

TECH BRIEF

MSAP.ai

업무를 아는 사람이 AI Agent 를 만든다 — MSAP.ai AAS 소개 백서

담당자가 만들고 시키고 지켜보는 에이전트 콘솔

AI Agent는 기업용 애플리케이션 안으로 빠르게 들어오고 있지만 부서의 반복 업무에 자리 잡은 사례는 드뭅니다. MSAP.ai AAS는 업무를 아는 담당자가 조직 안에서, 쓰던 에이전트 플랫폼을 고치지 않고 에이전트를 만들고 시키고 지켜보는 콘솔입니다.

2026-10-19 · 작성자: SMART CF Team · msap.ai

목차

업무를 아는 사람이 AI Agent 를 만든다 — MSAP.ai AAS 소개 백서

1장: 업무에 들어온 AI Agent에 업무 창구가 없는 이유 — 채팅 프로그램의 한계와 사람 없이 실행되는 에이전트

1.1 기업용 애플리케이션 40%의 AI Agent 탑재 전망과 업무 기능별 확대 적용 10% 이하의 간극

1.2 진행 단계와 실행 승인을 담을 자리가 없는 채팅 창구의 구조

1.3 세션 92%가 정기 업무에서 시작되는 에이전트와 알림이 안 가는 실패

1.4 에이전트형 AI 프로젝트 40% 중단 전망과 첫 유즈케이스 파일럿 판단

2장: AI Agent 도구 시장의 인접 6개 세그먼트와 비어 있는 자리 — 조직 안 업무 담당자용 콘솔

2.1 AI Agent 도구를 나누는 네 가지 기준과 여섯 가지 구분

2.2 만드는 쪽 세 구분의 완성도와 자사 실행 엔진이라는 전제

2.3 지켜보는 쪽 세 구분과 운영자 화면에 머무는 플랫폼 전용 콘솔

2.4 예약 실행·사내 공유·다중 에이전트 협업의 보급으로 운영의 질로 옮겨 간 AI Agent 도구 경쟁

2.5 국가 망 보안체계(N²SF)의 기밀 등급 아래에서 남는 온프레미스 설치 수요

2.6 조직 안 설치·업무 담당자 사용·만들기와 지켜보기를 함께 갖춘 조합의 공백과 AAS의 위치

3장: 업무를 아는 담당자가 에이전트를 직접 만드는 콘솔 MSAP.ai AAS와 폭스프로·디베이스 선례

3.1 AI Agent 플랫폼에 연결되는 일반 사용자용 콘솔이라는 MSAP.ai AAS의 정의

3.2 오픈소스 Hermes Agent 1종에 연결되는 현재 범위와 플랫폼에서 스킬까지 이어지는 계층

3.3 현업이 업무 프로그램을 직접 만들던 폭스프로·디베이스 선례와 AAS의 대응

3.4 부서 담당자부터 보안 감사 담당까지 사용자 넷의 역할과 역할 템플릿 20종

4장: 만들고 시키고 지켜보고 나누는 네 기능 묶음을 한 화면에 모은 AAS 콘솔의 실제 화면

4.1 에이전트 추가와 업무별 프로파일, 스킬 판 관리, 정기 업무 등록을 한 화면에서 정하는 만들기

4.2 진행 단계와 실행 승인 카드가 보이는 팀 채팅, 여러 에이전트가 함께 답하는 회의 탭

4.3 실패 작업과 만료 임박 자격증명을 첫 화면에 모은 「오늘 볼 것」

4.4 사내 스킬 마켓 패키지 51개와 OIDC 연동 사용자별 에이전트 한도

5장: 명함 인식에서 화자 구분 회의록까지 10개 카테고리 업무 에이전트 카탈로그

5.1 명함 사진에서 CRM 연락처 등록까지 — 등록 전 확인과 중복 시 정지를 갖춘 명함 인식

5.2 한글(HWP·HWPX) 공공문서 인식과 공공서식 빈칸 채우기, 기안문 작성

5.3 화자 구분 회의록에서 지시사항과 담당자별 할 일로 이어지는 회의 후속 처리

5.4 영업 보고에서 개인 비서까지 정기 업무로 실행되는 나머지 일곱 카테고리

6장: 보이지 않던 것이 보이는 관측 화면 — 알림이 안 가는 정기 업무와 자격증명 만료

6.1 지금도 실패 중인 작업과 이미 풀린 사건 62건을 나누는 Cron 헬스체크 화면

6.2 정기 업무 95개 중 알림이 안 가는 작업 15개와 공통 오류 문자열 집계

6.3 값을 보이지 않고 자격증명 103개의 만료와 빈 값, 복사 위치를 찾는 점검

6.4 스킬 문서와 실행 기록에서 뽑은 호출 관계 그림과 선마다 붙는 근거 줄

7장: 쓰던 에이전트 플랫폼을 고치지 않고 조직 안에서 구동되는 온프레미스 설치와 보안 원칙

7.1 읽기 전용 수집과 플랫폼 공식 API 단일 변경 경로로 나눈 연결 구조

7.2 공식 API에 길이 없는 마켓 패키지 설치와 삭제의 예외 처리 범위
7.3 외부 내려받기 없이 조직 안에서 구동되는 온프레미스 설치와 쿠버네티스 배포본
7.4 비밀값을 화면과 로그에 남기지 않고 못 읽은 것을 0건으로 표시하지 않는 설계 원칙 다섯 가지
8장: 부서별 AI Agent 업무 장면과 퇴사·부서 통합 때 조직에 남는 에이전트 구성
8.1 경영 부서와 현업 부서의 에이전트 장면 — 주간 회의 지시 원장부터 이력서 1차 심사까지
8.2 IT 운영과 공공기관의 에이전트 장면 — 장애 1차 조사, 토큰 유출 영향 범위, 망 분리 환경의 공문 처리
8.3 부서장이 보는 팀 에이전트 현황 — 에이전트별 준비 상태와 35일 추이
8.4 퇴사와 부서 이동·통합, 지사 확산, 감사 때 조직에 남는 스킬과 정기 업무
9장: 다른 선택지와 다른 점 — 제품별 비교로 본 AAS의 강점과 한계, 도입 검토 질문
9.1 대표 제품 12개 비교표에서 외부 클라우드 사용 가능 여부가 가르는 AAS의 위치
9.2 정기 업무 건강 감시와 값 없는 자격증명 관리 등 AAS가 앞서는 여섯 항목
9.3 연결 플랫폼 1종과 마켓 결제 미지원 등 아직 부족한 다섯 항목
9.4 무인 실행 감독과 비밀값 처리, 플랫폼 변경 여부를 묻는 도입 검토 질문 목록
10장: 로드맵과 첫 유즈케이스 하나로 시작하는 4단계 도입 방법
10.1 사용자별 에이전트까지 제공되는 현재 범위와 협업 방에서 두 번째 플랫폼 연결로 이어지는 로드맵 순서
10.2 반복량과 사람 확인 지점으로 명함과 회의록, 공문 가운데 고르는 첫 유즈케이스 선정 기준
10.3 첫 유즈케이스 선정에서 사내 마켓 확산까지 파일럿 4단계와 단계별 판단 기준
10.4 부서 담당자와 IT 관리자, 보안 담당이 파일럿 전에 준비할 목록
부록: 참고문헌과 용어 정의
Appendix A — 참고문헌 (References)
Appendix B — 용어 정의 (Glossary)

업무를 아는 사람이 AI Agent 를 만든다 — MSAP.ai AAS 소개 백서

AI Agent는 기업용 애플리케이션 안으로 빠르게 들어오고 있지만, 부서의 반복 업무에 자리 잡은 사례는 아직 드뭅니다. 이 백서는 그 간극의 원인을 에이전트를 만들고, 일을 시키고, 결과를 지켜보는 업무 창구가 없다는 데서 찾습니다. 그리고 업무를 아는 담당자가 조직 안에서, 쓰던 에이전트 플랫폼을 고치지 않고 이 세 가지를 한 화면에서 하는 콘솔로 MSAP.ai AAS(AI Agent Studio)를 소개합니다. 1장과 2장은 문제와 시장을, 3장부터 8장까지는 제품의 기능과 업무 장면, 설치와 보안 원칙을, 9장과 10장은 다른 선택지와의 비교와 도입 방법을 다룹니다. 끝까지 읽은 의사결정권자가 내릴 결정은 하나입니다. 부서 업무 가운데 에이전트에 맡길 첫 유즈케이스(명함·회의록·공문 등)를 골라 파일럿 대상을 정하는 것입니다.

1장: 업무에 들어온 AI Agent에 업무 창구가 없는 이유 — 채팅 프로그램의 한계와 사람 없이 실행되는 에이전트

AI Agent는 사람이 맡긴 일을 여러 단계로 나누고, 필요한 도구를 스스로 호출해 결과를 돌려주는 프로그램입니다. 이 기능은 이제 별도 시험 과제를 넘어 기업용 애플리케이션의 기본 기능으로 들어가고 있으며, Gartner는 특정 업무를 맡는 AI Agent를 탑재한 기업용 애플리케이션이 2025년 5% 미만에서 2026년 말 40%까지 늘어난다고 전망했습니다[S1]. 그런데 조직 안에서 시험 도입이 실제 업무 정착으로 이어지는 비율은 아직 낮습니다. 그 간극을 만드는 원인 가운데 조직이 직접 손댈 수 있는 것은 에이전트를 만들고, 일을 시키고, 결과를 지켜보는 업무 창구입니다. 1장은 이 문제를 채팅 프로그램이라는 창구의 구조적 한계와 사람이 보지 않는 동안 실행되는 정기 업무라는 두 갈래로 나누어 설명하고, 마지막에 부서 업무 가운데 첫 유즈케이스 하나를 골라 파일럿 대상을 정하는 결정과 그 판단 근거가 실린 장을 안내합니다.

1.1 기업용 애플리케이션 40%의 AI Agent 탑재 전망과 업무 기능별 확대 적용 10% 이하의 간극

AI Agent 도입 현황은 시장 전망과 조직 내부 정착률이라는 두 수치로 나누어 보아야 정확하게 읽힙니다. 시장 전망은 기업용 애플리케이션 대부분이 곧 에이전트 기능을 품게 된다고 말하지만, 조직 단위 설문은 업무 기능 하나를 기준으로 에이전트를 확대 적용한 비율이 10%를 넘지 않는다고 보여 줍니다[S1][S4]. 에이전트는 이미 업무 도구 안에 들어왔지만, 업무 담당자가 그것을 매일 쓰는 단계까지 간 조직은 소수입니다. 따라서 의사결정권자가 먼저 확인할 사실은 도입 여부보다 정착 여부이며, 아래 표는 두 수치를 출처별로 나란히 놓은 것입니다.

구분	수치	시점	출처
특정 업무 AI Agent를 탑재한 기업용 애플리케이션 비율	5% 미만 → 40%	2025년 → 2026년 말 전망	Gartner[S1]
조직 어딘가에서 에이전트형 AI를 시험 중인 응답	39%	2025년 조사	McKinsey[S4]

구분	수치	시점	출처
조직 어딘가에서 에이전트형 AI를 확대 적용 중인 응답	23%	2025년 조사	McKinsey[S4]
업무 기능 하나 기준 확대 적용 비율	10% 이하	2025년 조사	McKinsey[S4]

1.1.1 2025년 5% 미만에서 2026년 말 40%로 늘어나는 AI Agent 탑재 전망

기업용 애플리케이션의 AI Agent 탑재 전망치

Gartner는 2025년 8월 26일 보도자료에서 특정 업무를 맡는 AI Agent를 탑재한 기업용 애플리케이션 비율이 2025년 5% 미만에서 2026년 말 40%로 늘어난다고 전망했습니다[S1]. 여기서 특정 업무를 맡는 에이전트는 범용 대화 도우미와 구분되는 개념으로, 일정 조율·문서 분류·고객 문의 응대처럼 범위가 정해진 일을 맡아 스스로 단계를 밟는 기능을 가리킵니다. 이 전망은 조직이 에이전트 제품을 따로 구매하지 않아도, 이미 쓰고 있는 업무 애플리케이션이 판올림되면서 에이전트 기능이 함께 들어온다는 뜻으로 읽어야 합니다. 1년 남짓한 기간에 여덟 배 이상 늘어나는 속도이므로, 조직 입장에서는 도입을 미룰지 결정할 시간도 그만큼 줄어듭니다.

애플리케이션 탑재와 업무 정착의 차이

다만 애플리케이션에 에이전트 기능이 들어 있다는 사실이 곧 부서가 그 기능으로 일을 처리한다는 뜻은 아닙니다. 탑재는 공급자가 결정하는 일이고, 정착은 업무 담당자가 그 기능을 믿고 반복 업무를 맡기는 상태입니다. 예를 들어 회계 애플리케이션에 증빙 분류 에이전트가 들어 있어도, 담당자가 분류 결과를 어디서 확인하고 틀린 결과를 누가 고치는지 정해지지 않으면 기능은 켜진 채로 쓰이지 않습니다. 탑재율 40%는 시장 공급의 속도를 보여 주는 수치이고, 조직 내부의 정착 정도는 다른 수치로 따로 확인해야 합니다.

의사결정권자가 받는 도입 압력

이 전망이 의사결정권자에게 주는 압력은 구매 결정보다 운영 준비 쪽에서 더 크게 나타납니다. 쓰는 애플리케이션마다 에이전트 기능이 들어오면 부서마다 서로 다른 방식으로 에이전트를 켜고 쓰게 되며, 그 결과 어떤 에이전트가 어떤 데이터를 읽고 무엇을 실행하는지 한곳에서 보기 어렵습니다. 그래서 탑재 전망은 조직이 에이전트를 만들고 지켜보는 공통 창구를 언제 마련할지 묻는 질문으로 바꾸어 읽는 편이 실무에 맞습니다. 1장의 나머지 절은 그 창구가 없을 때 생기는 문제를 차례로 다룹니다.

1.1.2 시험 39%·확대 23% 응답과 업무 기능별 10% 이하 확대 적용 비율

에이전트형 AI 시험·확대 응답 비율

McKinsey가 2025년 11월 발표한 「The state of AI in 2025」 조사에서 응답자의 23%는 조직 어딘가에서 에이전트형 AI를 확대 적용하고 있다고 답했고, 39%는 시험 중이라고 답했습니다[S4]. 두 수치를 더하면 응답 조직의 60% 이상이 어떤 형태로든 에이전트를 다루고 있다는 뜻이므로, 에이전트는 더 이상 일부 선도 기업만의 과제가 아닙니다. 반면 이 수치는 조직 전체 가운데 한 부서라도 해당하면 그렇다고 답하는 방식으로 집계되므로, 조직 전반의 사용 정도를 그대로 보여 주지는 않습니다.

업무 기능 단위 확대 적용 10% 이하

같은 조사에서 업무 기능 하나를 기준으로 보면, 에이전트를 확대 적용했다고 답한 비율은 어느 기능에서도 10%를 넘지 않았습니다[S4]. 여기서 업무 기능은 마케팅·영업·재무·인사·IT 운영처럼 조직이 일을 나누는 단위를 말합니다. 조직 단위로는 다섯 곳 중 한 곳 이상이 확대 단계에 들어섰다고 답하지만, 특정 부서의 일상 업무로 좁혀 보면 열 곳 중 한 곳도 되지 않습니다. 이 차이는 에이전트가 시험 과제나 소수 담당자의 도구로는 쓰이지만, 부서 전체의 반복 업무를 맡는 단계로는 아직 넘어가지 못했다는 사실을 보여 줍니다.

시험 단계에 머무는 에이전트의 공통 조건

시험 단계에 머무는 에이전트에는 몇 가지 공통 조건이 있습니다. 에이전트를 만든 사람과 그 결과를 쓰는 사람이 다르고, 결과를 쓰는 부서 담당자는 에이전트의 구성이나 실행 기록을 직접 볼 수 없습니다. 에이전트가 무엇을 언제 실행했는지, 실패했을 때 누가 알게 되는지도 정해지지 않은 채 운영됩니다. 시험이 끝난 뒤 업무 담당자가 그 에이전트를 넘겨받아 계속 쓰기 어렵고, 에이전트는 만든 사람의 개인 도구로 남습니다. 1.2절과 1.3절은 이 두 조건, 즉 일을 시키는 창구와 지켜보는 창구가 없다는 문제를 각각 다룹니다.

1.2 진행 단계와 실행 승인을 담을 자리가 없는 채팅 창구의 구조

AI Agent에게 일을 시키는 가장 흔한 방법은 텔레그램이나 사내 메신저 같은 채팅 프로그램에 봇을 연결하는 것입니다. 이 방법은 설치가 빠르고 사람에게 익숙하지만, 채팅 프로그램은 사람끼리 주고받는 대화를 위해 만든 도구이므로 에이전트의 작업 상태를 표시할 화면 요소가 없습니다. 에이전트가 지금 몇 번째 단계에 있는지, 어떤 명령을 실행하려 하는지, 무엇을 되묻는지가 모두 같은 모양의 메시지로 흘러갑니다. 의사결정권자 입장에서 이 구조는 누가 무엇을 승인했는지 기록으로 남지 않는다는 통제 문제로 이어지며, 그 해법이 되는 채팅 화면은 4장에서 실제 모습으로 다룹니다.

1.2.1 메시지 한 줄로 흘러가는 실행 승인과 되묻기

채팅 프로그램의 설계 목적과 에이전트 대화의 차이

채팅 프로그램은 사람 두 명 이상이 짧은 글을 주고받는 용도로 설계한 도구이므로, 화면의 기본 단위가 메시지 한 줄입니다. 반면 에이전트와의 대화에는 지시, 진행 상황, 실행 전 확인 요청, 추가 정보 요청, 최종 결과처럼 성격이 다른 내용이 섞여 있습니다. 에이전트가 고객 명단을 정리한 뒤 CRM에 등록하려 할 때, 등록해도 되는지 묻는 확인 요청과 중간 진행 보고가 같은 말풍선 모양으로 나타납니다. 사람이 반드시 답해야 하는 메시지와 읽고 넘겨도 되는 메시지를 화면만 보고는 구분할 수 없습니다.

승인 요청과 일반 메시지의 혼재

이 구조에서 실행 승인은 담당자가 「네」라고 입력한 메시지 한 줄로 끝납니다. 그런데 메시지 한 줄은 어떤 명령에 대한 승인이었는지, 승인할 때 화면에 어떤 내용이 보였는지를 함께 남기지 않습니다. 대화가 길어지면 승인 요청이 다른 메시지에 밀려 올라가고, 담당자는 앞선 맥락을 다시 찾아 읽어야 합니다. 그 결과 승인이 필요한 일과 그렇지 않은 일의 경계가 대화 습관에 따라 달라지며, 같은 에이전트라도 담당자마다 다르게 쓰이게 됩니다.

승인 기록이 남지 않을 때의 통제 문제

승인 기록이 남지 않는 문제는 의사결정권자에게 감사 추적과 책임 소재의 문제로 돌아옵니다. Gartner는 2028년까지 허가되지 않은 AI Agent 행위의 80% 이상이 외부 공격보다 정보 과다 공유나 부적절한 사용 같은 내부 정책 위반에서 나온다고 전망했습니다[S3]. 내부 정책 위반을 가려내려면 어떤 실행이 누구의 승인을 거쳤는지를 먼저 기록해 두어야 합니다. 따라서 에이전트에게 일을 시키는 창구는 대화 기능에 더해 진행 단계,

실행 예정 명령, 승인과 되묻기를 구분해 보여 주고 그 이력을 남겨야 합니다. 아래 표는 채팅 프로그램과 에이전트 전용 콘솔이 같은 정보를 어떻게 다르게 다루는지 비교한 것입니다.

항목	채팅 프로그램	에이전트 전용 콘솔
진행 단계	일반 메시지로 표시, 단계 구분 없음	현재 단계를 별도 표시
실행하려는 명령	표시하지 않거나 본문에 섞임	실행 전 명령 내용을 따로 표시
실행 승인	「네」 메시지 한 줄	승인 카드와 승인 이력
되묻기	일반 질문 메시지	답이 필요한 항목을 따로 표시
정기 업무 결과	전달 대상 채널에만 도착	실행 기록과 실패 여부를 한 화면에서 조회

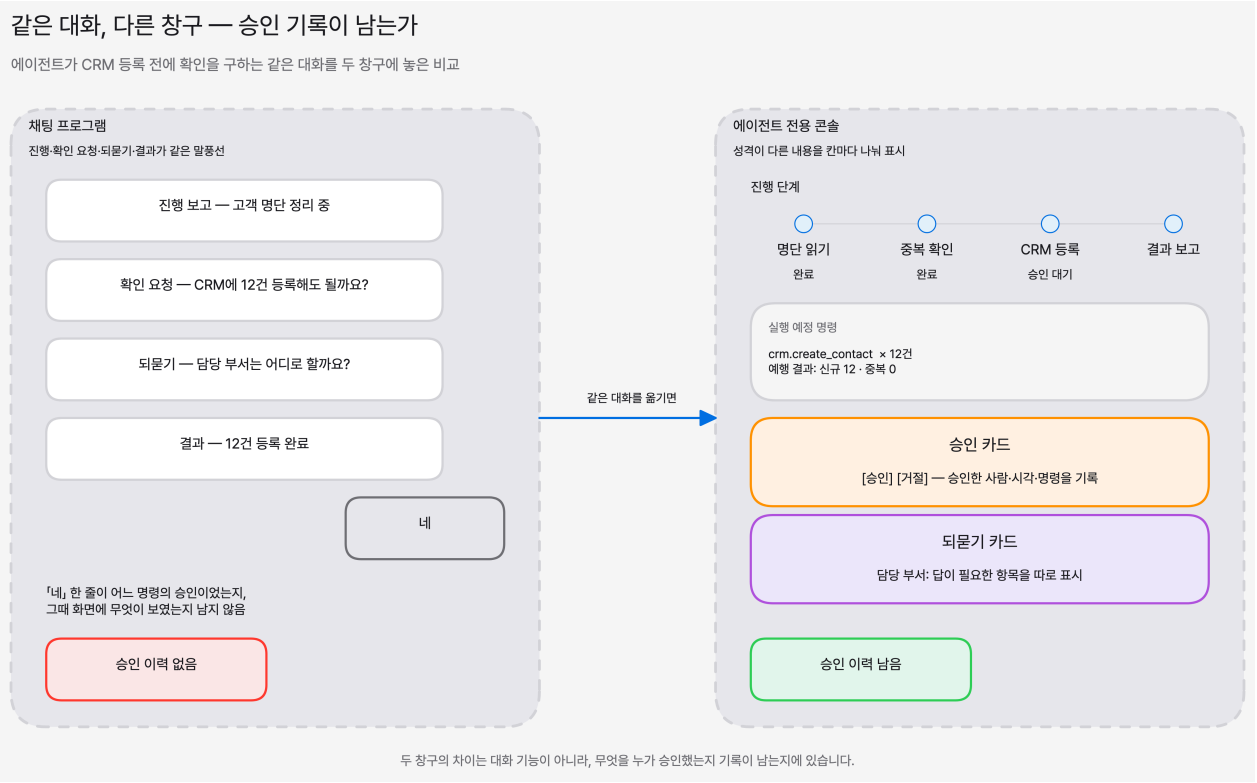


그림 1-1. 채팅 프로그램에서 한 줄 메시지로 섞이는 승인·진행 단계·되묻기와, 에이전트 전용 콘솔이 이를 따로 표시하는 구조 비교

사람 승인을 마지막 안전망으로 둘 때의 조건

사람 승인을 에이전트 통제의 마지막 안전망으로 삼는 조직일수록 승인하는 순간 담당자의 눈앞에 무엇이 보이는지가 중요해집니다. 에이전트가 골라 보여 준 근거만 보고 「네」를 누르면, 기록에는 담당자가 승인했다는 한 줄만 남고 무엇을 근거로 승인했는지, 그 근거를 누가 골랐는지는 남지 않습니다. 이런 상태에서 사고가 나면 조사 과정에서 에이전트의 역할은 드러나지 않고 결과가 담당자의 판단 착오로 정리되며, 같은 구조는 그대로 남아 다음 사고로 이어집니다. 그래서 에이전트에게 일을 시키는 창구는 승인 카드에 실행하려는 명령과 대상을 함께 보여 주고, 승인 이력에도 승인 당시 화면에 보였던 내용을 남겨야 감사에서 쓸 수 있는 기록이 됩니다. 승인 절차의 강도는 승인 버튼의 유무가 아니라 승인할 때 사람이 무엇을 보았는지가 정합니다.

1.2.2 봇 등록과 토큰 복사가 에이전트마다 반복되는 설정 분산

에이전트마다 반복되는 봇 등록 작업

채팅 프로그램을 창구로 쓰면 에이전트를 하나 늘릴 때마다 같은 준비 작업을 되풀이해야 합니다. 메신저 관리 화면에서 봇을 새로 등록하고, 발급받은 토큰을 복사해 에이전트 설정에 붙여 넣은 뒤, 봇을 대화방이나 채널에 연결합니다. 이 작업을 에이전트 수만큼 반복해야 하며, 토큰을 복사하는 과정에서 같은 값이 여러 설정 파일에 흩어지게 됩니다. 에이전트가 다섯 개를 넘어가면 어느 봇이 어느 에이전트에 연결되어 있는지, 토큰을 바꿔야 할 때 어디를 고쳐야 하는지를 기억에 의존하게 됩니다.

설정 파일·관리 화면·명령줄로 나뉜 설정 위치

에이전트를 구성하는 설정도 한곳에 모여 있지 않습니다. 에이전트가 쓰는 모델, 일하는 방법을 적은 스킬, 정해진 시각에 실행되는 정기 업무(크론), 메신저 연결 정보는 대개 서로 다른 위치에 따로 있습니다. 아래 표는 오픈소스 에이전트 플랫폼을 채팅 프로그램과 함께 쓸 때 흔히 나타나는 설정 위치를 정리한 것입니다.

설정 항목	흔히 관리되는 위치	대화창에서 확인 가능 여부
모델과 모델 제공자 키	설정 파일, 환경 변수	불가
스킬(일하는 방법을 적은 문서)	서버의 스킬 폴더	불가
정기 업무(실행 일정과 전달 대상)	명령줄(CLI) 또는 관리 화면	불가
메신저 봇 토큰	메신저 관리 화면에서 발급 후 설정 파일에 복사	불가
대화와 실행 결과	채팅 프로그램	가능

설정 분산이 만드는 변경 추적 공백

설정이 대화와 끊겨 여러 위치에 흩어지면, 에이전트의 동작이 바뀌었을 때 그 원인을 대화창에서 찾을 수 없습니다. 예를 들어 어제까지 잘 실행되던 보고서 작성 에이전트가 오늘 다른 형식으로 결과를 보냈다면, 담당자는 모델이 바뀌었는지, 스킬 문서가 고쳐졌는지, 정기 업무의 일정이 바뀌었는지를 각각 다른 곳에서 확인해야 합니다. 명령줄에 익숙하지 않은 부서 담당자는 이 확인을 IT 담당자에게 요청할 수밖에 없습니다. 에이전트를 업무에 맞게 고치는 일이 업무를 아는 담당자에게서 멀어지고, 변경 추적은 IT 담당자의 기억과 개별 메모에 기대게 됩니다.

1.3 세션 92%가 정기 업무에서 시작되는 에이전트와 알림이 안 가는 실패

에이전트가 업무에 정착할수록 실행의 대부분은 사람의 지시보다 정해진 일정에서 시작됩니다. 정기 업무는 매일 아침 보고서 작성이나 매시간 메일함 확인처럼 정해진 시각에 에이전트를 자동으로 실행하는 작업이며, 이 작업은 담당자가 화면을 보고 있지 않을 때도 동작합니다. 그래서 운영에서 중요한 질문은 대화창에서 무엇을 주고받았는지와 함께, 사람이 보지 않는 동안 어떤 작업이 실행되고 어떤 작업이 실패했는지로 넓어집니다. 이 질문에 답하지 못하는 상태는 경영 관점에서 업무가 멈춰도 아무도 모르는 위험이 됩니다.

1.3.1 최근 7일 세션 152개 가운데 사람이 시작한 세션의 비중

정기 업무가 시작한 세션의 비중

AAS의 활동 화면은 에이전트 실행 단위인 세션이 누구에게서 시작되었는지를 집계해 보여 줍니다. 그림 1-2의 예에서 최근 7일 동안 열린 세션은 152개이며, 그 가운데 92%가 사람이 건 대화가 아니라 정기 업무에서 시작되었습니다. 이 예에서는 에이전트 실행 열 건 중 아홉 건 이상이 담당자가 채팅 창을 열지 않은 상태에서 일정에 따라 시작한 실행입니다. 같은 화면은 최근 7일 동안 세션이 하나도 없는 에이전트 프로파일 4개를 따로 표시해, 만들어 두고 쓰이지 않는 프로파일도 함께 드러냅니다.

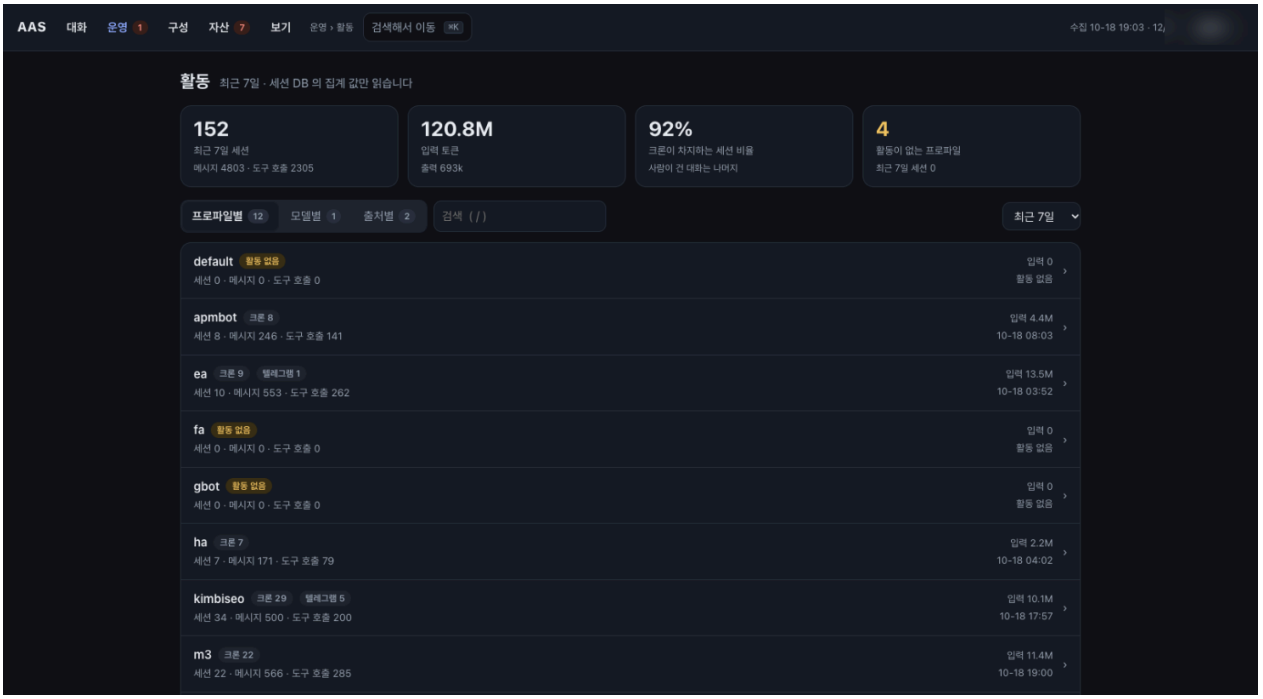


그림 1-2. AAS 활동 화면의 예. 상단 숫자 상자에서 최근 7일 세션 수와 정기 업무가 차지하는 세션 비율을 보고, 아래 목록에서 프로파일마다 정기 업무와 메신저 대화로 시작된 세션 수를 비교합니다

사람이 시작한 세션이 적을 때 생기는 확인 공백

이 비율은 채팅 프로그램이 에이전트 운영의 일부만 보여 준다는 사실을 수치로 드러냅니다. 채팅 창에는 사람이 시작한 세션 8% 남짓의 대화만 남고, 나머지 92%의 실행은 결과 메시지가 도착했을 때만 간접적으로 확인할 수 있습니다. 결과 메시지가 오지 않으면 담당자는 작업이 실행되지 않았는지, 실행되었지만 실패했는지, 결과를 보낼 곳이 없었는지를 구분할 수 없습니다. 담당자에게 필요한 것은 대화 기록보다 실행 기록이며, 그 기록이 대화창과 같은 화면에 있어야 업무 담당자가 직접 확인할 수 있습니다.

단계마다 사람이 빠질 때 커지는 오류의 전파

사람이 보지 않는 실행이 많아질수록 실행 기록에 담아야 할 내용도 달라집니다. 챗봇은 질문 하나에 답 하나를 돌려주고 멈추므로 다음에 무엇을 할지 정하는 주체가 언제나 사람이지만, 에이전트는 목표를 받으면 어떤 도구를 부르고 어떤 파일을 열고 언제 멈출지를 스스로 정하며 여러 단계를 이어 갑니다. 정기 업무로 실행되는 에이전트에서는 담당자가 중간 결과를 읽고 다음 지시를 내리던 확인 절차가 단계마다 빠지므로, 한 단계의 잘못된 판단이 그대로 다음 단계의 입력이 됩니다. 예를 들어 조회 단계에서 기간을 잘못 잡으면 작성 단계는 틀린 데이터로 그럴듯한 보고서를 만들고, 발송 단계는 그 보고서를 그대로 내보냅니다. 따라서 실행 기록은 성공과 실패 여부에 더해 각 실행이 어떤 스킬과 도구를 거쳤는지까지 보여 주어야, 이상한 결과가 나왔을 때 담당자가 원인을 거꾸로 따라갈 수 있습니다.

업무 화면 예시를 읽는 기준

그림 1-2의 숫자는 AAS가 하나의 운영 설치본에서 보여 주는 화면 예이며, 세션 수와 비율은 조직의 업무 구성에 따라 달라집니다. 다만 업무 자동화를 목적으로 에이전트를 쓰는 조직이라면, 정기 업무가 차지하는 비중은 사용 기간이 길어질수록 커지는 경향을 보입니다. 화면에 나오는 업무 에이전트와 연결 시스템(CRM·위키·드라이브 등)은 고객 환경에 맞춰 설정합니다. 의사결정권자가 이 화면에서 확인할 것은 숫자의 크기보다, 사람이 보지 않는 실행을 집계해 한 화면에 보여 주는 기능이 있는지 여부입니다.

1.3.2 전달 대상이 없는 정기 업무에서 실패가 드러나지 않는 경로

정기 업무의 실패 알림 경로

정기 업무는 만들 때 결과를 보낼 전달 대상을 함께 정합니다. 전달 대상은 특정 메신저 대화방, 채널, 메일 주소처럼 결과 메시지가 도착하는 곳이며, 작업이 실패했을 때의 알림도 대개 같은 대상으로만 갑니다. 따라서 전달 대상이 정해져 있지 않은 작업은 성공 결과뿐 아니라 실패 알림도 갈 곳이 없습니다. 데이터를 수집해 파일로만 저장하는 정기 업무는 결과를 메시지로 보낼 필요가 없어 전달 대상 없이 만들어지는 경우가 많고, 이런 작업이 실패하면 아무에게도 알려지지 않습니다.



그림 1-3. 정기 업무의 실패 알림이 전달 대상으로만 가는 경로와, 전달 대상이 없는 작업에서 실패가 드러나지 않는 경로

알림이 안 가는 작업이 생기는 조건

알림이 안 가는 작업은 대개 세 가지 조건에서 생깁니다. 처음부터 전달 대상 없이 만든 작업, 전달 대상으로 지정한 대화방이나 채널이 나중에 삭제되거나 봇이 빠진 작업, 그리고 담당자가 바뀌면서 전달 대상이 퇴사자 개인 대화방으로 남은 작업입니다. 세 경우 모두 작업 목록에서는 정상적으로 등록된 것처럼 보이므로, 설정 파일이나 명령줄로 작업을 하나씩 열어 보기 전에는 발견하기 어렵습니다. 정기 업무가 수십 개를 넘어가면 알림 경로 점검은 사람의 기억으로 감당하기 어려운 일이 됩니다.

실패가 드러나지 않을 때의 업무 영향

전달 대상이 없는 작업의 실패는 그 결과를 기다리던 업무가 멈춘 뒤에야 드러납니다. 예를 들어 매일 아침 영업 현황을 모아 두는 작업이 실패하면, 그 데이터를 쓰는 주간 보고서가 비어 있는 것을 발견할 때까지 며칠이 지날 수 있습니다. 반면 실행 기록을 한곳에 모아 보는 화면이 있으면, 알림 경로와 상관없이 실패한 작업과 멈춘 작업을 먼저 찾아낼 수 있습니다. AAS의 Cron 헬스체크 화면은 정기 업무 95개 중 알림이 안 가는 작업 15개를 목록으로 드러내며, 이 관측 기능은 6장에서 자세히 다룹니다. 다만 화면이 드러내는 것은 원인을 찾는 단서이고, 원인을 찾아 고치는 일은 여전히 담당자의 몫입니다.

실패하지 않은 작업이 맞는 결과를 냈다는 뜻은 아닌 이유

실행 기록이 보여 주는 것은 작업이 끝났는지와 실패했는지이고, 결과가 맞았는지까지는 아닙니다. 정상 종료된 작업도 엉뚱한 기간의 데이터를 모았거나 빈 결과를 성공으로 보고할 수 있으며, 에이전트는 결과를 그럴듯한 문장으로 다듬어 내놓기 때문에 겉으로는 구분이 어렵습니다. 그래서 반복 업무를 에이전트에 맡길 때는 실패 감시와 별도로 결과 검증의 주기와 기준을 정해 두어야 합니다. 예를 들어 영업 현황 수집 작업이라면 담당자가 정해진 주기마다 원본 시스템의 건수와 수집 결과의 건수를 대조하는 식입니다. 이 검증 절차는 10장의 첫 유즈케이스 선정 기준에서 「결과 확인 용이성」으로 다시 다룹니다.

1.4 에이전트형 AI 프로젝트 40% 중단 전망과 첫 유즈케이스 파일럿 판단

Gartner는 2025년 6월 25일 보도자료에서 에이전트형 AI 프로젝트의 40% 이상이 2027년 말까지 중단된다고 전망했습니다[S2]. 중단 사유로는 비용 증가, 불분명한 사업 가치, 부족한 위험 통제의 세 가지가 꼽혔으며, 이 사유들은 1.2절과 1.3절에서 다룬 창구 부재와 직접 맞닿아 있습니다. 에이전트 도입을 검토하는 조직은 프로젝트를 넓게 시작하기보다, 결과를 확인하기 쉬운 업무 하나를 골라 만들고 지켜보는 과정을 먼저 갖추는 편이 중단 위험을 낮춥니다. 이어지는 두 항은 중단 사유를 창구 관점으로 다시 정리하고, 의사결정권자가 내릴 첫 결정과 그 근거가 실린 장을 안내합니다.

1.4.1 비용·사업 가치·위험 통제 부족으로 정리되는 중단 사유

Gartner가 제시한 세 가지 중단 사유

Gartner는 에이전트형 AI 프로젝트 중단의 원인으로 비용 증가, 불분명한 사업 가치, 부족한 위험 통제를 들었습니다[S2]. 2025년 1월 3,400여 명이 참여한 Gartner 웨비나 설문에서 에이전트형 AI에 의미 있는 투자를 했다는 응답은 19%, 신중하게 투자했다는 응답은 42%, 아직 정하지 않았다는 응답은 31%였습니다[S2]. 투자 결정을 미루는 조직이 많은 상황에서 이미 시작한 프로젝트도 상당수가 중단 위험을 안고 있습니다.

넓게 시작한 프로젝트가 겪는 문제

넓은 범위로 시작한 에이전트 프로젝트는 세 가지 중단 사유를 한꺼번에 겪기 쉽습니다. 여러 부서의 업무를 동시에 다루면 모델 호출과 연결 작업이 늘어 비용이 먼저 커지고, 성과를 업무 단위로 나누어 보이기 어려워 사업 가치를 설명하기 어렵습니다. 에이전트가 많아질수록 무엇이 언제 실행되는지 지켜보기 어려워져 위험 통제가 뒤따르지 못합니다. 반면 업무 하나로 좁혀 시작하면 처리 건수와 담당자 확인 시간처럼 효과를 셀 수 있는 지표가 생기고, 실행 기록도 한 사람이 끝까지 확인할 수 있습니다.

중단 사유와 업무 창구 부재의 관계

세 가지 중단 사유는 모두 에이전트를 만들고 지켜보는 창구가 없을 때 더 커집니다. 아래 표는 각 사유를 창구 관점에서 다시 읽고, 그 대응 방법을 다루는 장을 짝지은 것입니다.

중단 사유[S2]	창구가 없을 때 나타나는 모습	대응을 다루는 장
비용 증가	실행 횟수와 모델 사용량을 에이전트별로 볼 수 없음	4장(만들기·지켜보기 화면), 6장
불분명한 사업 가치	어떤 업무를 몇 건 처리했는지 부서 단위로 남지 않음	5장(업무 에이전트 카탈로그), 8장
부족한 위험 통제	승인 이력·정기 업무 실패·자격증명 상태가 흩어져 있음	6장(관측 화면), 7장(보안 원칙)

1.4.2 명함·회의록·공문 중 첫 유즈케이스를 고르는 결정과 장별 판단 근거

의사결정권자에게 요청하는 첫 결정

이 백서가 의사결정권자에게 요청하는 결정은 하나입니다. 부서 업무 가운데 에이전트에 맡길 첫 유즈케이스 하나를 골라 파일럿 대상을 정하는 것입니다. 후보로는 받은 명함을 읽어 고객 정보로 등록하는 명함 인식, 회의 녹음을 화자 구분 회의록으로 만들고 지시사항과 할 일을 뽑아내는 회의록 정리, 공문과 공공서식을 읽어 기안문 빈칸을 채우는 공문 처리를 먼저 검토할 만합니다. 세 업무는 처리량이 많고 반복되며, 에이전트가 만든 결과를 담당자가 등록 전에 확인할 수 있다는 공통점이 있습니다. 따라서 결과가 틀렸을 때의 영향이 작고, 1.4.1에서 다룬 비용·가치·위험을 업무 하나 안에서 셀 수 있습니다.

첫 유즈케이스를 고르는 기준

첫 유즈케이스를 고를 때는 다음 세 가지 조건을 함께 확인합니다.

- 같은 형식의 일이 매주 수십 건 이상 반복되어 처리 건수로 효과를 셀 수 있는가
- 에이전트가 만든 결과를 담당자가 등록이나 발송 전에 확인할 수 있는가
- 결과가 틀렸을 때 되돌리기 쉬워 업무 영향이 작은가

이 조건을 모두 만족하는 업무가 여럿이면, 결과를 받아 쓰는 담당자가 가장 가까이 있는 업무를 먼저 고르는 편이 좋습니다. 그래야 에이전트의 결과를 매일 확인하고 스킬을 고치는 사람이 같은 부서 안에 있게 됩니다.

장별로 얻는 판단 근거

이 결정을 내리는 데 필요한 근거는 장별로 나뉘어 있습니다. 아래 표는 의사결정권자가 던질 질문과 그 답이 실린 장을 짝지은 것이며, 가격과 라이선스는 이 백서에서 다루지 않습니다.

결정 전에 확인할 질문	근거가 실린 장
AAS는 무엇이고 누가 쓰는가, 업무 담당자가 직접 에이전트를 만들 수 있는가	3장
명함 인식·화자 구분 회의록·공공서식 인식 등 어떤 업무 에이전트를 바로 쓸 수 있는가	5장

결정 전에 확인할 질문	근거가 실린 장
쓰던 에이전트 플랫폼을 고치지 않고 연결할 수 있는가, 온프레미스로 조직 안에 설치할 수 있는가	7장
다른 선택지와 비교해 앞서는 점과 부족한 점은 무엇인가	9장
첫 유즈케이스를 고른 뒤 어떤 순서로 도입을 시작하는가	10장

판단 전에 알아 둘 연결 범위

다만 AAS가 지금 연결하는 에이전트 플랫폼은 오픈소스 Hermes Agent 1종이므로, 조직이 다른 에이전트 플랫폼을 쓰고 있다면 7장과 9장의 연결 범위를 먼저 확인해야 합니다. 업무 에이전트가 쓰는 CRM·위키·드라이브 같은 연결 시스템은 조직의 환경에 맞춰 따로 설정합니다. 이 두 가지를 확인한 뒤 첫 유즈케이스 하나를 정하면, 이후 장에서 읽는 기능과 화면을 그 업무에 대입해 파일럿 범위를 구체적으로 그릴 수 있습니다. 그에 앞서 2장은 이 창구 문제를 시장의 도구들이 어디까지 풀었고 어느 자리가 비어 있는지를 살펴봅니다.

2장: AI Agent 도구 시장의 인접 6개 세그먼트와 비어 있는 자리 — 조직 안 업무 담당자용 콘솔

1장에서 본 창구 부재는 결국 어떤 도구를 고를 것인가라는 질문으로 이어집니다. 기업용 애플리케이션에 에이전트 탑재가 빠르게 늘어난다는 전망[S1]에 따라 도구 선택은 IT 부서의 시험 과제를 넘어 업무 부서의 도입 의사결정 문제가 됐습니다. 그런데 AI Agent 도구 시장은 하나의 제품군으로 묶이지 않고, 같은 「에이전트 도구」라는 이름 아래 하는 일과 사용자가 서로 다른 여섯 구분이 섞여 있습니다. 2장은 먼저 용어와 구분 기준을 정하고 여섯 구분을 표 하나로 보여 준 뒤, 구분마다 맡는 일과 맡지 않는 일, 시장 흐름, 국내 설치 조건을 차례로 겹쳐 어떤 조합이 비어 있는지를 설명합니다. 구분마다 대표 회사와 제품을 실명으로 적고, 9장 비교표에 올리는 대표 제품 12개는 2.1.3에서 따로 정리합니다.

2.1 AI Agent 도구를 나누는 네 가지 기준과 여섯 가지 구분

AI Agent 도구는 무엇을 다루는지, 누가 쓰는지, 실행 엔진을 스스로 갖는지, 어디에 설치하는지의 네 기준으로 나누면 여섯 구분으로 정리할 수 있습니다. 이 절은 그 기준에 쓰이는 용어 다섯 개를 먼저 정의하고, 여섯 구분과 구분별 대표 제품을 표 2-1로, 9장 비교에 쓰는 대표 제품 12개를 표 2-2로 보여 줍니다. 뒤의 절들은 모두 이 두 표의 순서를 따라 설명하므로, 두 표를 먼저 읽어 두면 2장과 9장의 비교를 같은 틀로 따라갈 수 있습니다.

2.1.1 에이전트를 직접 실행하는지로 구분한 다섯 가지 도구 용어

에이전트 도구 용어 다섯 개와 각 도구가 직접 실행하는 대상

시장 자료에서는 빌더, 콘솔, 플랫폼, 런타임, 관제 도구라는 말이 정의 없이 섞여 쓰이지만, 이 백서는 다섯 용어를 아래처럼 구분해 씁니다. 다섯 용어를 가르는 핵심은 그 도구가 에이전트를 직접 실행하는지, 아니면 다른 엔진에 일을 맡기거나 기록만 모으는지입니다. 예를 들어 같은 「에이전트를 만든다」는 화면이라도 자기 엔진에서 실행하는 빌더와 남의 엔진에 설정을 넘기는 콘솔은 도입했을 때 바꿔야 하는 시스템의 범위가 다릅니다.

용어	한 줄 정의	무엇을 직접 실행하는가
에이전트 플랫폼(런타임)	에이전트가 실제로 실행되는 엔진. 모델 호출, 도구 실행, 기억, 정기 업무를 처리한다	에이전트 자체(예: 오픈소스 Hermes Agent)
빌더	에이전트를 정의하는 화면. 대부분 자기 런타임과 한 제품으로 묶여 있다	자기 런타임에서 만든 에이전트
콘솔	이미 있는 에이전트 플랫폼 위에서 설정, 실행 지시, 기록 확인을 다루는 화면	직접 실행하지 않고 연결한 플랫폼에 맡긴다
관제·거버넌스 도구	조직 안의 여러 에이전트를 등록하고 감시하고 통제하는 도구	실행하지 않고 실행 기록을 모아 감시한다
채팅 UI	여러 AI 모델 가운데 하나를 골라 대화하는 화면	모델 호출과 대화 응답

런타임(runtime)이 공급사의 것이면 공급사가 에이전트 정의, 실행 기록, 자격증명을 모두 자기 환경에 저장합니다. 반면 콘솔은 조직이 고른 에이전트 플랫폼을 그대로 두고 그 위에서 동작하므로, 데이터가 머무는 위치는 플랫폼을 설치한 곳이 정합니다. 이 백서에서 「빌더」와 「콘솔」을 나눠 부르는 이유는 화면 모양의 차이보다 실행 엔진을 누가 갖느냐의 차이를 드러내기 위해서입니다.

2.1.2 만드는 쪽 셋과 지켜보는 쪽 셋으로 나뉘는 AI Agent 도구 여섯 구분

여섯 구분을 가르는 네 가지 기준

여섯 구분은 다음 네 기준을 차례로 적용해 나눈 결과입니다.

- ① 무엇을 다루는가 — 에이전트를 만드는 일, 일을 시키는 일, 실행을 지켜보는 일 가운데 어디까지 맡는가
- ② 누가 쓰는가 — 개발자, 플랫폼 운영자, IT·보안팀, 업무 담당자 가운데 누구를 위해 설계했는가
- ③ 실행 엔진을 스스로 갖는가 — 자기 런타임을 함께 제공하는가, 이미 있는 에이전트 플랫폼 위에 얹는가
- ④ 어디에 설치하는가 — 공급사의 외부 클라우드인가, 조직 안의 서버인가

앞의 두 기준이 「누구를 위해 무엇을 하는가」를 정한다면, 뒤의 두 기준은 「도입하면 무엇을 바꾸고 데이터가 어디에 남는가」를 정합니다. 기능 목록만 비교하면 비슷해 보이는 도구도 뒤의 두 기준에서 갈라지는 경우가 많습니다.

AI Agent 도구 여섯 구분의 대표 제품과 AAS와의 관계

네 기준을 적용한 여섯 구분과 구분별 대표 회사·제품, 각 구분이 AAS와 겹치는 점과 다른 점은 표 2-1과 같습니다. 「대표 회사 / 제품」 열은 구분마다 시장에서 자주 비교되는 제품을 적은 것이며, 그 가운데 AAS와 직접 견줄 12개는 2.1.3의 표 2-2에서 다시 풀어 씁니다.

표 2-1. AI Agent 도구의 여섯 구분과 대표 제품

구분	대표 회사 / 제품	하는 일	주로 쓰는 사람	다루는 것(만들기·시키기·지켜보기)	실행 엔진	AAS와 겹치는 점 / 다른 점
① 업무 담당자용 에이전트 빌더(상용)	Microsoft Copilot Studio, Google Gemini Enterprise, Salesforce Agentforce, Anthropic Claude Cowork, Dust, Glean, 삼성SDS	문장이나 노코드 화면으로 에이전트를 만들어 조직 안에서 나눠 쓴다	업무 담당자, 관리자	만들기·시키기, 지켜보기는 분석 화면 수준	자체(공급사 런타임 일체형)	대상 사용자, 만들기, 예약, 사내 공유가 겹침 / 자사 런타임 일체형이고 대부분 외부 클라우드(SaaS)

구분	대표 회사 / 제품	하는 일	주로 쓰는 사람	다루는 것(만들기·시키기·지켜보기)	실행 엔진	AAS와 겹치는 점 / 다른 점
	FabriX, 올거나이즈 Alli					
② 에이전트·워크플로 빌더(오픈소스)	Dify, Flowise, Langflow, n8n	캔버스에서 노드를 이어 에이전트 앱을 조립한다	개발자	만들기·시키기	자체 실행 엔진	화면에서 정의, 자체 호스팅이 겹침 / 개발자 지향, 자체 엔진
③ 채팅 UI·워크스페이스	Open WebUI, LibreChat, AnythingLLM	여러 AI 모델과 대화하는 화면을 업무 담당자에게 제공한다	업무 담당자	시키기	모델 호출 중심(에이전트 플랫폼 운영 없음)	대화, 그룹 권한, 예약이 겹침 / 에이전트 플랫폼의 구성·운영을 다루지 않음
④ 에이전트 관제·거버넌스	Microsoft Agent 365, ServiceNow AI Control Tower, Langfuse, Datadog AI Agents Console	조직의 에이전트를 등록하고 감시하고 통제한다	IT 운영팀, 보안팀	지켜보기	없음(다른 엔진의 실행을 감시)	실패 감시, 호출 추적, 감사가 겹침 / 만드는 화면이 없음
⑤ 에이전트 플랫폼 전용 콘솔(오픈소스)	Hermes Agent 내장 대시보드, hermes-webui, Ekko Studio, hermes-control-interface	특정 런타임의 프로파일, 정기 업무, 스킬, 키, 로그를 다룬다	플랫폼 운영자 한 명	만들기·시키기·지켜보기 (운영자 수준)	남의 플랫폼 (Hermes Agent) 위에 얹음	같은 플랫폼, 같은 메뉴가 대부분 겹침 / 한 사람 사용 전제, 권한 분리·사내 마켓 없음
⑥ 에이전트 조직 운영 콘솔(오픈소스)	Paperclip, Multica, Kortix	에이전트를 직원처럼 두고 과업과 예산을 관리한다	비개발자, 개발팀	만들기·시키기·지켜보기	남의 플랫폼 (여러 런타임) 위에 얹음	비개발자 대상, 스킬 공유, 예약, 감사, 플랫폼 중립이 겹침 / 화면 은유가 회사 경영이거나 개발팀 전용

표 2-1을 읽는 순서와 결론

표 2-1은 세로로 두 덩어리로 읽으면 이해하기 쉽습니다. ①②③은 에이전트를 만들고 일을 시키는 쪽이고, ④⑤⑥은 실행을 지켜보는 기능을 가진 쪽입니다. ⑤와 ⑥도 만들기 화면을 갖추지만, 자기 실행 엔진 없이 이미 있는 에이전트 플랫폼 위에 얹혀 그 플랫폼을 운영하고 지켜보는 화면에서 출발했다는 점에서 지켜보는 쪽으로 묶었습니다. 만드는 쪽의 두 빌더는 자기 실행 엔진을 함께 제공하고 채팅 UI는 에이전트 플랫폼 운영을 다루지 않으며, 지켜보는 쪽의 관제 도구는 만드는 화면이 없고 플랫폼 전용 콘솔은 운영자 한 명을 전제로 합니다. 이미 쓰는 에이전트 플랫폼 위에서 업무 담당자가 만들기와 지켜보기를 한 화면으로 함께 다루는 구분은 여섯 가운데 어디에도 온전히 들어 있지 않으며, 이것이 2장이 끝에서 확인하는 비어 있는 조합입니다. AAS는 ⑤에서 출발해 ①의 사용자를 겨냥하는 제품으로, 같은 플랫폼 위에 얹히되 대상은 부서의 업무 담당자입니다.

2.1.3 9장 비교에 쓰는 대표 제품 12개와 소속 구분

대표 제품 12개의 성격과 표 2-1 구분과의 대응

9장에서 AAS와 기능을 하나씩 견주는 제품은 표 2-1의 구분 ①③⑤⑥에서 AAS와 가장 가까운 12개입니다. 구분 ①에서는 기능 범위가 가장 넓은 글로벌 클라우드 빌더 셋과 온프레미스를 지원하는 글로벌·국내 플랫폼 셋을, 구분 ⑤에서는 AAS와 같은 오픈소스 에이전트 플랫폼인 Nous Research의 Hermes Agent 위에서 동작하는 콘솔 넷을, 구분 ⑥과 ③에서는 제품 정의가 가까운 Paperclip과 Open WebUI를 골랐습니다. 아래 표와 9장 비교표의 내용은 직접 써 본 결과가 아니라 각 공급사와 프로젝트가 공개한 공식 자료를 2026년 10월 8일 기준으로 읽은 결과입니다.

표 2-2. 9장 비교에 쓰는 대표 제품

회사	제품	성격	강한 것	표 2-1의 구분	설치 형태
Microsoft	Copilot Studio(+ Agent 365) [S9][S10]	에이전트와 워크플로를 만들고 관리하는 로코드 스튜디오. Agent 365는 IT·보안팀용 관제	자연어로 만들기, Agent Store, 역할 기반 접근, 비용 관리, 에이전트 맵(Agent 365)	① 글로벌 클라우드 빌더	자사 클라우드. 온프레미스는 공식 자료에서 확인되지 않음
Anthropic	Claude Cowork[S11]	비개발 직군이 스킬과 플러그인을 만들어 쓰는 업무 에이전트	스킬·사설 플러그인 마켓, 예약 작업, 지출 한도, 활동 기록 전송	① 글로벌 클라우드 빌더	데스크톱 앱과 클라우드. 온프레미스 설치형 아님
Dust	Dust[S12]	「AI 오퍼레이터」가 팀의 에이전트를 만들고 굴리는 빌더	지시문·모델·도구·스킬·접근 권한을 폼으로 다루는 빌더, 20개 넘는 모델	① 글로벌 클라우드 빌더	SaaS(미국·EU)와 단일 테넌트

회사	제품	성격	강한 것	표 2-1의 구분	설치 형태
IBM	watsonx Orchestrate[S13]	여러 에이전트를 한 제어 평면에서 만들고 관리하는 플랫폼	온프레미스 공식 지원, 노코드·프로코드 빌더, 에이전트·도구 카탈로그, 외부 에이전트 조율	① 글로벌 온프레미스	IBM Cloud, AWS, 온프레미스
삼성SDS	FabriX(Agent Studio)[S14]	검증된 템플릿과 자연어로 비개발자가 에이전트를 만드는 플랫폼	에이전트 스토어, 부서·사용자별 할당량, 에이전트 간 협업	① 국내 온프레미스	클라우드 기본, 하이브리드·온프레미스
올거나이즈	Alli[S15]	노코드 앱 빌더로 에이전트와 업무 자동화 앱을 만드는 플랫폼	직군별 에이전트 100여 개를 담은 앱 마켓, 여러 LLM	① 국내 온프레미스	SaaS와 온프레미스(폐쇄망 포함)
Nous Research	Hermes Agent 내장 대시보드[S16]	에이전트 플랫폼 본체가 제공하는 운영자용 웹 관리 화면	채팅, 프로파일, 정기 업무, 스킬, 키, 로그, 사용량이 한 화면	⑤ Hermes Agent 위 오픈소스 콘솔	조직 안 설치 (MIT 라이선스)
오픈소스 프로젝트	hermes-webui[S17]	채팅 중심의 Hermes Agent 웹 UI	채팅·세션·정기 업무 패널, 위험 명령 승인, 활발한 개발	⑤ Hermes Agent 위 오픈소스 콘솔	조직 안 설치 (MIT 라이선스)
오픈소스 프로젝트	Ekko Studio[S18]	Hermes Agent 를 포함한 여러 런타임을 묶는 스튜디오	여러 런타임 지원, 그룹 채팅, 캔버스 워크플로	⑤ Hermes Agent 위 오픈소스 콘솔	조직 안 설치·데스크톱 앱 (BUSL-1.1, 상업 사용은 별도 라이선스)
오픈소스 프로젝트	hermes-control-interface[S19]	Hermes Agent 운영자용 관제판	역할 3종과 사용자별 프로파일 제한, 사용량·예산 알림	⑤ Hermes Agent 위 오픈소스 콘솔	조직 안 설치 (MIT 라이선스)
오픈소스 프로젝트	Paperclip[S20]	에이전트를 직원처럼 두고 과업과 예산을 관리하는 회사 운영 콘솔	여러 런타임 어댑터, 비개발자 지향, 예산 자동 정지, Skill Studio	⑥ 플랫폼 중립 조직 운영 콘솔	조직 안 설치 (MIT 라이선스)
오픈소스 프로젝트	Open WebUI[S21]	자체 호스팅 AI 채팅 플랫폼	LDAP·OAuth·SCIM 연동, 그룹 권한, 채널, 예약 실행	③ 채팅 워크스페이스	조직 안 설치 (Open WebUI License, 브랜딩 변경 제한 조항)

표 2-2의 구분 ① 여섯 제품은 같은 구분에 속하지만 설치 위치에서 갈립니다. Copilot Studio, Claude Cowork, Dust는 공급사의 외부 클라우드에서 쓰고, watsonx Orchestrate와 FabriX, Alli는 조직 안에 설치할 수 있습니다. 반면 구분 ⑤의 Hermes Agent 콘솔 넷과 구분 ⑥의 Paperclip은 실행 엔진을 갖지 않고 이미 있는 에이전트 플랫폼 위에 얹는다는 점에서 AAS와 같은 방식을 쓰며, 차이는 사용자와 지켜보기 화면의 깊이에서 납니다.

2.2 만드는 쪽 세 구분의 완성도와 자사 실행 엔진이라는 전제

만드는 쪽의 세 구분인 업무 담당자용 에이전트 빌더, 에이전트·워크플로 빌더, 채팅 UI·워크스페이스는 제품 완성도가 가장 높지만 조직이 쓰던 에이전트 플랫폼을 그대로 두는 방식은 지원하지 않습니다. 에이전트 탑재가 빠르게 늘어나는 흐름에 맞춰 Microsoft, Google, Salesforce 같은 대형 벤더가 모두 이 시장에 들어왔으므로, 여섯 구분 가운데 기능 폭과 사용 편의는 만드는 쪽이 가장 앞서 있습니다. 다만 두 빌더 구분은 자기 실행 엔진을 함께 제공하고 채팅 UI는 에이전트 플랫폼의 구성과 운영을 다루지 않으므로, 기존 플랫폼 위에서 업무 담당자가 에이전트를 만들고 운영하는 방식은 세 구분 어디에도 들어 있지 않습니다.

