.

반면 부서별 담당자 팀에서는 영업 담당자, 재무 담당자, 인사 담당자가 각자 자기 책상과 자기 열쇠만 가지고 일합니다. 영업 담당자는 재무 장부를 볼 필요가 없고 재무 담당자는 영업 고객의 대화 기록을 알 필요가 없으므로, 누가 무엇을 보고 누가 결과를 책임지는지가 조직도만 보고도 정해집니다. 회사가 사람의 일을 부서와 담당자로 나누는 이유는 한 사람이 모든 일을 해낼 수 없어서이기도 하지만, 기록과 권한을 업무 단위로 갈라 두어야 관리

할 수 있기 때문이기도 합니다. 멀티에이전트 방식은 같은 이유로 AI 에이전트를 역할마다 나누는 구성이며, 이 백서가 「AI 에이전트 팀은 사람 팀과 같은 방식으로 이해하면 된다」고 보는 출발점도 여기에 있습니다.

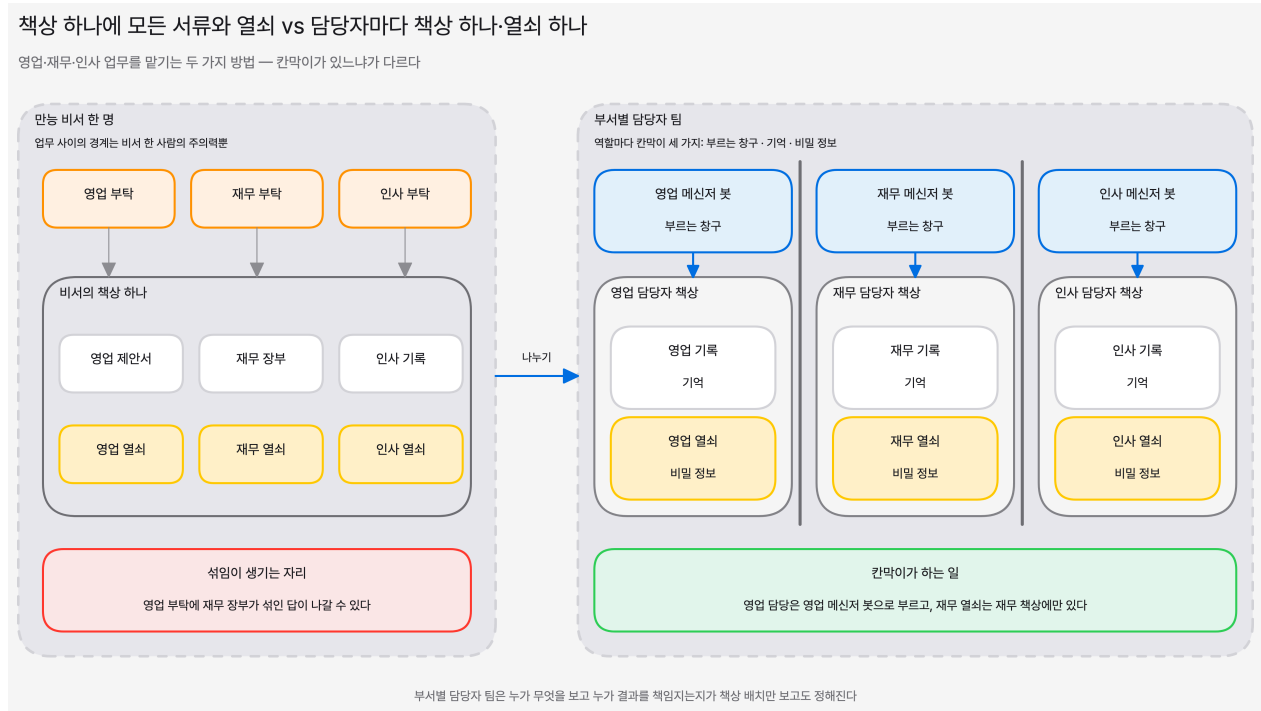


그림. 만능 비서 한 명의 책상과 부서별 담당자 팀의 책상 비교

2.1.2 영업 자료를 보던 에이전트가 재무 비밀 정보까지 갖게 되는 구성

예를 들면 1장의 입찰 공고 에이전트에게 「이번 달 손익도 정리해 줘」를 더 맡기면, 영업 자료를 보던 에이전트가 재무 시스템 접속 정보와 재무팀 대화 기록까지 함께 갖게 됩니다.

1장에서 「지난달 입찰 공고 정리해 줘」라는 요청을 받은 에이전트는 공고를 찾아 표로 만들고 메신저로 보내는 일을 끝까지 처리했습니다. 이 에이전트가 쓸모 있다는 판단이 서면 다음 요청으로 「이번 달 손익도 정리해 줘」가 붙는 것이 자연스러운 흐름입니다. 손익을 정리하려면 에이전트에게 재무 시스템 접속 정보를 주어야 하고, 재무팀과 주고받은 질문과 답도 그 에이전트의 대화 기록에 남습니다. 따라서 요청 하나를 더했을 뿐인데 영업 자료를 보던 에이전트가 다음 세 가지를 한꺼번에 갖게 됩니다.

한 에이전트에 담기는 것	원래 필요한 업무	그 정보가 필요한 사람
입찰 공고·고객 제안 자료	입찰 공고 정리	영업 담당
재무 시스템 접속 정보	이번 달 손익 정리	재무 담당
영업팀·재무팀과 나눈 대화 기록	두 업무 모두	각 부서 담당

기억 섞임: 다른 업무의 맥락으로 답하는 문제

에이전트가 한 번에 기억하는 대화 분량에는 한도가 있으므로, 영업 대화와 재무 대화가 한 에이전트에 함께 쌓이면 두 업무의 맥락이 그 한도를 나눠 씁니다. 영업 담당자가 입찰 공고를 물었는데 에이전트가 직전에 처리한 손익 수치를 끌어와 답하거나, 재무 대화가 길어지면서 앞서 정리한 영업 맥락이 기억에서 밀려나는 일이 생길

수 있습니다. Anthropic이 자사 조사 시스템을 설계하면서 도우미 에이전트마다 대화를 따로 기억하게 한 이유도 업무마다 맥락을 나눠 두기 위해서였습니다[S8]. 기억 섞임은 답의 품질을 떨어뜨리는 문제이고, 원인은 맥락을 업무별로 나누지 않은 구성에 있습니다.

권한 섞임: 맡은 일에 필요 없는 비밀 정보를 갖는 문제

권한 섞임은 기억 섞임보다 관리하는 쪽에서 더 무겁게 다뤄야 합니다. 재무 시스템 접속 정보를 가진 에이전트를 영업 담당자도 부를 수 있다면, 영업 담당자는 의도하지 않았더라도 에이전트를 거쳐 재무 시스템에 닿는 경로를 갖게 됩니다. 실제로 그런 요청이 오가지 않더라도 구성상 그렇게 될 수 있다는 사실만으로 이 에이전트는 영업 업무에도 재무 업무에도 맞지 않는 권한 범위를 가집니다. 다시 말해 에이전트 하나에 업무를 더할 때마다 그 에이전트를 부를 수 있는 사람 모두에게 새 업무의 권한 범위가 함께 열리므로, 업무를 더하는 결정은 곧 권한을 넓히는 결정입니다.

2.2 역할을 나눈 에이전트 여럿이 한 팀으로 일하는 멀티에이전트 방식

멀티에이전트 방식에서는 영업 에이전트, 재무 에이전트처럼 역할마다 에이전트를 따로 두고, 필요할 때 에이전트끼리 일을 주고받게 합니다. 이 구성으로 얻는 이점은 크게 두 가지입니다. 하나는 역할마다 기억·비밀 정보·부르는 창구를 따로 두는 칸막이이고, 다른 하나는 큰 일을 여러 에이전트가 나눠 동시에 처리하는 일 나누기입니다. 다만 에이전트 수가 늘어나면 AI 모델을 쓰는 양도 함께 늘어나므로, 이점과 사용량을 한 판단표 위에 같이 올려야 균형 잡힌 도입 의사결정을 할 수 있습니다.

에이전트가 목표를 받아 여러 단계를 스스로 이어 가는 방식을 넓게 Agentic AI(에이전틱 AI)라고 부르며, 생성형 AI가 답을 만드는 단계에서 일을 실행하는 단계로 넘어온 흐름은 공개된 입문 글[R3]에 정리되어 있습니다. 멀티에이전트 방식은 그 흐름 위에서 에이전트를 역할별로 여럿 두고 한 팀으로 묶는 구성입니다.

2.2.1 역할마다 기억·비밀 정보·부르는 창구를 따로 두는 칸막이의 이점

역할별 칸막이의 핵심은 영업 에이전트의 기억과 재무 에이전트의 비밀 정보가 섞이지 않고, 각 에이전트가 자기 메신저 창구로 불린다는 데 있습니다. 에이전트 제품의 공식 문서는 역할 하나에 해당하는 단위마다 설정, 비밀 정보, 성격, 기억, 대화 기록, 익힌 기술, 예약 작업을 각자 따로 보관하도록 설계하고, 그 단위를 목적별로 나눠 쓰는 예로 코딩 도우미·개인 비서·조사 담당 에이전트를 듭니다[S1]. 메신저 쪽도 같은 원칙을 따릅니다. 같은 메신저 봇 계정을 두 역할이 동시에 쓰지 못하게 막아 두었기 때문에, 텔레그램 메신저 봇 하나에는 개인 비서를 두고 다른 텔레그램 메신저 봇에는 코딩 담당 에이전트를 두는 식으로 창구도 역할마다 갈라집니다[S6].

칸막이	나누면 달라지는 것	자세히 다루는 장
기억	영업 대화와 재무 대화가 서로 다른 에이전트에 쌓여 맥락이 섞이지 않음	3장
비밀 정보	재무 시스템 접속 정보는 재무 에이전트에만 있음	3장
부르는 창구	영업 담당은 영업 에이전트의 메신저 봇으로, 재무 담당은 재무 에이전트의 메신저 봇으로 부름	5장

칸막이 세 가지는 서로를 보강합니다. 예를 들어 비밀 정보만 나누고 부르는 창구를 하나로 두면 누가 어느 에이전트에게 일을 시켰는지 기록이 섞이고, 창구만 나누고 기억을 한 곳에 두면 답의 맥락이 다시 섞입니다. 역할 하나를 나눌 때 세 가지를 한 묶음으로 나누는 것이 원칙입니다. 다만 이 칸막이는 업무 단위로 기록과 설정을 갈라두는 장치이고, 같은 서버 안의 파일 접근까지 막는 격리 공간과는 성격이 다릅니다[S1]. 칸막이가 보장하는 범위와 보장하지 않는 범위는 프로파일의 운영 조건과 함께 따로 정리해야 합니다(3장). 칸막이의 이점은 효과 수치로 약속할 성격이 아니며, 섞이지 않게 나눈다는 설계 이유로 판단하는 편이 정확합니다.

2.2.2 큰 조사를 나눠 동시에 처리하는 일 나누기와 늘어나는 AI 사용량

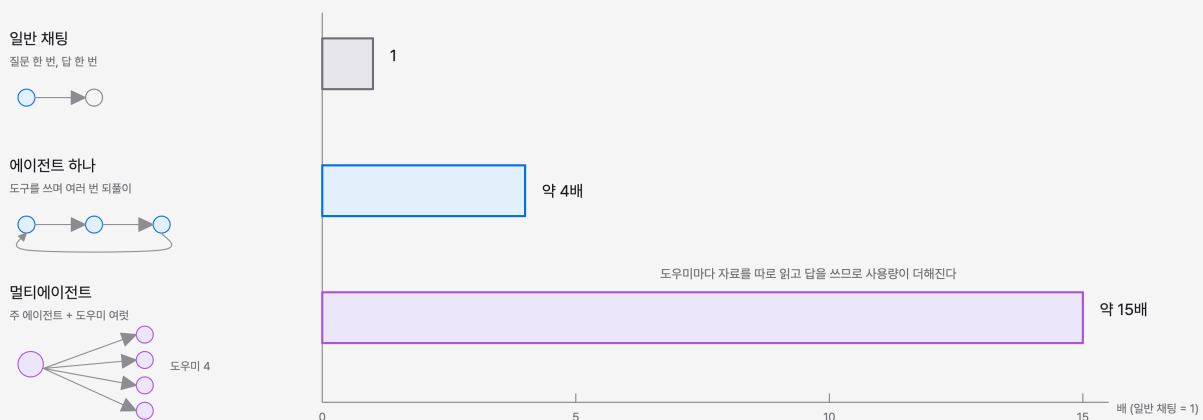
멀티에이전트 방식의 두 번째 이점은 큰 일을 여러 에이전트가 나눠 동시에 처리할 수 있다는 점입니다.

Anthropic이 공개한 조사 시스템에서는 주 에이전트가 조사 계획을 세운 뒤 도우미 에이전트 여럿을 띄우고, 도우미들이 각자 따로 기억하며 동시에 자료를 찾는 다음 핵심만 추려 주 에이전트에게 돌려줍니다[S8]. 에이전트 하나가 모든 자료를 직접 읽으면 한 번에 기억하는 대화 분량이 금방 차지만, 도우미에게 나눠 맡기면 각 도우미가 자기 몫만 읽고 요약을 넘기므로 주 에이전트는 더 넓은 범위를 다룰 수 있습니다. 예를 들어 경쟁사 다섯 곳의 기술을 비교하는 조사라면 도우미 다섯이 한 곳씩 맡아 동시에 조사하고 주 에이전트는 결과를 모아 비교표만 만들면 됩니다(4장).

이 이점에는 분명한 대가가 따릅니다. AI 모델은 글을 읽고 쓰는 양을 토큰(token, AI 모델이 처리하는 글의 양을 세는 단위)으로 세고 그 양만큼 비용을 받는데, 에이전트가 여럿이면 각자 자료를 읽고 답을 쓰므로 토큰 사용량이 함께 늘어납니다. Anthropic이 2025년 6월 공개한 자사 다중 에이전트 조사 시스템의 측정에서는 조사 업무를 처리할 때 에이전트 하나가 일반 채팅보다 토큰을 약 4배, 여러 에이전트가 함께 일하는 구성은 일반 채팅보다 약 15배 썼습니다[S8]. 같은 글은 이 방식이 경제적으로 맞으려면 늘어난 사용량을 감당할 만큼 업무의 가치가 높아야 한다고 덧붙입니다. 여럿으로 나누는 결정은 결국 업무 가치와 사용량을 견주는 비용 판단이기도 합니다.

같은 조사 업무, 늘어나는 AI 사용량 — 일반 채팅을 1로 놓고 잦 배수

토큰: AI 모델이 읽고 쓰는 글의 양을 세는 단위. 쓴 만큼 비용이 든다



측정 조건

Anthropic 자사 다중 에이전트 조사 시스템 · 조사 업무 · 2025년 6월 측정
업무 종류와 구성에 따라 달라진다 — 효과 약속이 아니라 비용을 따질 때 쓰는 참고값

여럿으로 나누는 결정은 업무 가치와 사용량을 견주는 비용 판단이기도 하다

그림. 조사 업무에서 켄 AI 사용량 비교 — 일반 채팅 1, 에이전트 하나 약 4, 멀티에이전트 약 15 (Anthropic 자사 다중 에이전트 조사 시스템, 조사 업무, 2025년 6월 측정 — 업무 종류와 구성에 따라 달라짐)

사용량 수치는 에이전트에 맡길 업무를 고르는 기준으로 쓸 때 가장 쓸모가 있습니다. Anthropic의 2024년 12월 공개 글도 에이전트 구성은 응답 시간과 비용을 더 쓰는 대신 업무 성과를 얻는 선택이므로 그 교환이 타당한 업무에만 쓰라고 권합니다[S7]. 실무에서는 매일 되풀이되고 결과의 가치가 분명한 업무부터 나누고, 한 번에 많은 도우미를 띄우는 큰 조사는 꼭 필요한 업무에만 허용하는 방식으로 사용량을 관리합니다.

2.3 에이전트 팀이 필요한 업무와 한 에이전트로 충분한 업무의 판단 기준

이렇게 쓴다 말기려는 업무 하나를 놓고 아래 분리 신호 네 가지를 차례로 대입해 보고, 신호가 뚜렷하면 역할마다 에이전트를 나누며 그렇지 않으면 에이전트 하나로 시작합니다.

에이전트를 몇 개로 시작할지는 기술 담당자보다 업무를 아는 의사결정권자가 먼저 판정할 수 있는 문제입니다. 판정에 필요한 정보가 에이전트 제품의 기능보다 업무의 성격, 곧 누가 무엇을 보고 누가 결과를 확인하는지에 있기 때문입니다. 나눌 신호가 뚜렷한 업무는 처음부터 역할마다 에이전트를 두고, 신호가 약하거나 업무끼리 맥락을 많이 공유하는 경우에는 한 에이전트로 시작해 필요할 때 늘립니다. 아래 두 항목은 그 판정에 쓸 점검표와 판단표입니다.

2.3.1 역할이 둘 이상이고 비밀 정보 범위가 다를 때의 분리 신호

에이전트를 나눌지 판단할 때는 기술 사양보다 업무를 둘러싼 사람과 정보의 범위를 먼저 확인합니다. 다음 네 가지 신호는 독자가 자기 조직의 업무 하나를 놓고 차례로 대입해 볼 수 있도록 만든 점검표입니다.

분리 신호	확인 질문	예를 들면
역할이 둘 이상이다	이 에이전트에 맡기려는 일이 서로 다른 부서·직무에 속하는가	입찰 공고 정리와 월 손익 정리
비밀 정보 범위가 다르다	업무마다 접속하는 시스템과 볼 수 있는 자료가 다른가	영업 고객 자료와 재무 시스템 접속 정보
결과를 확인하는 사람이 다르다	각 업무의 결과를 검토하고 책임지는 사람이 다른가	영업팀장과 재무팀장
부르는 사람과 창구가 다르다	업무마다 에이전트를 부르는 사람과 메신저가 다른가	영업 단체방과 재무 담당자 개인 메신저

네 신호 가운데 둘 이상에 해당하면 역할마다 에이전트를 나누는 편이 관리하기 쉽습니다. 특히 둘째 신호인 비밀 정보 범위가 다르다는 항목은 하나만 해당해도 나눌 이유가 되는데, 2.1.2의 예처럼 권한 섞임은 업무를 더하는 순간 그 에이전트를 부르는 모든 사람에게 번지기 때문입니다. 공식 문서가 드는 쓰임새도 이 신호와 맞닿아 있습니다. 목적별로 코딩 도우미와 조사 담당을 나누는 경우 외에, 같은 설정을 시험용과 운영용으로 따로 두거나 가족 구성원마다 또는 슬랙 작업 공간마다 에이전트를 하나씩 두는 쓰임새가 함께 실려 있습니다[S1][S6]. 이 점검표는 8장에서 「업무 하나 = 프로파일 하나」로 시범 에이전트 팀을 설계할 때 그대로 판단 근거로 씁니다.

기술 조직이라면 역할을 이렇게 나눠 볼 수 있습니다. 외부 자료를 찾아 정리하는 조사 담당, 서버 상태를 점검하고 장애 상황을 요약하는 운영 점검 담당, 회의와 작업 결과를 기록으로 남기는 정리 담당, 코드와 문서의 품질을

살피는 검토 담당입니다. 네 역할은 볼 자료와 접속할 시스템, 결과를 확인할 사람이 모두 달라 위 분리 신호에 그대로 해당하고, 역할마다 필요한 권한만 주고 기억과 익힌 기술을 따로 두면 서로의 일이 섞이지 않습니다. 역할 사이에 일을 넘길 때는 각자의 기억을 함께 쓰는 대신 넘길 내용을 메시지나 일감으로 분명히 적어 보내는 방식을 씁니다(6장).

2.3.2 같은 맥락을 모두 공유해야 하는 업무와 가장 단순한 구성에서 시작하는 원칙

모든 업무가 멀티에이전트 방식에 맞는 것은 아닙니다. Anthropic은 모든 에이전트가 같은 맥락을 공유해야 하거나 에이전트끼리 서로 기다리고 주고받을 일이 많은 업무에는 아직 멀티에이전트 방식이 잘 맞지 않는다고 밝히고, 그 예로 동시에 나눠 처리할 부분이 적은 코드 작성 업무를 듭니다[S8]. 이런 업무를 억지로 나누면 에이전트끼리 맥락을 전달하는 일이 늘어나 사용량만 커지고, 나눈 이점은 거의 남지 않습니다. 한 사람이 처음부터 끝까지 흐름을 쥐고 있어야 하는 업무는 한 에이전트에 맡기는 것이 기본입니다.

같은 이유로 처음 구성은 가장 단순한 형태에서 시작합니다. Anthropic이 2024년 12월 공개한 에이전트 설계 지침은 가장 단순한 해법을 먼저 찾고, 복잡도는 필요가 확인될 때만 늘리라고 권합니다[S7]. 에이전트 하나로 시작해 위의 분리 신호가 실제로 나타날 때 역할을 하나씩 떼어 내면, 나눈 이유가 업무 기록으로 남기 때문에 이후 에이전트 수를 늘리거나 줄이는 판단도 근거를 갖고 할 수 있습니다.

판단 항목	에이전트 팀이 맞는 경우	한 에이전트로 충분한 경우
역할 수	서로 다른 부서·직무의 일이 둘 이상	한 직무 안의 일
비밀 정보 범위	업무마다 접속 시스템과 자료가 다름	모든 업무가 같은 자료를 봄
결과 확인자	업무마다 검토·책임자가 다름	한 사람이 모든 결과를 확인
업무 사이의 연결	각자 끝낸 결과만 넘기면 됨	모든 단계가 같은 맥락을 계속 공유함
일의 크기	큰 조사를 여럿이 동시에 나눠 처리할 수 있음	한 흐름으로 처리하는 편이 빠름

기억할 것

- 에이전트 하나에 모든 업무를 맡기면 기억과 권한이 함께 섞이고, 업무를 더하는 결정은 곧 권한을 넓히는 결정입니다.
- 멀티에이전트 방식은 역할마다 기억·비밀 정보·부르는 창구를 나눠 주는 대신 AI 사용량이 늘어나므로, 업무 가치와 사용량을 함께 견뎌줍니다.
- 비밀 정보 범위·결과 확인자가 다른 업무는 나누고, 같은 맥락을 계속 공유하는 업무는 한 에이전트로 시작합니다.

8장으로 가져갈 질문 우리 조직이 고른 업무들은 역할마다 볼 수 있는 자료와 비밀 정보의 범위가 다른가?

2.4 역할 나누기를 프로파일 단위로 정리한 오픈소스 Hermes Agent

Hermes Agent는 Nous Research가 공개한 오픈소스 AI 에이전트로, 지금까지 살펴본 역할 나누기를 프로파일이라는 단위로 제품 안에 정리해 두었습니다. 공식 문서는 프로파일, 에이전트, 서브에이전트, 메신저 봇, Bot

Mode 봇을 서로 다른 용어로 정의하고, 역할마다 프로파일을 따로 두어 에이전트 여럿을 함께 운영하는 방법을 안내합니다[S1]. 따라서 앞에서 다룬 칸막이 세 가지와 일 나누기가 실제 제품에서 어떤 단위로 나뉘는지 확인하기에 알맞은 기준 사례입니다. 이 백서는 3장부터 Hermes Agent의 용어를 하나씩 열어 회사 조직에 빚대어 설명합니다.

Hermes Agent를 사내에 설치한 AI 모델과 함께 들어올 때의 준비 과정은 공개된 도입 가이드[R4]에서 따로 다룹니다. 이 백서는 설치 절차보다 프로파일과 에이전트, 그리고 에이전트를 부르는 창구의 구분에 집중합니다.

2.4.1 공식 문서가 구분한 다섯 용어와 회사 비유의 대응

Hermes Agent 공식 문서는 「프로파일은 어시스턴트의 설정과 데이터가 계속 남는 보관 단위이고, 에이전트는 그 설정으로 지금 실행 중인 어시스턴트」라고 구분합니다[S1]. 이 구분을 회사에 옮기면 프로파일은 직원의 자리와 기록, 에이전트는 그 프로파일의 설정으로 지금 일하는 직원이 됩니다. 여기에 직원이 잠깐 부르는 도우미인 서브에이전트, 직원을 부르는 두 가지 창구인 메신저 봇과 Bot Mode 봇, 부서가 함께 보는 업무 게시판을 더하면 3장부터 6장까지 다룰 구조가 한 장의 표에 들어옵니다.

공식 용어	회사 비유	하는 일	다루는 장
프로파일(Profile)	직원의 자리와 기록	설정·비밀 정보·성격·기억·대화 기록·스킬·예약 작업을 계속 보관함	3장
에이전트(Agent)	지금 일하는 직원	프로파일의 설정으로 실행되어 대화 한 건, 예약 작업 한 건을 처리함	4장
서브에이전트(Subagent)	잠깐 부르는 도우미	맡은 일을 새 대화로 시작해 처리하고 결과만 돌려줌. 에이전트 하나당 동시에 기본 최대 10개	4장
메신저 봇(Messaging bot)	사내 메신저로 부르는 창구	텔레그램·디스코드·슬랙의 계정 하나가 프로파일 하나에 연결됨	5장
Bot Mode 봇(Bot Mode bot)	데스크톱 명단으로 부르는 창구	데스크톱 앱의 Bot Mode 명단에 이름으로 오른 프로파일	5장
업무 게시판(Kanban)	부서가 함께 보는 업무 게시판	모든 프로파일이 함께 쓰는 일감 게시판으로, 일을 넘길 때마다 기록이 남음	6장

표 출처: Hermes Agent 공식 문서[S1][S3][S4][S5][S6]

표에서 눈여겨볼 관계는 두 가지입니다. 첫째, 프로파일 하나에서 대화마다·예약 작업마다 에이전트가 따로 실행되므로 프로파일 하나에 에이전트 여럿이 속합니다(4장). 둘째, Bot Mode 봇은 모두 프로파일이지만 모든 프로파일이 Bot Mode 봇은 아니며, 메신저 봇만 연결해 쓰는 프로파일도 있습니다[S1][S5]. 이 두 관계를 처음

부터 구분해 두면 「에이전트가 몇 개인가」와 「메신저 봇과 Bot Mode 봇이 몇 개인가」라는 질문에 서로 다른 답이 나오는 이유를 설명할 수 있습니다.

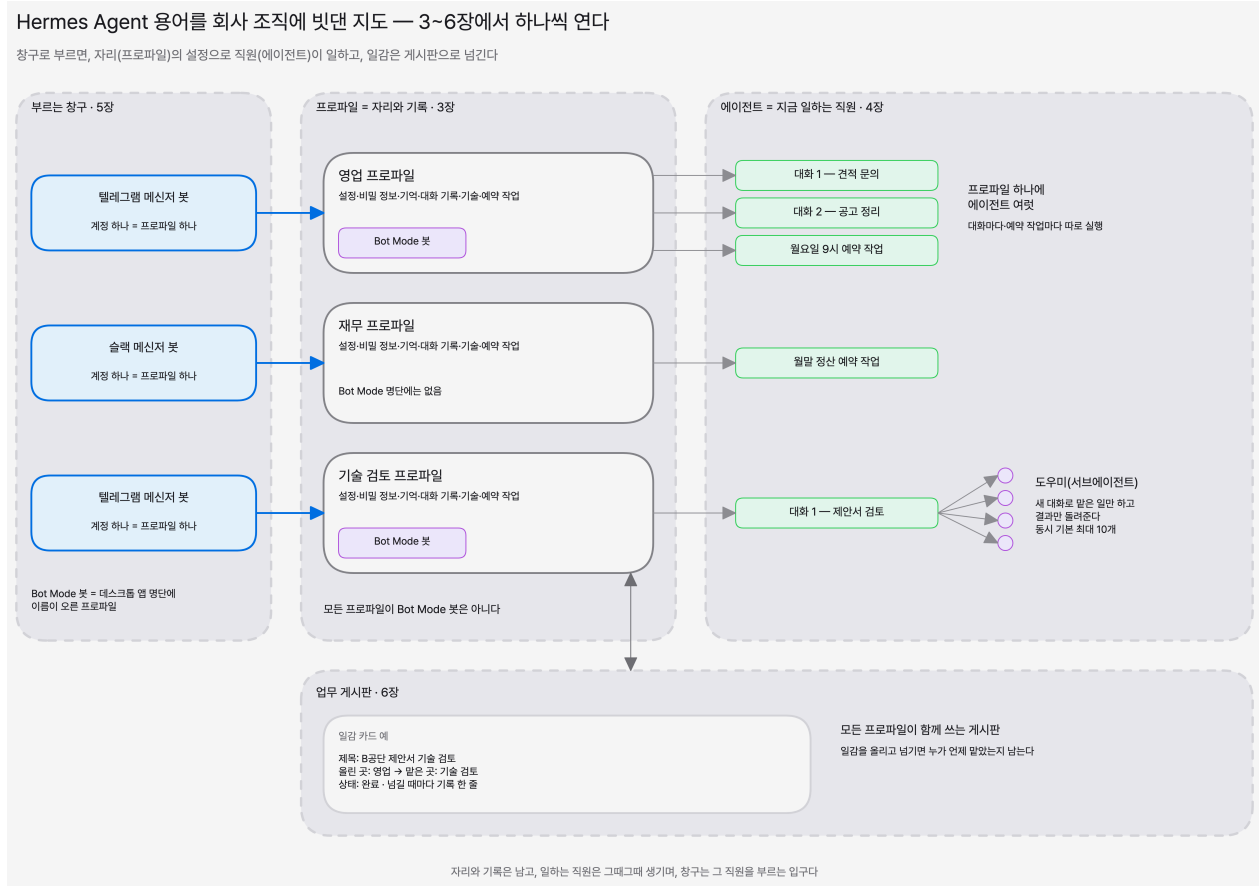


그림. Hermes Agent 용어를 회사 조직에 빗댄 전체 그림 — 프로파일, 지금 일하는 직원, 도우미, 부르는 창구, 업무 게시판

2.4.2 기준 버전 v0.21.0 과 최신 버전 기능의 구분 표기

이 백서의 수치와 동작 설명은 2026년 8월 31일 공개된 Hermes Agent v0.21.0과, 2026년 10월 기준 공식 문서 최신판을 기준으로 합니다[S1][S2][S3]. 서버에이전트 최대 10개처럼 기본값으로 소개하는 수치는 v0.21.0의 기본값이며 설정으로 바꿀 수 있습니다[S4]. 메신저 봇 복제 옵션처럼 최신 문서에만 실린 기능은 본문에서 「최신 버전 기능」으로 밝히고, 업무 게시판과 Bot Mode는 「최근 버전에서 제공」하는 기능으로 표기합니다[S3][S5]. 시범 도입 때 설치한 버전에 따라 일부 기능의 유무나 이름이 다를 수 있으므로, 도입 검토 목록에는 기준으로 삼을 버전을 함께 적어 두는 편이 안전합니다.

2.4.3 업무 역할 11개를 프로파일 11개로 나눈 운영 사례의 규모

역할 나누기가 실제 조직에서 어느 규모로 쓰이는지는 운영 사례로 확인할 수 있습니다. 한 IT 서비스 기업은 영업, 기술 검토, 재무, 인사처럼 부서 업무에 대응하는 업무 역할 11개를 Hermes Agent 프로파일 11개로 나누고, 역할마다 메신저 봇을 하나씩 연결해 대부분 상시 운영하고 있습니다. 이때 같은 프로파일 안에서도 메신저 대화 한 건, 예약 작업 한 건마다 에이전트가 따로 실행되고, 에이전트 하나는 큰 일을 맡으면 도우미를 기본 최대 10개까지 동시에 부릅니다[S4]. 결국 「일하는 AI」의 수는 역할 수에 역할마다 동시에 처리하는 일의 수를 곱한 만큼 늘어나므로, 에이전트 개수로는 조직의 규모를 셀 수 없고 세는 단위가 따로 필요합니다.

 데이터 업무 역할 11개 = 프로파일 11개 · 역할마다 메신저 봇 1개 · 대부분 상시 운영 · 에이전트 하나당
도우미 기본 최대 10개(v0.21.0 기본값, 설정으로 변경 가능)[S4]

Hermes Agent가 그 단위로 쓰는 것이 프로파일이며, 직원의 업무 기록과 설정을 함께 보관하는 이 단위에 무엇이 담기고 왜 역할마다 따로 두는지가 3장의 주제입니다. 운영 사례의 역할 구성과 역할끼리 일을 넘기는 방식은 업무 게시판과 함께 구성도로 다시 정리합니다(6장).

3장. 에이전트의 자리와 기록을 담는 프로파일

2장 끝에서 에이전트 개수 대신 조직의 규모를 세는 단위가 따로 필요하다고 했는데, Hermes Agent에서 그 단위가 프로파일입니다. Hermes Agent는 에이전트 한 명이 일하는 데 필요한 설정과 데이터를 프로파일(profile)이라는 단위로 묶어 보관합니다[S1]. 프로파일 하나에는 그 에이전트의 성격, 쓸 AI 모델, 익힌 기술, 비밀 정보, 기억, 대화 기록, 예약 작업, 메신저 계정 등이 함께 들어 있고, 대화가 끝나거나 프로그램을 다시 시작해도 이 내용은 그대로 남습니다. 에이전트 여럿을 한 팀으로 운영할 때 가장 먼저 정해야 하는 것이 바로 이 단위인데, 역할을 어디에서 나누느냐에 따라 어떤 기억과 비밀 정보가 서로 섞이지 않는지가 정해지기 때문입니다. 「업무 하나 = 프로파일 하나」라는 시범 도입의 설계 단위도 프로파일에 무엇이 담기는지를 알아야 판단할 수 있습니다. 이 장의 결론은 두 가지입니다. 프로파일은 역할별로 기억과 비밀 정보를 나누어 정리하는 칸막이 역할을 하고, 같은 서버 안의 파일 접근까지 막는 금고 역할은 하지 않습니다.