2.2.1 실행 엔진까지 공급사 것으로 묶인 Copilot Studio·FabriX 등 업무 담당자용 빌더의 높은 완성도

Copilot Studio·Claude Cowork가 앞서는 사내 마켓과 관리자 통제

구분 ①의 업무 담당자용 에이전트 빌더 가운데 Copilot Studio와 Claude Cowork 같은 글로벌 클라우드 제품은 이 시장에서 완성도가 가장 높은 선택지입니다. 사내 에이전트 스토어나 사설 플러그인 마켓, 역할 기반 접근, 지출 한도 설정을 한 공급사가 함께 제공합니다[S9][S11]. 부서가 만든 에이전트를 다른 부서에 배포하고 관리자가 비용과 권한을 한곳에서 통제하는 흐름이 한 제품 안에서 끝납니다. 외부 클라우드를 쓸 수 있는 조직이 마켓 운영과 관리자 통제의 완성도만 비교한다면 이 두 제품을 앞서는 선택지는 찾기 어렵습니다.

글로벌 클라우드 빌더의 장점이 자사 클라우드와 자사 런타임 위에서만 성립하는 구조

Copilot Studio와 Claude Cowork의 장점은 모두 자사 클라우드와 자사 에이전트 런타임 위에서 성립합니다. Copilot Studio는 실행 엔진을 공급사가 정한 몇 가지 가운데서 고르게 하고, Claude Cowork는 온프레미스 설치형을 제공하지 않습니다[S9][S11]. 이 구조에서는 공급사의 클라우드가 에이전트 정의, 실행 기록, 자격증명을 모두 보관합니다. 모델을 골라 쓸 수 있는 모델 중립을 내세우는 상용 제품은 많지만, 런타임까지 중립인 상용 제품은 공식 자료에서 확인되지 않습니다. 조직이 이미 쓰고 있는 오픈소스 에이전트 플랫폼을 그대로 두고 화면만 연결하는 방식은 이 제품들에서 지원되지 않습니다.

watsonx Orchestrate·FabriX·Alli 온프레미스 일체형 플랫폼의 장점과 전환 부담

온프레미스(on-premises, 조직이 직접 관리하는 서버에 설치하는 방식)를 공식 지원하는 글로벌 플랫폼인 IBM watsonx Orchestrate[S13]와 국내 상용 플랫폼인 삼성SDS FabriX[S14], 올거나이즈 Alli[S15]는 조직 안 설치와 폐쇄망 구성을 제공합니다. FabriX는 비개발자용 빌더와 에이전트 스토어, 부서·사용자별 할당량을, Alli는 노코드 빌더와 앱 마켓을 갖춰 국내 조직이 가장 직접적으로 비교하게 되는 제품입니다. 반면 빌더, 런타임, 스토어를 한 공급사가 묶어 제공하는 일체형이므로, 도입하면 에이전트 플랫폼 자체를 그 공급사의 것으로 바꾸게 됩니다. 이미 운영 중인 에이전트와 스킬이 있는 조직이라면 플랫폼 전환 비용과 기존 에이전트를 다시 만드는 부담을 도입 의사결정에 함께 넣어야 합니다.

2.2.2 오픈소스 워크플로 빌더와 채팅 UI가 맡는 사용자와 운영 범위

구분 ② 에이전트·워크플로 빌더의 개발자 중심 화면과 자체 엔진

구분 ②의 Dify, Flowise, Langflow, n8n 같은 오픈소스 에이전트·워크플로 빌더는 캔버스에서 노드를 이어 에이전트 앱을 조립하고 자체 호스팅이 가능하므로 조직 안 설치 조건은 충족합니다. 다만 노드, 변수, 분기를 직접 다루는 화면이어서 개발자에게 맞춰져 있고, 실행도 그 빌더의 자체 엔진이 맡습니다. 업무 담당자가 직접 에이전트를 고쳐 쓰려면 개발자의 도움이 계속 필요하고, 다른 에이전트 플랫폼을 이미 쓰는 조직은 실행 엔진을 하나 더 운영하게 됩니다.

구분 ③ 채팅 UI·워크스페이스가 다루지 않는 에이전트 플랫폼 운영

구분 ③의 채팅 UI·워크스페이스 가운데 Open WebUI는 여러 AI 모델과 대화하는 화면에 LDAP(Lightweight Directory Access Protocol, 사내 계정 디렉터리 연동 규약) 기반 그룹 권한, 채널, 예약 질의를 제공해 업무 담당자의 일상 사용에 가깝습니다[S21]. 하지만 에이전트 플랫폼의 프로파일, 스킬, 정기 업무를 구성하고 운영하는 기능은 다루지 않습니다. 채팅 UI는 일을 시키는 창구로는 쓸 수 있어도, 그 창구 뒤에서 도는 에이전트를 만들고 지켜보는 화면을 대신하지 못합니다.

2.3 지켜보는 쪽 세 구분과 운영자 화면에 머무는 플랫폼 전용 콘솔

지켜보는 쪽의 세 구분인 관제·거버넌스 도구, 에이전트 플랫폼 전용 콘솔, 에이전트 조직 운영 콘솔은 감독 수요가 커지는 흐름 속에 있지만, 대부분 운영자나 IT·보안팀 한쪽을 위해 설계되어 있습니다. Gartner는 다른 에이전트의 행동을 감시하고 통제하는 감독용 에이전트(guardian agent)가 2030년까지 에이전트형 AI 시장의 10~15%를 차지한다고 전망했습니다[S3]. 감독 기능이 별도 시장으로 자랄 만큼 수요가 크다는 뜻이므로, 「쓰던 플랫폼의 대시보드면 충분하지 않은가」라는 질문에는 그 화면을 누가 보는지를 기준으로 답해야 합니다.

2.3.1 감독용 에이전트 10~15% 전망과 만드는 화면이 없는 관제·거버넌스 도구

감독용 에이전트 전망과 내부 정책 위반 비중

Gartner는 2025년 6월 11일 보도자료에서 감독용 에이전트가 2030년까지 에이전트형 AI 시장의 10~15%를 차지한다고 전망했습니다. 감독용 에이전트는 다른 AI 에이전트의 결과와 행동을 검토하고, 필요하면 실행을 막는 기술을 말합니다. 같은 보도자료는 2028년까지 허가되지 않은 AI 에이전트 행위의 80% 이상이 외부 공격보다 정보 과다 공유나 부적절한 사용 같은 내부 정책 위반에서 나온다고 내다봤습니다[S3]. 에이전트 감독의 주된 대상은 조직 밖의 공격자보다 조직 안에서 에이전트를 만들고 쓰는 방식 자체입니다.

에이전트를 만든 부서 쪽에서 커지는 관측 수요

내부 정책 위반이 주된 위험이라면 감독은 IT·보안팀의 중앙 화면만으로 끝나지 않습니다. 에이전트를 만든 부서가 그 에이전트가 무엇을 읽고, 어떤 외부 시스템을 부르고, 언제 실패했는지를 스스로 확인할 수 있어야 정책 위반을 이른 시점에 찾아낼 수 있습니다. 예약 실행이 기본 기능이 되면서 사람이 화면을 보지 않는 시간에 실행되는 작업이 늘어났고, 이런 작업의 실패는 대화창에 나타나지 않습니다. 관측 수요는 감독 전용 제품과 함께 에이전트를 만드는 사람 쪽 화면에서도 커지고 있습니다.

에이전트 수가 늘어날 때 개별 에이전트 바깥에 필요한 재사용·관측·통제

에이전트는 흔히 목표, 도구, 기억, 결과 점검의 네 요소를 갖춘 실행 단위로 설명되며, 이 네 요소는 에이전트 하나의 범위 안에서 완결됩니다. 그러나 여러 부서와 여러 시스템에 걸친 업무가 에이전트에게 넘어가기 시작하면 사정이 달라집니다. 예를 들어 한 부서가 만든 스킬을 다른 부서가 다시 쓰는 일, 여러 에이전트의 실패와 사용량

을 한 화면에서 보는 일, 누가 어떤 에이전트를 바꿀 수 있는지 정하는 일은 어느 에이전트 하나도 맡지 않습니다. 재사용, 관측, 통제를 개별 에이전트 바깥에서 따로 마련해야 하고, 이것이 지켜보는 쪽 구분이 별도 시장으로 자라는 배경입니다.

구분 ④ 관제·거버넌스 도구에서 갈라지는 발견자와 수정자

구분 ④의 관제·거버넌스 도구는 조직의 에이전트를 등록하고 감시하고 통제하며, 실패 감시, 호출 추적, 감사 기능을 제공합니다. Microsoft Agent 365는 IT·보안팀을 위한 관제 평면으로 에이전트 레지스트리와 접근 통제, 에이전트 사이의 연결을 보여 주는 에이전트 맵을 제공하고[S10], Datadog AI Agents Console은 엔지니어링·플랫폼팀이 에이전트의 성능, 오류, 비용을 감시하는 관측 화면입니다[S22]. 오픈소스인 Langfuse는 개발자가 코드에 계측을 심어 호출을 추적하는 도구입니다[S23]. 세 제품 모두 에이전트를 만드는 화면은 제공하지 않습니다. 이 구조에서는 에이전트를 만든 부서 담당자와 그 에이전트를 감시하는 담당자가 서로 다른 도구를 쓰고, 그 결과 실패를 처음 발견한 사람과 원인을 고칠 수 있는 사람이 달라져 문제를 넘겨주는 단계가 하나 더 생깁니다.

2.3.2 플랫폼 전용 콘솔과 조직 운영 콘솔에 없는 역할별 화면

구분 ⑤ hermes-webui 등 플랫폼 전용 콘솔의 기능 범위와 한 사람 사용 전제

구분 ⑤의 에이전트 플랫폼 전용 콘솔은 특정 에이전트 런타임의 프로파일, 정기 업무, 스킬, 키, 로그, 사용량을 다루는 화면입니다. 오픈소스 에이전트 플랫폼인 Hermes Agent는 본체에 대시보드를 기본으로 제공하고[S16], 같은 플랫폼 위에 얹히는 오픈소스 콘솔로 hermes-webui, Ekko Studio, hermes-control-interface가 있습니다[S17][S18][S19]. 이 콘솔들은 기능 폭이 넓고 개발 속도가 빠르며 기능 목록이 AAS와 절반 이상 겹치므로, 한 사람이 플랫폼을 설치하고 직접 쓰는 환경이라면 내장 대시보드나 hermes-webui로 충분할 수 있습니다. 하지만 운영자 한 명을 전제로 설계했기 때문에 사용자별 권한 분리, 사용자마다 에이전트를 나눠 주는 기능, 사내 스킬 마켓이 없거나 제한적입니다. 공식 자료 기준으로 역할 구분과 사용자별 프로파일 제한을 밝힌 콘솔은 hermes-control-interface 하나이고, 이 프로젝트는 2026년 6월 이후 새 커밋이 없습니다[S19].

부서 담당자·부서장·IT 관리자·보안 담당이 각각 확인해야 하는 화면

같은 에이전트를 놓고도 부서 담당자, 부서장, IT·플랫폼 관리자, 보안·감사 담당이 확인해야 하는 내용은 서로 다른데, 운영자 화면은 그 차이를 나누지 않습니다. 역할별로 필요한 화면과 운영자용 플랫폼 대시보드가 제공하는 범위를 비교하면 다음과 같습니다.

역할	확인해야 하는 내용	운영자용 플랫폼 대시보드	업무 담당자용 콘솔에 필요한 화면
부서 담당자	내가 만든 에이전트와 정기 업무의 실패 여부	전체 로그에 섞여 있음	사람마다 배정되는 에이전트와 한도, 그 안의 업무별 프로파일
부서장·팀 리더	팀 에이전트가 맡은 업무와 결과	해당 화면 없음	팀 단위 활동과 실패 요약
IT·플랫폼 관리자	플랫폼, 모델, 자격증명, 권한	키 화면과 설정 화면	값을 보이지 않는 자격증명 만료·중복 점검

역할	확인해야 하는 내용	운영자용 플랫폼 대시보드	업무 담당자용 콘솔에 필요한 화면
보안·감사 담당	에이전트가 부르는 외부 시스템, 변경 이력	실행 로그 수준	스킬에서 외부 호스트까지의 호출 관계, 감사 추적

구분 ⑥ Paperclip 등 조직 운영 콘솔의 접근 방식과 지켜보기 화면의 깊이

구분 ⑥의 에이전트 조직 운영 콘솔은 에이전트를 직원처럼 두고 과업과 예산을 관리하는 오픈소스 제품군이며, Paperclip이 대표적입니다. Paperclip은 Hermes Agent를 포함한 여러 에이전트 런타임을 어댑터로 붙이는 플랫폼 중립 구조이고, 비개발자를 대상으로 Skill Studio와 조직 공유 스킬, 예산 자동 정지까지 제공해 제품 정의가 AAS와 가장 가깝습니다[S20]. 다만 Paperclip은 목표·조직도·예산 같은 회사 경영을 화면의 바탕 은유로 쓰고, 같은 구분의 Multica는 개발팀의 이슈 관리를 중심에 두어, 부서 담당자가 자기 업무 화면으로 받아들이기까지 거리가 있습니다. 정기 업무의 건강 상태나 실제 호출 관계처럼 지켜보는 화면의 깊이도 제품마다 차이가 큽니다.

2.4 예약 실행·사내 공유·다중 에이전트 협업의 보급으로 운영의 질로 옮겨 간 AI Agent 도구 경쟁

여섯 구분 전반에서 예약 실행, 사내 공유, 다중 에이전트 협업은 2026년 기준 기본 기능이 됐고, 그 결과 도구를 고르는 기준이 기능의 유무에서 운영의 질로 옮겨 가고 있습니다. 이 절은 기본 기능이 된 세 기능의 보급 현황과 AAS가 에이전트를 만드는 방식을 먼저 밝히고, 기능이 보급된 뒤 도입 평가에서 남는 질문을 정리합니다.

2.4.1 차별 요소에서 기본 기능으로 바뀐 세 가지 기능과 AAS의 에이전트·프로파일 만들기

예약 실행·사내 공유·다중 에이전트 협업의 보급 현황

예약 실행, 사내 공유, 다중 에이전트 협업은 더 이상 제품을 가르는 차별 요소가 되지 못합니다. 상용 빌더 대부분과 다수의 오픈소스 프로젝트가 일정 기반 실행을 기본 메뉴로 제공하고, 사내 스토어나 팀 템플릿으로 에이전트를 나누는 기능도 대부분의 제품이 갖췄습니다. 여러 에이전트가 한 과업을 나눠 맡는 구성 역시 빌더와 조직 운영 콘솔 양쪽에 기본 기능으로 들어왔습니다. 도입 평가표에 이 세 항목을 넣어도 후보 사이의 차이는 거의 드러나지 않습니다.

에이전트를 받고 그 안에 업무별 프로파일을 두는 AAS의 만들기 방식

AAS에서는 사람마다 에이전트를 받고, 그 안에 업무별 프로파일을 둡니다. 에이전트는 사용자 한 사람에게 배정되는 실행 단위로, 「에이전트 추가」에서 이름을 주면 저장 공간을 붙여 준비를 마치며 사용자당 개수 한도(기본 3개) 안에서 늘리고 지울 수 있습니다. 프로파일은 그 에이전트 안의 업무 묶음이며 성격, 설정, 비밀값, 스킬, 도구 묶음·MCP, 정기 업무, 메신저 연결, 모델을 프로파일마다 따로 가집니다. 새 프로파일은 기존 프로파일을 복제하거나 다른 에이전트의 프로파일을 가져와 출발점으로 삼고, 성격·스킬·정기 업무를 편집기와 대화로 다듬어 완성합니다. 복제할 때 비밀값은 따라오지 않아 자격증명은 새 프로파일에 새로 넣으므로, 잘 만든 업무 구성을 나눠 쓰면서도 자격증명이 사람 사이로 옮겨 가지 않습니다.

2.4.2 기능 보급 뒤 운영의 질로 옮겨 간 도입 평가 기준

사람이 보지 않는 동안 실행되는 작업이 늘어날 때 남는 질문

기본 기능이 넓게 보급되면 경쟁 기준은 기능의 유무에서 운영의 질로 옮겨 갑니다. 예약 실행이 늘어날수록 사람이 보지 않는 동안 실행되는 작업이 늘어나고, 그만큼 실패나 멈춤을 누가 언제 알게 되는지가 중요해집니다. 사내 공유가 쉬워질수록 공유된 스킬이 어떤 외부 시스템과 자격증명을 쓰는지 확인할 필요도 커집니다. 기능별로 지금 제공하는 구분과 보급된 뒤에도 도입 평가에서 확인해야 할 질문을 정리하면 다음과 같습니다.

기능	지금 제공하는 구분	보급된 뒤 남는 질문
예약 실행	① 빌더, ② 워크플로 빌더, ③ 채팅 UI, ⑤ 플랫폼 전용 콘솔	정기 업무가 실패하거나 멈췄을 때 누가 아는가
사내 공유	① 빌더의 스토어, ⑥ 조직 운영 콘솔의 템플릿	공유한 스킬이 어떤 외부 시스템과 자격증명을 쓰는가
다중 에이전트	① 빌더, ⑥ 조직 운영 콘솔	여러 에이전트의 실행 결과를 한 화면에서 볼 수 있는가

2.5 국가 망 보안체계(N²SF)의 기밀 등급 아래에서 남는 온프레미스 설치 수요

국내 공공기관이 AI Agent 도구를 고를 때는 표 2-1의 네 번째 기준인 설치 위치가 기능보다 먼저 검토 대상이 됩니다. 정부는 2024년 9월 11일 일률적인 망 분리를 데이터 중요도에 따라 보안을 차등 적용하는 다층보안체계(MLS, Multi-Level Security)로 바꾸겠다고 발표했습니다[S6]. 이어 국가정보원은 2025년 1월 국가 망 보안체계(N²SF, National Network Security Framework) 가이드라인 초안을 배포해 생성형 AI와 외부 클라우드를 업무에 쓸 길을 열었습니다[S5]. 다만 이 체계는 업무 정보를 등급으로 나눠 통제를 달리하는 구조이므로, 가장 높은 등급의 업무에는 외부 서비스가 쉽게 들어가지 못합니다.

2.5.1 공개 등급부터 넓어지는 N²SF 3등급 분류와 생성형 AI 활용 범위

N²SF 가이드라인의 세 등급 분류와 6개 통제 영역

N²SF 가이드라인은 기관이 다루는 정보를 기밀(Classified, C), 민감(Sensitive, S), 공개(Open, O)의 세 등급으로 나누며, 기관은 정보공개법에 따른 비공개 정보를 기밀과 민감 등급으로, 나머지 정보를 공개 등급으로 분류해야 합니다[S5]. 기관은 권한, 인증, 분리 및 격리, 통제, 데이터, 정보자산의 6개 영역에서 등급별로 필요한 보안 항목을 골라 적용하고, 위협을 먼저 식별해 보안 대책을 세운 뒤 국가정보원의 검토를 받습니다[S5]. 같은 기관 안에서도 업무마다 적용되는 보안 통제가 달라지며, 에이전트가 다루는 문서의 등급이 그 에이전트를 어디에 설치할 수 있는지를 정합니다. 등급별 분류 대상, 보안 통제 적용 방식, 생성형 AI·외부 클라우드 활용 범위를 정리하면 다음과 같습니다.

등급	분류 대상	보안 통제 적용	생성형 AI·외부 클라우드 활용
기밀(C)	정보공개법상 비공개 정보 가운데 기밀로 분류한 정보	6개 영역 보안 항목을 등급에 맞춰 적용, 분리 유지	외부 서비스 활용이 가장 제한됨
민감(S)	정보공개법상 비공개 정보 가운데 민감으로 분류한 정보	6개 영역 보안 항목을 등급에 맞춰 적용	보안 대책을 갖춘 범위에서 검토

등급	분류 대상	보안 통제 적용	생성형 AI·외부 클라우드 활용
공개(O)	그 밖의 정보	망 분리 규제 완화를 먼저 적용	활용 범위가 가장 넓음

공개 등급부터 넓어지는 생성형 AI 활용 범위

N²SF는 업무 환경에서 생성형 AI와 외부 클라우드 서비스(SaaS)를 쓸 수 있게 하는 것을 목표로 둡니다[S5]. 2026년 3월에는 공공기관 업무 PC에서 생성형 AI 서비스를 쓰는 N²SF 실증 공모가 시작되어, 제도가 실제 업무 환경으로 옮겨 가고 있습니다[S7]. 하지만 활용 범위가 넓어지는 순서는 공개 등급부터이며, 기밀 등급 업무까지 같은 속도로 열리지는 않습니다. 한 기관 안에서 외부 클라우드를 쓰는 업무와 조직 안에서만 처리하는 업무가 함께 존재하게 됩니다.

2.5.2 기밀 등급 업무에서 남는 두 가지 설치 형태와 도입 심사 검토 항목

기밀 등급 업무에서 Copilot Studio·Claude Cowork 같은 외부 클라우드 빌더가 빠지는 조건

망 분리 규제 완화는 데이터 중요도에 따라 차등 적용되고, 가장 낮은 등급의 데이터부터 공유와 활용이 넓어집니다[S6]. 따라서 기밀 등급 업무는 기존처럼 분리된 망 안에서 처리된다는 전제가 유지됩니다. 에이전트는 문서, 회의 녹음, 고객 정보를 직접 읽고 쓰기 때문에, 에이전트 정의와 실행 기록, 처리 데이터가 공급사의 클라우드로 나가는 구조라면 기밀 등급 업무에는 적용할 수 없습니다. 이 조건에서 Copilot Studio, Claude Cowork, Dust 같은 외부 클라우드 빌더는 기능 완성도와 관계없이 검토 대상에서 빠집니다.

국내 경쟁에서 기본 조건이 된 온프레미스와 남는 두 가지 도입 방식

글로벌 상용 제품 가운데 온프레미스 설치를 공식적으로 밝힌 제품은 IBM watsonx Orchestrate 등 일부에 그치는 반면[S13], 국내 상용 플랫폼인 FabriX와 Alli는 온프레미스와 폐쇄망 구성을 기본 선택지로 둡니다[S14][S15]. 온프레미스는 글로벌 제품과 비교할 때는 차별점이지만, 국내 시장에서는 공급사가 갖춰야 할 기본 조건입니다. 그래서 조직 안에 설치해야 하는 기관이 고를 수 있는 도입 방식은 크게 두 가지입니다. 하나는 watsonx Orchestrate, FabriX, Alli처럼 빌더, 런타임, 스토어를 한 공급사가 함께 제공하는 온프레미스 일체형 플랫폼을 새로 도입하는 방식이고, 다른 하나는 이미 쓰고 있거나 조직 안에 설치할 오픈소스 에이전트 플랫폼을 그대로 두고 그 위에 콘솔만 추가로 설치하는 방식입니다. AAS는 두 번째 방식을 따르며, 에이전트 플랫폼을 고치지 않고 그 위에 연결하는 것을 설계 원칙으로 둡니다. 현재 AAS가 연결되는 에이전트 플랫폼은 오픈소스 Hermes Agent 1종입니다.

보안성 검토·개인정보 검토·정보화 감사가 공통으로 묻는 데이터 위치

설치 형태는 기술 부서 한 곳보다 여러 검토 라인이 동시에 확인합니다. 공공기관이라면 보안성 검토, 개인정보 보호 책임자의 검토, 정보화 감사가 같은 질문을 서로 다른 각도에서 던지고, 민간 기업도 정보보호 조직과 법무, 내부 감사가 비슷한 역할을 나눠 맡습니다. 세 라인이 공통으로 묻는 것은 에이전트가 읽은 데이터와 그 실행 기록이 지금 어디에 있느냐이며, 한 곳에서라도 그 위치를 설명하지 못하면 사업은 다음 단계로 넘어가기 어렵습니다. 조직 안 콘솔을 검토할 때는 기능 시연과 함께 에이전트 정의, 실행 기록, 처리 데이터가 저장되는 위치를 구성도 한 장으로 설명할 수 있는지를 먼저 확인하는 편이 좋습니다. 그 구성도에 조직 밖으로 나가는 연결이 어떤 등급의 업무에서 무슨 목적으로 쓰이는지도 함께 적어 두어야, 세 라인이 같은 그림을 놓고 각자의 기준으로 판단할 수 있습니다.

2.6 조직 안 설치·업무 담당자 사용·만들기와 지켜보기를 함께 갖춘 조합의 공백과 AAS의 위치

표 2-1의 여섯 구분에 국내 설치 조건을 겹치면, 조직 안에 설치되면서 업무 담당자가 만들고 지켜보는 화면을 함께 쓰는 조합이 비어 있다는 점이 드러납니다. 업무 담당자를 위한 완성도는 외부 클라우드 빌더가, 조직 안 설치는 온프레미스 일체형과 오픈소스 콘솔이, 감독 기능은 관제·거버넌스 도구가 각각 앞서 있습니다. 감독용 에이전트가 별도 시장이 될 만큼 관측 수요가 크다는 전망[S3]과 기밀 등급 업무의 분리 유지[S5][S6]를 함께 놓으면, 세 조건을 한 제품에서 함께 갖춘 조합이 검토 대상으로 남습니다.

2.6.1 세 조건과 기존 플랫폼 연결을 교차한 구분별 충족 현황

구분별 세 조건 교차표

조직 안 설치, 업무 담당자 사용, 만들기와 지켜보기의 한 화면 제공이라는 세 조건을 표 2-1의 구분과 대표 제품별로 교차하면 다음과 같습니다. 표의 기호는 공개된 제품 자료의 기재를 기준으로 하며, ○는 제공, △는 일부 또는 제약이 있는 제공, ×는 공식 자료에서 확인되지 않는 경우를 뜻합니다. 마지막 열은 쓰던 에이전트 플랫폼을 고치지 않고 그 위에 연결할 수 있는지를 나타냅니다.

구분 (대표 제품)	조직 안 설치	업무 담당자 사용	만들기	지켜보기	쓰던 플랫폼에 연결
① 외부 클라우드 빌더 (Copilot Studio·Claude Cowork·Dust)	×	○	○	△ 분석 화면	×
① 온프레미스 일체형 (watsonx Orchestrate·FabriX·Alli)	○	○	○	△ 활동 기록	×
② 에이전트·워크플로 빌더 (Dify·Flowise·Langflow·n8n)	○	△ 개발자 지향	○	△ 실행 기록	×
③ 채팅 UI·워크스페이스 (Open WebUI)	○	○	△	×	해당 없음
④ 관제·거버넌스 도구 (Agent 365·Langfuse 등)	△ 제품별 상이	× IT·보안팀	×	○	△

구분 (대표 제품)	조직 안 설치	업무 담당자 사용	만들기	지켜보기	쓰던 플랫폼에 연결
⑤ 플랫폼 전용 콘솔 (Hermes Agent 내장 대시보드 ·hermes-webui 등)	○	△ 운영자 1인	○	△ 로그 수준	○
⑥ 조직 운영 콘솔 (Paperclip)	○	○	○	△	○
AAS	○	○	△ 스크립트 스킬은 콘솔 밖에서 편집	○	○ Hermes Agent 1종

교차표에서 드러나는 세 조건 조합의 공백

교차표에서 조직 안 설치와 업무 담당자 사용을 함께 충족하는 구분은 온프레미스 일체형, 채팅 UI, 조직 운영 콘솔입니다. 그러나 watsonx Orchestrate, FabriX, Alli 같은 온프레미스 일체형은 쓰던 에이전트 플랫폼 위에 연결할 수 없고, Open WebUI 같은 채팅 UI는 에이전트 플랫폼의 운영을 다루지 않습니다. Paperclip은 세 조건에 가장 가깝지만, 정기 업무의 실패·멈춤·알림 누락이나 실제 호출 관계를 먼저 보여 주는 지켜보기 화면의 깊이에서 차이가 있습니다. 비어 있는 것은 특정 기능 하나보다, 세 조건과 기존 플랫폼 연결 방식을 한 제품에서 함께 갖춘 조합입니다.

AAS의 위치와 아직 부족한 두 가지 항목

AAS는 구분 ⑤의 플랫폼 전용 콘솔에서 출발해 구분 ①의 업무 담당자를 겨냥하는 제품입니다. 플랫폼 전용 콘솔처럼 에이전트 플랫폼 위에 얹히지만, 대상은 플랫폼을 운영하는 한 사람보다 부서의 업무 담당자입니다. 다만 교차표에서 보듯 스크립트가 필요한 스킬은 콘솔에서 고치지 못하고, 연결되는 에이전트 플랫폼도 Hermes Agent 1종입니다. Microsoft 365나 외부 클라우드를 쓸 수 있는 조직이라면 마켓과 관리자 통제의 완성도까지 더해 Copilot Studio 같은 글로벌 클라우드 빌더를 고를 충분한 이유가 되므로, 도입 평가표에는 이 두 항목을 강점과 같은 무게로 올려야 합니다(9장 비교표).

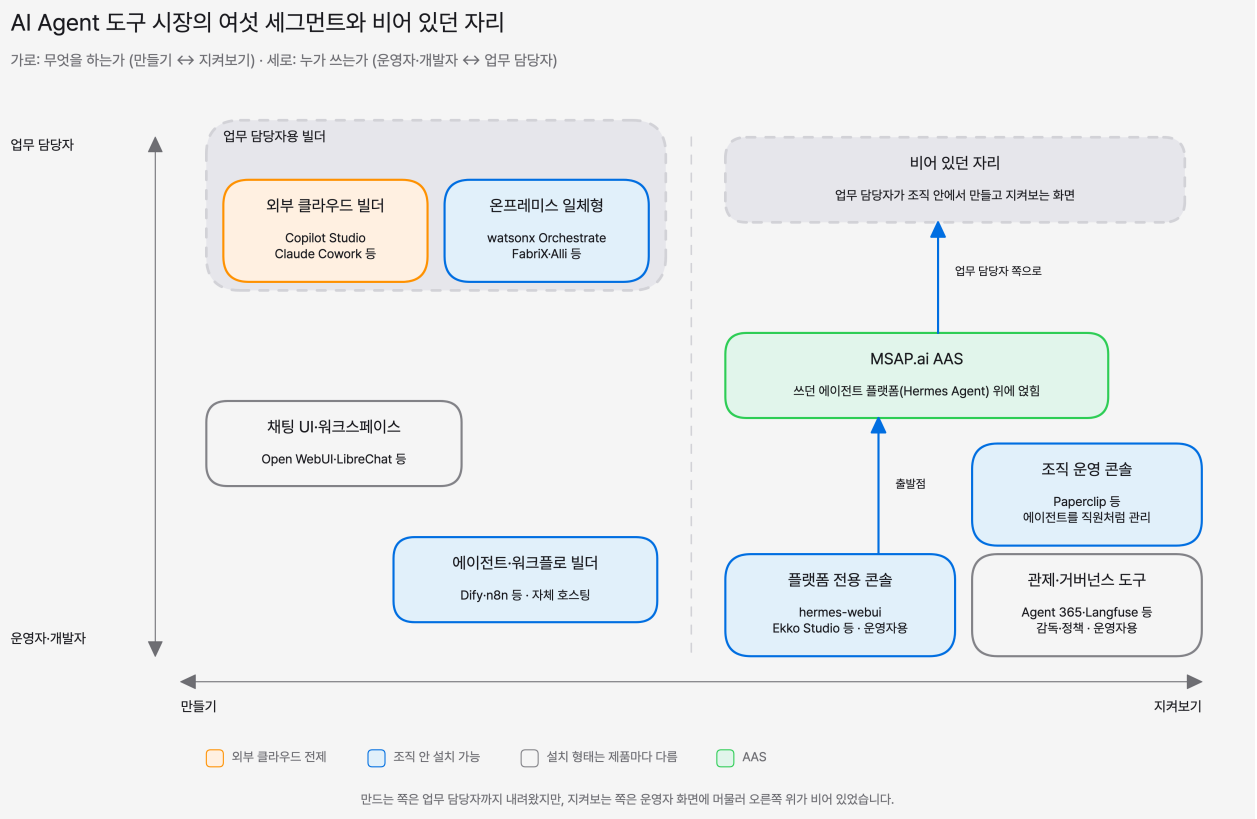


그림 2-1. 만드는 쪽과 지켜보는 쪽으로 나눈 여섯 구분과 AAS의 위치 — 오른쪽 위(업무 담당자 × 만들기와 지켜보기)가 비어 있는 조합입니다

2.6.2 만들기와 지켜보기가 다른 제품으로 나뉜 시장 구조와 한 화면 콘솔의 역할

제품 이름에 드러난 만들기 도구와 관제 도구의 분리

시장에서는 에이전트를 만드는 도구와 관리하는 도구가 이름부터 나뉘어 있습니다. 만드는 도구의 이름은 Copilot Studio처럼 Studio와 Builder로 모이고, 운영·관제 화면의 이름은 Datadog AI Agents Console이나 ServiceNow AI Control Tower처럼 Console과 Control로 모여 있습니다. 같은 공급사 안에서도 빌더 제품과 관제 제품을 따로 내놓는 경우가 많아, Microsoft는 만드는 쪽에 Copilot Studio를, 관제하는 쪽에 Agent 365를 둡니다[S9][S10]. 시장의 기본 구조는 만들기와 지켜보기를 서로 다른 제품, 서로 다른 사용자에게 맡기는 형태입니다.

만들기와 지켜보기가 두 제품으로 나뉠 때 생기는 운영 부담

만들기와 지켜보기가 다른 제품으로 나뉘면 운영 부담이 조직 안의 여러 부서로 흩어집니다. 예를 들어 부서 담당자는 빌더에서 정기 업무를 만들지만, 그 작업의 실패 기록은 IT·보안팀이 보는 관제 도구에 남습니다. 이때 실패 알림의 전달 대상이 정해지지 않은 작업은 어느 화면에서도 눈에 띄지 않고, 1장에서 다룬 알림이 안 가는 실패가 그대로 남습니다. 자격증명은 빌더와 관제 도구가 양쪽에서 따로 관리하고, 변경 이력은 두 제품의 기록을 맞춰 봐야 확인할 수 있습니다. 2.3.1에서 본 내부 정책 위반 전망[S3]을 고려하면, 만든 사람이 자기 에이전트의 실행 상태를 직접 보는 구조가 감사 추적의 출발점이 됩니다.

만들기와 지켜보기를 한 화면에 둔 AAS 콘솔의 판단 기준

AAS는 업무 담당자가 자기 에이전트 안에 업무별 프로파일을 두고 그 프로파일의 스킬과 정기 업무를 만드는 화면과, 그 에이전트가 무엇을 하다 실패했는지 지켜보는 화면을 한 콘솔에 둡니다. 이 구조에서는 정기 업무를 등록한 사람이 같은 콘솔에서 실패와 멈춤, 만료가 임박한 자격증명을 확인하고, IT·보안 담당은 같은 기록을 역할에 맞는 화면으로 봅니다. 반면 기능 폭과 완성도는 Copilot Studio 같은 외부 클라우드 빌더나 FabriX 같은 온프레미스 일체형 플랫폼이 앞서므로, 이 조합의 가치는 조직의 조건에 따라 달라집니다. 판단 기준은 외부 클라우드를 쓸 수 없거나 이미 오픈소스 에이전트 플랫폼을 쓰는 조직인지, 그리고 개발자가 아닌 부서 담당자가 직접 스킬을 만들어 업무에 쓰게 할 것인지의 두 가지입니다. 3장은 이 비어 있는 조합을 겨냥한 AAS가 어떤 제품이고 누구를 위한 것인지를 정의합니다.

3장: 업무를 아는 담당자가 에이전트를 직접 만드는 콘솔 MSAP.ai AAS와 폭스프로·디베이스 선례

2장에서 본 빈자리, 즉 조직 안에 설치되면서 업무 담당자가 만들고 지켜보는 화면을 함께 쓰는 조합이 AAS가 겨냥하는 자리입니다. AAS는 AI Agent 플랫폼에 연결되는 일반 사용자용 콘솔로, 기업 각 부서의 담당자가 에이전트의 성격과 모델, 일하는 방법, 실행 일정을 직접 정의해 자기 업무에 쓰도록 만든 제품입니다. 1장에서 본 것처럼 에이전트를 시험하는 조직은 많지만 부서 업무에 정착하는 비율은 아직 낮고[S4], 그 차이는 업무를 아는 사람이 에이전트를 직접 다룰 수 있느냐에서 벌어집니다. 3장은 AAS가 어떤 제품이고 지금 무엇에 연결되는지, 1980~90년대 현업이 업무 프로그램을 직접 만들던 폭스프로·디베이스 선례가 왜 이 제품의 설계 방향과 맞닿는지, 그리고 구매 결정에 참여하는 사용자 네 부류가 각각 무엇을 얻는지를 정리합니다. 이 장을 읽고 나면 AAS를 지금 우리 조직의 에이전트 플랫폼에 붙일 수 있는지, 부서별로 누가 무엇을 확인해야 하는지를 판단할 수 있습니다.

3.1 AI Agent 플랫폼에 연결되는 일반 사용자용 콘솔이라는 MSAP.ai AAS의 정의

AAS는 에이전트 플랫폼 위에서 부서 담당자가 에이전트를 정의하고 관찰하는 콘솔이며, 에이전트를 직접 실행하는 일은 플랫폼이 맡습니다. 에이전트 도입이 시험 단계에서 멈추는 원인은 대개 업무를 아는 사람과 에이전트를 설정할 수 있는 사람이 서로 다르다는 데 있습니다. 예를 들어 영업 담당자는 명함을 어디에 등록하고 중복을 어떻게 걸러야 하는지 알지만, 설정 파일과 명령줄을 다루는 일은 IT 부서에 맡겨야 합니다. AAS는 정의 대상을 담당자가 이해하는 말로 세 가지에 한정하고, 그 정의를 한 화면에서 끝내도록 설계했습니다. 이 절의 두 항은 정의 대상의 범위와 콘솔이 한 화면에 모으는 기능 묶음을 각각 설명합니다.

3.1.1 에이전트·스킬·정기 업무를 부서 담당자가 정의하는 콘솔의 범위

AAS가 정의하는 대상 세 가지

AAS에서 부서 담당자가 정의하는 대상은 에이전트, 스킬, 정기 업무의 세 가지입니다. 에이전트는 사람마다 받는 실행 단위이고 그 안에 업무별 프로파일을 두어 성격과 모델을 정하며, 스킬은 그 에이전트가 특정 업무를 처리하는 방법을 적은 문서이며, 정기 업무는 정해진 시각에 스킬을 실행하도록 걸어 두는 일정입니다. 「누가」, 「어떻게」, 「언제」를 각각 하나의 화면 객체로 나눈 구조입니다. 세 대상을 나눠 두면 영업 에이전트의 성격은 그대로 두고 명함 등록 스킬만 고치거나, 같은 스킬을 매일 아침과 매주 월요일 두 번 실행하도록 일정만 추가할 수 있습니다. 담당자는 프로그램 전체를 다시 만들지 않고 업무 규칙이 바뀐 부분만 손볼 수 있습니다.

정의 대상	영문 표기	담는 내용	담당자가 바꾸는 예
에이전트·프로파일	Agent·Profile	에이전트: 사람마다 받는 실행 단위, 프로파일: 그 안의 업무 묶음(성격(SOUL), 사용할 모델, 연결된 메신저)	에이전트를 추가하고, 업무별 프로파일을 만들어 응답 말투와 모델을 정한다
스킬	Skill	업무를 처리하는 방법과 순서, 사람 확인 조건	「중복이면 멈춘다」 같은 업무 규칙을 문서에 적는다

정의 대상	영문 표기	담는 내용	담당자가 바꾸는 예
정기 업무	Cron	실행 시각과 주기, 결과를 보낼 곳	매일 06시 50분 보고를 주 1회로 바꾼다

에이전트 관리 화면과 다른 콘솔의 범위

AAS의 범위는 특정 에이전트 제품의 관리 화면보다 넓고, 플랫폼 운영 도구보다 담당자 쪽에 가깝습니다. 관리 화면은 대개 설치·로그·설정값을 다루는 운영자용 도구여서, 업무 담당자가 「이 에이전트가 어떤 성격으로 무슨 일을 언제 하는가」를 읽기 어렵습니다. 반면 AAS는 성격·방법·일정이라는 업무 단위로 화면을 나누기 때문에, 부서 담당자가 직접 만들고 IT 담당자는 그 결과를 같은 화면에서 검토합니다. 인사 담당자가 이력서 1차 심사 기준을 스킬 문서로 적으면, 기준이 바뀐 이력이 문서 판으로 남아 나중에 누가 무엇을 바꿨는지 추적할 수 있습니다. 정의 대상이 업무 언어로 고정되어 있으므로 이후 장에서 다루는 기능·유즈케이스·관측 화면은 모두 이 세 대상 중 하나를 만들거나 바꾸거나 지켜보는 일로 읽을 수 있습니다.

3.1.2 만들기에서 나누기까지 한 화면에서 처리하는 조직 안 콘솔

한 화면에 모인 네 기능 묶음

AAS는 에이전트를 만들고, 일을 시키고, 실행 결과를 지켜보고, 잘 만든 스킬을 조직에 나누는 네 가지 기능 묶음을 한 콘솔에 모았습니다. 기존에는 이 네 가지가 설정 파일, 메신저, 로그 서버, 공유 폴더에 각각 흩어져 있어 담당자가 에이전트 하나를 운영하려면 서너 개의 도구를 오가야 했습니다. 한 화면에 모은다는 말은 메뉴를 합쳤다는 뜻보다, 만든 사람이 실행 결과를 같은 화면에서 보고 곧바로 스킬을 고칠 수 있다는 뜻에 가깝습니다. 각 묶음의 화면과 동작은 4장에서 실제 화면으로 설명합니다.

기능 묶음	담당자가 하는 일	대표 화면
만든다	에이전트 추가, 업무별 프로파일의 성격·모델 정의, 스킬 문서와 판 관리, 정기 업무 등록	에이전트, 프로파일, 스킬, 자동화
시킨다	진행 단계·실행 승인·되묻기가 보이는 채팅, 여러 에이전트에게 한 번에 묻는 회의	대화, 오피스
지켜본다	정기 업무의 실패·멈춤·알림 누락, 자격증명 만료, 호출 관계 확인	오늘 볼 것, Cron 헬스체크, 흐름
나눈다	사내 스킬 마켓 등록·설치, 사용자별 에이전트와 권한	마켓, 사용자·권한

조직 안 설치가 갖는 의미

AAS는 외부 클라우드 서비스가 아닌 조직 안 서버에 설치되는 온프레미스 콘솔입니다. 2장에서 본 것처럼 국가망 보안체계는 업무 정보를 기밀(C)·민감(S)·공개(O) 세 등급으로 나눠 보안 통제를 차등 적용하지만[S5], 기밀 등급 업무는 여전히 분리된 망 안에 남기 때문에, 에이전트가 다루는 회의 녹음·공문·고객 연락처를 외부로 보내지 않고 처리할 수 있어야 합니다. AAS는 에이전트 플랫폼과 같은 조직 망 안에서 실행되고, 음성 인식과 문자

인식(OCR, Optical Character Recognition)도 조직 안 모델로 연결해 쓰도록 구성합니다. 설치 방식과 보안 원칙은 7장에서 상세히 다룹니다.

3.2 오픈소스 Hermes Agent 1종에 연결되는 현재 범위와 플랫폼에서 스킬까지 이어지는 계층

현재 AAS가 연결되는 에이전트 플랫폼은 오픈소스 Hermes Agent 하나입니다. 에이전트 플랫폼은 에이전트를 실제로 실행하고 메신저·모델·외부 시스템과 연결하는 실행 환경이며, AAS는 그 위에서 정의와 관찰을 맡는 콘솔입니다. AAS를 검토하는 조직은 먼저 지금 쓰고 있거나 쓰려는 에이전트 플랫폼이 무엇인지부터 확인해야 합니다. 이 범위를 제품 소개 단계에서 밝혀 두는 이유는, 3장부터 8장까지의 기능 설명을 「어떤 에이전트 플랫폼에나 붙는 제품」의 기능으로 읽지 않도록 하기 위해서입니다. 다른 플랫폼 연결은 10장의 로드맵 항목입니다.

3.2.1 Hermes Agent를 이미 쓰는 조직과 다른 플랫폼을 쓰는 조직의 차이

Hermes Agent를 이미 쓰는 조직

Hermes Agent를 이미 쓰는 조직은 지금 운영 중인 에이전트와 스킬, 정기 업무를 그대로 둔 채 AAS를 얹을 수 있습니다. AAS는 에이전트 플랫폼을 고치지 않고, 플러그인·설정·버전을 바꾸지 않은 상태에서 플랫폼이 공식으로 제공하는 API로 변경을 요청합니다. 플랫폼 API에 길이 없는 마켓 패키지 설치·삭제 두 경우만 예외로, 범위와 처리 방식은 7장에서 밝힙니다. 설치 첫날부터 기존 프로파일 목록, 스킬 수, 정기 업무, 최근 활동이 콘솔에 나타나고, 담당자는 새로 만들기보다 이미 있는 에이전트를 확인하는 일부터 시작합니다. IT 부서가 명령줄로 등록해 둔 정기 업무가 실패해도 알림이 안 가는 상태라면, AAS는 그런 작업을 목록으로 먼저 보여 줍니다. 이런 조직에 AAS는 이미 운영 중인 에이전트를 업무 담당자에게 넘겨주는 콘솔 역할을 합니다.

다른 에이전트 플랫폼을 쓰는 조직

다른 에이전트 플랫폼을 쓰는 조직은 현재 AAS를 그 플랫폼에 바로 연결할 수 없습니다. 이 경우 선택지는 두 가지입니다. 첫째, 새 부서 업무 하나를 골라 Hermes Agent 위에서 따로 시작하고 기존 플랫폼은 그대로 운영하는 방법이 있습니다. 둘째, 로드맵 셋째 항목인 두 번째 플랫폼 연결이 제공될 때까지 업무 유즈케이스 선정과 스킬 문서 정리를 먼저 진행하는 방법이 있습니다. 반면 에이전트 플랫폼을 아직 정하지 않은 조직은 Hermes Agent와 AAS를 함께 설치해 시작하는 편이 검토 범위가 가장 좁습니다.

조직 유형	지금 적용 가능성	시작 방법
Hermes Agent를 이미 운영	바로 연결	기존 에이전트·정기 업무를 콘솔에서 확인한 뒤 부서 담당자에게 넘긴다
에이전트 플랫폼 미정	함께 설치	Hermes Agent와 AAS를 조직 안에 함께 설치하고 첫 유즈케이스 하나로 시작한다
다른 에이전트 플랫폼을 운영	현재 연결 불가	별도 업무로 병행하거나 두 번째 플랫폼 연결(10장 로드맵)을 기다린다

3.2.2 런타임에서 MCP 서버까지 이어지는 계층과 AAS가 바꾸는 범위

플랫폼에서 외부 시스템까지 이어지는 네 계층

Hermes Agent 위의 구성 요소는 네 계층으로 나뉩니다. 맨 아래 런타임은 에이전트 프로세스를 실행하고 메신저 게이트웨이와 모델을 연결하는 실행 환경이며, AAS의 에이전트는 사용자 한 사람에게 배정되는 이 실행 환경 하나입니다. 그 위의 프로파일(Profile)은 에이전트 안에서 업무별로 나눈 묶음으로, 성격·모델·메신저 연결·스킬 목록을 프로파일마다 따로 갖습니다. 프로파일 안에는 업무 방법을 적은 스킬(Skill)과 실행 일정인 정기 업무(Cron)가 있고, 스킬은 다시 스크립트와 MCP(Model Context Protocol) 서버, 외부 시스템 호출을 통해 CRM·위키·드라이브 같은 업무 시스템에 닿습니다. MCP는 에이전트가 외부 도구와 데이터를 일정한 규약으로 부르게 하는 공개 프로토콜입니다. 하나의 업무 결과는 런타임에서 시작해 프로파일, 스킬과 정기 업무를 거쳐 외부 시스템까지 이어지는 경로로 만들어집니다.

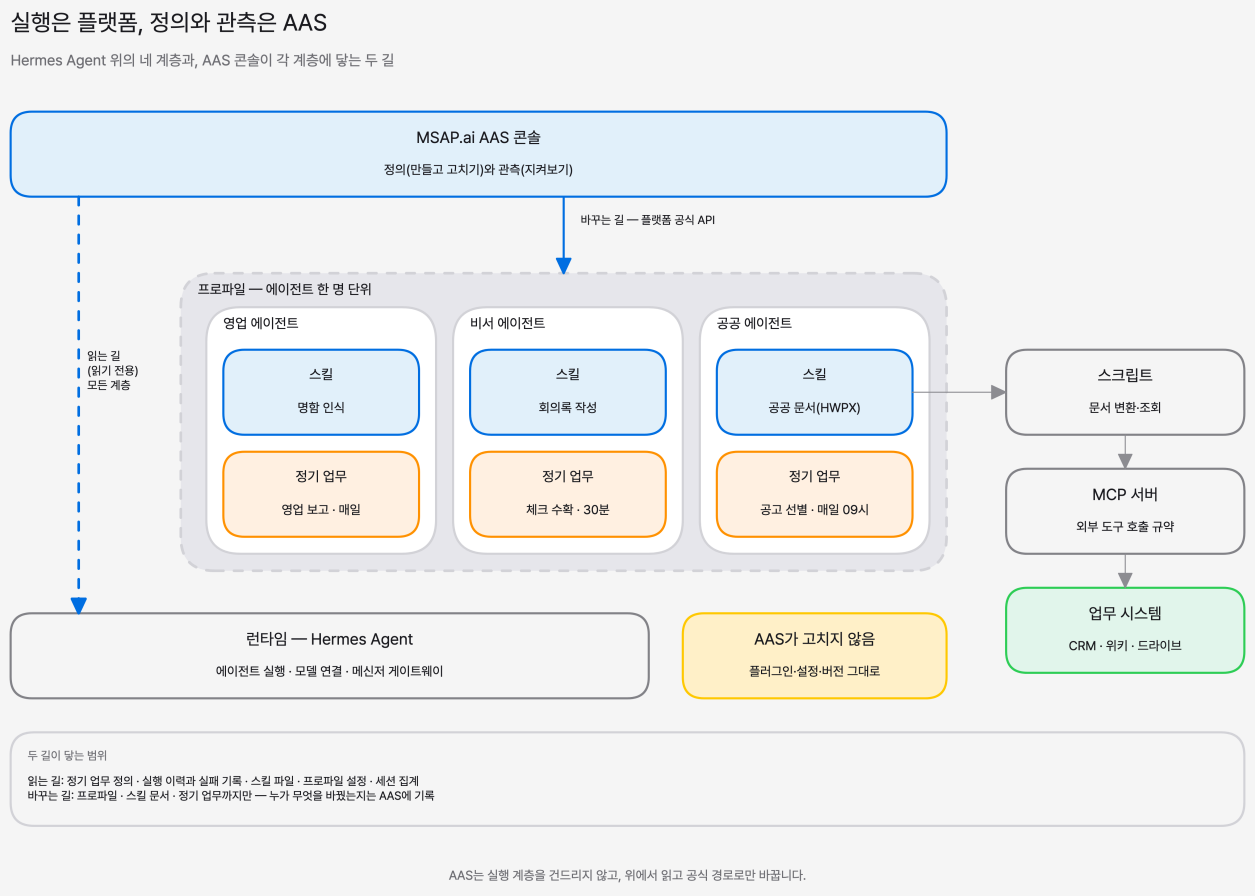


그림 3-1. Hermes Agent 런타임·프로파일·스킬과 정기 업무·MCP 서버로 이어지는 실행 계층과, 그 위에서 정의·관측을 맡는 AAS 콘솔

실행은 플랫폼이, 정의와 관측은 AAS가 맡는 역할 분담

이 계층에서 에이전트를 실제로 실행하는 주체는 Hermes Agent이고, AAS는 실행 결과를 읽고 정의를 바꾸는 일만 맡습니다. AAS가 멈추더라도 이미 걸어 둔 정기 업무는 플랫폼에서 계속 실행되고, 반대로 AAS를 새로 설치해도 실행 중인 에이전트에는 영향이 없습니다. AAS가 읽는 길과 바꾸는 길은 분리되어 있습니다. 읽는 길은 읽기 전용으로 실행 기록과 설정을 수집하고, 바꾸는 길은 마켓 패키지 설치·삭제 두 경우를 빼면 플랫폼의 공식 API 하나만 씁니다. 누가 언제 무엇을 바꿨는지는 AAS의 변경 기록에 남으므로, 감사 담당자는 플랫폼 로그와 콘솔 기록을 맞대어 볼 수 있습니다.

계층	실행 주체	AAS가 읽는 것	AAS가 바꾸는 것
런타임	Hermes Agent	게이트웨이 상태, 모델 연결	바꾸지 않음(플러그인·설정·버전 무변경)
프로파일	Hermes Agent	성격, 모델, 메신저 연결, 최근 활동	프로파일 만들기·내보내기·삭제, 성격·모델 정의(플랫폼 공식 API 경유)
스킬·정기 업무	Hermes Agent	스킬 문서와 판, 실행 일정, 실패·알림 대상	스킬 문서, 정기 업무 등록·수정
MCP 서버·외부 시스템	각 업무 시스템	스킬이 부르는 호출 관계, 자격증명 이름과 위치(값 제외)	바꾸지 않음(연결 시스템은 고객 환경에서 설정)

플랫폼 기능 항목과 조직이 보는 업무 단위의 차이

에이전트 플랫폼의 공식 문서는 메신저 게이트웨이, 이벤트 훅, MCP 연동 같은 연결 기능과 정기 업무, 스킬, 작업 보드, 하위 에이전트 위임 같은 실행 기능을 서로 독립된 항목으로 설명합니다. 각 항목은 그 자체로 완결된 규격이어서 따로따로 읽히지만, 조직이 인식하는 단위는 「주간 영업 보고」처럼 여러 기능이 한 번에 동원되는 업무 하나입니다. 업무 하나는 대개 시작 신호(정해진 일정이나 들어온 메시지) 하나, 처리 절차 여럿, 결과를 보낼 배달 경로 하나로 이루어지므로 기능 항목 서너 개에 동시에 걸칩니다. 기능 목록만으로는 업무 담당자가 자기 업무가 어디에 해당하는지 찾기 어렵기 때문에, AAS는 프로파일과 스킬, 정기 업무, 호출 관계를 업무 단위로 이어서 보여 주는 쪽을 택했습니다. 이 연결은 4장의 화면과 6장의 흐름 그림에서 다시 확인할 수 있습니다.

3.3 현업이 업무 프로그램을 직접 만들던 폭스프로·디베이스 선례와 AAS의 대응

업무를 아는 사람이 직접 업무 도구를 만드는 일은 처음 등장한 현상이 아닙니다. 1980~90년대 디베이스(dBase)와 그 계열 제품인 폭스프로(FoxPro)는 전산 전문가가 아닌 사무 담당자도 화면·메뉴·입력 검사가 붙은 업무 프로그램을 짧은 시간에 만들게 했습니다[S8]. 이 선례는 AAS의 설계 방향인 「업무를 아는 사람이 만든다」를 가장 짧게 설명하는 비유입니다. 다만 비유가 성립하는 범위는 역할 분담과 조직 확산 방식이며, 기술 구조가 같다는 뜻은 아닙니다.

3.3.1 데이터베이스 엔진 위에서 현업 도구가 만든 업무 프로그램

디베이스와 폭스프로가 만든 엔진·도구 분업

폭스프로는 Ashton-Tate의 디베이스 II·III에서 파생된 FoxBASE를 잇는 제품으로, 데이터베이스 관리 시스템과 빠른 업무 프로그램 개발 도구를 한 제품에 담았습니다[S8]. 데이터를 저장하고 찾는 일은 엔진이 맡고, 담당자는 그 위에서 입력 화면과 메뉴, 조회 조건만 정의하면 되었습니다. 예를 들어 마우스와 메뉴로 다루는 데이터베이스 조회 화면을 입력 검사가 붙은 입력 화면까지 포함해 100줄이 안 되는 코드로 만들 수 있었습니다[S8]. 회계·재고·고객 관리처럼 부서마다 조금씩 다른 업무 프로그램이 전산실을 거치지 않고 현장에서 만들어졌습니다. Microsoft는 1992년 Fox Software를 인수했고, 이후 Visual FoxPro라는 이름으로 이어진 제품군은 2007년 개발이 종료되었습니다[S8].

엔진과 현업 도구 분업이 업무 프로그램 확산을 만든 방식

이 분업이 확산을 만든 이유는 어려운 부분과 업무 부분을 나눴기 때문입니다. 데이터 무결성과 저장 구조처럼 전문 지식이 필요한 영역은 엔진이 책임지고, 어떤 항목을 입력받고 어떤 조건으로 조회할지는 업무를 아는 담당자가 결정했습니다. AAS도 같은 방식으로 역할을 나눕니다. 모델 호출과 에이전트 실행은 에이전트 플랫폼과 모델이 맡고, 에이전트의 성격과 업무 처리 방법, 실행 일정은 부서 담당자가 콘솔에서 정의합니다. 이 분업에서 IT 부서는 플랫폼과 모델, 자격증명의 안정성에 집중하고, 부서 업무 규칙이 바뀔 때마다 개발 요청을 받지 않아도 됩니다.



그림 3-2. 데이터베이스 엔진 위의 폭스프로·디베이스와 에이전트 플랫폼 위의 AAS를 직접 정의·현장에서 나옴·기다리지 않음·조직에 남음 네 기준으로 나란히 놓은 대응 구조

3.3.2 만든 사람이 떠나도 남는 업무 프로그램과 조직에 남는 에이전트

개인 작업이 조직 자산으로 바뀌는 대응

폭스프로로 만든 업무 프로그램은 만든 사람이 부서를 옮기거나 퇴사해도 파일로 남아 다음 담당자가 계속 썼습니다. 디스켓과 공유 폴더로 복사되면서 한 부서의 프로그램이 다른 부서와 지사로 퍼졌고, 같은 양식의 업무가 여러 곳에서 같은 방식으로 처리되었습니다. AAS에서는 사내 스킬 마켓이 이 역할을 맡습니다. 한 부서가 만든 스킬과 에이전트 구성을 마켓에 등록하면 다른 부서가 설치해 쓰고, 담당자가 바뀌어도 성격·스킬·정기 업무가 조직 안에 그대로 남습니다. 예를 들어 신규 입사자는 자기 에이전트를 받은 뒤 새 프로파일을 만들 때 「다른 에이전트에서 가져오기」로 전임자 에이전트의 성격·설정을 출발점으로 삼아, 첫 주부터 같은 업무 방식으로 시작할 수 있습니다.

폭스프로·디베이스 선례	AAS
데이터베이스 엔진	에이전트 플랫폼과 모델
폭스프로·디베이스	AAS
현장에서 만든 업무 프로그램	부서가 만든 스킬과 에이전트
디스켓·공유 폴더로 퍼진 프로그램	사내 스킬 마켓
만든 사람이 떠나도 남는 프로그램	조직에 남는 에이전트와 스킬

선례가 남긴 관리 문제와 AAS의 대응

다만 현업이 만든 업무 프로그램은 관리 문제도 함께 남겼습니다. 누가 어떤 판을 쓰는지, 어느 프로그램이 아직 쓰이는지 전산실이 알기 어려웠고, 만든 사람이 떠난 뒤에는 고칠 수 있는 사람이 남지 않는 경우도 생겼습니다. AAS는 이 문제를 처음부터 콘솔의 기능으로 다룹니다. 스킬 문서는 판 단위로 이력이 남고, 마켓 패키지는 어디에 설치되었는지 표시되며, 정기 업무의 실패·멈춤·알림 누락은 관측 화면에 모입니다. 부서가 직접 만든 에이전트가 늘어나더라도 IT 부서는 전체 목록과 상태를 한 콘솔에서 확인할 수 있습니다.

3.4 부서 담당자부터 보안 감사 담당까지 사용자 넷의 역할과 역할 템플릿 20종

AAS를 쓰는 사람은 부서 담당자, 부서장·팀 리더, IT·플랫폼 관리자, 보안·감사 담당의 네 부류입니다. 에이전트 도입 결정에는 보통 이 네 부류가 함께 참여하고, 각자 확인하려는 정보가 다릅니다. 예를 들어 부서 담당자는 업무 시간이 얼마나 줄어드는지를 묻고, 보안 담당자는 에이전트가 무엇에 접근하는지를 묻습니다. AAS는 같은 데이터를 역할마다 다른 화면으로 보여 주며, 각 역할이 얻는 것을 따로 정리해 두면 조직 내부 설득 자료로 바로 쓸 수 있습니다.

3.4.1 사용자 넷이 각자 보는 화면과 얻는 것

역할별 권한과 주 화면

네 부류 가운데 주 사용자는 부서 담당자이며, 나머지 세 부류는 담당자가 만든 결과를 보거나 그 기반을 관리합니다. 부서 담당자는 에이전트를 만들고 정기 업무를 예약하고 채팅으로 일을 시킵니다. 담당자는 관리자가 정한 한도 안에서 자기 에이전트를 추가하고, 그 안에 업무별 프로파일을 둡니다. 새 프로파일은 잘 쓰는 프로파일을 복제하거나 다른 에이전트에서 가져와 시작하고, 다 쓴 프로파일은 보관본을 내보낸 뒤 지웁니다(4.1.2절). 부서장·팀 리더는 팀 에이전트가 처리한 일과 실패한 일을 보고 우선순위를 정합니다. IT·플랫폼 관리자는 플랫폼·모델·자격증명·사용자 권한을 관리하며, 표준 로그인(OIDC, OpenID Connect) 그룹에 따라 사용자마다 볼 수 있는 에이전트를 정합니다. 권한이 역할별로 나뉘므로 부서 담당자가 늘어나도 플랫폼 설정은 IT 부서의 통제 아래 남습니다.