한 줄 요약 프로파일은 에이전트 한 명의 자리와 기록이고, 에이전트가 일을 마쳐도 그대로 남습니다.

3.1 사원증과 업무 노트처럼 대화가 끝나도 남는 프로파일의 정의

Hermes Agent 공식 문서는 「저장되는 것」과 「지금 실행 중인 것」을 서로 다른 이름으로 부릅니다. 저장되는 쪽이 프로파일이고 실행 중인 쪽이 에이전트이며, 에이전트는 프로파일에 담긴 설정과 기록을 읽어서 일합니다[S1]. 이 구분이 서야 「에이전트를 몇 개 두었는가」와 「지금 몇 건을 처리하는가」라는 두 질문에 각각 답할 수 있으므로, 도입 규모를 계산할 때도 이 정의가 출발점이 됩니다.

3.1.1 설정과 데이터가 계속 남는 자리라는 공식 정의와 회사 비유

공식 문서가 정한 프로파일과 에이전트의 정의

공식 문서에서 프로파일은 어시스턴트의 설정과 데이터가 계속 보관되는 단위로, 에이전트는 그 설정과 상태를 가지고 지금 실행되는 어시스턴트로 정의됩니다[S1]. 프로파일은 대화가 끝나도 남고, 에이전트는 대화 한 건이나 예약 작업 한 건이 진행되는 동안에만 존재합니다. 예를 들어 같은 프로파일로 어제 대화한 에이전트와 오늘 대화하는 에이전트는 실행으로 보면 서로 다른 에이전트이지만, 같은 기억과 같은 대화 기록을 읽기 때문에 사용자에게는 같은 동료로 보입니다. 「어제 한 이야기를 기억하는 AI 동료」라는 경험을 만드는 주체는 프로파일입니다.

사원증·책상·업무 노트·출입 카드로 본 프로파일

쉬운 비유 회사에서 직원 한 명에게 주어지는 사원증, 책상, 업무 노트, 출입 카드를 한데 모은 것이 프로파일입니다. 근무 시간이 끝나도 책상과 업무 노트는 그대로 남아 있고, 다음 근무에서는 그 노트를 근거로 전날 업무가 이어집니다.

이 비유에서 사원증은 그 직원이 어떤 역할을 맡은 누구인지를 나타내므로 프로파일의 성격에 해당합니다. 업무 노트는 기억과 대화 기록에, 출입 카드는 업무 시스템에 들어가는 비밀 정보에 대응합니다. 지금 책상에서 일하는 직원 본인은 에이전트에 해당하며, 맡은 일이 끝나면 책상을 떠납니다. 그래서 이 문서는 프로파일을 「자리와 기록」, 에이전트를 「지금 일하는 직원」으로 부르고, 두 낱말을 끝까지 같은 뜻으로 씁니다.

프로파일은 책상과 그 위의 기록, 에이전트는 그 책상에 앉은 직원

직원이 일을 마치고 자리를 떠나도 책상 위 다섯 가지는 남고, 다음 근무는 그 기록에서 이어집니다

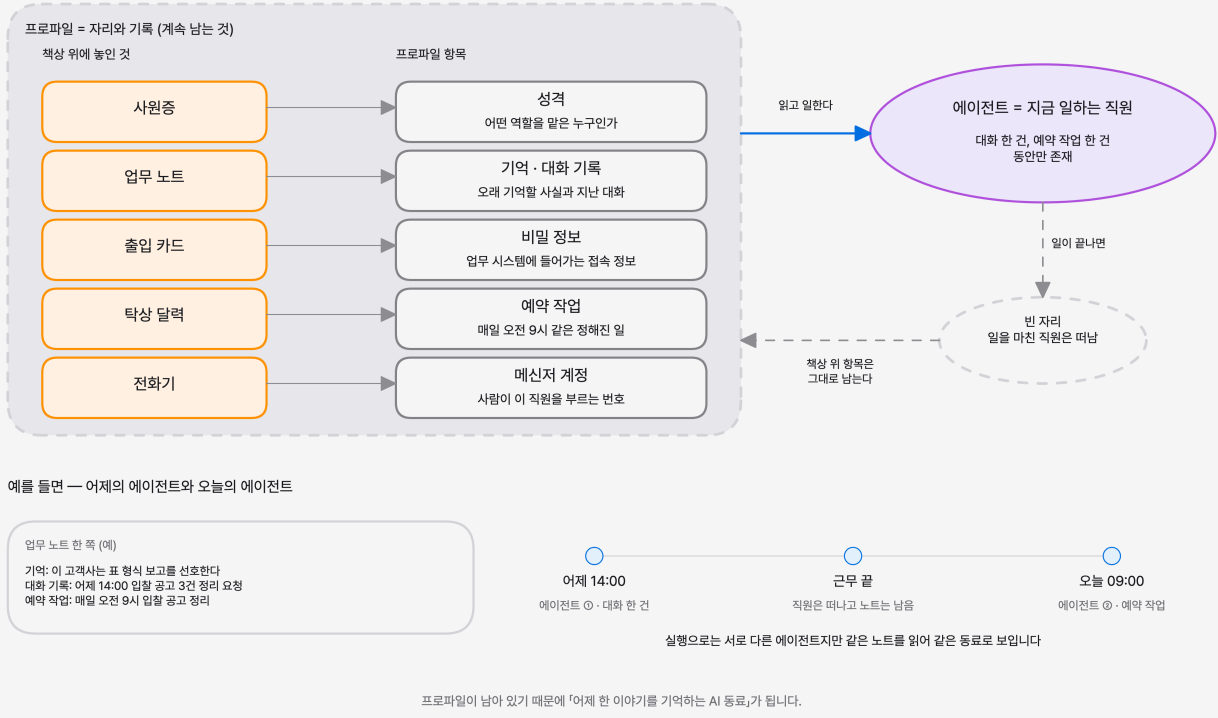


그림. 사원증·책상·업무 노트·출입 카드로 본 프로파일(자리와 기록)과 에이전트(지금 일하는 직원)

3.1.2 「영업 담당」 프로파일 하나를 열어 본 예

예를 들면 1장에서 입찰 공고 정리를 맡긴 에이전트를 「영업 담당」 프로파일로 만든다고 가정합니다. 이 프로파일 하나에 영업 업무에 필요한 여덟 가지가 모두 들어갑니다.

「영업 담당」 프로파일에 들어가는 여덟 가지 내용

「영업 담당」 프로파일을 열어 보면 다음 여덟 가지가 한곳에 모여 있습니다.

- 성격: 「공공 입찰 공고를 정리하고 영업 대표에게 보고하는 영업 지원 담당」이라는 역할 설명
- 쓸 AI 모델: 이 역할이 쓸 외부 AI 서비스 또는 사내 모델 하나
- 익힌 기술(스킬): 입찰 공고를 찾아 표로 정리하는 방법을 적은 문서
- 비밀 정보: 고객 관리 시스템 접속 정보
- 기억: 주력 고객사와 선호하는 보고 형식처럼 오래 기억할 사실
- 대화 기록: 지난 영업 관련 대화 전체
- 예약 작업: 매일 오전 9시 입찰 공고 정리
- 메신저 계정: 「영업봇」이라는 이름의 메신저 봇 계정

이 여덟 가지는 모두 영업 업무에만 쓰이고, 재무나 인사 업무의 정보는 하나도 들어 있지 않습니다. 프로파일을 열어 보면 그 에이전트가 무슨 일을 하고 어떤 시스템에 들어갈 수 있으며 무엇을 기억하는지가 한눈에 드러납니다. 다만 프로파일 안에 「에이전트」라는 항목은 따로 없습니다. 에이전트는 오전 9시 예약 작업이 시작되거나 누군가 「영업봇」에게 메시지를 보낼 때마다 이 여덟 가지를 읽어 실행되고, 일이 끝나면 사라지기 때문입니다(4

장). 시범 도입을 설계할 때 종이에 채울 칸도 이 여덟 칸이며, 8장의 설계표는 이 카드 한 장을 업무마다 한 줄씩 늘어놓은 모양이 됩니다.

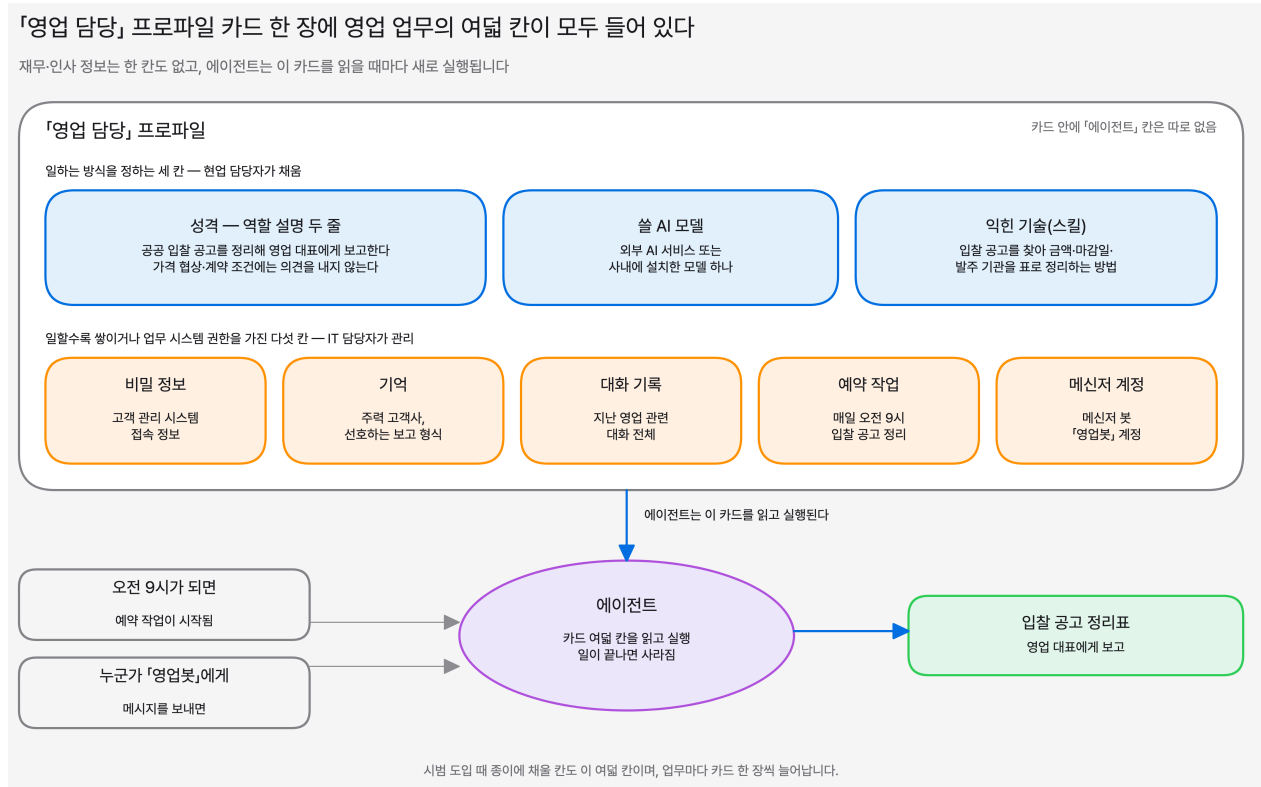


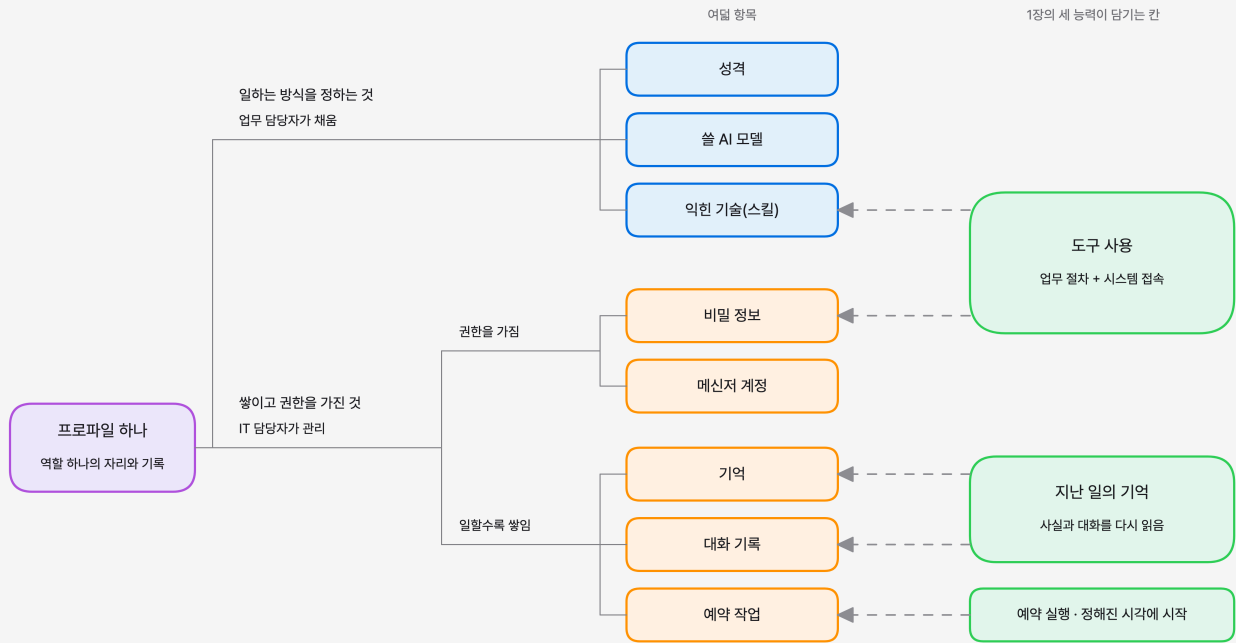
그림. 「영업 담당」 프로파일 카드 — 여덟 칸에 담긴 영업 업무의 설정과 데이터

3.2 프로파일 한 개에 담기는 여덟 가지 항목

Hermes Agent 공식 문서는 프로파일마다 설정, 비밀 정보, 성격, 기억, 대화 기록, 스킬, 예약 작업, 상태 저장소를 따로 가진다고 밝히고[S1], 메신저 봇 계정도 프로파일마다 따로 연결하도록 정합니다[S6]. 이 문서는 이 내용을 업무 담당자가 알아보기 쉽게 성격, 쓸 AI 모델, 익힌 기술(스킬), 비밀 정보, 기억, 대화 기록, 예약 작업, 메신저 계정의 여덟 항목으로 다시 묶었습니다. 쓸 AI 모델은 설정 안에 들어 있는 항목이고, 상태 저장소는 대화 기록을 담은 저장소라 대화 기록 항목에 포함됩니다. 이 여덟 항목은 성격이 두 갈래로 나뉩니다. 성격·AI 모델·스킬은 에이전트가 일하는 방식을 정하는 항목이라 업무 담당자가 내용을 채울 수 있고, 나머지 다섯은 일할수록 쌓이거나 업무 시스템 권한을 가진 항목이라 IT 담당자가 관리 책임을 져야 합니다. 1장에서 본 에이전트의 세 능력도 이 구분에 맞춰 들어갑니다. 도구 사용은 스킬과 비밀 정보에, 예약 실행은 예약 작업에, 지난 일의 기억은 기억과 대화 기록에 담깁니다.

프로파일 한 개의 여덟 항목은 두 갈래로 나뉜다

일하는 방식을 정하는 세 칸은 업무 담당자가 채움, 쌓이고 권한을 가진 다섯 칸은 IT 담당자가 맡습니다



여덟 항목으로 다시 묶은 근거

공식 문서의 항목: 설정 · 비밀 정보 · 성격 · 기억 · 대화 기록 · 스킬 · 예약 작업 · 상태 저장소 + 프로파일마다 연결하는 메신저 봇 계정
이 문서의 여덟 항목으로: 쓸 AI 모델은 설정 안의 항목, 상태 저장소는 대화 기록을 담는 곳이라 대화 기록에 포함

옮기거나 나눠 줄 때 먼저 점검할 대상은 아랫갈래 다섯 칸입니다.

그림. 프로파일 한 개에 담기는 여덟 항목 — 일하는 방식을 정하는 세 칸과 쌓이고 권한을 가진 다섯 칸

3.2.1 일하는 방식을 정하는 성격·AI 모델·익힌 기술(스킬)

에이전트의 성격을 정하는 역할 설명 두 줄

성격은 「이 에이전트는 무슨 일을 하는 누구인가」를 적은 글입니다. 에이전트는 대화를 시작할 때마다 이 글을 먼저 읽기 때문에, 성격에 적힌 역할과 업무 범위가 답의 말투와 판단 기준을 함께 정합니다. 예를 들어 「영업 담당」의 성격에 「공공 입찰 공고를 정리하고, 가격 협상이나 계약 조건에는 의견을 내지 않는다」라고 두 줄만 적어도 에이전트가 말을 일과 말지 않을 일이 분명해집니다. 데스크톱의 Bot Mode 화면에서도 Bot Mode 봇마다 역할, 모델, 기억, 스킬을 각자 따로 가지도록 되어 있어[S5], 성격은 어느 창구로 부르든 같은 에이전트를 같은 사람처럼 보이게 하는 기준이 됩니다. 따라서 성격은 IT 담당자보다 그 업무를 잘 아는 현업 담당자가 쓰는 편이 정확하며, 8장 설계표의 「역할 설명 두 줄」 칸이 바로 이 항목입니다.

프로파일마다 따로 정하는 쓸 AI 모델

쓸 AI 모델은 프로파일마다 다르게 정할 수 있습니다. 영업 자료 요약처럼 외부로 나가도 문제가 적은 업무는 외부 AI 서비스를 쓰고, 재무 수치처럼 바깥으로 보내기 어려운 자료를 다루는 업무는 사내에 설치한 모델을 쓰도록 프로파일 단위로 나눌 수 있습니다. 모델 선택은 성능과 함께 비용과 자료 반출 범위까지 정하는 결정이며, 그 결정을 역할마다 따로 내릴 수 있다는 점이 프로파일을 나누는 이점 가운데 하나입니다. 다만 모델을 바꾸면 같은 성격과 같은 스킬로도 결과물의 품질이 달라질 수 있으므로, 바꾸기 전에 시험용 프로파일에서 먼저 써 보는 방식을 권합니다(3.3.2).

일하는 방법을 문서로 적은 익힌 기술(스킬)

익힌 기술(스킬)은 특정 업무를 처리하는 방법을 순서대로 적은 문서입니다. 「입찰 공고 사이트에서 이번 주 공고를 찾고, 금액·마감일·발주 기관을 표로 정리한 뒤 영업 대표에게 보낸다」 같은 절차가 스킬 하나가 됩니다. 에이전트는 요청을 받으면 프로파일에 있는 스킬 가운데 맞는 것을 골라 그 순서대로 일하므로, 같은 요청에 매번 다른 방식으로 답하는 일이 줄어듭니다. 스킬은 신입 직원에게 건네는 업무 매뉴얼과 같은 역할을 하고, 현업 담당자가 지금 손으로 하는 절차를 그대로 적어 넣는 것으로 시작할 수 있습니다.

스킬이 쌓이면 같은 설명을 매번 되풀이하지 않아도 됩니다. 업무 절차를 한 번 스킬로 남겨 두면 다음 요청부터는 그 절차를 다시 말로 풀어 줄 필요 없이 에이전트가 해당 문서를 스스로 찾아 읽습니다. 절차가 담당자의 머릿속이 아니라 문서에 남으므로 담당자가 바뀌어도 같은 방식으로 일이 처리되고, 따로 만들던 인수인계 자료도 스킬을 다듬는 작업으로 합쳐집니다. 한 번 알려 준 절차를 다음 실행에서도 그대로 쓰는 이 능력은 기업이 에이전트를 고를 때 먼저 확인하는 항목 가운데 하나이며, 도입 전에 점검할 에이전트 기능 여덟 가지를 정리한 공개 글 [R5]에서도 다룹니다.

3.2.2 쌓이고 쥐는 것 — 비밀 정보·기억·대화 기록·예약 작업·메신저 계정

업무 시스템 권한을 가진 비밀 정보와 메신저 계정

비밀 정보는 에이전트가 업무 시스템에 들어갈 때 쓰는 접속 키와 비밀번호입니다. 「영업 담당」 프로파일이 고객 관리 시스템 접속 정보를 가지고 있다면, 그 프로파일로 실행되는 에이전트는 모두 고객 관리 시스템에 들어갈 수 있습니다. 메신저 계정도 같은 성격의 항목입니다. 메신저 봇 계정 하나는 프로파일 하나에서만 쓸 수 있고 같은 계정을 두 프로파일이 동시에 쓰지 못하므로[S6], 「영업봇」에게 메시지를 보낸 사람은 언제나 「영업 담당」 프로파일의 에이전트와 대화하게 됩니다. 이 두 항목은 누가 어떤 시스템에 접근하고 누가 그 에이전트를 부를 수 있는지를 정하는 권한 항목이며, IT 담당자가 발급과 회수를 관리해야 합니다.

일할수록 쌓이는 기억·대화 기록·예약 작업

기억, 대화 기록, 예약 작업은 에이전트가 일할수록 양이 늘어나는 항목입니다. 기억에는 「이 고객사는 표 형식 보고를 선호한다」 같은 사실이 쌓이고, 대화 기록에는 지난 대화가 그대로 남으며, 예약 작업은 정해진 시각에 에이전트를 실행시키는 일정표 역할을 합니다. 데스크톱의 Bot Mode 화면도 이 기록을 보여 주지만 하고 따로 보관하지 않으므로, Bot Mode를 꺼도 프로파일과 대화 기록, 예약 작업은 그대로 남습니다[S5]. 이 다섯 항목이 프로파일의 실제 무게이고, 영업 에이전트를 몇 달 운영하면 그 시간만큼의 고객 정보가 대화 기록과 기억에 쌓입니다.

여덟 항목을 누가 채우고 어떤 항목을 옮길 때 점검해야 하는지는 다음과 같습니다.

항목	하는 일	주로 채우는 사람	옮기거나 나눠 줄 때 점검
성격	역할과 업무 범위를 정함	현업 담당자	내용 확인
쓸 AI 모델	답을 만드는 모델 지정	IT 담당자	받는 쪽 사용 가능 여부
익힌 기술(스킬)	업무 절차를 문서로 보관	현업 담당자	내용 확인
비밀 정보	업무 시스템 접속	IT 담당자	반드시 점검
기억	오래 기억할 사실 보관	에이전트가 쌓음	반드시 점검

항목	하는 일	주로 채우는 사람	옮기거나 나눠 줄 때 점검
대화 기록	지난 대화 보관	에이전트가 쌓음	반드시 점검
예약 작업	정해진 시각에 실행	현업 담당자·IT 담당자	실행 시각과 대상 확인
메신저 계정	에이전트를 부르는 창구	IT 담당자	새로 연결

표 출처: [S1][S2][S6]을 바탕으로 정리

배포판 업데이트에서도 보존되는 기억과 비밀 정보

아랫줄 다섯 항목은 에이전트를 다른 서버로 옮기거나 다른 팀에 나눠 줄 때 가장 먼저 점검해야 하는 대상입니다. 예를 들어 Hermes Agent의 배포판은 성격·스킬·예약 작업·설정을 묶어 여러 곳에 나눠 주는 방식인데, 배포판을 업데이트해도 받는 쪽의 기억, 대화 기록, 비밀 정보, 로그는 건드리지 않도록 되어 있습니다[S2]. 반면 프로파일을 통째로 찍어 낸 내보내기 파일에는 기억과 대화 기록이 들어갈 수 있으므로[S2], 어느 방식으로 옮기느냐에 따라 이 다섯 항목이 함께 넘어가는지가 달라집니다. 이 차이와 점검 순서는 7장 「내보내기 비밀 정보」에서 다시 다룹니다.

3.3 역할마다 프로파일을 따로 두는 칸막이 — 설정을 서로 물려받지 않는 독립 단위

Hermes Agent의 프로파일은 서로 독립된 단위입니다. 프로파일마다 비밀 정보, 기억, 대화 기록, 예약 작업, 메신저 계정을 따로 가지고, 새 프로파일은 기존 프로파일의 설정을 자동으로 물려받지 않습니다[S1]. 2장에서 말한 「섞이지 않게 나눈다」는 원칙은 Hermes Agent에서 프로파일 단위로 이뤄지며, 공식 문서도 목적별·사용자별·단계별로 프로파일을 나누는 쓰임새를 예로 듭니다[S1][S6].

3.3.1 영업 프로파일의 기억과 재무 프로파일의 비밀 정보가 서로 보이지 않는 구조

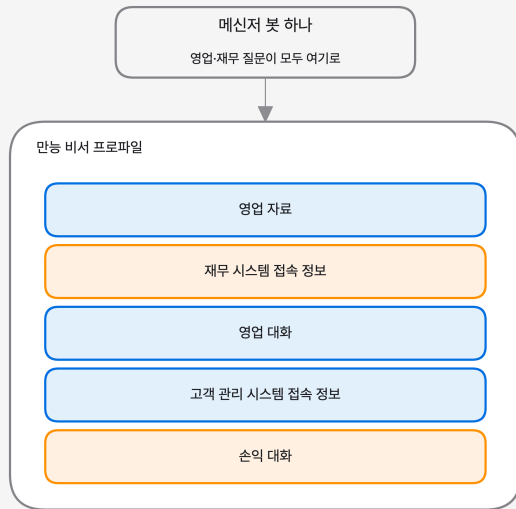
만능 비서 한 명에서 두 프로파일로 나눈 결과

2장의 예에서는 입찰 공고를 정리하던 에이전트 하나에게 이번 달 손익 정리까지 맡겼습니다. 그 구성에서는 영업 자료를 다루던 에이전트가 재무 시스템 접속 정보와 재무 대화 기록까지 한 프로파일에 함께 가지게 됩니다. 같은 일을 「영업 담당」과 「재무 담당」 두 프로파일로 나누면 고객 관리 시스템 접속 정보와 영업 대화는 「영업 담당」에만, 재무 시스템 접속 정보와 손익 대화는 「재무 담당」에만 남습니다. 따라서 「영업봇」에게 입찰 공고를 물었을 때 에이전트가 재무 대화를 근거로 엉뚱한 답을 하는 기억 섞임과, 영업 에이전트가 쓸 일 없는 재무 비밀 정보를 가지는 권한 섞임이 함께 줄어듭니다.

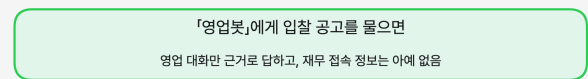
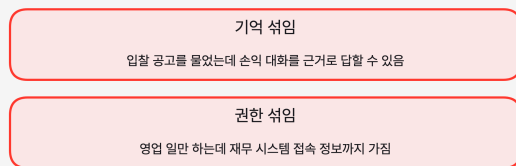
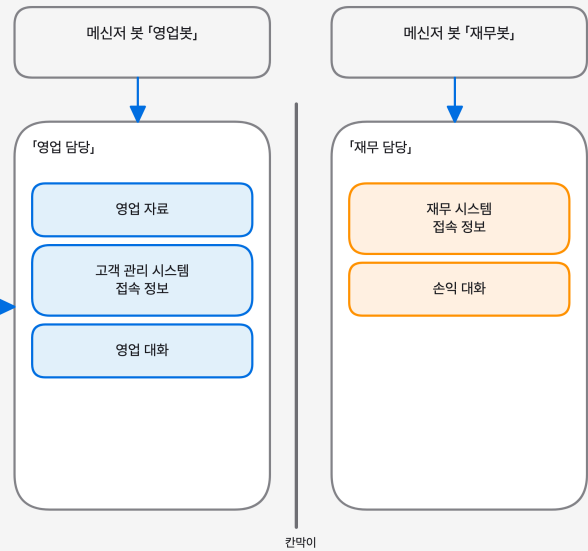
만능 비서 한 명을 「영업 담당」·「재무 담당」 두 프로파일로 나누면

같은 다섯 가지 정보가 역할별로 갈라져, 기억도 비밀 정보도 서로 섞이지 않습니다

나누기 전 — 프로파일 하나



나눈 뒤 — 역할마다 프로파일 하나



칸막이는 기억과 비밀 정보를 역할별로 정리하는 장치이며, 같은 서버 안의 파일 접근까지 막는 금고는 아닙니다

□ 영업 업무 정보 □ 재무 업무 정보

역할을 어디서 나누느냐가 어떤 기억과 비밀 정보가 섞이지 않는지를 정합니다.

그림. 만능 비서 한 명(프로파일 하나)과 「영업 담당」·「재무 담당」 두 프로파일의 비교

새 프로파일마다 설정을 다시 채우는 운영 부담

프로파일이 서로 설정을 물려받지 않는다는 성질에는 운영 부담도 따릅니다. 새 프로파일을 만들면 성격, AI 모델, 스킬, 비밀 정보를 그 프로파일에 맞게 다시 채워야 하고, 기존 프로파일을 바꿔도 다른 프로파일에는 반영되지 않습니다. 이 부담을 줄이도록 새 프로파일을 만들 때 기존 프로파일을 복제하는 선택지가 있는데, 기본 복제는 설정, 비밀 정보, 성격, 스킬, 정리된 기억을 복사하고 대화 기록은 복사하지 않습니다[S1]. 예약 작업도 복사하지 않는데, 복사하면 같은 작업이 두 프로파일에서 두 번 실행되기 때문입니다[S1]. 메신저 봇 계정은 별도로 지정하지 않으면 복제되지 않으며, 복제가 끝난 두 프로파일은 그때부터 서로 독립적으로 운영됩니다[S1]. 다만 복제는 비밀 정보까지 함께 옮기므로, 재무 프로파일을 본떠 영업 프로파일을 만들면 재무 접속 정보가 그대로 따라온다는 점을 IT 담당자가 확인해야 합니다.

3.3.2 목적별 분리와 시험용·운영용 분리 — 공식 문서가 든 프로파일 쓰임새

공식 문서가 든 프로파일 나누기 기준 네 가지

부서별로 나누는 것만이 프로파일을 나누는 기준은 아닙니다. 공식 문서는 한 사람이 코딩 도우미, 개인 비서, 조사 담당을 서로 다른 프로파일로 두는 목적별 분리를 대표 쓰임새로 듭니다[S1]. 가족 구성원마다 또는 슬랙 작업 공간마다 에이전트를 하나씩 두는 사용자별 분리와, 같은 설정을 시험용과 운영용으로 나누는 단계별 분리도 예로 듭니다[S6]. 각 기준이 무엇을 섞이지 않게 하는지는 다음과 같습니다.

나누는 기준	예	섞이지 않는 것
부서별	「영업 담당」과 「재무 담당」	업무 시스템 비밀 정보와 부서별 대화 기록
목적별	코딩 도우미·개인 비서·조사 담당	업무 성격에 맞춘 성격과 스킬
사용자별	구성원마다, 슬랙 작업 공간마다 하나	사람이나 팀마다 쌓이는 기억과 메신저 계정
단계별	같은 설정의 시험용과 운영용	시험 중 대화 기록과 실제 업무 기록

표 출처: [S1][S6]

시험용 프로파일에서 새 기능을 먼저 쓰는 운영 방식

시험용과 운영용을 나누는 방식은 의사결정권자가 특히 눈여겨볼 만한 쓰임새입니다. 새 스킬이나 다른 AI 모델을 운영 중인 「영업 담당」 프로파일에 바로 넣으면 그날부터 영업 대표가 받는 보고가 바뀌고, 결과가 나빠도 원래 상태로 되돌리기 어렵습니다. 반면 같은 설정을 복제한 「영업 담당 시험용」 프로파일을 따로 두면 새 기능을 거기서 먼저 써 보고, 결과를 확인한 뒤에 운영용에 반영할 수 있습니다[S6]. 이때 시험용 프로파일에는 운영용과 다른 메신저 봇 계정을 연결해야 하는데, 같은 메신저 봇 계정을 두 프로파일이 함께 쓰지 못하기 때문입니다[S6].

작은 수의 프로파일로 시작하는 원칙

프로파일을 나누는 기준이 여럿이라고 해서 처음부터 잘게 나눌 필요는 없습니다. 에이전트를 만들 때는 가장 단순한 구성에서 시작하고 필요할 때만 복잡도를 높이라는 것이 에이전트 설계의 일반 권고입니다[S7]. 프로파일 수가 늘어날수록 채우고 관리할 비밀 정보와 메신저 계정도 함께 늘어나므로, 시범 도입은 비밀 정보 범위가 확실히 다른 업무 몇 개만 골라 「업무 하나 = 프로파일 하나」로 시작하는 편이 관리하기 쉽습니다. 예를 들어 2.4.3의 운영 사례처럼 역할을 11개로 나눈 구성에서는 메신저 봇 계정과 비밀 정보도 11벌을 관리해야 합니다.