사용자	주로 하는 일	주 화면	결정에 쓰는 정보
부서 담당자	에이전트 추가, 프로파일 만들기(복제·가져오기)·삭제, 정기 업무 예약, 채팅으로 일 시키기	내 에이전트, 스킬, 자동화, 대화	스킬 실행 결과, 사람 확인이 필요한 항목
부서장·팀 리더	팀 에이전트가 하는 일 확인	대시보드, 오늘 볼 것, 오피스	팀 에이전트별 처리·실패 현황
IT·플랫폼 관리자	플랫폼·모델·자격증명·권한 관리, 사람별 에이전트 한도와 소유권 이전	사용자·권한, 에이전트, 자격증명	만료 임박 자격증명, 실패한 정기 업무
보안·감사 담당	접근 대상과 변경 이력 점검	흐름, 변경 기록, 활동	스킬이 부르는 외부 시스템, 누가 무엇을 바꿨는지

보안·감사 담당이 별도 사용자인 이유

보안·감사 담당을 별도 사용자로 둔 이유는 에이전트 위험의 상당 부분이 외부 공격보다 내부 사용 방식에서 생기기 때문입니다. 1장과 2장에서 본 것처럼 Gartner는 허가되지 않은 에이전트 행위의 대부분이 내부 정책 위반에서 나오고, 에이전트를 감독하는 기능이 별도 시장으로 자란다고 전망했습니다[S3]. AAS는 스킬 문서와 스크립트, 실행 기록에서 호출 관계를 뽑아 흐름으로 보여 주고, 자격증명은 값 없이 이름·위치·쓰는 곳만 표시합니다. 보안·감사 담당은 에이전트를 직접 다루지 않고도 무엇이 어디를 부르는지와 누가 무엇을 바꿨는지를 확인할 수 있습니다.

3.4.2 마케팅·영업·총무 등 역할 템플릿 20종으로 채우는 에이전트 성격

부서와 역할에 맞춘 성격 문서의 출발점

AAS는 에이전트 성격(SOUL)을 처음부터 쓰지 않아도 되도록 역할 템플릿 20종을 기본으로 제공합니다. 템플릿은 마케팅·영업·연구소·엔지니어링·총무·회계·인사·고객지원·기획 등 부서별로 한국어판과 영어판이 짝을 이루며, 프로파일의 성격 문서를 채우는 출발점이 됩니다. 템플릿 본문에는 회사·부서·역할·에이전트 이름을 넣는 빈칸이 있어서, 예를 들어 영업 템플릿에는 「○○회사 영업부 소속 고객 관리 담당 에이전트」 같은 소개 문장과 고객·리드 정리 같은 기본 업무 범위가 들어 있습니다. 다만 조직마다 쓰는 연결 시스템(CRM·위키·드라이브 등)은 고객 환경에 맞춰 설정하므로, 템플릿은 성격과 업무 범위의 출발점으로만 쓰입니다.

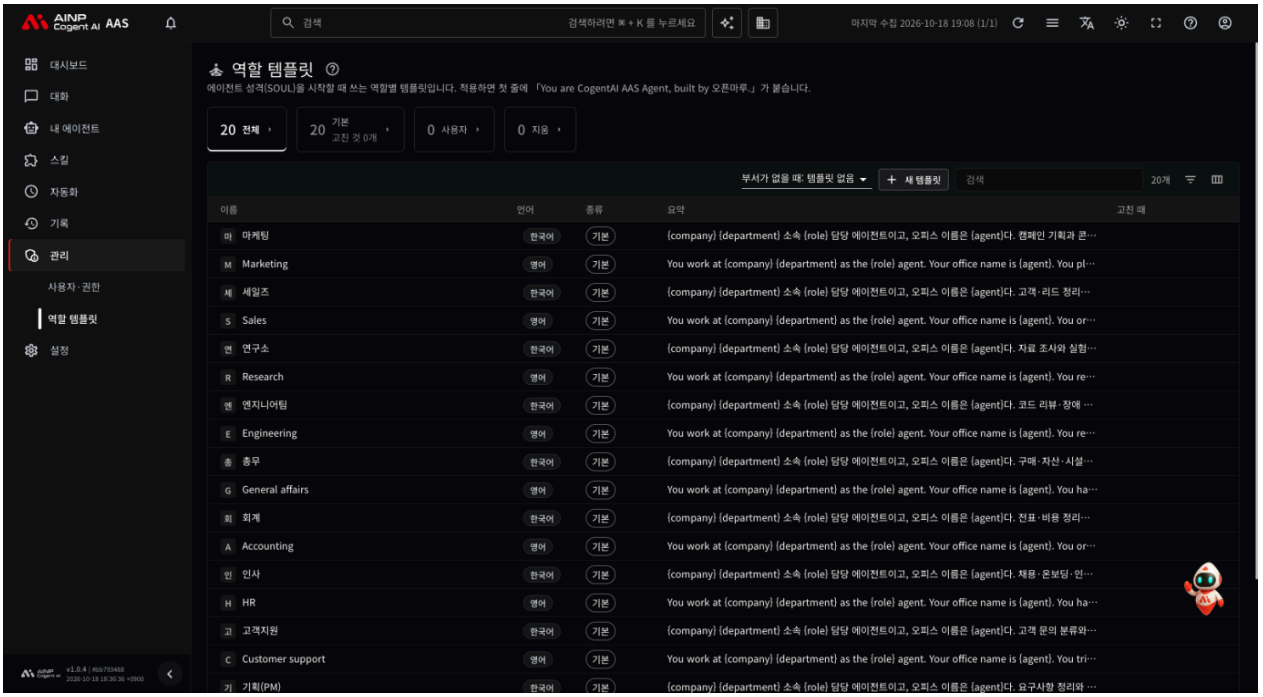


그림 3-3. 역할 템플릿 화면 — 상단의 「20 전체 · 20 기본」 숫자와, 부서마다 한국어·영어 템플릿이 짝으로 놓인 목록, 요약 열의 회사·부서·역할 빈칸을 보면 됩니다

템플릿을 조직 기준으로 고쳐 쓰는 방법

역할 템플릿은 조직이 직접 고치고 새로 추가할 수 있습니다. 화면 상단은 기본 템플릿, 사용자가 만든 템플릿, 지운 템플릿의 수를 따로 세고, 「새 템플릿」 버튼으로 조직 고유의 부서 템플릿을 등록합니다. 부서 정보가 없는 사용자에게 어떤 템플릿을 적용할지도 설정에서 정합니다. 이 기능으로 공공기관은 기안·민원 담당 템플릿을, 제조 기업은 품질·구매 담당 템플릿을 추가해 조직 전체의 에이전트 성격을 같은 기준으로 맞출 수 있습니다. 부서

담당자는 백지에서 성격 문서를 쓰지 않고, IT·플랫폼 관리자는 조직 표준에 맞는 성격만 배포되도록 관리할 수 있습니다. 4장은 이 사용자들이 실제로 쓰는 콘솔 화면을 네 기능 묶음 순서로 보여 줍니다.

4장: 만들고 시키고 지켜보고 나누는 네 기능 묶음을 한 화면에 모은 AAS 콘솔의 실제 화면

3장에서 정의한 네 기능 묶음, 즉 만들기·시키기·지켜보기·나누기는 오픈소스 에이전트 플랫폼 Hermes Agent에 연결된 AAS 콘솔 한 화면에 모여 있습니다. 1장에서 본 것처럼 에이전트를 만드는 도구, 일을 시키는 창구, 실행 결과를 보는 화면이 서로 다른 프로그램에 흩어져 있으면 시험 단계를 넘어 일상 업무로 옮겨 가기 어렵습니다. 네 묶음의 실제 화면을 차례로 보면 업무 담당자가 직접 하는 일과 관리자가 통제하는 항목이 어디서 갈리는지 판단할 수 있습니다. 제품 기능 화면은 여러 사용자가 함께 쓰는 쿠버네티스 배포본(v1.0.4)이고, 정기 업무가 실제로 실행되는 첫 화면은 하나의 운영 설치본에서 찍은 화면 예시입니다.

네 묶음에 공통으로 적용되는 원칙은 AAS가 에이전트 플랫폼을 고치지 않고, 화면에서 바꾼 설정을 모두 Hermes Agent 대시보드의 공식 API로만 보낸다는 것입니다. 값의 검사와 저장은 Hermes Agent가 맡고, 누가 언제 어느 대상에 무엇을 바꿨는지는 AAS의 변경 기록에 남습니다. AAS는 플랫폼이 거절한 요청도 같은 기록에 남기므로, 성공한 변경과 막힌 시도를 함께 추적할 수 있습니다. 1장에서 본 내부 정책 위반 전망[S3]을 고려하면, 만드는 권한을 업무 담당자에게 넘기려는 조직이라면, 변경이 한 경로로만 들어오고 그 기록이 남는 구조를 먼저 갖춰야 합니다.

네 묶음과 각 묶음의 대표 화면, 관리자가 통제하는 항목은 다음과 같습니다.

기능 묶음	대표 화면	업무 담당자가 하는 일	관리자 통제 항목
만든다	에이전트, 프로파일, 스킬 목록, 모델	에이전트 추가, 프로파일 만들기(복제·다른 에이전트에서 가져오기)·삭제, 성격·모델·스킬·정기 업무 정의	공식 API 경유 변경, 변경 기록, 사용자별 에이전트 한도, 삭제 전 내보내기와 재확인
시킨다	팀 채팅, 오피스 회의 탭	업무 지시, 실행 승인, 되묻기 응답	명령 실행 전 승인 카드
지켜본다	오늘 볼 것, 하루 두 번 요약	실패·만료·답 대기 항목 처리	첫 화면 지표, 요약 알림
나눈다	스킬 마켓, 에이전트·사용자	패키지 설치, 자기 에이전트 운용	OIDC 그룹, 사용자별 한도, 미사용 자동 멈춤

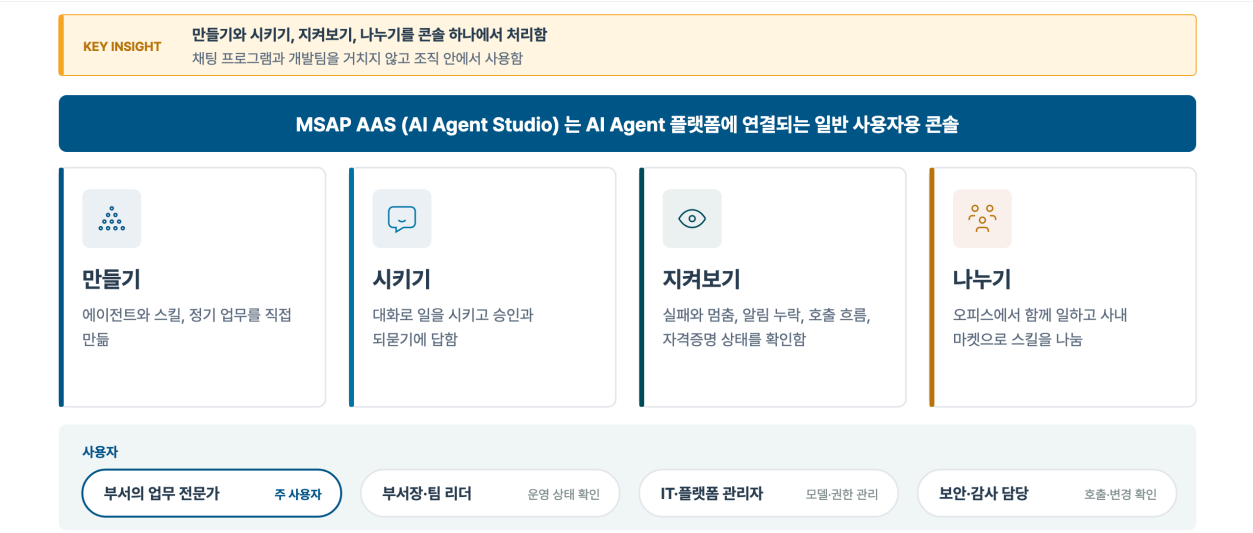


그림 4-1. 만들기·시키기·지켜보기·나누기 네 묶음을 콘솔 하나에 모은 AAS와, 주 사용자인 부서 업무 전문가를 포함한 네 사용자

4.1 에이전트 추가와 업무별 프로파일, 스킬 판 관리, 정기 업무 등록을 한 화면에서 정하는 만들기

AAS의 만들기 묶음은 두 층으로 나뉩니다. 사람마다 에이전트를 받고, 그 안에 업무별 프로파일을 둡니다. 성격·모델·스킬·정기 업무라는 네 요소는 프로파일마다 따로 정하며, 콘솔 한 곳에서 다룹니다. Hermes Agent만 쓰면 이 요소들이 설정 파일, 관리 화면, 명령줄에 나뉘어 있어 업무 담당자가 직접 다루기 어렵습니다. 3장에서 본 디베이스와 폭스프로가 전산 전문가가 아닌 사람도 업무 프로그램을 만들게 했듯이[S8], AAS는 에이전트 구성을 업무 담당자가 읽고 고칠 수 있는 화면으로 바꿉니다. 담당자는 관리자가 정한 한도 안에서 에이전트를 추가하고, 그 안에 프로파일을 만들 때 이미 쓰는 프로파일을 복제하거나 다른 에이전트에서 가져와 시작합니다. 다 쓴 프로파일은 보관본을 내보낸 뒤 지웁니다. 두 층의 작업 절차와 확인 장치는 4.1.2에서 따로 설명합니다.

4.1.1 모델과 게이트웨이 상태가 보이는 에이전트 프로파일 화면

프로파일에 모이는 에이전트 구성

Hermes Agent에서 프로파일은 성격 문서, 설정, 비밀값, 스킬, 정기 업무를 업무 하나에 맞춰 한데 묶은 단위입니다. AAS의 에이전트 하나는 프로파일을 여러 개 가질 수 있어, 기본 프로파일(main) 옆에 업무별 프로파일을 따로 둡니다. AAS의 프로파일 목록은 프로파일마다 게이트웨이(에이전트가 메신저·채팅 요청을 받는 상주 프로세스)가 실행 중인지, 연결된 채널, 확인할 것, 주 모델, 활성 정기 업무 수, 스킬 수, 최근 활동을 한 줄에 보여 줍니다. 예를 들어 그림 4-2의 배포본 화면에서는 프로파일 2개의 게이트웨이가 모두 실행 중이고, 각 프로파일에 스킬 58개가 들어 있으며, 위쪽 칸은 최근 7일 동안 활동이 없는 「쉬는 프로파일」 1개를 따로 셉니다.

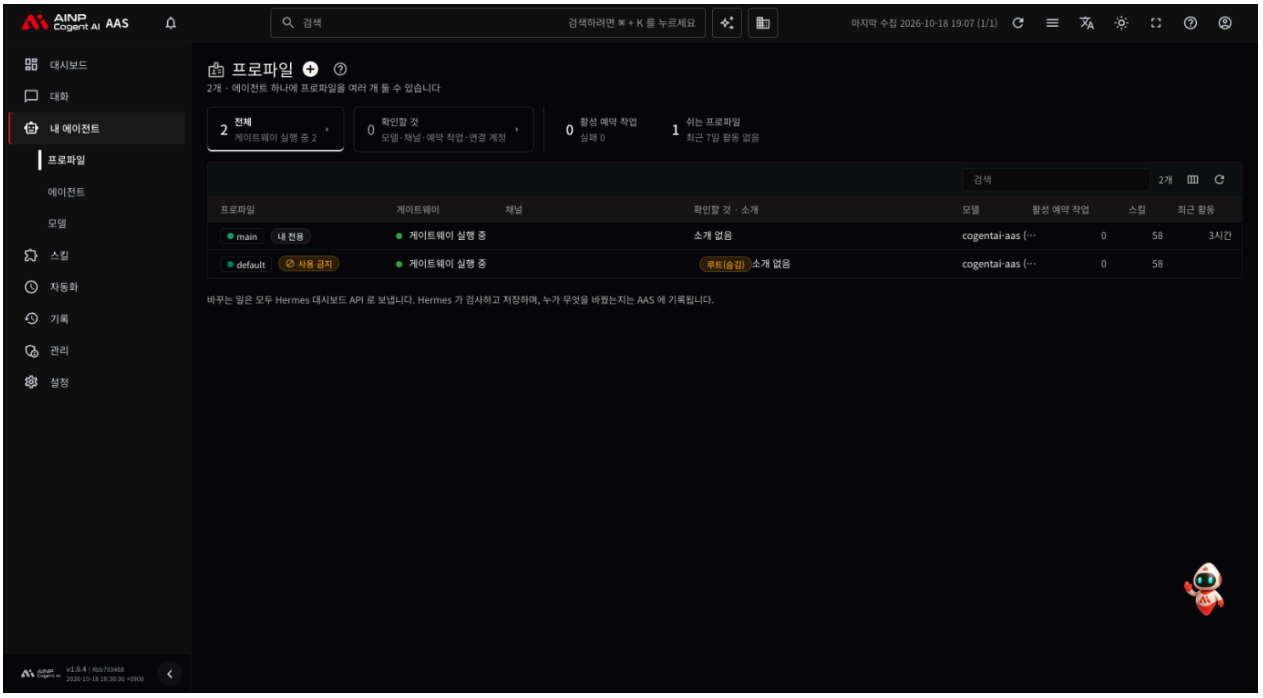


그림 4-2. 프로파일 목록. 위쪽 칸의 「전체 2 · 게이트웨이 실행 중 2」와 「쉬는 프로파일 1」, 표 아래의 「바꾸는 일은 모두 Hermes 대시보드 API로 보내고, 누가 무엇을 바꿨는지는 AAS에 기록」 안내 문구를 보면 변경 경로가 화면에 드러나 있습니다

프로파일을 누르면 상세 화면이 여덟 개 탭으로 열리고, 그 가운데에는 MCP 서버를 켜고 끄는 탭과 메신저 연결 탭도 있습니다. 탭마다 보이는 내용은 다음 표와 같이 나뉩니다.

탭	보이는 내용
개요	확인할 것(남은 오류, 만료되는 자격증명), 게이트웨이·채널·정기 업무·스킬·MCP 서버 수, 최근 7일 활동, 주 모델
성격(SOUL)	에이전트의 역할과 규칙을 적은 문서, 편집과 판 비교
설정	플랫폼 설정 값
비밀값	비밀값 이름과 채워졌는지 여부(값은 표시하지 않음)
스킬	이 프로파일이 쓰는 스킬과 켜기·끄기
도구묶음·MCP	도구묶음과 MCP 서버 켜기·끄기
정기 업무	이 프로파일에 등록된 정기 업무 목록
메신저 연결	이 프로파일이 쓰는 메신저 채널 연결

주 모델 점검과 값이 보이지 않는 비밀값

프로파일 상세의 개요 탭에서는 주 모델을 바꾸고 게이트웨이를 다시 시작하거나 멈출 수 있습니다. 다만 게이트웨이 중지와 모델 변경처럼 업무를 바로 멈출 수 있는 조작은 한 번 더 묻습니다. AAS는 조직의 모델 게이트웨이인 LiteLLM에 등록되어 실제로 응답하는 모델 가운데에서만 주 모델을 고르게 해, 존재하지 않는 모델 이름을

설정에 적는 실수를 막습니다. 모델 화면은 설정에 적힌 모델과 LiteLLM 목록을 맞대어 어긋난 프로파일을 표시하고, 모델마다 1토큰 호출을 보내 실제로 응답하는지 점검합니다. 비밀값 탭과 MCP 서버의 인증값은 이름과 채워졌는지 여부만 보이고 값은 화면에 나오지 않습니다.

4.1.2 사람마다 한도 안에서 추가하는 에이전트와 복제·가져오기로 시작해 보관본을 남기고 지우는 프로파일

사람마다 받는 에이전트와 그 안의 업무별 프로파일

AAS에서 무엇을 늘리고 줄이는지는 두 층으로 나뉩니다. 에이전트는 사용자 한 사람에게 배정되는 실행 단위입니다. 쿠버네티스 배포본에서는 에이전트를 하나 추가할 때마다 실행 이미지를 받고 저장 공간(디스크)을 붙인 실행 환경이 따로 생깁니다. 프로파일은 그 에이전트 안의 업무 묶음으로, 성격(SOUL)·설정·비밀값·스킬·도구묶음과 MCP 서버·정기 업무·메신저 연결·모델을 프로파일마다 따로 가집니다. 예를 들어 영업 담당자 한 사람은 에이전트 하나를 받고, 그 안에 기본 프로파일 main과 명함 등록용·주간 보고용 프로파일을 따로 둘 수 있습니다. Hermes Agent만 쓸 때는 이런 구성을 하나 더 만들려면 관리 화면과 명령줄에서 토큰과 설정을 일일이 다시 적어야 했습니다. AAS는 두 층의 작업을 「에이전트」와 「프로파일」 두 화면으로 나눕니다.

에이전트 층 — 추가, 소유권 이전, 지우기, 한도와 자동 멈춤

에이전트 화면은 전체 에이전트의 이름·상태·소유자·메시지·만든 때를 한 줄씩 보여 주고, 위쪽 칸에서 내 에이전트 수와 한도를 함께 셉니다. 제목 옆 「+」 버튼을 누르면 에이전트 만들기 창이 열리는데, 이 창이 받는 값은 이름(선택 입력) 하나뿐입니다. 만들기를 누르면 에이전트는 실행 이미지를 받고 디스크를 연결하는 동안 「준비 중」으로 표시되다가 사용할 수 있는 상태가 됩니다. 업무에 맞춘 성격·스킬·정기 업무는 이 단계가 아니라 그 안의 프로파일에서 정합니다. 에이전트 층에서 하는 작업은 다음과 같습니다.

작업	하는 일	확인 장치	남는 기록
추가	이름만 주고 에이전트를 만든다. 실행 이미지와 디스크가 준비되면 사용할 수 있다	사용자별 한도(기본 3개), 준비 중이거나 실패한 에이전트도 한도에 셈	상세의 이름·ID·소유자·상태·만든 때
소유권 이전	에이전트를 다른 사용자에게 넘긴다	에이전트 상세 서랍에서만 실행	상세의 소유자 칸
지우기	더 쓰지 않는 에이전트를 지운다	에이전트 상세 서랍에서만 실행, 남길 프로파일은 먼저 내보내기	미리 내보낸 프로파일 보관본
개수 한도	관리자가 「이 사람의 개수 한도」를 바꿔 저장한다	관리자만 보이는 칸	사용자별 한도 값
멈춤과 다시 시작	30일 동안 대화와 정기 업무 실행이 없거나 OIDC 그룹에서 빠지면 멈추고, 멈춘 에이전트는 행 메뉴에서 다시 시작한다	멈춘 동안 데이터 보존	상태 칸의 「멈춤」과 이유(예: 「OIDC 그룹에서 빠져 멈춤」)

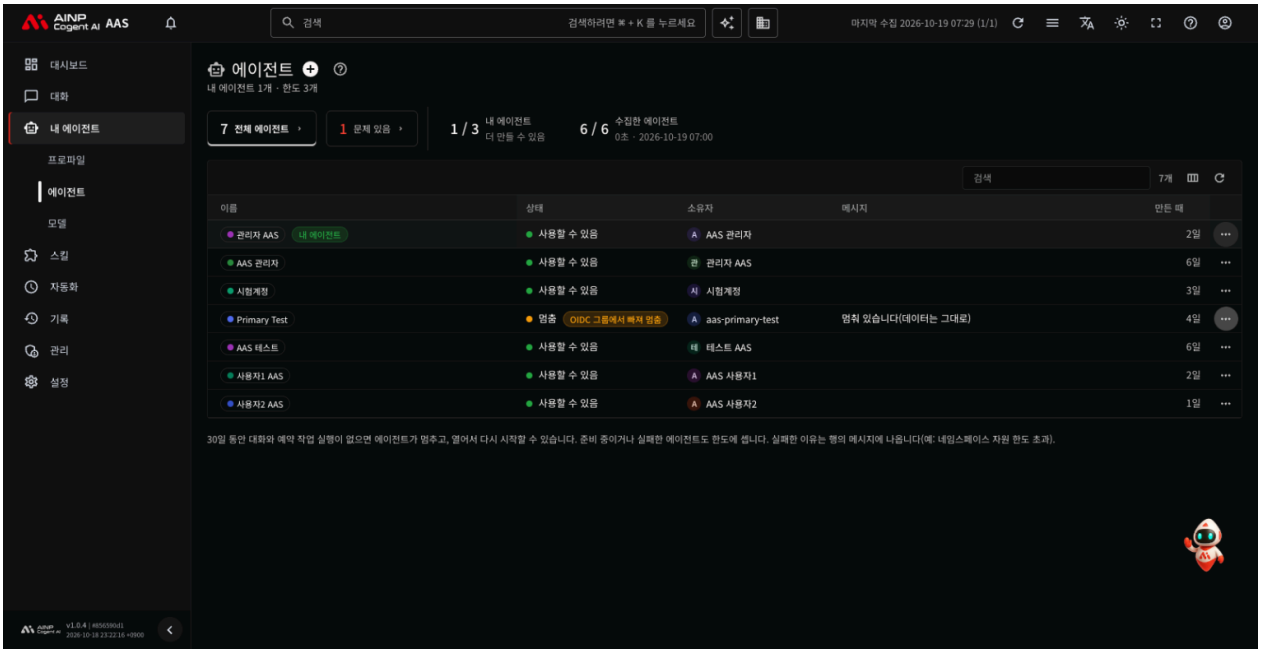


그림 4-3. 에이전트 목록. 제목 옆 「+」 버튼과 그 아래 「내 에이전트 1개 · 한도 3개」, 위쪽 칸의 「1 / 3 내 에이전트 · 더 만들 수 있음」을 보면 사람마다 정해진 한도 안에서 에이전트를 늘린다는 점이 드러납니다. 표 아래에는 30일 미사용 자동 멈춤과 한도 계산 규칙이 함께 적혀 있습니다

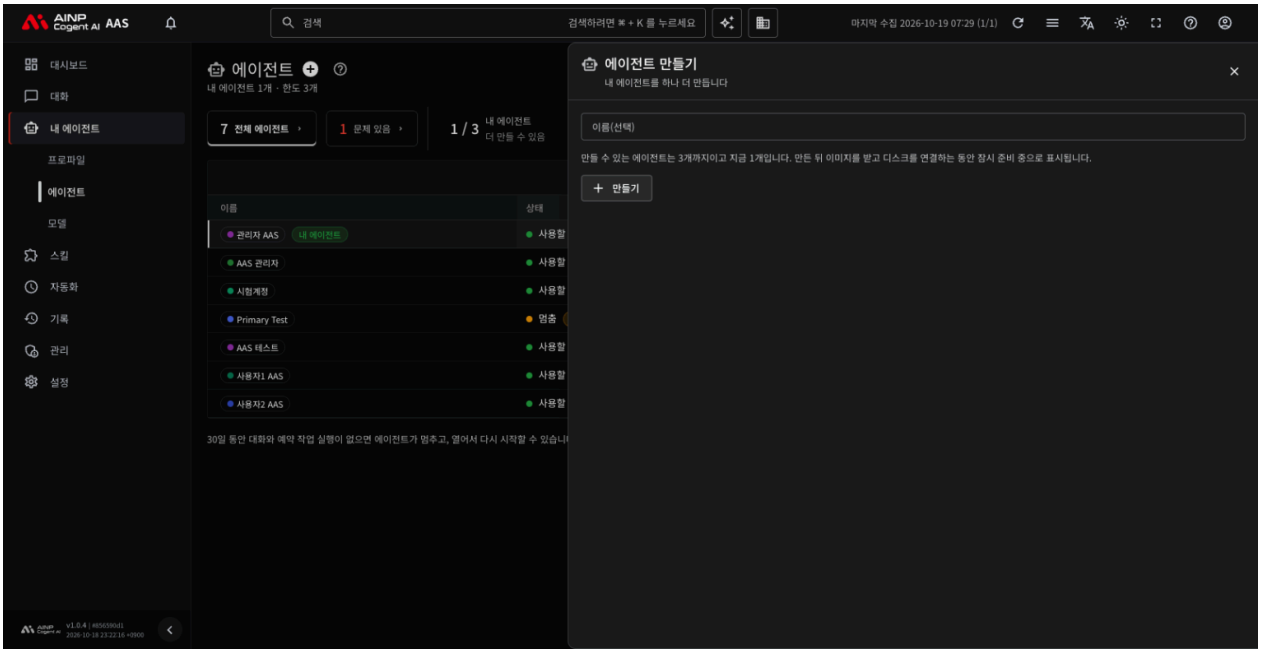


그림 4-4. 에이전트 만들기 창. 입력 칸은 「이름(선택)」 하나이고, 그 아래 「만들 수 있는 에이전트는 3개까지이고 지금 1개입니다」와 이미지를 받고 디스크를 연결하는 동안 준비 중으로 표시된다는 안내가 보입니다

에이전트를 누르면 오른쪽에 상세 서랍이 열립니다. 기본 정보에는 이름, ID, 소유자, 상태, 만든 때가 나오고, 서랍 위쪽 버튼으로 소유권을 이전하거나 에이전트를 지웁니다. 관리자에게는 같은 서랍에 「이 사람의 개수 한도」 칸이 더 보여, 사람마다 한도를 바꿔 저장합니다. 따라서 부서 담당자가 직접 에이전트를 추가하더라도 전체 수는 IT 관리자가 정한 범위를 넘지 않습니다. 담당자가 퇴사하거나 부서를 옮길 때는 에이전트를 지우지 않고 소

유권 이전으로 후임자에게 넘길 수 있고, OIDC 그룹에서 빠져 멈춘 에이전트도 데이터가 그대로 남아 있어 나중에 넘길 수 있습니다(4.4.2절, 8.4절).

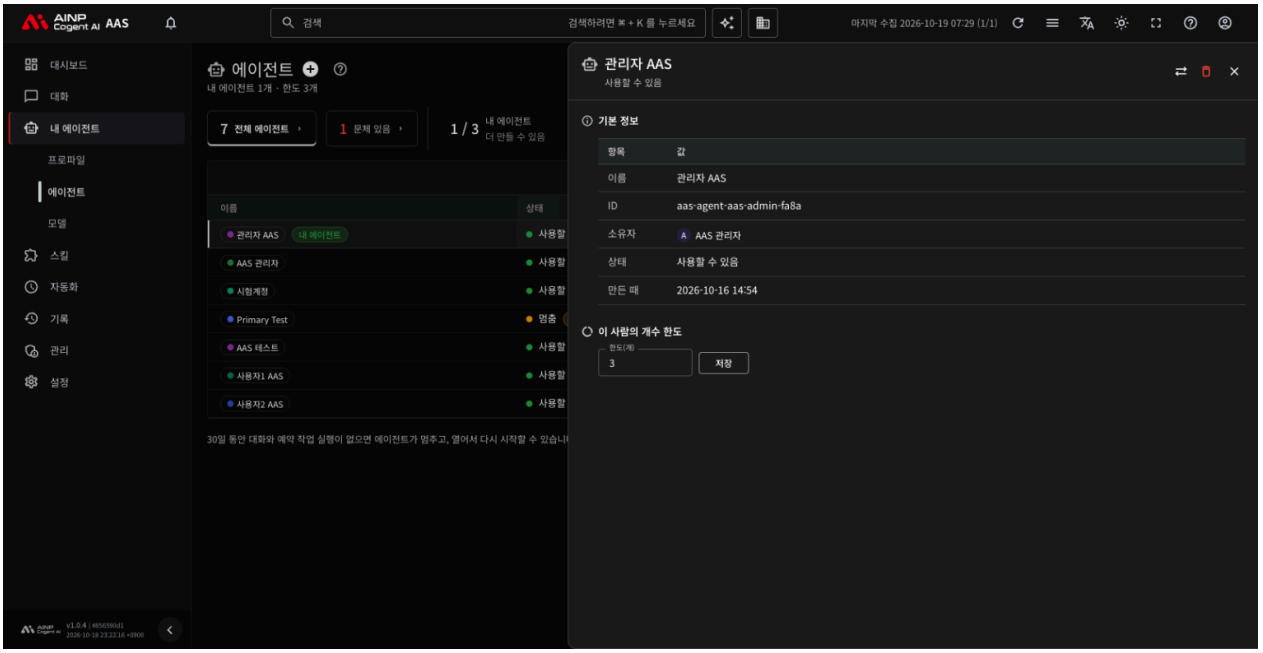


그림 4-5. 에이전트 상세 서랍. 기본 정보 표 아래 관리자용 「이 사람의 개수 한도」 칸과 저장 버튼이 있고, 서랍 오른쪽 위 두 버튼이 소유권 이전과 지우기입니다

프로파일 층 — 복제나 다른 에이전트에서 가져와 시작하는 새 프로파일

새 프로파일은 그림 4-2의 프로파일 화면 제목 옆 「+」 버튼에서 만듭니다. 이름은 영문 소문자·숫자·하이픈·밑줄로 정하고, 「어디서 시작할까요」에서 출발점을 고릅니다. 출발점은 두 가지입니다. 하나는 같은 에이전트의 기존 프로파일(예: main)을 복제하는 방법이고, 다른 하나는 「다른 에이전트에서 가져오기」로 다른 사람 에이전트의 main 성격·설정을 출발점으로 삼는 방법입니다. 복제할 때 「스킬은 가져오지 않기」를 고르면 성격과 설정만 넘겨받고 스킬은 새로 고릅니다. 마지막으로 소개를 적고 만들기를 누르면 새 프로파일이 생깁니다.

어느 출발점을 고르든 비밀값(.env)은 복사되지 않습니다. 메신저 봇 토큰이나 외부 시스템 계정처럼 사람마다 달라야 하는 자격증명이 원본 프로파일에서 그대로 따라오지 않으므로, 담당자는 새 프로파일에 자기 자격증명을 새로 넣습니다. 비밀값을 채워야 채널과 일부 스킬이 동작하고, 그 뒤 게이트웨이를 시작하면 새 프로파일이 채팅의 에이전트 목록에 나타납니다. 게이트웨이가 시작하지 못하면 화면이 실패 이유를 보여 주므로, 담당자는 설정 탭에서 원인을 고친 뒤 다시 시작합니다. 성격 문서의 첫 내용은 3.4.2절의 역할 템플릿을 출발점으로 삼아 채울 수 있습니다.

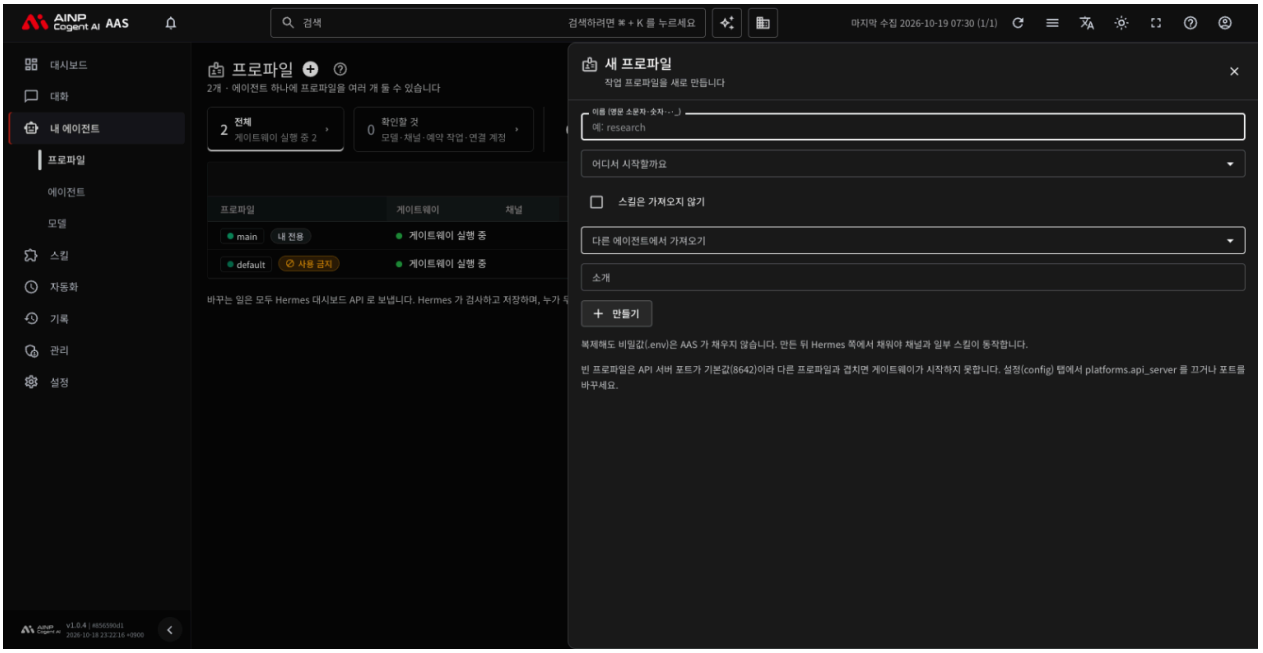


그림 4-6. 새 프로파일 창. 「어디서 시작할까요」에서 복제할 프로파일을, 「다른 에이전트에서 가져오기」에서 출발점이 될 다른 에이전트를 고르고, 「스킬은 가져오지 않기」로 스킬을 빼고 시작할 수 있습니다. 창 아래 「복제해도 비밀값(.env)은 AAS가 채우지 않습니다」 안내를 보면 자격증명이 따라 복사되지 않는다는 점을 알 수 있습니다. 왼쪽 프로파일 화면 제목 아래에는 「에이전트 하나에 프로파일을 여러 개 둘 수 있습니다」가 적혀 있습니다

프로파일 층 — 상세 화면의 내보내기·가져오기·이름 바꾸기·삭제와 모델 바꾸기

만든 뒤의 관리는 프로파일 상세 화면에서 합니다. 상세 화면에는 내보내기, PC에서 가져오기, 이름 바꾸기, 삭제가 모여 있고, 개요 탭에서 모델을 바꾸고 게이트웨이를 다시 시작합니다. 모든 작업은 Hermes Agent 대시보드의 공식 API로 보내고, 누가 언제 어느 프로파일을 만들고 바꾸고 지웠는지는 AAS의 변경 기록에 남습니다. 프로파일 층에서 하는 작업은 다음과 같습니다.

작업	하는 일	확인 장치	남는 기록
새 프로파일(복제)	같은 에이전트의 기존 프로파일을 출발점으로 새 이름의 프로파일을 만든다, 스킬 제외 선택 가능	이름 규칙, 비밀값(.env) 미복사	변경 기록(만든 사람·시각·새 이름)
새 프로파일(다른 에이전트에서 가져오기)	다른 에이전트의 main 성격·설정을 출발점으로 삼는다	이름 규칙, 비밀값(.env) 미복사	변경 기록(만든 사람·시각·새 이름)
내보내기·PC에서 가져오기	프로파일을 파일로 내보내 보관하거나, PC에 있는 파일로 프로파일을 들여온다	플랫폼이 값을 검사하고 저장	보관본 파일, 변경 기록
이름 바꾸기	프로파일 이름을 바꾼다	플랫폼이 값을 검사하고 저장	바꾼 이름, 변경 기록

작업	하는 일	확인 장치	남는 기록
삭제	보관본을 내보낸 뒤 프로파일을 지운다	한 번 더 묻기, 내보내기 성공, 프로파일 이름 다시 입력	내보낸 보관본, 삭제한 사람과 시각
모델 바꾸기·게이트웨이 재시작	모델 게이트웨이에 등록된 모델 가운데 주 모델을 고르고 게이트웨이를 다시 시작한다	업무를 멈출 수 있는 조작은 한 번 더 묻기	변경 기록

내보내기와 PC에서 가져오기는 프로파일을 설치본 밖으로 옮기는 통로입니다. 같은 AAS 안에서는 「다른 에이전트에서 가져오기」로 충분하지만, 다른 지사의 설치본이나 나중에 다시 쓸 보관본이 필요하면 프로파일을 파일로 내보내고 받는 쪽에서 PC에서 가져오기로 들여옵니다. 예를 들어 한 부서에서 자리 잡은 영업 보고 프로파일은 같은 AAS의 다른 부서 담당자가 가져오기로 출발점을 삼고, 다른 설치본을 쓰는 지사는 내보낸 파일로 받습니다(8.4절).

지우기 전에 보관본부터 남기는 삭제

프로파일 삭제는 되돌릴 수 없는 작업이라 AAS는 한 번 더 묻고, 먼저 프로파일을 내보내 보관본을 만든 뒤에만 지우기를 시작합니다. 담당자가 지울 프로파일의 이름을 다시 입력해야 삭제가 실행되므로, 비슷한 이름의 다른 프로파일을 잘못 지우는 일을 막습니다. 내보내기가 실패하면 AAS는 삭제를 멈추고 그 이유를 화면에 알립니다. 삭제는 에이전트 층의 자동 멈춤과도 다릅니다. OIDC 그룹에서 빠지거나 30일 동안 쓰지 않아 멈춘 에이전트는 데이터가 그대로 남아 다시 시작할 수 있지만, 삭제한 프로파일은 내보낸 보관본으로만 남습니다. 따라서 파일럿을 끝내거나 업무를 정리할 때는 멈춤으로 둘지, 소유권을 넘길지, 보관본을 남기고 지울지를 담당자와 관리자가 함께 정합니다.

4.1.3 스킬 문서의 판 관리와 AI 태그 분류로 찾는 스킬 58개

스킬 문서의 편집과 판 관리

스킬은 에이전트가 일하는 방법을 적은 문서이며, 업무 담당자가 가장 자주 고치게 되는 구성 요소입니다. 그래서 AAS의 편집기는 미리 보기, 임시 저장, 저장 메모, 저장 전 「바뀐 줄 확인」을 갖추고, 저장할 때마다 판(버전)을 남깁니다. 판 목록에서는 두 판을 비교하고 이름을 붙이거나 앞서 저장한 판으로 되돌릴 수 있습니다. 예를 들어 다른 사람이나 에이전트가 그사이 같은 문서를 고쳤다면 편집기는 저장을 막고 차이를 먼저 보여 줍니다. 같은 편집기가 성격 문서와 정기 업무 지시문에도 쓰이므로, 업무 담당자는 문서 종류마다 다른 도구를 익힐 필요가 없습니다.

에이전트가 직접 고친 스킬을 검토하는 규칙

스킬은 사람만 쓰는 문서가 아닙니다. Hermes Agent에서는 에이전트가 작업 도중에 스스로 스킬을 쓰기도 하고, 턴이 끝난 뒤 백그라운드에서 도는 자기개선 검토가 스킬을 만들거나 고치기도 합니다. 이 구조는 문서화 부담을 줄여 주지만, 사람이 보지 않는 동안 잘못된 절차도 함께 문서로 굳을 수 있다는 뜻이기도 합니다. 한 번 어긋난 절차가 스킬로 남으면 다음 실행부터 그 절차가 기본값처럼 쓰이고, 결과물은 그럴듯하게 다듬어져 나오므로 담당자가 이상을 알아채기까지 시간이 걸립니다. 그래서 에이전트가 만들거나 고친 스킬을 정기 검토 대상에 넣는 규칙은 도입하는 조직이 직접 정해야 하며, 검토자는 스킬 목록에서 바뀐 스킬을 열어 내용을 확인하고 편

집기의 판 비교로 앞선 내용과 대조합니다. 에이전트 플랫폼의 기능을 이런 검토 관점에서 하나씩 대조한 자료는 [R1]에 정리되어 있습니다.

AI 태그로 나뉘는 스킬 목록

스킬 목록은 스킬마다 위치, 출처, 태그, 설명과 함께 그 스킬을 거는 정기 업무 수, 스크립트 수, MCP 호출 수, 외부 URL 호출 수를 보여 줍니다. 태그는 AI가 스킬 설명을 읽어 붙이며, 「AI 태그 다시 분류」 버튼으로 언제든 다시 나눌 수 있습니다. 그림 4-7의 배포본 화면은 Hermes Agent에 기본으로 들어 있는 스킬 58개를 다음 분류로 나눠 보여 줍니다. 한 스킬에 태그가 둘 이상 붙을 수 있어 분류별 수의 합은 58보다 큽니다.

- 자동화·도구 28개, 개발 절차 12개
- 문서·글쓰기 11개, 지식·데이터 10개
- 코드 품질 9개, 이미지 생성 6개, 디자인 5개
- 에이전트 활용·테스트 각 2개, API·구조와 학습·안내 각 1개

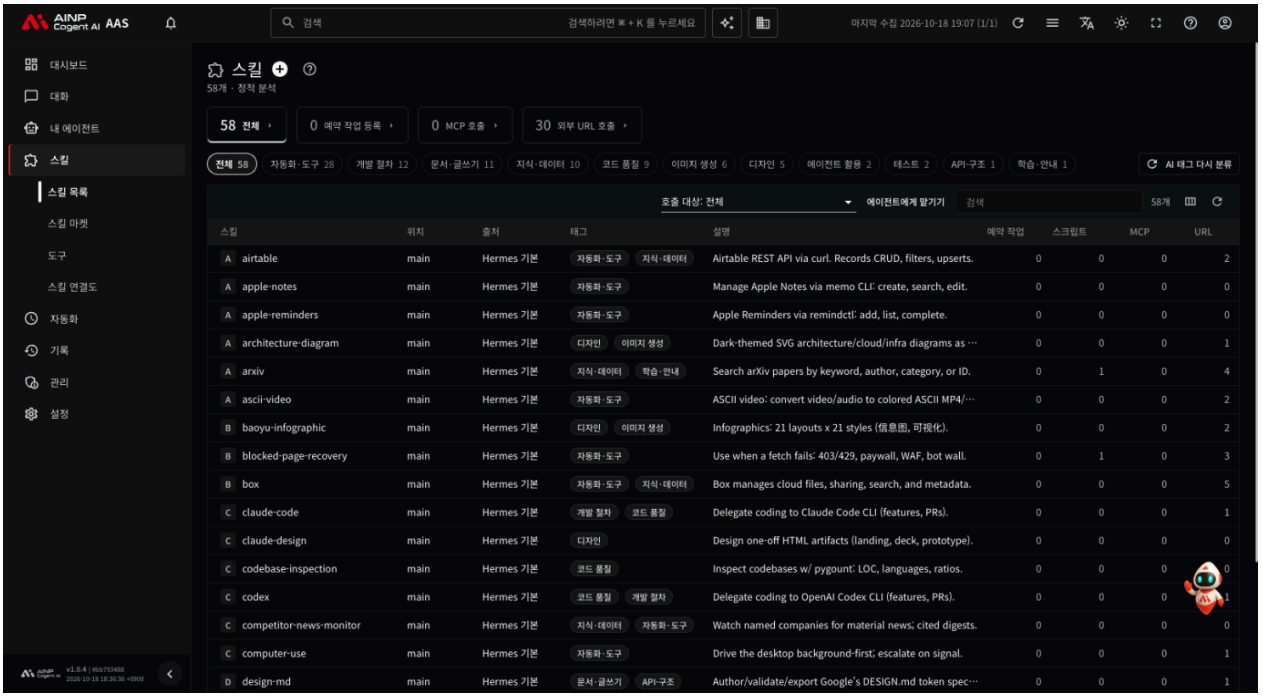


그림 4-7. 스킬 목록과 AI 태그 분류. 위쪽 칸의 「외부 URL 호출 30」과 오른쪽 「AI 태그 다시 분류」 버튼, 표의 정기 업무·스크립트·MCP·URL 열을 보면 스킬마다 무엇을 부르는지가 목록 단계에서 드러납니다

명함 인식이나 회의록 정리 같은 업무 스킬을 추가해도 같은 분류 체계에 들어가므로, 스킬이 수백 개로 늘어난 뒤에도 업무 담당자는 태그와 「호출 대상」 거르기로 필요한 스킬을 찾습니다. 「호출 대상」 거르기는 특정 MCP 서버나 외부 호스트를 부르는 스킬만 추리는 기능입니다. 어떤 외부 시스템의 계정을 바꾸기 전에 영향을 받는 스킬을 먼저 찾아낼 수 있습니다.

스크립트형 스킬의 편집 범위

모든 스킬을 콘솔에서 고칠 수 있지는 않습니다. 스킬 문서는 편집기로 고치지만, 스킬이 부르는 파이썬 같은 스크립트 파일은 콘솔에서 읽기만 됩니다. 플랫폼에 스크립트를 저장하는 공식 API가 없고, AAS는 플랫폼의 파일

을 직접 쓰지 않는다는 원칙을 지키기 때문입니다. 즉 문서만으로 완결되는 스킬은 업무 담당자가 직접 만들고 고치지만, 스크립트가 필요한 스킬은 지금도 개발 인력의 손을 거쳐야 합니다(9.3절의 한계 항목).

4.2 진행 단계와 실행 승인 카드가 보이는 팀 채팅, 여러 에이전트가 함께 답하는 회의 탭

AAS의 시키기 묶음은 팀 채팅과 오피스 회의 탭 두 화면으로 이뤄지며, 1.2절에서 짚은 채팅 프로그램의 구조적 한계에 하나씩 대응합니다. 채팅 프로그램은 사람끼리의 대화를 위해 만들어져, 에이전트가 지금 어느 단계에 있는지와 무엇을 실행하려는지를 보여 줄 수단이 없습니다. 에이전트를 하나 늘릴 때마다 봇 등록과 토큰 복사를 되풀이해야 합니다. 1장에서 본 시험 39%와 확대 23%의 차이[S4]를 좁히려면, 시험에서 일상 업무로 넘어가려는 조직은 일을 맡기고 결과를 확인하는 창구부터 업무용으로 갖춰야 합니다. 1.2절의 문제와 AAS 화면의 대응은 다음과 같습니다.

채팅 프로그램의 문제(1.2절)	AAS 화면의 대응
진행 단계와 실행하려는 명령이 보이지 않음	진행 단계(상태·도구·추론)를 접어서 표시
실행 승인과 되묻기가 메시지 한 줄로 흘러감	승인 카드, 질문별 되묻기 카드로 분리
봇 등록과 토큰 복사가 에이전트마다 반복됨	콘솔 로그인만으로 에이전트 목록에서 바로 대화
대화와 모델·스킬·정기 업무 설정이 끊겨 있음	정기 업무·스킬 화면에서 질문을 채워 채팅으로 이동

4.2.1 승인 카드와 되묻기 카드로 기록이 남는 업무 지시

에이전트 목록에서 바로 열리는 대화

팀 채팅 화면의 왼쪽에는 업무 담당자가 쓸 수 있는 에이전트가 이름, 소개, 마지막 활동, 게이트웨이 상태와 함께 놓이고, 하나를 누르면 곧바로 대화가 열립니다. 따라서 에이전트를 추가해도 메신저에 봇을 등록하거나 토큰을 복사하는 작업이 따로 필요하지 않습니다. 지난 대화 목록에는 콘솔에서 시작한 대화뿐 아니라 메신저, 명령줄, 정기 업무에서 시작된 세션도 함께 들어 있어, 다른 경로로 시작한 일을 콘솔에서 이어서 지시할 수 있습니다. 정기 업무 화면의 「대화로 조사」나 스킬 화면의 「고치기 요청」을 누르면 질문이 미리 채워진 채 채팅으로 넘어오는데, 자동으로 보내지는 않으므로 사람이 내용을 확인한 뒤 보냅니다.

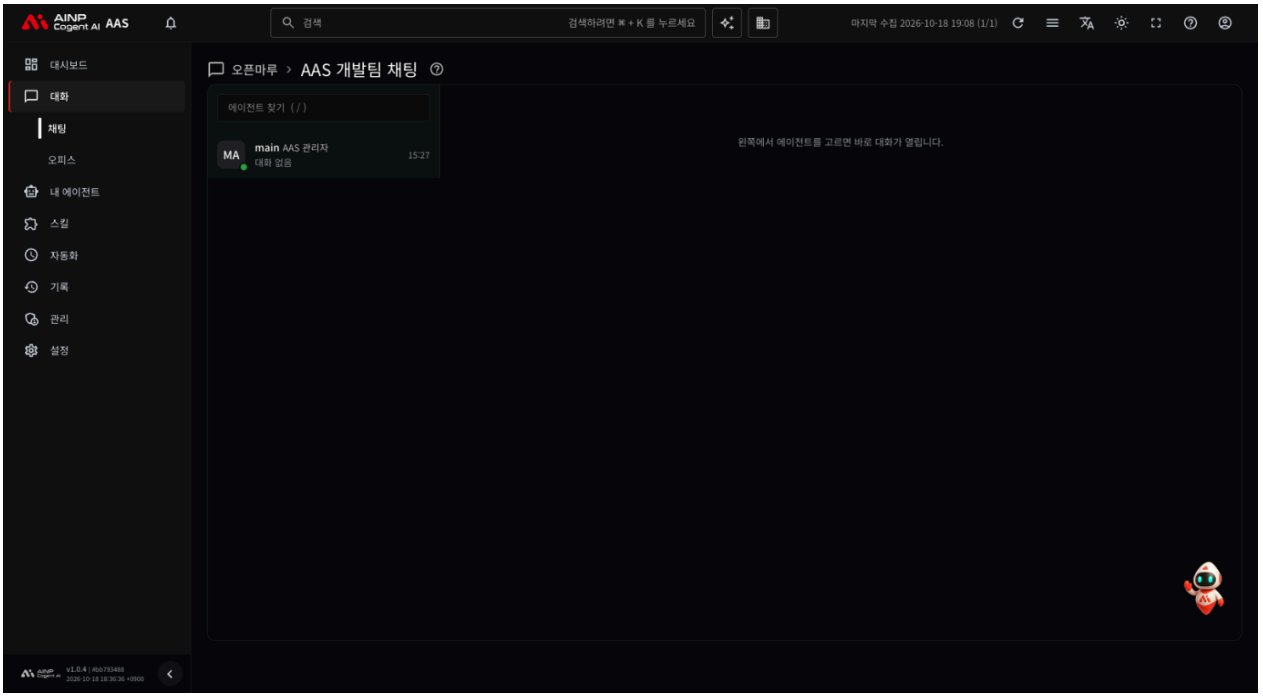


그림 4-8. 팀 채팅. 왼쪽 「에이전트 찾기」 아래 목록에서 에이전트를 고르면 오른쪽에 바로 대화가 열립니다. 에이전트마다 봇을 등록하고 토큰을 복사하던 채팅 프로그램의 설정 부담(1.2.2)을 콘솔 로그인 하나로 대신합니다

대화 안에 남는 카드 네 종류

대화가 시작되면 에이전트의 동작은 메시지 한 줄이 아니라 성격이 다른 카드로 나뉘어 표시됩니다. 카드마다 담는 내용과 업무상 쓰임은 다음과 같습니다.

카드	담는 내용	업무상 쓰임
진행 단계	상태, 부른 도구, 추론 과정(접힌 상태로 표시)	에이전트가 지금 무엇을 하는지 확인
승인 카드	실행하려는 명령	명령 실행 전 사람의 승인
되묻기 카드	에이전트가 사람에게 묻는 질문(질문마다 한 장)	빠진 조건을 채워 지시를 완성
지난 대화	이전 세션 전체(다른 경로에서 시작한 것 포함)	일을 이어서 지시

승인 카드는 1.2.1절에서 짚은 「메시지 한 줄로 흘러가는 실행 승인」에 대한 직접 대응입니다. 명령 실행 요청이 대화 흐름과 분리된 카드로 나타나므로 사람이 어떤 명령을 허락했는지가 대화 기록 안에 남습니다. 앞서 본 대로 허가되지 않은 에이전트 행위의 대부분이 내부 정책 위반에서 나온다는 전망을 고려하면[S3], 명령마다 사람의 승인이 기록되는 구조는 감사 추적의 출발점이 됩니다. 다만 에이전트가 먼저 말을 거는 알림은 지금도 메신저로 받으며, 콘솔 채팅이 메신저를 완전히 대체하지는 않습니다.

4.2.2 여러 설치본의 에이전트가 한 회의방에서 답하고 칸반으로 이어지는 흐름

회의 탭에서 여러 에이전트에게 보내는 메시지

업무별 에이전트가 늘어나면 하나의 안건에 여러 에이전트의 답이 필요한 경우도 늘어납니다. 오피스 화면은 오피스·칸반·회의·배치·TFT 방 다섯 탭으로 구성되며, 회의 탭은 한 메시지를 여러 에이전트에게 동시에 보내는 기능입니다. 업무 담당자가 회의방을 고르고 메시지를 올리면 「받는 에이전트」로 지정된 에이전트가 각자 답하고, 답은 같은 방에 차례로 쌓입니다. 받는 에이전트는 같은 설치본에 있을 필요가 없어, 서로 다른 Hermes Agent 설치본에서 실행되는 에이전트들이 한 회의방에 참여합니다. 예를 들어 그림 4-9의 회의방에는 받는 에이전트 3개가 지정되어 있고, 메시지에는 한 번에 10개, 25MB까지 파일을 붙일 수 있으며, 오른쪽 위 「자료」 폴더에서 회의 자료를 함께 봅니다.

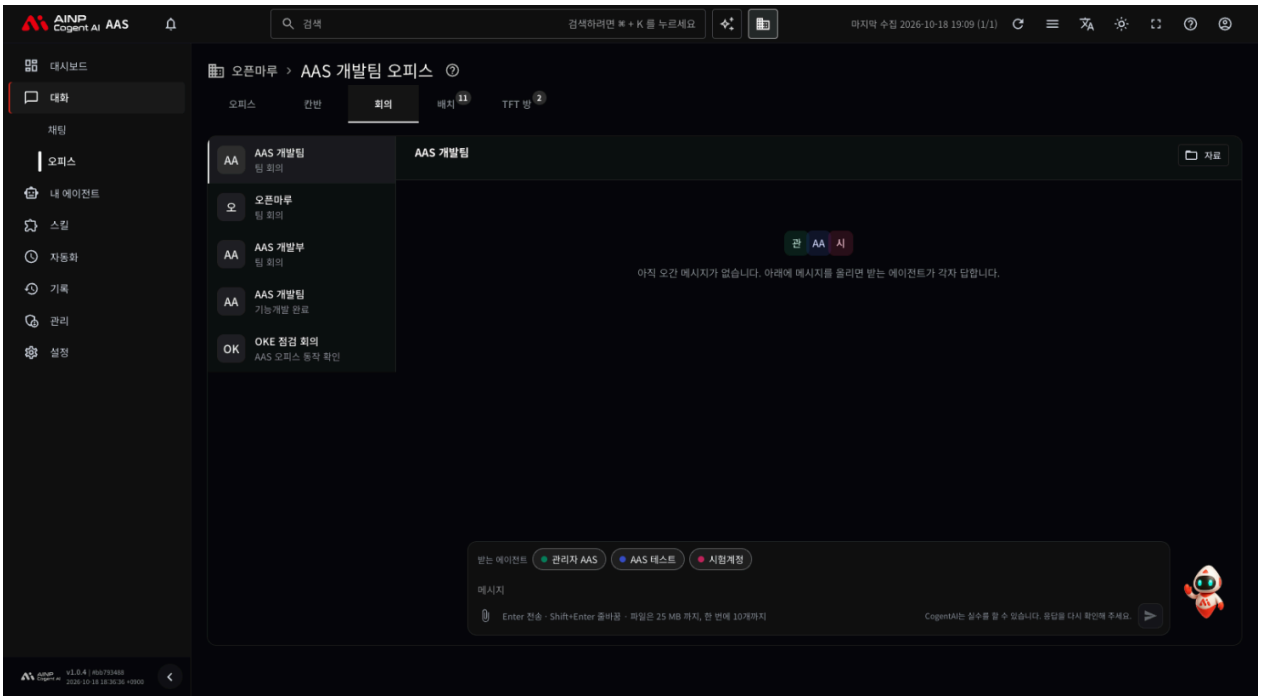


그림 4-9. 오피스 회의 탭. 아래 입력 칸의 「받는 에이전트」 세 개와 위쪽 탭 줄(오피스·칸반·회의·배치·TFT 방)을 보면, 한 메시지에 여러 에이전트가 각자 답하는 구조가 드러납니다. 채팅 프로그램에서는 에이전트마다 따로 대화방을 열어야 했던 일을 한 방에서 처리합니다

회의 결과가 칸반 카드로 이어지는 경로

회의에서 나온 할 일은 칸반 탭의 카드로 이어집니다. 카드는 담당 에이전트가 속한 설치본에 만들어지고, 칸반 화면은 여러 설치본의 카드를 한 보드로 합쳐 보여 줍니다. 반면 담당 에이전트가 정해지지 않은 카드는 분류 대기 열에 따로 모여 사람이 담당을 정하게 됩니다. 이 기능 역시 Hermes Agent의 플러그인·설정·버전을 바꾸지 않고, AAS가 설치본 사이에서 메시지와 카드를 중계하는 방식으로 동작합니다. 아직 한 설치본의 카드를 다른 설치본의 에이전트에게 넘기는 기능은 없으므로, 담당을 바꿀 때는 새 카드를 만들어야 합니다.

에이전트끼리 주고받는 메시지가 늘어날 때의 점검

회의방에서 여러 에이전트가 같은 메시지를 받고 답하는 구조는 담당자가 지시를 한 번만 쓰게 해 주지만, 운영 관점에서는 점검할 대상도 하나 늘립니다. 에이전트가 하나일 때는 사람의 지시와 에이전트의 응답만 보면 되지만, 여러 에이전트가 한 방의 메시지를 읽고 그 답에서 할 일이 생기면 메시지 자체가 다음 실행의 입력이 됩니다. 조직 밖의 도구 서버나 협력사 에이전트와 메시지를 주고받기 시작하면, 메시지가 중간에 바뀌거나 보낸 쪽

을 속이는 경우까지 고려해야 합니다. 따라서 파일럿 단계에서는 회의방에 넣는 에이전트를 조직 안 설치본으로 한정하고, 외부 에이전트나 외부 도구 서버와 잇는 일은 별도 보안 검토 대상으로 떼어 두는 편이 안전합니다. 나중에 외부 연결을 열 때는 메시지를 보낸 쪽을 확인하는 방법과 중간에 바뀐 메시지를 가려내는 방법이 무엇인지를 그 검토에서 먼저 정합니다.