3.4 칸막이와 금고의 차이 — 프로파일이 보장하지 않는 운영 조건

Hermes Agent 공식 문서는 프로파일에 관해 두 가지를 분명히 경고합니다. 프로파일은 에이전트를 격리 공간(샌드박스)에 가두지 않는다는 점, 그리고 한 프로파일에 에이전트 프로그램 두 개를 동시에 연결하지 말라는 점입니다[S1]. 두 경고 모두 「프로파일을 나누면 보안 설계가 끝난다」는 오해와 닿아 있으므로, 서버와 계정 권한은 프로파일과 별도로 설계해야 합니다.

3.4.1 같은 서버의 파일 접근까지는 막지 않는 프로파일 칸막이의 범위

프로파일은 격리 공간(샌드박스)이 아니라는 공식 경고

프로파일은 기억과 비밀 정보를 역할별로 나누어 정리하는 칸막이 역할을 하지만, 서로 열 수 없게 잠그는 금고 역할은 하지 않습니다. 공식 문서에 따르면 기본 실행 방식에서 에이전트는 그 프로그램을 실행한 서버 사용자 계정과 같은 파일 접근 권한을 가지며, 프로파일은 에이전트가 자기 프로파일 밖의 폴더에 접근하는 것을 막지 않습니다[S1]. 「영업 담당」과 「재무 담당」이 같은 서버, 같은 사용자 계정으로 실행된다면 영업 에이전트가 파일을 직접 찾아 읽을 때 재무 프로파일의 비밀 정보에 접근할 수 있는 구조입니다. 또한 일부 외부 서비스 로그인(OAuth) 정보는 기본적으로 프로파일마다 따로 두지 않고 모든 프로파일이 공용 위치에서 함께 읽으며, 필요하

면 특정 프로파일에만 따로 로그인하도록 바꿀 수 있습니다[S1]. 프로파일 분리가 보장하는 것과 보장하지 않는 것을 나누어 보면 다음과 같습니다.

구분	프로파일로 나뉘는 것	프로파일로 막지 않는 것
기억과 대화 기록	에이전트가 평소 읽는 기억과 대화 기록은 자기 프로파일 것만	같은 서버 사용자 계정으로 다른 프로파일 파일을 직접 여는 접근
비밀 정보	프로파일마다 따로 보관	같은 서버에 있는 다른 프로파일의 비밀 정보 파일 접근
로그인 정보	—	일부 외부 서비스 로그인(OAuth) 정보는 모든 프로파일이 공용으로 읽음
메신저 계정	메신저 봇 계정 하나는 프로파일 하나에서만 사용	—
공유 업무	—	모든 프로파일이 함께 보는 업무 게시판(6장)은 의도된 공유

표 출처: [S1][S3][S6]

비밀 정보 범위가 크게 다른 역할의 서버·계정 분리 판단

위 표의 오른쪽 열은 프로파일 설정만으로는 해결되지 않습니다. 비밀 정보의 민감도가 크게 다른 역할, 예를 들어 영업 지원과 급여·재무 업무를 함께 운영할 때는 두 프로파일을 서로 다른 서버 사용자 계정이나 다른 서버에서 실행하는 결정을 따로 내려야 합니다. 반면 영업 지원과 마케팅처럼 다루는 비밀 정보의 수준이 비슷한 역할은 같은 서버에서 프로파일만 나누어도 운영상 충분한 경우가 많습니다. 프로파일은 기억 섞임과 권한 섞임을 줄이는 정리 단위이고, 누가 무엇을 열 수 있는지를 강제하는 보안 경계는 서버와 계정 설계가 맡습니다. 이 판단은 8장에서 업무 3개를 고를 때 「비밀 정보 보호 범위를 어디까지로 볼 것인가」라는 의사결정 질문으로 다시 이어집니다.

3.4.2 한 프로파일에 에이전트 프로그램 두 개를 동시에 연결하지 않는 규칙

같은 프로파일의 에이전트 프로그램 두 개가 기억을 어긋나게 만드는 이유

공식 문서는 같은 프로파일에 에이전트 프로그램 두 개를 동시에 연결하지 말라고 명시합니다[S1]. 두 프로그램은 각자 기억을 자동으로 기록하고, 대화를 시작할 때마다 상대가 기록한 내용까지 읽어 들입니다. 한쪽이 쓴 기억을 다른 쪽이 읽고 그 위에 다시 기록하는 일이 반복되고, 결국 프로파일의 기억이 처음 정한 설정과 다른 내용으로 바뀌어 갑니다[S1]. 예를 들어 「영업 담당」 프로파일을 서버 두 대에서 동시에 실행하면 같은 업무 노트를 두 사람이 동시에 고쳐 쓰는 상황과 같아집니다. 여러 에이전트가 기억을 함께 써야 한다면 프로파일을 공유하지 말고 공식 문서가 원하는 대로 외부 기억 저장 서비스를 따로 두어야 합니다[S1].

에이전트 프로그램 두 개와 프로파일 하나에 에이전트 여럿의 차이

이 규칙은 4장에서 다룰 「프로파일 하나에 에이전트 여럿」과 다른 이야기입니다. 에이전트 프로그램 두 개는 같은 프로파일을 대상으로 Hermes Agent를 두 번 실행한 상태를 말하며, 이 구성은 금지 대상입니다. 반면 프로파일 하나에 에이전트 여럿은 프로그램 하나 안에서 대화 한 건, 예약 작업 한 건마다 에이전트가 따로 실행되는 정상 동작입니다. 이 안에서 에이전트가 부르는 서브에이전트도 부모 에이전트의 AI 모델과 접속 키를 이어받아

같은 프로파일 안에서 일하고, 새 대화로 시작해 부모의 지난 대화 내용을 모릅니다[S4]. 따라서 「오전 9시 예약 작업과 메신저 질문을 동시에 처리하는 영업 에이전트 두 개」는 허용되는 구성이고, 「같은 영업 프로파일을 서버 두 대에서 동시에 실행하는 것」은 피해야 할 구성입니다.

기억할 것

- 프로파일은 에이전트 한 명의 설정과 데이터를 보관하는 단위이며, 성격·AI 모델·스킬·비밀 정보·기억·대화 기록·예약 작업·메신저 계정 여덟 가지를 담고 대화가 끝나도 남습니다.
- 프로파일은 서로 설정을 물려받지 않는 독립 단위라서 역할마다 기억과 비밀 정보가 섞이지 않지만, 같은 서버의 파일 접근까지 막는 금고 역할은 하지 않습니다.
- 한 프로파일에는 에이전트 프로그램을 하나만 연결하고, 비밀 정보 범위가 크게 다른 역할은 서버나 계정을 따로 나눕니다.

8장으로 가져갈 질문 업무마다 프로파일 하나를 둔다면 각 프로파일에 무엇을 넣고 무엇을 빼는가.

4장. 지금 일하는 직원인 에이전트와 그 에이전트가 부르는 도우미 서브에이전트

3장 끝에서 「프로파일 하나에 에이전트 여럿」은 정상 동작이고 「같은 프로파일을 두 곳에서 동시에 실행하는 것」은 피할 구성이라고 같았는데, 그 구분의 바탕이 되는 에이전트의 정의를 여기서 세웁니다. Hermes Agent 공식 문서는 에이전트를 「프로파일의 설정과 상태를 써서 지금 실행 중인 어시스턴트」로 정의합니다[S1]. 3장에서 다룬 프로파일이 대화가 끝나도 남는 자리와 기록이라면, 에이전트는 그 프로파일의 설정을 쓰며 지금 일하는 직원입니다. 같은 문서는 에이전트가 큰 일을 나눠 맡기려고 잠깐 부르는 도우미를 서브에이전트(subagent)라는 별도 용어로 구분하고, 도우미는 새 대화로 시작한다고 밝힙니다[S1].

두 용어를 구분해야 하는 이유는 「에이전트 몇 개를 운영하는가」라는 질문에 답이 두 개 나오기 때문입니다. 에이전트는 대화 한 건, 예약 작업 한 건, 업무 게시판 일감 한 건마다 하나씩 생기고 일이 끝나면 사라지므로, 같은 역할 하나가 오전에는 에이전트 세 개를 쓰고 오후에는 하나도 쓰지 않을 수 있습니다. 따라서 IT 담당자는 동시에 일하는 에이전트와 도우미의 수로 처리량과 AI 사용량을 가늠하고, 임원 보고에서는 저장되어 남는 프로파일의 수로 AI 동료의 규모를 세면 숫자가 서로 어긋나지 않습니다. 도우미는 Hermes Agent v0.21.0 기본값으로 동시에 최대 10개까지 부를 수 있고 이 값은 설정으로 바꿀 수 있습니다[S4].

한 줄 요약 에이전트는 프로파일의 자리와 기록을 쓰며 지금 일하는 직원이고, 일이 세 건 들어오면 같은 직원이 세 건을 따로 처리하며, 큰 일은 도우미 서브에이전트에게 나눠 맡깁니다.

4.1 대화 한 건, 예약 작업 한 건마다 실행되고 끝나면 사라지는 에이전트

Hermes Agent의 에이전트는 미리 만들어 두는 설정 항목이 아니며, 일이 들어오는 순간 프로파일 하나를 골라 그 설정으로 생기는 실행 중인 어시스턴트입니다[S1]. 일이 들어오는 경로는 메신저 대화, 정해진 시각의 예약 작업, 모든 프로파일이 함께 보는 업무 게시판의 일감 세 가지이며, 어느 경로든 일을 마치면 그 에이전트는 사라지고 대화 기록과 기억만 프로파일에 남습니다. 프로파일과 에이전트의 관계는 회사의 책상과 그 책상에서 지금 일하는 직원의 관계로 이해하면 정확합니다.

4.1.1 프로파일의 설정으로 지금 일하는 직원이라는 에이전트의 정의

책상 하나에서 일감마다 따로 일하는 직원이라는 에이전트 비유

쉬운 비유로 말하면 프로파일은 이름표가 붙은 책상과 서랍 속 업무 노트이고, 에이전트는 그 책상에 앉아 지금 일감 하나를 처리하는 직원입니다. 다만 사람과 다르게 이 직원은 일감이 셋이면 셋으로 나뉘어 각자 따로 일하며, 셋 모두 같은 책상의 성격 설정, 같은 AI 모델, 같은 업무 노트를 씁니다. 공식 문서는 프로파일을 「어시스턴트의 설정과 데이터가 계속 남는 자리」로, 에이전트를 「그 설정과 상태를 쓰는 실행 중인 어시스턴트」로 나누어 정의합니다[S1]. 성격·기억·비밀 정보처럼 오래 남는 것은 모두 프로파일 쪽에 있고, 에이전트는 그것을 빌려 쓰는 동안만 존재합니다.

AI 모델이 도구를 쓰며 다음 행동을 고르는 에이전트의 동작 방식

지금 일하는 직원이 하는 일은 1장에서 본 에이전트의 동작과 같습니다. Anthropic은 에이전트를 AI 모델이 일하는 순서와 쓸 도구를 스스로 정하고, 도구를 쓴 결과를 보며 다음 행동을 고르는 반복 구조로 설명합니다[S7].

예를 들어 입찰 공고를 정리하는 에이전트는 공고 사이트를 검색하고, 결과 파일을 읽고, 빠진 항목이 있으면 다시 검색한 뒤 표를 만들어 보냅니다. 검색 도구, 파일 도구, 메신저 연결 정보는 전부 프로파일에 설정된 것을 그대로 쓰므로, 같은 프로파일에서 생긴 에이전트는 몇 개든 같은 도구 묶음으로 일합니다.

대화·예약 작업·게시판 일감이라는 에이전트 생성 계기 세 가지

에이전트가 생기는 계기는 세 가지이며, 계기마다 끝나는 때가 다릅니다. 아래 표는 같은 「영업 담당」 프로파일을 예로 세 계기를 나란히 놓은 것입니다.

계기	예	에이전트가 끝나는 때
대화 한 건	영업 담당의 메신저 봇에 고객 질문을 보냄	답을 보내고 대화가 끝날 때
예약 작업 한 건	오전 9시 입찰 공고 정리 예약 작업	정리 결과를 보낸 뒤
게시판 일감 한 건	업무 게시판에서 영업 담당에게 배정된 고객 자료 정리	일감을 완료 상태로 넘긴 뒤

메신저 대화는 프로파일마다 따로 연결된 메신저 봇 계정으로 들어오고[S6], Bot Mode 봇의 정기 루틴도 일반 예약 작업과 같은 방식으로 동작하며[S5], 업무 게시판의 일감은 담당 프로파일 하나에 배정됩니다[S3]. 세 계기는 들어오는 경로만 다를 뿐 결과는 같아서, 모두 담당 프로파일의 설정으로 에이전트 하나를 만들고 일이 끝나면 그 에이전트를 없앱니다. IT 담당자가 「지금 몇 건이 처리 중인가」를 셀 때는 이 세 경로에서 들어온 일감 수를 더하면 됩니다.

4.1.2 오전 9시 입찰 공고 정리와 동시에 들어온 메신저 질문을 따로 처리하는 영업 에이전트 두 개

예약 작업 1건과 메신저 대화 1건으로 생기는 영업 에이전트 두 개

예를 들면 「영업 담당」 프로파일에 오전 9시 입찰 공고 정리 예약 작업이 걸려 있고, 그 작업이 진행되는 9시 5분에 메신저 봇으로 고객 견적 질문이 하나 들어왔다고 가정합니다. 이 경우 같은 프로파일 아래에 에이전트 두 개가 따로 생기며, 하나는 입찰 공고를 모아 표로 만들고 다른 하나는 견적 질문에 답합니다. 예약 작업 1건과 메신저 대화 1건을 더하면 에이전트 2개이고, 두 에이전트는 서로의 대화 내용을 주고받지 않으므로 입찰 공고 목록이 견적 답변에 섞여 들어가지 않습니다. 반면 두 에이전트 모두 영업 담당 프로파일의 기억과 고객 관리 시스템 접속 정보를 함께 쓰기 때문에, 지난주에 정리해 둔 고객 메모는 양쪽 모두 참고할 수 있습니다.

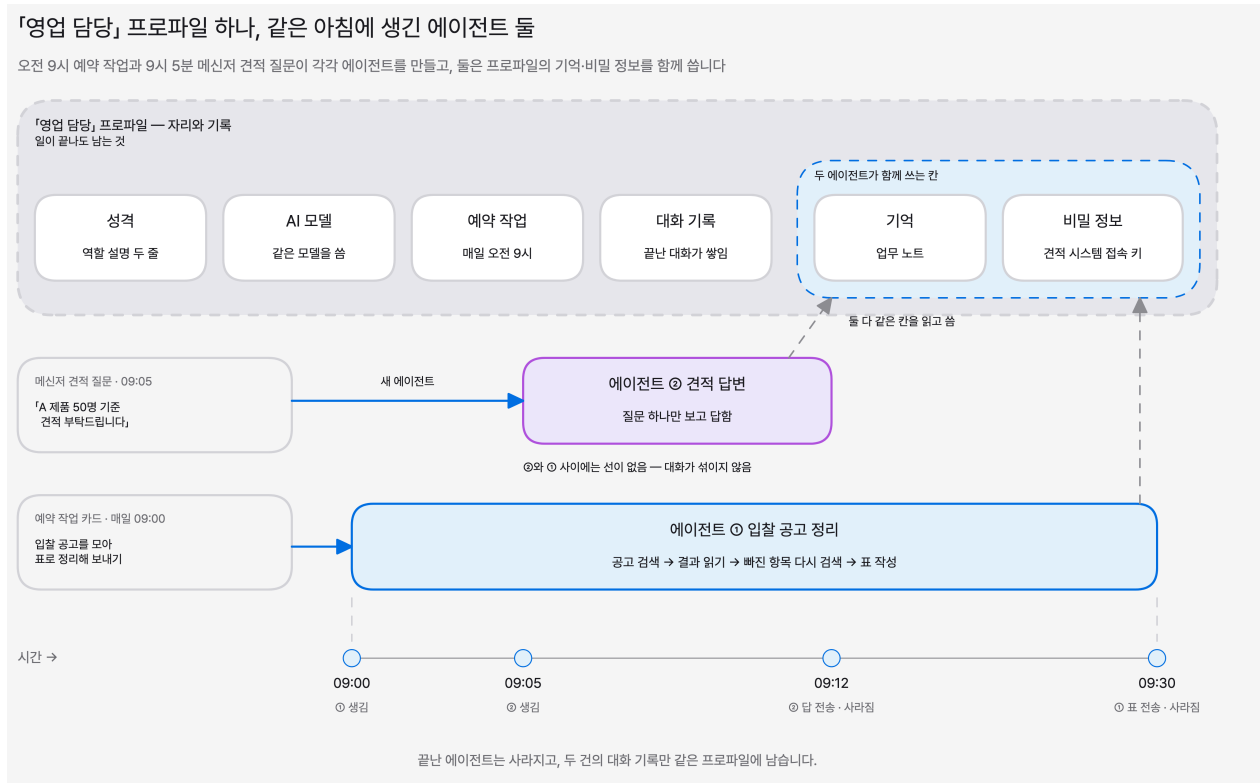


그림. 「영업 담당」 프로파일 하나 아래에서 예약 작업과 메신저 대화가 각각 에이전트를 만드는 구조

대화끼리 섞이지 않으면서 같은 기억을 쓰는 구조의 운영상 이득

이 구조의 이득은 역할 하나를 늘리지 않고도 같은 역할이 여러 일을 동시에 처리할 수 있다는 것입니다. 사람 담당자라면 공고 정리를 멈추고 건적 질문에 답해야 하지만, 에이전트는 일감마다 새로 생기므로 앞선 일을 멈출 이유가 없습니다. 다만 두 에이전트가 같은 기억을 함께 쓰므로, 무엇을 기억에 남길지는 역할 설명에서 범위를 좁혀 두는 편이 관리하기 쉽습니다. 영업 담당 하나에 일이 몰리는 시간대가 있는지 확인해 두면, 그 시간에 동시에 일하는 에이전트 수와 AI 사용량을 미리 가늠할 수 있습니다.

4.2 프로파일 하나에 에이전트 여럿 — 1:N 관계와 저장되지 않는 에이전트

Hermes Agent에서 프로파일과 에이전트는 프로파일 하나에 에이전트 여럿이 속하는 관계이며, 에이전트 하나가 두 프로파일에 걸쳐 일하는 경우는 없습니다. 에이전트 자체는 일이 끝나면 사라지므로, 남아서 셀 수 있는 대상은 프로파일과 그 안의 대화 기록뿐입니다[S1]. 의사결정권자에게 보고할 규모는 프로파일 수로, IT 담당자가 관리할 처리량은 동시에 일하는 에이전트 수로 나누어 세야 합니다.

4.2.1 에이전트 하나는 프로파일 하나에만 속하는 소속 규칙과 프로파일 수로 세는 규모

에이전트 하나가 한 프로파일의 설정·기억·비밀 정보만 쓰는 소속 규칙

에이전트는 생기는 순간 담당 프로파일 하나를 정하고, 그 프로파일의 설정·기억·비밀 정보만 씁니다. 예를 들어 영업 담당 프로파일에서 생긴 에이전트는 영업 담당의 설정과 접속 정보로 일하고 재무 담당 프로파일의 회계 시스템 접속 정보를 쓰지 않는데, 프로파일마다 설정·비밀 정보·성격·기억·대화 기록·스킬·예약 작업을 각자 따로 갖기 때문입니다[S1]. 메신저 봇 계정도 같은 규칙을 따르며, 공식 문서는 프로파일마다 플랫폼별로 서로 다른 메신저 봇 토큰을 써야 하고 같은 토큰을 두 프로파일이 동시에 쓰지 못한다고 적습니다[S6]. 그래서 메신저 봇

하나로 들어온 대화는 언제나 같은 프로파일의 에이전트가 받습니다. 다만 3장에서 본 대로 프로파일은 격리 공간(샌드박스)이 아니므로[S1], 이 소속 규칙은 역할별 설정을 나누는 칸막이이고 서버 파일 접근까지 막는 보안 경계는 아닙니다.

프로파일 수와 에이전트 수로 나누어 세는 AI 동료의 규모

이 소속 규칙 덕분에 세는 기준이 둘로 깔끔하게 나뉩니다. 「AI 동료를 몇 명 두었는가」는 역할마다 하나씩 만든 프로파일 수로 세고, 「지금 몇 건을 처리하는가」는 그 순간 일하는 에이전트 수로 셉니다. 예를 들어 반복 업무 세 개로 시범 팀을 꾸리면 규모는 프로파일 3개이지만, 오전 9시에 예약 작업 세 건과 메신저 대화 두 건이 겹치면 그 순간 일하는 에이전트는 5개입니다. 2.4.3의 운영 사례(역할 11개)에서도 보고서에 적는 숫자는 프로파일 11개이고, 에이전트 수는 시간대마다 달라집니다.

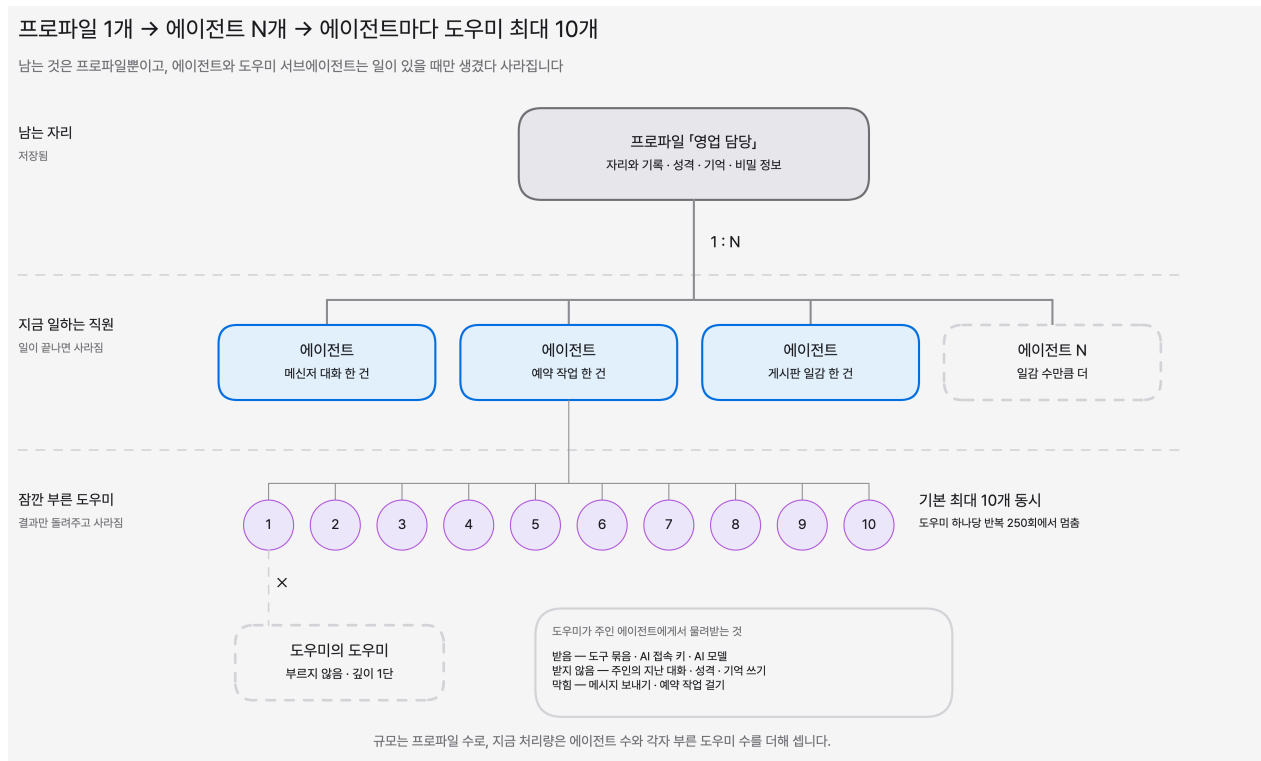


그림. 프로파일 1개 → 에이전트 N개 → 에이전트마다 도우미 서버에이전트 최대 10개(기본값)

한 프로파일에 에이전트 프로그램 두 개를 연결하지 않는 규칙과의 구분

「프로파일 하나에 에이전트 여럿」은 Hermes Agent 프로그램 하나가 한 프로파일을 맡아 일감마다 에이전트를 만드는 구조를 말합니다. 반면 공식 문서는 같은 프로파일에 Hermes Agent 프로그램 두 개를 동시에 연결하지 말라고 경고하는데[S1], 이것은 3장에서 다룬 운영 규칙이고 여기서 말하는 에이전트 여럿과는 다른 이야기입니다. 한 프로파일에서 동시에 여러 일을 처리하려고 프로그램을 하나 더 띄울 필요는 없으며, 프로그램 하나가 일감 수만큼 에이전트를 만들어 처리합니다. IT 담당자는 서버에 띄운 프로그램 수와 그 안에서 일하는 에이전트 수를 구분해 기록해 두면 장애 점검 때 혼동이 줄어듭니다.

4.2.2 「에이전트를 옮긴다」의 실제 대상인 프로파일과 대화 기록

일이 끝나면 사라지는 에이전트와 남는 프로파일·대화 기록

에이전트는 일을 마치면 사라지므로 서버를 옮기거나 다른 팀에 나눠 줄 때 옮길 에이전트가 따로 존재하지 않습니다. 옮기는 실제 대상은 에이전트가 쓰던 프로파일, 그리고 그 안에 쌓인 기억과 대화 기록입니다. 공식 문서도 배포판을 「완성된 Hermes 에이전트 하나를 묶은 것」으로 설명하면서, 그 내용물로 성격·스킬·예약 작업·외부 도구 연결·설정을 둡니다[S2]. 다시 말해 「에이전트를 옮긴다」는 말은 책상과 업무 노트를 옮긴다는 뜻이고, 새 서버에서 일감이 들어오면 그 책상에서 새 에이전트가 생겨 일을 이어 받습니다.

프로파일 단위로 정하는 이전·배포 계획

이전과 배포 계획의 단위는 처음부터 프로파일로 잡아야 합니다. 서버를 옮길 때 쓰는 내보내기 파일과 여러 팀이 계속 받아 쓰는 배포판은 모두 프로파일을 대상으로 하며, 두 방식이 무엇을 담고 무엇을 남기는지는 7장에서 비교합니다[S2]. 다만 계획 단계에서 미리 정해 둘 것은 대화 기록과 기억까지 함께 옮길지, 성격과 스킬만 옮기고 기록은 새로 쌓을지입니다. 이 선택에 따라 넘겨주는 파일에 담기는 내용이 달라지므로, 시범 도입 검토 목록에 「옮길 대상은 프로파일과 대화 기록」이라는 한 줄을 적어 두는 편이 좋습니다.

4.3 큰 일을 나눠 맡기는 서브에이전트 — 기본 최대 10개의 도우미

서브에이전트는 에이전트가 큰 일을 쪼개 잠깐 부르는 도우미로, 목표 하나만 받아 일하고 결과만 주인 에이전트에게 돌려줍니다[S4]. Hermes Agent v0.21.0 기본값으로 도우미는 동시에 최대 10개까지 부를 수 있고, 도우미가 다시 도우미를 부르지 않으며, 도우미 하나는 반복 250회에서 멈춥니다[S4]. 긴 조사를 나눠 동시에 처리하면 결과가 빨리 나오지만, 도우미는 새 대화로 시작해 주인의 지난 대화를 모르므로 일을 맡길 때 목표를 충분히 적어 줘야 합니다.

4.3.1 기본 최대 10개 동시·한 단계 깊이·도우미당 반복 250회라는 기본값

도우미 서브에이전트 기본값 세 가지와 바꿀 수 있는 범위

Hermes Agent는 도우미 부르기에 세 가지 기본값을 둡니다. 아래 표의 숫자는 v0.21.0 기본값이며 모두 설정으로 바꿀 수 있습니다[S4].

항목	기본값	바꿀 수 있나	뜻
동시에 부르는 도우미 수	최대 10개	설정으로 변경, 고정 상한 없음	한 번에 나눠 맡길 수 있는 일의 수
깊이	한 단계	설정으로 늘릴 수 있음	도우미가 다시 도우미를 부르지 않음
도우미 하나당 반복 횟수	250회	설정으로 변경	끝나지 않는 일을 끊는 장치

동시 도우미 수는 한 에이전트가 동시에 일을 맡길 수 있는 도우미의 수이고, 공식 문서는 기본 10개이며 고정 상한은 없다고 밝힙니다. 깊이 한 단계는 도우미가 또 도우미를 부르는 연쇄를 막아 AI 사용량이 예상 밖으로 불어나는 것을 줄입니다. 반복 250회는 도우미가 도구를 쓰고 결과를 보는 과정을 몇 번까지 되풀이할지 정한 상한으로, 끝나지 않는 일이 AI 사용량을 계속 쓰지 않도록 끊는 장치입니다[S4].

동시 처리량과 AI 사용량을 가늠하는 도우미 수

이 숫자들은 동시 처리량과 AI 사용량을 가늠하는 데 바로 쓰입니다. 에이전트 하나가 도우미 10개를 부르면 그 순간 AI 모델을 쓰는 주체는 11개가 되고, 4.2절에서 센 동시 에이전트 수에 각자가 부른 도우미 수를 더해야 실제 사용량이 나옵니다. 2장(2.2.2)의 조사 업무 측정에서 본 대로 여러 에이전트가 나눠 일하면 AI 사용량이 일반 채팅보다 크게 늘어납니다. 따라서 기본값 10개를 그대로 두되, 시범 운영 기간에는 도우미를 부른 횟수와 사용량을 함께 기록해 2장에서 다룬 사용량 판단의 근거로 삼는 편이 안전합니다.

4.3.2 새 대화로 시작해 주인의 지난 대화를 모르는 도우미가 물려받는 것

새 대화로 시작하는 도우미와 목표를 적어 주는 주인 에이전트의 역할

도우미는 완전히 새로운 대화로 시작하므로 주인 에이전트가 사람과 나눈 지난 대화를 모르고, 주인이 넘겨준 목표와 맥락만 압니다[S4]. 예를 들어 영업 담당자가 메신저에서 「지난번처럼 정리해 줘」라고 말했다면, 주인 에이전트는 「지난번」이 무엇인지 풀어서 도우미에게 넘겨야 합니다. 일을 마친 도우미는 최종 결과 요약만 주인에게 돌려주므로[S4], 주인 에이전트가 한 번에 기억하는 대화 분량도 도우미의 중간 작업으로 채워지지 않습니다. Anthropic이 2025년 6월 글에서 도우미가 각자 따로 기억하며 동시에 일하기 때문에 큰 일을 나눠 처리할 수 있다고 설명한 것도 같은 원리입니다[S8].

도우미가 물려받는 것과 받지 않는 것

도우미가 주인에게서 물려받는 것과 받지 않는 것은 공식 문서가 다음과 같이 밝힙니다[S4].

물려받는 것	받지 않거나 막히는 것
주인이 쓰는 도구 묶음	주인의 지난 대화 (새 대화로 시작)
AI 서비스 접속 키와 연결 설정	성격 설정
AI 모델 (따로 정하지 않으면 주인과 같은 모델)	기억 도구 (공유 기억에 쓰지 못함)
—	메시지 보내기 도구
—	예약 작업 도구

물려받는 쪽은 일을 처리하는 데 필요한 능력이고, 막히는 쪽은 프로파일에 흔적을 남기거나 바깥으로 영향을 주는 동작입니다. 그래서 도우미는 기억 도구로 프로파일의 기억을 고치지 못하고, 메신저로 남에게 메시지를 보내지 못하며, 주인의 이름으로 새 예약 작업을 걸지 못합니다. 즉 도우미를 아무리 많이 불러도 프로파일의 기억과 바깥으로 연락하는 창구는 주인 에이전트가 맡으므로, 프로파일에 남는 기록이 도우미 수만큼 늘어나지 않습니다.

4.3.3 경쟁사 다섯 곳 조사를 도우미 다섯에게 나눠 맡기는 예

경쟁사 다섯 곳 기술 비교를 도우미 다섯에게 한 곳씩 맡기는 흐름

쓰임새의 예로, 엔지니어 담당 프로파일의 에이전트가 경쟁사 다섯 곳의 기술 비교 조사를 맡았다고 가정합니다. 주인 에이전트는 회사마다 확인할 항목(제품 구성, 지원하는 AI 모델, 설치 방식, 공개 자료 출처)을 적은 목표를 다섯 개 만들고, 도우미 다섯에게 한 곳씩 동시에 맡깁니다. 각 도우미는 새 대화에서 검색과 문서 읽기를 반복한 뒤 회사 하나에 대한 결과 요약만 돌려주고, 주인 에이전트는 다섯 요약을 모아 비교표 하나로 만들어 담당자에게 보냅니다. 다섯 곳을 차례로 조사하는 대신 동시에 처리하므로 결과가 빨리 나오고, 주인 에이전트의 대화에는 다섯 개의 요약만 남습니다.

경쟁사 다섯 곳 조사를 도우미 다섯에게 나눠 맡기고 결과 요약만 돌려받는 흐름

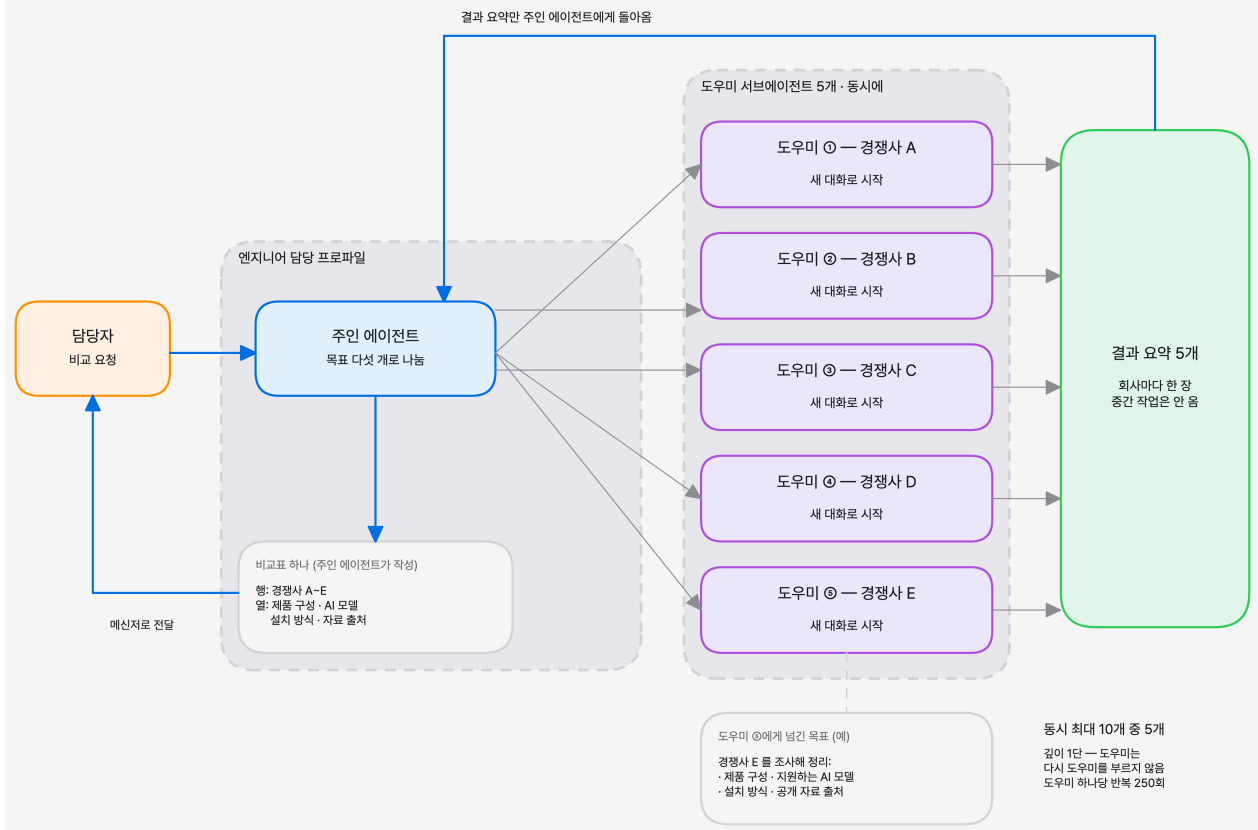


그림. 주인 에이전트 → 도우미 서브에이전트 5개 → 결과 요약 모음 → 비교표

짧게 나눠 결과만 받는 일에 맞는 도우미 부르기

도우미 부르기가 맞는 일은 이 예처럼 서로 독립된 조각으로 나뉘고, 각 조각의 결과만 받아 주인이 바로 이어 쓰는 일입니다. 반면 다른 역할의 확인이 필요하거나, 서버를 다시 시작해도 기록이 남아야 하거나, 사람이 중간에 승인해야 하는 일은 업무 게시판에 일감으로 올리는 편이 맞습니다[S3]. 공식 문서는 도우미 부르기를 짧은 일을 맡기고 바로 답을 받는 호출로, 업무 게시판을 일을 넘길 때마다 한 줄씩 기록이 남는 일감 대기열로 구분합니다[S3]. 두 방식의 선택 기준은 6장에서 업무 게시판과 함께 비교하며, 여기서는 「짧게 나눠 결과만 받는 일은 도우미」라는 기준만 기억해 두면 됩니다.

기억할 것 세 줄

- 에이전트는 대화·예약 작업·게시판 일감마다 생기고, 일이 끝나면 사라지는 지금 일하는 직원입니다.
- 프로파일 하나에 에이전트 여럿이 속하므로, 규모는 프로파일 수로 세고 처리량은 에이전트 수로 셉니다.
- 도우미 서브에이전트는 기본 최대 10개를 동시에 부를 수 있고, 새 대화로 시작해 주인의 지난 대화를 모릅니다.

8장으로 가져갈 의사결정 질문

- 우리 조직에서 역할 하나에 동시에 몇 건의 일이 들어오고, 도우미에게 나눠 맡길 만한 큰 조사 업무가 있는가.

5장. 에이전트를 부르는 두 가지 창구 — 메신저 봇과 Bot Mode 봇

한 줄 요약 메신저 봇과 Bot Mode 봇은 프로파일에 속한 직원을 부르는 두 가지 창구이고, 어느 창구로 불러도 같은 프로파일의 에이전트가 답합니다.

Hermes Agent 공식 문서는 사람이 에이전트를 부르는 경로를 두 가지로 나누어 정의합니다. 하나는 텔레그램·슬랙·디스코드 같은 메신저 플랫폼에 만든 계정인 메신저 봇(Messaging bot)이고, 다른 하나는 Hermes Agent 데스크톱 앱의 명단에 이름과 얼굴 그림을 달고 오른 프로파일인 Bot Mode 봇(Bot Mode bot)입니다[S1]. 메신저 봇은 프로파일에 연결된 외부 계정이고 Bot Mode 봇은 프로파일을 명단에 보여 주는 얼굴이므로, 둘 다 일하는 에이전트 자체와는 구분되는 경로로서 프로파일의 에이전트를 불러내는 같은 역할을 맡습니다.

두 창구를 구분해야 하는 이유는 제품 화면과 설명서, 업계 기사에서 둘이 같은 영어 낱말 Bot으로 함께 불리기 때문입니다. 도입 검토 회의에서 「Bot을 몇 개 만들 것인가」라는 질문이 나오면 메신저 계정 수를 묻는 것인지 데스크톱 명단의 인원을 묻는 것인지가 섞이고, 두 대상은 따르는 규칙도 서로 다릅니다. 메신저 봇은 계정 하나가 프로파일 하나에만 연결되는 잠금 규칙을 따르고[S6], Bot Mode 봇은 데스크톱 화면에서 프로파일을 보여 주는 기능이라 꺼도 프로파일과 대화 기록이 그대로 남습니다[S5]. 따라서 두 창구를 한 낱말로 묶어 계획하면 메신저 계정을 모자라게 준비하거나 필요 없는 프로파일까지 명단에 올리는 설계가 나옵니다.

3장은 프로파일을 직원의 자리와 기록으로, 4장은 에이전트를 그 프로파일의 설정으로 지금 일하는 직원으로 설명했습니다. 메신저 봇과 Bot Mode 봇은 이 비유에서 직원에게 말을 거는 창구에 해당하므로, 창구 수와 직원 수를 따로 세는 기준이 함께 필요합니다. 이 장에서 IT 담당자가 시범 팀 설계에 가져갈 결과물은 두 가지로, 메신저 봇과 Bot Mode 봇을 정체·개수 규칙·끼면 남는 것·대표 쓰임으로 비교한 표와 「새 역할인가, 같은 역할의 창구 추가인가」를 가르는 판단 질문입니다.

5.1 「봇」 한 낱말이 가리키는 두 대상 — 메신저 계정과 자리 배치도 이름표

Hermes Agent 공식 용어 정의는 프로파일·에이전트·서브에이전트와 함께 메신저 봇과 Bot Mode 봇을 서로 다른 항목으로 나누어 둡니다[S1]. 프로파일은 설정과 데이터가 계속 남는 보관 단위이고, 에이전트는 그 설정으로 지금 실행 중인 어시스턴트이며, 메신저 봇과 Bot Mode 봇은 그 에이전트에 말을 거는 경로입니다. 제품 설명을 읽거나 도입 계획서를 쓸 때는 Bot이라는 낱말이 나올 때마다 메신저 계정인지 데스크톱 명단의 항목인지를 먼저 정해 두어야 뒤따르는 판단이 어긋나지 않습니다.

5.1.1 사내 메신저 계정과 사무실 자리 배치도 이름표 비유로 가른 두 봇

쉬운 비유 메신저 봇은 직원에게 연락할 때 쓰는 사내 메신저 계정이고, Bot Mode 봇은 사무실 좌석 배치도에 붙은 이름표입니다. 계정을 눌러도, 이름표를 눌러도 같은 직원이 답합니다.

메신저 봇을 사내 메신저 계정에 견준 비유

회사 메신저에서 재무 담당자의 계정을 눌러 말을 걸면 그 담당자가 답하는 것처럼, 텔레그램이나 슬랙에서 메신저 봇 계정에 메시지를 보내면 그 계정에 연결된 프로파일의 에이전트가 답합니다[S1]. 이때 메신저 계정 자체는

업무 능력도 기억도 갖지 않고, 메시지를 받아 정해진 직원에게 전달하는 경로 역할만 맡습니다. 메신저 봇 연결을 끊어도 직원의 기억과 업무 기록은 프로파일에 그대로 남습니다.

Bot Mode 봇을 좌석 배치도 이름표에 견준 비유

배치도를 보면 누가 어떤 일을 맡는지 얼굴과 직함이 한눈에 보이고, 이름표를 눌러 바로 그 직원과 대화를 시작할 수 있습니다. Hermes Agent 데스크톱 앱의 Bot Mode는 프로파일마다 역할·모델·기억·스킬·얼굴 그림을 보여 주는 명단을 만들고, 명단의 한 줄을 누르면 그 프로파일의 고정 대화방이 열립니다[S5]. 다만 이름표를 떼어 내도 직원이 회사를 떠나지 않는 것처럼, Bot Mode를 꺼도 프로파일은 지워지지 않습니다.

두 창구가 회사 비유 그림에서 말하는 칸

회사 비유 전체로 보면 프로파일은 직원의 설정과 기록이고, 에이전트는 지금 일하는 직원이며, 메신저 봇과 Bot Mode 봇은 그 직원을 부르는 창구 두 개입니다. 「Bot을 몇 개 둘 것인가」라는 질문은 「직원을 몇 명 둘 것인가」와 다른 질문이 되며, 직원 수는 프로파일 수로 세고 창구 수는 메신저 계정 수와 명단 등록 수로 따로 셉니다.

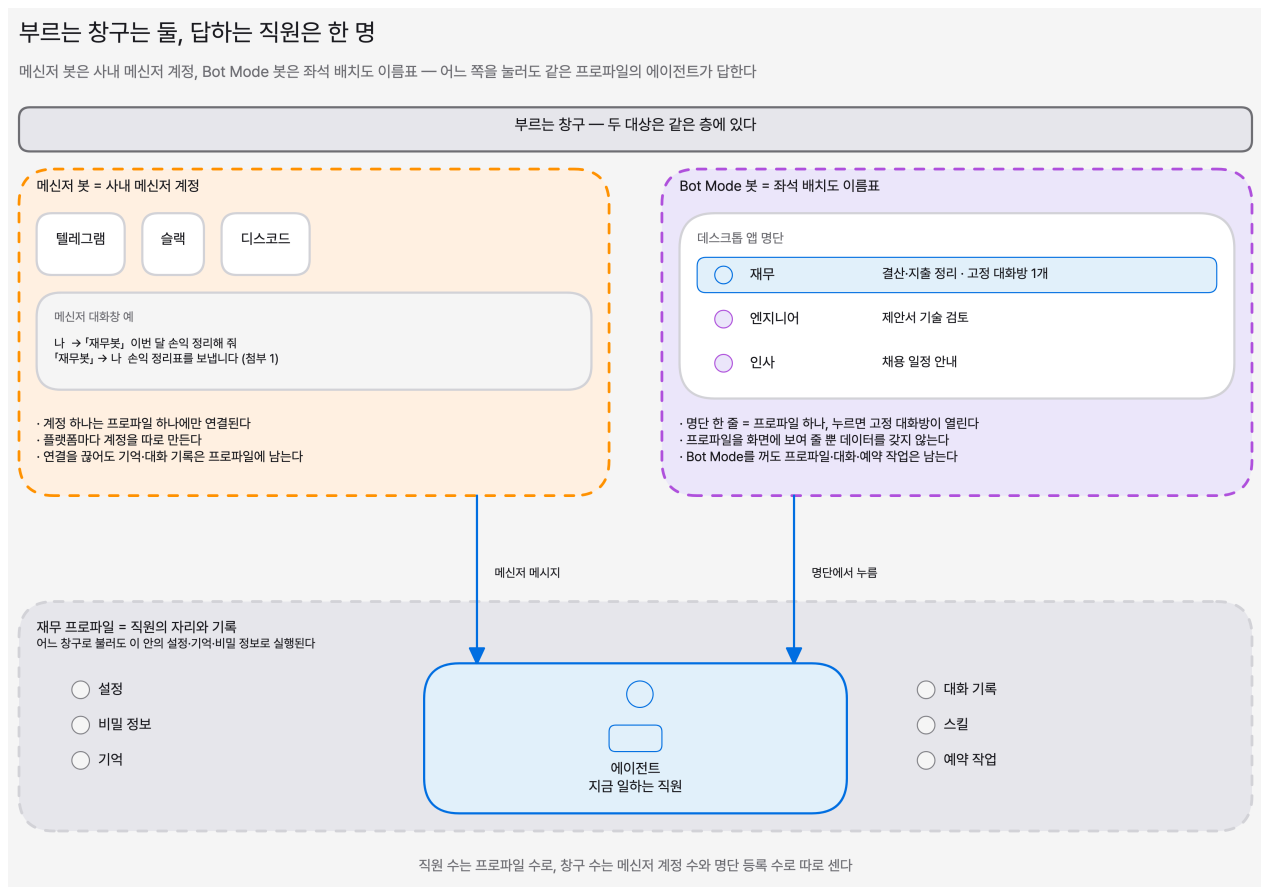


그림. 프로파일·에이전트와 두 가지 부르는 창구를 회사 조직에 견준 그림 — 메신저 계정을 눌러도, 명단 이름표를 눌러도 같은 직원이 답한다

5.1.2 「모든 Bot 은 프로파일이지만 모든 프로파일이 Bot 은 아니다」 원칙

공식 문서의 Bot과 프로파일 포함 관계 원칙

Hermes Agent 공식 문서는 두 대상의 관계를 "Every Bot is a profile, but not every profile is a Bot"이라는 한 문장으로 정리합니다[S1]. 뜻으로 옮기면 「모든 Bot은 프로파일이지만 모든 프로파일이 Bot은 아니다」

입니다. 여기서 Bot은 데스크톱 명단에 오른 Bot Mode 봇을 가리키므로, Bot Mode 봇은 예외 없이 프로파일 하나에 대응하지만 프로파일 가운데 일부만 명단에 오릅니다. Bot Mode 봇의 집합은 결국 프로파일 집합 안에 들어 있는 부분 집합입니다.

명단에 없는 프로파일의 작업 방식

데스크톱 명단에 오르지 않은 프로파일도 일하는 데는 지장이 없습니다. Bot Mode는 같은 프로파일 기능을 화면으로 보여 주는 기능이고, 같은 에이전트를 명령줄 대화로도 그대로 부를 수 있기 때문입니다[S5]. 예를 들어 메신저 봇으로만 부르는 영업 프로파일이나, 정해진 시각에 예약 작업만 실행하는 시장 리포트 프로파일은 데스크톱 명단에 없어도 정상적으로 일합니다.

포함 관계 원칙이 정하는 Bot Mode 등록 범위

이 원칙으로 달라지는 것은 Bot Mode 등록의 운영 범위입니다. 모든 프로파일을 데스크톱 명단에 올릴 필요가 없으므로, 화면에서 직접 대화하거나 여러 의견을 한 번에 받으려는 역할만 골라 Bot Mode 봇으로 보여 주면 됩니다. 반대로 데스크톱 앱에서 Bot Mode 봇을 하나 새로 만들면 그것은 곧 프로파일 하나를 새로 만드는 일이므로, 설정·비밀 정보·기억이 새로 생기고 관리 대상도 하나 늘어납니다[S1][S5].

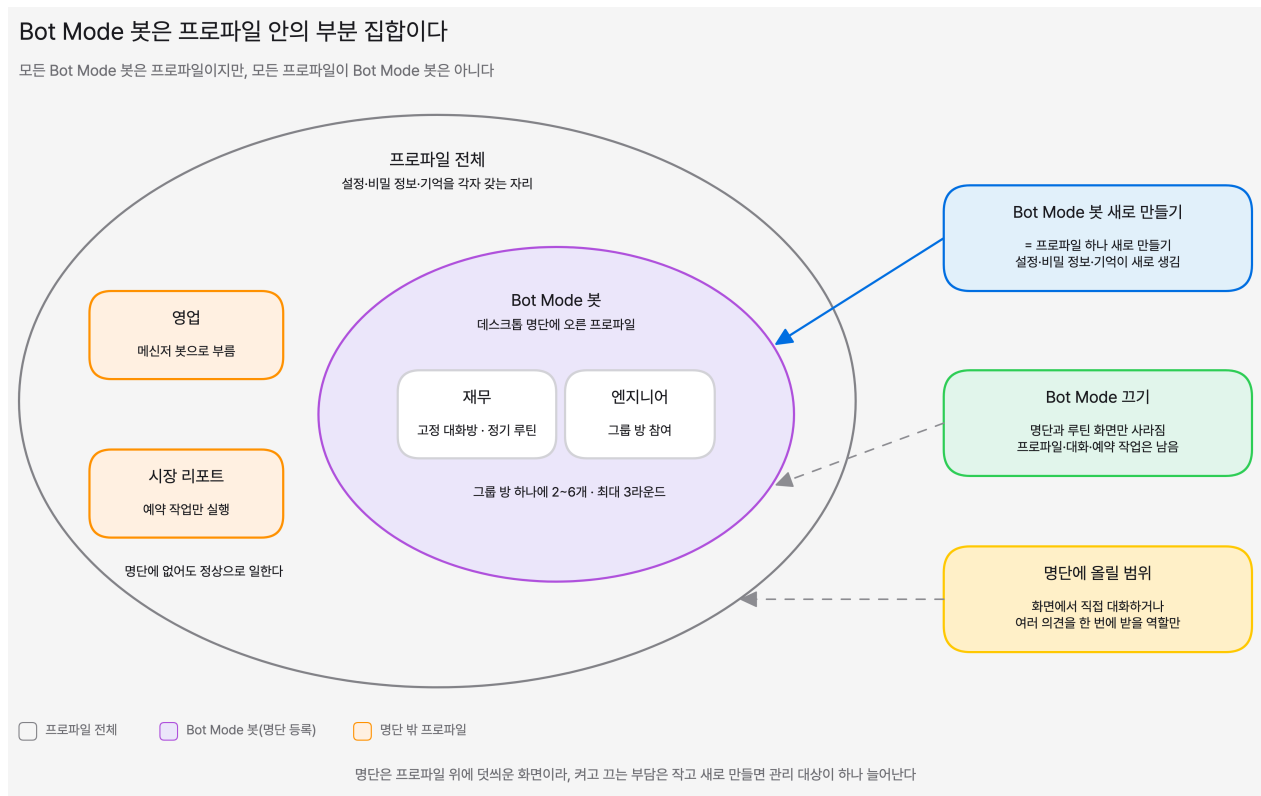


그림. 프로파일 집합 안에 들어 있는 Bot Mode 봇 집합 — 모든 Bot Mode 봇은 프로파일이지만 모든 프로파일이 Bot Mode 봇은 아니다

5.2 메신저 봇 하나는 프로파일 하나에만 연결되는 텔레그램·슬랙 계정

메신저 봇은 직원이 이미 쓰는 메신저 앱 안에서 에이전트를 부르게 해 주는 창구이고, Hermes Agent는 메신저 봇 계정 하나를 프로파일 하나에만 연결하도록 강제합니다[S6]. 이 규칙 덕분에 메신저 봇의 이름만 보고도

어느 프로파일의 에이전트가 답할지 정해지고, 서로 다른 역할의 기억과 비밀 정보가 한 대화에 섞이지 않습니다. 메신저 봇을 몇 개 만들지도 메신저로 부를 프로파일 수와 메신저 플랫폼 수로 바로 계산할 수 있습니다.

5.2.1 같은 메신저 봇 계정을 두 프로파일이 쓰지 못하게 막는 잠금 규칙

메신저 봇 계정과 프로파일의 1:1 잠금 규칙

Hermes Agent 공식 문서는 프로파일마다 메신저 플랫폼별로 고유한 메신저 봇 계정을 쓰도록 정하고, 같은 메신저 봇 계정을 두 프로파일이 동시에 받을 수 없다고 밝힙니다[S6]. 최신 버전은 한 서버의 여러 프로파일을 메신저 연결 창구 하나가 함께 받는 방식을 기본 방향으로 삼지만, 이 방식에서도 메신저 봇 계정과 프로파일의 1:1 연결은 그대로 유지됩니다[S6]. 결과적으로 「재무봇」에게 보낸 메시지는 재무 프로파일의 에이전트만 답합니다.

메신저로 부를 프로파일 수와 같은 메신저 봇 계정 수

이 잠금 규칙에서 나오는 계산 기준은 단순합니다. 메신저로 부를 프로파일이 다섯이면 메신저 플랫폼마다 메신저 봇 계정도 다섯 개가 필요하고, 같은 프로파일을 텔레그램과 슬랙 양쪽에서 부르려면 플랫폼마다 계정을 하나씩 따로 만듭니다[S6]. 최신 버전 기능인 프로파일 복제로 새 프로파일을 만들어도 메신저 봇 계정은 따라오지 않으므로, 복제로 만든 새 프로파일에는 새 메신저 봇 계정을 연결해야 합니다[S1]. 다른 서버로 프로파일을 옮길 때는 같은 메신저 봇 계정을 두 서버가 동시에 받지 않도록 옛 서버의 연결을 먼저 끊는 운영 규칙이 필요하며, 그 절차는 7장에서 이어집니다.

메신저 봇을 열어 둘 때의 기본 안전 수칙

메신저 봇은 누구나 말을 걸 수 있는 메신저 안에 있으므로, 연결하는 순간부터 누가 부를 수 있는지를 함께 정합니다. 기본은 아무도 부를 수 없게 막아 두고 허용한 사람이나 대화방만 열어 주는 방식이며, 여러 사람이 있는 공개 대화방에서는 메신저 봇 이름을 직접 불렀을 때만 답하도록 하는 조건을 검토합니다. 시험용 대화방과 실제 업무 대화방을 나누어 두면 새 스킴이나 설정을 시험하다 생긴 엉뚱한 답이 업무 대화방에 섞이지 않습니다. 대화창에 비밀번호나 접속 키를 붙여 넣지 않고, 결과를 받을 때는 「끝났다」는 문장보다 실제 기록·링크·상태를 함께 보내 달라고 정해 두는 것도 같은 맥락의 운영 수칙입니다.

운영 중인 메신저 봇의 설정을 바꿀 때도 같은 원칙을 따릅니다. 연결 대상이나 허용 범위를 바꾸는 일은 변경 요청과 승인, 문제가 생겼을 때 되돌리는 방법을 함께 기록으로 남기고 진행합니다. 메신저 봇이 답하지 않을 때는 연결 상태, 같은 시간대의 오류 기록, 메신저 쪽 계정과 대화방 권한, 허용 목록에 그 사람이 들어 있는지를 차례로 확인하고, 아주 짧은 시험 메시지를 보내 AI 모델 문제인지 메시지 전달 문제인지를 먼저 가립니다. 접속 키가 새어 나갔다고 의심되면 메신저 봇 연결을 멈춘 뒤 키를 바꿉니다.

5.2.2 「재무봇」에게 이번 달 손익 정리를 요청하는 장면

예를 들면 회사 메신저에 「재무봇」이라는 메신저 봇이 있고 이 계정이 재무 프로파일에 연결되어 있다고 하겠습니다. 재무 담당자가 「재무봇」에게 「이번 달 손익 정리해 줘」라고 보내면, 재무 프로파일의 설정으로 에이전트가 실행되어 재무 프로파일에 저장된 비밀 정보로 회계 자료에 접근하고, 정리한 결과를 같은 메신저 대화창으로 회신합니다.

「재무봇」에게 손익 정리를 요청하는 대화 흐름

이 장면에서 담당자는 새 프로그램을 설치하거나 별도 화면에 접속할 필요 없이, 평소 동료에게 말을 거는 메신저에서 그대로 요청합니다. 메신저 봇 계정은 메시지를 재무 프로파일에 넘기는 일만 하고, 회계 자료에 접근하는 비밀 정보와 지난달 손익 정리에 대한 기억은 모두 재무 프로파일에 들어 있습니다[S1]. 「재무봇」 계정을 다른 메신저 봇 계정으로 바꾸어 연결해도, 재무 에이전트가 일하는 방식과 쌓인 기억은 달라지지 않습니다.

같은 메신저 앱 안의 「영업봇」과 「재무봇」 기억 분리

같은 메신저 앱 목록에 「영업봇」과 「재무봇」이 나란히 있어도 두 메신저 봇은 서로 다른 프로파일에 연결되어 있으므로 상대의 기억과 대화 기록을 보지 않습니다. 프로파일마다 설정·비밀 정보·성격·기억·대화 기록·스킬·예약 작업을 각자 따로 갖기 때문입니다[S1]. 다만 프로파일은 역할을 나누는 칸막이일 뿐 격리 공간이 아니어서 같은 서버 안의 파일 접근까지 막지는 않으므로, 재무 자료처럼 민감한 업무는 서버 계정 권한 설계를 함께 검토합니다(3장).

공식 문서가 예로 든 메신저 봇 쓰임새

Hermes Agent 공식 문서는 메신저 봇 운영 예로 텔레그램 메신저 봇 하나에는 개인 비서를, 다른 하나에는 코딩 담당 에이전트를 두는 구성을 듭니다[S6]. 가족 구성원마다 또는 슬랙 워크스페이스마다 에이전트를 하나씩 두는 구성과, 같은 설정의 시험용·운영용 프로파일을 따로 두는 구성도 같은 목록에 있습니다. 메신저 봇은 직원이 이미 쓰는 메신저에서 바로 AI 동료를 부르게 해 주므로, 새 화면에 대한 사용 교육 부담이 작다는 점을 도입 판단에서 눈여겨볼 만합니다.

5.3 Bot Mode 봇 — 데스크톱 명단에 오른 프로파일의 얼굴과 고정 대화방

Bot Mode는 최근 버전의 Hermes Agent 데스크톱 앱에 기본으로 켜진 채 들어 있는 기능으로, 프로파일들을 이름 붙은 Bot 명단으로 보여 줍니다[S5]. 명단의 Bot Mode 봇마다 역할·모델·기억·스킬·얼굴 그림이 있고, 고정 대화방과 정기 루틴, 여러 Bot Mode 봇이 함께 답하는 그룹 방을 쓸 수 있습니다. Bot Mode 봇은 화면에서 팀원 목록을 보듯 에이전트를 고르고, 여러 관점의 답을 한 번에 받으려는 조직에 맞는 창구입니다.

5.3.1 Bot Chat 고정 대화방과 일반 예약 작업으로 동작하는 정기 루틴

Bot Mode 봇마다 하나인 Bot Chat 고정 대화방

Bot Mode 봇마다 끊기지 않고 계속 이어지는 고정 대화방(Bot Chat)이 하나 있습니다[S5]. 이 대화방에서 새 대화를 시작하는 명령을 입력해도 대화방이 새로 생기지 않고, 같은 대화를 유지한 채 쌓인 작업 맥락만 압축해 정리합니다. 재무 Bot Mode 봇과 나눈 지난달 대화와 이번 달 대화가 한 대화방에 이어져 남고, 사용자는 여러 대화 목록을 뒤질 필요 없이 그 Bot Mode 봇의 대화방 하나만 열면 됩니다.

정기 루틴과 일반 예약 작업의 관계

정기 루틴은 Bot Mode 봇에 지정한 반복 작업이지만, 3장에서 설명한 일반 예약 작업과 같은 것입니다[S5]. 루틴은 이름 앞에 Bot Mode 봇 이름 표시가 달린 예약 작업으로 저장되므로 명령줄의 예약 작업 목록과 기본 예약 작업 화면에도 그대로 보입니다. 예를 들어 재무 Bot Mode 봇에 「매주 월요일 지출 현황 정리」 루틴을 만들면, 그 루틴은 재무 프로파일의 예약 작업 하나로 저장되어 다른 예약 작업과 같은 방법으로 관리됩니다.

새 루틴은 처음부터 정해진 일정으로 돌리기보다 단계를 밟아 켜는 편이 안전합니다. 먼저 같은 요청을 대화방에서 손으로 한 번 실행해 결과를 보고, 입력·결과·실패했을 때의 처리를 분명히 적은 뒤, 루틴을 멈춘 상태나 낮은 빈도로 만들어 한 번 시험 실행합니다. 결과가 제대로 전달되는 것을 확인한 다음에 정식 일정을 켜고, 연속으로

실패하면 사람에게 알림이 가도록 확인 절차를 붙여 둡니다. 자동으로 도는 일이 이상해 보이면 다시 돌려 보기 보다 먼저 멈추고 원인을 확인하는 것이 기본입니다.

Bot Mode를 꺼도 남는 프로파일·대화·예약 작업

Hermes Agent 공식 문서는 Bot Mode가 데이터를 소유하지 않고 화면에 보여 주기만 한다고 밝힙니다[S5]. 데스크톱 앱의 플러그인 설정에서 Bot Mode 기능을 끄면 명단과 루틴 화면은 앱을 다시 시작하지 않아도 바로 사라지지만, 프로파일·대화 기록·예약 작업은 그대로 남습니다. Bot Mode는 프로파일 위에 덧씌운 화면이므로 켜고 끄는 결정의 부담이 작고, 시범 기간에 켜 보았다가 맞지 않으면 꺼도 쌓인 기록을 잃지 않습니다. Bot Mode 봇을 이루는 요소와 기능을 켜고 끄는 때 남는 것은 다음 표와 같습니다.

구성 요소	내용	Bot Mode를 끄면
얼굴과 역할	이름·직함·설명·얼굴 그림, 프로파일의 모델·기억·스킬	명단 화면만 사라지고 프로파일 설정은 남음
고정 대화방(Bot Chat)	Bot Mode 봇마다 하나, 계속 이어지는 대화	대화 기록은 프로파일에 남음
정기 루틴	일반 예약 작업과 같음, 이름 앞에 Bot Mode 봇 이름 표시	루틴 화면은 사라지고 예약 작업은 남음

출처: Hermes Agent Bot Mode 공식 문서[S5]

5.3.2 Bot 2~6개가 한 메시지에 최대 3라운드로 의견을 나누는 그룹 방

그룹 방 하나에 모이는 Bot Mode 봇 2~6개

데스크톱 앱에서는 Bot Mode 봇 2~6개를 그룹 방 하나에 모아 함께 질문할 수 있습니다[S5]. 사용자가 메시지를 한 번 보내면 방 안의 Bot Mode 봇들이 차례로 의견을 내는 라운드가 최대 3번까지 이어집니다. 방 안의 Bot Mode 봇은 서로 @멘션으로 의견을 주고받고, 사람의 판단이 필요한 문제는 사용자에게 넘깁니다.

전문가 그룹 방으로 받는 여러 관점의 답

예를 들어 재무·영업·엔지니어 Bot Mode 봇을 한 방에 모아 「다음 분기 공공 사업 입찰에 참여할 것인가」를 물으면, 재무 Bot Mode 봇은 수익성을, 영업 Bot Mode 봇은 고객 관계를, 엔지니어 Bot Mode 봇은 기술 요구 사항 충족 여부를 각자의 기억과 스킬로 답합니다. 사람이 세 담당에게 따로 물어 답을 모으던 일을 한 방에서 한번에 처리하는 셈입니다. 따라서 그룹 방은 결론을 대신 내리는 기능으로 쓰기보다, 결정권자가 여러 관점을 한 화면에서 비교하도록 돕는 도구로 쓰는 편이 맞습니다.

그룹 방 수치 상한과 쓰임새의 한계

그룹 방에는 끝없이 이어지는 대화를 막는 상한이 있습니다. 공식 문서 기준으로 라운드는 최대 3번, 한 번 보낼 때 메시지는 10개까지이고, 각 Bot Mode 봇은 방 대화를 약 200개 메시지 또는 32,000자 가운데 먼저 차는 쪽까지만 읽으며, 지나치게 긴 메시지 한 건은 8,000자 분량으로 잘립니다[S5]. 그래서 긴 보고서를 넘겨 검토 시키거나 여러 날 이어지는 일을 맡기기에는 맞지 않고, 그런 일은 모든 프로파일이 함께 보는 업무 게시판에 일감으로 올리는 편이 기록과 재시작 면에서 안전합니다[S3]. 또한 여러 Bot Mode 봇이 함께 답하면 AI 모델 사

용량도 그만큼 늘어나므로, 여러 관점이 실제로 필요한 질문에만 그룹 방을 쓰는 편이 비용 면에서도 맞습니다. 그룹 방 수치는 다음과 같습니다.

항목	공식 문서 기준
참여 Bot Mode 봇	2~6개
사용자 메시지 1번당 라운드	최대 3라운드
한 번 보낼 때 메시지	최대 10개
각 Bot Mode 봇이 읽는 방 대화 분량	약 200개 메시지 또는 32,000자
긴 메시지 1건	8,000자 분량으로 잘림

출처: Hermes Agent Bot Mode 공식 문서[S5]

5.4 새 역할에는 새 프로파일, 같은 역할에는 창구 추가 — 두 봇을 함께 쓰는 판단

한 프로파일은 메신저 봇과 Bot Mode 봇을 함께 가질 수 있고, 어느 창구로 부르든 같은 기억과 비밀 정보를 쓰는 같은 동료가 답합니다[S1][S5]. 시범 팀 설계의 둘째 결정은 요청이 들어올 때마다 「역할이 늘었는가, 창구가 늘었는가」를 가르는 일입니다. 역할이 늘었으면 프로파일을 새로 만들고, 같은 역할을 다른 곳에서도 부르려면 프로파일은 그대로 두고 창구만 더합니다.