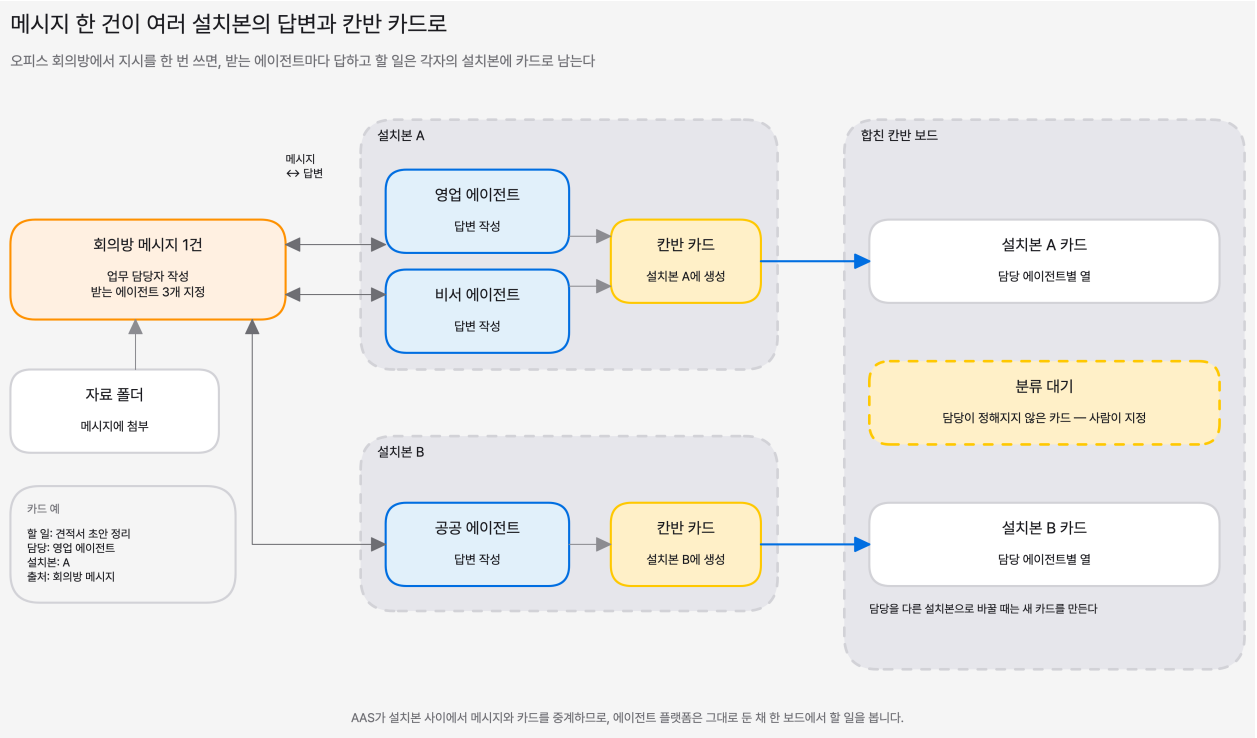


그림 4-10. 회의방 메시지 한 건이 여러 설치본의 에이전트 답변과 칸반 카드로 이어지는 흐름

4.3 실패 작업과 만료 임박 자격증명을 첫 화면에 모은 「오늘 볼 것」

AAS의 지켜보기 묶음은 첫 화면인 「오늘 볼 것」과 하루 두 번 보내는 정기 업무 요약으로 시작합니다. 사람이 보지 않는 동안 정기 업무로 실행되는 에이전트가 늘면, 실패와 만료 같은 손볼 항목이 여러 화면에 흩어져 어디부터 봐야 할지 알기 어려워집니다. 2장에서 본 감독용 에이전트 전망[S3]처럼, 에이전트를 지켜보는 기능은 별도 시장이 생길 만큼 운영의 기본 요건이 되고 있습니다. 「오늘 볼 것」은 새 정보를 만들지 않고, 다른 화면이 이미 아는 것 가운데 지금 사람이 손대야 하는 항목만 모읍니다. 이 절의 업무 화면은 하나의 운영 설치본에서 찍은 화면 예시이므로, 화면 속 연결 시스템(CRM·위키·드라이브 등)은 고객 환경에 맞춰 따로 설정합니다.

4.3.1 실패 작업과 답을 기다리는 대화를 한곳에 모으는 첫 화면의 항목

첫 화면 위쪽의 네 지표

「오늘 볼 것」의 위쪽 네 칸은 게이트웨이가 실행 중인 프로파일 수, 활성 정기 업무 수, 실패했거나 멈춘 작업 수, 만료됐거나 곧 만료되는 자격증명 수입니다. 그림 4-11의 화면은 프로파일 12개 가운데 9개의 게이트웨이가 실행 중이고, 정기 업무 95개 가운데 76개가 활성 상태이며, 실패한 작업 1개와 만료(임박) 자격증명 7개가 있음을 보여 줍니다. 게이트웨이가 꺼진 프로파일의 정기 업무는 실패로 기록되지 않고 아예 실행되지 않기 때문에, 첫 칸의 「9/12」가 실패 건수만큼 중요한 신호가 됩니다. 따라서 관리자는 실패 목록을 보기 전에 실행 자체가 멈춘 에이전트가 있는지부터 확인할 수 있습니다.

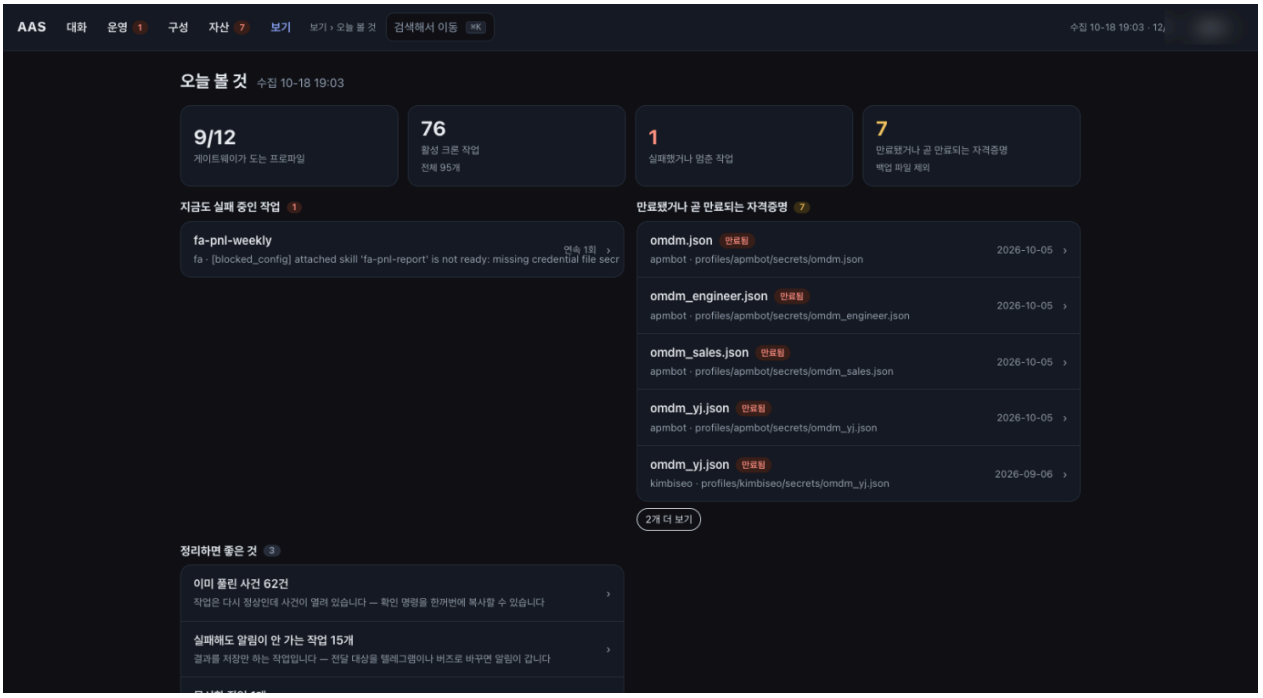


그림 4-11. 「오늘 볼 것」 화면 예시. 위쪽 네 칸 아래 「지금도 실패 중인 작업」에는 오류 문구가 함께 보이고, 오른쪽 「만료됐거나 곧 만료되는 자격증명」에는 값 없이 파일 이름·위치·만료일만 보입니다. 아래 「정리하면 좋은 것」에는 이미 풀린 사건 62건과 실패해도 알림이 안 가는 작업 15개가 모여 있습니다. 연결 시스템(CRM·위키·드라이브 등)은 고객 환경에 맞춰 설정합니다

첫 화면에 올라오는 묶음과 선정 기준

네 지표 아래에는 다음 묶음이 이어지며, 선정 기준은 「지금 사람이 결정하거나 손대야 하는 항목인가」 하나입니다.

- 답을 기다리는 대화 — 에이전트가 승인이나 되묻기에 대한 답을 기다리는 대화
- 지금도 실패 중인 작업 — 마지막 실행이 실패했고 아직 회복되지 않은 정기 업무
- 문제 있는 프로파일 — 게이트웨이 중단, 모델 설정 오류 등
- 만료됐거나 곧 만료되는 자격증명 — 이름·위치·만료일만 표시
- 정리하면 좋은 것 — 이미 풀린 사건, 알림이 안 가는 작업, 무시한 작업
- 최근에 바꾼 것 — 변경 기록의 최근 항목

줄을 누르면 해당 화면이나 상세 서랍으로 바로 이동하고, 어느 화면에서든 ⌘K로 에이전트·스킬·작업·자격증명을 이름으로 찾아갈 수 있습니다. 예를 들어 이미 회복된 사건은 「정리하면 좋은 것」으로 따로 분리되므로, 지금도 실패 중인 작업 1건이 회복된 사건 62건에 묻히지 않습니다. 각 항목의 원인을 가려내는 상세 화면(Cron 헬스체크, 자격증명, 흐름)은 6장의 관측 화면이 맡습니다.

4.3.2 하루 두 번 정기 업무 요약으로 받는 실패 알림

알림이 안 가는 작업을 메우는 요약

Hermes Agent에서 정기 업무의 실패 알림은 그 작업에 지정된 전달 대상으로만 갑니다. 결과를 저장만 하도록 설정한 작업은 실패해도 아무에게도 알리지 않으며, 그림 4-11의 화면 예시에서는 이런 작업이 15개로 집계

됩니다. AAS는 이 공백을 메우려고 매일 08시 30분과 18시 30분 두 차례 정기 업무 요약을 메신저 봇으로 직접 보냅니다. 요약은 플랫폼의 알림 경로를 거치지 않고, 새로 생긴 실패가 없어도 0건이라는 사실을 담아 보냅니다. 요약이 오지 않는 날은 그 자체로 수집이나 발송에 문제가 생겼다는 신호가 됩니다.

요약 알림에 담기는 항목

요약 한 건에는 수집 시각, 수집에 성공한 프로파일 수, 열린 사건의 신규·지금도 실패·이미 풀림 구분, 실패·멈춤·알림 없음·무시 작업 수가 들어갑니다. 그림 4-11과 같은 상태라면 요약은 다음과 같은 형태가 됩니다.

> *정기 업무 요약 08:30 — 수집 성공 프로파일 12/12 · 신규 실패 0 · 지금도 실패 1 · 이미 풀림 62 · 멈춤 0 · 알림 없음 15*

메신저 봇의 자격증명이 설정되지 않은 환경에서는 같은 내용이 파일로만 남습니다. 알림이 안 가는 작업 15개 각각을 그대로 둘지, 전달 대상을 붙일지는 사람이 정기 업무 서랍에서 결정합니다. 화면과 요약은 상태를 드러낼 뿐이고, 원인을 찾아 고치는 것은 담당자입니다. 어떤 작업이 왜 실패했는지를 오류 문자열로 묶어 보는 화면은 6.2절에 있습니다.

4.4 사내 스킬 마켓 패키지 51개와 OIDC 연동 사용자별 에이전트 한도

AAS의 나누기 묶음은 사내 스킬 마켓과 사용자·에이전트 관리로 이뤄지며, AAS를 개인 도구에서 조직 단위로 나누고 통제하는 콘솔로 만듭니다. 특정 업무를 맡는 에이전트가 기업용 애플리케이션 곳곳에 들어오면 한 조직 안에서 만들어지는 에이전트와 스킬의 수도 함께 늘어납니다[S1]. 이때 한 부서에서 만든 스킬을 다른 부서가 쓰려면 폴더를 손으로 복사해야 하고, 누가 어떤 에이전트를 얼마나 갖고 있는지 알 수 없다면 IT 관리자는 확산을 허용하기 어렵습니다. 따라서 AAS는 배포 경로를 마켓 하나로 모으고, 에이전트 소유를 조직의 계정 체계에 묶습니다. 두 기능의 통제 항목은 다음과 같습니다.

영역	통제 항목	동작
스킬 마켓	패키지 원본	사내 저장소(GitLab)에 두고, 배포는 마켓 서버(SkillHub)가 맡음
스킬 마켓	설치 범위	스킬 패키지는 기존 프로파일에만, 에이전트 패키지는 새 프로파일로 설치
스킬 마켓	설치 기록	어느 패키지를 어느 프로파일에 설치했는지, 실패한 요청까지 기록
사용자 관리	로그인	OIDC 표준 로그인, 그룹 연동
사용자 관리	한도	사용자별 에이전트 기본 3개, 관리자가 사람마다 조정
사용자 관리	자원 회수	그룹에서 빠지면 멈춤, 30일 미사용 시 자동 멈춤

4.4.1 사내 등록과 외부 가져옴으로 구성되는 스킬 패키지 배포

사내 등록 2개와 외부 가져옴 49개

스킬 마켓은 스킬이나 에이전트를 패키지로 받아 프로파일에 설치하는 화면입니다. 그림 4-12의 배포본 화면에는 패키지 51개가 있고, 그중 2개는 사내에서 등록한 것이며 49개는 외부 공개 저장소에서 가져온 것입니다. 패키지마다 출처, 태그, 설명, 버전, 설치된 곳이 보이고, 위쪽 태그 칸(개발 절차 19개, 에이전트 활용 13개, 디자인 12개 등)으로 범위를 좁혀 찾습니다. 위쪽 칸의 「올리기 요청 2」처럼 부서가 만든 스킬을 마켓에 올려 달라는 요청도 같은 화면에서 관리합니다. 한 부서가 문서로 정리한 업무 방법이 패키지가 되어 다른 부서의 에이전트에 설치되는 경로가 하나로 정해집니다.

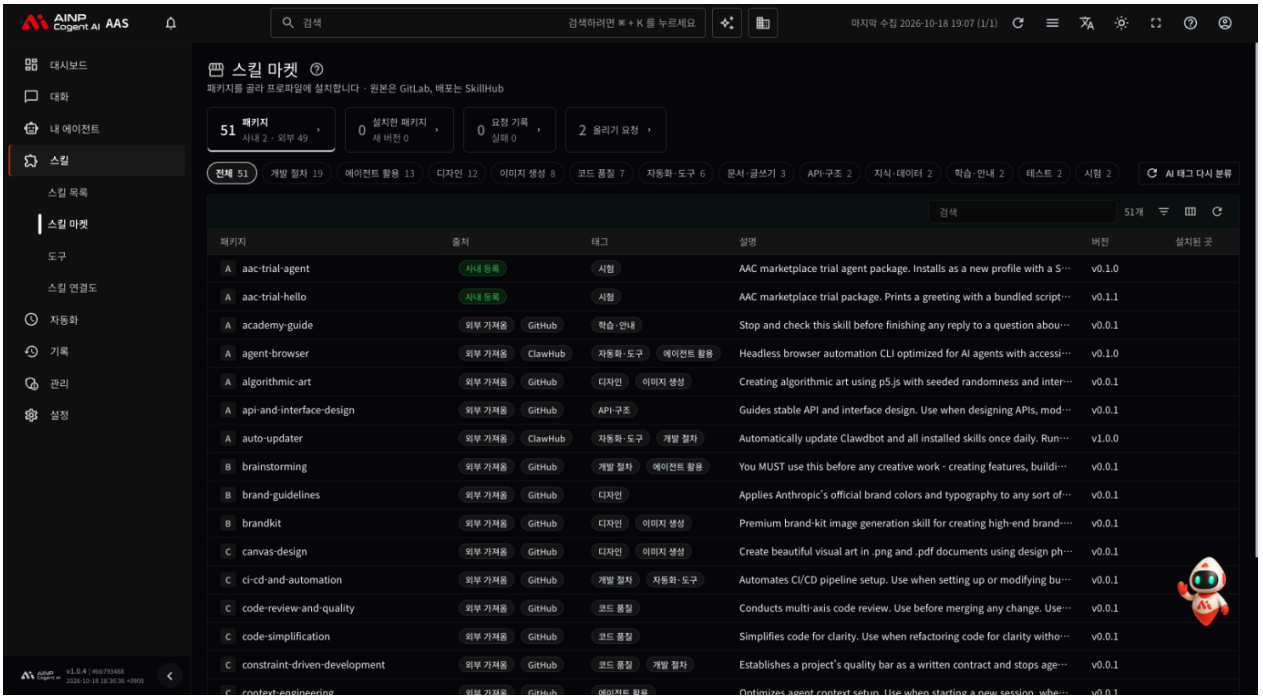


그림 4-12. 스킬 마켓. 위쪽 칸의 「패키지 51 · 사내 2 · 외부 49」와 화면 제목 아래 「원본은 GitLab, 배포는 SkillHub」 문구, 출처 열의 「사내 등록」·「외부 가져옴」 표시를 보면 원본 보관과 배포가 분리되어 있음을 알 수 있습니다

패키지 설치 요청에서 설치 기록까지의 흐름

패키지 설치는 다음 순서로 진행됩니다.

1. 업무 담당자가 패키지와 설치할 프로파일을 고르면 AAS가 설치 요청을 남깁니다.
2. 호스트의 설치 도우미가 마켓 서버에서 패키지를 받아 파일마다 해시를 대조합니다.
3. 도우미가 Hermes Agent 자신의 설치 명령으로 패키지를 프로파일에 넣습니다.
4. 결과가 「설치한 패키지」와 「요청 기록」 탭에 남습니다.

이 흐름은 AAS가 플랫폼 공식 API로만 바꾼다는 원칙의 예외입니다. 플랫폼 API에 패키지 설치·삭제 경로가 없어서 플랫폼 자신의 명령을 쓰며, 그 대신 범위를 좁혀 둡니다. 예를 들어 지우기는 AAS가 설치했다고 기록한 폴더 하나에만 적용되고, 공용 프로파일에는 설치하지 않습니다. 이 예외는 숨기지 않고 화면과 제품 문서에 범위를 밝혀 둡니다(7장 설계 원칙).

4.4.2 OIDC 그룹 연동과 30일 미사용 자동 멈춤으로 관리하는 사용자별 에이전트

OIDC 그룹에 묶이는 사용자별 에이전트

AAS는 사내 OIDC 계정 체계로 로그인하고, 사용자마다 볼 수 있는 에이전트를 정합니다. 2장에서 본 것처럼 기밀 등급 업무는 국가 망 보안체계 아래에서도 분리된 망에 남으므로[S5][S6], 조직 안(온프레미스)에 AAS를 설치하는 조직은 계정도 외부 서비스가 아닌 사내 OIDC 계정 체계에 연결합니다. 4.1.2절 그림 4-3의 에이전트 화면은 전체 에이전트 7개와 소유자를 보여 주며, 사용자 한 명이 만들 수 있는 에이전트는 기본 3개(「내 에이전트 1 / 3」)이고 관리자가 사람마다 한도를 바꿉니다(그림 4-5). 사용자·권한 화면에서는 사용자 19명, 관리자 2명, 부서 2개, OIDC 계정이 아직 없는 사용자 12명이 각각 집계됩니다. 그림 4-3의 표에서 한 행에 붙은 주황색 「OIDC 그룹에서 빠져 멈춤」 표시와 「멈춰 있습니다(데이터는 그대로)」 메시지, 표 아래 30일 미사용 자동 멈춤 안내를 보면 자원 회수 규칙이 화면에 그대로 드러납니다.

계정 체계 연동과 자원 회수 규칙

사용자별 에이전트에는 다음 규칙이 적용됩니다.

규칙	동작
사용자별 한도	한 사람이 만들 수 있는 에이전트 기본 3개(관리자가 사람마다 조정), 준비 중이거나 실패한 에이전트도 한도에 셈
그룹 이탈	OIDC 그룹에서 빠지면 에이전트가 멈추고 데이터는 보존
미사용 회수	30일 동안 대화와 정기 업무 실행이 없으면 자동으로 멈춤
다시 시작	멈춘 에이전트는 행 메뉴에서 다시 시작
소유권 이전	에이전트 상세에서 다른 사용자에게 넘김
실패 이유	행의 메시지에 표시(예: 쿠버네티스 네임스페이스의 자원 한도 초과)

이 규칙은 IT 관리자가 에이전트를 사람 단위로 관리하게 해 줍니다. 예를 들어 퇴사나 부서 이동으로 그룹에서 빠진 사람의 에이전트는 자동으로 멈추고 데이터는 남기 때문에, 관리자는 나중에 에이전트 상세의 소유권 이전으로 후임자에게 넘길지를 결정할 수 있습니다. 에이전트형 AI를 시험 중인 조직이 39%에 이르는 만큼[S4], 시험 삼아 만든 뒤 잊힌 에이전트도 생기기 쉽습니다. 30일 미사용 자동 멈춤은 이런 에이전트가 자원을 계속 차지하는 일을 막습니다. 다만 그룹·부서 단위로 세밀하게 권한을 나누는 기능과 부서별 비용 할당은 아직 충분하지 않아, 당분간은 운영 규칙으로 보완해야 합니다(9.3절). 5장은 이 화면 위에서 실제로 실행되는 업무 에이전트를 카테고리별로 살펴봅니다.

5장: 명함 인식에서 화자 구분 회의록까지 10개 카테고리 업무 에이전트 카탈로그

AAS의 업무 에이전트 카탈로그는 4장에서 본 콘솔 위에서 실행되는 업무 유즈케이스를 문서·OCR부터 개인 비서까지 10개 카테고리로 나눈 목록입니다. 현재 AAS가 연결하는 에이전트 플랫폼은 오픈소스 Hermes Agent 1종이며, 카탈로그의 유즈케이스는 모두 이 플랫폼의 스킬과 정기 업무로 구현되어 있습니다. 각 유즈케이스는 무엇이 업무를 시작시키는지(트리거), 어느 시스템을 읽고 쓰는지(연결 시스템), 쓰기 전에 사람이 무엇을 확인하는지(사람 확인) 세 칸으로 설명합니다. 따라서 10개 카테고리를 같은 틀로 나란히 놓으면 부서마다 어떤 업무를 에이전트에 먼저 맡길지 같은 기준으로 비교할 수 있습니다.

1장에서 본 것처럼 에이전트의 확대 적용은 업무 기능 하나 단위로 보면 아직 어느 기능에서도 10%를 넘지 않습니다[S4]. 에이전트의 쓰임은 업무 기능 하나 단위로 정해야 하며, 그 판단에는 부서 업무와 바로 맞대어 볼 수 있는 구체적인 유즈케이스 목록이 필요합니다.

이 카탈로그는 명함 인식, 공공문서와 공공서식 인식, 화자 구분 회의록과 지시사항 세 가지를 대표 사례로 자세히 설명하고, 나머지 일곱 카테고리는 정기 업무를 중심으로 묶어 설명합니다. 각 절의 마지막 문단에는 반복량, 사람 확인 단계 수, 연결 시스템 수로 본 파일럿 후보 특성이 정리되어 있습니다. 1장에서 본 프로젝트 중단 사유 세 가지(비용 증가, 불분명한 사업 가치, 부족한 위험 통제)[S2]에 견주면, 반복량은 사업 가치를, 사람 확인 단계는 위험 통제를, 연결 시스템 수는 설치 비용을 가늠하는 항목입니다. 이 세 항목은 10장의 첫 유즈케이스 선정 기준과 같으므로, 카탈로그를 읽으면서 부서 업무 하나를 후보로 표시해 두면 도입 순서를 정할 때 그대로 쓸 수 있습니다.

이 장의 업무 화면은 업무 에이전트 11개와 스킬 313개가 설정된 운영 설치본 한 곳에서 찍은 화면 예시입니다. CRM·위키·드라이브·메일·메신저 같은 연결 시스템은 고객 환경에 맞춰 설정하며, 화면에 보이는 시스템 이름과 페이지 구조는 설정의 한 예입니다. 다만 모든 유즈케이스에 공통으로 적용하는 원칙은 설정과 관계없이 같습니다. 음성 인식과 OCR은 조직 안의 서버에서 처리하고, 에이전트가 외부 시스템에 기록하기 전에는 사람에게 결과를 먼저 보여 줍니다. 스킬과 정기 업무는 에이전트 플랫폼을 고치지 않고 플랫폼이 원래 제공하는 형식으로 등록하므로, 카탈로그 항목을 더하거나 빼도 플랫폼의 플러그인·설정·버전은 바뀌지 않습니다.

10개 카테고리를 한 표로 놓으면 담당 에이전트와 주된 트리거가 카테고리마다 다르다는 점이 드러납니다. 문서·OCR, 공공 문서·서식, 음성·회의 세 카테고리는 사람이 사진·파일·녹음을 보내면서 시작하고, 나머지 일곱 카테고리는 정해진 시각에 실행되는 정기 업무의 비중이 큽니다.

#	카테고리	대표 유즈케이스	담당 에이전트	주된 트리거
1	문서·OCR	명함 → CRM 연락처, PDF·스캔 문서 판독	영업, 비서	사진·파일 첨부
2	공공 문서·서식	한글(HWP·HWPX) 공공문서 인식, 공공서식 채우기, 기안문 생성, 법령 인용 확인	공공(중앙부처형, 지자체형)	첨부, 대화, 정기

#	카테고리	대표 유즈케이스	담당 에이전트	주된 트리거
3	음성·회의	화자 구분 회의록 → 지시사항 → 담당자별 할 일, 음성 지시	비서, 마케팅, 엔지니어링	녹음, 음성 메시지
4	영업·CRM	영업기회 등록, 일·주·월 영업 보고, 무활동 딜 점검, 조달 공고 선별	영업	정기, 대화
5	마케팅·지표	웹·검색·유튜브 지표 보고, 브랜드 보고, 이상 감지	마케팅	정기
6	재무	손익 보고, 채권·채무 조회	재무	정기, 대화
7	인사	이력서 1차 심사, 면담 정리	인사	정기, 녹음
8	IT 운영·관제	인프라 정기 점검 보고, 장애 1차 조사	APM, 엔지니어링	정기, 대화
9	리서치·콘텐츠	기술 조사, 백서·블로그·장표 제작, 시장 리포트	엔지니어링, 콘텐츠, 리서치	대화, 정기
10	개인 비서	아침 브리핑, 휴가자 안내, 저녁 정리, 리마인더, 메모	비서	정기, 대화, 음성

표의 담당 에이전트는 AAS 채팅 화면의 에이전트 목록과 그대로 대응합니다. 예를 들어 영업 담당자는 채팅 화면에서 영업 에이전트를 골라 명함을 보내고, 같은 에이전트가 새벽에 실행하는 영업 보고 정기 업무의 상태는 Cron 헬스체크 화면에서 확인합니다. 카탈로그의 한 줄은 AAS에서 업무 프로파일 하나에 스킬과 정기 업무 몇 개를 묶은 조합으로 나타나며, 부서 담당자는 그 조합을 콘솔에서 직접 만들고 지켜봅니다.

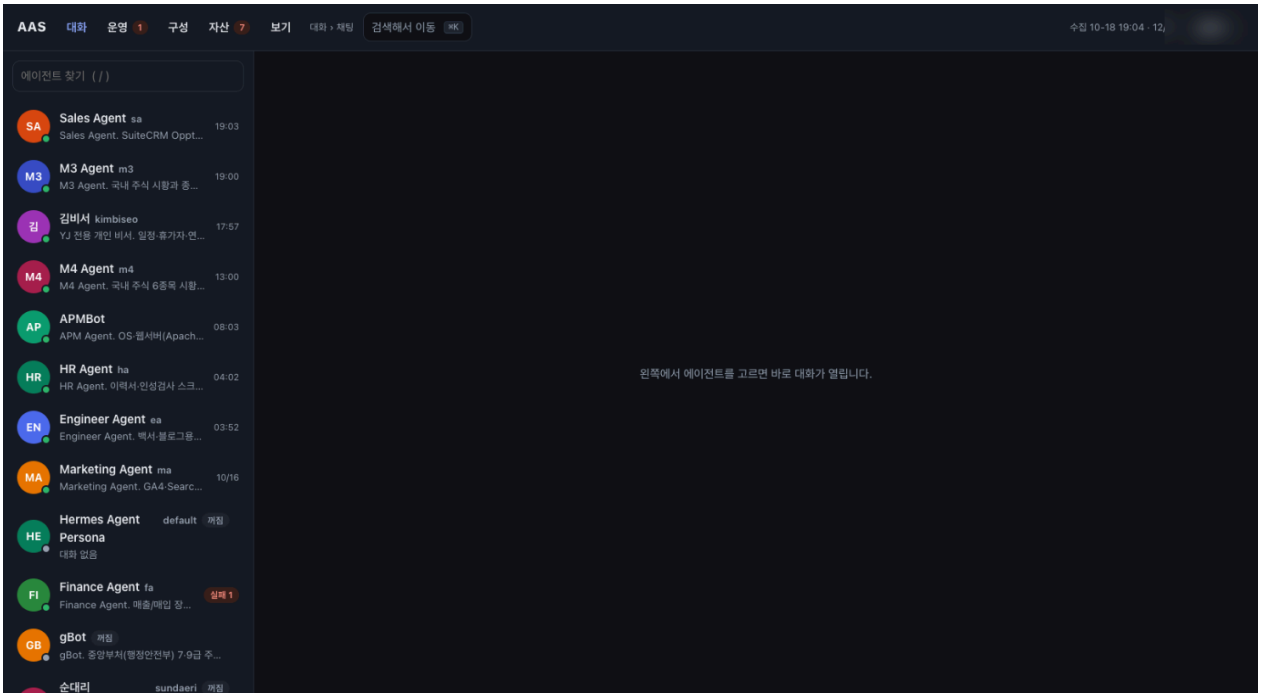


그림 5-1. AAS 채팅 화면의 업무 에이전트 목록. 영업, 시장 리포트, 비서, APM, 인사, 엔지니어, 마케팅, 재무, 공공(중앙부처형·지자체형) 에이전트가 보입니다. 업무 화면은 하나의 운영 설치본에서 찍은 화면 예시이며, 연결 시스템(CRM·위키·드라이브 등)은 고객 환경에 맞춰 설정합니다.

5.1 명함 사진에서 CRM 연락처 등록까지 — 등록 전 확인과 중복 시 정지를 갖춘 명함 인식

명함 인식은 명함 사진 한 장을 받아 이름·직함·회사·연락처를 읽고, 기존 고객사에 연결해 CRM 연락처와 위키 명함집에 등록하는 유즈케이스입니다. 영업 부서가 전시회나 고객 미팅에서 받은 명함을 손으로 옮겨 적는 작업은 반복량이 많고, 잘못 옮긴 연락처가 CRM에 그대로 남기 쉽습니다. 그래서 이 유즈케이스는 판독을 조직 안에서 처리하는 구조와 잘못된 등록을 막는 사람 확인 단계를 함께 갖추고 있습니다. 트리거는 메신저의 `/명함` 명령과 사진 첨부이고, 연결 시스템은 CRM, 연락처, 위키 세 곳입니다.

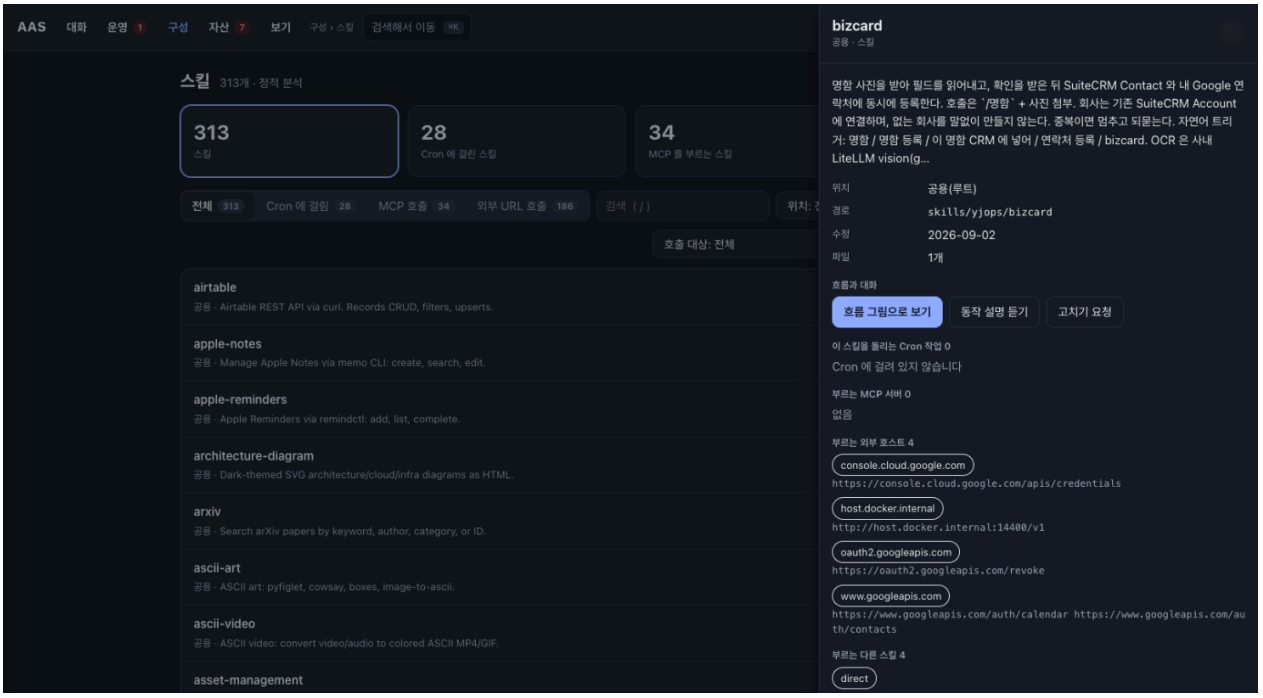


그림 5-2. 명함 인식 스킬의 상세 화면. 등록 전 확인, 없는 회사는 만들지 않음, 중복이면 멈춤 규칙과 이 스킬이 호출하는 외부 시스템 4곳을 한 화면에서 볼 수 있습니다.

5.1.1 조직 안 AI 게이트웨이의 비전 모델로 읽는 명함 판독

명함 판독은 외부 OCR 서비스를 쓰지 않고, 조직 안의 AI 게이트웨이에 연결된 비전 모델로 처리합니다. 판독 결과는 CRM 연락처, 연락처, 위키 명함집 세 곳에 함께 기록하며, 이 과정 전체를 AAS의 스킬 상세와 흐름 화면에서 확인할 수 있습니다.

외부 OCR 서비스 없는 명함 판독 구조

AI 게이트웨이는 조직이 쓰는 여러 언어 모델과 비전 모델을 하나의 접속 경로로 묶어 주는 사내 중계 서버입니다. 명함 사진은 이 게이트웨이로만 전달되므로, 고객의 이름과 휴대전화 번호가 담긴 이미지가 조직 밖 OCR 서비스로 나가지 않습니다. 따라서 업무 정보를 등급별로 나눠 외부 전송을 통제하는 공공 환경[S5]처럼 개인정보가 들어 있는 이미지를 외부로 보낼 수 없는 조직에서도 같은 유즈케이스를 그대로 쓸 수 있습니다. 어떤 비전 모델로 읽을지는 게이트웨이 설정에서 정하므로, 조직이 모델을 교체하더라도 명함 인식 스킬 문서는 그대로 유지합니다.

판독 항목과 기존 고객사 연결 규칙

비전 모델이 명함에서 읽는 항목은 다섯 가지이고, 에이전트는 그중 회사명을 CRM의 기존 고객사(Account)와 맞대어 연결할 고객사를 찾습니다. 각 항목이 어느 시스템에 기록되는지는 다음과 같습니다.

판독 항목	기록하는 곳
이름	CRM 연락처, 연락처, 위키 명함집 페이지 제목
직함·부서	CRM 연락처, 고객사 위키 페이지의 직원 표
회사	기존 고객사 연결 기준, 위키 명함집의 회사 단위 묶음

판독 항목	기록하는 곳
전화·휴대전화	CRM 연락처, 연락처
이메일	CRM 연락처, 연락처

위키 명함집은 「명함집 › 회사 › 이름」 순서의 페이지 계층으로 쌓이고, 에이전트는 명함을 등록할 때마다 해당 고객사 페이지의 직원 표도 함께 갱신합니다. 예를 들어 같은 고객사 직원의 명함이 여러 장 등록되면 고객사 페이지에 부서와 직함이 붙은 직원 목록이 생깁니다. 명함이 영업 담당자 개인의 명함첩에 머무르지 않고 CRM과 위키에 조직의 기록으로 남으므로, 담당자가 바뀌어도 고객 연락처가 함께 사라지지 않습니다.

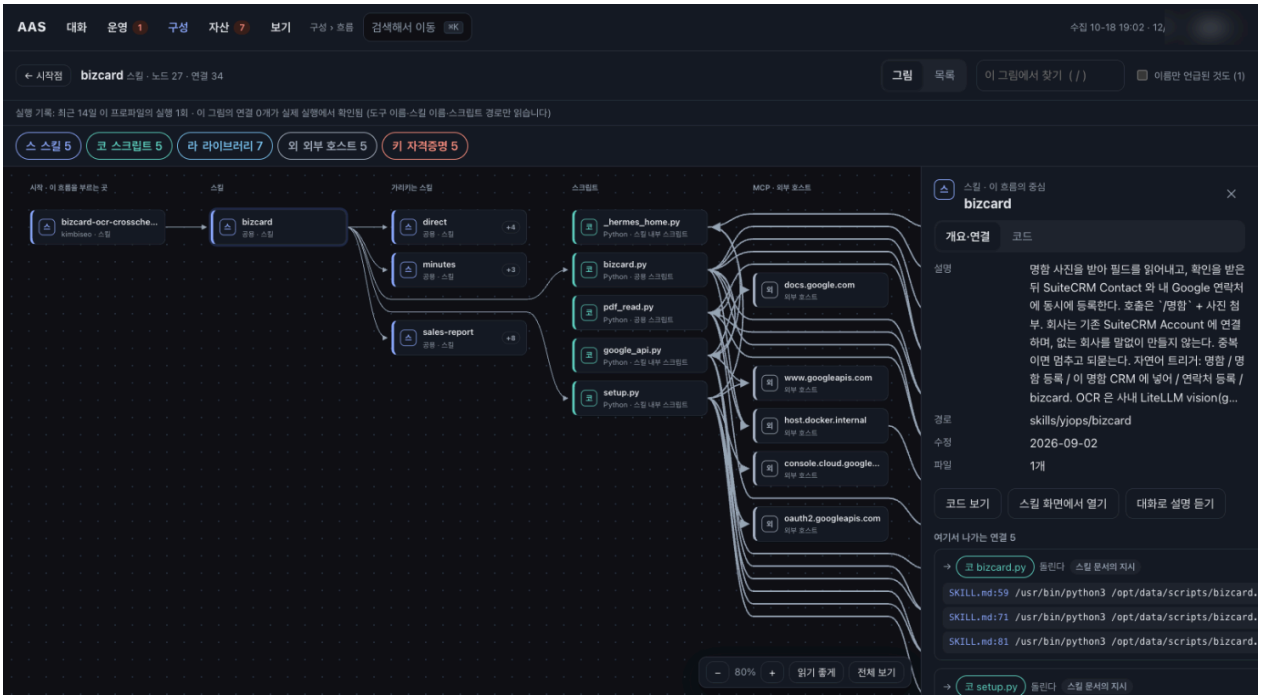


그림 5-3. 명함 인식 스킬의 흐름 화면. 스킬이 부르는 스크립트 5개와 외부 시스템, 사용하는 자격증명 5개가 선으로 이어지고, 선마다 스킬 문서의 근거 줄이 붙습니다.

흐름 화면이 보여 주는 명함 인식의 호출 관계

흐름 화면은 스킬 문서, 스크립트, 실행 기록에서 뽑아낸 호출 관계를 그린 화면이며, 사람이 따로 그린 설계도와는 다릅니다. 명함 인식의 경우 스킬 하나가 판독·PDF 읽기·연락처 등록 스크립트를 거쳐 CRM, 연락처, 위키로 이어지고, 각 연결에 필요한 자격증명 5개가 함께 표시됩니다. 따라서 IT 담당자는 이 유즈케이스가 어떤 외부 시스템에 쓰는지, CRM 토큰이 만료되면 어떤 기능이 멈추는지를 스킬 문서를 열지 않고 확인할 수 있습니다. 자격증명은 값을 보여 주지 않고 이름, 위치, 사용하는 곳만 보여 주며, 만료가 가까워진 CRM 토큰은 자격증명 화면에 따로 표시됩니다.

PDF·스캔 문서로 넓어지는 판독 범위

같은 문서·OCR 카테고리에는 명함 외에도 PDF·이미지 판독, 스캔 문서 원문 옮기기, 상품 이미지 읽기 유즈케이스가 함께 들어 있습니다. PDF 판독은 파일 안의 글자층을 먼저 읽고, 글자층이 없는 쪽만 비전 모델로 읽어 마크다운으로 바꿉니다. 스캔 문서 원문 옮기기는 쪽의 표 구조를 유지한 채 글자를 그대로 옮기고, 가려져 읽을

수 없는 부분은 [지워짐] 으로 표시합니다. 즉 명함 인식을 먼저 도입하면 같은 AI 게이트웨이와 같은 판독 스킬을 계약서·견적서 같은 다른 문서로 넓히는 일이 설정 추가 수준에서 끝납니다.

5.1.2 등록 전 예행 결과 확인과 중복 시 정지로 막는 잘못된 고객 등록

명함 인식에서 가장 먼저 나오는 반론은 「잘못 읽은 명함이 CRM에 그대로 등록되면 어떻게 하는가」입니다. 이 유즈케이스는 판독 정확도에 기대는 대신, 기록하기 전에 사람이 결과를 보고 결정하는 단계를 스킬 안에 넣어 그 반론에 답합니다.

잘못 등록된 고객 정보가 CRM에 남기는 부담

CRM에 잘못 들어간 연락처나 중복된 고객사는 한 번 생기면 영업 보고, 딜 일지, 메일 기록에 연쇄적으로 따라 붙습니다. 예를 들어 같은 회사가 이름 표기만 달리해 두 고객사로 등록되면, 영업기회가 두 곳에 나뉘어 쌓이고 월간 보고의 고객사별 집계가 어긋납니다. 에이전트가 사람 몰래 기록하는 구조는 조직의 정보 관리 정책과 부딪힙니다. 허가되지 않은 에이전트 행위의 대부분이 내부 정책 위반에서 나온다는 1장의 전망[S3]을 고려하면, 외부 시스템에 쓰는 동작 앞에 사람 확인을 두는 것은 업무 에이전트의 기본 통제이며, 명함 인식은 그 통제를 가장 단순한 형태로 보여 주는 사례입니다.

명함 인식 스킬의 사람 확인 규칙 세 가지

명함 인식 스킬은 다음 세 가지 규칙에 따라 기록을 멈추고 사람에게 묻습니다.

- 등록 전 예행(dry-run) 결과 확인: 어느 시스템의 어떤 항목에 무엇을 쓸지 먼저 보여 주고, 사람이 확인한 뒤에만 실제로 기록합니다.
- 중복 시 정지: CRM에 같은 사람이 이미 있으면 기록을 멈추고 기존 연락처를 갱신할지 되묻습니다.
- 없는 회사 미생성: CRM에 없는 고객사는 에이전트가 임의로 만들지 않고, 새 고객사로 등록할지 사람에게 묻습니다.

예행은 실제 기록 없이 기록할 내용만 계산해 보여 주는 실행 방식이며, 위험 통제가 부족한 에이전트 프로젝트가 중단 위험이 크다는 전망[S2]에 대응하는 가장 단순한 통제 수단입니다. 영업 담당자는 명함 사진을 보낸 직후 채팅 화면에서 「CRM 연락처 1건 추가, 연락처 1건 추가, 위키 명함집 페이지 1개 생성」 같은 예정 목록을 보고 승인 여부를 정합니다. 반면 판독이 틀린 경우에는 승인하지 않고 틀린 항목을 채팅으로 고쳐 다시 예행을 요청합니다. 이 규칙은 스킬 문서에 적혀 있으며, AAS 스킬 상세 화면은 그 규칙을 부서 담당자가 읽을 수 있는 형태로 보여 줍니다.

없는 회사를 만들지 않는 규칙의 효과

세 규칙 가운데 없는 회사를 만들지 않는 규칙은 CRM의 고객사 목록을 영업 조직이 관리하는 기준 데이터로 지키는 장치입니다. 고객사는 계약, 영업기회, 담당 영업 같은 다른 정보의 기준이 되므로, 판독 결과 하나로 새 고객사가 생기면 그 뒤의 모든 집계가 영향을 받습니다. 에이전트는 기존 고객사와 맞는 경우에만 연결하고, 맞는 고객사가 없으면 사람에게 결정을 넘깁니다. 다만 이 규칙 때문에 처음 만나는 회사의 명함은 한 번 더 확인을 거치게 되므로, 신규 고객 발굴이 많은 부서는 확인 빈도를 감안해 파일럿 범위를 정해야 합니다.

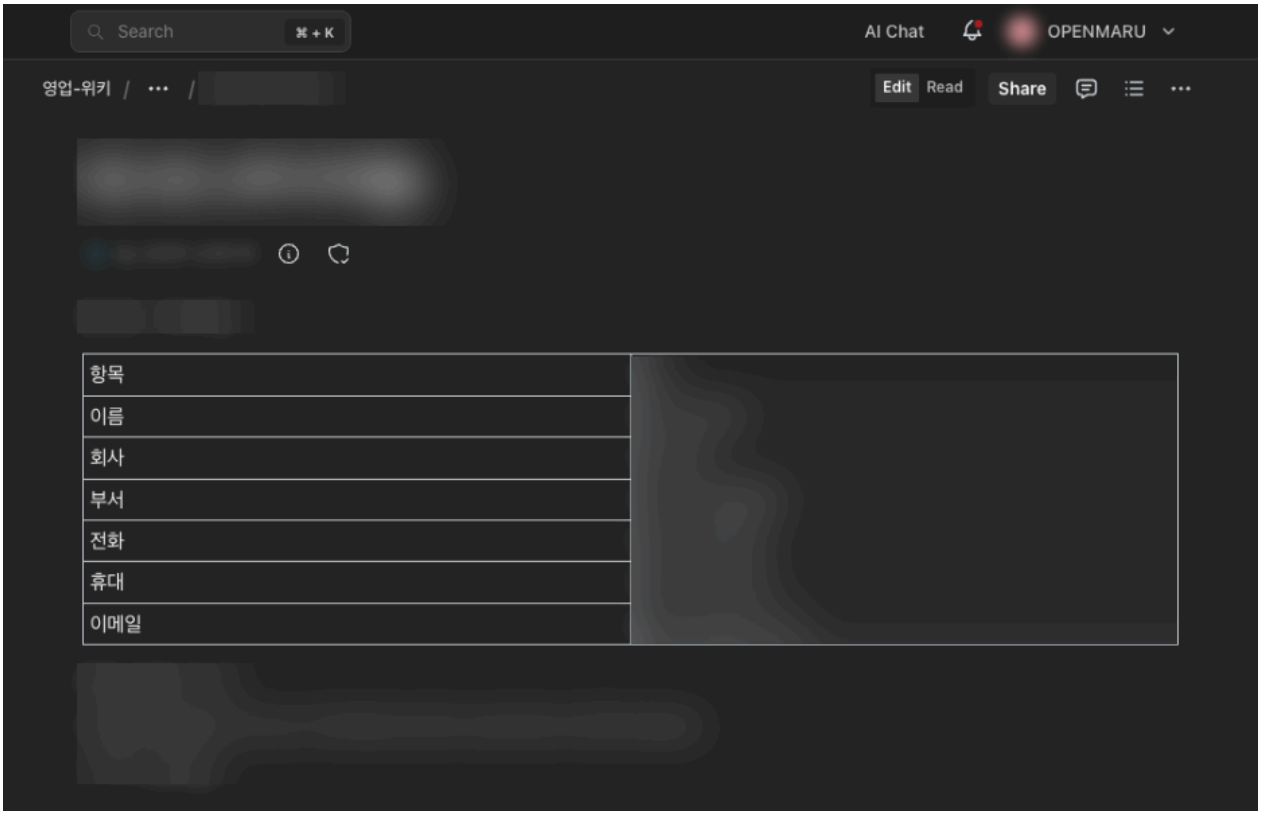


그림 5-4. 명함 인식 결과로 만들어진 위키 명함집 페이지. 명함집 › 회사 › 이름 계층 아래에 판독 항목과 CRM 연결 정보가 함께 기록됩니다. 화면의 개인 정보는 가림 처리했고, 연결 시스템(CRM·위키·드라이브 등)은 고객 환경에 맞춰 설정합니다.

명함 인식의 파일럿 후보 특성

명함 인식은 반복량이 많고(전시회·고객 미팅마다 수십 장), 위험 통제 수단인 사람 확인이 등록 전 1회로 단순하며, 연결 시스템이 CRM·연락처·위키 3곳으로 정해져 있습니다. 영업이라는 업무 기능 하나 안에서 시작과 끝이 닫히므로, 업무 기능별 확대 적용 비율이 10%를 넘지 않는 현실[S4]에서 첫 범위를 좁게 잡기 좋은 후보입니다. 즉 영업 부서가 있는 조직이라면 명함 인식을 첫 파일럿 후보 목록의 맨 앞에 두고 검토할 수 있습니다.

5.2 한글(HWP·HWPX) 공공문서 인식과 공공서식 빈칸 채우기, 기안문 작성

공공문서·공공서식 카테고리는 다른 기관에서 온 한글(HWP·HWPX) 공문을 읽어 요약하고, 받은 공공서식의 빈칸을 채우며, 기안문과 보고서를 한글 파일로 만들고, 법령 인용을 확인하는 공공 업무 묶음입니다. 2장에서 본 것처럼 국가 망 보안체계는 업무 정보를 세 등급으로 나눠 생성형 AI와 클라우드를 쓸 길을 열었지만[S5], 기밀 등급 업무는 여전히 망을 분리해 두므로, 외부 OCR 서비스나 외부 언어 모델 키를 전제로 한 도구는 그 업무에 쓰기 어렵습니다. 이 카테고리의 처리는 문서 변환, OCR, 언어 모델 호출까지 모두 조직 안에서 끝나도록 구성되어 있으며, AAS 자체도 외부 내려받기 없이 조직 안에 온프레미스로 설치합니다.

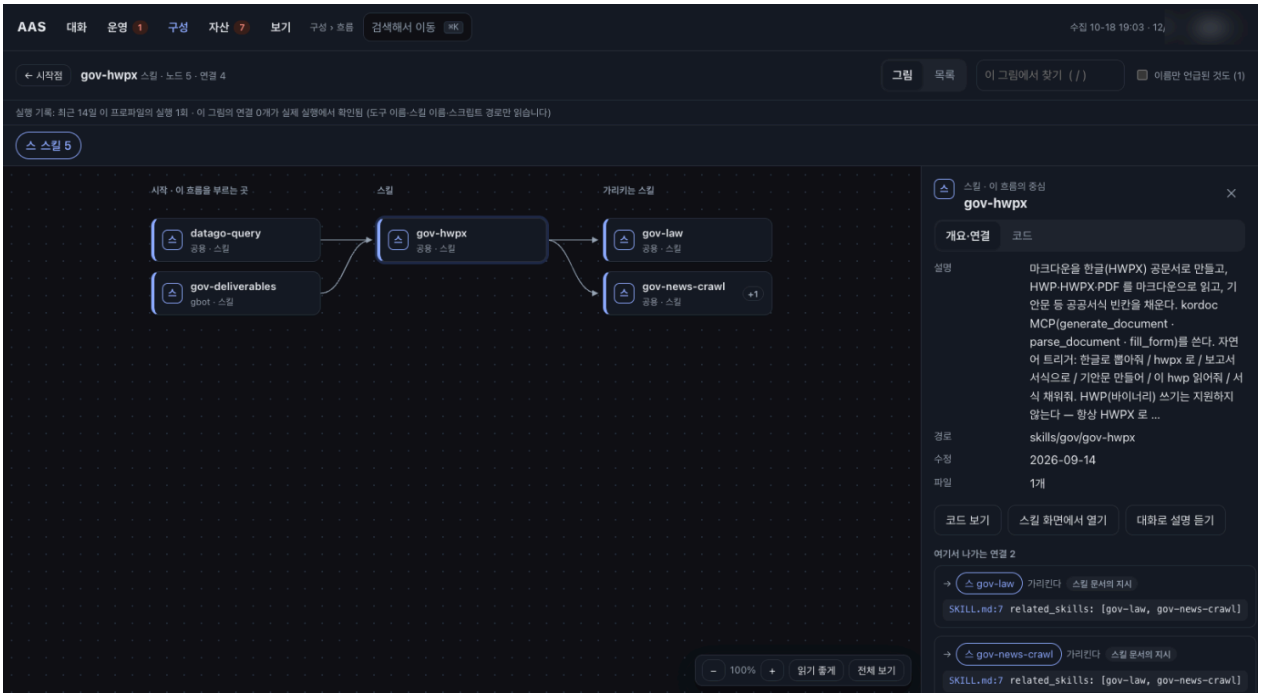


그림 5-5. 공공 문서(HWPX) 스킬의 흐름 화면. 공공데이터 조회와 공무원 산출물 스킬이 이 스킬을 부르고, 이 스킬은 법령 조회와 보도자료 수집으로 이어집니다. 화면 설명란에 HWPX 생성, HWP·HWPX·PDF 읽기, 기안문 서식 채우기 기능이 적혀 있습니다.

5.2.1 오프라인 OCR로 읽는 스캔 공문과 공공서식 구조 분석

공공문서 인식은 문서 변환을 맡는 MCP 도구 서버와 내장 오프라인 OCR 두 가지로 구성됩니다. 에이전트는 문서 형식을 직접 해석하지 않고 MCP 도구 서버에 변환을 요청합니다.

한글 공문을 마크다운으로 읽는 문서 변환 도구 서버

담당자가 채팅 화면에서 공문 파일을 첨부하고 「이 hwp 읽어줘」라고 요청하면, 에이전트는 문서 변환 도구 서버로 파일을 마크다운으로 바꾼 뒤 요약을 작성합니다. 마크다운은 제목·목록·표를 기호로 표시하는 텍스트 형식으로, 언어 모델이 문서 구조를 잃지 않고 읽을 수 있습니다. 지원하는 형식과 처리 방식은 다음과 같습니다.

형식	처리 방식	주된 쓰임
HWP	마크다운으로 변환한 뒤 요약	다른 기관에서 받은 공문
HWPX	마크다운으로 변환한 뒤 요약, 서식 분석과 빈칸 채우기, 새 문서 생성	기안문·보고서·시행문
PDF	글자층을 먼저 읽고, 스캔본은 오프라인 OCR로 판독	스캔 공문, 첨부 자료
DOCX	마크다운으로 변환한 뒤 요약	워드 형식 협조 문서

문서 변환이 MCP 도구 서버 한 곳에 모여 있으므로, 공공 업무 에이전트가 여러 개여도 변환 기능은 한 번만 설치하면 됩니다. 이 도구 서버도 조직 안에 설치하므로, 망분리 규제 개선 뒤에도 분리가 유지되는 업무망[S6]에

서 같은 구성을 쓸 수 있습니다. AAS 흐름 화면에서 공공 문서 스킬이 MCP 도구 서버를 호출하는 관계가 선으로 표시되므로, IT 담당자는 어떤 스킬이 문서 변환에 의존하는지 한 화면에서 확인할 수 있습니다.

외부 키 없이 실행되는 오프라인 OCR

스캔한 공문은 글자층이 없는 이미지라서 문서 변환만으로는 내용을 읽을 수 없습니다. 이 경우 문서 변환 도구 서버에 내장된 오프라인 OCR이 한국어 모델로 글자를 읽으며, 이 OCR은 CPU에서 실행되고 외부 API 키를 요구하지 않습니다. 따라서 GPU 서버가 없는 기관이나 외부 서비스 접속이 막힌 업무망에서도 스캔 공문을 판독할 수 있습니다. 기밀 등급 업무처럼 망 분리가 유지되는 환경[S5]에서도 공문 판독 유즈케이스는 그대로 실행됩니다.

공공서식의 빈칸 구조 분석과 채운 값 확인

공공서식 채우기는 받은 서식 파일의 빈칸 구조를 먼저 분석하고, 각 빈칸에 들어갈 값을 채운 뒤 서식 모양 그대로 파일을 돌려주는 유즈케이스입니다. 서식 분석은 표 안의 어느 칸이 입력란이고 어느 칸이 고정 문구인지 가려 빈칸 목록을 만드는 단계입니다. 에이전트는 채운 값을 담당자에게 먼저 보여 주고, 담당자가 확인한 뒤에만 파일을 저장합니다. 예를 들어 「서식 채워줘」라고 요청하면 빈칸 목록과 채울 값이 채팅 화면에 표로 나타나고, 담당자는 틀린 값을 고친 뒤 저장을 승인합니다. 이 확인 단계 덕분에 서식 칸 위치를 잘못 읽은 경우에도 잘못 채운 파일이 결재로 넘어가지 않습니다.

5.2.2 중앙부처형과 지자체형 업무 에이전트가 맡는 각 10개 업무

공공 카테고리는 중앙부처형과 지자체형 두 가지 업무 에이전트로 나뉘며, 각각 10개 업무를 스킬로 갖추고 있습니다. 두 에이전트는 문서 변환·법령 조회·공공데이터 조회 같은 공통 도구를 함께 쓰고, 맡는 업무 범위는 기관 성격에 맞춰 다르게 구성되어 있습니다.

중앙부처형과 지자체형 에이전트의 업무 범위 비교

중앙부처형은 정책과 국회·언론 대응에, 지자체형은 주민 민원과 지역 행정에 업무가 모여 있습니다. 두 에이전트의 업무 목록은 다음과 같습니다.

순번	중앙부처형 업무 에이전트	지자체형 업무 에이전트
1	정책·언론 모니터링	언론 모니터링
2	법령 해석	조례 검토
3	국회·언론 답변 초안	민원 답변
4	시도 현황 취합	고시·공고 작성
5	해외 사례 조사	전통시장 정보 조회
6	보고서·메모 작성	복지 서비스 조회
7	회의록 작성	시설 점검
8	예산 조회	축산·야생동물 업무
9	민원 동향 분석	회의록 작성

순번	중앙부처형 업무 에이전트	지자체형 업무 에이전트
10	재난안전 요약	공모사업 신청

표에서 회의록 작성은 두 에이전트에 공통으로 들어 있으며, 5.3의 화자 구분 회의록 스킬을 그대로 호출합니다. 반면 조례 검토, 전통시장, 복지, 공모사업처럼 지자체에만 있는 업무는 공공데이터포털 조회와 자치법규 조회를 함께 씁니다. 기관이 두 유형 가운데 하나를 골라 시작하더라도, 공통 스킬은 다른 유형에서도 다시 만들 필요가 없습니다.

기안문 작성과 법령 인용 확인의 처리 흐름

기안문 작성은 담당자가 채팅으로 준 내용을 기안문 서식의 빈칸에 채우고, 결과를 한글(HWPX) 파일로 돌려주는 순서로 진행됩니다. 공문·보고서 생성 스킬은 마크다운 원고를 보고서·기안문·시행문 서식의 HWPX로 바꾸며, 기안문 템플릿은 스킬 안에 들어 있습니다. 본문에 법령이나 판례를 인용했다면 법령 조회 스킬이 국가법령 도구 서버에서 법령·시행령·자치법규·판례를 찾아 인용 문구가 원문과 맞는지 확인합니다. 다만 국가법령 도구 서버의 접속 키가 없으면 에이전트는 확인 없이 진행하지 않고 멈춘 뒤 담당자에게 알리며, 키 상태는 AAS 자격 증명 화면에서 값 없이 확인할 수 있습니다.

보도자료·정책 모니터링 정기 업무와 스킬 자동 생성 승인

보도자료·정책 모니터링은 매일 06:00에 실행되는 정기 업무로, 부처 RSS, 정책브리핑, 지자체 게시판을 모아 아침 브리핑을 만들고 위키 페이지나 한글 문서로 발행합니다. 이 정기 업무가 실패하거나 결과를 보낼 곳이 없으면 AAS Cron 헬스체크 화면에 그 상태가 표시되므로, 브리핑이 오지 않은 원인을 담당자가 직접 찾을 수 있습니다. 지자체형 에이전트는 반복 요청을 바탕으로 새 스킬을 자동으로 만들 수 있는데, 자동으로 만든 스킬은 담당자가 승인한 뒤에만 반영합니다. 즉 공공 카테고리에서도 에이전트가 스스로 업무 범위를 넓히는 동작 앞에는 사람 확인이 있습니다.

공공 문서 카테고리의 파일럿 후보 특성

공공문서·공공서식 카테고리는 반복량이 많고(매일 들어오는 공문과 서식), 사람 확인이 저장 전 1회이며, 필수 연결 시스템이 문서 변환 도구 서버 1곳으로 가장 적습니다. 법령 조회와 공공데이터 조회는 업무에 따라 더하는 선택 연결입니다. 따라서 망 분리가 남아 있는 공공기관[S5][S6]이라면 공문 판독과 공공서식 채우기를 첫 파일럿 후보로 검토할 수 있으며, 외부 키가 필요 없다는 점에서 설치 준비도 가장 가볍습니다. 공공기관 업무 PC에 국가 망 보안체계를 적용하는 공모가 2026년 3월에 시작된 만큼[S7], 망 보안 체계 정비와 같은 시기에 공문 판독 파일럿을 함께 검토할 수 있습니다.

5.3 화자 구분 회의록에서 지시사항과 담당자별 할 일로 이어지는 회의 후속 처리

화자 구분 회의록 유즈케이스는 회의 녹음을 받아 조직 안 GPU 서버에서 음성 인식(STT, Speech-to-Text)과 화자 분리를 처리하고, 목소리 지문으로 화자 이름을 붙인 부서별 회의록을 만든 뒤, 회의록의 지시사항을 담당자별 할 일로 넘기는 회의 후속 처리 묶음입니다. 경영진에게 이 유즈케이스의 가치는 회의가 끝나면 할 일 목록이 이미 칸반에 있다는 점입니다. 회의 녹음에는 경영 판단과 인사·고객 정보가 섞여 있으므로, 녹음 파일을 외부 음성 인식 API로 보내는 것 자체가 정보 과다 공유가 될 수 있습니다. 정보 과다 공유를 내부 정책 위반의 대표 유형으로 꼽은 전망[S3]을 고려하면, 음성 인식부터 위키 발행까지를 조직 안에서 끝내는 구조는 회의록 유즈케

이스의 도입 조건입니다. 트리거는 메신저의 `/회의록 <부서> [주제]` 명령과 녹음 파일 첨부이며, 연결 시스템은 음성 인식 서버, 드라이브, 위키, 업무 채팅 네 곳입니다.