5.4.1 메신저와 데스크톱 어디서 불러도 같은 기억을 쓰는 한 프로파일

이렇게 쓴다 5.2.2의 재무 프로파일을 데스크톱 명단에도 올리면, 재무 프로파일은 메신저의 「재무봇」과 데스크톱의 Bot Chat이라는 창구 두 개를 갖습니다. 외근 중인 재무 담당자는 휴대전화 메신저로 「재무봇」에게 묻고, 결산 회의를 준비하는 팀장은 데스크톱 그룹 방에서 재무 Bot Mode 봇의 의견을 받습니다.

메신저와 데스크톱 양쪽에서 부르는 재무 프로파일

두 창구 모두 같은 재무 프로파일의 설정과 기억, 비밀 정보로 에이전트를 실행하므로 어디서 불러도 같은 동료가 답합니다[S1]. 다만 공식 문서는 Bot Chat을 Bot Mode 봇마다 하나인 고정 대화로 정의하고 같은 프로파일의 일반 대화는 그와 따로 둔다고 설명합니다[S5]. 따라서 두 창구가 함께 쓰는 것은 설정·기억·비밀 정보이고, 메신저에서 나눈 대화가 Bot Chat 화면에 합쳐져 보인다고 기대하지 않는 편이 맞습니다.

창구 추가와 관리 대상 프로파일 수의 관계

창구는 둘로 늘었지만 관리할 프로파일은 여전히 하나입니다. 관리할 설정, 갱신할 스킬, 점검할 비밀 정보가 재무 프로파일 하나에 모여 있으므로 창구를 늘려도 운영 부담이 그만큼 늘지 않습니다. 반면 메신저 봇 계정은 플랫폼마다 하나씩 늘어나므로[S6], 텔레그램과 슬랙을 함께 쓰는 조직은 어느 메신저 봇 계정이 어느 프로파일에 연결되어 있는지 창구 목록 표로 기록해 두는 편이 안전합니다. 같은 프로파일을 배포판으로 다른 팀에 나눠 줄 때도 배포판에는 비밀 정보가 담기지 않고 설치하는 쪽이 자기 비밀 정보를 직접 채우게 되어 있으므로[S2], 메신저 봇 계정 역시 받는 팀이 자기 계정으로 연결합니다.

5.4.2 정체·개수 규칙·끼면 남는 것으로 비교한 메신저 봇과 Bot Mode 봇

메신저 봇과 Bot Mode 봇의 네 가지 비교 기준

두 창구의 차이를 정체·개수 규칙·끄면 남는 것·대표 쓰임 네 가지 기준으로 나란히 놓으면 다음과 같습니다. 개수 규칙이 서로 다르기 때문에 메신저 봇은 계정 수를, Bot Mode 봇은 명단에 올릴 프로파일 수를 따로 계획합니다.

기준	메신저 봇	Bot Mode 봇
정체	텔레그램·슬랙·디스코드 같은 메신저 플랫폼의 계정	데스크톱 앱 명단에 이름과 얼굴로 오른 프로파일
개수 규칙	계정 하나는 프로파일 하나에만 연결, 플랫폼마다 따로 만듦	Bot Mode 봇 하나가 프로파일 하나, 그룹 방은 2~6개
끄면 무엇이 남나	연결을 끊어도 프로파일의 기억·대화 기록은 남음	Bot Mode를 꺼도 프로파일·대화·예약 작업이 남음
대표 쓰임	직원이 이미 쓰는 메신저에서 바로 부르기	화면에서 팀원 목록처럼 고르기, 여러 관점을 한 번에 받기

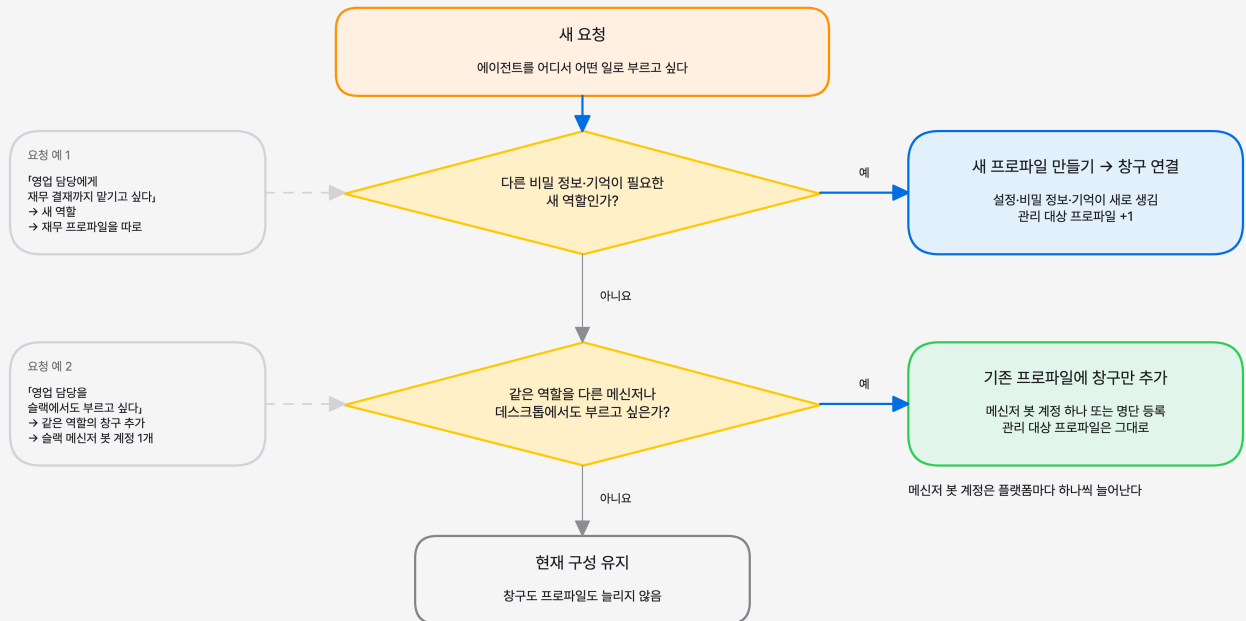
출처: Hermes Agent 공식 문서[S1][S5][S6]

새 프로파일과 창구 추가를 가르는 판단 질문

판단 질문은 두 개입니다. 첫째 질문은 다른 비밀 정보와 다른 기억이 필요한 새 역할인가이며, 그렇다면 프로파일을 새로 만들고 그 프로파일에 메신저 봇이나 Bot Mode 봇 창구를 연결합니다. 둘째 질문은 이미 있는 역할을 다른 메신저나 데스크톱에서도 부르고 싶은가이며, 그렇다면 프로파일은 그대로 두고 창구만 추가합니다. 예를 들어 영업 담당에게 재무 결재까지 맡기려는 요청은 새 역할이므로 재무 프로파일을 따로 만들고, 영업 담당을 슬랙에서도 부르려는 요청은 창구 추가이므로 슬랙 메신저 봇 계정만 하나 더 만듭니다. Anthropic이 에이전트 설계 원칙으로 권하는 「가장 단순한 구성에서 시작해 필요할 때만 복잡도를 높인다」는 기준은 창구 설계에도 그대로 맞으므로[S7], 시범 단계에서는 역할마다 직원이 이미 쓰는 메신저 창구 하나로 시작하는 편이 무난합니다.

역할이 늘었나, 창구가 늘었나

요청 하나마다 두 질문으로 가른다 — 새 역할이면 새 프로파일, 같은 역할이면 창구만 추가



시범 단계에서는 역할마다 직원이 이미 쓰는 메신저 창구 하나로 시작하고, 창구는 필요할 때 늘린다

그림. 새 프로파일과 창구 추가를 가르는 판단 흐름

기억할 것

- 메신저 봇과 Bot Mode 봇은 에이전트를 부르는 창구이고, 창구는 이 두 가지입니다.
- 메신저 봇 계정 하나는 프로파일 하나에만 연결됩니다.
- 모든 Bot은 프로파일이지만 모든 프로파일이 Bot은 아닙니다.

8장으로 가져갈 질문 역할마다 어느 창구로 부르는가 — 직원이 이미 쓰는 메신저인가, 데스크톱의 화면 콘솔인가. 시범 팀의 업무 3개마다 이 질문의 답을 한 줄씩 적어 두면, 8장의 설계표에서 창구 칸과 메신저 봇 계정 수를 바로 채울 수 있습니다.

6장. 에이전트 팀이 함께 일하는 방식 — 업무 게시판으로 주고받는 일감

5장까지 프로파일·에이전트·부르는 창구로 역할 하나를 갖췄다면, 남은 문제는 역할과 역할 사이에 일을 넘기는 방법입니다. Hermes Agent의 업무 게시판(칸반, Kanban)은 한 서버에 있는 모든 프로파일이 함께 쓰는 일감 게시판이고, 일감이 넘어갈 때마다 기록이 한 줄씩 남습니다[S3]. 칸반은 일감 하나를 카드 한 장으로 만들어 처리 상태별 칸에 놓고 옮겨 가며 관리하는 업무 방식이며, Hermes Agent는 이 방식을 프로파일 사이의 일감 전달에 씁니다. 업무 게시판과 함께 Bot Mode 봇끼리 직접 메시지를 주고받는 기능도 최근 버전에서 제공되므로, 역할을 나눈 에이전트들이 서로 일을 넘기는 방법은 두 가지가 됩니다[S5].

역할마다 프로파일을 나누면 기억과 비밀 정보가 섞이지 않는 대신 일이 역할 사이를 오가야 하는 문제가 새로 생깁니다. 영업 담당 에이전트가 만든 제안서 초안을 엔지니어가 검토해야 하는 경우가 그 예입니다. 이때 사람이 두 메신저 창을 오가며 결과를 복사해 옮기면 에이전트를 여럿 둔 효과가 줄어들고, 누가 언제 무엇을 넘겼는지도 남지 않습니다. 업무 게시판은 이 전달을 일감 단위로 기록하고, 사람이 확인해야 하는 단계를 일감 흐름 안에 둘 수 있게 합니다[S3].

이 장을 읽고 나면 에이전트 사이에 일을 넘기는 세 가지 방법인 도우미 부르기, 업무 게시판, Bot Mode 봇끼리 직접 메시지 가운데 하나를 고르는 기준과, 업무 역할 11개로 구성된 운영 사례를 시범 팀 설계의 견본으로 가져갈 수 있습니다.

한 줄 요약 모든 프로파일이 같이 보는 업무 게시판에 일감을 올리면, 역할 설명을 읽고 맞는 프로파일에 배치되고 그 프로파일의 에이전트가 처리한 뒤 사람이 결과를 확인합니다.

6.1 모든 프로파일이 함께 보는 업무 게시판(칸반)

업무 게시판은 Hermes Agent의 모든 프로파일이 같은 일감 목록을 읽고 쓰는 공용 게시판이며, 서버에 있는 저장소에 기록되므로 특정 에이전트 프로그램이 종료되어도 일감이 그대로 남습니다[S3]. 일감은 담당 프로파일을 하나씩 가지고, 그 프로파일의 설정과 기억으로 실행된 에이전트가 일감을 처리합니다. 업무 게시판은 3장의 프로파일(자리와 기록)과 4장의 에이전트(지금 일하는 직원)를 일감 단위로 잇는 장치이며, 이 장에서 「업무 게시판」은 이 기능만을 가리킵니다.

쉬운 비유 사무실 벽에 붙은 업무 게시판을 떠올리면 Hermes Agent의 업무 게시판 구조를 그대로 이해할 수 있습니다. 누구나 일감 쪽지를 붙일 수 있고, 쪽지에는 담당자 이름이 하나 적히며, 일이 진행되면 쪽지를 「진행 중」 칸에서 「검토」 칸과 「완료」 칸으로 옮깁니다. 쪽지는 담당자가 자리를 비우거나 바뀌어도 게시판에 남아 있으므로 다음 담당자가 이어서 처리할 수 있습니다. 에이전트 팀에서도 같은 원리로 일감 카드가 프로파일 사이를 옮겨 다니며, 사람은 카드에 의견을 남기거나 멈춘 카드를 다시 진행시키는 방식으로 언제든지 끼어들 수 있습니다[S3].

6.1.1 역할 설명을 읽고 맞는 프로파일에 일감을 배정하는 방식

업무 게시판 일감마다 정해지는 담당 프로파일 하나

업무 게시판의 일감은 담당 프로파일을 반드시 하나만 가지며, 담당이 정해진 일감은 그 프로파일의 에이전트가 맡아 처리합니다[S3]. 담당이 둘 이상이면 결과에 대한 책임이 흐려지기 때문에 일감 하나에 담당 하나라는 규칙을 지키고, 여러 역할이 필요한 큰 일은 담당이 하나씩 붙은 작은 일감 여러 개로 나눕니다. 일감은 분류를 기다리는 상태에서 시작해 처리 중, 막힘, 검토, 완료 같은 상태를 거치며, 상태를 보면 지금 어느 역할이 무엇을 들고 있는지 알 수 있습니다. 업무 게시판 한 장으로 에이전트 팀 전체의 진행 상황을 볼 수 있습니다.

역할 설명을 읽고 담당을 고르는 자동 분해 기능

일감을 분류 대기 칸에 올리면 자동 분해 기능이 프로파일 명단과 각 프로파일의 역할 설명을 읽고, 큰 일감을 작은 일감으로 나눈 뒤 가장 잘 맞는 프로파일에 하나씩 배정합니다[S3]. 자동 분해 기능은 나눈 일감을 담당 없이 남겨 두지 않으며, 명단에 없는 프로파일을 고르면 미리 정해 둔 기본 담당에게 보냅니다. 역할 설명이 없는 프로파일도 이름만으로 배정될 수는 있지만, 이름만으로는 그 프로파일이 무슨 일을 하는지 판단할 근거가 적어 배정이 덜 정확해집니다. 반면 사람이 직접 배정하고 싶은 조직은 자동 분해를 끄고 분류 대기 칸의 일감을 손으로 나눠 줄 수도 있습니다.

넘길 때마다 남는 기록과 재시작 뒤에도 유지되는 일감

일감이 다른 프로파일로 넘어가거나 상태가 바뀔 때마다 업무 게시판에는 그 변화가 한 줄씩 기록되고, 기록은 지워지지 않고 계속 쌓입니다[S3]. 일감을 맡은 에이전트는 실행될 때 그 일감에 달린 의견을 처음부터 끝까지 읽고 시작하며, 일을 마치면 요약과 확인 내용을 정리해 다음 담당에게 넘깁니다. 처리 도중 에이전트 프로그램이 비정상 종료되면 업무 게시판이 그 일감을 다시 대기열로 돌려 다른 에이전트가 이어받게 합니다. 그래서 서버를 다시 시작해도 일감이 사라지지 않고, 나중에 누가 언제 무엇을 넘겼는지를 일감 기록만으로 되짚을 수 있습니다.

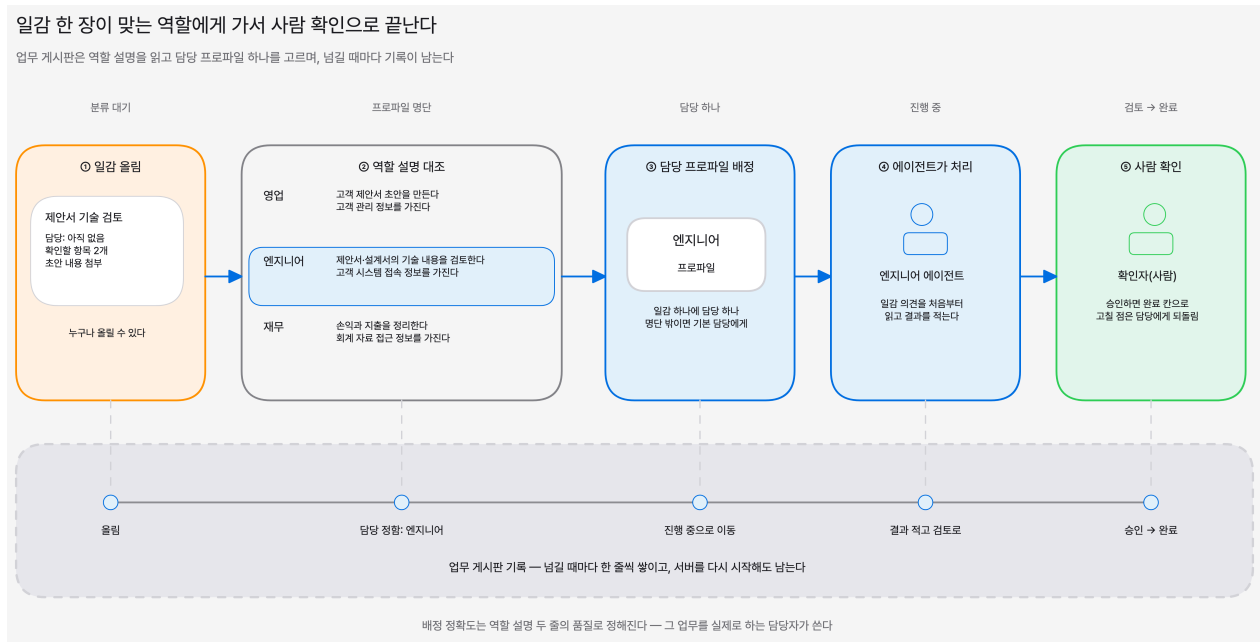


그림. 업무 게시판에 올린 일감이 역할 설명 대조를 거쳐 담당 프로파일의 에이전트에게 가고 사람 확인으로 끝나는 흐름

역할 설명 두 줄이 정하는 배정 정확도

업무 게시판의 배정 정확도는 자동 분해 기능이 읽는 역할 설명의 품질로 정해지므로, 역할 설명은 IT 담당자보다 그 업무를 실제로 하는 담당자가 쓰는 편이 맞습니다. 예를 들어 「엔지니어」라는 이름만 있는 프로파일보다 「제안서와 설계서의 기술 내용을 검토하고 구성 오류를 지적한다, 고객 시스템 접속 정보를 가진다」처럼 맡는 일과 가진 정보를 두 줄로 적은 프로파일이 기술 검토 일감을 더 정확히 받습니다. 8장의 설계표가 프로파일마다 역할 설명 두 줄을 적게 하는 이유가 이 배정 방식에 있습니다. 결국 업무 게시판을 도입할 때 기능 설정보다 먼저 준비할 것은 역할마다 무엇을 맡고 무엇을 맡지 않는지를 적은 짧은 글입니다.

6.1.2 영업 에이전트가 올린 제안서 기술 검토가 엔지니어 에이전트에게 배정되는 예

예를 들면 3장의 「영업 담당」 프로파일에서 실행된 영업 에이전트가 고객 제안서 초안을 만들다가 기술 구성이 맞는지 확인이 필요해지면, 업무 게시판에 「제안서 기술 검토」 일감을 올리고 초안 내용과 확인할 항목을 일감에 적습니다. 자동 분해 기능은 프로파일 명단의 역할 설명을 대조해 「제안서와 설계서의 기술 내용을 검토한다」고 적힌 엔지니어 프로파일을 담당으로 정합니다[S3]. 엔지니어 프로파일의 설정과 기억으로 엔지니어 에이전트가 실행되고, 일감에 달린 내용을 읽은 뒤 구성 오류와 보완할 문장을 정리해 일감에 결과로 남깁니다. 결과가 남은 일감은 검토 칸으로 옮겨지고, 엔지니어 팀장이 결과를 확인해 승인하면 완료 칸으로 갑니다.

사람 전달 없이 이동하는 일감과 사람이 맡는 승인

이 장면에서 영업 담당자는 엔지니어에게 메신저로 초안을 보내거나 회의를 잡지 않았는데도 기술 검토가 맞는 역할에게 도착했습니다. 엔지니어 에이전트는 영업 프로파일의 지난 대화 기록이나 고객 관리 시스템 접속 정보를 보지 않고, 일감에 적힌 내용만으로 일합니다. 프로파일마다 설정·비밀 정보·기억을 따로 가지므로 일감을 주고 받아도 두 역할의 칸막이가 유지됩니다[S1]. 다만 검토 결과를 고객에게 보낼 제안서에 반영해도 되는지는 엔지니어 팀장이 판단하며, 업무 게시판은 검토 상태를 따로 두어 이 승인 단계를 일감 흐름 안에 넣습니다[S3].

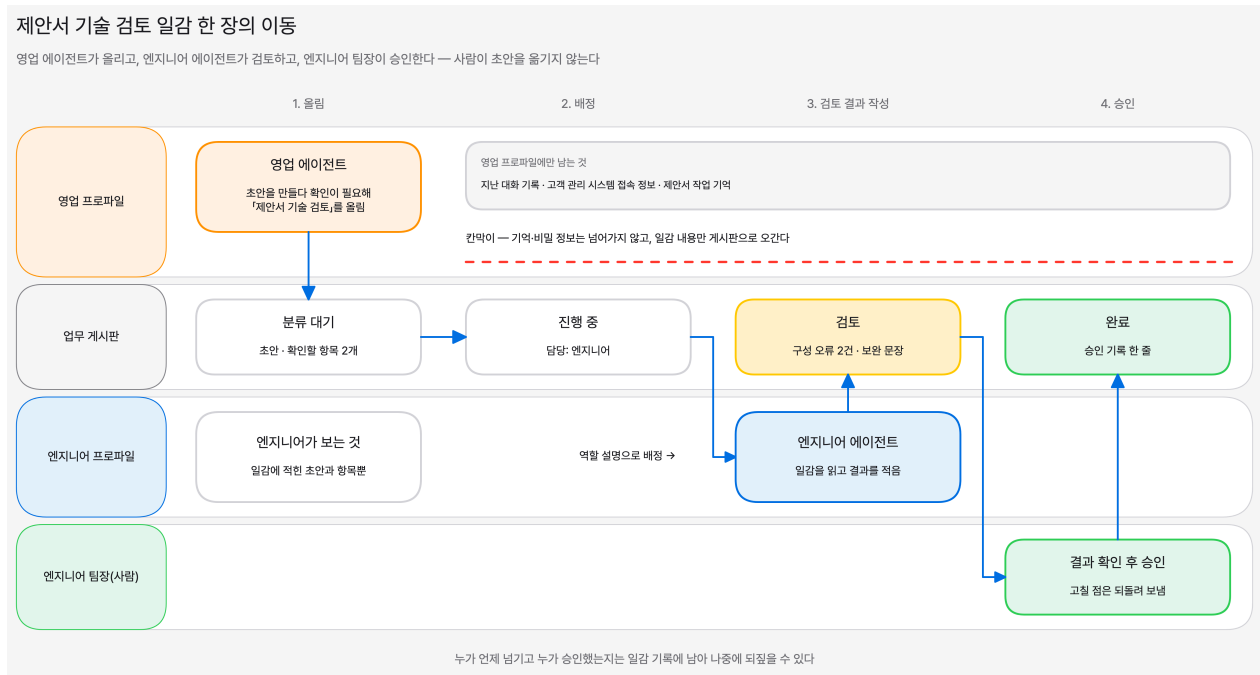


그림. 영업 에이전트가 올린 「제안서 기술 검토」 일감이 엔지니어 에이전트를 거쳐 엔지니어 팀장의 승인으로 끝나는 흐름

6.2 도우미 부르기과 업무 게시판 사이의 선택 기준

Hermes Agent에서 에이전트가 다른 에이전트에게 일을 맡기는 방법은 4장의 서브에이전트(도우미) 부르기 와 이 장의 업무 게시판 두 가지이며, 공식 문서는 도우미 부르기를 「바로 답을 받는 호출」로, 업무 게시판을 「넘길 때마다 한 줄씩 기록이 남는 일감 대기열」로 구분합니다[S3]. 두 방법은 모두 일을 나누지만 기록이 남는 위치, 실패했을 때의 처리, 사람이 끼어들 수 있는지가 다릅니다. 그래서 같은 일을 어느 쪽으로 보내느냐에 따라 나중에 결과를 되짚을 수 있는지와 승인 단계를 넣을 수 있는지가 달라집니다. 판단이 어려우면 가장 단순한 방법으로 시작하고 필요할 때만 구성을 복잡하게 만들라는 에이전트 설계의 일반 원칙을 따릅니다[S7].

6.2.1 짧은 답을 받아 바로 이어 가는 일에 맞는 서브에이전트

도우미 부르기가 맞는 일 — 같은 역할 안에서 쪼개고 바로 모으는 일

도우미 부르기는 에이전트가 큰 일을 잘게 나눠 도우미에게 맡기고, 결과를 바로 돌려받아 자기 대화에서 이어 쓰는 「바로 답을 받는 부탁」입니다. 4장의 예에서 엔지니어 에이전트가 경쟁사 다섯 곳의 기술 비교 조사를 도우미 다섯에게 한 곳씩 맡기고 결과를 모아 비교표를 만든 것이 전형적인 경우입니다. Hermes Agent v0.21.0 기본값으로 도우미는 동시에 최대 10개까지 실행되고, 도우미가 다시 도우미를 부르지 않는 1단 구조이며, 도우미 하나는 최대 250회까지 반복 작업을 합니다[S4]. 이 기본값은 설정으로 바꿀 수 있습니다. 즉, 같은 역할 안에서 끝나고 몇 분 안에 결과가 돌아오는 일이 도우미에 맞습니다.

도우미 결과가 남는 위치와 재시작 때의 한계

도우미는 새 대화로 시작해 주인 에이전트의 지난 대화를 모르고, 주인이 적어 준 지시만 받아 일한 뒤 결과를 돌려줍니다[S4]. 도우미가 한 일의 기록은 주인 에이전트의 대화 안에만 남고, 대화 분량이 많아져 앞부분이 압축 되면 그 기록도 함께 줄어듭니다. 공식 문서의 비교표에 따르면 도우미 부르기는 실패하면 그대로 실패로 끝나 이어서 다시 실행할 수 없고, 처리 도중 사람이 끼어드는 기능도 지원하지 않습니다[S3]. 따라서 결과를 사람이 승인해야 하거나 며칠에 걸쳐 진행되는 일은 도우미에 맡기지 않는 편이 맞습니다.

여러 도우미를 동시에 쓸 때 늘어나는 AI 사용량

도우미를 여럿 동시에 부르면 일이 빨리 끝나는 대신 AI 모델 사용량이 함께 늘어나며, 2장(2.2.2)에서 본 것처럼 여러 에이전트로 나눠 처리하는 방식은 일반 채팅보다 사용량이 크게 늘어납니다[S8]. 도우미 수를 늘리는 결정은 비용 결정이기도 합니다. 도우미는 결과를 바로 받아 같은 대화에서 이어 쓰는 일에 한정하고, 동시에 부르는 수는 필요한 만큼만 둡니다.

6.2.2 역할을 넘거나 오래 걸리거나 사람 확인이 필요한 일에 맞는 업무 게시판

업무 게시판이 맞는 일 — 역할을 넘는 일, 오래 걸리는 일, 사람 확인이 필요한 일

공식 문서는 업무 게시판을 써야 하는 경우로 세 가지를 듭니다[S3]. 첫째는 다른 역할의 프로파일이 받아야 하는 일로, 6.1.2의 제안서 기술 검토처럼 영업에서 엔지니어로 넘어가는 일이 여기에 해당합니다. 둘째는 서버나 에이전트 프로그램이 다시 시작되어도 남아 있어야 하는 일이며, 업무 게시판은 막힌 일감을 풀어 다시 실행하고 비정상 종료된 일감을 회수합니다. 셋째는 사람이 중간에 확인하거나 의견을 줘야 하는 일이며, 사람은 업무 게시판에서 언제든지 일감에 의견을 달거나 막힌 일감을 풀 수 있습니다.

사람 확인 단계를 일감 흐름에 넣는 검토 상태와 막힘 상태

업무 게시판에는 사람 확인을 위한 상태가 두 가지 있습니다. 에이전트는 사람의 판단이나 추가 자료가 필요하면 이유를 적어 일감을 막힘 상태로 두고, 일을 마치면 일감을 검토 상태로 넘겨 확인자에게 보냅니다[S3]. 확인자는 검토 상태의 일감을 승인해 완료로 옮기거나 고칠 점을 적어 담당에게 되돌려 보낼 수 있고, 완료·보관·막힘처럼 되돌리기 어려운 이동은 화면에서 한 번 더 확인을 받습니다. 이렇게 확인 단계가 일감 상태로 남기 때문에 「누가 승인했는가」를 나중에 일감 기록에서 찾을 수 있습니다.

아래 표는 공식 문서의 구분 기준을 판단 항목별로 놓은 것이며, 6.3의 Bot Mode 봇끼리 직접 메시지 열을 함께 붙였습니다.

판단 항목	도우미 부르기(서브에이전트)	업무 게시판(칸반)	Bot Mode 봇끼리 직접 메시지
일의 길이	짧은 일, 결과를 바로 받음	오래 걸려도 됨	짧은 확인·문의
역할을 넘는가	같은 역할 안에서 나눔	다른 역할 프로파일에 배정	다른 역할 Bot Mode 봇에게 보냄
재시작에도 남아야 하는가	실패하면 그대로 끝남	막힘 해제·재실행·회수	답이 나중에 옴
사람 확인	지원하지 않음	의견·막힘 해제·검토 상태	별도 단계 없음
기록 위치	주인 에이전트의 대화	업무 게시판 일감 기록	두 Bot Mode 봇의 대화

출처: Hermes Agent 공식 문서[S3][S4][S5]

이 표를 판단 질문으로 바꾸면 세 가지가 됩니다. 이 일을 다른 역할이 받아야 하는가, 일이 끝나기 전에 서버가 다시 시작되어도 이어져야 하는가, 결과를 사람이 확인한 뒤에 다음 단계로 넘어가야 하는가를 묻고, 하나라도 「예」이면 업무 게시판으로 보냅니다. 세 질문이 모두 「아니오」이고 결과를 바로 받아 같은 대화에서 이어 쓰면 도우미 부르기로 충분합니다.

 **결정 포인트** 사람 확인이 필요한 일감은 업무 게시판으로 보내고, 일감마다 검토 상태에서 승인할 확인자를 한 명씩 정합니다. 8장의 설계표에 적는 결과 확인자가 이 역할을 맡습니다.

6.3 Bot 끼리 주고받는 직접 메시지와 다른 서버 Bot 과의 연결

Bot Mode 봇은 데스크톱 앱의 Bot Mode 명단에 이름을 올린 프로파일이며, 공식 문서의 정의대로 모든 Bot은 프로파일이지만 모든 프로파일이 Bot은 아닙니다[S1]. 최근 버전의 Bot Mode는 Bot Mode 봇마다 역할·AI 모델·기억·스킬을 따로 두고, Bot Mode 봇끼리 업무 게시판을 거치지 않고 직접 메시지를 보내는 기능을 제공합니다[S5]. 따라서 Bot Mode 봇을 쓰는 조직은 6.2의 두 방법에 더해 짧은 확인이나 문의를 직접 메시지로 처리할 수 있습니다. 다만 직접 메시지는 일감 기록과 검토 상태를 남기지 않으므로, 기록이 필요한 일은 여전히 업무 게시판으로 보냅니다.

6.3.1 접수 확인 뒤 답이 나중에 오는 Bot 사이 메시지와 답 길이 16,000자 상한

Bot Mode 봇끼리 메시지의 접수 확인과 나중에 오는 답

Bot Mode 봇이 다른 Bot Mode 봇에게 메시지를 보내면 보낸 쪽은 먼저 접수 확인만 받고, 받은 쪽의 답은 처리가 끝난 뒤에 따로 도착합니다[S5]. 보낸 쪽 Bot Mode 봇은 답을 기다리며 멈춰 있지 않고 자기 일을 계속하므로, 재무 Bot Mode 봇에게 이번 분기 예산 범위를 묻는 영업 Bot Mode 봇처럼 답이 조금 늦어도 되는 문의에 맞습니다. 받은 쪽 Bot Mode 봇은 자기 프로파일의 기억과 비밀 정보로 답을 만들기 때문에, 보낸 쪽이 재무 비밀 정보를 직접 보지 않고도 필요한 답만 받을 수 있습니다.

Bot Mode 봇 사이에 일을 넘길 때는 넘길 내용을 메시지에 분명히 적는 것이 원칙입니다. 받은 쪽은 보낸 쪽의 대화 기록이나 기억을 읽지 못하므로, 무엇을 언제까지 어떤 형식으로 돌려받고 싶은지를 메시지 한 통 안에 담아야 엉뚱한 답이 돌아오지 않습니다. 예를 들어 영업 Bot Mode 봇이 「다음 주 제안에 쓸 3분기 예산 범위를 부서별 표로, 금요일까지」라고 적어 보내면 재무 Bot Mode 봇은 추가 질문 없이 자기 자료로 답을 만들 수 있습니다. 이렇게 역할마다 권한과 기억은 따로 두고 넘길 내용만 글로 주고받는 방식이 칸막이를 지키면서 함께 일하는 기본 모양입니다.