5.3.1 조직 안 음성 인식과 목소리 지문으로 만드는 화자 구분 회의록

화자 구분 회의록은 음성 인식, 화자 분리, 화자 실명화, 템플릿 회의록 작성의 네 단계로 만들어집니다. 네 단계 모두 조직 안 서버에서 처리하며, 외부 STT 서비스는 쓰지 않습니다.

외부 STT 없는 음성 인식과 화자 분리

에이전트는 MP3·M4A·OGG 형식의 녹음을 받아 조직 안 GPU 서버의 음성 인식으로 글자를 만들고, 화자 분리로 발언마다 화자 라벨을 붙입니다. 화자 분리는 녹음 안에서 목소리가 다른 사람을 구분해 「화자 1」·「화자 2」처럼 나누는 처리이며, 이 단계에는 오픈소스 sherpa-onnx를 씁니다. 회의 음성은 조직 안 GPU 서버를 벗어나지 않으므로 민감 등급 정보의 외부 전송을 통제하는 기준[S5]과 충돌하지 않고, 음성 인식 엔진 이름은 회의록 머리에 함께 기록되어 나중에 결과를 해석할 때 근거로 쓰입니다. 다만 GPU 서버가 없는 조직은 음성 인식 서버를 먼저 준비해야 하므로, 이 유즈케이스는 명함 인식이나 공문 판독보다 설치 준비가 큽니다.

목소리 지문으로 화자 이름을 붙이는 원칙

목소리 지문은 미리 등록한 사람의 목소리 특징값이며, 에이전트는 화자 라벨의 목소리를 등록된 지문과 비교해 이름을 붙입니다. 원칙은 근거가 있을 때만 실명을 쓰는 것이며, 지문이 맞지 않거나 등록된 지문이 없으면 그 화자를 「미확인」으로 남깁니다. 화자 표에는 화자 라벨, 추정한 이름, 그 이름을 붙인 근거가 함께 기록되므로, 회의록을 읽는 사람은 어떤 발언자가 지문으로 확인된 사람인지 구분할 수 있습니다. 즉 회의록이 사람의 발언을 잘못된 이름에 붙이는 위험을 근거 표시로 드러내고, 이름을 고칠지는 회의록을 읽는 사람이 정합니다.

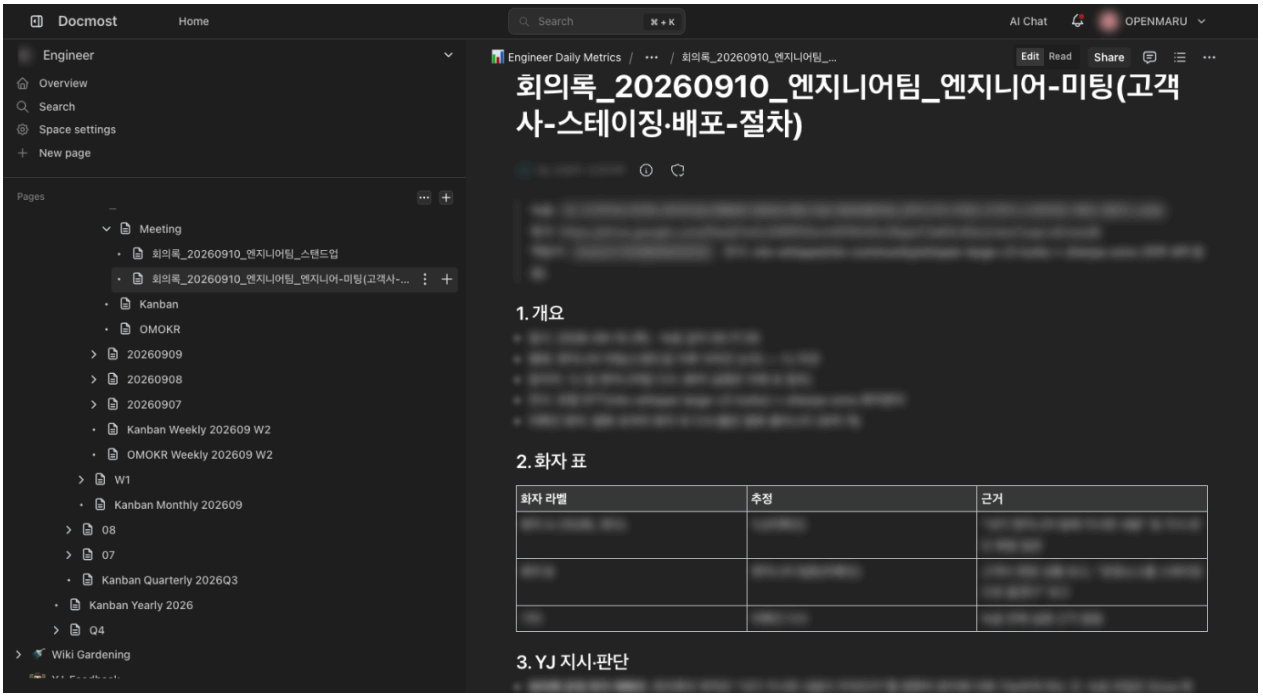


그림 5-6. 화자 구분 회의록의 머리 부분. 원본 음성 보관 위치와 음성 인식 엔진, 회의 개요, 화자 표(화자 라벨·추정 이름·근거)가 차례로 나옵니다. 화면의 사람 이름은 가림 처리했습니다.

부서별 템플릿 회의록의 구성 항목

회의록은 부서별 템플릿에 맞춰 작성되며, 기본 템플릿의 구성 항목은 다음과 같습니다.

구성 항목	담기는 내용
개요	회의 주제, 참석 화자, 원본 음성 보관 위치
화자 표	화자 라벨, 추정 이름, 이름을 붙인 근거
지시·판단	리더의 지시, 지시의 근거, 기한
보고·의견	참석자의 보고와 의견
이견	합의하지 못하고 남은 쟁점
결정 사항	회의에서 정한 내용
액션 아이템	항목, 담당, 기한
발언 원문	화자별 발언 기록

고객 회의에는 별도 템플릿을 씁니다. 고객 회의 템플릿은 고객 요구, 우려, 일정·예산, 「우리가 약속한 것(리스크)」, 답하지 못한 질문, 합의와 미합의 사항을 따로 정리하고, 회의록을 CRM의 영업기회에 연결합니다. 다만 고객 회의록은 조직과 영업기회를 반드시 지정해야 만들어지므로, 연결 대상이 불분명한 녹음은 담당자가 먼저 지정해야 합니다.

원본 음성 보관과 위키 발행 순서

원본 음성은 드라이브의 부서·날짜별 폴더에 보관하고, 회의록은 부서 위키에 발행합니다. 발행 순서에도 규칙이 있어, 원본 음성 보관이 실패하면 에이전트는 회의록을 위키에 올리지 않습니다. 근거가 되는 음성이 없는 회의록이 먼저 퍼지면 나중에 발언 내용을 다시 확인할 방법이 없기 때문입니다. 드라이브와 위키는 예시이며, 연결 시스템(CRM·위키·드라이브 등)은 고객 환경에 맞춰 설정합니다.

5.3.2 지시·근거·기한으로 정리한 지시사항이 칸반 할 일과 지시 원장으로 쌓이는 흐름

회의록의 지시사항과 액션 아이템은 회의록 발행 직후 자동으로 칸반 할 일로 넘어가고, 지시 원장에 번호를 달고 쌓입니다. 이 흐름 덕분에 회의에서 나온 지시는 회의록 문서 안에 머무르지 않고 담당자의 할 일 목록과 조직의 지시 기록으로 이어집니다.

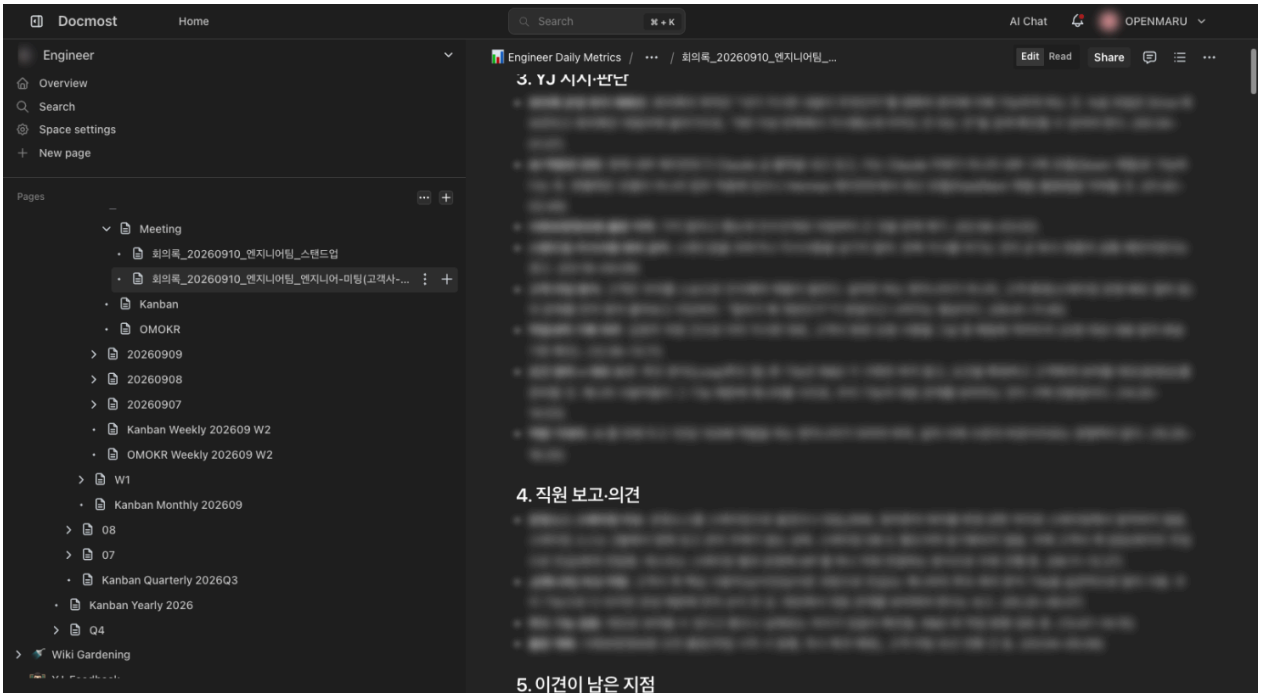


그림 5-7. 회의록의 지시·판단 부분. 리더의 지시가 지시·근거·기한 세 칸으로 정리되고, 직원 보고·의견과 이견이 남은 쟁점이 별도 항목으로 나옵니다.

지시사항과 액션 아이템의 구분

지시사항은 리더가 회의에서 내린 판단을 「지시·근거·기한」 세 칸으로 정리한 항목이고, 액션 아이템은 실행할 일을 「항목·담당·기한」으로 정리한 항목입니다. 두 가지를 나누는 이유는 쓰임이 다르기 때문입니다. 지시사항은 나중에 「그때 왜 그렇게 정했는가」를 확인하는 기록이므로 근거가 함께 남아야 하고, 액션 아이템은 누가 언제까지 무엇을 하는지가 분명해야 합니다. 에이전트는 회의록의 지시·판단 항목과 액션 아이템 항목을 각각 뽑아 지시는 지시 원장에, 할 일은 칸반에 보냅니다.



그림 5-8. 화자 구분 회의록에서 지시사항과 액션 아이템이 칸반 할 일, 지시 원장, 담당자별 알림으로 이어지는 처리 흐름

칸반 할 일과 지시 원장의 누적

에이전트는 액션 아이템을 그날의 칸반 페이지에 담당자별 체크박스로 합치고, 같은 날 여러 회의가 있으면 한 페이지에 모읍니다. 지시 원장은 지시에 D-번호, 피드백에 F-번호를 붙여 쌓고 일·주·월 단위로 집계하는 기록입니다. 30분마다 실행되는 정기 업무가 칸반에서 사람이 체크한 항목을 거둬들여 원장에 반영하고, 담당자별 요약을 업무 채팅방에 보냅니다. 체크 표시는 사람이 하며, 에이전트는 완료 여부를 스스로 판단해 체크하지 않습니다. 결과적으로 리더는 지시 원장에서 지시 번호별로 근거와 진행 상태를 함께 보고, 「그때 뭐라고 지시했는가」를 회의록 원문까지 거슬러 확인할 수 있습니다.

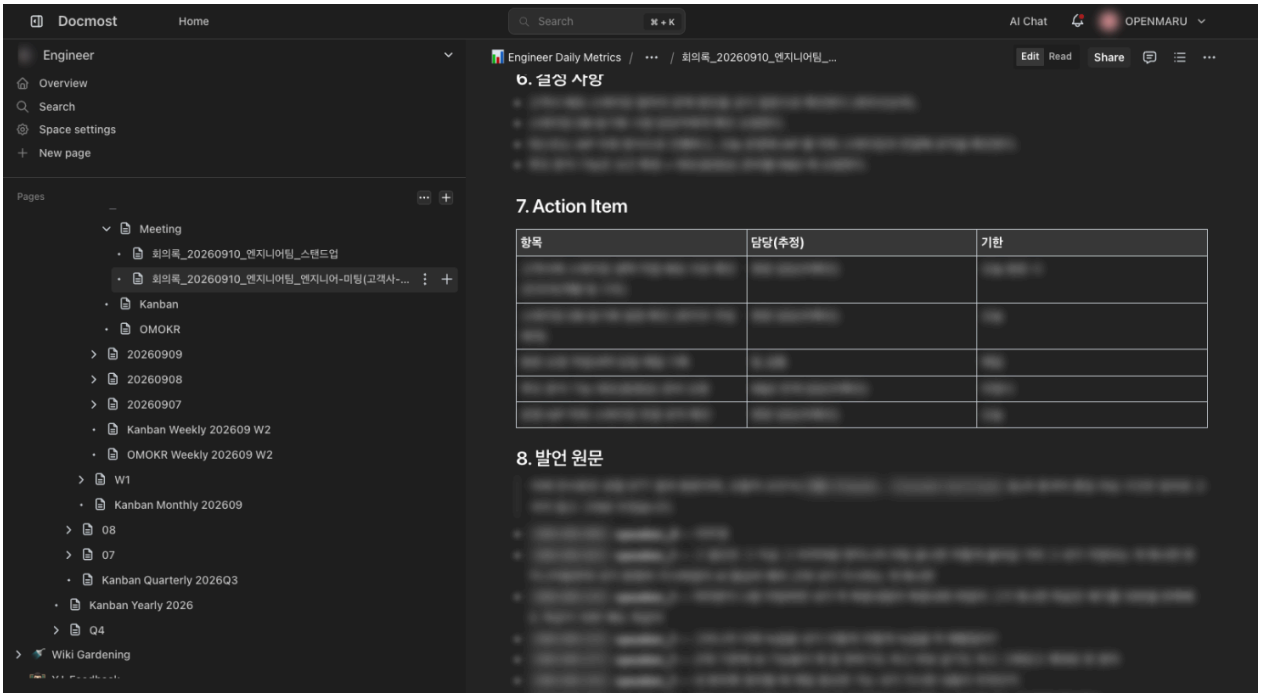


그림 5-9. 회의록의 결정 사항과 액션 아이템 부분. 항목·담당·기한으로 정리한 액션 아이템이 칸반 할 일로 넘어가고, 아래에 화자별 발언 원문이 붙습니다.

AAS 화면에서 보는 회의 후속 처리 상태

회의 후속 처리는 회의록 스킬, 체크 수확 정기 업무, 위키·채팅 연결의 조합이므로 AAS의 세 화면에서 상태를 봅니다. 흐름 화면은 회의록 스킬이 음성 인식·지문 적용·위키 발행 스크립트를 거쳐 위키와 AI 게이트웨이로 이어지는 관계를 보여 주며, 명함 인식과 면담 정리를 포함해 이 스킬을 부르는 다른 스킬 6개도 함께 표시합니다. Cron 헬스체크 화면은 30분 주기 수확 작업이 마지막으로 언제 성공했는지와 결과를 보낼 곳이 있는지를 보여 주고, 활동 화면은 회의록 요청이 들어온 세션을 시간순으로 보여 줍니다. 담당자별 알림이 오지 않으면 부서 담당자가 수확 작업의 실패 여부를 직접 확인하고 IT 담당자에게 넘길 수 있습니다.

회의록 유즈케이스의 파일럿 후보 특성

화자 구분 회의록은 반복량이 정례 회의 수만큼(주 1회 이상) 꾸준하고, 사람 확인이 화자 이름 확인과 체크 표시 두 단계이며, 연결 시스템이 음성 인식 서버·드라이브·위키·업무 채팅 4곳으로 많습니다. 따라서 설치 준비는 다른 대표 사례보다 크지만 경영진이 결과를 직접 체감하는 유즈케이스입니다. 업무 기능 하나에서 확대 적용 비율

이 낮은 상황[S4]을 고려하면, 처음에는 부서 하나의 주간 회의로 범위를 좁혀 시작하는 편이 좋습니다. 연결 시스템이 많을수록 설치 비용이 커지므로, 비용 증가를 중단 원인으로 꼽은 전망[S2]도 같은 판단을 뒷받침합니다.

5.4 영업 보고에서 개인 비서까지 정기 업무로 실행되는 나머지 일곱 카테고리

영업·CRM, 마케팅·지표, 재무, 인사, IT 운영·관제, 리서치·콘텐츠, 개인 비서 일곱 카테고리는 대부분 정해진 시각에 실행되는 정기 업무로 구성됩니다. 사람이 채팅으로 시키는 유즈케이스도 있지만, 담당자가 보지 않는 시각에 보고서를 만들고 알림을 보내는 작업이 중심입니다. 이렇게 사람이 보지 않는 동안 실행되는 정기 업무의 상태를 확인할 화면이 함께 있어야 업무에 맡길 수 있습니다. 일곱 카테고리에도 대표 사례와 같은 공통 원칙이 적용되어, 처리는 조직 안에서 하고 외부 시스템에 쓰기 전에는 사람이 확인하며, 연결 시스템은 고객 환경에 맞춰 설정합니다.

일곱 카테고리의 대표 업무, 트리거, 연결 시스템, 사람 확인을 같은 틀로 놓으면 다음과 같습니다.

카테고리	대표 업무와 트리거	연결 시스템	사람 확인
영업·CRM	일·주·월 영업 보고, 무활동 딜 점검, 조달 공고 선별(정기), 영업기회 등록(대화)	CRM, 위키, 드라이브, 메일	영업기회 등록 전, CRM 수정 전
마케팅·지표	웹·검색·유튜브 지표 보고, 브랜드별 보고, 이상 감지(정기)	웹 분석, 검색 콘솔, 위키	없음(읽기 중심 보고)
재무	주간·월간 손익 보고(정기), 채권·채무 질의(대화)	원장 시트	없음(읽기 중심 보고)
인사	이력서 1차 심사(정기 04:00), 면담 정리(녹음)	공유 드라이브, 위키	채용 판단은 사람이
IT 운영·관제	인프라 정기 점검 보고(정기), 장애 1차 조사(대화)	사내 APM 도구 서버(MCP)	부담 큰 수집과 쓰기 도구는 명시 요청 때만
리서치·콘텐츠	기술 조사, 백서·블로그·장표 제작(대화·칸반), 시장 리포트(정기)	위키, 칸반, 웹사이트	칸반 카드 단위 진행 확인
개인 비서	아침 브리핑, 휴가자 안내, 저녁 정리(정기), 리마인더·메모(대화·음성)	캘린더, 메일, 메신저	없음(본인 업무 기록)

표에서 마케팅·지표, 재무, 리서치·콘텐츠, 개인 비서 네 카테고리는 읽기 중심의 정기 보고가 대부분입니다. 마케팅 에이전트는 웹 분석의 트래픽·리드·캠페인 성과, 검색 콘솔의 목표 키워드, 유튜브 채널 지표를 일·주·월 단위로 모아 브랜드별 보고를 발행하고, 지표가 급변하면 알림을 보냅니다. 재무 에이전트는 원장 시트를 정해진 형식의 주간·월간 손익 보고로 요약하고, 「이번 달 미수금」 같은 질문에는 채팅으로 답합니다. 리서치·콘텐츠 에이전트는 기술 조사에서 백서·블로그·장표 제작과 발행까지를 칸반 카드로 나눠 진행하며, 시장 리포트는 하루 2~3회와 주간·월간 단위로 만듭니다. 개인 비서는 07:00 아침 브리핑, 평일 08:30 휴가자 안내, 평일 18:00

저녁 정리를 메신저로 보내고, 「내일 3시에 전화 알려줘」 같은 요청은 일회성 예약 작업으로 등록합니다. 이 네 카테고리는 사람 확인이 거의 없는 대신 결과가 제때 오지 않는 실패가 가장 큰 위험이므로, AAS Cron 헬스체크 화면의 실패·멈춤·알림 누락 표시가 운영의 중심이 됩니다.

5.4.1 영업 보고와 무활동 딜 점검을 맡는 영업 에이전트의 정기 업무

영업 에이전트는 명함 인식 외에도 영업 보고, 딜 일지, 무활동 딜 점검, 조달 공고 선별을 정기 업무로 실행합니다. 이 정기 업무들은 CRM의 영업기회 데이터를 읽어 위키에 보고서를 발행하는 구조이며, 영업기회 등록처럼 CRM에 쓰는 업무는 사람 확인을 거칩니다.

영업 에이전트의 정기 업무 일정

화면 예시의 영업 에이전트에 설정된 정기 업무와 실행 주기는 다음과 같습니다.

정기 업무	실행 시각·주기	결과
영업 보고	매일 06:50, 주간, 월간	CRM 영업기회 현황을 위키 영업 보고 페이지에 발행
보낸 메일 → 딜 일지	매일 11:00·19:00	회사 메일로 보낸 내용을 해당 딜의 위키 일지에 기록
무활동 딜 점검	일·주·월	활동 없는 딜, 마감 지난 딜, 퇴사자 담당 딜, 갱신 대상을 보고
조달 공고 선별	매일 09:00	조달 공고 알림 메일에서 사업과 맞는 공고만 골라 일일 페이지로 발행
연체 정리	분기	마감이 지난 딜을 모아 정리

무활동 딜 점검은 일정 기간 활동이 없는 딜, 마감이 지난 딜, 퇴사자가 담당하던 딜, 갱신 대상 딜을 매일 골라 보고합니다. 담당자가 바뀌거나 영업 담당이 바쁜 시기에도 딜이 기록 없이 방치되는 일을 영업 리더가 보고서에서 먼저 알 수 있습니다. 조달 공고 선별은 매일 들어오는 공공조달 알림 메일 가운데 회사 사업과 맞는 공고만 남겨 하루 한 페이지로 정리합니다.

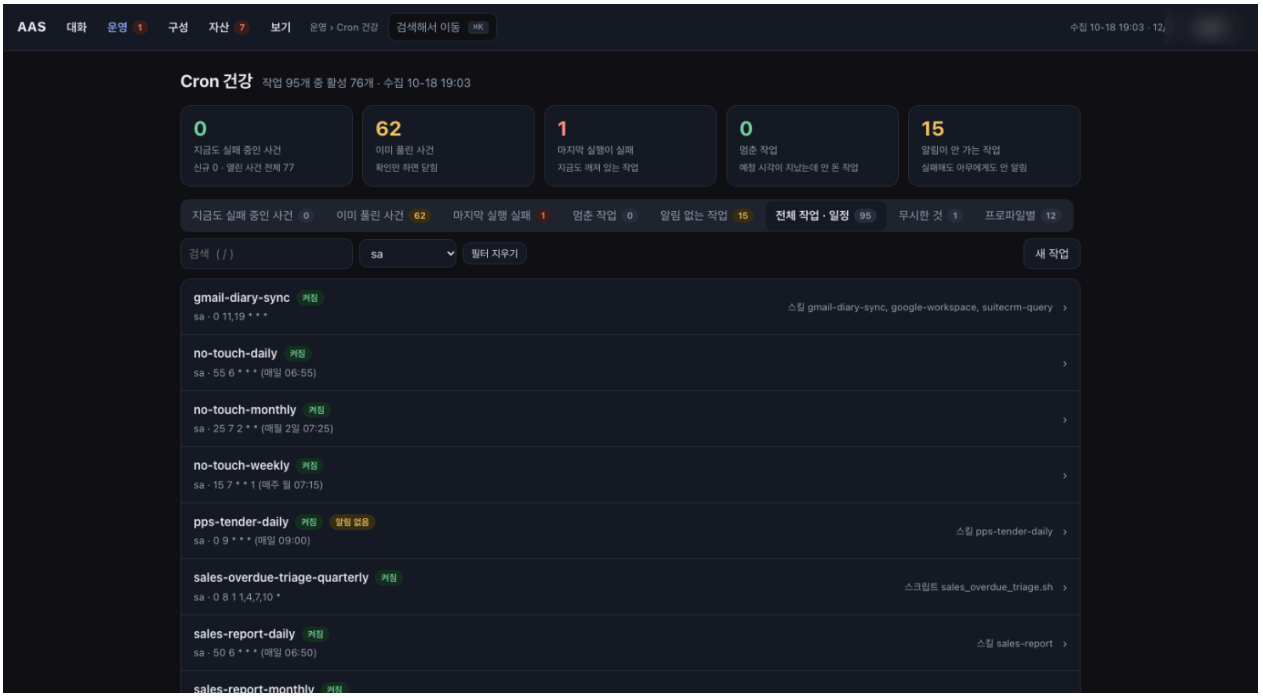


그림 5-10. Cron 헬스체크 화면의 영업 에이전트 정기 업무 목록. 딜 일지(11시·19시), 무활동 딜(일·주·월), 조달 공고 선별(09시), 연체 정리(분기), 영업 보고(06:50)가 보이며, 조달 공고 선별 작업에는 결과를 보낼 곳이 없다는 표시가 붙어 있습니다.

알림이 안 가는 작업 표시와 영업 보고 흐름

그림 5-10에서 조달 공고 선별 작업에는 알림이 안 가는 작업이라는 표시가 붙어 있습니다. 실패 알림은 그 작업에 지정한 전달 대상으로만 가므로, 전달 대상이 없는 작업은 실패해도 아무에게도 알려지지 않습니다. 그래서 Cron 헬스체크 화면은 이런 작업을 따로 표시하고, 부서 담당자는 이 표시를 보고 전달 대상을 지정할지 정합니다. 영업 보고의 흐름 화면은 일·주·월 정기 업무 3개가 영업 보고 스킬을 부르고, 스킬이 CRM MCP 도구 서버와 스크립트 6개를 거쳐 위키에 발행하는 관계를 보여 줍니다. 화면 예시에서는 최근 14일 동안 실행 20회가 기록되어 있고, 실제 실행에서 호출이 확인된 연결에는 확인 표시가 붙습니다.

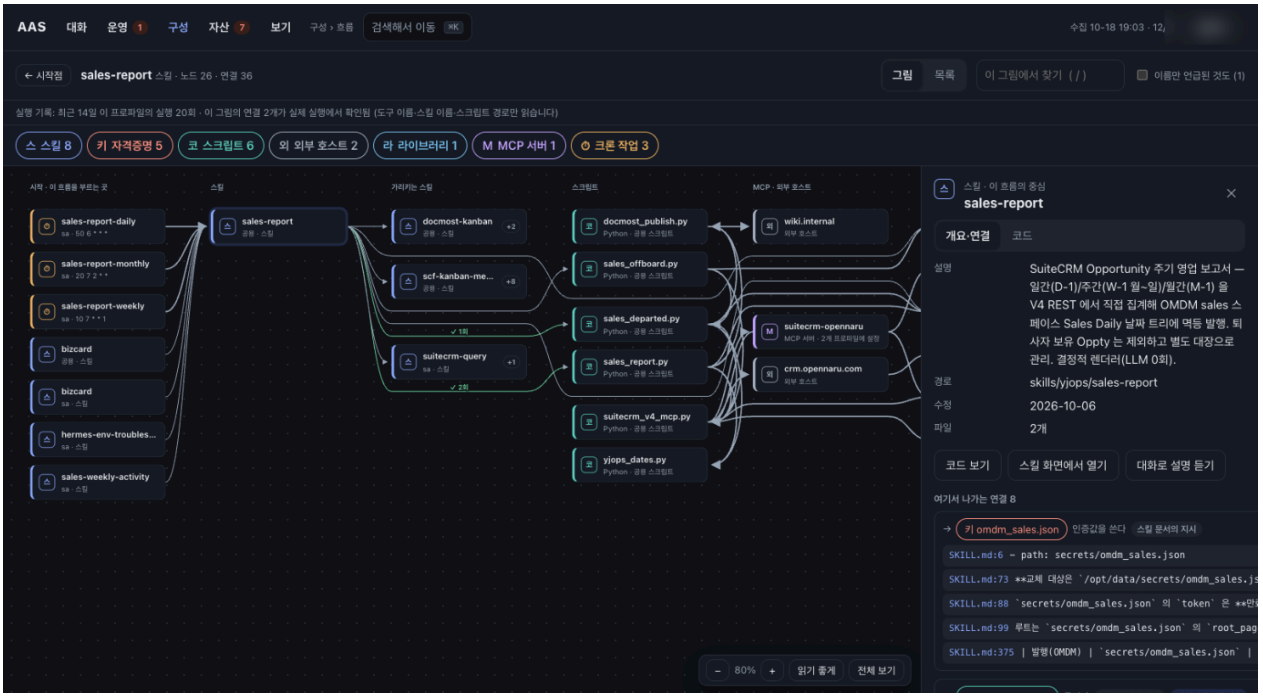


그림 5-11. 영업 보고 스킬의 흐름 화면. 정기 업무 3개(일·주·월)에서 영업 보고 스킬, CRM MCP 도구 서버와 스크립트, 위키로 이어지는 호출 관계와 실제 실행에서 확인된 연결 표시를 봅니다. 연결 시스템(CRM·위키·드라이브 등)은 고객 환경에 맞춰 설정합니다.

세 곳에 한 번에 만드는 영업기회 등록

영업기회 등록은 새 사업 이야기가 나왔을 때 같은 이름으로 드라이브 고객 폴더, CRM 고객사·영업기회, 위키 고객 일지 세 곳을 한 번에 만드는 대화형 유즈케이스입니다. 같은 요청을 다시 실행해도 이미 만든 항목은 다시 만들지 않으므로 세 시스템에 중복이 생기지 않으며, 등록 전에는 명함 인식과 같은 방식으로 사람이 예정 목록을 확인합니다. 세 시스템의 고객사 이름이 처음부터 같게 맞춰지고, 이후 영업 보고와 딜 일지가 같은 이름을 기준으로 쌓입니다. 영업 정기 업무 전체는 읽기 중심이라 사람 확인이 적고 연결 시스템이 CRM·위키·메일로 정해져 있어, 명함 인식 다음 단계로 같은 영업 에이전트에 붙여 넣히기 좋은 후보입니다.

5.4.2 판단은 사람이 내리는 이력서 1차 심사와 장애 1차 조사

인사의 이력서 1차 심사와 IT 운영의 장애 1차 조사는 에이전트가 근거를 모으고 사람이 판단하는 역할 경계가 가장 분명한 유즈케이스입니다. 두 유즈케이스 모두 결과가 사람의 채용·장애 대응 결정으로 이어지므로, 에이전트의 묶은 근거를 갖춘 1차 정리에서 멈춥니다.

이력서 1차 심사에서 에이전트가 남기는 점수와 근거

이력서 1차 심사는 매일 04:00에 실행되는 정기 업무로, 공유 드라이브에 새로 들어온 이력서를 읽어 회사 인재 기준에 따라 점수와 근거를 기록합니다. 인재 기준은 짧은 재직 기간 감점이나 자기주도성 평가 축 같은 항목을 담은 기준 파일로 관리하므로, 채용 담당자가 기준 파일을 고치면 심사 기준이 함께 바뀝니다. 채용 판단은 개인정보와 공정성 문제가 겹치는 업무라서 판단 권한을 사람에게 두는 편이 맞습니다. 서류 합격 여부는 채용 담당자가 정하며, 에이전트의 점수는 담당자가 어느 후보부터 읽을지 정하는 참고 자료입니다. 따라서 채용 담당자는 근거가 붙은 후보부터 검토하고, 기준이 맞지 않으면 기준 파일을 고쳐 다음 날 심사에 반영합니다.

사내 APM 도구 서버로 하는 인프라 점검과 장애 1차 조사

IT 운영·관제 카테고리는 사내 APM 도구 서버가 제공하는 도구 80개를 MCP로 호출합니다. APM(Application Performance Monitoring)은 애플리케이션의 응답시간과 트랜잭션 처리를 추적해 성능 문제를 찾는 관제 도구입니다. 인프라 정기 점검은 OS, 웹서버, WAS(Web Application Server, 웹 애플리케이션 서버), 응답시간, JVM(Java Virtual Machine, 자바 실행 환경) 상태를 점검해 일·주·월 보고를 발행합니다. 장애 1차 조사는 「어제 오후 3시에 응답이 느렸다」 같은 증상을 받아 그 시간대의 응답시간, 트랜잭션 추적, JVM 상태를 조사하고 원인 후보를 정리합니다. 다만 스레드 덤프처럼 대상 서버에 부담을 주는 수집은 증상과 시간대를 정한 경우에만 실행하고, 고객 제출용 확인서 발행 같은 쓰기 도구는 사람이 명시적으로 요청할 때만 호출합니다.

인사와 IT 운영 업무의 역할 경계

두 카테고리에서 에이전트와 사람의 역할은 다음과 같이 나뉩니다.

업무	에이전트가 하는 일	사람이 하는 일
이력서 1차 심사	새 이력서 읽기, 기준 파일에 따른 점수와 근거 기록	서류 합격 판단, 기준 파일 수정
인프라 정기 점검	점검 항목 수집, 일·주·월 보고 발행	보고 검토, 조치 결정
장애 1차 조사	증상·시간대에 맞춘 지표 조사, 원인 후보 정리	부담 큰 수집 승인, 원인 판단과 조치, 확인서 발행 요청

이 경계는 각 스킬 문서에 적힌 실행 조건이며, AAS 스킬 상세 화면에서 부서 담당자와 보안 담당자가 그 조건을 읽을 수 있습니다. 한편 IT 운영 카테고리에는 에이전트 자신의 운영 감시도 들어 있으며, 정기 업무 실패·멈춤·알림 누락, 자격증명 만료, 모델 설정 불일치는 AAS의 Cron 헬스체크·자격증명·모델 화면이 직접 보여 줍니다(6장).

인사·IT 운영 카테고리의 파일럿 후보 특성

이력서 1차 심사는 채용 시기에 반복량이 몰리고, 사람 확인이 최종 판단 1회이며, 연결 시스템이 공유 드라이브 1곳입니다. 장애 1차 조사는 요청 시점이 불규칙하지만 사내 APM 도구 서버 1곳에 연결하면 정기 점검과 함께 쓸 수 있습니다. 채용 공고가 잦은 조직의 인사 부서와 관제 업무가 많은 IT 운영 부서는 각자 이 두 유즈케이스를 부서 단위 파일럿 후보로 검토할 수 있습니다.

부서가 직접 늘리는 업무 에이전트 카탈로그

카탈로그의 10개 카테고리는 부서가 자기 업무를 스킬로 더해 가는 출발 목록이며, 항목 수는 부서가 스킬을 추가할 때마다 늘어납니다. 3장에서 본 폭스프로·디베이스 선례[S8]처럼, AAS의 카탈로그도 같은 방식으로 쓰도록 구성되어 있어, 부서 담당자는 기존 스킬을 고쳐 자기 부서의 서식과 일정에 맞추고 새 업무를 스킬로 추가합니다. 부서가 직접 스킬을 늘리는 방식은 업무 기능별 정착률이 낮은 문제[S4]를 부서 단위로 풀어 가는 한 가지 방법입니다. 이렇게 만든 스킬과 정기 업무는 위키·CRM·드라이브에 쌓이는 결과와 함께 조직에 남으므로, 첫 유즈케이스 하나에서 시작한 카탈로그가 부서의 업무 기록으로 이어집니다. 6장은 이렇게 늘어난 업무 에이전트가 사람이 보지 않는 동안 무엇을 했는지 드러내는 관측 화면을 다룹니다.

6장: 보이지 않던 것이 보이는 관측 화면 — 알림이 안 가는 정기 업무와 자격증명 만료

5장의 업무 에이전트 대부분은 사람이 보지 않는 시각에 정기 업무로 실행됩니다. AAS의 관측 화면은 그렇게 실행된 일을 숫자와 목록으로 드러냅니다. 정기 업무의 실패와 멈춤, 실패해도 알림이 안 가는 작업, 만료가 다가온 자격증명, 스킬이 실제로 부르는 외부 시스템이 그 대상입니다. 1장에서 본 것처럼 부족한 위험 통제는 에이전트형 AI 프로젝트가 중단되는 세 사유 가운데 하나입니다[S2]. 6장은 AAS가 그 위험 통제의 첫 단계, 즉 상태를 먼저 보이게 하는 일을 어떤 화면으로 수행하는지 운영 화면 예시로 설명하고, 제품이 드러내는 범위와 사람이 판단하는 범위를 함께 정리합니다.

6.1 지금도 실패 중인 작업과 이미 풀린 사건 62건을 나누는 Cron 헬스체크 화면

Cron 헬스체크 화면은 여러 에이전트 프로파일에 흩어진 정기 업무를 한 목록으로 모으고, 그 상태를 다섯 가지 숫자로 요약합니다. 에이전트 플랫폼 Hermes Agent는 정기 업무가 실패하면 실패 기록을 열어 두고, 사람이 확인 명령을 실행해야 그 기록을 닫습니다. 따라서 작업이 다음 실행에서 다시 성공해도 열린 실패 기록의 숫자는 줄지 않으며, 그 숫자만으로는 지금 손을 대야 하는 작업이 무엇인지 알 수 없습니다. 아래 화면 예시는 작업 95개 가운데 활성 76개를 대상으로, 열린 기록 77건 중 62건이 이미 회복된 작업의 것이고 지금도 실패 중인 기록은 0건이라는 사실을 첫 줄에서 보여 줍니다. 업무별 에이전트가 늘어나면 정기 업무와 열린 기록도 함께 늘어나, 사람이 하나씩 확인하기 어려운 규모에 이릅니다.

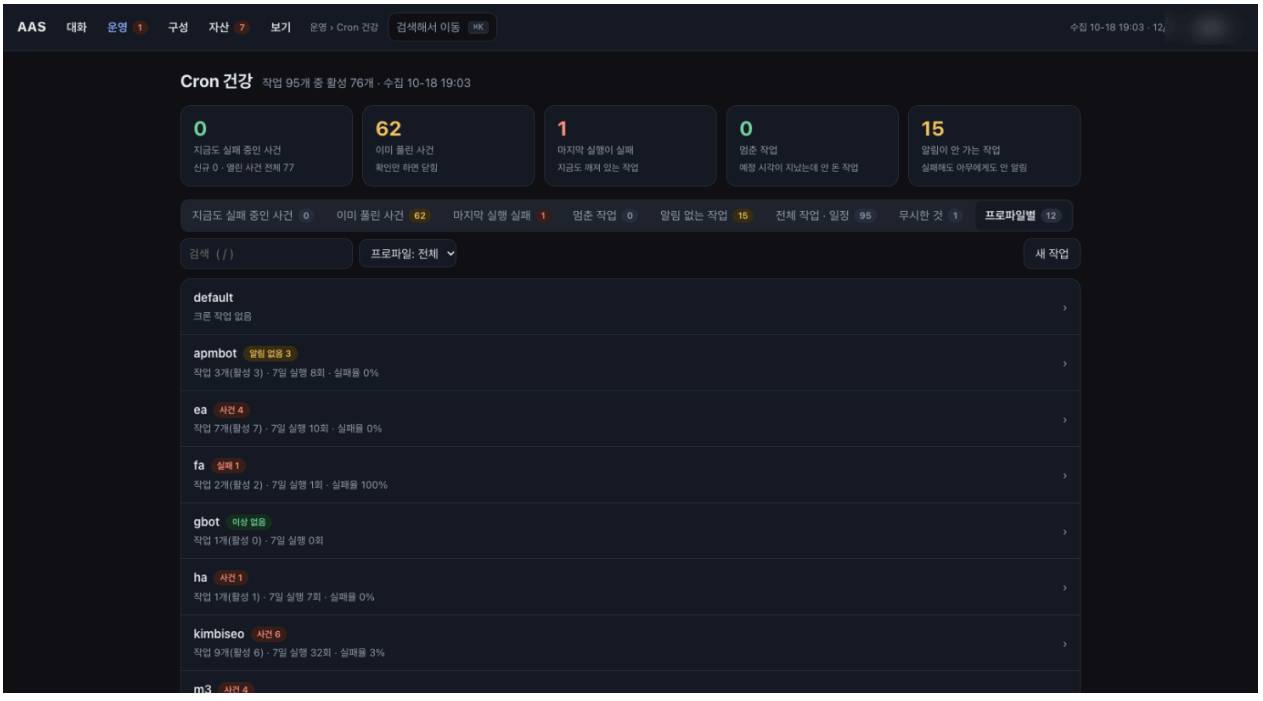


그림 6-1. Cron 헬스체크 화면의 프로파일별 보기. 위쪽 다섯 칸(지금도 실패 0 · 이미 풀림 62 · 마지막 실행 실패 1 · 멈춤 0 · 알림이 안 가는 작업 15)을 먼저 보고, 아래 각 행의 작업 수·7일 실행 수·실패율과 「알림 없음」·「실패」 표시를 봅니다.

6.1.1 회복된 사건이 현재 실패를 가리지 않게 나누는 판정 기준

열린 실패 기록의 네 갈래 구분

AAS는 열린 실패 기록과 작업의 최근 실행 결과를 함께 읽어, 지금 조치가 필요한 작업과 기록 정리만 남은 작업을 서로 다른 탭으로 나눕니다. 판정에 쓰는 정보는 플랫폼이 이미 남기는 실행 이력과 작업 설정뿐이므로, 플랫폼 쪽에 새로운 기록 장치를 추가하지 않습니다. 예를 들어 실패 기록이 열려 있더라도 같은 작업의 마지막 실행이 성공했다면 AAS는 그 기록을 「이미 풀린 사건」으로 옮기고 첫 탭의 숫자에서 뺍니다. 회복된 기록 수십 건이 쌓여 있어도 지금 실패 중인 한 건이 그 속에 묻히지 않습니다. 구분 기준은 다음 표와 같습니다.

화면 구분	판정 기준	사람이 할 일
지금도 실패 중	실패 기록이 열려 있고 그 작업의 마지막 실행도 실패	원인 조사와 조치
이미 풀린 것	실패 기록은 열려 있으나 마지막 실행은 성공	확인 명령으로 기록 정리
마지막 실행 실패	열린 기록과 관계없이 최근 실행 결과가 실패	다음 실행 전 점검
멈춘 작업	예정 시각이 지났는데 실행 기록이 없음	일정·게이트웨이 상태 확인
알림이 안 가는 작업	실패해도 결과를 전달할 대상이 없음	전달 대상 지정 여부 결정

기록을 닫는 주체는 사람

AAS는 플랫폼의 실패 기록을 대신 닫지 않습니다. 기록을 닫는 일은 플랫폼의 운영 데이터를 바꾸는 일이므로, AAS는 「이미 풀린 사건」 탭에서 닫는 데 필요한 확인 명령을 한 번에 복사할 수 있게 내어 주고 실행은 운영자에게 맡깁니다. 계속 실패하지만 당장 고칠 계획이 없는 작업은 「무시한 것」으로 따로 둘 수 있으며, 이때 누가 언제 어떤 이유로 무시했는지가 기록으로 남습니다. 무시한 작업은 요약 숫자에서 빠지지만 플랫폼에서는 그대로 실행되므로, 판단을 미뤘다는 사실 자체를 감사 추적에서 다시 볼 수 있습니다. 화면이 제시하는 것은 상태의 분류이고, 기록을 정리할지와 작업을 고칠지는 운영 책임자가 결정합니다.

못 읽은 프로파일의 별도 표시

관측 화면에서 가장 위험한 숫자는 읽지 못했는데 0으로 표시되는 숫자입니다. 이 경우 멈춘 작업을 정상으로 믿게 되기 때문에, AAS는 프로파일의 실행 이력을 읽지 못하면 0건 대신 「수집 실패」로, 이력 데이터가 오래 갱신되지 않았으면 「이력 뒤처짐」으로 화면 상단에 알립니다. 그림 6-1의 오른쪽 위 「수집 10-18 19:03 · 12/12」 표시는 12개 프로파일을 모두 읽었다는 뜻입니다. 「지금도 실패 0」이라는 숫자는 12개 프로파일을 전부 읽은 뒤의 0이고, 화면은 이 0을 읽지 못해서 생긴 0과 구분해 보여 줍니다. 숫자의 신뢰도를 화면이 스스로 밝히는 기능은 운영 판단의 전제 조건입니다.

6.1.2 프로파일별 7일 실행 수와 실패율로 보는 정기 업무 상태

프로파일 단위 집계 항목

프로파일별 탭은 같은 숫자를 프로파일 단위로 다시 나눠, 문제가 어느 업무 프로파일에 몰려 있는지 보여 줍니다. 각 행에는 등록된 작업 수와 그중 활성 작업 수, 최근 7일 동안의 실행 횟수, 실패율이 한 줄로 붙습니다. 그림 6-1의 예를 보면 작업 9개(활성 6개)를 가진 한 프로파일은 7일 동안 32회 실행에 실패율 3%이고, 작업 2개를

가진 다른 프로파일은 7일 동안 1회 실행에 실패율 100%입니다. 실행 횟수가 적은 프로파일은 실패 한 번이 곧 실패율 100%가 되므로, 실패율은 항상 실행 수와 함께 읽어야 합니다.

행마다 붙는 상태 표시

각 행의 오른쪽에는 「알림 없음 3」·「사건 4」·「실패 1」·「이상 없음」 같은 표시가 색을 달리해 붙습니다. 이 표시는 프로파일 이름을 눌러 들어가기 전에 우선순위를 정하는 데 쓰입니다. 실패율은 0%인데 「알림 없음 3」이 붙은 프로파일은 지금은 정상이지만, 다음에 실패하면 아무도 모르게 되는 작업을 세 개 갖고 있다는 뜻입니다. 반면 「사건 4」만 붙은 프로파일은 기록 정리만 남은 경우가 많아 조치 순서가 뒤로 밀립니다.

부서장이 읽는 정기 업무 상태

프로파일이 부서나 업무 에이전트 단위로 나뉘어 있으면, 이 탭은 부서장이 자기 팀 에이전트가 정해진 일을 하고 있는지 확인하는 화면으로 쓸 수 있습니다. 1장에서 본 시험과 정착의 간극[S4]을 좁혀 시험 단계를 지나 업무에 정착하려면 담당자가 아닌 사람도 에이전트의 상태를 읽을 수 있어야 하고, 프로파일별 집계는 그 요구에 맞춘 형태입니다. 다만 이 화면은 실행 결과를 보여 줄 뿐이며, 실패율이 어느 수준을 넘으면 업무를 사람에게 되돌릴지는 조직이 정합니다.

6.2 정기 업무 95개 중 알림이 안 가는 작업 15개와 공통 오류 문자열 집계

정기 업무가 실패했을 때 사람이 그 사실을 아는 방법은 알림뿐인데, 알림이 갈 곳이 정해지지 않은 작업은 실패해도 조용히 남습니다. Hermes Agent는 실패 알림을 그 작업의 전달 대상으로만 보내므로, 결과를 저장만 하도록 설정된 작업이나 전달 대상이 비어 있는 작업은 실패가 반복되어도 아무에게도 알리지 않습니다. 화면 예시에서는 정기 업무 95개 가운데 15개가 이런 상태로 목록에 올라 있습니다. 허가되지 않은 에이전트 행위의 대부분이 내부 정책 위반에서 나온다는 1장의 전망[S3]도, 감독의 출발점이 조직 안의 설정과 운영 상태라는 점을 보여 줍니다.

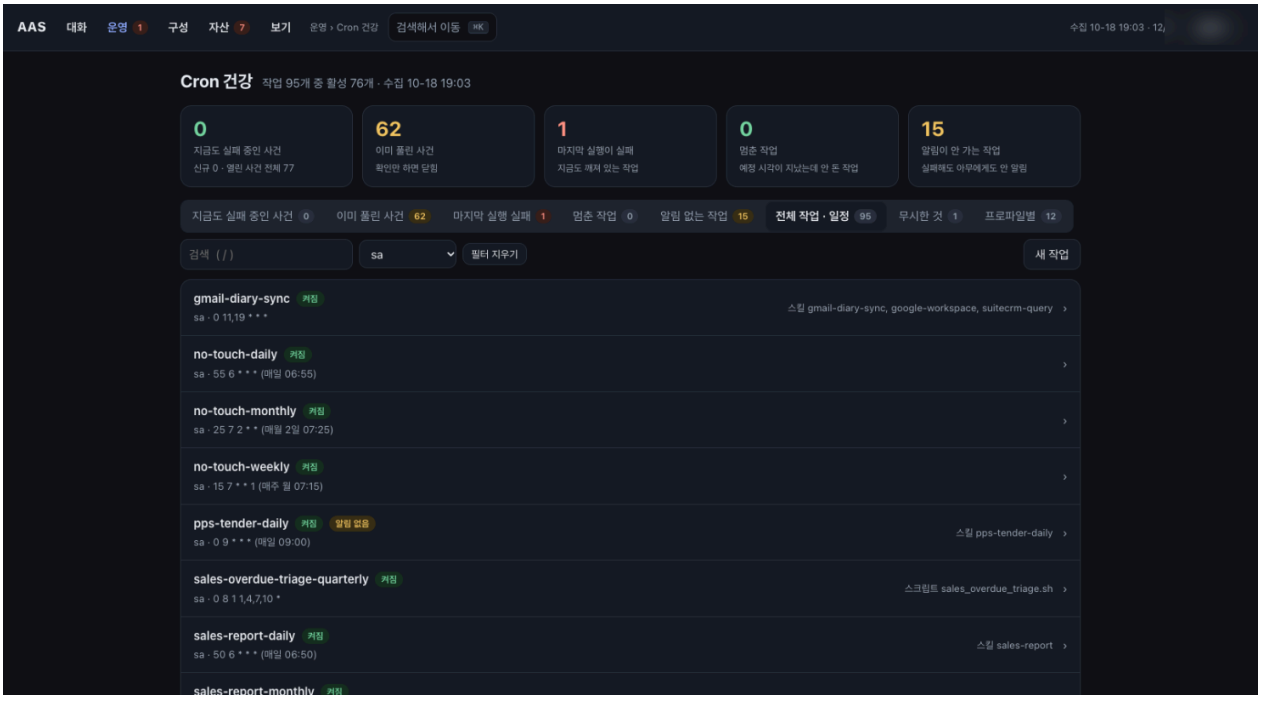


그림 6-2. 영업 에이전트의 정기 업무 목록. 각 행의 실행 주기 풀이(「매일 06:50」 등)와 오른쪽의 실행 스킬, 조달 공고 선별 작업에 붙은 「알림 없음」 표시를 봅니다. 연결 시스템(CRM·위키·드라이브 등)은 고객 환경에 맞춰

설정합니다.

6.2.1 실패해도 아무에게 전달되지 않는 정기 업무 목록

저장 전용 정기 업무에서 알림 수신자가 사라지는 경로

알림이 안 가는 작업은 흔히 작업을 만들 때의 선택에서 생깁니다. 보고서를 파일이나 위키에 저장하는 작업은 메신저로 결과를 보낼 필요가 없어 전달 대상을 비워 두는 경우가 많고, 그 결과 실패 알림의 수신자도 함께 사라집니다. 그림 6-2의 조달 공고 선별 작업은 매일 09시에 실행되지만, 작업 설정에는 실패 알림을 받을 사람이 없습니다. 이 작업이 비밀값 누락으로 멈추면 담당자는 공고 선별 결과가 며칠째 비어 있다는 사실을 업무 현장에서 뒤늦게 압니다. 실패 알림이 갈 곳이 없으면 작업이 멈춘 기간만큼 업무 공백이 쌓이고, 그 공백은 결과물을 기다리던 사람이 가장 먼저 발견합니다.

전달 대상이 없는 작업의 목록화

AAS의 「알림 없는 작업」 탭은 전달 대상이 저장 전용이거나 비어 있는 작업을 빠짐없이 모으고, 행마다 그 이유를 적습니다. 운영자는 이 목록을 보며 15개 작업 각각에 대해 지금처럼 둘지, 전달 대상을 붙일지를 결정할 수 있습니다. 작업 상세 화면에서 전달 대상을 바로 바꿀 수 있고, AAS는 이 변경을 플랫폼의 공식 API로 보내며 누가 무엇을 바꿨는지가 AAS에 기록됩니다. 다만 어떤 작업에 알림을 붙일지는 업무의 중요도에 따라 달라지므로, AAS는 목록과 이유를 제시하는 데서 멈춥니다. 알림 설정 하나도 조직이 정한 운영 정책의 일부로 관리해야 합니다.

하루 두 번 보내는 상태 요약

화면을 더 만드는 것만으로는 알림 누락이 풀리지 않습니다. 열지 않는 화면이 하나 더 늘어날 뿐이기 때문입니다. 그래서 AAS는 오전과 오후 하루 두 번, 수집 시각과 수집에 성공한 프로파일 수, 지금도 실패 중인 작업, 멈춘 작업, 알림이 안 가는 작업 수를 담은 요약을 메신저로 직접 보냅니다. 이 요약은 실패가 0건인 날에도 발송되므로, 요약이 오지 않았다는 사실 자체가 관측 경로의 이상 신호가 됩니다. 개별 작업의 알림 설정과 관계없이 운영 책임자는 하루 두 번 전체 상태를 받아 봅니다.

6.2.2 같은 오류 문자열을 한 화면에 모아 드러내는 공통 원인

여러 작업에 찍힌 같은 오류

정기 업무 여러 개가 같은 날 함께 실패하면, 원인은 개별 작업보다 공통 설정에 있을 가능성이 높습니다. 모델 게이트웨이(예: LiteLLM)의 모델 이름 변경, 만료된 토큰, 꺼진 메신저 게이트웨이처럼 여러 작업이 함께 쓰는 구성 요소가 바뀌면 작업마다 같은 오류 문자열이 남습니다. AAS는 실패한 작업들의 오류 문자열을 한 화면에 모아, 같은 문장이 몇 개 작업에 찍혔는지를 보여 줍니다. 예를 들어 같은 오류 문장이 여러 프로파일의 작업에 동시에 나타나면, 운영자는 작업을 하나씩 열지 않고도 설정 하나가 여러 정기 업무를 멈추고 있다고 의심할 수 있습니다.



그림 6-3. 여러 정기 업무의 실패 오류 문자열을 묶어 공통 원인 후보를 드러내고, 원인 판단과 조치는 운영자가 맡는 역할 경계

원인을 고치는 역할의 경계

오류 묶음 화면이 하는 일은 공통 원인의 후보를 제시하는 데까지입니다. 같은 문자열이 찍힌 작업 목록에서 출발해 어느 설정이 잘못되었는지 판단하고, 그 설정을 고치고, 다음 실행에서 회복되었는지 확인하는 일은 운영자가 합니다. 이렇게 역할을 나눈 이유는 AAS가 에이전트 플랫폼을 고치지 않는다는 설계 원칙 때문이기도 하지만, 원인 판단에는 업무 맥락이 필요하기 때문이기도 합니다. 예를 들어 같은 오류가 모델 교체 직후에 생겼다면 되돌리는 것이 맞고, 예정된 토큰 교체 중이라면 기다리는 것이 맞습니다. 2장에서 본 감독용 에이전트와 달리, AAS의 관측 화면은 판단을 대신하는 감독 기능보다 판단에 필요한 사실을 한곳에 모으는 기능에 맞춰져 있습니다.

6.3 값을 보이지 않고 자격증명 103개의 만료와 빈 값, 복사 위치를 찾는 점검

에이전트가 외부 시스템을 부르려면 API 키, 토큰, 서비스 계정 파일 같은 자격증명(Credential)이 필요하고, 에이전트와 스킬이 늘어날수록 자격증명은 설정 파일과 비밀값 파일 여러 곳에 흩어집니다. AAS의 자격증명 화면은 이 자격증명을 값 없이 이름, 위치, 쓰는 곳만으로 훑어 상태를 분류합니다. 화면 예시에서는 자격증명 103개 가운데 만료됐거나 14일 안에 만료되는 것이 7개, 이름만 있고 값이 비어 있는 것이 3개, 같은 값이 여러 곳에 복사된 것이 17개로 표시됩니다. 비밀값이 어디에 몇 벌 있는지 아는 일은 보안 담당자의 기본 점검 항목입니다.

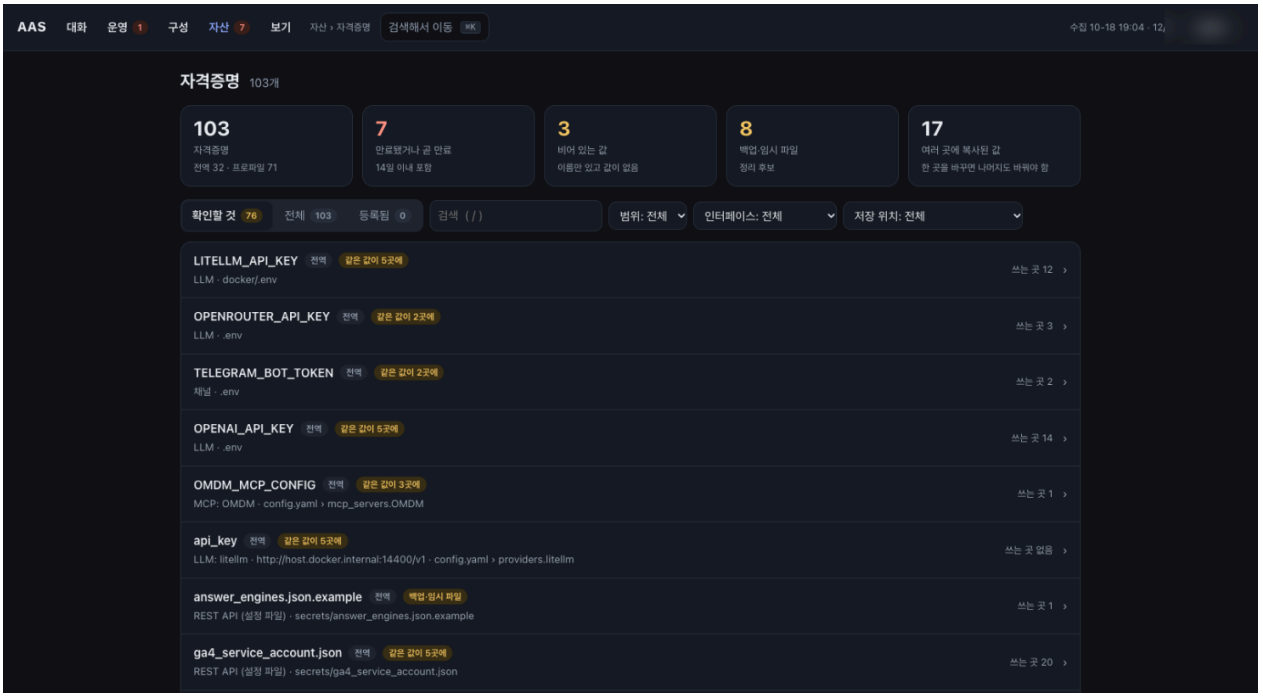


그림 6-4. 자격증명 화면. 위쪽 칸의 「만료됐거나 곧 만료 7」·「여러 곳에 복사된 값 17」과 각 행의 「같은 값이 5곳에」 표시, 오른쪽의 「쓰는 곳」 수를 봅니다. 값은 어디에도 나오지 않습니다.

6.3.1 이름과 위치, 쓰는 곳만으로 점검하는 자격증명 상태

값을 수집하지 않는 판정 방식

AAS는 자격증명의 값을 화면, 로그, 기록 어디에도 남기지 않는다는 원칙에 따라 상태를 판정합니다. 만료일은 토큰 안에 들어 있는 만료 정보를 읽어 계산하고, 중복은 값의 해시를 비교해 판정하고 「같은 값이 N곳에」라는 그룹 정보로만 알립니다. 따라서 화면을 보는 사람은 어떤 토큰이 다섯 곳에 복사되어 있는지는 알 수 있지만, 그 토큰의 값은 볼 수 없습니다. 이 방식 덕분에 보안 담당자와 부서장이 함께 화면을 보더라도 비밀값이 새로 노출되지 않습니다. 정보 과다 공유가 허가되지 않은 에이전트 행위의 대표 유형으로 꼽히는 만큼[S3], 점검 화면이 또 하나의 노출 경로가 되지 않도록 설계한 것입니다.

상태 분류와 확인 대상

화면은 자격증명을 범위(전역·프로파일), 인터페이스(MCP·채널·LLM 등), 저장 위치로 거를 수 있고, 위쪽 칸의 상태별 숫자가 그대로 확인 대상 목록이 됩니다. 화면 예시에서 103개 중 확인이 필요한 항목은 76개로 표시되며, 분류 기준은 다음과 같습니다.

상태	화면 예시 수	판정 근거	확인할 내용
만료됐거나 곧 만료	7	토큰의 만료 정보, 14일 이내 포함	교체 일정과 담당자
비어 있는 값	3	이름은 있으나 값이 없음	해당 작업의 실행 가능 여부
백업·임시 파일	8	파일 이름 형식	정리 대상 여부
여러 곳에 복사된 값	17	값 해시 비교	교체 시 함께 바꿀 위치

빈 값이 만드는 조용한 멈춤

비어 있는 값은 숫자로는 작아 보이지만, 운영 영향은 만료보다 클 수 있습니다. 메신저 게이트웨이나 외부 서비스 연결에 필요한 비밀값이 비어 있으면 그 프로파일의 정기 업무가 아예 실행되지 않고, 앞 절의 알림 누락과 겹치면 아무도 모르는 채로 오래 멈춰 있게 됩니다. 그래서 AAS는 빈 값을 별도 칸으로 세고, 첫 화면 「오늘 볼 것」에도 만료됐거나 곧 만료되는 자격증명을 따로 묶어 보여 줍니다. 각 항목에는 상태(등록됨·검토 필요·폐기 예정), 담당, 메모를 AAS 쪽에 적어 둘 수 있으므로, 점검 결과가 사람에게 할당된 일로 이어집니다.