Bot Mode 봇 사이 메시지 답 길이 16,000자 상한과 긴 결과물의 전달 방법

Bot Mode 봇끼리 보내는 메시지의 답은 길이 상한이 16,000자이며, 이 상한은 그룹 대화방 메시지에는 해당하지 않고 Bot Mode 봇 사이 직접 메시지의 답에만 적용됩니다. 답이 16,000자를 넘으면 넘는 부분은 잘린 채 도착하고, 얼마나 잘렸는지가 함께 표시됩니다[S5]. 16,000자는 짧은 확인이나 요약물 주고받기에는 충분하지만, 제안서 전체나 긴 검토 보고서를 담기에는 부족할 수 있습니다. 긴 결과물을 주고받는 일은 직접 메시지 대신 업무 게시판 일감에 결과를 남기거나 파일로 전달하는 편이 맞습니다. 정리하면 직접 메시지는 짧은 확인과 문의에, 업무 게시판은 기록과 승인이 필요한 일감에 씁니다.

6.3.2 데스크톱 없이 다른 서버의 Bot 과 주고받는 메시지 연결

Bot Mode 봇은 다른 서버에 있는 Bot Mode 봇과도 데스크톱 앱을 거치지 않고 서로 메시지를 보낼 수 있습니다[S5]. 업무 게시판은 한 서버의 프로파일이 함께 쓰는 게시판이므로, 부서나 지사마다 서버를 따로 둔 조직에서 서버 사이의 문의는 이 연결이 맞습니다. 예를 들어 본사 서버의 영업 Bot Mode 봇이 지사 서버의 엔지니어 Bot Mode 봇에게 장비 재고를 묻고 답을 받을 수 있습니다. 3장에서 다룬 부서별 서버 분리 결정이 AI 동료 사이의 연락을 막지 않으며, 연결 설정 절차는 각 조직의 IT 담당자가 공식 문서를 기준으로 정합니다.

6.4 업무 역할 11개로 구성한 에이전트 팀 운영 사례

2.4.3에서 규모만 소개한 운영 사례를 여기서 구성과 운영 흐름까지 펼쳐 봅니다. 이 기업은 Hermes Agent로 업무 역할 11개를 프로파일 11개로 나누고 역할마다 메신저 봇을 하나씩 연결했습니다. 이 사례는 3장의 프로파일, 4장의 에이전트와 도우미, 5장의 메신저 봇, 이 장의 업무 게시판이 한 조직 안에서 함께 움직이는 모습을 보여 줍니다. 부서마다 자기 AI 동료를 두는 구성이 실제 운영 규모에서 가능하다는 점과, 그 구성에서 사람이 맡는 확인 역할이 어디에 있는지가 드러납니다.

6.4.1 영업·엔지니어·재무·인사·마케팅·성능 관제 등 역할별 프로파일과 메신저 봇 구성

이렇게 쓴다 이 기업은 영업, 엔지니어, 재무, 인사, 마케팅, 성능 관제, 개인 비서, 시장 리포트 등 업무 역할 11개를 각각 프로파일 하나로 만들었습니다. 역할마다 메신저 봇 계정을 하나씩 연결했고, 직원은 평소 쓰는 메신저에서 해당 역할의 메신저 봇을 불러 일을 맡깁니다. 메신저 봇 계정 하나는 프로파일 하나에서만 쓸 수 있고 같은 계정을 두 프로파일이 동시에 쓰지 못하므로, 역할 11개에는 메신저 봇 계정도 11개가 필요합니다[S6]. 이 구성에서 재무 프로파일의 비밀 정보와 기억은 영업 프로파일의 에이전트에게 보이지 않

며, 메신저 앱 안에 재무 메신저 봇과 영업 메신저 봇이 나란히 있어도 두 에이전트는 서로의 기록을 읽지 않습니다[S1].

메신저 봇만 쓰는 구성과 Bot Mode 봇의 관계

이 사례는 역할마다 메신저 봇만 연결했고 Bot Mode 봇은 쓰지 않습니다. 5장에서 본 것처럼 Bot Mode 봇은 데스크톱 앱에서 프로파일을 명단으로 보여 주는 창구이므로, 직원 대부분이 메신저로 일하는 조직은 메신저 봇만으로도 역할별 에이전트 팀을 꾸릴 수 있습니다. Bot Mode를 커더라도 프로파일과 대화 기록, 예약 작업은 그대로 프로파일에 남기 때문에 나중에 창구를 더하는 결정이 기존 구성을 바꾸지 않습니다[S5]. 그래서 시범 팀은 직원이 이미 쓰는 메신저 하나로 시작하고, 창구는 필요해질 때 늘리는 순서가 무리가 없습니다.

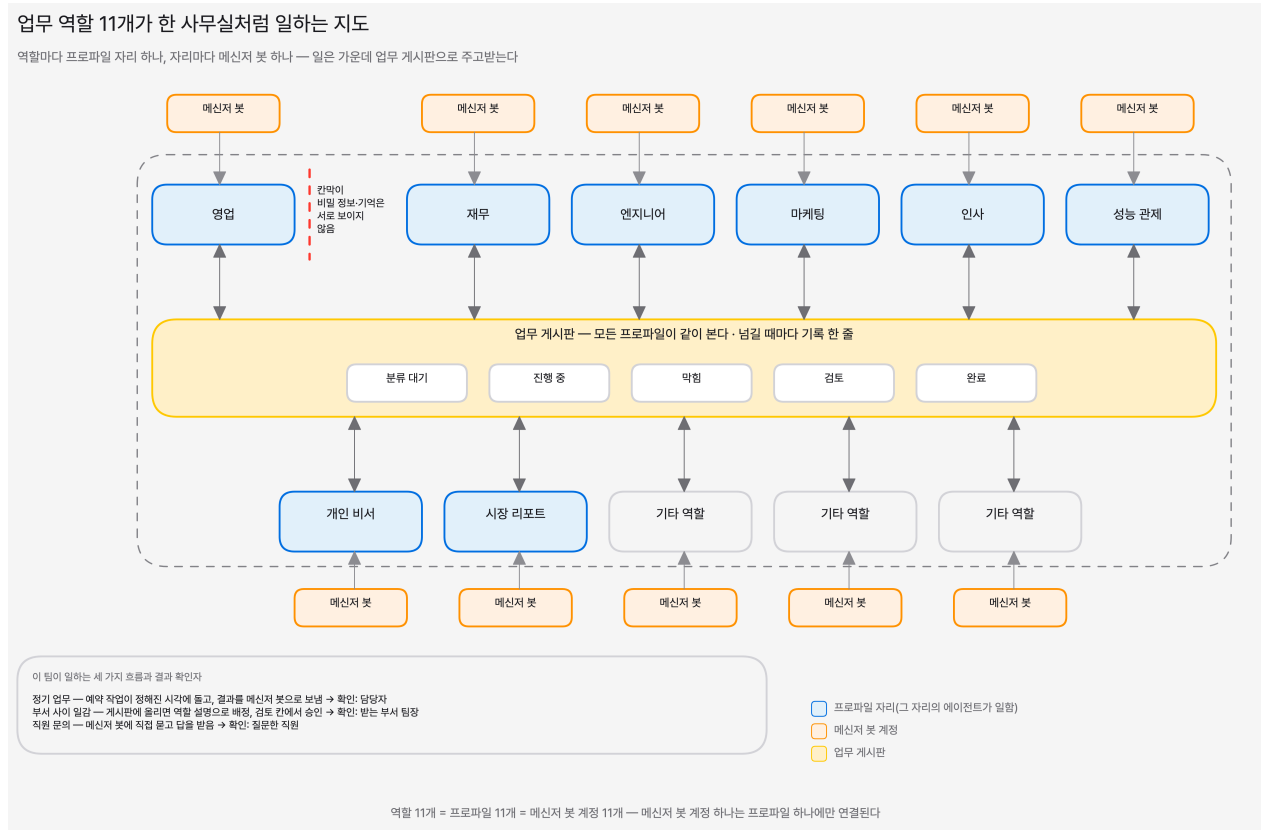


그림. 업무 역할 11개를 프로파일 11개로 나누고 역할마다 메신저 봇 하나를 연결한 뒤 업무 게시판으로 서로 일감을 넘기는 에이전트 팀 구성도

6.4.2 오전 정기 업무와 부서 사이 일감 전달, 결과 확인자로 이어지는 운영 흐름

예약 작업·일감 전달·직원 문의로 나눈 운영 흐름 세 가지

이 기업의 에이전트 팀은 세 가지 흐름으로 운영되며, 흐름마다 시작 신호와 쓰는 기능, 결과를 확인하는 사람이 다릅니다. 첫 번째 흐름에서는 영업 프로파일의 예약 작업이 매일 오전 정해진 시각에 실행되어 입찰 공고를 모아 정리하고, 그 결과를 영업 메신저 봇으로 영업 담당자에게 보냅니다. 두 번째 흐름에서는 한 역할의 에이전트가 다른 부서가 맡아야 할 일감을 업무 게시판에 올리고, 받는 부서의 에이전트가 처리한 결과를 그 부서의 확인자가 검토합니다. 세 번째 흐름은 직원이 메신저 봇에 직접 묻고 답을 받는 일상 문의이며, 질문한 직원이 답을 확인합니다.

흐름	시작 신호	쓰는 기능	결과 확인자
정기 업무(입찰 공고 정리)	예약 작업의 정해진 시각	예약 작업 → 메신저 봇으로 결과 전달	영업 담당자
부서 사이 일감 전달(제안서 기술 검토 등)	업무 게시판에 일감 등록	업무 게시판 배정 → 검토 상태	받는 부서의 팀장
직원 문의	메신저 메시지	역할별 메신저 봇 → 필요 시 도우미	질문한 직원

흐름마다 결과 확인자를 먼저 정하는 운영 원칙

세 흐름의 공통점은 에이전트가 만든 결과를 받는 사람이 흐름마다 미리 정해져 있다는 것입니다. 예약 작업의 결과는 매일 같은 담당자에게 가고, 업무 게시판 일감은 검토 상태에서 받는 부서의 팀장이 승인하며, 직원 문의는 질문한 사람이 답을 판단합니다. 따라서 이 사례를 시범 팀에 옮길 때는 역할 수를 먼저 늘리기보다 업무 하나마다 시작 신호와 결과 확인자를 표 한 줄로 적어 보는 것이 출발점입니다. 업무 게시판은 그 확인 단계를 일감 기록으로 남겨, 나중에 어느 결과를 누가 승인했는지를 되짚을 수 있게 합니다[S3].

기억할 것

1. 업무 게시판은 모든 프로파일이 같이 보는 일감 게시판이고, 역할 설명을 읽고 맞는 프로파일에 일감을 배정합니다.
2. 짧은 일을 바로 받아 이어 가면 도우미, 역할을 넘거나 오래 걸리거나 사람 확인이 필요한 일은 업무 게시판으로 보냅니다.
3. 사람 확인은 일감 흐름 안의 검토 상태에 두고, 흐름마다 결과 확인자를 한 명씩 정합니다.

8장으로 가져갈 질문 우리 조직에서 역할 사이에 넘기는 일은 무엇이고, 그 일의 결과는 어디서 누가 확인하는가?

7장. 에이전트를 옮기고 나눠 줄 때 지키는 비밀 정보 — 내보내기 파일과 배포판의 차이

6장의 운영 사례처럼 역할별 에이전트 팀이 자리를 잡으면, 잘 다듬은 역할을 다른 서버로 옮기거나 지사에도 두자는 요청이 뒤따릅니다. Hermes Agent는 잘 다듬은 역할 하나를 다른 서버로 옮기거나 다른 부서에 나눠 주는 방법으로 프로파일 내보내기 파일, 서버 전체 백업, 프로파일 배포판 세 가지를 제공합니다[S1][S2]. 세 방식은 겉으로 비슷해 보이지만 파일에 담기는 내용과 받는 쪽에서 보존되는 내용이 서로 다릅니다. 내보내기 파일은 프로파일을 있는 그대로 찍은 사본이어서 업무 대화 기록과 기억이 함께 들어가므로, 다른 사람에게 전달하기 전에 무엇이 들어 있는지 확인하는 단계가 반드시 필요합니다[S2]. 따라서 이전·배포 계획에는 방식 선택 기준 한 줄과 내보내기 비밀 정보 점검표 한 장이 함께 있어야 하며, IT 담당자와 결재자는 이 두 가지를 같은 표로 보고 판단할 수 있습니다.

한 줄 요약: 다른 서버로 옮기는 대상은 지금 일하는 직원인 에이전트가 아니라 그 직원의 자리와 기록인 프로파일이며, 다른 팀에 나눠 줄 때는 내보내기 파일 대신 배포판을 씁니다.

7.1 직원 대신 책상과 업무 노트를 옮기는 세 가지 이전 방식

Hermes Agent에서 옮길 수 있는 단위는 프로파일 하나입니다. 프로파일은 설정, 비밀 정보, 성격, 기억, 대화 기록, 스킬, 예약 작업을 역할마다 따로 담아 두는 자리와 기록이고, 에이전트는 그 프로파일을 읽어 지금 일하는 실행 단위입니다[S1]. 에이전트는 대화나 예약 작업이 시작될 때마다 새로 실행되고, 에이전트가 부르는 서버에 이진트(도우미)도 매번 새 대화로 시작하므로 서버를 옮길 때 따로 챙길 대상이 되지 않습니다[S4]. 다만 옮기는 목적이 서버 이전인지, 재해 대비인지, 다른 팀 배포인지에 따라 알맞은 방식이 달라지므로 목적부터 정한 뒤 방식을 고릅니다.

7.1.1 프로파일 하나의 내보내기·가져오기로 하는 서버 이전

쉬운 비유 사무실을 옮길 때 이삿짐에 싣는 것은 책상, 업무 노트, 사원증이고, 새 사무실에서 그 책상에 앉아 일할 직원은 이삿짐에 들어가지 않습니다.

사무실 이사와 같은 구조의 서버 이전

Hermes Agent의 서버 이전도 같은 구조로, 프로파일을 파일 하나로 내보내 새 서버에서 가져오면 그 프로파일을 읽는 에이전트가 새 서버에서 다시 실행됩니다. 3장에서 프로파일을 사원증·책상·업무 노트에 비유한 것처럼, 내보내기 파일에는 역할의 설정과 성격, 스킬, 기억, 대화 기록이 담기고 새 서버에서는 같은 역할이 같은 기억을 가지고 일을 이어 갑니다[S1]. 이전 계획서에 적을 대상은 「영업 담당 에이전트」라는 직원 한 명보다 「영업 담당 프로파일」이라는 책상 하나로 보는 편이 정확합니다.

서버 이전은 직원이 아니라 책상과 업무 노트를 옮기는 이사입니다

책상·업무 노트 = 프로파일 · 일하는 직원 = 에이전트 · 전화와 출입증 = 메신저 봇 연결과 로그인

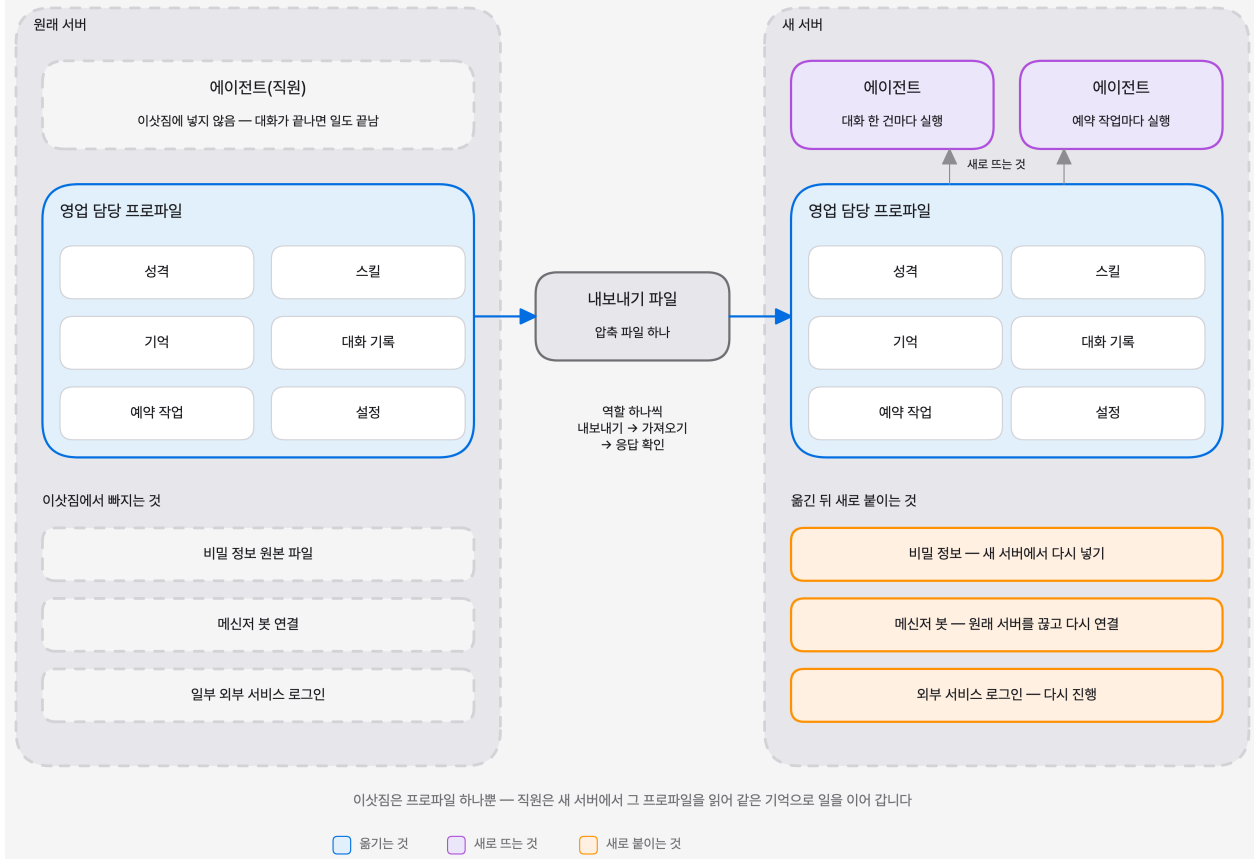


그림. 서버 이전 때 옮기는 프로파일과 새 서버에서 새로 실행되는 에이전트

프로파일 단위로 세우는 서버 이전 계획

프로파일 하나를 단위로 계획을 세우면 이전 범위와 확인 대상을 분명하게 정할 수 있습니다. Hermes Agent 는 프로파일 하나를 압축 파일 하나로 내보내고 새 서버에서 이름을 정해 가져오는 절차를 제공하며, 새 서버에 같은 이름의 프로파일이 이미 있으면 가져오기를 거부합니다[S2]. 새 서버에 같은 이름의 역할이 남아 있지 않은지 먼저 확인하고, 역할 하나를 옮길 때마다 그 역할이 정상으로 응답하는지 확인하는 순서가 안전합니다. 예를 들어 영업·재무·인사 역할 세 개를 옮기는 경우에도 역할별로 내보내기, 가져오기, 응답 확인을 반복하면 문제가 생긴 역할을 바로 찾아낼 수 있습니다.

기본 프로파일과 이름 있는 프로파일의 내보내기 방식

Hermes Agent는 설치할 때 만들어지는 기본 프로파일과 사용자가 이름을 붙여 만든 프로파일을 서로 다른 방식으로 내보냅니다. 기본 프로파일은 정해진 항목만 담은 허용 목록 방식을 쓰고, 이름 있는 프로파일은 폴더의 대부분을 담고 자격 증명 저장소 같은 일부 항목만 뺍니다[S2]. 그래서 이름 있는 프로파일의 내보내기 파일에는 상태 저장소, 로그, 캐시까지 들어가 파일이 커질 수 있습니다. 내보내기 파일을 기본 프로파일로 가져오는 것은 허용되지 않습니다. 그래서 업무 역할은 처음부터 이름 있는 프로파일로 만들어 두는 편이 나중에 옮길 범위를 미리 예측하기 쉽고, 이전 후에도 같은 역할 이름을 그대로 씁니다.

7.1.2 서버 전체 백업과 프로파일 하나 내보내기의 범위 차이

서버 전체 백업이 맡는 재해 대비

서버 전체 백업은 한 서버에 있는 모든 프로파일을 통째로 보존하는 재해 대비용 방식입니다. Hermes Agent 는 대화 기록과 예약 작업까지 포함한 전체 백업이 필요하면 전체 백업 기능이나 프로파일 내보내기를 쓰도록 안내하며, 로컬 모델 실행 파일처럼 다시 내려받을 수 있는 큰 폴더는 백업에서 제외합니다[S1]. 반면 프로파일 하나 내보내기는 역할 하나를 다른 서버로 옮기는 용도이므로 범위가 그 역할의 폴더에 그칩니다. 서버 장애에 대비할 때는 전체 백업을, 역할 하나를 새 서버로 옮길 때는 내보내기를 쓰는 식으로 목적에 따라 나눠 씁니다.

업무 게시판 일감의 이전 범위 확인

업무 게시판(칸반)은 한 서버의 모든 프로파일이 함께 쓰는 공용 일감 게시판입니다[S3]. 이 게시판의 기록이 서버 전체 백업이나 프로파일 하나 내보내기에 포함되는지는 공개 문서에서 확인되지 않으므로, 두 방식 어느 쪽에 서도 포함된다고 가정하지 않습니다. 따라서 게시판에 진행 중인 일감이 있으면 이전 전에 마무리하거나, 새 서버에서 같은 일감을 다시 등록하는 단계를 이전 절차에 넣어 둡니다. 이 단계를 두면 서버를 옮긴 직후 담당 역할이 비어 있는 일감이 생기는 문제를 미리 막을 수 있습니다.

목적별 세 가지 이전 방식 비교

계속 고치면서 여러 곳이 따라 받을 에이전트에는 배포판이 맞고, 한 번 전달하거나 서버를 옮길 때는 내보내기 파일이 맞습니다[S2]. 아래 표는 이 구분에 서버 전체 백업을 더해 세 방식을 목적별로 나란히 놓은 것으로, 행 이름은 방식이 아닌 목적으로 적었습니다.

목적	방식	들어가는 것	빠지는 것	받는 쪽에서 보존되는 것	남에게 줘도 되나
서버 이전	프로파일 하나 내보내기·가져오기	설정, 성격, 스킬, 예약 작업, 기억, 대화 기록, 로그	비밀 정보 원본 파일, 로그인 정보 파일	해당 없음(새로 만들어짐)	열어서 확인한 뒤 조직 내부 이전에만
재해 대비	서버 전체 백업	모든 프로파일의 대화 기록과 예약 작업	다시 내려받을 수 있는 모델 실행 파일	해당 없음(같은 서버로 복원)	아니요(서버 보관용)
다른 팀 배포	배포판(git 저장소)	성격, 스킬, 예약 작업, 외부 도구 연결, 설정	기억, 대화 기록, 비밀 정보, 로그	받는 쪽의 기억·대화 기록·비밀 정보·로그, 설정(기본값)	예(그렇게 설계됨)

출처: [S1][S2]

표에서 결재자가 가장 먼저 볼 열은 마지막 열입니다. 다른 팀에 전달해도 되도록 설계된 방식은 배포판 하나이고, 내보내기 파일과 서버 전체 백업은 업무 기록을 함께 담기 때문에 조직 내부의 이전과 보관에만 씁니다. 이 구분을 승인 기준으로 정해 두면, 지사나 협력 부서가 「에이전트 파일을 하나 보내 달라」고 요청할 때 담당자가 내보내기 파일을 그대로 보내는 일을 막을 수 있습니다.

7.2 다른 팀이 설치하고 업데이트하는 배포판

Hermes Agent의 프로파일 배포판(profile distribution)은 완성된 에이전트 하나를 git 저장소 하나에 담아 다른 팀이 설치하고 업데이트하게 하는 방식입니다[S2]. git 저장소는 고친 내용이 판(버전)마다 기록되는 버전 관리 공유 저장소이므로, 만든 쪽이 스킬이나 성격을 고쳐 새 판을 올리면 받는 쪽은 업데이트 한 번으로 같은 품질의 역할을 이어 받습니다. 잘 다듬은 AI 동료를 여러 부서나 지사에 나눠 줄 때 배포판이 내보내기 파일보다 알맞은 이유는 두 방식이 담는 내용 자체가 다르기 때문입니다.

7.2.1 성격·스킬·예약 작업·설정을 git 저장소 하나로 묶고 받는 쪽 기억은 보존하는 배포판

배포판에 들어가는 다섯 가지와 빠지는 세 가지

배포판에는 역할을 다른 서버에서 똑같이 재현하는 데 필요한 것만 들어갑니다. 성격 정의, 스킬, 예약 작업, 외부 도구 연결 설정, 일반 설정의 다섯 가지가 들어가고, 기억·대화 기록·비밀 정보의 세 가지는 설치 단계에서 제외됩니다[S2]. 설치 프로그램은 비밀 정보 파일과 로그인 정보 파일 같은 자격 증명 저장소, 기억 폴더, 대화 기록, 상태 저장소, 로그를 설치 때 가져오지 않습니다. 새로 배포된 예약 작업은 일시 정지 상태로 설치되므로, 받는 쪽 담당자가 작업 내용을 확인한 뒤 켜는 단계가 기본 절차에 들어갑니다.

배포판 저장소에서 비밀 정보를 빼는 제외 목록

배포판의 제외 규칙은 설치와 업데이트 단계에서만 작동하며, Hermes Agent가 git 저장소 자체를 관리하지는 않습니다[S2]. 배포판을 만드는 쪽은 저장소의 제외 목록 파일에 비밀 정보 파일과 기억·대화 기록 폴더를 적어, 그 파일들이 처음부터 저장소에 올라가지 않게 해야 합니다. 예를 들어 영업 지원 역할을 배포판으로 낼 때 만든 쪽 서버의 모델 접속 키나 고객 기억이 저장소에 함께 올라가면, 받는 쪽 설치 프로그램이 그 파일을 쓰지 않더라도 저장소를 볼 수 있는 사람은 그 내용을 열어 볼 수 있습니다. 배포판을 처음 만들 때 제외 목록을 작성하고 저장소 내용을 한 번 확인하는 단계를 만든 쪽 점검 항목으로 둡니다.

업데이트 때 바뀌는 것과 보존되는 것

배포판의 가장 큰 특징은 업데이트할 때 받는 쪽 데이터를 건드리지 않는다는 점입니다. 성격 정의와 외부 도구 연결 설정처럼 배포판이 소유한 파일은 새 판으로 바뀌고, 스킬은 항목별로 합쳐지며, 예약 작업은 작업 식별자 기준으로 합쳐져 받는 쪽이 추가한 작업과 켜고 끈 상태가 그대로 유지됩니다[S2]. 반면 기억, 대화 기록, 로그인 정보, 비밀 정보 파일, 로그, 상태 저장소는 업데이트 대상에서 빠집니다. 일반 설정은 기본적으로 받는 쪽 값이 보존되고, 배포판 쪽 설정으로 덮어쓰려면 업데이트할 때 별도 선택 옵션을 지정해야 합니다.

업데이트 때 새 판으로 바뀌는 것	업데이트가 건드리지 않는 것
성격 정의, 외부 도구 연결 설정	기억, 대화 기록
스킬(항목별로 합침)	비밀 정보 파일, 로그인 정보
예약 작업(작업별로 합침, 켜고 끈 상태 유지)	로그, 상태 저장소
일반 설정(선택 옵션을 지정한 경우만)	일반 설정(기본값은 받는 쪽 값 유지)

출처: [S2]

이 표의 오른쪽 열이 배포판과 내보내기 파일을 가르는 핵심입니다. 배포판은 남에게 줘도 되는 것만 담고, 업데이트를 거듭해도 받는 쪽이 쌓은 기억과 비밀 정보는 받는 쪽 서버에만 남습니다. 즉 만든 쪽의 개선은 계속 전달되고 받는 쪽의 업무 기록은 한 번도 만든 쪽으로 넘어가지 않습니다.

7.2.2 본사가 다듬은 영업 지원 에이전트를 지사가 설치하고 업데이트하는 예

예를 들면: 본사가 3장의 「영업 담당」 프로파일을 다듬어 입찰 공고 정리 스킬, 경쟁사 조사 스킬, 매주 정해진 시각에 실행되는 시장 동향 예약 작업을 갖춘 「영업 지원 에이전트」로 완성한 경우입니다. 본사는 이 프로파일을 배포판으로 만들어 사내 git 저장소에 올리고, 지사 IT 담당자는 저장소 주소 하나로 설치합니다. 설치 직후 지사의 영업 지원 에이전트에는 본사가 다듬은 성격과 스킬이 그대로 들어오지만 기억과 대화 기록은 비어 있고, 모델 접속 키 같은 비밀 정보는 지사가 자기 계정으로 새로 넣습니다. 이후 본사가 경쟁사 조사 스킬을 고쳐 새 판을 올리면 지사는 업데이트만 실행하고, 그동안 쌓인 지사 고객 기억과 지사 비밀 정보는 그대로 남습니다[S2].

본사의 품질 관리와 지사의 데이터 관리 분업

배포판을 쓰면 본사는 역할의 품질을 책임지고 지사는 자기 데이터를 책임지는 분업이 생깁니다. 배포판에 담기는 내용이 남에게 줘도 되는 것뿐이므로, 본사가 지사 고객 기억을 받아 볼 일도 지사가 본사 비밀 정보를 받을 일도 생기지 않습니다. git 저장소에는 판마다 태그와 변경 기록이 남아, 어느 지사가 어느 판을 기준으로 설치했는지 추적할 수 있습니다[S2]. 배포판을 쓰면 잘 만든 에이전트를 통째로 다른 팀으로 옮기는 일이 개인 간 파일 전달이 아닌, 판 관리가 되는 배포 업무로 바뀝니다.

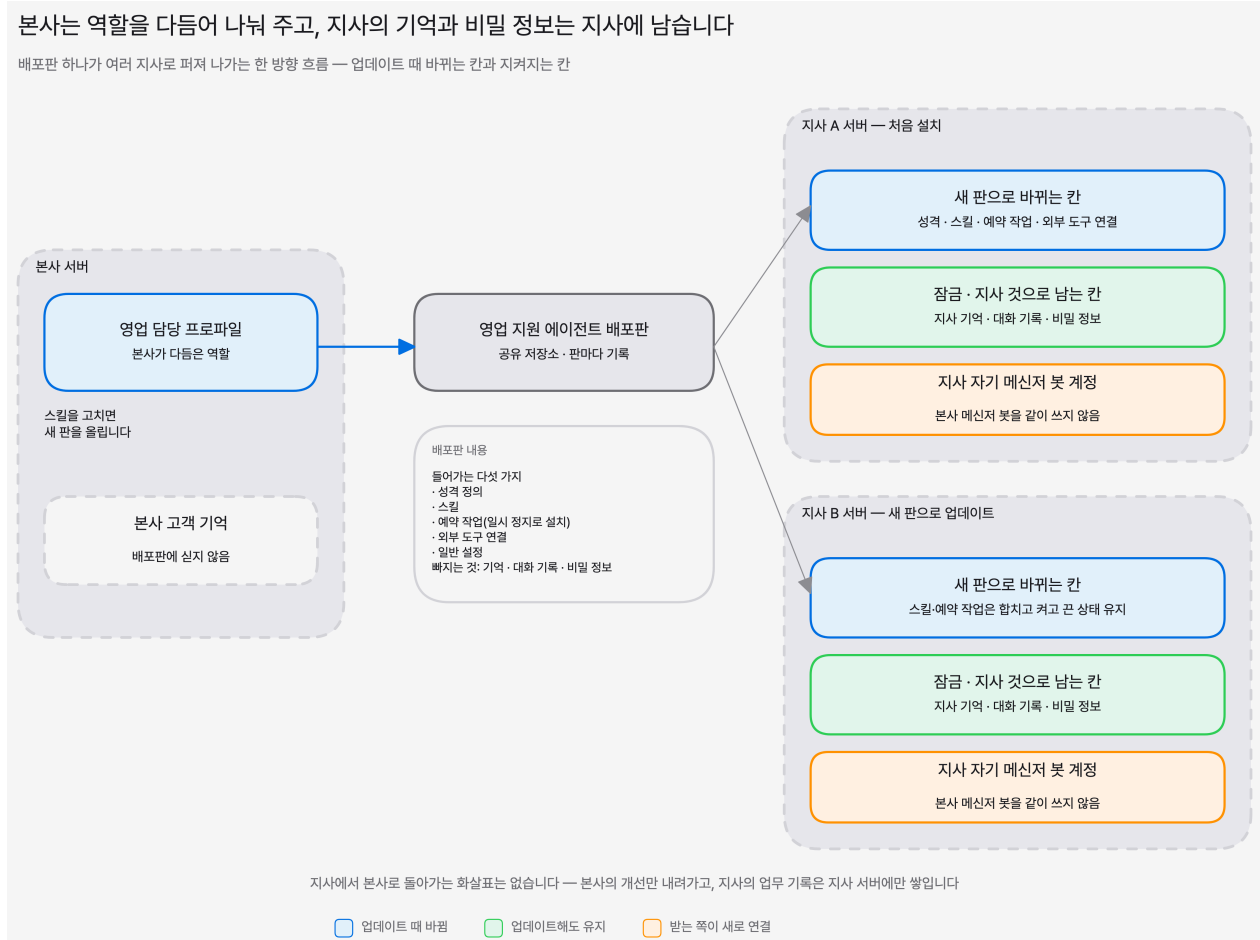


그림. 본사가 만든 배포판을 지사가 설치하고 업데이트하는 흐름

지사의 메신저 봇과 Bot Mode 봇 연결

배포판으로 받은 역할을 지사 직원이 부르려면 지사가 자기 창구를 새로 연결해야 합니다. 메신저 봇 하나는 프로파일 하나에만 연결되고 같은 메신저 봇 토큰을 두 프로파일이 동시에 받을 수 없으므로, 지사는 본사의 메신저 봇을 함께 쓰지 않고 자기 메신저 봇 계정을 만들어 연결합니다[S6]. 한편 Bot Mode 봇은 프로파일을 이름 있는 목록 항목으로 보여 주는 창구일 뿐 데이터를 따로 가지지 않습니다[S5]. 지사가 같은 역할을 메신저 봇으로 부르든 Bot Mode 봇으로 부르든, 배포판으로 받은 성격과 지사에서 쌓인 기억은 같은 프로파일 하나에 남습니다.