6.3.2 토큰 교체 전에 멈출 스킬과 정기 업무를 미리 찾는 영향 범위 확인

토큰 하나를 쓰는 곳의 역추적

토큰을 교체하거나 유출이 의심될 때 가장 먼저 필요한 정보는 그 토큰을 쓰는 스킬과 정기 업무의 목록입니다. 업무별 에이전트가 늘어날수록 토큰 하나를 공유하는 스킬의 수도 늘어나므로, 이 목록 없이 토큰을 바꾸면 어느 업무가 멈출지 예측하기 어렵습니다. AAS의 자격증명 상세 서랍은 범위, 인터페이스, 저장 파일, 만료일 아래에 「같은 값이 있는 곳」과 「쓰는 곳」을 스크립트 이름으로 이어서 보여 줍니다. 예를 들어 그림 6-4의 모델 게이트웨이 키 행에는 「같은 값이 5곳에」와 「쓰는 곳 12」가 붙어 있으며, 이 키를 바꾸면 다섯 군데의 설정과 열두 개의 스크립트를 함께 확인해야 한다는 뜻입니다. 운영자는 값을 한 번도 보지 않고 교체 작업의 영향 범위를 미리 정할 수 있습니다.

교체 전 확인 순서

영향 범위 확인은 다음 순서로 진행합니다.

- 자격증명 화면에서 교체할 토큰을 열고 만료일과 「같은 값이 N곳에」를 확인합니다.
- 「쓰는 곳」 목록에서 그 토큰을 쓰는 스크립트와 스킬을 확인하고, 흐름 화면으로 넘어가 그 스킬을 실행하는 정기 업무를 찾습니다.
- 교체 시각 동안 실행될 정기 업무를 미리 일시정지하거나, 교체 직후 다음 실행 결과를 Cron 헬스체크 화면에서 확인합니다.

쓰는 곳 표시의 한계

「쓰는 곳」은 스크립트와 설정에 적힌 이름을 맞춰 보는 방식이 섞여 있어, 실제로는 쓰지 않는 곳이 목록에 들어가는 경우가 있습니다. 비밀값 폴더의 파일이나 컨테이너 전역 환경 변수는 AAS 화면에서 바꿀 수 없고, 토큰 교체와 회전을 자동으로 수행하는 기능도 없습니다. 따라서 이 화면은 교체 작업을 대신하지 않고, 교체 전에 영향받는 범위를 좁혀 주는 점검 도구로 쓰는 것이 맞습니다. 교체 자체와 그 결과에 대한 책임은 IT·플랫폼 관리자에게 남습니다.

6.4 스킬 문서와 실행 기록에서 뽑은 호출 관계 그림과 선마다 붙는 근거 줄

감사 담당자가 에이전트에 대해 묻는 첫 질문은 「이 에이전트가 무엇을 부르는가」이지만, 스킬이 수백 개로 늘어나면 스킬 문서와 스크립트를 하나씩 열어서는 답할 수 없습니다. AAS의 흐름 화면은 스킬 문서, 스크립트, 정기 업무 설정, 실행 기록에서 호출 관계를 뽑아 그림으로 그리고, 그림의 선마다 그 관계를 읽어 낸 파일과 줄을 붙입니다. 사람이 그린 흐름도는 시간이 지나면 실제와 어긋나기 시작하므로, AAS는 그림을 저장해 두지 않고 원천 파일에서 주기적으로 다시 만듭니다. 호출 관계의 근거를 파일 단위로 보여 주는 기능은 감사 추적의 출발점이 됩니다.

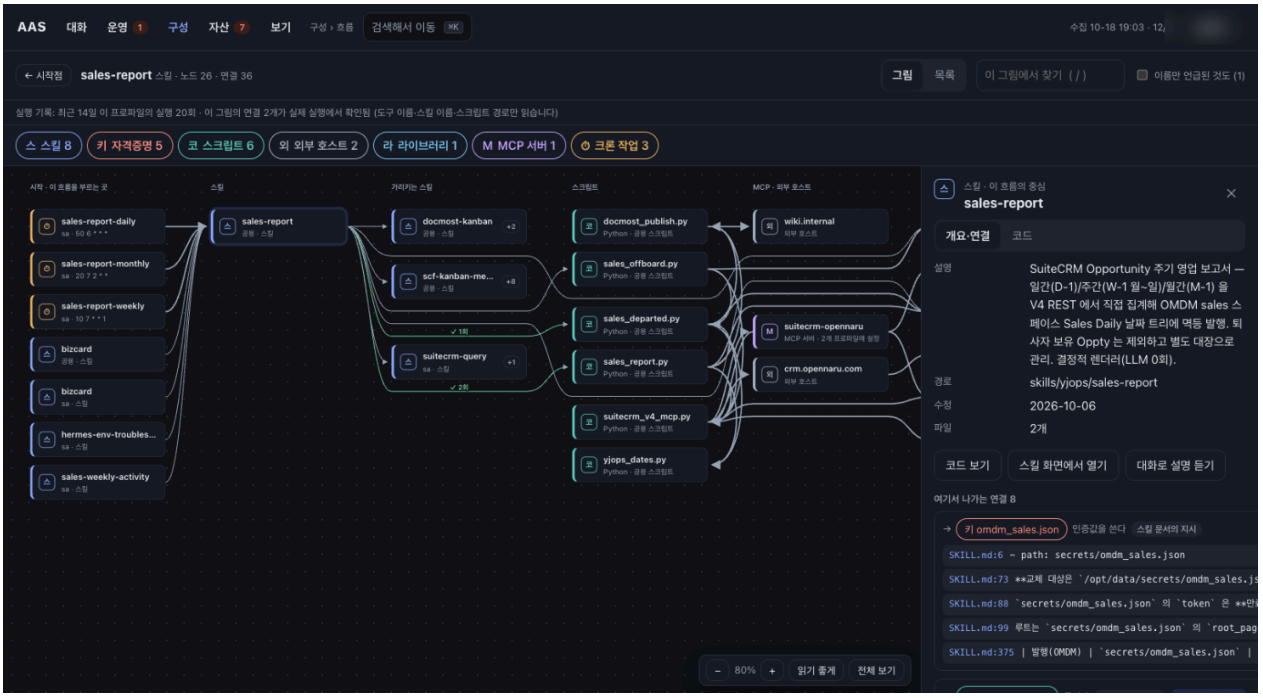


그림 6-5. 영업 보고 스킬의 호출 관계 그림. 위쪽 띠의 종류별 개수(스킬 8 · 자격증명 5 · 스크립트 6 · 외부 호스트 2 · MCP 서버 1 · 정기 업무 3), 초록색 「1회」·「2회」 표시가 붙은 실제 실행 확인 연결, 오른쪽 칸의 근거 줄을 봅니다. 연결 시스템(CRM·위키·드라이브 등)은 고객 환경에 맞춰 설정합니다.

6.4.1 스킬에서 외부 호스트까지 자동으로 그려지는 호출 관계

그림의 원천과 그리는 규칙

흐름 그림은 왼쪽에서 오른쪽으로 「시작(정기 업무 또는 다른 스킬) → 스킬 → 가리키는 스킬 → 스크립트 → MCP 서버·외부 호스트」 순서로 배치됩니다. 그림에서는 MCP 서버가 별도 노드로 표시됩니다. 원천은 정기 업무 설정, 스킬 문서, 스크립트 코드, 최근 실행 기록 네 가지이고, AAS는 이 파일들에서 도구 이름, 스킬 이름, 스크립트 경로만 읽습니다. 예를 들어 그림 6-5의 영업 보고 스킬은 일간·주간·월간 정기 업무 3개에서 시작해 스크립트 6개를 거쳐 CRM용 MCP 서버 1개와 외부 호스트 2곳에 닿고, 그 과정에서 자격증명 5개를 씁니다.

구성 요소와 확인 방법

그림의 구성 요소는 다음과 같으며, 노드를 누르면 오른쪽 칸에 일정, 마지막 결과, 전달 대상 같은 상세 정보와 「여기서 나가는 연결」이 근거 줄과 함께 나옵니다.

구성 요소	그림에서의 의미	감사에서의 쓰임
정기 업무	흐름을 시작하는 자동 실행 일정	언제 자동 실행되는가
스킬	업무 절차를 적은 문서	무엇을 하도록 지시받았는가
스크립트	스킬이 실행하는 코드	실제로 무엇을 실행하는가
MCP 서버·외부 호스트	호출 대상 시스템	어디로 데이터가 나가는가
자격증명	호출에 쓰는 인증 정보	어떤 권한으로 부르는가

역방향 질문에 대한 답

흐름 화면은 한 스킬에서 출발하는 정방향 질문뿐 아니라 「이 외부 시스템을 부르는 스킬이 전부 무엇인가」 같은 역방향 질문에도 답합니다. 그림 6-5의 왼쪽 열 「이 흐름을 부르는 곳」에는 영업 보고 스킬을 부르는 다른 스킬들이 함께 나열됩니다. 외부 시스템 하나의 주소가 바뀌거나 계약이 끝날 때, 영향받는 스킬과 정기 업무를 파일을 뒤지지 않고 찾을 수 있습니다. 다만 변수로 조립되는 주소나 스크립트가 다시 부르는 다른 스크립트는 그림에서 빠질 수 있으므로, 중요한 시스템은 근거 줄에서 코드를 열어 직접 확인하는 것이 안전합니다.

6.4.2 실제 실행에서 확인된 연결과 「수집 실패」 표시의 구분

선마다 붙는 확실한 정도

흐름 그림의 선은 모두 같은 무게가 아닙니다. AAS는 각 선에 근거 파일과 줄 번호를 붙이고, 그 관계를 어떻게 알았는지에 따라 확실한 정도를 다섯 가지로 표시합니다. 이 구분이 있어야 감사 담당자가 어떤 연결은 실행으로 확인되었고 어떤 연결은 문서에 이름만 나왔는지를 가려 읽을 수 있습니다.

표시	뜻
크론 설정	정기 업무 설정 파일에 그 스킬을 실행하도록 적혀 있음
코드에서 확인	스크립트 코드에서 호출이 확인됨
스킬 문서의 지시	스킬 문서가 그 도구나 파일을 쓰라고 지시함
이름만 언급	문서에 이름만 나옴(기본 화면에서는 숨김)
실행에서만 보임	정적 분석에는 없고 실행 기록에서만 나타남

실행 기록으로 확인된 연결

그림 6-5의 상단 안내 줄은 「최근 14일 이 프로파일의 실행 20회 · 이 그림의 연결 2개가 실제 실행에서 확인됨」이라고 적고, 해당 선에는 초록색으로 실행 횟수가 붙습니다. 문서와 코드에서 읽어 낸 연결 가운데 어느 것이 최근에 실제로 쓰였는지가 그림 위에 겹쳐 표시됩니다. 감사 담당자는 실행 확인 표시가 붙은 선을 먼저 보고, 오랫동안 실행되지 않은 연결은 정리 대상으로 분류할 수 있습니다. 에이전트를 시험 단계에서 업무로 넓히려는 조직은 이런 근거 자료를 보안·감사 검토의 참고 자료로 쓸 수 있습니다. 다만 에이전트를 거치지 않고 스크립트만 실행되는 작업은 세션 기록이 남지 않으므로, 실행 확인 표시가 없다는 사실이 곧 쓰이지 않는다는 뜻은 아닙니다.

못 읽은 것을 0건으로 쓰지 않는 원칙

흐름 그림과 Cron 헬스체크 화면은 같은 원칙을 따릅니다. 프로파일이나 파일을 읽지 못하면 결과를 0건으로 표시하지 않고 「수집 실패」로 알리며, 그림의 연결 수가 적은 이유가 실제로 적어서인지 읽지 못해서인지를 화면이 스스로 밝힙니다. 감사 보고서에 흐름 그림을 근거로 첨부할 때, 그 그림이 어디까지를 읽고 그린 것인지가 함께 남습니다. 부족한 위험 통제가 에이전트형 AI 프로젝트 중단의 이유로 꼽히는 만큼[S2], 위험 통제의 근거 자료에는 읽은 범위가 함께 남아야 합니다. 이 장에서 본 화면은 모두 같은 역할 경계 위에 있습니다. AAS는 실패, 알림 누락, 자격증명 상태, 호출 관계를 먼저 보이게 하고, 그 사실을 근거로 원인을 판단하고 고치는 일은 업무를 아는 담당자와 운영 책임자가 맡습니다. 이 관측이 플랫폼을 고치지 않고 어떤 구조로 이뤄지고 어떤 보안 원칙을 지키는지는 7장에서 다룹니다.

7장: 쓰던 에이전트 플랫폼을 고치지 않고 조직 안에서 구동되는 온프레미스 설치와 보안 원칙

6장에서 본 관측이 가능한 것은 AAS가 쓰던 에이전트 플랫폼 위에 그대로 얹히는 구조이기 때문입니다. AAS는 이미 운영 중인 에이전트 플랫폼 위에 연결하는 콘솔이며, 지금 연결되는 에이전트 플랫폼은 오픈소스 Hermes Agent 한 종류입니다. 에이전트가 업무 애플리케이션 곳곳에 들어오면서[S1], 에이전트를 운영하는 플랫폼은 곧 조직의 업무 시스템 목록에 오르게 됩니다. 콘솔을 도입하는 조직의 IT·보안 담당이 먼저 묻는 것은 세 가지로 모입니다. 도입하면 운영 중인 플랫폼의 플러그인이나 설정을 바꿔야 하는지, 업무 자료가 조직 밖으로 나가는지, 플랫폼에 들어 있는 토큰과 키가 콘솔 화면이나 로그에 드러나는지가 그것입니다. 생성형 AI 활용을 넓히려는 공공 부문의 망 보안 제도 개편이 2024년부터 이어지고 있으므로[S6], 이 세 질문에 대한 답은 도입 검토 회의에서 기술 사양과 같은 무게를 가집니다. 이 장은 AAS가 플랫폼에 연결되는 구조, 그 구조의 예외 두 가지, 조직 안에서 완결되는 온프레미스 설치 구성, 보안 검토표에 옮겨 쓸 수 있는 설계 원칙 다섯 가지를 차례로 정리하므로, 보안 담당은 이 장만으로 세 질문의 답과 확인 방법을 함께 얻을 수 있습니다.

7.1 읽기 전용 수집과 플랫폼 공식 API 단일 변경 경로로 나눈 연결 구조

AAS는 에이전트 플랫폼에 닿는 경로를 둘로 나눕니다. 화면에 보여 줄 정보를 모으는 읽기 경로는 플랫폼의 데이터 폴더를 읽기 전용으로만 열고, 정기 업무나 스킬 문서를 바꾸는 변경 경로는 전부 플랫폼이 공식으로 제공하는 대시보드 API 하나로 보냅니다. 따라서 AAS를 도입해도 플랫폼의 플러그인을 설치하거나 설정 파일을 고치거나 버전을 올릴 일이 생기지 않으며, 운영 중인 정기 업무와 에이전트를 멈추지 않고 콘솔을 붙일 수 있습니다. 이 구조는 「도입하면 기존 플랫폼을 손대야 하는가」라는, IT 담당이 가장 먼저 묻는 질문에 대한 직접적인 답이기도 합니다.

두 경로를 나눈 이유는 플랫폼이 스스로 하는 검사를 건너뛰지 않기 위해서입니다. 콘솔이 플랫폼의 파일을 직접 고치면 플랫폼의 입력 검사를 거치지 않게 되고, 플랫폼이 다음 판에서 파일 구조를 바꾸면 콘솔이 운영 데이터를 망가뜨릴 수 있습니다. 반면 공식 API로 요청을 보내면 플랫폼이 직접 검사하고 저장하며, 요청이 거절되면 플랫폼이 낸 거절 문구가 AAS 화면에 그대로 나타납니다. AAS는 플랫폼의 규칙을 대신 판단하지 않고, 플랫폼이 허용한 변경만 사람에게 전달합니다.

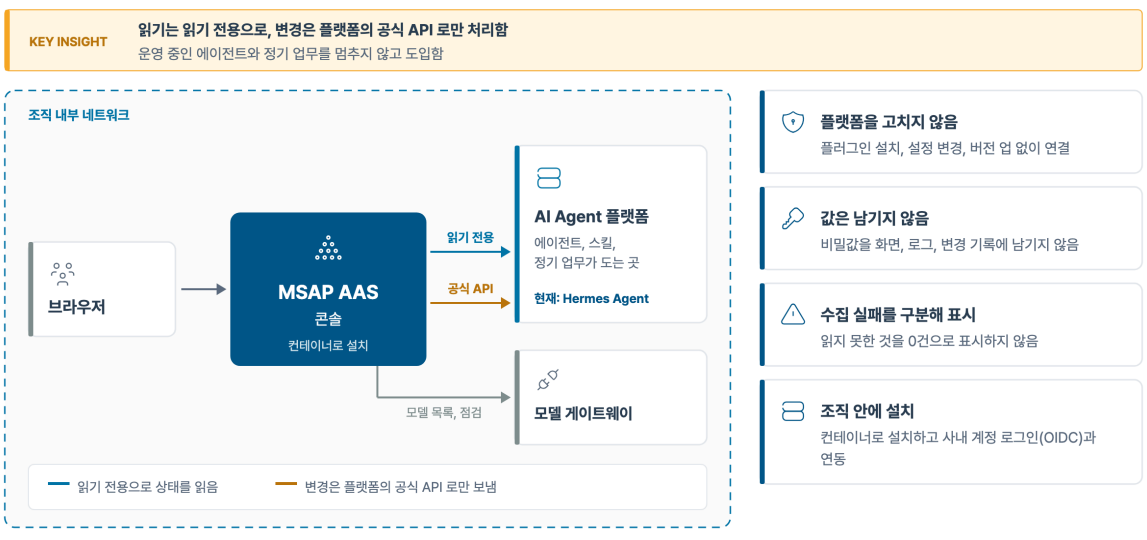


그림 7-1. AAS가 에이전트 플랫폼에 닿는 두 경로 — 읽기 전용 수집과 공식 API 변경

두 경로에 주어진 권한을 표로 나누면 다음과 같습니다. 콘솔 컨테이너 자체에는 플랫폼 데이터에 대한 쓰기 권한이 없으며, 호스트의 컨테이너 엔진을 조작할 수 있는 소켓도 연결하지 않고 일반 사용자 권한으로 실행됩니다.

경로	대상	권한	방식
읽기 경로	정기 업무 정의, 실행 이력, 스킬 파일, 프로파일 설정, 세션 집계	읽기만	데이터 폴더를 읽기 전용으로 연결, 실행 이력 DB도 변경 불가 모드로 열기
변경 경로	정기 업무, 스킬 문서, 프로파일, 비밀값 넣기	플랫폼이 허용한 변경만	플랫폼 대시보드의 공식 API
모델 점검	모델 목록, 모델별 응답 여부	읽기	조직 안 모델 게이트웨이 (LiteLLM)
콘솔 자체 저장소	판 관리, 변경 기록, 무시 목록, 권한	읽기·쓰기	AAS 전용 DB

7.1.1 플러그인과 설정, 버전을 바꾸지 않는 읽기 전용 수집 경로

읽기 경로가 다루는 플랫폼 정보

AAS의 읽기 경로는 에이전트 플랫폼이 이미 디스크에 남기고 있는 정보를 읽기 전용으로 가져옵니다. 대상은 프로파일별 정기 업무 정의, 실행 이력과 실패 기록, 공용·프로파일별 스킬 파일, 프로파일 설정, 세션 집계 다섯 가지입니다. 이 정보를 읽으려고 플랫폼에 수집용 플러그인을 넣거나 로그 전송 설정을 추가하지 않으며, 데이터 폴더를 콘솔 컨테이너에 읽기 전용으로 연결하면 AAS가 바로 수집을 시작합니다. IT 담당이 플랫폼 쪽에서 준비할 일은 데이터 폴더의 위치를 알려 주는 것 하나로 줄어듭니다.

읽는 대상	AAS 화면에서 쓰는 곳	읽지 않는 것
정기 업무 정의	정기 업무 목록, 알림이 안 가는 작업 찾기	—
실행 이력·실패 기록	Cron 헬스체크, 지금도 실패/이미 풀림 구분	—
스킬 파일	스킬 목록, 흐름 그림의 호출 관계	—
프로파일 설정	모델·게이트웨이 상태, 자격증명 상태	비밀값의 값
세션 기록	활동 집계, 실제 호출한 도구·스킬 이름	대화 내용, 호출 인자 값

세션 기록에서 대화 내용을 읽지 않는 이유

세션 기록에는 에이전트가 실제로 부른 도구와 스킬의 이름이 있지만, 같은 기록 안에 사용자의 대화 내용과 호출 인자도 함께 들어 있습니다. 대화와 인자에는 개인 정보와 비밀값이 섞일 수 있으므로, AAS는 세션 기록에서

집계 항목과 도구 이름, 스킬 이름, 명령 속 스크립트 경로만 읽고 대화 본문과 인자 값은 읽지 않습니다. 예를 들어 활동 화면은 어떤 프로파일이 하루에 몇 번 실행됐는지와 어떤 스킬을 불렀는지는 보여 주지만, 사용자가 에이전트에게 무엇을 물었는지는 보여 주지 않습니다. 이 제한 덕분에 운영 관측과 개인 정보 보호를 따로 협상하지 않아도 됩니다.

플랫폼 버전이 올라갈 때의 읽기 경로 동작

플랫폼의 파일과 DB 구조를 아는 코드는 AAS 안에서 한 모듈에만 모여 있으며, 현재 기준 버전은 Hermes Agent v0.21.0입니다. 플랫폼을 새 판으로 올린 뒤 기대하던 항목이 사라졌다면 AAS는 그 프로파일을 0건으로 세지 않고 「수집 실패」로 표시합니다. 이 표시 덕분에 플랫폼 업그레이드가 AAS를 조용히 틀리게 만드는 일은 없고, 운영자는 점검 명령 한 번으로 프로파일별 수집 상태를 확인한 뒤 화면을 믿을지 판단할 수 있습니다. 다만 실행 이력 DB를 변경 불가 모드로 여는 방식에는 한계가 있어, 플랫폼이 아직 본 파일에 반영하지 않은 최신 기록을 놓칠 수 있으며 이때는 「실행 이력이 최신이 아닐 수 있습니다」라는 안내를 함께 띄웁니다.

7.1.2 모든 변경을 플랫폼 공식 API로 보내고 변경 기록을 남기는 경로

변경 요청이 플랫폼에 도달하는 순서

AAS에서 담당자가 정기 업무 주기를 바꾸거나 스킬 문서를 고치면, AAS 서버가 그 요청을 플랫폼 대시보드의 공식 API로 전달합니다. 공식 API로 바꿀 수 있는 대상은 정기 업무(만들기·삭제·주기·전달 대상·켜기와 끄기·즉시 실행), 스킬 문서, 프로파일(만들기·이름 바꾸기·내보내기·가져오기·삭제, 소개·성격·설정·모델·게이트웨이·도구 묶음), 비밀값 넣기입니다. 공식 API에 저장 기능이 없는 대상은 AAS에서도 바꿀 수 없으며, 스킬에 딸린 스크립트가 대표적인 예로 AAS 화면에서는 보기만 가능합니다. AAS가 할 수 있는 변경의 범위는 플랫폼이 공식으로 열어 둔 범위와 정확히 같습니다. 에이전트를 추가하거나 지우는 작업은 플랫폼 안의 설정을 바꾸는 일이 아니라 조직의 인프라 위에 사용자별 실행 환경을 새로 띄우거나 정리하는 일이므로, 이때도 에이전트 플랫폼의 코드와 설정은 바뀌지 않습니다.

바꾸는 요청에 붙는 공통 통제

변경 요청에는 경로와 관계없이 같은 통제가 붙습니다. 바꿀 수 있는 범위는 역할로 나뉩니다. 부서 담당자는 자기 에이전트 안에서 프로파일을 만들고 지우며 스킬 문서와 정기 업무를 고치고 마켓 패키지를 설치할 수 있고, 사람별 에이전트 개수 한도처럼 조직 전체에 걸린 설정은 관리자만 바꿉니다. 요청은 전용 헤더와 같은 출처 확인을 통과해야 하며, AAS가 허용한 형태의 요청만 플랫폼에 넘어갑니다. 모든 변경은 누가 언제 무엇을 바꿨는지 AAS의 변경 기록에 남고, 스킬 문서는 판 관리가 함께 이루어져 바뀌기 전 내용과 비교하거나 되돌릴 수 있습니다. 감사 담당에게 필요한 「변경 추적」이 플랫폼을 고치지 않고 콘솔 쪽에서 확보되는 셈입니다.

변경 기록 항목	남는 내용	남기지 않는 내용
누가	로그인한 사용자	—
언제	요청 시각	—
무엇을	대상 프로파일, 정기 업무·스킬·설정·비밀값의 이름	비밀값의 값
어떻게	변경 종류(만들기·고치기·삭제·실행)	—
결과	플랫폼의 수락 또는 거절 문구	—

변경 기록이 덮지 못하는 범위

AAS의 변경 기록에는 AAS를 거친 변경만 남습니다. 운영자가 플랫폼 대시보드나 명령줄 도구로 직접 바꾼 내용은 AAS가 알 수 없으므로, 감사 범위를 정할 때는 플랫폼 쪽 접근 권한을 함께 좁혀 두는 편이 맞습니다. 예를 들어 부서 담당자에게는 AAS 계정만 주고 플랫폼 대시보드와 서버 접속은 IT 관리자에게만 열어 두면, 일상적인 변경은 모두 AAS 기록으로 모입니다. 이 한계를 처음부터 밝혀 두는 이유는 변경 기록이 전부를 덮는다고 믿고 감사 계획을 세우면 기록 밖의 변경이 검토에서 빠지기 때문입니다.

7.2 공식 API에 길이 없는 마켓 패키지 설치와 삭제의 예외 처리 범위

「에이전트 플랫폼을 고치지 않는다」는 원칙에는 예외가 정확히 두 가지 있으며, 둘 다 사내 스킬 마켓에서 받은 패키지를 다루는 기능입니다. 플랫폼 대시보드의 공식 API에 패키지 설치 기능과 스킬 패키지 삭제 기능이 없기 때문에, 이 두 경우만 별도 도우미가 맡습니다. 예외를 먼저 밝혀야 「고치지 않는다」는 주장이 기술적으로 정확해지고, 보안 담당도 예외의 권한 범위를 따로 검토할 수 있습니다. AAS는 이 두 예외를 숨기지 않고 화면과 제품 문서에 적어 둡니다.

7.2.1 별도 도우미가 플랫폼 명령으로 처리하는 예외 두 가지

패키지 설치를 플랫폼 명령으로 처리하는 예외

첫 번째 예외는 사내 스킬 마켓에서 고른 패키지를 에이전트 프로파일에 설치하는 기능입니다. 플랫폼 대시보드에는 사내 마켓 주소에서 패키지를 받아 설치하는 공식 API가 없으므로, AAS는 설치 요청을 대기열에 남기기만 하고 실제 설치는 호스트에서 실행되는 마켓 도우미가 처리합니다. 도우미는 30초마다 대기열을 확인해 사내 마켓 서버에서 요청된 판을 받고, 파일마다 해시를 대조한 다음 플랫폼 자신의 설치 명령으로 프로파일에 설치합니다. 이 구조에서 프로파일에 파일을 쓰는 주체는 끝까지 플랫폼이며, AAS 컨테이너는 플랫폼 데이터를 쓰지 않습니다.

스킬 패키지 삭제를 폴더 하나로 제한한 예외

두 번째 예외는 마켓에서 설치한 스킬 패키지를 지우는 기능입니다. 플랫폼에는 이 방식으로 설치한 스킬을 지우는 명령이 없으므로, 도우미가 플랫폼 컨테이너 안에서 마켓 전용 스킬 폴더 하나를 직접 삭제합니다. 이것이 AAS 쪽 구성 요소가 플랫폼 폴더를 직접 건드리는 유일한 경우이며, 그래서 삭제 조건을 좁게 걸어 두었습니다. 지울 수 있는 것은 AAS가 설치했다고 기록한 패키지뿐이고, 그 폴더가 실제 폴더이면서 스킬 문서를 담고 있을 때만 도우미가 삭제합니다.

예외	공식 API로 못 하는 이유	처리 주체	플랫폼에 쓰는 것
마켓 패키지 설치	대시보드에 사내 마켓 설치 기능이 없음	호스트의 마켓 도우미	플랫폼 자신의 설치 명령
마켓 스킬 패키지 삭제	플랫폼에 해당 삭제 명령이 없음	같은 도우미	마켓 전용 스킬 폴더 하나 삭제

7.2.2 예외 도우미의 권한을 좁혀 화면과 문서에 밝히는 방식

도우미 권한을 좁힌 세 가지 장치

마켓 도우미는 콘솔 컨테이너 밖에서 실행되지만, 손댈 수 있는 대상을 세 가지 장치로 제한합니다. 도우미는 등록부에 이름이 오른 플랫폼 컨테이너만 다루므로 같은 호스트의 다른 컨테이너에는 접근하지 않습니다. 설치 기록의 정본은 AAS 쪽에 남아 있어 어떤 패키지가 언제 어느 프로파일에 들어갔는지를 AAS 화면에서 추적할 수 있고, 삭제 대상도 이 기록에 있는 것뿐입니다. 콘솔 컨테이너에는 컨테이너 엔진 소켓을 주지 않았기 때문에, 콘솔이 침해되더라도 그 권한으로 호스트 전체를 조작할 수는 없습니다.

권한 항목	콘솔 컨테이너	마켓 도우미
플랫폼 데이터 쓰기	없음	설치는 플랫폼 명령으로만, 삭제는 기록된 폴더 하나
컨테이너 엔진 소켓	없음	등록된 플랫폼 컨테이너에 한정
다루는 패키지	설치 요청 작성	사내 마켓 서버의 요청된 판, 파일별 해시 대조
기록	설치·삭제 요청과 결과	처리 결과를 AAS 기록에 반영

예외를 밝히는 화면과 사내 마켓 심사의 역할

AAS 화면에서는 마켓 설치가 즉시 반영되는 동작으로 보이지 않고 「요청」으로 남아, 사용자는 설치가 별도 처리 단계를 거친다는 것을 알 수 있습니다. 다만 플랫폼의 명령줄 설치는 대시보드 설치 경로가 하는 외부 출처 검사를 거치지 않으므로, 이 경로의 보안 통제는 사내 마켓에 어떤 패키지를 올릴지 정하는 등록 심사가 맡게 됩니다. 예를 들어 외부에서 가져온 패키지를 사내 마켓에 올릴 때 스크립트가 부르는 외부 주소를 검토하는 절차를 두면, 도우미가 설치하는 패키지는 모두 그 심사를 통과한 것이 됩니다. 정기 업무가 함께 들어 있는 에이전트 패키지도 설치만으로 정기 업무가 켜지지 않으므로, 담당자가 내용을 확인한 뒤에 직접 켜는 순서를 그대로 지킵니다.

7.3 외부 내려받기 없이 조직 안에서 구동되는 온프레미스 설치와 쿠버네티스 배포본

AAS는 조직 안 서버에 설치하는 온프레미스 제품으로, 콘솔과 에이전트 플랫폼, 모델과 음성 인식·OCR 처리를 모두 조직 안에 둘 수 있습니다. 2장에서 본 것처럼 공공 부문에서는 국가정보원이 2025년 1월 국가 망 보안체계(N²SF) 가이드라인을 내놓아 업무 정보를 기밀(C)·민감(S)·공개(O) 세 등급으로 나누고 등급에 따라 보안 통제를 달리 적용하는 방향을 정했습니다[S5]. 다만 이 제도에서도 기밀 등급 업무는 여전히 망을 분리해 다루므로[S6], 「외부 클라우드를 쓸 수 없다」는 조건은 상당수 기관에서 계속 유효합니다. AAS의 설치 구성은 그 조건을 전제로 짜여 있습니다.

AAS 서버는 파이썬 3.12 표준 라이브러리 위에 외부 패키지 두 개(websockets, PyYAML)만 쓰고, 화면은 빌드 단계가 없는 자바스크립트 모듈로 되어 있습니다. 이 구성 덕분에 망 안으로 반입한 컨테이너 이미지만으로 기동되며, 설치 과정에서 외부 패키지 저장소에 접속하거나 화면을 새로 빌드할 일이 없습니다. 배포 형태는 단일 서버에 컨테이너 구성 파일 하나로 띄우는 형태와, 여러 사용자를 받는 쿠버네티스(Kubernetes, 컨테이너 운영 플랫폼) 배포본 두 가지입니다. 쿠버네티스 배포본에서는 표준 로그인(OIDC) 그룹에 따라 사용자마다 쓸 수 있는 에이전트가 정해지고, 그룹에서 빠진 사용자의 에이전트는 멈춥니다.

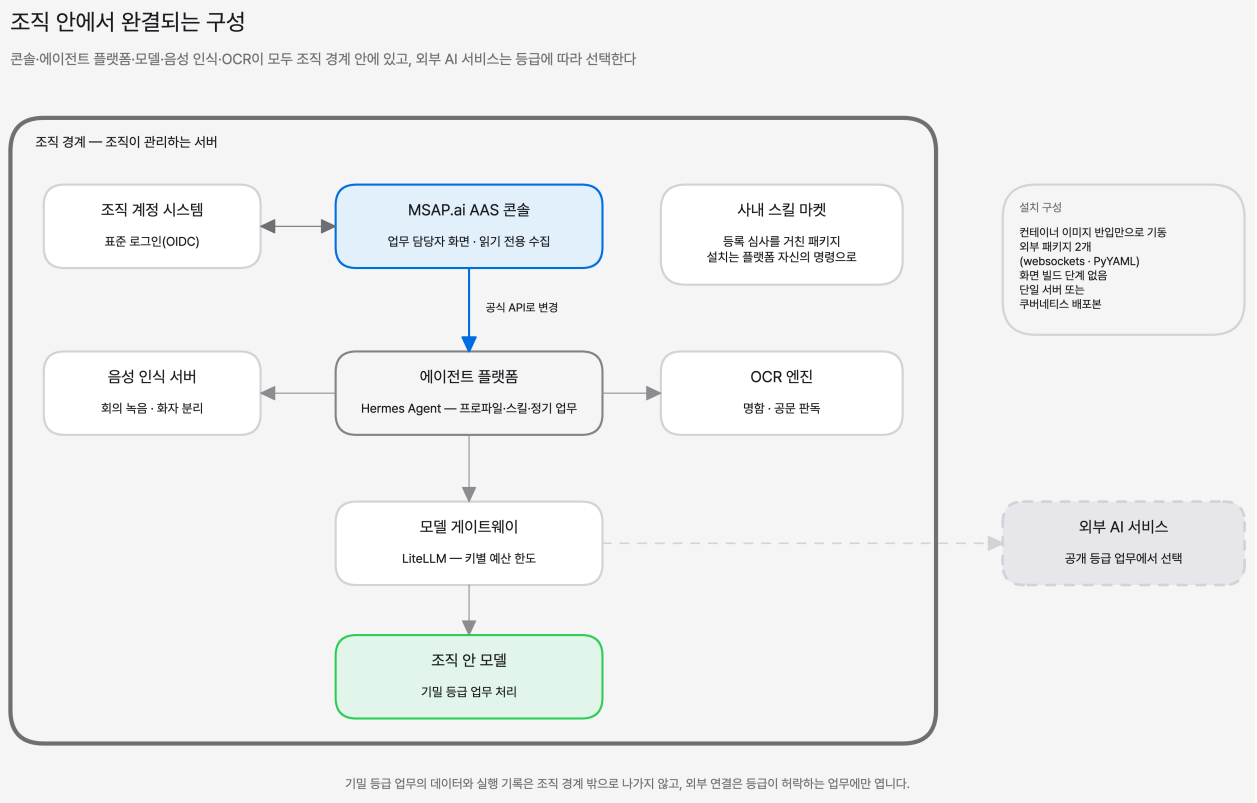


그림 7-2. 조직 안에서 완결되는 AAS 온프레미스 구성 — 콘솔, 에이전트 플랫폼, 모델·음성 인식·OCR

7.3.1 조직 안 모델과 음성 인식, OCR로 완결되는 처리 구성

업무 유즈케이스별 조직 안 처리 구성

5장의 업무 에이전트들은 외부 AI 서비스를 부르지 않고도 조직 안 구성 요소만으로 처리를 끝낼 수 있습니다. 명함 인식은 조직 안 AI 게이트웨이의 비전 모델로 이름·직함·회사·연락처를 읽고, 공공문서와 공공서식 인식은 HWP·HWPX·PDF를 마크다운으로 바꾼 뒤 스캔본에 한해 CPU로 실행되는 한국어 오프라인 OCR 엔진을 씁니다. 화자 구분 회의록은 녹음 파일을 조직 안 GPU 서버로 보내 음성 인식과 화자 분리를 함께 처리하며, 외부 음성 인식 API를 부르지 않습니다. 업무 정보의 등급은 기관이 자료의 중요도에 따라 정하므로[S5], 회의 녹음이나 공문처럼 민감한 자료를 다루는 이 세 처리는 조직 안에 두는 구성을 기본으로 삼습니다. 결과를 등록할 연결 시스템(CRM·위키·드라이브 등)은 고객 환경에 맞춰 설정하고, 쓰기 전에 사람이 확인하는 단계를 둡니다.

구성 요소	설치 위치	맡는 일	외부 연결
AAS 콘솔	조직 안 서버 또는 쿠버네티스	만들기·시키기·지켜보기·나누기 화면	없음
에이전트 플랫폼(Hermes Agent)	조직 안 서버 또는 쿠버네티스	에이전트·스킬·정기 업무 실행	스킬이 부르는 업무 시스템에 한정
모델 게이트웨이(LiteLLM)	조직 안	모델 목록·라우팅, 모델 점검	조직이 허용한 모델만
음성 인식·화자 분리	조직 안 GPU 서버	회의 녹음 처리	없음

구성 요소	설치 위치	맡는 일	외부 연결
OCR	조직 안 AI 게이트웨이 또는 오프라인 엔진	명함·스캔 문서 판독	없음
사내 스킬 마켓	조직 안	스킬 패키지 등록·배포	외부 패키지 반입은 심사 후
계정 연동	조직 계정 시스템	표준 로그인(OIDC)	조직 정책에 따름

외부로 나가는 연결을 등급에 맞춰 고르는 방식

조직 안 구성으로 완결되더라도 업무에 따라 밖으로 나가는 연결이 남을 수 있으므로, 설치 단계에서 그 목록을 따로 확인해야 합니다. 예를 들어 하루 두 번 보내는 운영 요약은 메신저 채널로 전달되는데, 이 채널이 외부 메신저라면 요약 내용이 조직 밖으로 나갑니다. 영업 에이전트처럼 외부 CRM을 부르는 스킬은 그 CRM이 조직 밖에 있으면 고객 정보가 밖으로 나가게 됩니다. AAS의 흐름 화면은 스킬 문서와 실행 기록에서 각 스킬이 부르는 외부 호스트를 뽑아 보여 주므로, 보안 담당은 설치 전에 이 목록을 등급 기준과 대조할 수 있습니다.

7.3.2 망 보안 등급별로 달라지는 쿠버네티스 배포본의 배치

등급별 배치 기준

국가 망 보안체계는 업무 정보의 등급에 따라 통제 수준을 달리 적용하며[S5], 2026년 3월에는 공공기관 업무 PC에서 생성형 AI를 쓰도록 이 체계를 적용하는 공모가 시작됐다는 보도도 나왔습니다[S7]. 망분리 규제를 개선하면서도 기밀 업무의 분리는 유지하는 것이 정부 개편의 방향이므로[S6], 한 기관 안에서도 업무 등급에 따라 에이전트의 배치가 달라질 수 있고, AAS 쿠버네티스 배포본은 등급별로 설치본을 나누는 방식으로 이를 수용합니다. 다만 아래 표는 등급별로 검토할 배치 기준을 정리한 것이며, 실제 적용은 기관의 보안 정책과 보안성 검토 결과를 따릅니다.

등급	AAS·플랫폼 배치	모델·음성 인식·OCR	메신저·외부 연결	스킬 마켓
기밀(C)	분리된 업무망 안 별도 설치본	조직 안 모델과 오프라인 엔진만	내부 채널만, 외부 호출 스킬 제외	내부 등록 패키지만 반입
민감(S)	업무망 안 설치본, 보안 통제 적용	조직 안 우선, 외부 모델은 정책 허용 시	허용 목록에 오른 시스템만	심사를 거친 패키지
공개(O)	업무망 또는 클라우드	외부 모델 선택 가능	일반 업무 시스템	심사를 거친 패키지

등급을 나눌 때 설치본을 나누는 이유

AAS는 하나의 콘솔이 여러 플랫폼 설치본을 등록부로 함께 볼 수 있지만, 등급이 다른 설치본을 한 콘솔에 묶으면 화면 자체가 등급 경계를 넘게 됩니다. 이런 이유로 기밀 등급 설치본에는 같은 망 안에 별도 콘솔을 두고, 민감·공개 등급처럼 같은 망에서 함께 다룰 수 있는 설치본만 한 콘솔에 등록하는 배치가 안전합니다. 콘솔과 플랫폼을 등급 경계 안에서 한 쌍으로 묶어 두면, 표준 로그인 그룹과 사용자별 에이전트 한도 같은 통제도 등급마다 따로 운영할 수 있습니다. 쿠버네티스 배포본은 사용자마다 에이전트를 두고 30일 동안 쓰지 않은 에이전트를 자동으로 멈추므로, 등급별 설치본의 자원도 실제 사용량에 맞춰 줄어듭니다.

7.4 비밀값을 화면과 로그에 남기지 않고 못 읽은 것을 0건으로 표시하지 않는 설계 원칙 다섯 가지

AAS의 기능은 다섯 가지 설계 원칙을 지키는 방식으로만 만들어지며, 원칙에 어긋나는 방식은 기능에 넣지 않습니다. 1장에서 본 것처럼 허가되지 않은 에이전트 행위의 대부분이 외부 공격보다 내부 정책 위반에서 나온다는 전망[S3]대로라면 에이전트 운영 콘솔이 막아야 할 위험의 대부분은 침입보다 콘솔 자신이 값을 흘리거나 틀린 상태를 맞다고 보여 주는 일에 가깝습니다. 이 때문에 다섯 원칙 가운데 넷은 기능이 무엇을 하지 않는지를 정하고 있으며, 보안·감사 담당이 도입 검토표에 그대로 옮겨 쓸 수 있도록 원칙마다 확인 방법을 짝지어 둡니다.

#	설계 원칙	이 원칙 때문에 넣지 않은 기능
1	에이전트 플랫폼을 고치지 않는다	쓰기 연결, 플러그인 설치, 설정 변경, 버전 변경
2	바꾸는 경로는 플랫폼 공식 API 하나다	파일 직접 수정, 스크립트 편집
3	비밀값은 화면·로그·기록 어디에도 남기지 않는다	관리자에게 값 보여 주기, 변경 기록에 값 적기, 대화 내용 읽기
4	못 읽은 것을 0건이라고 하지 않는다	수집에 실패해도 0을 내는 화면
5	흐름 그림을 사람이 그리지 않는다	파이프라인 편집기, 손으로 적는 작업 설명

7.4.1 비밀값 비보관과 「수집 실패」 표시가 감사 기록에 주는 신뢰

값 없이 상태만 다루는 비밀값 원칙

AAS는 자격증명을 다룰 때 이름, 위치, 쓰는 곳, 값이 채워졌는지, JWT(JSON Web Token) 만료일, 같은 값이 여러 곳에 복사됐는지만 내보내고 값 자체는 내보내지 않습니다. 같은 값의 중복은 값 대신 해시끼리 대조해 알아내므로, 「같은 토큰이 9곳에 복사돼 있다」는 사실을 값을 보지 않고도 화면에 드러낼 수 있습니다. 비밀값 탭은 새 값을 넣는 기능만 있고 저장된 값을 다시 보여 주지 않으며, 변경 기록에도 값은 적지 않습니다. 코드·설정·오류 메시지처럼 화면에 내보내는 글에서도 비밀값 모양의 문자열을 가리고, 비밀값으로 보이는 줄이 있는 글은 고치기를 막습니다. 관리자에게도 값을 보여 주지 않는 이유는 화면 캡처나 브라우저 기록, 로그로 값이 새는 경로를 처음부터 없애기 위해서이며, 값을 직접 확인해야 하는 작업은 플랫폼 쪽에서 합니다. 정보 과다 공유가 무단 에이전트 행위의 주된 원인으로 꼽히는 만큼[S3], 콘솔이 값을 아예 갖지 않는 설계가 운영 규칙으로 막는 방식보다 확실합니다.

수집 실패를 숨기지 않는 표시 원칙

운영 콘솔이 틀린 정보를 맞다고 보여 주면, 운영자는 이미 멈춘 정기 업무를 살아 있다고 믿게 됩니다. 이를 막기 위해 AAS는 읽지 못한 프로파일을 0건으로 세지 않고 「수집 실패」로 표시하며, 하루 두 번 보내는 운영 요약에도 수집에 성공한 프로파일 수를 「수집 12/12 프로파일」처럼 함께 적습니다. 예를 들어 실패 작업이 0건으로 보이는 요약을 받은 운영자는 같은 줄의 수집 성공 수를 보고, 그 0건이 실제로 실패가 없다는 뜻인지 읽지 못했다는 뜻인지를 구분할 수 있습니다. 감사 기록의 신뢰는 기록에 무엇이 있는지만큼 무엇이 빠졌는지를 알려 주는 데서 생기므로, 이 원칙은 변경 기록이 AAS를 거친 변경만 담는다는 한계를 밝히는 것과 같은 목적을 지닙니다.

흐름 그림을 실행 근거에서 만드는 원칙

다섯 번째 원칙은 감사 담당이 「이 에이전트가 무엇을 부르는가」를 확인할 때 사람의 설명 대신 실행 근거를 보게 합니다. AAS의 흐름 그림은 스킬 문서와 스크립트, 실행 기록에서 호출 관계를 뽑아 그리고, 선마다 그 관계를 찾은 근거 줄과 근거의 종류(크론 설정, 코드에서 확인, 스킬 문서의 지시)를 붙입니다. 이 방식에서는 사람이 그린 파이프라인이 실제 동작과 조금씩 어긋나는 문제가 생기지 않습니다. 다만 정적 분석이라는 한계가 있어, 변수로 조립되는 주소나 스크립트가 다시 부르는 스크립트는 놓칠 수 있다는 점을 검토 때 함께 고려해야 합니다.

7.4.2 보안 검토표에 옮겨 쓰는 원칙 다섯 가지의 확인 항목

설계 원칙별 확인 질문과 확인 방법

다섯 원칙은 도입 검토 회의에서 질문과 확인 방법으로 바꿔 쓸 수 있습니다. 아래 표의 확인 방법은 모두 설치 환경에서 직접 볼 수 있는 화면이나 설정이므로, 보안 담당은 제품 설명 대신 설치본을 열어 원칙 준수 여부를 확인하면 됩니다. 제품의 자동 시험 항목에도 플랫폼 파일이 바뀌지 않았는지 확인하는 항목이 들어 있어, 판을 올릴 때마다 원칙 1을 함께 점검합니다.

#	검토 질문	확인 방법
1	플랫폼의 플러그인·설정·버전이 도입 전후로 같은가	데이터 폴더 연결 설정의 읽기 전용 표시, 도입 전후 플러그인·설정·버전 목록 비교, 마켓 설치가 「요청」으로 남는지
2	모든 변경이 플랫폼 공식 API를 거치는가	거절된 변경에 플랫폼의 문구가 그대로 뜨는지, 스크립트 화면에 「고치기」가 없는지, 변경 기록의 항목
3	비밀값의 값이 화면·로그·변경 기록 어디에도 없는가	비밀값 탭에 「있음」만 보이는지, 자격 증명 화면에 「같은 값이 N곳에」만 보이는지, 변경 기록에 값이 없는지
4	수집하지 못한 정보를 0건으로 보이지 않는가	Cron 헬스체크 화면의 「실행 이력이 최신이 아닐 수 있습니다」 안내, 운영 요약의 수집 성공 프로파일 수
5	호출 관계 그림이 실행 근거에서 만들어졌는가	흐름 그림의 선마다 붙은 근거 줄과 근거 종류

원칙 밖에서 함께 확인할 운영 항목

다섯 원칙은 AAS 자신의 동작을 정하므로, 설치 환경에서 정하는 항목은 검토표에 따로 적어 두는 것이 좋습니다. 첫째는 접속 보안으로, AAS는 허용한 호스트 이름으로 들어온 요청만 받고 세션 쿠키를 12시간 동안 유지하며 서버에는 세션 해시만 남깁니다. 그러나 사내 접속에 TLS 인증서를 적용하는 방식은 설치 환경에 따라 달라지므로, 조직 인증서로 암호화 접속을 구성했는지를 확인해야 합니다. 둘째는 로그인 방식으로, 표준 로그인(OIDC)을 쓰면 조직의 계정 시스템과 그룹이 그대로 권한 기준이 되고, 자체 계정을 쓸 때는 AAS가 IP 하나당 로그인 시도를 5분에 5회로 제한합니다. 셋째는 7.2에서 다룬 마켓 도우미의 실행 위치와 사내 마켓의 패키지 등록 심사 절차로, 이 둘이 정해져야 예외 경로까지 검토표가 닫힙니다.

운영 확인 항목	확인 내용
접속 암호화	사내 접속에 조직 인증서 기반 TLS를 적용했는가
로그인	표준 로그인(OIDC) 그룹과 관리자 등록부가 조직 권한 체계와 맞는가
플랫폼 직접 접근	플랫폼 대시보드·서버 접속을 IT 관리자로 한정했는가
외부 연결	메신저 채널과 스킬이 부르는 외부 호스트가 등급 기준 안에 있는가
마켓 예외	도우미의 실행 호스트와 사내 마켓 등록 심사 절차가 정해졌는가

이 원칙들이 실제 부서 업무에서 어떤 장면으로 나타나는지는 8장의 부서별 장면에서 이어집니다.

8장: 부서별 AI Agent 업무 장면과 퇴사·부서 통합 때 조직에 남는 에이전트 구성

3장부터 7장까지 AAS의 기능과 설치·보안 원칙을 보았다면, 남은 질문은 이 콘솔 위의 업무 에이전트가 부서마다 어떤 일을 맡는가입니다. 1장에서 본 것처럼 에이전트를 시험하는 조직은 많아도 특정 부서의 정해진 업무에 정착시킨 조직은 아직 적습니다[S4]. 그래서 도입을 결정할 때 필요한 정보는 기술 사양보다 어느 부서의 어떤 업무를 어떤 시작 신호로 맡기고 결과가 어디에 쌓이는지에 가깝습니다. 이 장의 부서별 장면 카드와 조직 변화 표는 첫 파일럿 대상 업무를 고르고, 개인 생산성 도구에 조직 예산을 쓰는 근거를 설명하는 데 쓸 수 있습니다.

아래 업무 화면은 업무 에이전트 11개가 정기 업무를 실행하는 하나의 운영 설치본에서 찍은 화면 예시이고, 부서장 화면은 여러 사용자가 함께 쓰는 쿠버네티스 배포본에서 찍었습니다. 화면에 보이는 숫자는 설치본 하나의 상태를 보여 주는 예이며, 에이전트 수와 정기 업무 구성은 조직마다 다릅니다. 연결 시스템(CRM·위키·드라이브·메일·메신저 등)은 고객 환경에 맞춰 설정하므로, 장면 카드의 「CRM에 등록한다」는 그 조직이 쓰는 CRM에 연결한다는 뜻입니다. 지금 AAS가 연결하는 에이전트 플랫폼은 오픈소스 Hermes Agent 1종이며, 모든 장면은 이 플랫폼 위에 스킬과 정기 업무로 만든 것입니다.

8.1 경영 부서와 현업 부서의 에이전트 장면 — 주간 회의 지시 원장부터 이력서 1차 심사까지

AAS 위의 업무 에이전트는 모두 「스킬 + 정기 업무 + 호출하는 연결 시스템」의 조합입니다. 경영 부서에서는 회의 녹음이 시작 신호가 되고, 영업·마케팅·재무·인사 부서에서는 명함 사진, 정기 실행 시각, 새로 올라온 이력서 파일이 시작 신호가 됩니다. McKinsey 조사에서 업무 기능별 에이전트 확대 적용 비율이 10% 이하였다는 결과는[S4] 부서 단위 업무로 범위를 좁혀야 정착 여부를 판단할 수 있다는 뜻이기도 합니다. 장면 카드는 부서마다 「시작 신호 · 에이전트가 하는 일 · 사람이 판단하는 단계 · 남는 결과물」 네 칸으로 되어 있습니다.

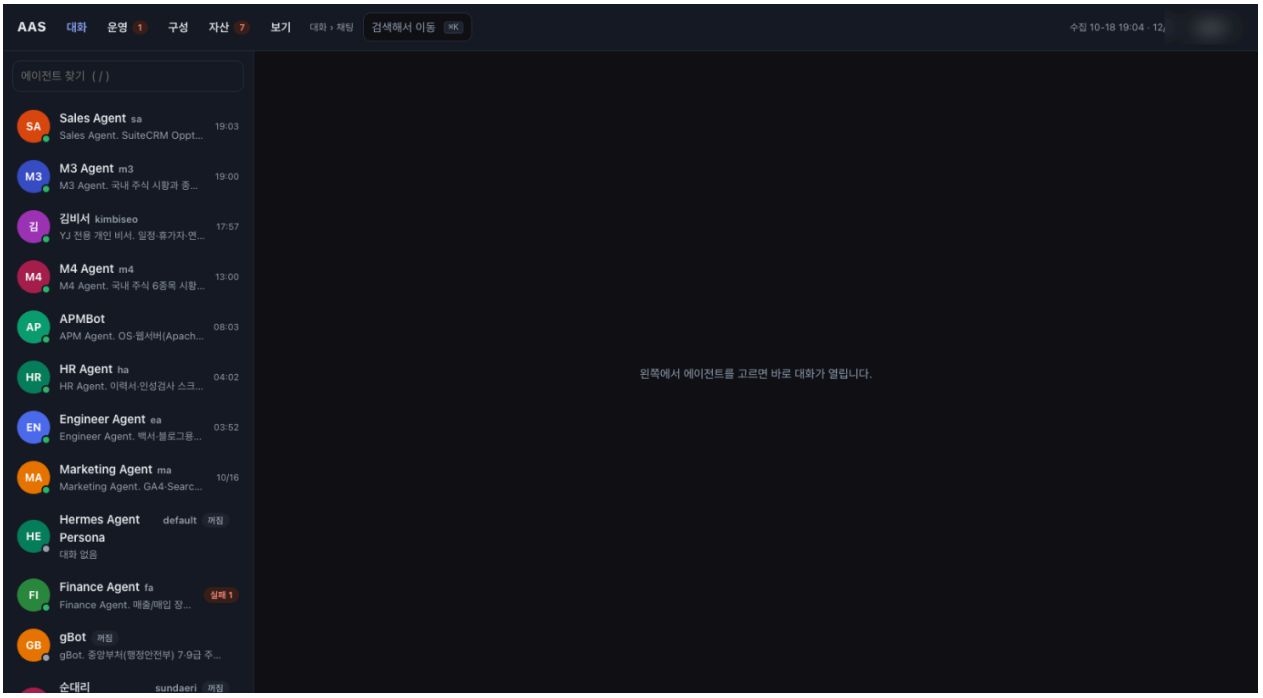


그림 8-1. 부서별 업무 에이전트 목록 — 에이전트마다 담당 업무 설명과 마지막 대화 시각이 보이고, 재무 에이전트에는 실패 1건 배지가 붙어 있습니다. 왼쪽 목록에서 에이전트를 고르면 바로 대화가 열립니다.

그림 8-1은 대화 화면 왼쪽에 부서별 업무 에이전트가 나열된 화면 예시입니다. 영업, 비서, 인사, 엔지니어, 마케팅, 재무, 공공(중앙부처형·지자체형) 에이전트가 각자의 스킬과 정기 업무를 갖고, 꺼진 에이전트에는 「꺼짐」 표시가 붙습니다. 예를 들어 재무 에이전트 옆의 「실패 1」 배지는 그 에이전트의 정기 업무 하나가 마지막 실행에서 실패했다는 뜻이므로, 담당자는 대화를 열기 전에 어느 에이전트부터 봐야 하는지 알 수 있습니다. 업무 에이전트 목록은 담당자가 일을 시키는 창구이면서 동시에 상태를 확인하는 첫 화면 역할을 합니다.

8.1.1 회의 지시가 할 일과 지시 원장으로 남는 경영 부서 장면

회의 녹음에서 지시사항까지 이어지는 처리 흐름

경영 부서에 맡길 첫 업무로는 주간 회의의 지시를 담당자별 할 일로 바꾸는 회의 후속 처리를 먼저 검토할 만합니다. 회의 녹음 파일(MP3·M4A·OGG)을 받으면 에이전트는 조직 안 GPU 서버에서 음성 인식과 화자 분리를 실행하고, 목소리 지문으로 화자 이름을 붙이되 근거가 없으면 「미확인」으로 남깁니다. 화자 구분 회의록은 개요, 화자 표, 지시·판단, 보고·의견, 이견, 결정 사항, 액션 아이템, 발언 원문의 순서로 부서별 템플릿을 채우고, 에이전트가 이를 위키에 발행합니다. 회의 후속 처리는 어느 부서에나 있는 업무라 첫 적용 대상으로 고르기 쉽습니다. 외부 음성 인식 서비스를 거치지 않으므로 경영 회의 녹음이 조직 밖으로 나가지 않는다는 점이 보안 검토에서 먼저 확인할 사항입니다.

지시 원장에 번호로 쌓이는 리더의 지시

회의록이 발행되면 에이전트는 「지시·판단」 항목에서 지시사항을 「지시 · 근거 · 기한」 세 칸으로 뽑고, 액션 아이템은 담당자와 기한을 붙여 그날의 칸반 페이지에 사람별 체크박스로 합칩니다. 동시에 지시는 D-번호, 피드백은 F-번호로 지시 원장에 쌓이고, 원장은 일·주·월 단위로 집계됩니다. 체크는 사람이 하고, 에이전트는 30분마다 체크 상태를 거둬들여 담당자별 요약을 업무 채팅방에 알립니다. 따라서 지난달 회의에서 무엇을 지시했고 그 지시가 어디까지 처리됐는지를 기억이 아닌 원장의 번호로 추적할 수 있습니다.

아침 상황판과 음성 지시, 팀 처리량 집계

경영 부서의 나머지 장면은 정기 업무와 음성 메시지를 시작 신호로 씁니다. 아침 브리핑은 07:00 정기 업무로 일정과 메일 요약, 밤사이 실패한 정기 업무 목록을 메신저로 보내고, 같은 내용을 파일로도 보관합니다. 메신저 음성 메시지로 남긴 지시는 음성 인식을 거쳐 첫 단어에 따라 메모·할 일·팀 피드백 스킬로 전달되며, 팀 칸반의 처리량과 지연 건수는 주간·월간으로 집계됩니다. 아래 장면 카드는 경영 부서의 네 장면을 같은 형식으로 정리한 것입니다.

시작 신호	에이전트가 하는 일	사람이 판단하는 단계	남는 결과물
주간 회의 녹음 업로드	화자 구분 회의록 작성, 지시사항을 지시·근거·기한으로 추출, 담당자별 할 일을 칸반에 등록	화자 실명 확정, 할 일 완료 체크	회의록, 지시 원장(D·F 번호)
07:00 정기 실행	일정·메일 요약과 밤사이 실패한 정기 업무 목록을 메신저로 발송	그날 우선순위 결정	브리핑 파일

시작 신호	에이전트가 하는 일	사람이 판단하는 단계	남는 결과물
메신저 음성 메시지	받아 적은 뒤 첫 단어로 메모·할 일·팀 피드백에 분류	분류 결과 확인	메모·할 일 페이지
주간·월간 정기 실행	팀 칸반 처리량과 지연 건수 집계	1:1 면담 주제 선정	팀 지표 이력

8.1.2 명함 등록과 손익 보고, 이력서 심사를 맡기는 현업 부서 장면

영업 부서의 명함 인식과 딜 관리

영업 부서에서 에이전트가 맡는 업무는 사람이 옮겨 적던 정보를 여러 시스템에 같은 이름으로 등록하는 일과, 아무도 손대지 않은 딜을 찾아내는 일입니다. 명함 사진을 보내면 에이전트는 조직 안 AI 게이트웨이의 비전 모델로 이름·직함·회사·전화·메일을 읽고, 기존 고객사에 연결한 뒤 등록 전 예행 결과를 먼저 보여 줍니다. 같은 사람이 이미 있으면 멈추고 되묻고, 없는 회사는 말없이 만들지 않으므로 CRM에 중복 연락처가 생기지 않습니다. 새 사업 이야기가 나오면 드라이브 고객 폴더, CRM 영업기회, 위키 고객 일지를 같은 이름으로 한 번에 만들고, 정기 업무가 무활동 딜·마감 지난 딜·퇴사자 담당 딜을 매일 골라 보고하며, 09:00에는 공공조달 공고 메일에서 사업과 맞는 공고만 골라 일일 페이지로 정리합니다.

마케팅 지표 보고와 재무 손익 보고

마케팅과 재무 부서의 공통점은 형식이 정해진 정기 보고입니다. 마케팅 에이전트는 웹 분석·검색 콘솔·유튜브 지표를 일·주·월·분기 단위로 수집해 브랜드별 보고로 발행하고, 지표가 급변하면 다음 보고를 기다리지 않고 알림을 보냅니다. 재무 에이전트는 원장 시트를 읽어 정해진 형식으로 주간·월간 손익 보고를 만들고, 「이번 달 미수금」 같은 채권·채무 질의에 대화로 답합니다. 보고 형식이 매번 같기 때문에 달마다 수치를 바로 비교할 수 있다는 것이 사람이 만든 보고서와 다른 점입니다. 명함 등록이나 손익 보고처럼 입력과 출력 형식이 정해진 업무는 Gartner가 말하는 특정 업무 AI 에이전트(task-specific AI agent)의 전형에 해당합니다[S1].

인사 부서의 이력서 1차 심사와 사람의 판단

인사 부서의 이력서 1차 심사는 에이전트가 점수와 근거를 내고 채용 판단은 사람이 내리는 구조입니다. 정기 업무가 04:00에 공유 드라이브의 새 이력서를 읽고, 회사 인재 기준을 적은 기준 파일(짧은 재직 기간 감점, 자기주도성 평가 축 등)로 점수와 근거를 남깁니다. 기준은 파일로 관리되므로 인사 담당자가 평가 기준을 직접 고칠 수 있고, 담당자는 점수와 함께 붙은 근거를 보고 후보를 검토합니다. 직원 면담 녹음도 같은 음성 인식 경로로 면담 기록 페이지가 되므로, 면담 내용이 담당자 개인의 기억에만 의존하지 않습니다.

부서	시작 신호	에이전트가 하는 일	사람이 판단하는 단계	남는 결과물
영업	명함 사진	명함을 읽어 기존 고객사에 연결, CRM·연락처·위키 명함집에 등록	등록 전 예행 결과 확인, 중복 시 판단	CRM 연락처, 명함집 페이지

부서	시작 신호	에이전트가 하는 일	사람이 판단하는 단계	남는 결과물
영업	매일 정기 실행	무활동·마감 지난·퇴사자 담당 딜 선별 보고	딜 재배정	딜 보고 이력
마케팅	주간 정기 실행	웹·검색·유튜브 지표 수집과 브랜드별 보고 발행, 급변 알림	대응 캠페인 결정	지표 이력
재무	주간·월간 정기 실행	원장 시트를 정해진 형식의 손익 보고로 요약	손익 해석과 조치	정형 보고서
인사	04:00 정기 실행	새 이력서를 기준 파일로 1차 심사, 점수와 근거 기록	채용 판단 전부	심사 근거 기록, 기준 변경 이력

8.2 IT 운영과 공공기관의 에이전트 장면 — 장애 1차 조사, 토큰 유출 영향 범위, 망 분리 환경의 공문 처리

IT 운영 부서와 공공기관은 규정이 엄격해 에이전트 도입을 신중하게 검토하는 조직이지만, 반복 점검과 정형 문서 처리가 많아 맡길 업무도 분명합니다. 1장에서 본 내부 정책 위반 전망[S3]은 이런 조직에서 특히 무겁게 읽힙니다. 두 조직의 에이전트에는 서버에 부담을 주는 수집과 쓰기 도구를 명시 요청 때만 쓰는 원칙, 외부 AI 서비스 없이 조직 안 모델로 처리하는 원칙이 함께 적용됩니다.

8.2.1 인프라 점검 보고와 장애 1차 조사를 맡는 IT 운영 에이전트

인프라 정기 점검 보고

IT 운영 에이전트의 기본 업무는 APM 도구를 정기 업무로 호출해 점검 보고를 만드는 일입니다. 에이전트는 MCP 서버로 연결된 사내 APM에서 OS, 웹서버, WAS, 응답시간, JVM 상태를 읽어 일·주·월 보고로 발행합니다. 운영 담당자가 매일 점검표를 손으로 채우던 작업이 정기 업무 하나로 바뀌고, 점검 이력은 위키에 날짜별로 쌓입니다.

장애 1차 조사의 범위와 쓰기 도구 사용 원칙

장애 1차 조사는 「어제 오후 3시에 응답이 느렸다」 같은 질문을 시작 신호로 삼아, 그 시간대의 응답시간·트랜잭션 추적·JVM 지표를 조사해 1차 원인 후보를 제시하는 업무입니다. 다만 스레드 덤프처럼 대상 서버에 부담을 주는 수집은 증상과 시간대가 정해진 경우에만 실행하고, 고객 제출용 확인서 발행 같은 쓰기 도구는 사람이 명시적으로 요청할 때만 씁니다. 에이전트가 읽기 도구로 범위를 좁히고, 운영 시스템에 영향을 주는 동작은 사람의 지시로만 실행되도록 스킬 문서에 적어 둡니다. 이 원칙은 규정이 엄격한 운영 조직이 에이전트에 장애 조사를 맡길 수 있는지를 판단하는 첫 기준이 됩니다.

에이전트 자체의 멈춤 감지와 토큰 유출 영향 범위

IT 운영 부서는 에이전트가 맡은 업무 외에 에이전트 자신의 운영도 책임집니다. AAS는 정기 업무의 실패와 멈춤, 알림이 안 가는 작업, 만료 임박 토큰, 모델 설정 불일치를 첫 화면에 먼저 보여 주므로, 에이전트가 멈춘 사실을 다음 보고가 빠진 뒤에야 알게 되는 일을 줄입니다. 예를 들어 토큰 하나가 유출됐다고 의심되면, 자격증명 화면이 값을 보이지 않은 채 그 토큰 이름을 쓰는 스킬과 정기 업무의 위치를 찾아 줍니다. 앞서 본 Gartner 전망처럼 무단 행위의 대부분이 내부 정책 위반에서 나온다면[S3], 어떤 비밀값을 어느 업무가 쓰는지 값 없이 찾는 기능은 사고 대응 시간을 정하는 요소가 됩니다.

시작 신호	에이전트가 하는 일	사람이 판단하는 단계	남는 결과물
매일 아침 정기 실행	APM으로 OS·웹서버·WAS·응답시간·JVM 점검 보고	이상 항목 조치	점검 이력
「어제 오후 3시 응답 지연」 질문	해당 시간대 트랜잭션·JVM 조사, 1차 원인 후보 제시	부담 큰 수집과 쓰기 도구 사용 지시	조사 기록
AAS 상시 감시	정기 업무 실패·멈춤·알림 누락, 만료 임박 토큰 표시	재실행·알림 대상 지정	운영 이력
토큰 유출 의심	그 토큰을 쓰는 스킬·정기 업무를 값 없이 찾음	토큰 교체와 영향 업무 재실행	영향 범위 목록

8.2.2 외부 AI 서비스 없이 공문과 법령 확인을 처리하는 공공기관 에이전트

망 분리 규제 변화와 남는 온프레미스 수요

공공기관의 에이전트 도입은 2장에서 본 망 분리 규제 변화와 함께 판단해야 합니다. 국가 망 보안체계(N²SF)가 등급별로 생성형 AI와 클라우드 활용 길을 열었고[S5], 2026년 3월에는 공공기관 업무 PC에서 생성형 AI를 쓰는 공모도 시작됐습니다[S7]. 그러나 기밀 등급 업무는 여전히 망을 분리해 두므로[S6], 외부 AI 서비스 없이 조직 안 모델·음성 인식·OCR로 처리하는 온프레미스 설치 수요는 계속 남습니다.

한글 공문 판독과 공공서식 빈칸 채우기

공공기관 에이전트의 대표 업무는 다른 기관에서 온 한글(HWP·HWPX) 공문을 읽고, 정해진 공공서식에 맞춰 문서를 만드는 일입니다. HWPX는 한글 문서를 XML로 저장하는 개방형 형식이며, 에이전트는 HWP·HWPX·PDF·DOCX를 마크다운으로 읽어 요약하고 스캔본은 내장 오프라인 OCR(한국어 모델, CPU 실행, 외부 키 불필요)로 처리합니다. 받은 공공서식의 빈칸 구조를 분석해 값을 채운 뒤 서식 그대로 돌려주고, 기안문 템플릿으로 보고서·기안문·시행문 서식의 한글 파일을 만듭니다. 채운 값을 담당자에게 먼저 보여 준 뒤 저장하므로, 서식을 맞추는 작업은 줄고 내용 판단은 담당자에게 남습니다. 민감(S)·공개(O) 등급 업무에서 생성형 AI 활용 길이 열렸더라도[S5], 공문 판독과 서식 작업을 조직 안 OCR과 모델로 처리하면 문서가 조직 밖으로 나가지 않으므로 외부 서비스 이용 검토의 부담을 덜고 시작할 수 있습니다.

보도 답변 초안의 법령 확인과 아침 동향 브리핑

보도자료 답변 초안을 쓸 때 에이전트는 국가법령 도구 서버에서 법령·시행령·자치법규·판례를 찾아 인용이 맞는지 확인합니다. 조회 키가 없거나 만료되면 추측으로 채우지 않고 멈춰서 알리며, 그 키 상태는 AAS 자격증명 화면에 표시됩니다. 06:00 정기 업무는 부처 보도자료, 정책브리핑, 지자체 게시판을 모아 아침 브리핑을 위키와

한글 문서로 발행합니다. 중앙부처형과 지자체형 공무원 에이전트는 각각 10개 업무(언론 모니터링, 법령·조례 검토, 국회·민원 답변 초안, 회의록 등)를 스킬로 갖추고 있어 기관 유형에 맞는 쪽에서 시작할 수 있습니다.

시작 신호	에이전트가 하는 일	사람이 판단하는 단계	남는 결과물
HWP·HWPX 공문 첨부	마크다운 변환과 요약, 스캔본은 오프라인 OCR	처리 방침 결정	공문 요약
「서식 채워줘」「기안문 만들어」	공공서식 빈칸 분석과 값 채우기, 한글 파일 생성	채운 값 확인 후 저장	한글 공문
보도 답변 요청	관련 법령 조회와 인용 확인, 답변 초안 작성	답변 내용 확정	답변 초안
06:00 정기 실행	부처·지자체 보도와 정책 소식 브리핑	대응 업무 선정	동향 브리핑

8.3 부서장이 보는 팀 에이전트 현황 — 에이전트별 준비 상태와 35일 추이

업무별 에이전트가 늘어나면 한 부서 안에서도 팀원마다 에이전트를 운영하는 경우가 늘어납니다. 부서장에게 필요한 화면은 팀원 각자의 에이전트가 오늘 일할 준비가 됐는지와, 지난 한 달 동안 작업·문제·사용량이 어떻게 변했는지를 한 번에 보여 주는 대시보드입니다. 2장에서 본 감독용 에이전트 전망[S3]처럼 에이전트 수가 늘어날수록 감독 기능의 비중도 커지며, AAS 대시보드는 그 감독을 사람이 읽는 화면으로 제공합니다. 아래 화면은 사용자마다 에이전트를 하나씩 둔 쿠버네티스 배포본의 화면 예시입니다.

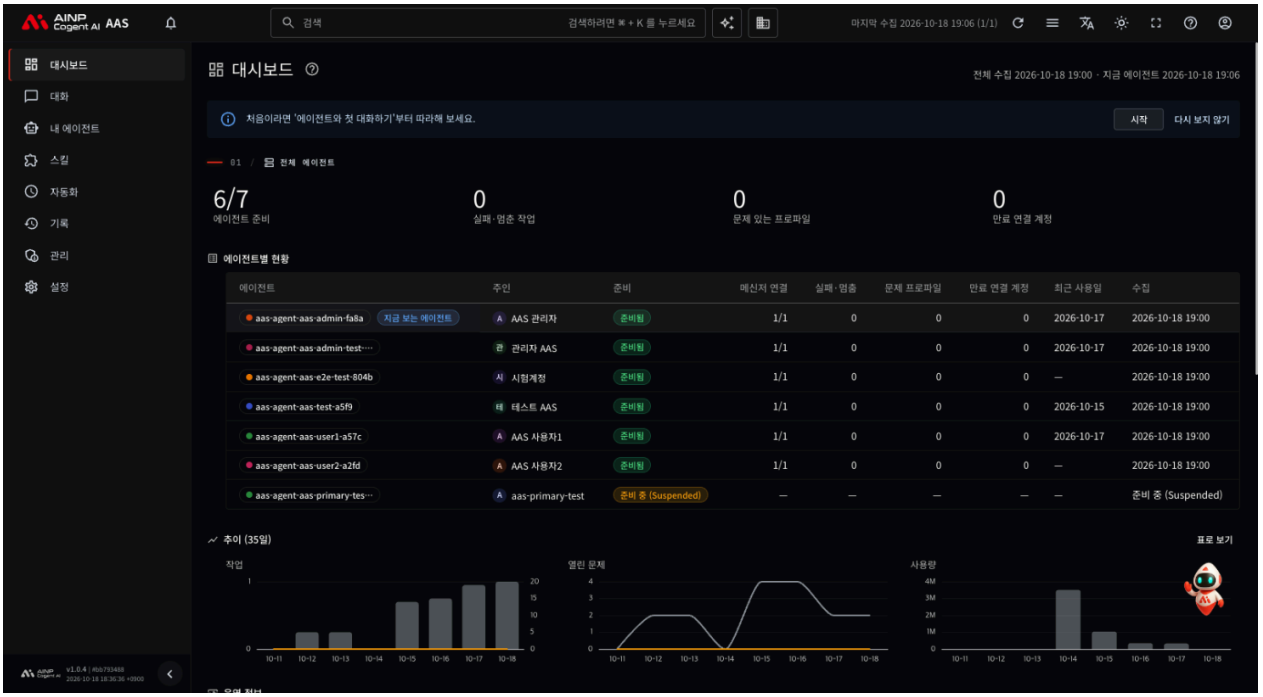


그림 8-2. 팀 에이전트 대시보드 — 위쪽 숫자 네 개(에이전트 준비, 실패·멈춘 작업, 문제 있는 프로파일, 만료 연결 계정)를 먼저 보고, 0이 아닌 항목이 있으면 가운데 표에서 해당 에이전트의 행을 찾습니다. 아래 세 그래프는 35일 추이입니다.

8.3.1 에이전트마다 한 줄로 보이는 준비 상태와 실패, 만료 계정

대시보드 상단 숫자 네 개와 에이전트별 현황 표

대시보드 상단은 에이전트 준비, 실패·멈춘 작업, 문제 있는 프로파일, 만료 연결 계정 네 숫자를 보여 줍니다. 그림 8-2의 화면 예시는 에이전트 7개 중 6개가 준비됐고 실패·멈춘 작업, 문제 있는 프로파일, 만료 연결 계정이 모두 0인 상태를 보여 줍니다. 가운데 표는 에이전트마다 한 줄씩 주인, 준비 상태, 메신저 연결, 실패·멈춤, 문제 프로파일, 만료 연결 계정, 최근 사용일, 마지막 수집 시각을 나란히 보여 주므로, 숫자가 0이 아닐 때 어느 팀원의 에이전트인지 바로 찾을 수 있습니다. 예를 들어 화면의 마지막 에이전트는 「준비 중(Suspended)」으로 표시돼 있어 나머지 칸이 비어 있고, 부서장은 이 행만 보고 해당 에이전트가 멈춘 상태임을 압니다.

사용자별 에이전트 한도와 자동 멈춤

쿠버네티스 배포본에서는 표준 로그인(OIDC)으로 로그인한 사용자마다 볼 수 있는 에이전트가 정해지고, 화면 예시의 관리자는 사용자당 에이전트 한도를 3개로 정해 두었습니다. 사용자가 OIDC 그룹에서 빠지면 그 사용자의 에이전트는 멈추고, 30일 동안 쓰지 않은 에이전트도 자동으로 멈췄다가 다시 시작할 수 있습니다. 대시보드의 「최근 사용일」 칸은 곧 멈출 에이전트를 미리 알려 주는 신호로도 읽어야 합니다. 부서장이 매일 확인할 지표와 판단은 아래 표와 같습니다.

지표	화면 표시	0이 아닐 때 부서장이 할 판단
에이전트 준비	준비된 수 / 전체 수	준비되지 않은 에이전트의 주인에게 원인 확인 요청
메신저 연결	연결된 채널 수 / 설정된 채널 수	알림이 안 가는 상태인지 IT 담당자에게 확인
실패·멈춘 작업	에이전트별 건수	그 정기 업무가 만드는 보고서를 오늘 쓸 수 있는지 판단
문제 있는 프로파일	에이전트별 건수	모델·설정 불일치 여부를 IT 담당자와 확인
만료 연결 계정	에이전트별 건수	계정 갱신 담당자 지정
최근 사용일	날짜	30일 미사용 자동 멈춤 전에 유지 여부 결정

8.3.2 작업과 열린 문제, 사용량의 35일 추이로 보는 팀 운영

35일 추이 그래프 세 개의 의미

대시보드 하단의 35일 추이는 작업, 열린 문제, 사용량 세 그래프이며, 각각 팀 에이전트가 얼마나 일했는지, 해결되지 않은 문제가 얼마나 쌓였는지, 모델 호출에 입력 토큰을 얼마나 소비했는지를 날짜별로 보여 줍니다. 그림 8-2의 화면 예시에서는 작업이 10월 15일 이후 늘어나는 동안 열린 문제가 10월 15~16일 4건까지 올랐다가 2건으로 줄었고, 사용량은 10월 14일에 가장 높았습니다. 세 그래프를 같은 날짜 축에 두면, 작업 증가와 문제 증가가 같은 날 일어났는지를 한눈에 대조할 수 있습니다. 부서장은 그래프 하나보다 세 그래프의 관계를 먼저 읽어야 합니다.

추이 그래프를 읽고 조치를 정하는 기준

추이 그래프는 조치를 정하는 판단 근거로 쓸 때 의미가 있으며, 대표적인 조합은 아래 표의 네 가지입니다. 예를 들어 작업과 열린 문제가 함께 늘면 새로 등록한 정기 업무가 실패하고 있을 가능성이 크고, 작업은 그대로인데 사용량만 급증하면 특정 스킬이 같은 호출을 반복하고 있을 수 있습니다. 다만 AAS는 지금 사용량을 보여 주기만 하고, 한도를 넘었을 때 자동으로 정지하거나 부서별로 사용량을 할당하는 기능은 아직 없습니다. 사용량 관리는 부서장이 추이를 보고 IT 담당자와 함께 모델이나 정기 업무 일정을 바꾸는 방식으로 운영합니다.

그래프 조합	의심할 원인	조치
작업 증가 + 열린 문제 증가	새로 등록한 정기 업무의 실패	Cron 헬스체크 화면에서 해당 작업의 실패 사유 확인
작업 유지 + 사용량 급증	스킬의 반복 호출이나 모델 변경	해당 날짜의 활동 기록과 프로파일 모델 확인
작업 감소 + 열린 문제 유지	멈춘 작업이나 만료 계정	상단 숫자와 에이전트별 현황 표 확인
작업 0 + 사용량 0 지속	쓰지 않는 에이전트	30일 자동 멈춤 전에 유지·정리 결정

8.4 퇴사와 부서 이동·통합, 지사 확산, 감사 때 조직에 남는 스킬과 정기 업무

AAS에서 에이전트 구성은 사람마다 받는 에이전트 안의 프로파일(성격과 모델), 스킬(일하는 방법을 적은 문서와 스크립트), 정기 업무(실행 일정), 그리고 그 결과물(회의록·명함집·보고서·고객 일지)로 이루어지며, 이 넷은 개인 노트북이 아닌 조직이 운영하는 에이전트 플랫폼과 위키·CRM·드라이브에 저장됩니다. 3장에서 본 폭스프로·디베이스 선례[S8]에서 현업 담당자가 만든 업무 프로그램은 파일로 조직에 남아 만든 사람이 다른 부서로 옮기거나 회사를 떠난 뒤에도 계속 쓰이는 경우가 많았고, AAS가 에이전트 구성에서 겨냥하는 효과도 같습니다. 의사결정권자가 묻는 「개인 생산성 도구에 왜 조직 예산을 쓰나」에 대한 답은 사람이 떠나거나 조직이 바뀌어도 에이전트 구성이 조직 자산으로 이어진다는 데 있습니다.



그림 8-3. 프로파일·스킬·정기 업무·결과물로 이루어진 에이전트 구성이 퇴사, 신규 입사, 부서 통합, 지사 확산, 감사, 인수 여섯 순간에 각각 어떻게 넘어가는지 보여 주는 구조

8.4.1 담당자가 떠난 뒤에도 업무가 이어지는 스킬과 정기 업무의 인계

담당자 퇴사 때 넘어가는 항목

담당자가 퇴사하면 그 사람의 스킬, 정기 업무, 회의록, 고객 일지는 플랫폼과 연결 시스템에 그대로 남고, 후임자는 그 목록을 인계 대상으로 삼습니다. 예를 들어 영업 에이전트가 매일 보고하는 「퇴사자 담당 딜」 목록은 후임자가 넘겨받을 딜 목록이 되고, 고객 회의 템플릿으로 정리한 위키 고객 일지에는 고객이 어떤 요구와 우려를 말했는지가 남아 있습니다. 다만 개인 계정에 묶인 토큰은 퇴사와 함께 교체해야 하므로, 자격증명 화면에서 그 토큰을 쓰는 스킬과 정기 업무의 위치를 값 없이 찾은 뒤 교체합니다. OIDC 그룹에서 퇴사자를 빼면 그 사람의 에이전트는 멈추고 데이터는 그대로 남습니다. 업무를 통째로 이어 갈 때는 관리자가 에이전트 상세의 소유권 이전으로 퇴사자의 에이전트를 후임자에게 넘기면, 그 안의 프로파일·스킬·정기 업무가 에이전트째 후임자 소유가 됩니다. 멈춘 동안에는 정기 업무도 실행되지 않으므로, 매일 나가야 하는 보고가 있다면 그룹에서 빼기 전에 소유권 이전을 마치는 순서를 인계 절차에 넣습니다. 일부 업무만 넘길 때는 그 프로파일을 내보내고 후임자가 자기 에이전트에서 PC에서 가져오기로 들여오며, 더 쓰지 않을 프로파일은 내보내기로 보관본을 남긴 뒤 이름을 다시 입력해 삭제합니다(4.1.2절). 내보내기가 실패하면 삭제가 멈추므로, 보관본 없이 구성이 사라지는 일은 생기지 않습니다.

부서를 옮길 때 나누는 에이전트와 프로파일

부서를 옮기는 사람은 자기 에이전트를 그대로 가져가고, 옛 부서에 두고 갈 업무만 프로파일 단위로 나눕니다. 새 부서 업무는 자기 에이전트 안에 새 프로파일로 만들고, 옛 부서 업무 프로파일은 내보내 후임자가 PC에서 가져오기로 받게 한 뒤 자기 에이전트에서는 지웁니다. 부서 이동과 함께 OIDC 그룹이 바뀌어 AAS를 쓰는 그룹에서 빠지면 에이전트가 멈추지만 데이터는 남으므로, 관리자는 그룹 정리 뒤에도 소유권 이전이나 다시 시작으로 이어 갈 방법을 고를 수 있습니다.

절차가 문서로 남을 때 줄어드는 반복 설명

인계에서 스킬이 중요한 이유는 반복 비용에 있습니다. 업무 절차가 사람의 기억이나 대화창 속 지시로만 남아 있으면 담당자가 바뀔 때마다 같은 설명을 처음부터 되풀이해야 하고, 그동안 에이전트에게 맡긴 시간은 사람이 직접 처리하는 시간보다 짧아지지 않습니다. 반대로 절차가 스킬 문서로 남아 있으면 후임자는 설명을 다시 듣는 대신 문서를 읽고 자기 업무에 맞게 바꿀 부분만 고칩니다. 다만 문서로 남은 절차가 오래된 판일 수도 있으므로, 인계 시점에는 스킬의 판 기록과 그 스킬을 거는 정기 업무의 최근 실행 결과를 함께 확인해 전임자가 마지막으로 쓰던 절차가 맞는지 가려야 합니다. 이 확인을 인계 체크리스트의 한 줄로 넣어 두면 담당자가 바뀐 뒤 첫 주에 생기는 결과 차이를 줄일 수 있습니다.

신규 입사자가 전임자 구성을 출발점으로 삼는 방식

신규 입사자는 먼저 에이전트 화면에서 관리자가 정한 한도 안에 자기 에이전트를 추가합니다. 그 안에 새 프로파일을 만들 때 「다른 에이전트에서 가져오기」를 고르면 전임자나 같은 팀 선임 에이전트의 main 성격·설정을 출발점으로 삼고, 전임자의 업무 프로파일을 그대로 받아야 하면 전임자 쪽에서 내보낸 파일을 PC에서 가져오기로 들여옵니다. 어느 쪽이든 비밀값(.env)은 따라오지 않으므로, 메신저 토큰과 외부 시스템 계정은 본인 것으로 새로 채웁니다. 전임자가 없는 직무라면 마케팅·세일즈·연구소·엔지니어링·총무·회계·인사·고객지원·기획 등 역할 템플릿 20종 가운데 하나를 출발점으로 성격 문서를 채운 뒤 시작합니다. 신규 입사자는 첫 주부터 전임자가 쓰던 보고 형식과 정기 업무 일정으로 일을 시작하고, 바꿀 부분만 스킬 문서에서 고치면 됩니다. 아래 표는 퇴사와 신규 입사 때 넘어가는 항목을 정리한 것입니다.

인계 항목	담는 내용	담당자 퇴사 때	신규 입사 때
에이전트·프로파일	사람마다 받는 실행 단위와 그 안의 업무 묶음(성격, 모델, 메신저 연결)	업무째 이어 가면 소유권 이전, 일부만 넘기면 내보낸 뒤 후임자가 가져오기, 정리하면 내보낸 뒤 삭제	자기 에이전트 추가 뒤 다른 에이전트에서 가져오기·PC에서 가져오기, 또는 역할 템플릿으로 시작
스킬	일하는 방법을 적은 문서와 스크립트	그대로 유지	넘겨받은 뒤 필요한 부분만 수정
정기 업무	실행 일정, 알림 대상	후임자 에이전트로 이전, 알림 대상 변경	전임자 일정 그대로 시작
자격증명	토큰·키의 이름과 쓰는 위치(값은 비표시)	개인 토큰 교체	본인 계정으로 새로 발급
결과물	회의록, 명함집, 고객 일지, 보고서	위키·CRM·드라이브에 그대로 보존	바로 열람

8.4.2 지사 확산과 감사 대응에 쓰이는 마켓 배포와 변경 기록

지사 확산과 부서 통합에 쓰는 사내 스킬 마켓과 Cron 헬스체크

한 부서에서 정착한 일하는 방식을 다른 부서나 지사로 넓힐 때는 에이전트·스킬 패키지를 사내 스킬 마켓으로 배포합니다. 화면 예시의 마켓에는 사내 등록 2개와 외부에서 가져온 49개를 합쳐 패키지 51개가 있고, 원본은 사내 저장소에, 배포본은 마켓 서버에 두며 태그 필터와 설치된 곳을 함께 보여 줍니다. 다만 지금 연결되는 에이전트 플랫폼은 Hermes Agent 1종이므로, 지사에도 같은 플랫폼이 설치돼 있어야 패키지가 그대로 동작합니

다. 같은 AAS 안의 다른 팀이 같은 업무를 시작할 때는 패키지를 만들 필요 없이, 그 팀 담당자가 자기 에이전트에서 「다른 에이전트에서 가져오기」로 새 프로파일을 만듭니다. 한 사람이 같은 업무를 다른 부서용으로 하나 더 둘 때는 자기 프로파일을 복제하고, 설치본이 다른 지사에는 프로파일을 내보낸 파일을 보내 지사 담당자가 PC에서 가져오기로 들여옵니다. 부서가 합쳐질 때는 Cron 헬스체크 화면에서 두 부서의 정기 업무를 나란히 놓고 같은 보고를 만드는 작업을 찾아 하나로 정리합니다. 정리 뒤 역할이 겹쳐 남는 프로파일은 내보내기로 보관본을 남기고 삭제하므로, 쓰지 않는 에이전트가 정기 업무를 계속 실행하는 일이 남지 않습니다.

감사 대응에 쓰는 흐름과 변경 기록

감사가 오면 무엇에 접근했고 누가 무엇을 바꿨는지를 흐름 화면과 변경 기록으로 제출할 수 있습니다. 흐름 화면은 스킬 문서·스크립트·실행 기록에서 자동으로 뽑은 호출 관계(스킬 → 스크립트 → 외부 호스트·자격증명)를 그리고, 선마다 근거가 된 문서의 줄을 붙이므로 사람이 그림을 따로 그려 관리하지 않습니다. AAS는 에이전트 플랫폼을 고치지 않고 얹는 방식이어서, 설정을 바꾸는 일은 플랫폼이 공식으로 제공하는 변경 경로로만 실행하고 누가 무엇을 바꿨는지는 AAS에 기록합니다. 이 감사 추적 기록은 보안·감사 담당자가 에이전트 도입을 승인할 때 확인할 증빙 자료가 됩니다.

회사 인수 때 일하는 방식째 넘기는 인계

회사를 인수하거나 사업부를 넘겨받을 때도 업무 매뉴얼 문서와 함께 에이전트 구성 자체를 인계할 수 있습니다. 넘겨받는 쪽은 프로파일과 스킬 문서로 그 조직이 어떤 업무를 어떤 순서로 처리했는지를 읽고, 정기 업무 목록으로 어떤 보고가 언제 나왔는지를 확인합니다. 아래 표는 조직이 바뀌는 여섯 순간에 에이전트 구성이 하는 역할과 그때 쓰는 AAS 화면을 정리한 것입니다.

조직이 바뀌는 순간	에이전트 구성이 하는 역할	쓰는 AAS 화면
담당자 퇴사·부서 이동	스킬·정기 업무·회의록·고객 일지가 조직에 남고, 멈춘 에이전트도 데이터 보존	에이전트(소유권 이전), 자격증명, Cron 헬스체크, 프로파일(내보내기·삭제)
신규 입사	자기 에이전트를 추가하고 전임자 구성을 가져오거나 역할 템플릿으로 시작	에이전트(추가), 프로파일(다른 에이전트에서 가져오기·PC에서 가져오기), 역할 템플릿
부서 통합	겹치는 정기 업무를 하나로 정리하고 남는 프로파일은 보관본을 남겨 삭제	Cron 헬스체크, 프로파일(내보내기·삭제)
지사 확산	에이전트·스킬 패키지를 같은 방식으로 배포, 프로파일은 가져오기나 내보낸 파일로 전달	사내 스킬 마켓, 프로파일(복제·다른 에이전트에서 가져오기·내보내기·PC에서 가져오기)
감사	접근한 시스템과 변경 이력을 증빙으로 제출	흐름, 변경 기록
회사 인수	일하는 방식을 에이전트 구성째 인계	프로파일, 스킬, 정기 업무

부서별 장면 카드가 보여 주는 것은 에이전트가 맡는 업무의 범위이고, 조직 변화 표가 보여 주는 것은 그 업무가 사람과 조직의 변화 뒤에도 이어지는 구조입니다. 따라서 첫 파일럿 대상은 장면 카드에서 시작 신호와 사람이 판단하는 단계가 분명하고, 결과물이 위키·CRM·드라이브처럼 조직이 이미 쓰는 시스템에 쌓이는 업무 가운데

서 고르는 것이 판단하기 쉽습니다. 명함 인식, 화자 구분 회의록, 공공서식 채우기는 세 조건을 모두 갖춘 대표 업무입니다. 업무 기능 단위의 확대 적용이 아직 10% 이하인 시장 상황을 감안하면[S4], 이런 업무 하나에서 정착을 확인한 뒤 사내 스킬 마켓으로 다른 부서에 넓히는 순서가 위험이 가장 작습니다. 9장은 이런 구성을 다른 선택지와 나란히 놓고 앞서는 점과 부족한 점을 비교합니다.

9장: 다른 선택지와 다른 점 — 제품별 비교로 본 AAS의 강점과 한계, 도입 검토 질문

8장까지 AAS가 무엇을 하는지 보았다면, 도입을 검토하는 조직은 이제 비슷한 일을 약속하는 여러 제품과 AAS를 나란히 놓고 고르게 됩니다. 1장에서 본 것처럼 에이전트를 품은 기업용 애플리케이션은 빠르게 늘고 있지만[S1], 업무 기능 하나를 놓고 보면 확대 적용 비율은 아직 10%를 넘지 않습니다[S4]. 제품은 많아졌지만 어떤 제품이 조직의 업무에 정착할지는 아직 가려지지 않았습니다. 이 장에서는 2장 표 2-2에서 고른 대표 제품 12개와 AAS를 실명으로 비교하고, AAS가 앞서는 여섯 항목과 아직 부족한 다섯 항목을 같은 무게로 적은 다음, 어느 공급사에게나 똑같이 던질 수 있는 도입 검토 질문을 제시합니다.

9.1 대표 제품 12개 비교표에서 외부 클라우드 사용 가능 여부가 가르는 AAS의 위치

AI Agent 도구 시장의 상용·오픈소스 제품은 무엇을 전제로 동작하느냐에 따라 다섯 묶음으로 나뉩니다. 묶음을 나누는 가장 큰 기준은 외부 클라우드를 쓸 수 있느냐입니다. Microsoft Copilot Studio 같은 글로벌 클라우드 빌더는 자사 클라우드와 자사 런타임을 전제로 하고, IBM watsonx Orchestrate나 삼성SDS FabriX 같은 온프레미스 상용 플랫폼은 에이전트 실행 엔진부터 화면까지 한 공급사가 일체형으로 제공하며, hermes-webui 같은 오픈소스 콘솔은 이미 설치된 에이전트 플랫폼 위에서 동작합니다. 같은 「에이전트를 만든다」는 기능이라도 어떤 제품을 고르느냐에 따라 데이터가 머무는 곳과 새로 들여야 하는 시스템의 범위가 달라집니다.

다섯 묶음의 강점은 서로 다른 자리에 있습니다. Microsoft Copilot Studio(+ Agent 365), Anthropic Claude Cowork, Dust로 이루어진 글로벌 클라우드 빌더는 스크립트까지 포함한 스킬 제작, 사내 마켓, 관리자 통제, 운영 이력에서 앞섭니다. IBM watsonx Orchestrate, 삼성SDS FabriX, 올거나이즈 Alli로 이루어진 온프레미스 상용 플랫폼은 빌더와 런타임, 스토어를 일체형으로 조직 안에 설치하고 부서별 비용 통제까지 갖췄습니다. Hermes Agent 내장 대시보드, hermes-webui, Ekko Studio, hermes-control-interface는 AAS와 같은 오픈소스 에이전트 플랫폼 위에서 동작하는 운영자용 콘솔로, 기능 폭과 커뮤니티, 개발 속도가 강점입니다. 플랫폼 중립 조직 운영 콘솔인 Paperclip은 여러 런타임과 비개발자 지향, 예산 자동 정지를, 채팅 워크스페이스인 Open WebUI는 LDAP·SCIM 같은 조직 기능과 그룹 권한, 채널을 내세웁니다. 묶음별 성격과 설치 형태는 2장 표 2-2에 제품마다 정리했습니다.

아래 두 비교표는 직접 써 본 결과가 아니라 각 공급사와 프로젝트가 공개한 공식 자료를 2026년 10월 8일 기준으로 읽은 결과이며, 제품별 출처는 2장 표 2-2와 같습니다[S9][S10][S11][S12][S13][S14][S15][S16][S17][S18][S19][S20][S21]. AAS의 칸은 현재 제공 기능을 기준으로 했습니다. 기호는 ○(있음), △(일부이거나 제약 있음), ×(공식 자료에서 확인되지 않음), ?(확인하지 못함), —(해당 없음)로 표시했습니다. 이 표는 순위표로 읽기보다, 조직이 어떤 조건을 반드시 지켜야 하는지에 따라 어느 열을 먼저 볼지 고르는 용도로 쓰는 편이 정확합니다.

표 9-1. 상용 제품과 AAS 비교

비교 항목	AAS	Copilot Studio	Claude Cowork	Dust	watsonx Orchestrate	FabriX	Alli
에이전트를 만든다	○	○	○	○	○	○	○
스크립트까지 포함한 스킬 제작	△	○	○	○	○	○	○
예약 실행	○	○	○	○	?	○	△
정기 업무 건강 감시 (실패·멈춤·알림 누락)	○	△	△	△	△	△	△
실제 호출 관계 시각화 (근거 줄 포함)	○	△	×	×	×	×	×
값을 보지 않는 자격증명 만료·중복 점검	○	×	×	×	×	×	×
사용자·그룹 단위 권한	△	○	○	○	○	○	○
사내 마켓	△	○	○	○	○	○	○
비용 한도·자동 정지	△	○	○	○	○	○	○
조직 안(온프레미스) 설치	○	?	×	×	○	○	○
쓰던 에이전트 플랫폼 위에 얹기	○	×	×	×	△	×	×
여러 에이전트 플랫폼 지원	×	×	×	×	△	×	×
운영 이력·사용자 규모	△	○	○	○	○	○	○

표 9-2. 오픈소스 제품과 AAS 비교

비교 항목	AAS	Hermes Agent 내장 대시보드	hermes-webui	Ekko Studio	hermes-control-interface	Paperclip	Open WebUI
에이전트를 만든다	○	○	○	○	○	○	○
스크립트까지 포함한 스킬 제작	△	△	△	△	×	○	○
예약 실행	○	○	○	○	○	○	○
정기 업무 건강 감시 (실패·멈춤·알림 누락)	○	△	△	△	○	△	×
실제 호출 관계 시각화 (근거 줄 포함)	○	×	×	△	×	×	×
값을 보지 않는 자격증명 만료·중복 점검	○	△	×	×	×	△	×
사용자·그룹 단위 권한	△	×	×	?	○	○	○
사내 마켓	△	△	×	×	×	○	△
비용 한도·자동 정지	△	○	△	○	○	○	△
조직 안(온프레미스) 설치	○	○	○	○	○	○	○
쓰던 에이전트 플랫폼 위에 얹기	○	—	○	○	○	○	—
여러 에이전트 플랫폼 지원	×	×	×	○	×	○	—

비교 항목	AAS	Hermes Agent 내장 대시보드	hermes-webui	Ekko Studio	hermes-control-interface	Paperclip	Open WebUI
운영 이력·사용자 규모	△	○	○	○	△	○	○

「에이전트를 만든다」 행은 모든 제품이 ○입니다. AAS에서는 사람마다 에이전트를 받고 그 안에 업무별 프로파일을 둡니다. 에이전트는 사용자 한도 안에서 추가하고 지우며 소유권을 다른 사람에게 넘길 수 있고, 프로파일은 기존 프로파일을 복제하거나 다른 에이전트에서 가져와 만든 뒤 성격·스킬·정기 업무를 다듬습니다. 표를 가로로 읽으면 AAS의 ○는 관측과 설치 방식에 관한 항목에 모여 있고, ×와 △는 스크립트 스킬 제작, 조직 통제, 운영 이력, 여러 플랫폼 지원에 관한 항목에 모여 있습니다. Copilot Studio와 Claude Cowork의 ×와 ?는 조직 안 설치, 쓰던 플랫폼 위에 얹기, 값을 보지 않는 자격증명 점검에 몰려 있습니다. 오픈소스 쪽에서는 hermes-control-interface가 예산 알림으로 정기 업무 건강 감시 행에서 ○를 받았지만 운영 이력은 △로, 2026년 6월 이후 새 커밋이 없습니다[S19]. 결국 이 표가 보여 주는 차이는 기능의 많고 적음보다 각 제품이 무엇을 전제로 설계되었느냐에서 나오며, 그 전제가 조직의 보안 규정과 맞는지가 첫 판단 기준이 됩니다. 예를 들어 외부 클라우드 사용이 금지된 조직에서는 Copilot Studio 열의 ○가 아무리 많아도 도입 대상이 될 수 없으므로, 조직 안 설치 행에서 ○를 받은 열만 남기고 나머지 항목을 비교하는 순서가 맞습니다.

9.1.1 외부 클라우드를 쓸 수 있는 조직에서 Copilot Studio·Claude Cowork가 앞서는 영역

Copilot Studio·Claude Cowork의 완성도 우위

외부 클라우드를 쓸 수 있는 조직이라면 Copilot Studio와 Claude Cowork의 완성도가 AAS보다 높습니다. 비교표에서 두 제품은 스크립트까지 포함한 스킬 제작, 사용자·그룹 단위 권한, 사내 마켓, 비용 한도의 네 항목에서 모두 ○를 받았고, AAS는 같은 네 항목에서 △에 머뭅니다. 두 제품은 운영 이력과 사용자 규모에서도 ○를 받아, 장애 대응 절차나 교육 자료처럼 제품 바깥의 준비물을 구하기 쉽습니다. Microsoft 365와 Azure를 쓸 수 있는 조직이라면 Copilot Studio 쪽이 완성도가 높고, 데이터를 외부 클라우드에 둘 수 있으며 공급사의 런타임을 그대로 받아들일 수 있는 조직이라면 이 두 제품을 먼저 검토하는 것이 합리적입니다.

사내 마켓과 관리자 통제의 성숙도

글로벌 클라우드 빌더가 특히 앞서는 자리는 마켓 운영과 관리자 통제입니다. Copilot Studio의 Agent Store와 Claude Cowork의 사설 플러그인 마켓에서는 부서가 만든 에이전트를 다른 부서로 배포할 수 있고, 관리자는 Claude Cowork의 지출 한도 같은 통제 기능을 씁니다[S11]. AAS는 프로파일 복제와 편집기로 업무 프로파일을 만들고 사내 마켓도 갖췄지만, 마켓은 사내 등록과 외부 패키지 가져오기까지만 제공하고 결제와 지출 한도는 없습니다.

watsonx Orchestrate·FabriX·Alli가 앞서는 온프레미스 일체형 기능

외부 클라우드를 쓸 수 없는 조직에서도 watsonx Orchestrate, FabriX, Alli는 AAS보다 넓은 기능 폭을 제공합니다. FabriX와 Alli는 비개발자 빌더, 사내 스토어나 앱 마켓, 폐쇄망을 포함한 온프레미스 설치, 부서별 비용 통제를 한 제품으로 묶어 국내 조직의 요구에 맞춰 왔기 때문에, AAS와 가장 직접적으로 부딪치는 제품입니다[S14][S15]. 다만 세 제품은 에이전트 실행 엔진까지 공급사가 제공하는 일체형이므로, 이미 오픈소스 에이전트 플랫폼을 운영하는 조직은 그 플랫폼을 바꾸거나 두 체계를 함께 운영해야 합니다. watsonx Orchestrate는 외부 에이전트를 함께 조율하는 기능을 밝혀 「쓰던 플랫폼 위에 얹기」 행에서 △를 받았지만[S13], 이 역시 IBM

의 제어 평면이 중심이 되는 구조입니다. 기능 폭에서는 이 세 제품이 앞서고, 기존 투자를 그대로 두는 방식에서는 AAS가 다른 선택지가 됩니다.

9.1.2 망 분리 조직과 오픈소스 플랫폼 보유 조직에서 AAS가 맞는 조건

망 분리 조직의 설치 조건

외부 클라우드를 쓸 수 없는 조직에서는 Copilot Studio, Claude Cowork, Dust가 처음부터 선택지에서 빠지고, 그때부터 AAS가 검토 대상이 됩니다. 국내 공공 부문은 망 분리 규제를 고쳐 가고 있으며, 그 방향은 정보 등급별로 통제를 달리하는 것입니다. 국가 망 보안체계 가이드라인은 업무 정보를 기밀(C)·민감(S)·공개(O) 세 등급으로 나누고 등급에 따라 보안 통제를 차등 적용하며[S5], 정부는 18년 만에 공공망 분리 규제를 고치면서도 기밀 등급 업무는 분리된 망에 두도록 했습니다[S6]. 2026년 3월에는 공공기관 업무 PC에서 생성형 AI를 쓰는 새 체계의 시범 공모가 시작됐습니다[S7]. 따라서 생성형 AI를 쓰는 범위는 넓어지더라도, 기밀 등급 업무를 맡는 에이전트는 계속 조직 안에 두어야 합니다.

오픈소스 에이전트 플랫폼을 이미 쓰는 조직의 조건

두 번째 조건은 조직이 이미 오픈소스 에이전트 플랫폼을 쓰고 있느냐입니다. AAS는 오픈소스 에이전트 플랫폼인 Hermes Agent 위에 얹히는 콘솔이며, 플랫폼의 플러그인·설정·버전을 바꾸지 않고 플랫폼이 공식으로 제공하는 변경 경로 하나만 씁니다. Hermes Agent를 운영하는 조직은 에이전트 실행 엔진을 바꾸지 않고, 그 위에 업무 담당자용 화면과 관측 화면을 더하는 방식으로 도입할 수 있습니다. 같은 플랫폼 위의 오픈소스 콘솔도 같은 방식으로 얹히지만, 한 사람이 쓰는 환경이라면 hermes-webui가 AAS보다 나은 선택일 수 있고, Ekko Studio는 업무 사용이 상업 사용에 해당해 별도 라이선스가 필요하며[S18], hermes-control-interface는 활동이 멎어 있어 지속성을 따로 확인해야 합니다. 다만 현재 AAS가 연결되는 에이전트 플랫폼은 Hermes Agent 1종이므로, 다른 플랫폼을 쓰는 조직은 두 번째 플랫폼 연결이 로드맵에 올라 있다는 사실(10.1)을 확인하고 일정을 공급사와 따로 맞춰야 합니다.

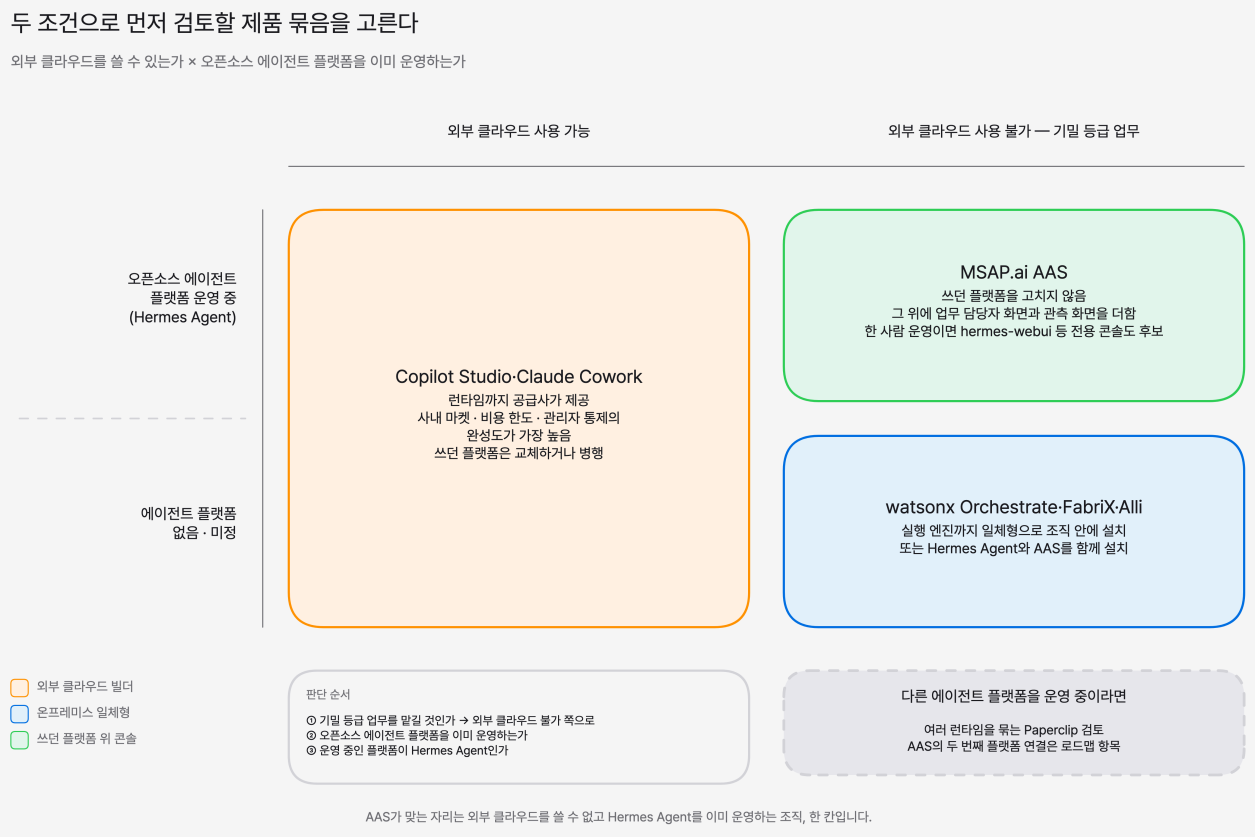


그림 9-1. 외부 클라우드 사용 가능 여부와 오픈소스 에이전트 플랫폼 보유 여부로 나눈 네 가지 조직 조건과 각 조건에서 먼저 검토할 제품 묶음

조건 점검표

정리하면, 아래 네 가지 질문에 대한 답이 AAS가 맞는 조직과 다른 제품이 맞는 조직을 가릅니다. 첫 질문에 「아니요」이고 둘째 질문에 「예」라면 AAS가 맞는 조건이며, 첫 질문에 「예」라면 Copilot Studio나 Claude Cowork를 먼저 검토하는 것이 맞습니다.

점검 질문	「예」일 때	「아니요」일 때
업무 데이터를 외부 클라우드에 둘 수 있는가	Copilot Studio·Claude Cowork·Dust 우선 검토	조직 안 설치 제품(AAS, watsonx Orchestrate, FabriX, Alli, Hermes Agent 위 콘솔, Paperclip)으로 좁힘
Hermes Agent를 이미 운영하거나 도입할 계획인가	AAS 또는 hermes-webui 등 Hermes Agent 위 콘솔	watsonx Orchestrate·FabriX·Alli 또는 Paperclip 검토
여러 사람이 각자 에이전트를 만들고 관리자가 전체를 봐야 하는가	AAS, watsonx Orchestrate·FabriX·Alli	한 사람 운영이면 Hermes Agent 내장 대시보드나 hermes-webui로 충분할 수 있음
마켓 결제와 부서별 비용 통제가 첫 도입의 필수 조건인가	Copilot Studio·Claude Cowork, FabriX 등 상용 제품	AAS로 시작 가능

9.2 정기 업무 건강 감시와 값 없는 자격증명 관리 등 AAS가 앞서는 여섯 항목

AAS가 다른 제품보다 앞서는 항목은 여섯 가지이며, 대부분 6장과 7장에서 화면으로 보인 기능을 비교 항목으로 다시 묶은 것입니다. 이 여섯 항목은 에이전트를 만드는 기능보다 에이전트가 사람이 보지 않는 동안 무엇을 했는지 드러내는 기능에 몰려 있습니다. 이 방향은 시장 전망과도 맞습니다. 2장에서 본 것처럼 Gartner는 에이전트를 감독하는 감독용 에이전트가 2030년까지 에이전트형 AI 시장의 10~15%를 차지하고, 2028년까지 허가되지 않은 에이전트 행위의 80% 이상이 정보 과다 공유나 부적절한 사용 같은 내부 정책 위반에서 나온다고 전망했습니다[S3]. 에이전트를 만든 뒤 지켜보는 기능이 앞으로 도입 판단의 중요한 기준이 됩니다. 다만 아래 항목은 「다른 제품에 없다」가 아니라 「공식 자료에서 전면에 내세운 곳을 확인하지 못했다」는 뜻이므로, 차별점으로 판단하려면 실제 화면을 놓고 비교해야 합니다.

앞서는 항목	AAS가 하는 일	다른 제품의 일반 수준	근거 장
정기 업무 건강 감시	안 돈 작업과 알림이 안 가는 작업을 먼저 보여 줌	실행 로그와 분석 화면	6장
실제 호출 관계 시각화	실행 기록에서 뽑은 호출 관계와 근거 줄	사람이 그린 설계 흐름	6장
값 없는 자격증명 관리	값 없이 만료·빈 값·중복·쓰는 곳 표시	비밀값 저장	6장·7장
쓰던 플랫폼 위에 얹는 방식	플랫폼을 고치지 않고 공식 변경 경로만 씀	일체형 또는 플랫폼 교체	7장
만들기와 지켜보기가 한 화면	만들고 실패를 확인하는 메뉴가 한 콘솔에 있음	빌더와 관제 도구가 따로 있음	4장
업무 에이전트 카탈로그 동봉	명함·회의록·공문 등 업무 에이전트 예시 제공	빈 빌더에서 시작	5장

9.2.1 관측 기능에서 앞서는 정기 업무 감시와 호출 관계 시각화

정기 업무 건강 감시의 비교 우위

다른 제품도 예약 실행과 실행 로그를 제공하지만, 대부분은 실행된 작업의 결과를 보여 주는 데서 그칩니다. Copilot Studio는 분석 화면을, watsonx Orchestrate는 평가 대시보드를, FabriX는 활동 기록을 제공하는 수준입니다[S9][S13][S14]. AAS의 Cron 헬스체크 화면은 「돌았어야 할 작업이 안 돌았다」와 「실패해도 알림이 갈 곳이 없다」를 먼저 보여 줍니다. Cron 헬스체크 화면은 정기 업무 95개 중 알림이 안 가는 작업 15개를 목록으로 드러내고, 이미 회복된 실패 기록 62건을 지금도 실패 중인 작업과 따로 나눠, 오래된 기록이 진짜 문제를 가리지 않게 합니다. 이 차이가 중요한 이유는 무인 실행 작업의 실패 알림이 그 작업에 지정된 전달 대상으로만 가기 때문입니다. 따라서 전달 대상이 없는 작업은 실패해도 아무도 모르며, 이런 작업을 찾아내는 기능은 실행 로그만으로는 대신할 수 없습니다.

실제 호출 관계와 자격증명의 비교 우위

흐름 화면은 스킬 문서, 스크립트, 실행 기록에서 뽑은 실제 호출 관계(스킬 → 스크립트 → MCP 서버·외부 서비스)를 그리고, 선마다 그 관계를 찾은 근거 줄을 붙입니다. Microsoft Agent 365의 에이전트 맵은 IT·보안

관리자가 에이전트 사이의 연결을 보는 화면이고[S10], Ekko Studio의 캔버스는 사람이 설계한 워크플로를 그리는 화면이어서[S18], 설계와 실제 실행이 어긋나도 그림은 바뀌지 않습니다. 자격증명 화면은 값을 보지 않고 상태만 훑습니다. 자격증명 화면은 103개 항목 중 만료되었거나 만료가 임박한 7개, 값이 빈 3개, 여러 곳에 복사된 17개를 보여 줍니다. Hermes Agent 내장 대시보드에도 키 화면이 있고 Paperclip은 시크릿을 암호화해 저장하지만[S16][S20], 만료와 중복, 쓰는 곳을 값 없이 훑는 기능은 공식 자료에서 확인되지 않습니다. 값 없이 상태를 보는 방식은 앞서 본 내부 정책 위반 전망[S3]처럼 조직 내부에서 생기는 노출 위험을 살피는 데 쓰입니다. 다만 화면이 원인을 드러낼 뿐 고치는 일은 담당자가 해야 하며, AAS는 그 판단에 필요한 목록을 먼저 보여 주는 역할을 맡습니다.

9.2.2 업무 카탈로그 동봉과 한 화면 통합이 도입 기간에 주는 차이

만들기와 지켜보기를 한 화면에 둔 효과

AI Agent 도구 시장은 에이전트를 만드는 빌더와 운영 상태를 감시하는 관제 도구로 나뉘어 있고, Microsoft도 만드는 쪽의 Copilot Studio와 관제하는 쪽의 Agent 365를 따로 둡니다[S9][S10]. 빌더는 관제 기능이 얕고 관제 도구는 에이전트를 만들지 못합니다. AAS는 에이전트와 그 안의 업무별 프로파일, 스킬, 정기 업무를 만드는 메뉴와 Cron 헬스체크, 흐름, 자격증명을 보는 메뉴를 한 콘솔에 둡니다. 업무 담당자는 자신이 만든 정기 업무가 실패했을 때 다른 도구로 옮기지 않고 같은 화면에서 원인을 보고 설정을 고칠 수 있습니다. 두 도구를 따로 들일 때 생기는 계정 연결, 권한 설계, 교육 부담이 한 번으로 줄어듭니다.

업무 에이전트 카탈로그가 줄이는 준비 기간

빌더 제품은 대부분 빈 화면에서 시작하므로, 조직은 첫 에이전트를 만들기 전에 어떤 업무를 맡길지부터 설계해야 합니다. Alli처럼 직군별 에이전트 100여 개를 앱 마켓에 담아 두는 제품도 있지만[S15], 이는 공급사 플랫폼 안에서 쓰는 앱입니다. AAS는 명함 인식, 공공문서와 공공서식 인식, 화자 구분 회의록과 지시사항 정리, 영업 보고, 관제 같은 업무 에이전트 예시를 함께 제공합니다. 운영 화면에는 업무 에이전트 11개와 스킬 313개가 등록된 모습이 보이고, 배포본에는 마케팅·영업·연구소·총무·회계·인사 등 역할 템플릿 20종과 마켓 패키지 51개가 들어 있습니다. 다만 명함을 등록할 CRM, 회의록을 올릴 위키, 문서를 보관할 드라이브 같은 연결 시스템은 고객 환경에 맞춰 설정합니다. 카탈로그는 완성품이라기보다 조직의 첫 유즈케이스를 고르는 출발점이며, 파일럿 대상을 정하는 기간을 줄이는 데 쓰입니다.

항목	내용	도입 기간에 주는 차이
한 화면 통합	만들기 메뉴와 지켜보기 메뉴가 같은 콘솔에 있음	계정·권한·교육을 한 번에 준비
역할 템플릿 20종	부서·역할별 성격(SOUL)을 채우는 출발점	첫 프로파일을 다듬는 시간을 줄임
업무 에이전트 카탈로그	명함·회의록·공문·영업·관제 등 예시	첫 유즈케이스 선정의 기준점
사내 마켓	부서가 만든 스킬을 다른 부서가 설치	잘 만든 스킬의 사내 확산

9.3 연결 플랫폼 1종과 마켓 결제 미지원 등 아직 부족한 다섯 항목

AAS에는 다른 제품보다 부족한 항목이 다섯 가지 있으며, 도입을 검토하는 조직은 이 항목을 강점과 같은 무게로 따져야 합니다. 부족한 항목은 두 갈래로 나뉩니다. 하나는 로드맵(10.1)에 올라 있어 제품이 메워 갈 항목이

고, 다른 하나는 당장은 운영 규칙으로 보완해야 하는 항목입니다. 이 구분이 필요한 이유는 한계가 첫 유즈케이스에 걸리면 도입 범위를 다시 정해야 하기 때문이며, McKinsey 조사에서도 업무 기능 하나에서 에이전트 확대 적용 비율은 10%를 넘지 않아 대부분의 조직이 아직 좁은 범위에서 시작하고 있습니다[S4]. 따라서 부족한 항목이 첫 유즈케이스에 걸리는지를 먼저 확인하면, 도입 범위를 좁게 정하고 위험을 미리 알 수 있습니다.

부족한 항목	지금 할 수 있는 것	대응
두 번째 에이전트 플랫폼 연결 없음	Hermes Agent 1종 연결	로드맵(10.1)
마켓 결제 없음	사내 등록과 외부 패키지 가져오기, 프로파일 설치	로드맵(10.1) 마켓 운영
스크립트가 필요한 스킬은 콘솔에서 고칠 수 없음	스킬 문서 편집, 스크립트 보기, 흐름 화면으로 호출 관계 확인	운영 규칙(역할 분담)
비용 자동 정지·부서별 할당 없음	사용량 보기	운영 규칙(모델 게이트웨이 한도)
그룹·부서 권한 미흡	표준 로그인(OIDC), 사람마다 배정되는 에이전트와 개수 한도, 그룹 탈퇴 시 멈춤	운영 규칙(부서별 소유자 지정)

다섯 항목마다 앞선 제품이 분명히 있습니다. 마켓 결제는 Copilot Studio, Claude Cowork, FabriX, Alli가 먼저 갖췄고, 스크립트까지 포함한 스킬 제작은 상용 제품 전반이 AAS보다 깊습니다. 여러 플랫폼 연결, 비용 통제, 그룹 권한에서 앞선 제품은 아래 두 항에서 한계마다 함께 적었습니다.

9.3.1 로드맵 둘째·셋째 순서에 놓인 마켓 결제와 두 번째 플랫폼 연결

연결 플랫폼 1종과 여러 런타임을 붙이는 제품

현재 연결되는 에이전트 플랫폼은 Hermes Agent 1종이며, 다른 플랫폼을 쓰는 조직은 지금 AAS를 바로 쓸 수 없습니다. Paperclip은 어댑터 구조로 여러 에이전트 런타임을 붙이고 Ekko Studio는 Hermes Agent를 포함한 여러 런타임을 지원하므로[S18][S20], 플랫폼을 섞어 쓰는 조직에서는 이 두 제품이 앞섭니다. 마켓도 사내 등록과 외부 패키지 가져오기까지만 제공하므로, 부서 사이에 스킬 사용료를 정산하거나 판매 권한을 나눠야 하는 조직은 Copilot Studio, Claude Cowork, FabriX, Alli의 마켓이 먼저 맞습니다.

AAS 로드맵의 세 항목 순서

로드맵은 날짜 대신 순서로 정해져 있으며, 아래 세 항목이 차례로 놓입니다. 이 중 뒤의 두 항목이 9.3의 한계와 직접 대응합니다.

1. 만들고 지울 수 있는 협업 방
2. 마켓 운영(결제·권한 구분 포함)
3. 두 번째 에이전트 플랫폼 연결

마켓 결제는 로드맵의 둘째, 두 번째 플랫폼 연결은 셋째 순서에 있으므로, 이 두 기능이 꼭 필요한 조직은 공급사와 시점을 따로 확인한 뒤 도입 범위를 정하는 것이 맞습니다.

한계	대응하는 로드맵 항목	로드맵 순서
마켓 결제 없음	마켓 운영	2
연결 플랫폼 1종	두 번째 에이전트 플랫폼 연결	3

로드맵 순서에서 보듯, 첫 도입 범위를 정할 때는 현재 제공되는 기능만으로 끝나는 업무를 고르는 편이 안전합니다. 명함 인식이나 화자 구분 회의록처럼 스킬 문서와 정기 업무만으로 동작하고 Hermes Agent 위에서 실행되는 업무는 위 두 가지 한계의 영향을 거의 받지 않습니다. 반면 부서 사이에 스킬을 사고팔거나 다른 에이전트 플랫폼과 섞어 써야 하는 업무는 해당 로드맵 항목이 제공된 뒤로 미루는 것이 도입 위험을 줄이는 방법입니다. 그룹·부서 권한과 비용 통제는 로드맵을 기다리지 않고 아래 운영 규칙으로 보완합니다.