7.3 내보내기 파일에 들어가는 것과 넘기기 전 비밀 정보 점검

Hermes Agent의 내보내기 파일은 프로파일을 압축 파일 하나로 짊어지는 사본이며, 정리해서 내놓는 배포용 판이 아닌 있는 그대로의 사본입니다[S2]. 서버를 옮길 때는 이 성질 덕분에 같은 역할이 같은 기억으로 일을 이어가지만, 파일을 다른 사람에게 전달하면 업무 대화와 기억도 함께 전달됩니다. 따라서 내보내기 비밀 정보 점검은 선택 단계로 두지 않고 이전 절차의 정해진 단계로 넣으며, 그 점검은 무엇이 들어가는지 알고, 전달 전에 열어 확인하고, 옮긴 뒤 다시 연결하는 세 단계로 이루어집니다.

7.3.1 대화 기록·기억이 함께 담기는 있는 그대로의 사본

내보내기 파일에 포함되는 대화 기록·기억·로그

이름 있는 프로파일을 내보내면 프로파일 폴더의 대부분이 그대로 들어갑니다. 비밀 정보 원본 파일과 로그인 정보 파일 같은 자격 증명 저장소는 제외되지만, 대화 기록, 기억, 사용자에 대한 메모, 로그, 예약 작업은 포함되고 데스크톱 화면의 테마와 배치 정보까지 함께 담깁니다[S2]. 내보내기 파일 하나에 그 역할이 지금까지 나눈 업무 대화와 고객·거래처에 대해 기억한 내용이 모두 들어 있을 수 있습니다. 예를 들어 영업 담당 프로파일의 내보내기 파일에는 입찰 공고를 정리하며 나눈 대화와 경쟁사 조사 결과가 기억으로 남아 있을 수 있으므로, 이 파일은 설정 파일보다 업무 기록에 가까운 민감 자료로 분류해 보관하고 전달합니다.

내보내기 파일에 포함되는 것	내보내기 파일에서 제외되는 것
설정, 성격 정의, 스킬, 예약 작업	비밀 정보 원본 파일
기억, 사용자에 대한 메모	로그인 정보 파일 등 자격 증명 저장소
대화 기록, 로그, 상태 저장소, 캐시	Hermes Agent가 스스로 남기는 자격 증명 복구용 사본(최신 버전)
데스크톱 화면 테마와 배치	—

출처: [S2]

개인 정보 검사 없이 만들어지는 내보내기 파일

내보내기 기능은 파일 이름으로 자격 증명을 거를 뿐 파일 안의 내용은 검사하지 않습니다. 대화 기록 안에 개인 연락처나 계약 금액이 적혀 있어도 그대로 들어가며, Hermes Agent 공식 안내도 공유하기 전에 압축 파일의 목록을 열어 무엇이 들어 있는지 확인하도록 권합니다[S2]. 내보내기 파일을 만드는 담당자와 전달 전에 내용을 확인하는 담당자를 미리 정해 두면 점검 단계가 빠지지 않습니다. 확인 담당자는 파일 목록에 기억·대화 기록 폴더가 들어 있는지와 받는 쪽이 그 기록을 받아도 되는 대상인지를 함께 판단합니다.

받는 쪽 범위에 따라 달라지는 내보내기 파일 처리

내보내기 파일을 받는 쪽이 같은 역할을 운영할 같은 조직의 새 서버라면, 대화 기록과 기억이 함께 가는 것이 오히려 이전의 목적에 맞습니다. 반면 받는 쪽이 다른 부서나 지사라면 그 대화 기록과 기억은 받는 쪽에 필요하지 않은 정보이며, 고객 정보가 섞여 있으면 정보 보호 기준에 따라 전달 여부를 따로 판단해야 합니다. 내보내기 파일은 받는 쪽 범위를 기준으로 처리를 달리합니다. 조직 내부의 서버 이전이면 확인 후 전달하고, 다른 팀이면 내보내기 파일을 쓰지 않고 7.2절의 배포판으로 바꿉니다.

7.3.2 파일 이름으로 거르는 방식이라 가려지지 않을 수 있는 백업 사본과 일부 인증 파일

파일 이름 목록으로 거르는 비밀 정보

Hermes Agent 공식 안내는 모델 접속 키가 내보내기 파일에 들어가지 않아 서버를 떠나지 않는다고 설명하면서, 같은 안내에서 자격 증명은 파일 이름으로 거르고 내용은 거르지 않는다고 밝힙니다[S2]. 두 설명은 거르는 방식의 한계를 함께 보여 줄 뿐 서로 어긋나지 않습니다. 정해진 이름의 비밀 정보 파일은 확실히 빠지지만, 그 이름 목록에 없는 파일은 안에 비밀 값이 들어 있어도 거르는 대상이 되지 않기 때문입니다. 이 방식의 보호 범위는 비밀 정보가 정해진 이름의 파일에만 들어 있다는 전제가 지켜질 때까지만 효과가 있습니다.

v0.21.0에서 가려지지 않을 수 있는 백업 사본과 인증 파일

Hermes Agent v0.21.0 기준으로는 이 한계 때문에 비밀 정보 파일을 손으로 복사해 둔 백업 사본처럼 이름이 다른 파일과 일부 외부 서비스 인증 파일이 가려지지 않은 채 내보내기 파일에 들어갈 수 있습니다. 다른 일부 설정 파일은 비밀 값이 가려진 채 들어가므로, 같은 내보내기 파일 안에서도 파일마다 처리 결과가 다릅니다. 최신 공식 안내는 Hermes Agent가 스스로 남기는 자격 증명 복구용 사본(백업 폴더와 비밀 정보 파일의 백업 사본 등)을 두 종류 프로파일 모두에서 뺀다고 적고, 사용자가 직접 이름을 붙여 만든 설정 사본은 원래 설정 파일처럼 비밀 값을 가린 채 담는다고 적습니다[S2]. 같은 안내가 거르는 기준은 여전히 파일 이름이고 내용은 아니라고 밝히므로, 어느 버전이든 걸러지는 범위는 이름 규칙에 달려 있습니다[S2]. 버전마다 걸러지는 파일이 다르다는 점이 결론이며, 그래서 쓰는 버전에서 만든 내보내기 파일을 직접 열어 확인하는 단계를 점검표에 둡니다. 외부 기억 서비스의 설정 파일에는 그 서비스의 접속 키가 들어 있을 수 있어, 가져온 뒤 해당 기억 서비스 설정을 다시 하도록 안내하고 있습니다[S2].

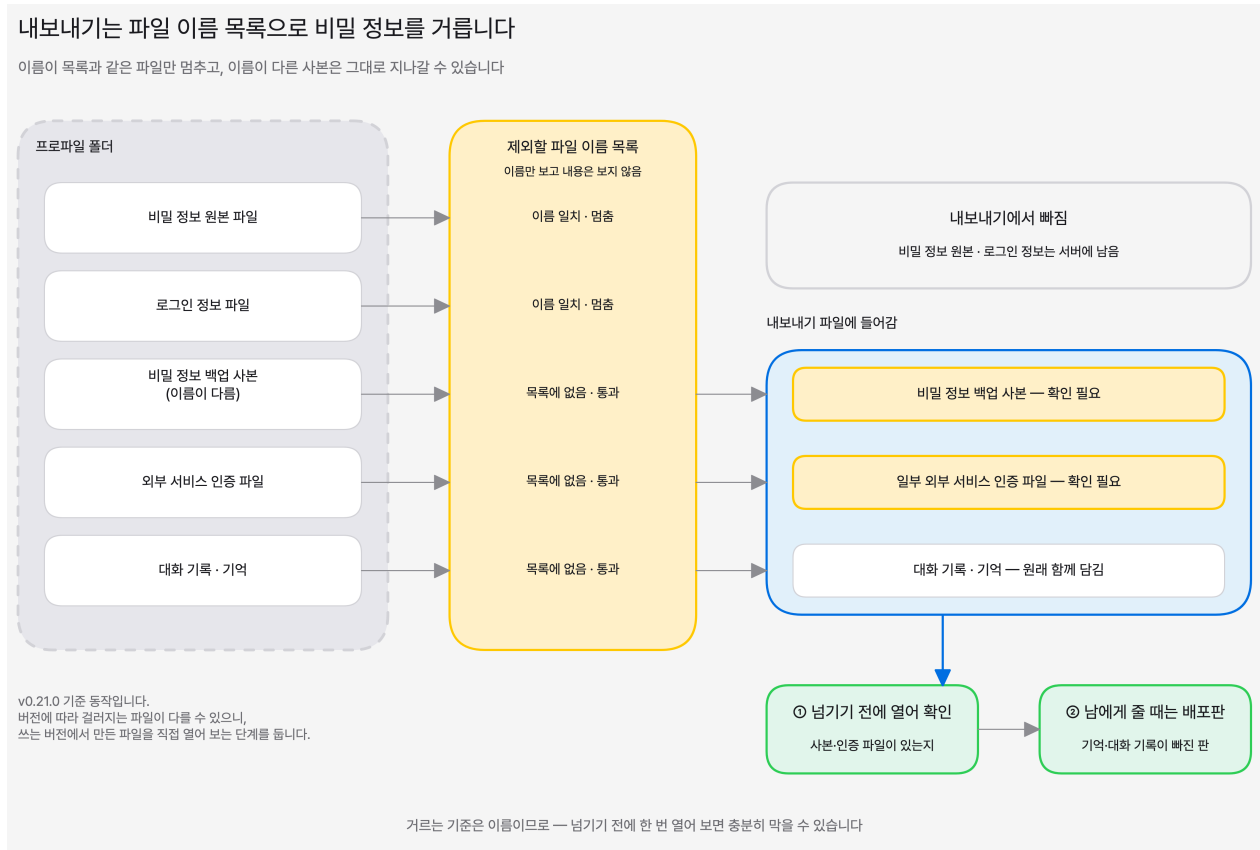


그림. 파일 이름 목록으로 비밀 정보를 거르는 내보내기 방식

운영 버전과 무관하게 두는 두 가지 점검 단계

운영 중인 Hermes Agent 버전이 무엇이든 같은 점검을 두면 버전 차이를 일일이 따지지 않아도 됩니다. 점검의 첫 단계는 내보내기 전에 프로파일 폴더 안의 비밀 정보 백업 사본과 쓰지 않는 인증 파일을 지우는 정리이고, 두 번째 단계는 만든 내보내기 파일의 목록을 열어 남은 비밀 정보가 없는지 확인하는 검사입니다. 예를 들어 설정을 바꾸기 전에 비밀 정보 파일을 복사해 둔 사본이 프로파일 폴더에 남아 있으면, 첫째 단계에서 그 사본을 지우고 둘째 단계에서 파일 목록에 사본이 없는지 다시 확인합니다. 이 두 단계를 7.4.2의 점검표에 고정 항목으로 넣고, 확인 담당자가 서명한 뒤에만 파일을 전달합니다.

7.3.3 옮긴 뒤 새로 연결하는 메신저 봇 계정과 일부 로그인

메신저 봇 계정과 일부 로그인의 재연결

메신저 봇 계정과 일부 외부 서비스 로그인도 프로파일을 옮겨도 함께 복제되지 않습니다. Hermes Agent는 프로파일을 복제할 때 메신저 봇 계정 토큰과 채널 설정을 빼고 복사하며, 한 번 쓰면 바뀌는 갱신 토큰을 쓰는 일부 외부 서비스 로그인도 복제본에서 제외합니다[S1]. 따라서 새 서버에서는 해당 역할의 메신저 봇을 다시 연결하고, 필요한 외부 서비스 로그인을 그 프로파일에서 새로 진행해야 합니다. 최신 버전에는 프로파일을 복제할 때 메신저 연결까지 함께 복제하는 선택 옵션이 추가되었지만, 기본 동작은 여전히 메신저 연결을 뺀 복제입니다[S1].

원래 서버와 새 서버의 같은 메신저 봇 동시 연결 방지

메신저 봇 하나는 프로파일 하나에만 연결되고, 같은 메신저 봇 토큰을 두 프로파일이 동시에 받을 수 없습니다 [S6]. 5장에서 다룬 이 규칙은 서버 이전에도 그대로 적용되므로, 새 서버에 메신저 봇을 연결할 때는 원래 서버가 그 메신저 봇의 메시지를 더 받지 않는 상태여야 합니다. 원래 서버가 계속 같은 메신저 봇에 연결되어 있으면 메시지 수신에 충돌해 한쪽 서버의 에이전트가 응답하지 못할 수 있고, 두 서버의 대화 기록도 서로 다른 내용으로 쌓입니다. 이전 절차에는 원래 서버의 수신 중지, 새 서버 연결, 시험 메시지로 응답 확인을 하나의 작업 단위로 넣어 둡니다.

7.4 남에게 줄 때는 배포판, 서버를 옮길 때는 내보내기 — 방식 선택과 이전 전 점검표

Hermes Agent의 배포판과 내보내기 파일은 쓰임새가 분명히 나뉩니다. 배포판은 오래 유지하며 계속 고쳐 나가는 방식이고, 내보내기 파일은 준비 작업 없이 한 번에 빠르게 전달하는 방식입니다[S2]. 의사결정권자가 승인할 기준을 한 줄로, IT 담당자가 실행할 절차를 점검표 한 장으로 정해 두면 이전·배포 요청이 들어올 때마다 같은 판단을 같은 순서로 반복할 수 있습니다.

7.4.1 한 번 넘기는 내보내기와 계속 고쳐 나눠 주는 배포판의 선택 기준

오래 가는 배포판과 빠른 내보내기 파일

Hermes Agent 공식 안내는 배포판을 오래 가는 방식으로, 내보내기 파일을 빠른 방식으로 구분합니다[S2]. 배포판은 저장소 준비와 제외 목록 작성 같은 초기 작업이 필요한 대신 판마다 기록이 남고 업데이트 명령 하나로 새 판이 여러 곳에 전달됩니다. 반면 내보내기 파일은 준비 작업 없이 바로 만들 수 있지만 판 관리가 없어 고칠 때마다 파일을 다시 보내야 하고, 대화 기록과 기억이 함께 담깁니다. 따라서 다른 팀에 나눠 주는 요청에는 배포판을 승인하고, 같은 조직 안에서 서버를 옮기거나 한 번만 전달하는 요청에는 확인을 거친 내보내기 파일을 승인하는 것이 승인 기준 한 줄이 됩니다.

배포판과 내보내기 파일을 함께 쓰는 구성

두 방식은 서로를 대신하지 않고 함께 쓸 수 있습니다[S2]. 예를 들어 본사가 배포판으로 영업 지원 역할을 나눠 준 뒤 지사가 자기 서버를 새 장비로 옮길 때는, 지사 안에서 그 프로파일을 내보내기 파일로 옮기면 지사 고객 기억까지 그대로 이어집니다. 이 경우 내보내기 파일은 지사 조직 안에서만 쓰이므로 7.3절의 점검을 거치면 되고, 본사는 계속 배포판으로 새 판을 전달합니다. 선택 기준은 방식 하나를 고르는 문제보다 받는 쪽이 같은 조직인지 다른 팀인지를 먼저 가르는 문제입니다.

상황	방식	이유
다른 부서·지사에 같은 역할을 나눠 줌	배포판	기억·대화 기록·비밀 정보가 담기지 않고, 받는 쪽 데이터가 업데이트에도 보존됨
계속 고치며 여러 곳이 같은 판을 따라 받음	배포판	판마다 기록이 남고 업데이트 명령으로 개선을 전달
같은 조직 안에서 서버를 옮김	내보내기 파일	기억과 대화 기록까지 옮겨야 같은 상태로 일을 이어 감
한 번만 전달하는 역할	내보내기 파일	저장소 준비 없이 바로 만들 수 있음

상황	방식	이유
서버 장애에 대비한 보관	서버 전체 백업	모든 프로파일의 대화 기록과 예약 작업을 함께 보존

출처: [S1][S2]

7.4.2 내보내기·가져오기·배포판 설치의 최소 명령과 이전 전 점검표

이렇게 쓴다: 프로파일 내보내기·가져오기·배포판 설치 명령

Hermes Agent에서 프로파일을 옮기고 나눠 주는 명령은 세 줄이면 충분합니다. 첫 줄은 원래 서버에서 프로파일 하나를 압축 파일로 내보내고, 둘째 줄은 새 서버에서 그 파일을 같은 이름의 프로파일로 가져오며, 셋째 줄은 다른 팀이 배포판 저장소 주소로 역할을 설치합니다[S2]. 배포판을 받은 쪽은 이후 새 판이 나오면 업데이트 명령 하나로 받으며, 이때도 받는 쪽의 기억과 비밀 정보는 보존됩니다.

```
hermes profile export sales-support
hermes profile import sales-support.tar.gz --name sales-support
hermes profile install <배포판 저장소 주소>
```

이전·배포 전 점검표 여섯 항목

점검표는 앞 항목이 끝나야 다음 항목으로 넘어가는 순서이며, 각 항목은 결재 양식의 확인란 하나에 대응합니다. 셋째와 넷째 항목은 내보내기 파일을 쓸 때 빠뜨리기 쉬운 단계이므로 확인 담당자의 서명을 따로 받습니다.

1. 목적 확인: 서버 이전, 재해 대비, 다른 팀 배포 가운데 무엇인지 적습니다.
2. 방식 선택: 다른 팀 배포는 배포판, 서버 이전은 내보내기 파일, 재해 대비는 서버 전체 백업으로 정합니다.
3. 백업 사본 정리: 프로파일 폴더에 남은 비밀 정보 백업 사본과 쓰지 않는 인증 파일을 지웁니다.
4. 파일 열어 확인: 확인 담당자가 내보내기 파일의 목록을 열어 대화 기록, 기억, 인증 파일이 받는 쪽에 가도 되는지 판단합니다.
5. 메신저 재연결: 새 서버의 프로파일에 메신저 봇과 필요한 외부 서비스 로그인을 다시 연결하고 시험 메시지로 응답을 확인합니다.
6. 원래 서버 연결 끊기: 원래 서버의 같은 메신저 봇 연결을 해제하고, 전달에 쓴 내보내기 파일을 지워 같은 역할이 두 곳에서 실행되지 않게 합니다.

이 점검표는 배포판에도 그대로 쓸 수 있습니다. 배포판에서는 셋째 항목이 저장소 제외 목록 확인으로, 넷째 항목이 저장소에 올라간 파일 목록 확인으로 바뀌고, 다섯째 항목은 받는 쪽이 자기 메신저 봇 계정을 새로 만들어 연결하는 단계가 됩니다[S6]. 따라서 IT 담당자는 하나의 점검표로 서버 이전과 다른 팀 배포를 모두 처리하고, 의사결정권자는 둘째 항목의 방식 선택과 넷째 항목의 확인 서명만 보고 승인할 수 있습니다.

기억할 것

- 다른 서버로 옮기는 대상은 지금 일하는 에이전트가 아니라 자리와 기록인 프로파일이며, 이전 계획은 프로파일 단위로 세웁니다.

- 다른 부서나 지사에 역할을 나눠 줄 때는 받는 쪽의 기억과 비밀 정보를 보존하는 배포판을 씁니다.
- 내보내기 파일에는 대화 기록과 기억이 함께 들어가므로, 전달하기 전에 확인 담당자가 파일을 열어 점검합니다.

8장으로 가져갈 질문 잘 다듬은 역할을 다른 팀이나 지사에 나눠 줄 계획이 있는가, 그리고 내보내기 파일을 전달하기 전에 누가 열어 점검하는가. 이 의사결정 질문의 답이 8장 시범 팀 설계표의 「배포 방식」과 「확인 담당자」 칸이 됩니다.

8장. 우리 조직의 첫 에이전트 팀 — 반복 업무 3개로 꾸리는 시범 도입과 MSAP.ai AAS

1~7장에서 나눈 구분을 한 문장으로 모으면 다음과 같습니다. Hermes Agent는 업무 역할 하나를 프로파일 하나로 나누고, 그 프로파일의 설정으로 일감마다 에이전트를 실행하며, 메신저 봇이나 Bot Mode 봇을 부르는 창구로 연결하는 구조입니다[S1]. 이 세 가지 구분은 조직이 첫 에이전트 팀을 설계할 때 그대로 설계 양식이 됩니다. 다만 처음부터 모든 부서에 에이전트를 두면 어느 역할에서 무엇이 잘못됐는지 가려내기 어려우므로, 가장 단순한 구성으로 시작해 필요할 때만 복잡하게 만드는 편이 안전합니다[S7]. 이 장에서는 반복 업무 3개로 시범 팀을 종이에 그리는 양식, 창구·결과 확인자를 정하는 기준, 2주 시범 운영의 확인 항목, 1~7장에서 모은 의사결정 질문 묶음을 한곳에 정리했습니다. 장을 다 읽으면 종이 한 장에 시범 팀을 그리고, 업무마다 창구와 결과 확인자를 정해 시범 도입 검토 목록에 올릴 수 있습니다.

한 줄 요약 매일 되풀이되는 업무 3개를 골라 업무 하나에 프로파일 하나를 두고, 부르는 창구와 결과 확인자를 정한 다음 2주 동안 운영해 보고 넓힐지를 정합니다.

쉬운 비유 회사는 새 팀을 꾸릴 때 사람을 뽑기 전에 책상과 업무 설명서, 연락 창구, 결재자부터 정합니다. 에이전트 팀에서는 프로파일이 책상과 업무 노트에 해당하고, 역할 설명 두 줄이 업무 설명서, 메신저 봇이나 콘솔이 연락 창구, 결과 확인자가 결재자에 해당합니다.

첫 에이전트 팀은 네 단계로 꾸립니다

날짜가 아니라 순서 — 업무 3개 · 프로파일 3개 · 확인자 3명으로 시작해, 같은 확인표로 다음을 정합니다

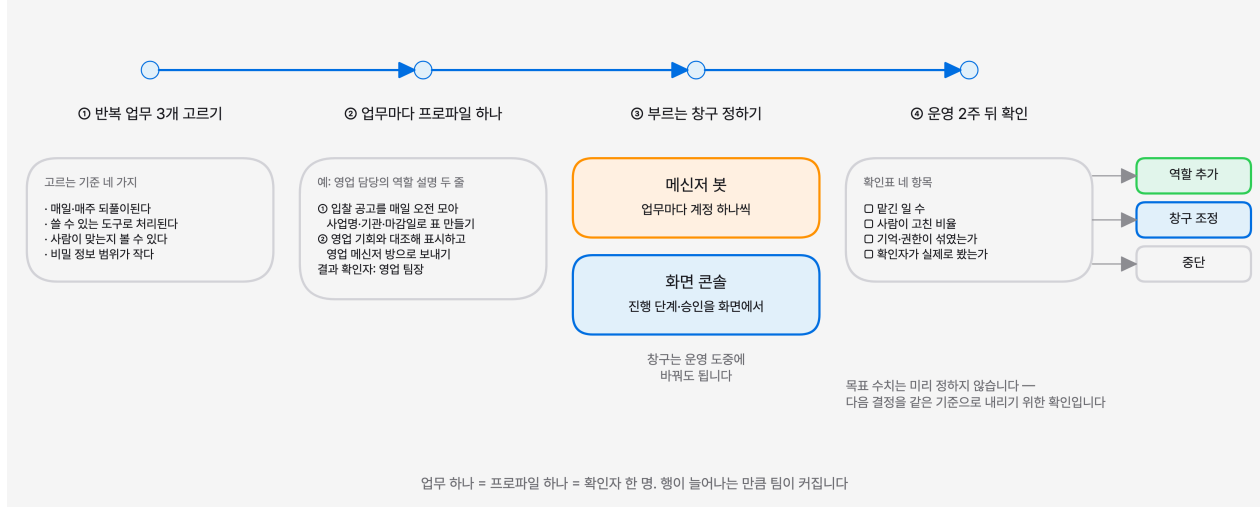


그림. 반복 업무 3개에서 출발하는 에이전트 팀 시범 도입 4단계

8.1 반복 업무 3개와 「업무 하나 = 프로파일 하나」로 그리는 종이 위의 시범 팀

시범 도입의 첫 두 단계는 말길 업무를 고르고 업무마다 프로파일 하나를 배정하는 일입니다. Hermes Agent의 프로파일은 성격·AI 모델·스킬·비밀 정보·기억·대화 기록·예약 작업을 각자 따로 가지는 독립 단위입니다[S1].

그래서 업무 하나에 프로파일 하나를 두면 업무마다 무엇을 맡기고 무엇을 보게 할지가 프로파일 경계와 그대로 일치하고, 서버를 준비하기 전에 종이 한 장으로 시범 팀의 구성이 정해집니다.

8.1.1 매일 되풀이되고 결과를 사람이 확인할 수 있는 업무 3개의 선정 기준

시범 업무 선정 기준 네 가지

첫 시범 팀에 올릴 업무는 다음 네 가지 조건을 함께 만족하는 업무에서 고릅니다.

- 매일 또는 매주 같은 형태로 되풀이됩니다.
- 검색, 문서, 메신저, 업무 시스템 조회처럼 에이전트가 쓸 수 있는 도구로 처리할 수 있습니다.
- 결과물을 사람이 보고 맞는지 틀린지 판단할 수 있습니다.
- 다루는 비밀 정보의 범위가 작고, 조회 권한만으로 일을 끝낼 수 있습니다.

첫째 조건은 예약 작업과 이어집니다. 프로파일은 정해진 시각에 스스로 실행되는 예약 작업을 가지므로 되풀이 되는 업무일수록 사람이 매번 요청하지 않아도 에이전트가 일을 시작합니다[S1]. 넷째 조건은 프로파일 칸막이의 한계에서 나옵니다. Hermes Agent 공식 문서는 프로파일이 에이전트를 격리 공간(샌드박스)에 가두지 않는다고 밝히므로, 같은 서버에 있는 파일 접근까지 프로파일이 막아 주지는 않습니다[S1]. 따라서 첫 시범에서는 접속 정보가 적고 조회만 하는 업무를 먼저 고르는 편이 운영 부담이 작습니다.

부서별 시범 업무 후보 점검표

다음 표는 1장에서 본 부서별 반복 업무와 같은 틀로 후보를 늘어놓은 예시입니다. 조직마다 업무 구성이 다르므로 이 표는 권고 목록이 아니며, 자기 조직의 업무를 같은 열에 채워 넣어 비교하는 용도로 씁니다.

부서	후보 업무	되풀이 주기	쓰는 도구	결과 확인자	비밀 정보 범위
영업	입찰 공고를 모아 사업명·기관·마 감일로 표 만들기	매일	검색·문서·메 신저	영업 팀장	작음(공개 공고 조회)
마케팅	웹·검색 지표를 모아 주간 보고 초안 만들기	매주	지표 조회·문서	마케팅 담당자	중간(지표 서비 스 읽기 권한)
IT 운영	서버 정기 점검 결과를 모아 메신 저로 보고하기	매일	모니터링 조회· 메신저	운영 담당자	중간(조회 권한)
재무	월 손익 자료를 모아 정리표 만들 기	매월	회계 시스템 조회 · 문서	재무 담당자	큼(회계 시스템 접속 정보)
인사	지원서를 채용 기 준표와 대조해 1 차 분류하기	채용 기간 매일	문서	채용 담당자	큼(지원자 개인 정보)

표의 재무·인사 업무는 되풀이 주기도 분명하고 결과를 확인하기도 쉽지만 비밀 정보 범위가 큼니다. 이런 업무는 첫 3개에서 빼 두었다가, 시범 운영에서 기억과 권한이 섞이지 않는다는 점을 확인한 뒤 두 번째 차례에 올리

는 편이 판단 근거를 쌓기에 좋습니다.

업무 3개로 시작하는 시범 범위

업무를 3개로 정하는 이유는 칸막이를 확인할 수 있는 가장 작은 규모이기 때문입니다. 업무가 하나뿐이면 역할 사이에 기억이나 비밀 정보가 섞이는지를 볼 대상이 없고, 다섯 개를 넘기면 결과가 나뉘었을 때 어느 역할의 설정이 원인인지 가려내기 어렵습니다. Anthropic은 에이전트를 설계할 때 가장 단순한 방법을 찾고 필요할 때만 복잡도를 높이라고 권합니다[S7]. 또한 모두가 같은 맥락을 공유해야 하거나 에이전트끼리 주고받는 의존이 많은 일은 아직 여러 에이전트로 나누기에 잘 맞지 않으므로[S8], 고른 3개 업무는 서로 결과를 기다리지 않고 따로 끝나는 업무로 맞춥니다.

8.1.2 프로파일마다 역할 설명 두 줄과 결과 확인자 한 명을 적는 설계표

예를 들면 3장의 「영업 담당」 프로파일을 견본 행으로 두고, 나머지 행에 우리 조직의 업무를 채웁니다.

시범 팀 설계표의 견본 행과 빈 행

설계표는 업무, 프로파일 이름, 역할 설명 두 줄, 프로파일에 담을 비밀 정보 범위, 결과 확인자 다섯 칸으로 구성합니다. 견본 행은 1장의 입찰 공고 정리 업무를 맡은 「영업 담당」 프로파일이고, 아래 세 행은 독자 조직이 8.1.1에서 고른 업무를 적는 빈칸입니다.

업무	프로파일	역할 설명 두 줄	담을 비밀 정보 범위	결과 확인자
매일 입찰 공고 정리	영업 담당	① 공공 조달 사이트의 입찰 공고를 매일 오전 모아 사업명·기관·마감일·예산으로 표를 만든다. ② 고객 관리 시스템의 영업 기회와 대조해 검토할 만한 공고에 표시하고 영업 메신저 방으로 보낸다.	조달 사이트 조회, 고객 관리 시스템 읽기 권한	영업 팀장
(업무 1)				
(업무 2)				
(업무 3)				

역할 설명 두 줄이 정하는 일감 배정 정확도

역할 설명 두 줄은 사람에게 보여 주는 소개 문구 이상의 일을 합니다. Hermes Agent의 업무 게시판(칸반)은 모든 프로파일이 함께 쓰는 일감 게시판이며, 큰 일을 나누는 자동 분해 기능이 프로파일 명단과 역할 설명을 읽고 맞는 담당 프로파일에 일감을 보냅니다[S3]. 역할 설명이 없어도 프로파일 이름만으로 배정은 이루어지지만 정확도가 떨어집니다[S3]. 따라서 역할 설명은 IT 담당자가 아니라 그 업무를 실제로 하는 담당자가 「무엇을 모아서 무엇으로 만든다」와 「누구에게 어떻게 보낸다」 두 줄로 쓰는 편이 배정 결과가 정확합니다.

결과 확인자 한 명과 프로파일 하나에 에이전트 여럿

결과 확인자는 업무마다 이름이 있는 사람 한 명으로 정합니다. 사람 확인이 필요한 일은 넘길 때마다 기록이 남는 업무 게시판으로 보내고 확인 단계를 일감 흐름 안에 둘 수 있으므로[S3], 확인자 칸이 비어 있으면 그 업무는 아직 시범에 올릴 준비가 되지 않은 것으로 봅니다. 한편 프로파일 하나에 에이전트 여럿이 동시에 실행되는 구조라서, 오전 예약 작업과 메신저 질문이 겹쳐 들어와도 같은 프로파일 안에서 대화가 섞이지 않고 따로 처리됩니다[S1]. 시범 팀의 규모는 동시에 처리하는 일감 수가 아니라 설계표의 행 수, 곧 프로파일 수로 셉니다.

8.2 부르는 창구 선택과 2주 시범 운영의 확인 항목

시범 도입의 셋째와 넷째 단계는 직원이 에이전트를 부를 창구를 정하고, 운영 기간이 끝난 뒤 무엇을 보고 넓힐지 판단할지를 미리 적어 두는 일입니다. Hermes Agent에서 창구는 텔레그램·슬랙 같은 메신저 계정인 메신저 봇과 데스크톱 명단에 오른 Bot Mode 봇 두 가지이며, 어느 쪽을 골라도 일하는 단위는 같은 프로파일입니다[S1]. 확인 항목을 시작 전에 정해 두면 시범 결과를 두고 효과가 있었는지를 다시 논쟁하지 않고 같은 기준으로 다음 결정을 내릴 수 있습니다.

8.2.1 이미 쓰는 메신저와 화면 콘솔 가운데 부서별 창구를 고르는 기준

메신저 봇과 화면 콘솔의 부서별 선택 기준

직원이 이미 사내 메신저로 일하고 결과도 메신저로 받기를 원하면 메신저 봇이 맞습니다. 반대로 에이전트가 지금 어느 단계에 있는지, 무엇을 실행하려고 승인을 기다리는지, 어떤 설정으로 움직이는지를 화면에서 보고 싶은 부서에는 화면 콘솔이 맞습니다. 다음 표는 두 창구를 부서 상황에 따라 비교한 것입니다.

상황	메신저 봇	화면 콘솔
직원이 결과를 받는 곳	이미 쓰는 메신저 방	콘솔 화면의 대화와 실행 기록
진행 단계와 실행 승인 확인	메시지로 오가는 범위에서만 확인	단계·승인 요청·되문기를 화면에서 확인
성격·스킬·예약 작업 변경	메신저 창 밖에서 따로 변경	같은 화면에서 변경
준비 작업	프로파일마다 메신저 봇 계정을 따로 만들어 연결	콘솔 계정과 접속 권한 준비

메신저 봇을 고르면 준비 작업 하나를 빼먹지 않아야 합니다. 같은 메신저 봇 계정을 두 프로파일이 동시에 쓰지 못하므로 프로파일마다 고유한 메신저 봇 계정이 하나씩 필요하고, 시범 팀이 업무 3개라면 메신저 봇 계정도 3개를 준비합니다[S6].

시범 팀 설계에서 다시 쓰는 5장의 판단 질문

5장의 판단 질문은 창구를 고를 때 그대로 씁니다. 다른 비밀 정보와 다른 기억이 필요한 새 역할이면 새 프로파일을 만들고, 같은 역할을 다른 곳에서도 부르고 싶으면 그 프로파일에 창구만 추가합니다. Bot Mode는 프로파일의 데이터를 소유하지 않고 화면에 보여 주기만 하므로, Bot Mode를 꺼도 프로파일과 대화 기록, 예약 작업은 그대로 남습니다[S5]. 이 성질 때문에 창구 선택은 시범 도중에 바뀌도 되는 결정이며, 영업은 메신저 봇으로 시작하고 IT 운영은 화면 콘솔로 시작하는 식으로 부서마다 달리 정해도 관리할 프로파일 수는 늘지 않습니다.

8.2.2 말긴 일 수·사람이 고친 비율·기억과 권한 섞임 여부의 2주 확인표

시범 운영 확인표의 네 항목

운영 기간이 끝나면 다음 네 항목을 업무별로 확인합니다. 목표 수치는 미리 정하지 않습니다. 시범의 목적은 효과를 증명하는 데 있지 않고, 다음 결정을 내릴 근거를 같은 기준으로 모으는 데 있기 때문입니다.

항목	재는 법	결과에 따른 다음 결정
말긴 일 수	예약 작업 실행 횟수와 메신저·콘솔 요청 건수, 업무 게시판 일감 수를 업무별로 셉니다	건수가 적으면 그 업무가 실제로 자주 되풀이되는 업무였는지 선정을 다시 봅니다
사람이 고친 비율	결과 확인자가 그대로 쓴 결과와 고쳐 쓴 결과를 나눠 셉니다	고친 이유가 역할 설명이나 스킬 부족이면 역할 설명을 고쳐 같은 업무로 한 번 더 운영합니다
기억·비밀 정보 섞임	한 프로파일의 답에 다른 역할의 대화 내용이나 접속 정보가 나온 적이 있는지 확인자가 기록합니다	한 번이라도 있으면 프로파일 구성과 서버 분리부터 다시 봅니다
확인자의 확인 여부	결과마다 확인자가 실제로 보고 승인 했는지 기록이 남았는지 봅니다	확인 기록이 비면 확인자를 다시 정하거나 업무 게시판의 사람 확인 단계로 옮깁니다

사람이 고친 비율과 섞임 기록으로 내리는 다음 결정

네 항목 가운데 의사결정에 가장 직접 쓰이는 것은 사람이 고친 비율과 섞임 기록입니다. 고친 비율이 높으면 업무 자체가 맞지 않는지, 역할 설명과 스킬이 부족한지를 고친 이유로 가를 수 있고, 섞임이 한 번이라도 나오면 업무를 늘리기 전에 칸막이 설계를 먼저 고쳐야 합니다. 프로파일은 같은 서버의 파일 접근까지 막는 격리 공간이 아니므로[S1], 비밀 정보 범위가 크게 다른 역할을 추가할 계획이 있으면 이 단계에서 서버를 나눌지도 함께 정합니다. 확인 결과로 내리는 결정은 역할 추가, 창구 조정, 중단 세 가지이며, 어느 쪽이든 같은 확인표로 다음 회차를 다시 판단합니다.

문제가 생겼을 때 원인을 좁히는 순서

시범 운영 중 에이전트가 기대와 다른 결과를 내면, 곧바로 설정을 고치기보다 원인을 좁히는 순서를 지키는 편이 빠릅니다. 먼저 어떤 요청을 언제 어느 프로파일에 보냈는지를 그대로 적어 현상을 고정하고, 도구 없이 답만 하는 요청부터 자료를 읽기만 하는 요청, 무엇을 기록하거나 보내는 요청 순서로 범위를 넓혀 가며 어느 단계에서 어긋나는지 찾습니다. 그다음 네트워크·접속 카·AI 모델의 사용 한도 같은 바깥 조건을 확인하고, 고친 뒤에는 같은 요청으로 다시 실행해 결과를 비교합니다. 기록을 다른 사람이나 공급사에 보여 줄 때는 비밀 정보가 드러나지 않도록 먼저 가린 뒤 공유합니다.

시범 기간 중 프로파일의 성격·스킬·예약 작업처럼 일하는 방식을 바꿀 때는 바꾸기 전에 다섯 가지를 한 줄씩 적어 둡니다. 문제가 생기면 돌아갈 복구 지점, 그 변경에 필요한 가장 작은 권한, 먼저 적용해 볼 좁은 범위, 바꾼 뒤 지켜볼 기록, 성공과 실패를 가를 기준입니다. 이 다섯 줄이 있으면 확인표의 「사람이 고친 비율」이 달라졌을 때 어떤 변경 때문인지 되짚을 수 있고, 결과가 나빠지면 같은 기록으로 바로 되돌릴 수 있습니다.

8.3 시범 도입 검토 목록에 올릴 1~7장의 의사결정 질문 묶음

1~7장의 끝에는 각 장의 개념을 우리 조직의 결정으로 옮기는 질문이 하나씩 있었습니다. 일곱 질문 가운데 넷은 업무 담당 부서장이 답하고 셋은 IT 담당자가 함께 답하며, 두 묶음에 모두 답이 적히면 시범 팀 설계표의 빈 칸도 함께 채워집니다. 아래 두 표는 질문마다 나온 장을 적어 두었으므로 답이 막히면 그 장으로 돌아가 근거를 다시 볼 수 있고, 검토 회의에는 이 표를 그대로 가져가 「우리 조직의 답」 칸을 채우면 됩니다.

8.3.1 역할·창구·결과 확인자에 관한 의사결정 질문

업무 담당 부서장이 답할 의사결정 질문 네 가지

첫 묶음은 어떤 업무를 누구에게 맡기고 결과를 누가 보는지에 관한 질문입니다. 이 네 질문의 답은 설계표의 업무·창구·결과 확인자 칸으로 바로 옮겨지므로 업무를 실제로 아는 부서장이 답하는 편이 정확합니다.

의사결정 질문	나온 장	우리 조직의 답
우리 조직에서 매일 되풀이되고 결과를 사람이 확인할 수 있는 업무는 무엇인가	1장	
역할마다 볼 수 있는 자료와 비밀 정보의 범위가 다른가	2장	
역할마다 어느 창구로 부르는가, 이미 쓰는 메신저인가 화면 콘솔인가	5장	
역할 사이에 넘기는 일은 무엇이고 어디서 사람이 확인하는가	6장	

첫째 질문의 답은 설계표의 업무 칸으로, 둘째 질문의 답은 비밀 정보 범위 칸으로, 셋째 질문의 답은 8.2.1의 창구 선택으로 각각 옮겨 적습니다. 예를 들어 둘째 질문에 「영업과 재무가 보는 자료가 다르다」고 답했다면 두 업무는 반드시 다른 프로파일로 나누고, 재무 업무는 첫 시범에서 빼 둘지를 8.1.1의 기준으로 다시 판단합니다. 질문마다 답을 한 줄로 적어 두면 검토 회의에서 같은 논의를 되풀이하지 않고 설계표의 빈칸을 그 자리에서 채울 수 있습니다.

역할 사이 일 넘기기 질문과 업무 게시판의 기록

넷째 질문은 시범 팀이 업무 3개를 넘어설 때 가장 먼저 다시 보게 되는 질문입니다. 같은 역할 안에서 짧은 답을 받아 이어 가는 일은 서버에이전트에게 맡기고, 다른 역할이 받아야 하거나 재시작에도 남아야 하거나 사람 확인이 필요한 일은 업무 게시판으로 보냅니다[S3]. 업무 게시판에서는 일을 넘길 때마다 기록이 한 줄씩 남으므로 [S3], 이 질문에 「어디서 사람이 확인하는가」를 적어 두면 그 지점이 곧 게시판의 사람 확인 단계가 됩니다. 시범 단계에서 이 질문의 답이 「넘기는 일 없음」이어도 괜찮습니다. 고른 3개 업무가 서로 독립적이라는 뜻이고, 8.1.1의 선정 원칙과도 맞습니다.

8.3.2 서버·AI 모델·비밀 정보와 이전·배포에 관한 의사결정 질문

IT 담당자와 함께 답할 의사결정 질문 세 가지

둘째 묶음은 프로파일에 무엇을 담고, 일이 몰릴 때 어떻게 나누며, 잘 다듬은 역할을 어디까지 나눠 줄지에 관한 질문입니다. 서버 구성과 비밀 정보 관리가 함께 걸려 있으므로 업무 담당자와 IT 담당자가 같이 답합니다.

의사결정 질문	나온 장	우리 조직의 답
업무마다 프로파일 하나를 둔다면 각 프로파일에 무엇을 넣고 무엇을 빼는가	3장	
한 역할에 동시에 몇 건의 일이 들어오고, 나눠 맡길 큰 조사 업무가 있는가	4장	
잘 다듬은 역할을 다른 팀·지사에 나눠 줄 계획이 있는가, 내보내기 전에 누가 점검하는가	7장	

넷째 장 질문은 서브에이전트 사용량과 이어집니다. Hermes Agent v0.21.0 기본값으로 서브에이전트는 최대 10개까지 동시에 실행되고 설정으로 바꿀 수 있으며[S4], 큰 조사를 여럿이 나눠 처리하면 AI 사용량도 함께 늘어납니다. 2장(2.2.2)에서 본 것처럼 여러 에이전트가 함께 일하는 구성은 조사 업무에서 일반 채팅보다 사용량이 크게 늘어납니다. 그래서 나눠 맡길 큰 조사 업무가 있다고 답한 역할은 쓸 AI 모델의 종류와 사용량 한도를 IT 담당자가 먼저 정해 둡니다.

일곱째 장 질문은 내보내기 비밀 정보 점검으로 이어집니다. 프로파일 내보내기 파일은 있는 그대로 찍은 사본이라 기억과 대화 기록이 함께 들어가고, 계속 고치며 여러 곳에 나눠 줄 에이전트에는 배포판이 맞습니다[S2]. 또한 내보내기는 비밀 정보를 파일 이름으로 거르는 방식이므로 이름이 다른 백업 사본이나 일부 인증 파일이 가려지지 않은 채 들어갈 수 있습니다. 그래서 「누가 점검하는가」 칸에는 파일을 열어 확인할 사람의 이름을 적습니다.

시범 도입 전에 갖춰야 할 것 점검표

질문 묶음과 함께 시범을 시작하기 전에 갖춰야 할 것을 확인합니다. 다음 다섯 가지 가운데 하나라도 비어 있으면 시범 일정을 잡기 전에 그 항목부터 채웁니다.

갖춰야 할 것	확인 방법	준비 여부
서버 한 대	시범 프로파일 3개를 둘 서버와 관리 담당자를 정했는가	
쓸 AI 모델	업무별로 쓸 AI 모델과 사용량 한도를 정했는가	
직원이 쓰는 메신저	메신저 봇을 고른 업무의 메신저와 메신저 봇 계정 발급 절차를 확인했는가	
역할 설명을 적을 업무 담당자	업무마다 역할 설명 두 줄을 쓸 사람이 정해졌는가	

갖춰야 할 것	확인 방법	준비 여부
결과 확인자	업무마다 결과를 보고 승인할 사람 한 명이 정해졌는가	

다섯 항목 가운데 서버 한 대와 쓸 AI 모델은 IT 담당자가, 역할 설명을 적을 업무 담당자와 결과 확인자는 업무 담당 부서장이 채우는 칸입니다. 시범 프로파일 3개는 서버 한 대에 함께 둘 수 있지만, 8.3.2의 3장 질문에서 비밀 정보 범위가 크게 다르다고 답한 역할이 있으면 서버를 나눌지를 이 점검표에서 함께 정해 둡니다. 다섯 칸이 모두 채워진 상태가 시범 도입 검토 목록에 올릴 수 있는 최소 조건입니다.

8.4 명령줄 없이 화면에서 에이전트 팀을 쓰는 MSAP.ai AAS

MSAP.ai AAS(AI Agent Studio)는 AI Agent 플랫폼에 연결해 쓰는 일반 사용자용 콘솔로, 부서 담당자가 명령줄을 쓰지 않고 화면에서 에이전트에게 일을 시키고 프로파일·예약 작업을 관리하도록 만든 제품입니다. 지금 MSAP.ai AAS가 연결하는 에이전트 플랫폼이 Hermes Agent이므로, 1~7장에서 본 프로파일·예약 작업·스킬이 콘솔 화면에 같은 단위로 나타납니다. 8.2.1에서 화면 콘솔을 창구로 고른 부서라면 MSAP.ai AAS가 실제 선택지 가운데 하나가 됩니다.

8.4.1 Hermes Agent 에 연결되는 일반 사용자 콘솔 MSAP.ai AAS 와 화면 용어의 대응

AAS 화면의 에이전트와 프로파일 두 층

MSAP.ai AAS는 사람마다 에이전트를 하나씩 배정하고, 그 안에 업무별 프로파일을 두는 두 층 구조로 화면을 구성합니다. 여기서 화면의 「에이전트」는 한 사람에게 배정되는 단위이며, 그 사람 묶으로 설치된 Hermes Agent 한 벌에 해당합니다. 그 한 벌 안에 3장의 프로파일이 여러 개 들어 있으므로, 화면의 「에이전트」와 4장의 에이전트(프로파일의 설정으로 지금 일하는 직원)는 이름은 같지만 가리키는 대상이 다릅니다. 화면의 「프로파일」은 3장에서 자리와 기록에 비유한 프로파일을 그대로 가리킵니다.

AAS 화면 용어	이 문서의 개념	다른 장
에이전트	한 사람에게 배정되는 Hermes Agent 한 벌. 안에 프로파일 여러 개가 들어 있음(4장의 에이전트와 다름)	3장 · 4장
프로파일	프로파일(성격·모델·스킬·비밀 정보·예약 작업·메신저 연결을 담는 단위)	3장
대화와 실행 기록	지금 일하는 에이전트와 서브에이전트가 일감 단위로 보이는 곳	4장
예약 작업	프로파일의 예약 작업	1장 · 4장
스킬	프로파일이 익힌 일하는 방법	3장

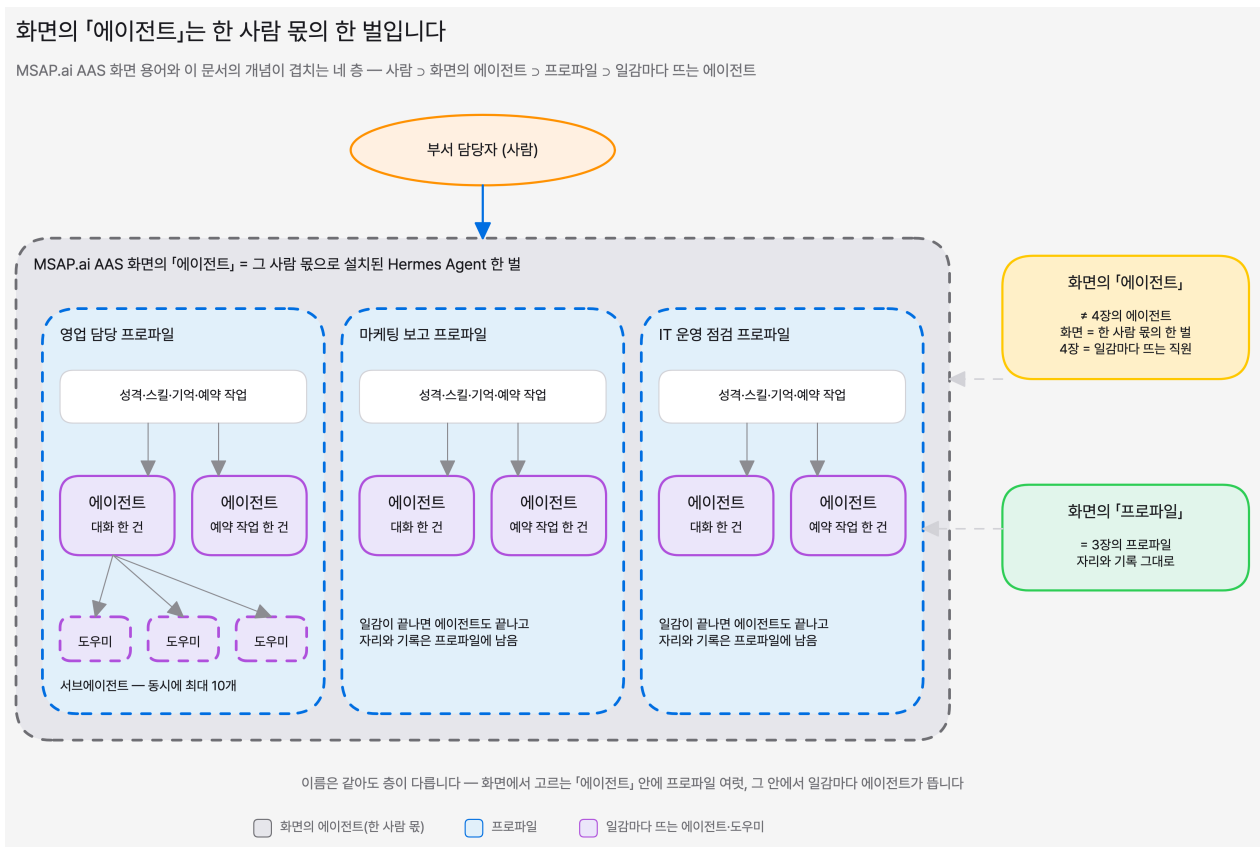


그림. MSAP.ai AAS 화면의 에이전트·프로파일과 이 문서의 개념이 겹치는 방식

8.4.2 화면 대화와 마켓 설치로 쓰는 에이전트 팀과 현재 구현 범위

부서 담당자가 MSAP.ai AAS 화면에서 하는 일

부서 담당자는 MSAP.ai AAS 화면에서 에이전트를 골라 대화하고, 에이전트가 진행 중인 단계를 보며, 실행 승인 요청과 되묻는 질문에 답합니다. 프로파일은 기존 프로파일을 복제하거나 다른 에이전트에서 가져와 새로 만들고, 성격·AI 모델·스킬·도구를 화면에서 고칩니다. 예약 작업은 실행 주기와 결과를 받을 대상을 화면에서 등록하고 바꿉니다. 스킬 하나가 어떤 스크립트와 외부 도구를 부르는지를 흐름 그림으로 보여 주므로, 결과 확인자가 에이전트가 무엇을 했는지 따라가기 쉽습니다. 마켓에서는 스킬과 에이전트 패키지를 골라 자기 프로파일에 설치합니다. 접속은 표준 로그인 방식인 OIDC(OpenID Connect)로 사람마다 자기 에이전트에 연결하며, 외부에서 내려받는 과정 없이 조직 안 서버에 직접 설치하는 온프레미스 방식으로 운영합니다.

MSAP.ai AAS 기능별 현재 구현 범위

다음 표는 위 쓰임새를 기능별로 나눠 지금 쓸 수 있는 범위를 밝힌 것입니다. 검토 목록에는 「구현」 항목만 시범 범위로 올리고, 「부분」과 「미구현」 항목은 시범 설계에서 다른 방법으로 대신할지를 따로 적어 둡니다.

기능	하는 일	현재 구현 범위
화면 대화	에이전트 선택, 진행 단계 보기, 실행 승인, 되묻기 응답	구현
프로파일 만들기과 편집	기존 프로파일 복제, 다른 에이전트에서 가져오기, 성격·모델·스킬·도구 편	구현

기능	하는 일	현재 구현 범위
	집	
예약 작업	주기와 결과 전달 대상 등록·변경	구현
스킬 흐름 그림	스킬이 부르는 스크립트와 외부 도구를 그림으로 표시	구현
사용자별 연결	표준 로그인(OIDC)으로 사람마다 자기 에이전트에 연결	구현
조직 안 설치	조직 안 서버에 설치(온프레미스)	구현
스킬 편집	문서로 된 스킬을 화면에서 고침. 스크립트는 화면에서 보기만 하고 고칠 수 없음	구현(문서만)
마켓	스킬·에이전트 패키지를 골라 프로파일에 설치. 공유 범위는 아직 정해지지 않음	부분
협업 공간	여러 에이전트가 함께 쓰는 공간	부분(일부 기능)
메신저 연결 마법사	메신저 봇 계정을 화면에서 연결	미구현

표에서 「부분」은 기능은 화면에 있지만 쓸 수 있는 범위가 제한된다는 뜻입니다. 스킬 편집도 문서로 된 스킬까지만 화면에서 고칠 수 있으므로, 스크립트를 함께 쓰는 스킬을 고칠 일이 생기면 IT 담당자가 Hermes Agent 쪽에서 직접 고쳐야 합니다. 마켓과 협업 공간은 시범 범위에서 필수 기능으로 두지 않고, 시범 팀이 화면 대화·프로파일 편집·예약 작업만으로 운영되도록 설계하는 편이 판단 근거를 깨끗하게 남깁니다.

메신저 봇 창구를 고른 부서의 AAS 준비 사항

구현 범위에서 시범 설계에 바로 영향을 주는 항목은 메신저 연결 마법사입니다. 이 기능이 아직 없으므로 8.2.1에서 메신저 봇을 고른 부서는 메신저 봇 계정 연결을 Hermes Agent 쪽에서 IT 담당자가 직접 해야 하며, 이 일을 갖춰야 할 것 점검표의 「직원이 쓰는 메신저」 칸에 담당자 이름과 함께 적어 둡니다. 마켓도 설치되지만 무엇을 어디까지 공유할지는 아직 정해지지 않았으므로, 7장 질문에서 다른 팀·지사에 나눠 줄 계획이 있다고 답한 조직은 당분간 배포판으로 나눠 주는 방식을 함께 검토합니다[S2].

기억할 것 ① 반복 업무 3개를 골라 업무 하나에 프로파일 하나를 둡니다. ② 부르는 창구와 결과 확인자를 시작 전에 먼저 정합니다. ③ 2주 뒤 확인 항목으로 역할 추가, 창구 조정, 중단 가운데 하나를 정합니다.

프로파일은 자리와 기록, 에이전트는 지금 일하는 직원, 메신저 봇과 Bot Mode 봇은 부르는 창구라는 구분은 용어를 외우기 위한 것이 아니라 시범 팀 설계표의 칸을 나누는 기준입니다. 업무 하나에 프로파일 하나를 두면 기억과 비밀 정보가 역할마다 갈라지고(3장), 같은 역할이 여러 일을 동시에 처리하며(4장), 직원은 이미 쓰는 창구로 에이전트를 부르고(5장), 역할 사이의 일은 업무 게시판에서 사람의 확인을 거쳐 넘어갑니다(6장). 잘 다듬은 역할을 다른 팀에 나눠 줄 때 지킬 비밀 정보의 범위(7장)까지 정해 두면 에이전트 팀은 사람 팀과 같은 방

식으로 관리됩니다. 남은 결정은 하나입니다. 매일 되풀이되는 업무 3개를 고르고, 업무마다 부르는 창구와 결과 확인자를 한 줄씩 적은 설계표를 시범 도입 검토 목록에 올리는 일입니다.

부록: 참고문헌과 용어 정의

Appendix A — 참고문헌 (References)

이 부록은 백서 본문에 인용한 자료와 본문에 나오는 주요 용어의 뜻을 모아 둔 참조 자료입니다. [S#] 번호는 본문 내용의 근거로 확인한 공개 외부 자료이고, [R#] 번호는 같은 주제를 더 읽어 볼 수 있도록 고른 MSAP.ai 공개 블로그 글이라 근거 번호와 따로 매깁니다.

확인 근거 자료

- [S1] Nous Research (공식 문서 최신판, 2026-10-23 열람). Profiles: Running Multiple Agents — 프로파일로 에이전트 여럿 운영하기. <https://hermes-agent.nousresearch.com/docs/user-guide/profiles>
- [S2] Nous Research (공식 문서 최신판, 2026-10-23 열람). Profile Distributions — 프로파일 배포판. <https://hermes-agent.nousresearch.com/docs/user-guide/profile-distributions>
- [S3] Nous Research (공식 문서 최신판, 2026-10-23 열람). Kanban — Multi-Agent Profile Collaboration — 업무 게시판으로 프로파일끼리 함께 일하기. <https://hermes-agent.nousresearch.com/docs/user-guide/features/kanban>
- [S4] Nous Research (공식 문서 최신판, 2026-10-23 열람). Subagent Delegation — 서브에이전트에게 일 나눠 맡기기. <https://hermes-agent.nousresearch.com/docs/user-guide/features/delegation>
- [S5] Nous Research (공식 문서 최신판, 2026-10-23 열람). Bot Mode — 데스크톱 앱의 Bot Mode. <https://hermes-agent.nousresearch.com/docs/user-guide/bot-mode>
- [S6] Nous Research (공식 문서 최신판, 2026-10-23 열람). Multi-profile Gateways — 프로파일마다 메신저 봇 연결하기. <https://hermes-agent.nousresearch.com/docs/user-guide/multi-profile-gateways>
- [S7] Anthropic (2024-12-19). Building effective agents — 쓸모 있는 에이전트를 만드는 방법. <https://www.anthropic.com/engineering/building-effective-agents>
- [S8] Anthropic (2025-06-13). How we built our multi-agent research system — 다중 에이전트 조사 시스템을 만든 과정. <https://www.anthropic.com/engineering/multi-agent-research-system>

함께 읽을 자료

- [R1] MSAP.ai (2026-07-28). AI 에이전트와 챗봇의 차이 — 자율성·도구·메모리로 가르는 5가지 기준. <https://www.msap.ai/blog-home/ai-blog/ai-agent-vs-chatbot/>
- [R2] MSAP.ai (2026-07-30). AI 에이전트란 무엇인가 — 정의, 구조, 기업 도입 기준. <https://www.msap.ai/blog-home/ai-blog/what-is-ai-agent/>
- [R3] MSAP.ai (2026-08-06). Agentic AI(에이전틱 AI)란 무엇인가 — 생성형 AI의 다음 단계. <https://www.msap.ai/blog-home/ai-blog/what-is-agentic-ai/>

- [R4] [MSAP.ai](https://www.msap.ai/resource/whitepaper/opeunweiteu-ilm-seonjeong/) (2026-07-27). 오픈소스 AI 에이전트 Hermes 도입 가이드 — Gemma 4 사내 AI 결합. <https://www.msap.ai/resource/whitepaper/opeunweiteu-ilm-seonjeong/>
- [R5] [MSAP.ai](https://www.msap.ai/resource/hermes-agent-eight-essential-ai-agent-features-2/) (2026-08-22). AI 에이전트 필수 기능 여덟 가지, 도입 전 점검 기준. <https://www.msap.ai/resource/hermes-agent-eight-essential-ai-agent-features-2/>

Appendix B — 용어 정의 (Glossary)

본문에 나오는 순서와 관계없이 가나다순, 알파벳순으로 정리했습니다.

용어	정의
그룹 방	여러 Bot Mode 봇이 한 대화방에서 함께 답하는 Bot Mode 기능으로, 회의실에 담당자 여럿을 불러 한꺼번에 묻는 것과 같습니다.
기억	에이전트가 일하며 알게 된 사실(예: 고객사가 좋아하는 보고 형식)을 프로파일에 남겨 다음 일에 다시 쓰는 기록입니다.
내보내기 파일	프로파일 하나를 있는 그대로 압축 파일 하나에 담은 사본으로, 서버를 옮길 때 쓰며 기억과 대화 기록이 함께 들어가므로 넘기기 전에 비밀 정보를 점검해야 합니다.
대화 기록	에이전트와 나눈 지난 대화가 프로파일에 그대로 남은 기록입니다.
메신저 봇	텔레그램·슬랙·디스코드 같은 메신저에 만든 계정으로, 직원이 평소 쓰는 메신저에서 에이전트를 부르는 창구이며 계정 하나는 프로파일 하나에만 연결됩니다.
멀티에이전트	역할을 나눈 에이전트 여럿이 한 팀으로 일하는 방식으로, 이 백서에서는 「에이전트 팀」과 같은 뜻으로 씁니다.
배포판	성격·스킬·예약 작업·설정을 묶어 다른 팀이 설치하고 업데이트해 받도록 만든 프로파일 꾸러미로, 업데이트해도 받는 쪽의 기억·대화 기록·비밀 정보는 건드리지 않습니다.
비밀 정보	에이전트가 외부 서비스와 업무 시스템에 들어갈 때 쓰는 접속 열쇠와 비밀번호 같은 정보로, 프로파일마다 따로 보관합니다.
서버 전체 백업	한 서버에 있는 모든 프로파일을 한꺼번에 사본으로 남기는 방식으로, 서버를 통째로 옮길 때 씁니다.
서브에이전트(도우미)	에이전트가 큰 일을 나눠 맡기려고 잠깐 부르는 도우미로, 새 대화에서 일을 시작해 결과만 돌려주며 에이전트 하나당 동시에 기본 최대 10개까지 부릅니다.
성격	에이전트의 말투와 일하는 태도를 정해 둔 프로파일 항목으로, 직원의 업무 수칙에 해당합니다.

용어	정의
스킬(익힌 기술)	특정 업무를 처리하는 방법을 순서대로 적은 문서로, 에이전트는 요청에 맞는 스킬을 골라 그 순서대로 일합니다.
업무 게시판(칸반)	한 서버의 모든 프로파일이 함께 쓰는 일감 게시판으로, 일감 하나가 카드 한 장이 되고 일을 넘길 때마다 기록이 남습니다.
에이전트(AI 에이전트)	프로파일의 설정으로 지금 일하는 직원으로, 도구를 직접 써서 맡은 일을 결과물까지 끝내며 대화 한 건·예약 작업 한 건마다 따로 실행되고 끝나면 사라집니다.
예약 작업	사람의 지시 없이 정해진 시각에 에이전트가 정해진 일을 시작하게 하는 일정 등록입니다.
온프레미스	클라우드가 아닌 조직 안 서버에 설치해 운영하는 방식입니다.
정기 루틴	Bot Mode 봇에 걸어 두는 반복 업무로, 실제로는 일반 예약 작업으로 등록되어 실행됩니다.
직접 메시지	Bot Mode 봇끼리 업무 게시판을 거치지 않고 서로 주고 받는 메시지로, 답 길이에 상한이 있습니다.
챗봇	질문을 받으면 글로 된 답을 내놓고 대화를 마치는 대화형 AI로, 회사 로비의 안내 데스크 직원에 해당합니다.
토큰	AI 모델이 읽고 쓰는 글의 양을 세는 단위로, 사용료가 이 양에 따라 매겨집니다.
프로파일	에이전트 한 명이 일하는 데 필요한 성격·AI 모델·스킬·비밀 정보·기억·대화 기록·예약 작업을 묶어 계속 보관하는 단위로, 직원의 자리와 기록에 해당합니다.
Agentic AI(에이전틱 AI)	AI 모델이 답하는 데서 멈추지 않고 도구를 직접 써서 맡은 일을 끝내는 방식입니다.
Bot Chat	Bot Mode 봇마다 하나씩 있는 고정 대화방으로, 새 대화를 시작해도 대화방이 바뀌지 않고 같은 대화가 이어집니다.
Bot Mode 봇	Hermes Agent 데스크톱 앱 명단에 이름과 얼굴 그림을 달고 오른 프로파일로, 자리 배치도의 이름표처럼 눌러서 부르는 창구이며 모든 프로파일이 Bot Mode 봇인 것은 아닙니다.
CRM	Customer Relationship Management, 고객 관리 시스템입니다.

용어	정의
Hermes Agent	Nous Research가 공개한 오픈소스 AI 에이전트 제품으로, 이 백서의 기준 사례입니다.
LLM	Large Language Model, 대규모 언어 모델로, 에이전트가 판단하고 글을 쓰는 데 쓰는 AI 모델입니다.
OAuth	비밀번호를 넘기지 않고 외부 서비스 로그인 권한을 빌려주는 표준 방식으로, 일부 OAuth 로그인 정보는 모든 프로파일이 함께 읽습니다.
OIDC	OpenID Connect, 여러 서비스가 같은 계정으로 로그인하게 하는 표준 로그인 방식입니다.

Hermes Agent 로 이해하는 프로파일·에이전트·봇 — Agentic AI 멀티에이전트 입문

CONTACT

WEB

msap.ai

www.msap.ai/

EMAIL

hello@msap.ai

TEL

02-6953-5427

0269535427

YOUTUBE

@msaptv

www.youtube.com/@msaptv

LINKEDIN

linkedin.com/showcas...

www.linkedin.com/showcase/msap-ai/

FACEBOOK

facebook.com/opennaru

www.facebook.com/opennaru



SCAN