9.3.2 비용 자동 정지와 부서별 권한처럼 운영 규칙으로 보완하는 한계

비용 통제를 보완하는 모델 게이트웨이 한도

AAS는 활동 화면과 대시보드에서 누가 얼마나 쓰는지 보여 주지만, 한도를 넘으면 실행을 멈추는 자동 정지나 부서별 예산 할당은 제공하지 않습니다. FabriX는 부서·사용자별 할당량을, Paperclip은 예산 자동 정지를, Claude Cowork는 지출 한도를 제공합니다[S11][S14][S20]. 이 한계는 운영 규칙으로 보완할 수 있습니다. AAS가 모델 목록을 읽는 모델 게이트웨이(LiteLLM)에 키별 예산 한도를 걸어 두고, 부서마다 다른 키를 쓰게 하면 AAS 화면에서는 사용량을 보고 실제 한도는 게이트웨이가 지키는 분담이 됩니다.

그룹·부서 권한과 스크립트 스킬의 역할 분담

AAS는 표준 로그인(OIDC)으로 사용자를 받고, 사용자마다 볼 수 있는 에이전트와 에이전트 한도를 정하며, OIDC 그룹에서 빠진 사용자의 에이전트는 멈춥니다. 부서 단위로 권한 묶음을 주는 기능은 아직 얕으므로, 부서별로 에이전트 소유자를 지정하고 관리자가 전체를 보는 운영 규칙으로 보완합니다. 이 항목은 역할 기반 권한(RBAC)과 사용자 그룹, SCIM 연동을 오픈소스 버전 기능으로 밝힌 Open WebUI가 앞서 있습니다[S21]. 스크립트가 필요한 스킬은 콘솔에서 고칠 수 없는데, 이는 연결된 플랫폼에 스크립트를 저장하는 공식 경로가 없기 때문입니다. 그래서 IT 담당자가 스크립트를 맡고 부서 담당자는 스킬 문서를 맡는 분담이 현실적이며, 흐름 화면이 어떤 스킬이 어떤 스크립트를 부르는지 보여 주므로 두 사람이 같은 그림을 보고 일을 나눌 수 있습니다.

한계	운영 규칙으로 보완하는 방법	맡는 사람
비용 자동 정지 없음	모델 게이트웨이(LiteLLM)에 키별 예산 한도, 부서별 키 분리	IT·플랫폼 관리자
부서별 비용 할당 없음	부서별 키 사용량을 정기 보고에 포함	IT·플랫폼 관리자, 부서장
그룹·부서 권한 미흡	부서별 에이전트 소유자 지정, 관리자 전체 보기	IT·플랫폼 관리자
스크립트 스킬 편집 불가	스크립트는 IT 담당자, 스킬 문서는 부서 담당자	IT 담당자, 부서 담당자

9.4 무인 실행 감독과 비밀값 처리, 플랫폼 변경 여부를 묻는 도입 검토 질문 목록

도입 검토 질문은 AAS를 포함한 모든 후보 공급사에게 똑같이 던져야 비교가 공정해집니다. 질문의 초점은 기능 목록보다 사람이 보지 않는 동안 에이전트가 무엇을 하는지, 그리고 조직이 바뀔 때 무엇이 남는지에 둡니다. 묻는 이유는 9.2에서 본 것처럼 에이전트 관련 위험의 상당 부분이 조직 내부에서 생기기 때문입니다. 따라서 아래 질문표는 경쟁 평가 회의와 내부 보고서에 그대로 옮겨 쓸 수 있도록, 질문마다 확인 방법과 AAS의 해당 장을 함께 적었습니다.

9.4.1 무인 실행과 자격증명 관리에 관한 공급사 공통 질문

무인 실행 감독에 관한 질문

정기 업무로 실행되는 에이전트는 담당자가 화면을 보지 않는 시간에 일하므로, 실패를 어떻게 알게 되는지가 첫 질문입니다. 실패 알림을 받을 대상이 지정되지 않은 작업은 실패해도 아무에게도 알리지 않으므로, 이런 작업을 목록으로 찾을 수 있는지를 따로 물어야 합니다. 데이터를 읽지 못했을 때 그 결과를 0건으로 표시하는지, 「수집 실패」로 따로 표시하는지도 확인해야 합니다. 0건과 수집 실패를 구분하지 않는 화면에서는 문제가 없는 상태와 데이터를 읽지 못한 상태가 같아 보이기 때문입니다.

비밀값과 자격증명에 관한 질문

에이전트는 메신저 토큰, 외부 서비스 키, 모델 게이트웨이 키처럼 여러 비밀값을 씁니다. 도입 전에는 비밀값이 화면, 로그, 변경 기록 가운데 어디에라도 남는지를 확인하고, 만료와 중복 복사를 값을 보지 않고 점검할 수 있는지를 물어야 합니다. 같은 토큰 값이 여러 곳에 복사돼 있으면 한 곳에서 키를 바꿔도 나머지 작업이 멈추므로, 「쓰는 곳」을 보여 주는 기능이 있는지가 운영 부담을 크게 가릅니다.

실행 결과 검증과 승인 담당자에 관한 질문

무인 실행 감독과 함께 물어야 할 것은 실행이 끝난 뒤 결과가 맞는지를 누가 확인하느냐입니다. 위험 명령 승인은 삭제나 외부 발송처럼 되돌리기 어려운 명령이 실행되기 직전에 개입할 뿐, 명령 자체는 안전해도 내용이 틀린 산출물까지 걸러 주지는 않습니다. 오픈소스 에이전트 플랫폼의 공개 문서를 기능 요구 항목에 대조해 보아도 실행 결과 검증은 플랫폼이 기본으로 맡지 않는 영역으로 남습니다[R1]. 따라서 검증을 누가, 언제, 무엇을 기준으로 할지는 조직이 정해야 하고, 승인 알림이 왔을 때 판단할 담당자와 그 사람이 자리에 없을 때 대신할 사람도 미리 지정해 두어야 합니다. 공급사에는 이 검증 절차와 대리 승인자를 제품의 어느 화면과 기록에 걸 수 있는지를 함께 물으면 됩니다.

질문	확인 방법	AAS의 답(해당 장)
사람이 보지 않을 때 실패한 정기 작업을 어떻게 알 수 있는가	실패·멈춤을 집계하는 화면을 시연으로 확인	Cron 헬스체크 화면의 네 집계(6장)
알림이 안 가는 작업을 목록으로 찾을 수 있는가	전달 대상이 없는 작업을 일부러 만들어 표시되는지 확인	알림이 안 가는 작업 목록과 하루 두 번 요약(6장)
이미 회복된 실패와 지금 실패 중인 작업을 구분하는가	회복된 기록이 경고에 섞이는지 확인	지금도 실패 / 이미 회복 구분(6장)
읽지 못한 데이터를 0건으로 표시하지 않는가	수집 대상을 끊고 화면 표시를 확인	「수집 실패」로 표시(7장)
비밀값이 화면·로그·기록에 남는가	화면, 로그, 변경 기록을 직접 검색	어디에도 남기지 않음(7장)

질문	확인 방법	AAS의 답(해당 장)
자격증명 만료·중복·쓰는 곳을 값 없이 볼 수 있는가	만료 임박 키와 중복 키로 시연	자격증명 화면(6장)

9.4.2 플랫폼 변경 여부와 조직 안 설치, 인계에 관한 공급사 공통 질문

플랫폼 변경과 조직 안 설치에 관한 질문

콘솔을 들이기 위해 이미 운영 중인 에이전트 플랫폼의 플러그인, 설정, 버전을 바꿔야 하는지가 구조에 관한 첫 질문입니다. 플랫폼을 고쳐야 하는 제품은 플랫폼을 올릴 때마다 콘솔과의 호환을 다시 확인해야 하므로 운영 부담이 늘어납니다. 망 분리 환경에서는 설치 과정에서 외부 저장소에서 내려받거나 빌드해야 하는 단계가 있는지, 음성 인식이나 문서 인식(OCR) 같은 처리를 조직 안에서 끝낼 수 있는지를 확인해야 합니다. 국가 망 보안체계가 시행되더라도 기밀 등급 업무는 분리된 망에 남으므로[S6], 이 질문은 공공기관에서 계속 유효합니다. AAS는 에이전트 플랫폼을 고치지 않고 얹히며, 외부 내려받기나 빌드 없이 조직 안에서 설치·실행되고, 쿠버네티스 배포본도 제공합니다.

사람과 조직이 바뀔 때 남는 것에 관한 질문

마지막 질문은 담당자가 떠나거나 부서가 합쳐질 때 무엇이 남느냐입니다. 에이전트의 성격, 스킬, 정기 업무, 호출 관계, 자격증명 목록이 조직의 자산으로 남아 다음 담당자에게 넘어가는지, 아니면 개인 계정과 함께 사라지는지를 물어야 합니다. 누가 무엇을 바꿨는지 기록이 어디까지 남는지도 확인해야 합니다. 예를 들어 AAS의 변경 기록은 콘솔을 거친 변경만 남기고, 플랫폼의 관리 화면이나 명령줄에서 직접 바꾼 내용은 담지 못하므로, 변경 경로를 콘솔로 모으는 운영 규칙을 함께 정해야 합니다.

질문	확인 방법	AAS의 답(해당 장)
쓰던 에이전트 플랫폼을 고쳐야 하는가	설치 전후 플랫폼의 플러그인·설정·버전 비교	고치지 않음, 공식 변경 경로 하나만 씀(7장)
망 분리 환경에 외부 내려받기 없이 설치되는가	외부망을 끊은 시험 환경에서 설치	조직 안에서 설치, 쿠버네티스 배포본(7장)
음성 인식·OCR 처리를 조직 안에서 끝낼 수 있는가	처리 중 외부 호출 여부 확인	조직 안에서 처리(5장·7장)
담당자가 떠나면 에이전트 구성이 남는가	담당자 계정을 비활성화한 뒤 구성 유지 확인	에이전트·스킬·정기 업무가 조직에 남음(8장)
누가 무엇을 바꿨는지 어디까지 기록되는가	콘솔 밖에서 바꾼 내용이 기록되는지 확인	콘솔을 거친 변경만 기록(4장·7장)
지원하는 에이전트 플랫폼은 몇 종인가	지원 목록과 추가 계획 확인	Hermes Agent 1종, 두 번째 연결은 로드맵(10장)

위 열두 질문은 공급사의 설명 자료만으로는 답을 가릴 수 없으므로, 시연이나 시험 설치에서 직접 확인하는 방식으로 쓰는 것이 좋습니다. 알림이 안 가는 작업, 수집 실패 표시, 비밀값 노출 여부처럼 정상 상태에서는 드러나지 않는 항목은 일부러 실패 조건을 만들어 화면이 어떻게 반응하는지 보아야 차이가 보입니다. AAS 역시 같

은 방식으로 시연할 수 있으며, 질문마다 해당 장의 화면과 설명을 대조하면 강점과 한계를 같은 기준으로 판단할 수 있습니다. 10장은 이 비교를 바탕으로 첫 유즈케이스 하나를 골라 도입을 시작하는 방법을 다룹니다.

10장: 로드맵과 첫 유즈케이스 하나로 시작하는 4단계 도입 방법

9장의 비교에서 AAS가 맞는 조건을 확인했다면, 남은 일은 무엇으로 어떻게 시작할지를 정하는 것입니다. 1장에서 본 것처럼 에이전트를 품은 기업용 애플리케이션은 빠르게 늘고 있지만[S1], 에이전트형 AI 프로젝트의 40% 이상은 2027년 말까지 중단될 것이라는 전망도 있습니다[S2]. 따라서 도입 의사결정은 두 가지 확인으로 나뉩니다. 하나는 AAS가 지금 무엇을 제공하고 다음에 무엇이 추가되는지이고, 다른 하나는 조직이 어떤 업무 하나로 시작할지입니다. 10장은 현재 제공 범위와 추가 순서, 첫 유즈케이스 선정 기준, 단계마다 판단 기준을 둔 파일럿 4단계, 역할별 준비 목록을 차례로 제시하고 파일럿 대상을 확정하는 회의 안건으로 마무리합니다.

10.1 사용자별 에이전트까지 제공되는 현재 범위와 협업 방에서 두 번째 플랫폼 연결로 이어지는 로드맵 순서

AAS 로드맵은 날짜 대신 순서로 관리됩니다. 지금 제공되는 범위는 에이전트 운영 상태를 보는 기능, 그 화면에서 설정을 고치는 기능, 콘솔 안에서 에이전트에게 일을 맡기는 기능, 사람마다 자기 에이전트를 받아 쓰는 기능의 네 묶음입니다. 이어지는 순서는 필요할 때 만들고 끝나면 지우는 협업 방, 사내 마켓 운영, 두 번째 에이전트 플랫폼 연결의 세 항목입니다. 1장에서 본 시험과 정착의 간극[S4]을 고려하면, 업무 정착을 좌우하는 것은 제품이 앞으로 갖출 기능의 폭보다 지금 바로 쓸 수 있는 범위이며, 도입 검토자는 9장 3절에서 본 한계 하나하나가 로드맵의 어느 순서에서 메워지는지를 함께 확인해야 합니다.

10.1.1 사용자별 에이전트까지 갖춰 파일럿을 바로 시작할 수 있는 현재 제공 범위

지금 제공되는 네 묶음 기능

AAS가 현재 제공하는 기능은 보기, 고치기, 시키기, 사용자별 에이전트의 네 묶음이며 넷 모두 운영 화면에서 쓸 수 있습니다. 보기 묶음은 Cron 헬스체크, 흐름, 스킬, 활동, 채널, 모델, 자격증명 화면으로 구성되고, 정기 업무가 사람이 보지 않는 동안 어떻게 실행됐는지를 먼저 보여 줍니다. 고치기 묶음은 정기 업무, 스킬 문서, 프로파일, 비밀값을 그 화면에서 바로 수정하는 기능이며, 프로파일을 복제하거나 다른 에이전트에서 가져와 새로 만들고, 내보낸 뒤 지우는 작업도 여기에 들어갑니다. 이때 모든 변경은 에이전트 플랫폼의 공식 API 한 경로로만 나가고, 누가 무엇을 바꿨는지는 AAS의 변경 기록에 남습니다. 시키기 묶음은 채팅에서 에이전트를 고르고, 진행 단계를 보고, 실행 전에 승인하고, 에이전트의 되묻기에 답하는 기능입니다. 사용자별 에이전트 묶음은 표준 로그인(OIDC)으로 들어온 사람이 관리자가 정한 한도 안에서 자기 에이전트를 추가하고, 관리자가 소유권 이전과 사람별 한도 조정, 그룹 이탈·30일 미사용 자동 멈춤으로 관리하는 기능입니다(4.1.2절).

아래 표는 현재 제공 범위를 제공 상태별로 나눈 것입니다.

기능 묶음	제공 상태	포함 내용
보기	제공	Cron 헬스체크, 흐름, 스킬, 활동, 채널, 모델, 자격증명
고치기	제공	정기 업무, 스킬 문서, 프로파일(복제·다른 에이전트에서 가져오기·내보내기·삭제 포함), 비밀값 수정과 변경 기록

기능 묶음	제공 상태	포함 내용
시키기	제공	채팅(에이전트 선택, 실행 승인, 되묻기, 지난 대화)
사용자별 에이전트	제공	표준 로그인(OIDC), 에이전트 추가와 사람별 한도, 소유권 이전, 그룹 이탈·30일 미사용 자동 멈춤
함께 일하는 오피스	일부 제공	여러 설치본의 에이전트가 모이는 상시 방 제공, 만들고 지우는 방은 로드맵
사내 스킬 마켓	일부 제공	사내 등록 패키지와 외부 패키지 설치 제공, 마켓 운영 체계는 로드맵

일부 제공 기능의 경계

일부 제공으로 표시한 두 기능은 쓸 수 있는 부분과 아직 없는 부분이 명확히 구분됩니다. 오피스는 여러 설치본의 에이전트가 한 방에서 회의하고 칸반 카드를 나누는 상시 방까지 제공합니다. 마켓은 사내에서 등록한 스킬 패키지와 외부에서 가져온 패키지를 설치하는 기능까지 제공하며, 패키지의 유통 규칙을 정하는 운영 체계는 다음 순서에 놓여 있습니다.

아직 제공하지 않는 기능의 범위

아직 부족한 항목은 다섯 가지이고, 9장 3절에서 부족한 항목으로 밝힌 내용과 같습니다.

- Hermes Agent 외 다른 에이전트 플랫폼 연결
- 사내 마켓의 결제
- 스크립트가 필요한 스킬을 콘솔에서 고치는 기능
- 비용 자동 정지와 부서별 비용 할당
- 그룹·부서 단위 권한 묶음

셋째 항목은 설계 원칙에서 나온 제한입니다. AAS는 에이전트 플랫폼을 고치지 않고 플랫폼의 공식 API로만 변경을 보내는데, Hermes Agent에는 스크립트를 저장하는 API가 없어서 스크립트는 화면에서 보기만 됩니다. 따라서 파일럿 대상은 스킬 문서와 정기 업무 설정만으로 동작하거나, 스크립트가 이미 준비된 업무에서 고르는 편이 안전합니다.

10.1.2 협업 방과 마켓 운영 다음에 두 번째 에이전트 플랫폼 연결이 놓이는 순서

현재 범위 다음의 세 항목

현재 범위 다음에 추가될 항목은 세 가지이며, 아래 번호는 날짜 없이 제시한 진행 순서입니다.

1. 협업 방 생성·삭제 — 필요할 때 방을 만들고 일정 초대 방식으로 에이전트를 부르며 끝나면 지운다
2. 마켓 운영 — 실제 업무 패키지를 등록하고 결제·권한 구분을 포함한 사내 유통 규칙을 갖춘다
3. 두 번째 에이전트 플랫폼 연결 — Hermes Agent 외 플랫폼에 붙는 연결 계층을 분리한다

세 항목은 지금 쓰는 오피스와 마켓을 넓히는 일이 앞에, 새 플랫폼 연결이 뒤에 놓입니다. 다만 각 항목을 언제 내놓을지는 날짜로 정하지 않았으므로, 도입 검토 때 공급사에게 항목별 진행 상황을 직접 확인하는 것이 정확합니다.

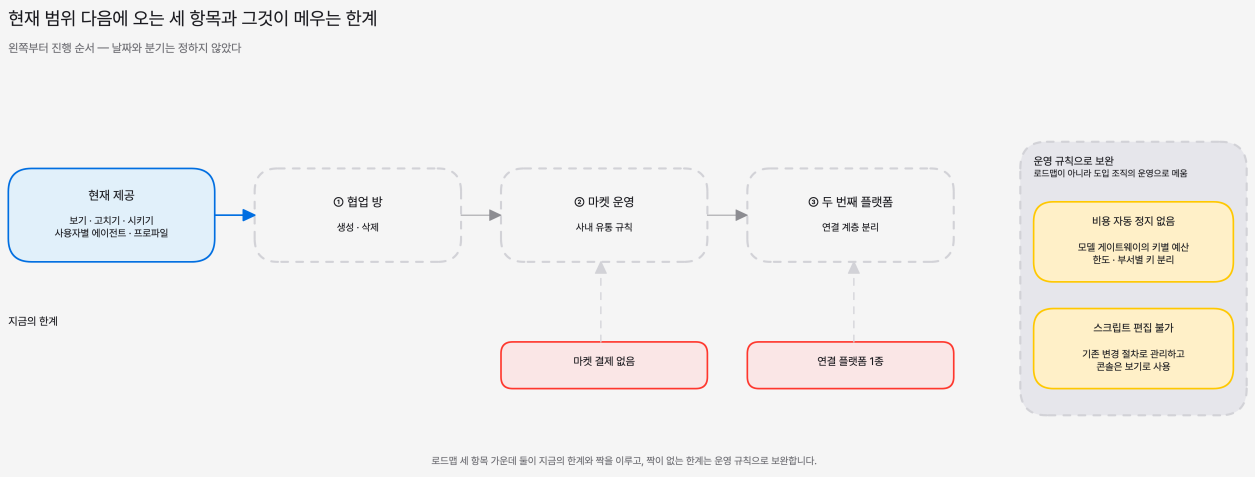


그림 10-1. 현재 범위 다음에 오는 세 항목과 그것이 메우는 한계 — 현재 제공 범위(보기·고치기·시키기, 사용자별 에이전트·프로파일) 다음의 협업 방·마켓 운영·두 번째 플랫폼과 9장 3절 한계의 대응

9장 3절 한계와 로드맵의 대응

아래 표는 9장 3절에서 부족한 항목으로 적은 한계가 어떤 방식으로 메워지는지를 정리한 것입니다.

한계	메우는 방식
마켓 결제 없음	로드맵 둘째 항목(마켓 운영)
연결되는 에이전트 플랫폼은 Hermes Agent 1종	로드맵 셋째 항목
스크립트형 스킬을 콘솔에서 고칠 수 없음	운영 규칙 — 스크립트는 조직의 기존 변경 절차로 관리하고 콘솔은 보기로 쓴다
비용은 보기만 되고 자동 정지·부서별 할당 없음	운영 규칙 — 모델 게이트웨이(LiteLLM)에 키별 예산 한도를 걸고, 모델·사용량 화면을 정기 점검 항목에 넣어 사람이 판단한다
그룹·부서 단위 권한 미흡	운영 규칙 — 사용자마다 볼 수 있는 에이전트를 관리자가 지정하고 부서별 에이전트 소유자를 정한다

표의 함의는 파일럿 범위를 고르는 기준으로 이어집니다. 명함 인식, 화자 구분 회의록, 공문 판독은 모두 현재 제공 범위인 스킬·정기 업무·채팅과 이미 준비된 스크립트로 동작하므로 로드맵 항목이 추가되기를 기다리지 않고 현재 범위 안에서 시작할 수 있습니다. 로드맵은 파일럿을 미루는 이유가 되지 않고, 4단계 확산 때 무엇이 추가로 필요한지를 미리 적어 두는 근거로 쓰입니다.

10.2 반복량과 사람 확인 지점으로 명함과 회의록, 공문 가운데 고르는 첫 유즈케이스 선정 기준

첫 유즈케이스는 넓게 잡을수록 실패 가능성이 커집니다. Gartner는 현재 에이전트형 AI 프로젝트 대부분이 과장된 기대에 이끌린 초기 실험이나 개념 검증이며 잘못 적용되는 경우가 많다고 진단했습니다[S2]. 같은 발표가 꼽은 중단 원인인 비용 증가, 불분명한 사업 가치, 부족한 위험 통제는 업무 범위가 넓을수록 함께 커지는 항목입니다. 첫 유즈케이스를 하나로 좁히면 비용은 업무 한 건 단위로 계산되고, 사업 가치는 그 업무의 처리 시간으로 측정되며, 위험 통제는 사람이 확인하는 단계 한두 곳으로 줄어듭니다. 특정 업무를 맡는 에이전트가 기업용 애플리케이션 안으로 먼저 퍼진다는 전망[S1]도 범용 비서보다 업무 단위 에이전트가 먼저 정착한다는 근거가 됩니다.

10.2.1 반복량과 결과 확인 용이성으로 좁히는 첫 파일럿 후보

첫 유즈케이스 선정 기준 다섯 가지

첫 파일럿 후보는 다섯 기준으로 평가하며, 각 기준은 부서 담당자가 지금 가진 자료로 측정할 수 있도록 정의했습니다. 기준의 뜻과 측정 방법은 아래 표와 같습니다.

기준	뜻	측정 방법
반복량과 시간대 병목	같은 형식의 일이 자주 생기고 특정 시각에 몰리는가	처리 대장의 월간 건수, 몰리는 시각과 그때의 처리 지연
결과 확인 용이성	담당자가 결과의 맞고 틀림을 몇 분 안에 판정할 수 있는가	원본과 결과를 나란히 놓고 대조하는 데 드는 시간
사람 확인 단계	쓰기 전에 사람에게 보여 주고 멈출 단계를 정할 수 있는가	업무 절차에서 결재·확인이 이미 있는 단계의 수
연결 시스템 수	결과를 써야 하는 시스템이 몇 개인가	CRM·위키·드라이브·메신저 등 대상 시스템 목록
외부 반출 여부	음성·이미지·문서가 조직 밖으로 나가야 하는가	업무 정보의 보안 등급과 외부 서비스 사용 가능 여부

반복량과 확인 용이성의 우선순위

다섯 기준 가운데 반복량과 결과 확인 용이성을 먼저 봅니다. 반복량이 적은 업무는 에이전트가 맞게 처리했는지 판단할 표본이 쌓이지 않아 파일럿 결과를 해석할 수 없고, 사업 가치도 처리 시간 절감으로 환산되지 않습니다. 결과 확인이 어려운 업무는 담당자가 에이전트 결과를 처음부터 다시 검토하게 되므로 오히려 일이 늘어납니다. 예를 들어 명함 인식은 명함 사진과 등록된 연락처를 나란히 놓으면 이름·회사·전화번호가 맞는지 바로 판정되고, 공문 판독도 원문 서식과 요약을 대조하면 누락이 드러납니다. 두 기준을 모두 충족하는 업무를 1차 후보로 남기고, 나머지 세 기준으로 후보 간 순서를 정합니다.

사람 확인과 외부 반출의 판정

사람 확인 단계는 에이전트가 CRM이나 위키에 쓰기 전에 결과를 보여 주고 멈추는 단계를 말합니다. 이 단계를 업무 절차 안에서 정할 수 있어야 잘못된 등록이 쌓이기 전에 사람이 막을 수 있으며, 명함 인식처럼 등록 전에 예행 결과를 보여 주고 같은 사람이 있으면 멈추는 방식이 대표적입니다. 외부 반출 여부는 조직의 보안 규정이 먼저 정합니다. 2장에서 본 것처럼 국가 망 보안체계는 업무 정보를 등급으로 나눠 보안 통제를 달리 적용하지만

[S5], 기밀 등급 업무는 여전히 망을 분리해 두므로, 음성과 문서가 조직 밖으로 나가지 않는 온프레미스 구성이 외부 반출 기준을 충족하는 조건이 됩니다.

후보 업무를 네 칸에 대입해 보는 점검

후보를 좁힌 뒤에는 그 업무를 절차 기억, 채널, 무인 실행, 검증의 네 칸에 대입해 빈 칸이 남는지 확인합니다. 절차 기억은 수행 절차를 스킬 문서로 적어 둘 수 있는지를, 채널은 담당자가 대화창 앞에 없을 때도 요청과 결과가 오가는 입구가 있는지를 묻습니다. 무인 실행은 그 업무를 정기 업무로 걸어 사람 개입 없이 끝까지 돌릴 수 있는지를, 검증은 결과를 누가 어떤 기준으로 확인하는지를 묻습니다. 업무 하나는 시작 신호와 처리 절차, 배달 경로로 이루어지므로 이 점검은 플랫폼 기능 목록이 아니라 실제 업무 흐름을 따라가며 해야 합니다. 명함 인식은 네 칸이 모두 채워지는 대표 사례이고, 화자 구분 회의록은 검증 칸에 참석자 확인이 필요하다는 점에서 조건부로 남습니다. 네 칸 가운데 하나라도 비어 있는 업무는 첫 파일럿보다 확산 단계의 후보로 미루는 편이 안전합니다.

10.2.2 부서별 첫 유즈케이스 후보 매트릭스 — 영업 명함, 경영 회의록, 공공 공문

부서별 후보 네 가지의 기준 충족 여부

아래 표는 5장 카탈로그에서 부서별로 하나씩 고른 후보 네 가지를 10.2.1의 다섯 기준으로 평가한 것입니다. ○는 충족, △는 조건부 충족을 뜻합니다.

부서	후보 유즈케이스	반복량	확인 용이성	사람 확인	연결 시스템	외부 반출 없음
영업	명함 인식 → CRM·연락처 등록	○ 행사 직후 몰림	○ 원본 대조	○ 등록 전 예행, 중복이면 멈춤	△ CRM·연락처·위키 3곳	○ 이미지는 조직 안 AI 게이트웨이로만
경영·팀	화자 구분 회의록과 지시 사항 → 할 일	○ 정례 회의	△ 참석자 확인 필요	○ 할 일 체크는 사람이	△ 드라이브·위키·업무 채팅	○ 음성 인식·화자 분리는 조직 안 GPU 서버
공공	공문 판독과 공공서식 채우기	○ 공문 접수 상시	○ 서식 빈칸 대조	○ 채운 값을 보여 준 뒤 저장	○ 문서 변환 도구 서버 1곳	○ 오프라인 OCR
IT 운영	인프라 정기 점검 보고	○ 매일	○ 점검표 대조	△ 읽기 위주, 쓰기 도구는 명시 요청 때만	○ 사내 성능 관측(APM) 도구 1곳	○ 조직 안 실행

명함 인식과 공문 판독의 공통 장점

명함 인식과 공문 판독은 결과 확인이 쉽고 사람 확인 단계가 업무 절차에 이미 들어 있다는 공통점이 있습니다. 명함 인식 에이전트는 사진에서 이름·직함·회사·연락처를 읽어 기존 고객사에 연결하고, 등록 전에 예행 결과를 보여 준 뒤 확인을 받으며, 없는 회사는 말없이 만들지 않습니다. 공공 부서의 에이전트는 HWP·HWPX·PDF 공문을 읽어 요약하고, 받은 공공서식의 빈칸 구조를 분석해 값을 채운 뒤 사람에게 보여 주고 나서 저장합니다. 스

캔본은 조직 안의 오프라인 OCR 엔진으로 읽으므로 외부 서비스가 필요 없습니다. 두 후보는 확인 비용이 낮아 파일럿 결과를 짧은 기간 안에 판정하기 좋습니다.

화자 구분 회의록이 넓히는 효과

화자 구분 회의록은 결과 확인에 회의 참석자가 필요해 확인 용이성이 조건부이지만, 조직 전체로 넓혔을 때의 효과는 가장 큽니다. 에이전트는 녹음에서 화자를 구분해 회의록을 쓰고, 리더의 지시사항을 지시·근거·기한으로 뽑아 담당자별 할 일로 칸반에 넣으며, 사람이 체크한 결과를 정기적으로 거둬 지시 원장에 쌓습니다. 화자 실명은 목소리 지문 같은 근거가 있을 때만 붙고, 근거가 없으면 「미확인」으로 남습니다. 경영진이 직접 쓰는 업무라서 파일럿 결과가 의사결정권자에게 바로 보인다는 점도 이 후보의 장점입니다.

연결 시스템 설정 범위와 최종 선택 규칙

표의 연결 시스템 칸은 업무 에이전트가 결과를 쓰는 대상이며, 연결 시스템(CRM·위키·드라이브 등)은 고객 환경에 맞춰 설정합니다. 표에 적은 연결 수는 예시 구성 기준이고, 조직이 쓰는 CRM이나 문서 저장소가 다르면 그 시스템에 맞는 스킬 설정이 파일럿 준비 항목에 들어갑니다. 최종 선택 규칙은 단순합니다. ○가 가장 많은 후보 가운데 연결 시스템 수가 가장 적은 하나를 첫 유즈케이스로 고르고, 나머지 후보는 4단계 확산 대상 목록에 올립니다. 이 규칙을 적용하면 공공 조직은 공문 판독과 공공서식 채우기, 영업 조직은 명함 인식이 첫 후보가 되는 경우가 많습니다.

10.3 첫 유즈케이스 선정에서 사내 마켓 확산까지 파일럿 4단계와 단계별 판단 기준

AAS 파일럿 4단계를 구분하는 기준은 다음 단계로 넘어가는 조건이며, 단계마다 기간은 정하지 않습니다. 에이전트형 AI 프로젝트의 중단 원인으로 꼽힌 불분명한 사업 가치와 부족한 위험 통제[S2]는 언제 넓히고 언제 멈출지 미리 정하지 않은 프로젝트에서 커지기 때문입니다. 따라서 각 단계는 하는 일, 남기는 산출물, 다음 단계로 넘어가는 조건을 함께 가집니다.

단계	하는 일	산출물	다음 단계로 넘어가는 조건
① 첫 유즈케이스와 파일럿 대상 확정	10.2 기준으로 업무 하나와 참여 담당자를 정한다	선정 매트릭스, 사람 확인 단계 정의, 성공 판정 기준	업무 소유 부서장과 IT·보안 담당이 범위에 합의
② 조직 안 설치와 기존 플랫폼 연결	AAS를 조직 안에 설치하고 Hermes Agent에 연결한다	설치 구성 기록, 로그인 연동, 연결된 프로파일 목록	스킬·정기 업무가 조직 안 모델로 실행되고 결과가 연결 시스템에 기록됨
③ 지켜보기	Cron 헬스체크·자격증명·알림 대상을 정기 점검한다	점검 기록, 사람이 처리한 문제 목록	성공 판정 기준 충족, 알림이 안 가는 작업 0개
④ 사내 마켓 확산	판정 기준을 통과한 스킬을 패키지로 다른 부서·지사에 배포한다	마켓 패키지, 설치 부서 목록	설치한 부서에서도 ③의 기준을 다시 충족

업무 프로파일 하나의 쓰임새로 보면 네 단계는 만들고, 넓히고, 정리하는 순서입니다. 2단계에서 담당자는 에이전트를 추가하고 그 안에 첫 업무 프로파일을 만듭니다. 3단계 기준을 통과하면 4단계에서 그 프로파일을 복제하거나, 다른 부서 담당자가 「다른 에이전트에서 가져오기」로 출발점을 삼거나, 패키지로 배포해 다른 부서로 넓

힙니다. 파일럿을 중단하거나 끝낸 프로파일은 내보내기로 보관본을 남긴 뒤 지우므로, 시험 삼아 만든 프로파일이 정기 업무를 계속 실행한 채 잊히지 않습니다.

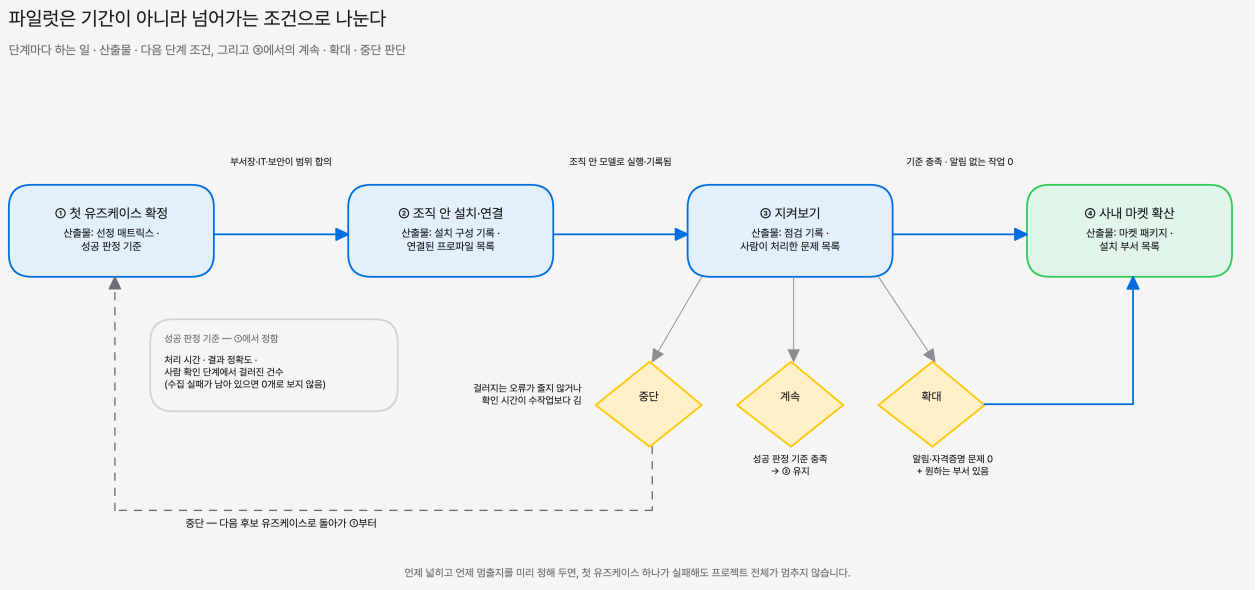


그림 10-2. AAS 파일럿 4단계 — 단계마다 산출물과 계속·확대·중단 판단을 붙인 흐름

10.3.1 조직 안 설치와 지켜보기 단계에서 확인할 알림 대상과 자격증명

2단계 조직 안 설치 점검 항목

2단계의 목표는 첫 유즈케이스가 조직 밖으로 데이터를 보내지 않고 실행되는 상태를 만드는 것입니다. AAS는 외부 내려받기나 빌드 없이 조직 안에서 기동되고 쿠버네티스 배포본을 제공하며, 이미 Hermes Agent를 쓰는 조직이라면 에이전트 플랫폼을 고치지 않고 그 위에 콘솔을 얹습니다. 플러그인·설정·버전을 바꾸지 않으며, AAS가 플랫폼 데이터를 읽는 경로는 읽기 전용이고 변경은 플랫폼의 공식 API로만 보냅니다. 점검 항목은 다음과 같습니다.

- 설치 위치와 조직 망 안에서의 접속 방식
- 표준 로그인(OIDC) 연동, 파일럿 참여자별 에이전트 한도와 볼 수 있는 에이전트 지정
- 연결할 Hermes Agent 설치본과 프로파일 목록
- 모델·음성 인식·OCR이 조직 안에서 실행되는지 여부
- 첫 유즈케이스의 연결 시스템 설정과 그 자격증명 등록

3단계 지켜보기 점검 항목

3단계에서는 에이전트가 사람이 보지 않는 동안 실행한 결과를 정기적으로 점검합니다. 알림이 안 가는 작업이 가장 먼저 볼 항목인데, 정기 업무의 실패 알림은 그 작업의 전달 대상으로만 가므로 전달 대상이 없는 작업은 실패해도 아무도 모르기 때문입니다. Cron 헬스체크 화면은 정기 업무 95개 중 알림이 안 가는 작업 15개를 목록으로 드러내고, 「이미 풀린 사건」 62건이 지금도 실패 중인 작업을 가리지 않도록 따로 나눠 보여 줍니다.

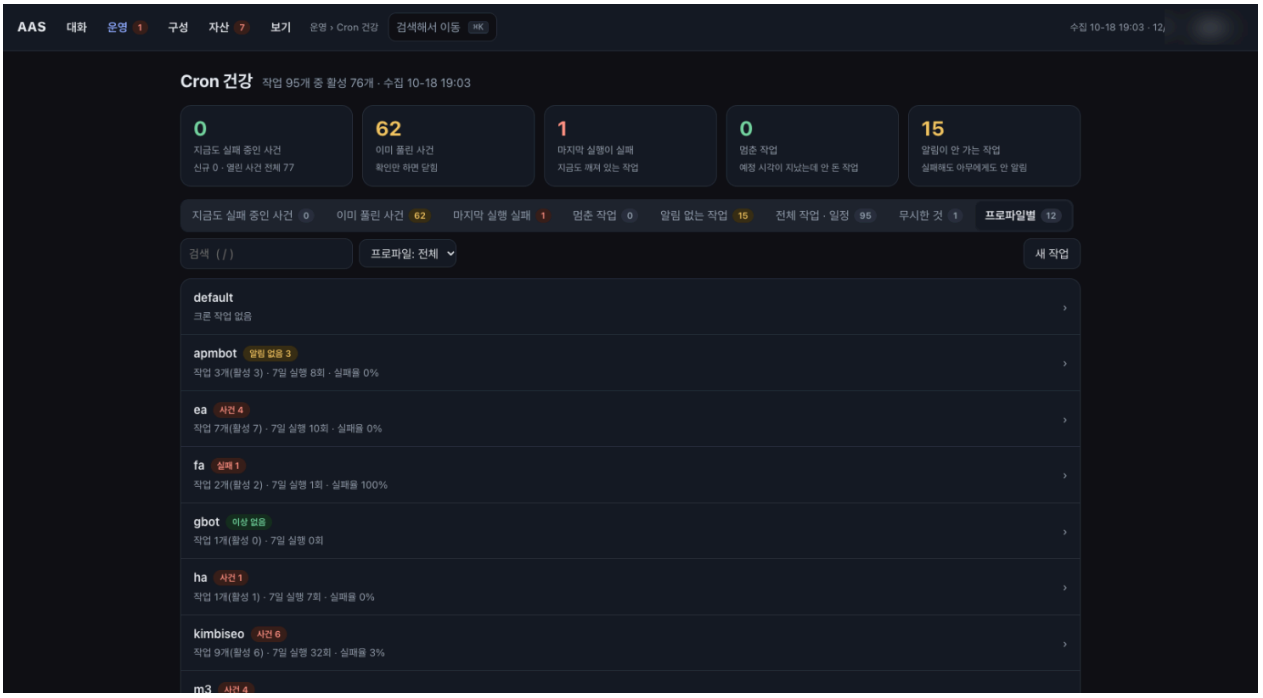


그림 10-3. Cron 헬스체크 화면(프로파일별) — 상단 숫자 가운데 「알림 안 가는 작업」과 「이미 풀린 사건」을 먼저 보고, 표에서 프로파일별 7일 실행 수와 실패율을 확인합니다

자격증명 점검도 같은 단계에 들어갑니다. 1장에서 본 내부 정책 위반 전망[S3]을 고려하면, 토큰이 어디에 복사돼 있는지, 만료가 다가오는지를 값을 드러내지 않고 확인하는 것이 파일럿의 위험 통제 항목이 됩니다. 자격증명 화면은 자격증명 103개를 값 없이 훑어 만료(임박) 7개, 빈 값 3개, 여러 곳에 복사된 값 17개를 보여 줍니다.

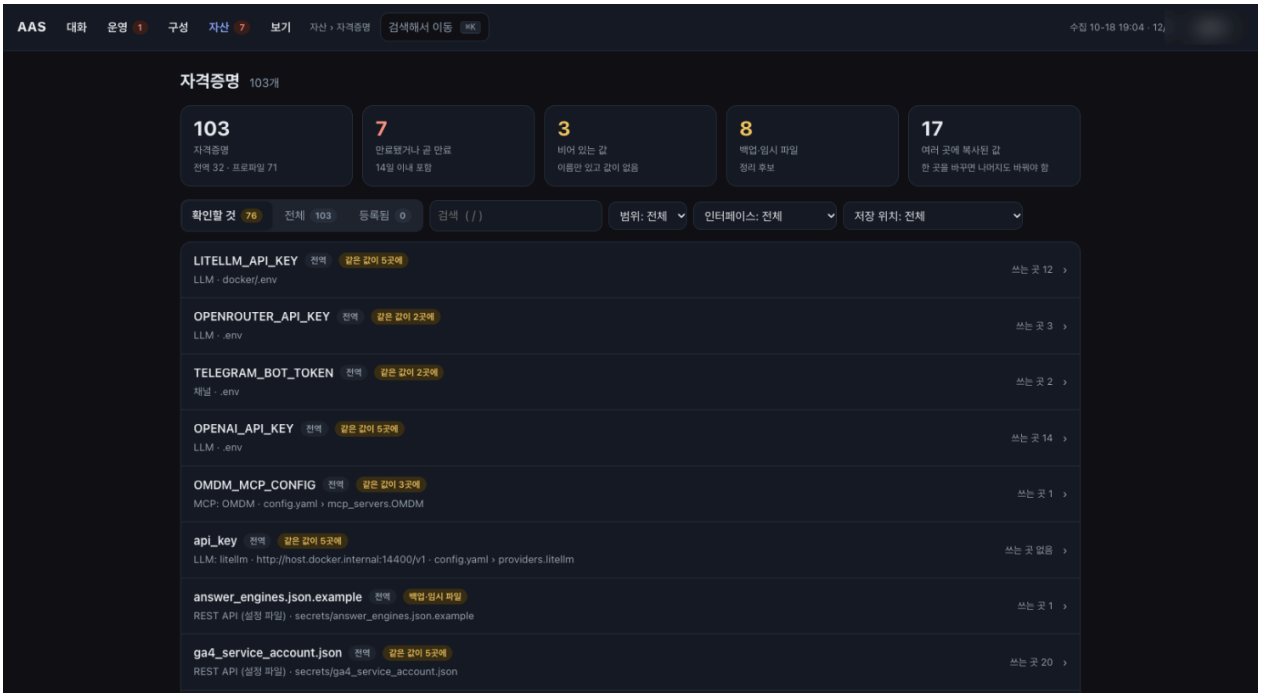


그림 10-4. 자격증명 화면 — 값은 표시되지 않고, 상단의 만료(임박)·빈 값·여러 곳에 복사된 값 숫자와 각 자격증명을 쓰는 스킬·정기 업무 목록을 봅니다

3단계 계속·확대·중단 판단 기준

지켜보기 단계의 판단은 화면이 드러낸 문제를 사람이 처리했는지에 달려 있습니다. 화면은 원인을 드러내고, 전달 대상을 지정하거나 만료 토큰을 교체하는 것은 담당자이므로 판단 기준도 사람이 처리한 결과로 정합니다. 판단 기준은 세 가지로 정합니다. 첫째, 1단계에서 정한 성공 판정 기준(처리 시간, 결과 정확도, 사람 확인 단계에서 걸러진 건수)을 충족하면 계속합니다. 둘째, 알림이 안 가는 작업과 만료 임박 자격증명이 0개로 유지되고 같은 업무를 원하는 다른 부서가 있으면 4단계로 확대합니다. 셋째, 사람 확인 단계에서 걸러지는 오류가 줄지 않거나 담당자의 확인 시간이 수작업 시간보다 길면 중단하고 10.2.2의 다음 후보로 돌아갑니다. 다만 AAS는 읽지 못한 항목을 「수집 실패」로 따로 표시하므로, 수집 실패가 남아 있는 상태에서는 0개 기준을 충족한 것으로 보지 않습니다.

10.3.2 사내 스킬 마켓으로 다른 부서와 지사에 넓히는 확산 단계

4단계 확산 조건

4단계는 3단계 판단 기준을 통과한 스킬을 사내 스킬 마켓에 패키지로 등록하고, 같은 업무를 가진 다른 부서와 지사가 설치해 쓰는 단계입니다. 확산 조건은 두 가지입니다. 하나는 원래 부서에서 성공 판정 기준과 알림·자격증명 기준을 함께 충족했는지이고, 다른 하나는 설치할 부서의 연결 시스템이 같은지 또는 그 부서에 맞게 다시 설정할 수 있는지입니다. 스킬 마켓 화면은 사내에서 등록한 패키지 2개와 외부에서 가져온 패키지 49개, 모두 51개를 태그별로 보여 주고 패키지가 설치된 곳을 표시합니다.

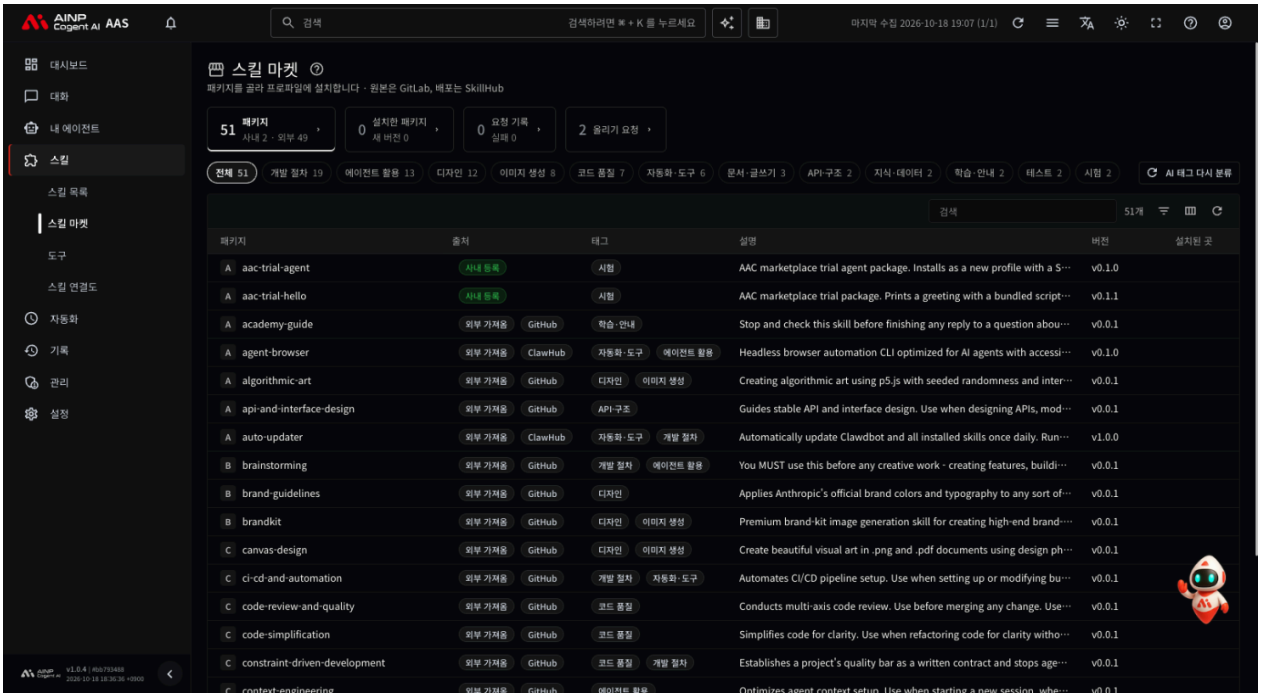


그림 10-5. 사내 스킬 마켓 화면 — 패키지마다 출처(사내·외부)와 태그, 설치된 곳을 보고 다른 부서에 배포할 패키지를 고릅니다

폭스프로 시기 업무 프로그램의 확산 선례

부서가 만든 스킬이 다른 부서로 퍼지는 방식은 1980~90년대 업무 프로그램의 확산과 닮았습니다. 3장에서 본 디베이스·폭스프로 시기[S8]에 현장에서 만든 프로그램은 디스켓과 공유 폴더를 거쳐 다른 부서로 옮겨 갔고, 만든 사람이 떠나도 프로그램은 조직에 남았습니다. AAS에서는 사내 스킬 마켓이 디스켓과 공유 폴더를 대신하고, 부서가 만든 스킬과 에이전트 구성이 조직의 자산으로 남습니다.

계속·확대·중단 판단표

확산 단계에서도 판단 기준은 3단계와 같은 형식을 씁니다. 다만 판단 대상이 한 부서에서 설치한 부서 전체로 넓어집니다.

판단	조건	다음 행동
계속	설치한 부서에서 성공 판정 기준 충족, 알림·자격증명 문제 없음	패키지를 그대로 유지하고 정기 점검을 이어 간다
확대	두 개 이상 부서에서 기준을 다시 충족하고 같은 업무 요청이 추가로 있음	지사와 다른 부서에 배포하고 10.2.2의 다음 후보를 1단계로 올린다
중단	설치 부서의 연결 시스템이 달라 재설정 비용이 수작업 절감보다 큼	그 부서의 설치를 철회하고 원래 부서 운영만 유지한다

10.4 부서 담당자와 IT 관리자, 보안 담당이 파일럿 전에 준비할 목록

파일럿 1단계를 시작하려면 부서 담당자, IT 관리자, 보안 담당의 준비가 함께 끝나야 합니다. 세 역할 가운데 하나라도 준비가 늦으면 파일럿은 업무 범위 없이 설치만 되거나, 설치는 됐는데 보안 검토에서 멈추는 상태로 남습니다. 2장에서 본 감독용 에이전트 전망[S3]에 비추어 보면 파일럿에서도 에이전트를 만드는 기능만큼 지켜보는 기능과 그 운영 책임자를 함께 준비해야 합니다. 의사결정권자가 내릴 다음 지시는 세 역할의 준비 목록을 들고 모이는 파일럿 대상 확정 회의 하나로 정리됩니다.

10.4.1 업무 선정과 사람 확인 지점을 정하는 부서 담당자의 준비

부서 담당자가 가져올 업무 정보

부서 담당자는 업무를 가장 잘 아는 사람이므로, 첫 유즈케이스의 범위와 사람 확인 단계를 정하는 책임을 맡습니다. 회의 전에 준비할 정보는 다음과 같습니다.

- 후보 업무의 월간 건수와 몰리는 시각
- 지금 그 업무에 드는 처리 시간과 담당 인원
- 결과를 판정하는 방법과 판정에 드는 시간
- 쓰기 전에 사람이 확인해야 하는 단계와 확인할 사람
- 결과를 기록하는 시스템(CRM·위키·드라이브·메신저) 목록
- 다루는 정보의 보안 등급과 외부 반출 가능 여부

성공 판정 기준의 초안

부서 담당자는 위 정보를 바탕으로 3단계에서 쓸 성공 판정 기준의 초안도 가져옵니다. 예를 들어 명함 인식이라면 행사 뒤 명함 처리에 드는 시간, 등록 전 확인에서 고친 항목 수, 중복 등록 건수가 기준이 됩니다. 화자 구분 회의록이라면 회의 종료 뒤 할 일 목록이 칸반에 올라오기까지의 시간과, 참석자가 확인했을 때 빠진 지시사항 수가 기준이 됩니다. 기준을 업무 단위 숫자로 미리 정해 두면 파일럿 결과를 사업 가치로 설명할 수 있고, 불분명한 사업 가치가 중단 원인이 되는 경우[S2]를 줄일 수 있습니다.

설치가 아니라 운영 결과를 과업으로 적는 이유

파일럿을 외부 사업자와 함께 진행한다면 계획서나 계약서에 무엇을 과업으로 적는지도 성공 판정 기준만큼 중요합니다. 도구 설치와 화면 구성만 과업으로 적으면, 설치는 끝났는데 실패 알림을 누가 확인하고 만료 계정을 누가 교체하는지는 비어 있는 상태로 파일럿이 시작됩니다. 도구를 갖춘 것만으로 운영이 성립하지 않으므로, 확인 주기와 확인 담당, 그 결과를 어떤 형식으로 제출하는지를 과업에 함께 적어야 합니다. 과업 항목만 늘리고 투입 인력을 그대로 두면 늘어난 항목은 기록으로만 남고 실제 확인은 얕아지므로, 파일럿 범위를 업무 하나로 좁히는 것이 이 점에서도 유리합니다.

10.4.2 설치 환경과 보안 검토 범위를 정하는 IT 관리자와 보안 담당의 준비

IT 관리자의 설치 환경 준비

IT 관리자는 2단계 설치를 위한 환경과 연결 정보를 준비합니다. 준비 항목은 다음과 같습니다.

- 설치 환경(조직 안 서버 또는 쿠버네티스 클러스터)과 망 구성
- 표준 로그인(OIDC) 공급자와 파일럿 참여 사용자 그룹
- 연결할 Hermes Agent 설치본, 신규 설치가 필요하면 그 계획
- 조직 안에서 쓸 모델과 음성 인식·OCR 실행 환경
- 첫 유즈케이스의 연결 시스템 계정과 자격증명 발급 절차

보안 담당의 검토 범위 준비

보안 담당은 7장에서 설명한 보안 원칙을 기준으로 검토 범위를 정합니다. AAS는 비밀값을 화면·로그·기록 어디에도 남기지 않고, 플랫폼 데이터를 읽는 경로와 변경을 보내는 경로를 분리하며, 마켓 패키지 설치·삭제처럼 공식 API에 경로가 없는 두 경우는 범위를 좁혀 문서에 밝힙니다. 보안 검토는 이 원칙이 조직 환경에서 지켜지는지와 함께 다음 항목을 확인합니다.

- 업무 정보의 보안 등급(국가 망 보안체계의 C·S·O 구분을 쓰는 조직은 그 등급)[S5]
- 에이전트가 부르는 외부 호스트 목록과 흐름 화면의 호출 관계
- 자격증명 보관 위치와 만료·교체 책임자
- 변경 기록의 보존 범위와 감사 때 제출 방식

운영 기록의 보관 위치와 열람 권한

보안 검토에서는 기록이 어디에 쌓이고 누가 열어 볼 수 있는지도 함께 정합니다. 에이전트 운영 기록은 어떤 에이전트가 언제 무엇을 실행했는지 남는 실행 기록, 콘솔에서 무엇을 바꿨는지 남는 변경 기록, 사람이 어떤 명령을 허락하거나 막았는지 남는 승인 기록으로 나눠 볼 수 있습니다. 이 기록에는 조직의 업무 흐름과 민감한 맥락이 누적되므로, 세 기록이 모두 조직 안 저장소에만 남는지, 공급사가 원격으로 수집하거나 외부로 전송하는 경로가 없는지, 보존 기간과 열람 권한을 누가 정하는지를 설치 구성과 계약 문서에서 함께 확인해야 합니다. 사고가 났을 때 책임 소재를 밝히는 근거가 바로 이 기록이므로, 조직이 기록을 직접 열람할 수 없으면 원인 조사가 공급사의 응답 속도에 묶이게 됩니다.

파일럿 대상 확정 회의 안건

세 역할의 준비가 끝나면 파일럿 대상 확정 회의를 엽니다. 회의 안건은 다섯 가지로 정리됩니다.

1. 10.2.2 매트릭스로 첫 유즈케이스 하나 확정

2. 사람 확인 단계와 성공 판정 기준 합의
3. 설치 환경과 연결 시스템 범위 확정
4. 보안 검토 범위와 담당자 지정
5. 3단계 계속·확대·중단 판단을 내릴 책임자 지정

이 회의에서 정해지는 것은 업무 하나, 기준 하나, 책임자 한 명입니다. 넓게 시작한 에이전트형 AI 프로젝트가 비용과 위험 통제 문제로 중단되는 경향[S2]을 고려하면, 첫 결정이 작을수록 다음 결정의 근거가 분명해집니다. 업무를 아는 담당자가 조직 안에서, 쓰던 에이전트 플랫폼을 고치지 않고 에이전트를 만들고 시키고 지켜보는 한 화면이 있어야 에이전트가 업무에 자리 잡는다는 것이 이 백서의 결론입니다. 따라서 의사결정권자가 할 첫 행동은 부서 업무 가운데 명함·회의록·공문처럼 반복량이 많고 결과를 쉽게 확인할 수 있는 업무 하나를 파일럿 대상으로 정하고, 세 역할에게 위 준비 목록을 지시하는 것입니다.

부록: 참고문헌과 용어 정의

Appendix A — 참고문헌 (References)

본 부록은 백서 본문에 인용된 참고문헌과 본문에 등장하는 주요 기술 용어의 정의를 모아 정리한 참조 자료입니다. 참고문헌 번호는 본문의 출처 표기 [S1]~[S23]과 같습니다.

1. [S1] Gartner. (2025-08-26). "Gartner Predicts 40% of Enterprise Apps Will Feature Task-Specific AI Agents by 2026, Up from Less Than 5% in 2025". https://www.gartner.com/en/newsroom/press-releases/2025-08-26-gartner-predicts-40-percent-of-enterprise-apps-will-feature-task-specific-ai-agents-by-2026-up-from-less-than-5-percent-in-2025 (접속일 2026-10-18)
2. [S2] Gartner. (2025-06-25). "Gartner Predicts Over 40% of Agentic AI Projects Will Be Canceled by End of 2027". https://www.gartner.com/en/newsroom/press-releases/2025-06-25-gartner-predicts-over-40-percent-of-agentic-ai-projects-will-be-canceled-by-end-of-2027 (접속일 2026-10-18)
3. [S3] Gartner. (2025-06-11). "Gartner Predicts that Guardian Agents will Capture 10-15% of the Agentic AI Market by 2030". https://www.gartner.com/en/newsroom/press-releases/2025-06-11-gartner-predicts-that-guardian-agents-will-capture-10-15-percent-of-the-agentic-ai-market-by-2030 (접속일 2026-10-18)
4. [S4] McKinsey & Company. (2025-11). "The state of AI in 2025: Agents, innovation, and transformation". https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-2025 (접속일 2026-10-18)
5. [S5] 바이라인네트워크. (2025-01-30). "공공 망분리 대신할 '국가 망 보안체계' 가이드라인 나왔다". https://byline.network/2025/01/30-371/ (접속일 2026-10-18)
6. [S6] 뉴시스. (2024-09-11). "공공 데이터 빗장 풀린다…정부, 18년 만에 공공망 분리 규제 개선". https://www.newsis.com/view/NISX20240911_0002884654 (접속일 2026-10-18)
7. [S7] 뉴시스. (2026-03-13). "공공기관 업무PC에서도 챗GPT 쓴다…新국가망보안체계(N2SF) 공모 착수". https://mobile.newsis.com/view/NISX20260313_0003547805 (접속일 2026-10-18)
8. [S8] Wikipedia. (게시일 미표기, 수시 갱신). "FoxPro". https://en.wikipedia.org/wiki/FoxPro (접속일 2026-10-18)
9. [S9] Microsoft. (미상). "What is Microsoft Copilot Studio? (Microsoft Learn)". https://learn.microsoft.com/en-us/microsoft-copilot-studio/fundamentals-what-is-copilot-studio (접속일 2026-10-08)
10. [S10] Microsoft. (미상). "Microsoft Agent 365". https://www.microsoft.com/en-us/microsoft-agent-365 (접속일 2026-10-08)

11. [S11] Anthropic. (미상). "Claude Cowork". https://claude.com/product/cowork (접속일 2026-10-08)
12. [S12] Dust. (미상). "Dust". https://dust.tt/ (접속일 2026-10-08)
13. [S13] IBM. (미상). "IBM watsonx Orchestrate". https://www.ibm.com/products/watsonx-orchestrate (접속일 2026-10-08)
14. [S14] 삼성SDS. (미상). "FabriX". https://www.samsungsds.com/kr/ai-fabrix/fabrix.html (접속일 2026-10-08)
15. [S15] 올거나이즈. (미상). "Alli". https://www.allganize.ai/en/alli-gpt (접속일 2026-10-08)
16. [S16] Nous Research. (미상). "Hermes Agent Web Dashboard (User Guide)". https://hermes-agent.nousresearch.com/docs/user-guide/features/web-dashboard (접속일 2026-10-08)
17. [S17] hermes-webui 프로젝트. (미상). "hermes-webui (GitHub 저장소)". https://github.com/nesquena/hermes-webui (접속일 2026-10-08)
18. [S18] Ekko Studio 프로젝트. (미상). "Ekko Studio (GitHub 저장소)". https://github.com/EKKOLearnAI/ekko-studio (접속일 2026-10-08)
19. [S19] hermes-control-interface 프로젝트. (미상). "hermes-control-interface (GitHub 저장소)". https://github.com/xaspx/hermes-control-interface (접속일 2026-10-08)
20. [S20] Paperclip 프로젝트. (미상). "Paperclip (GitHub 저장소)". https://github.com/paperclipai/paperclip (접속일 2026-10-08)
21. [S21] Open WebUI 프로젝트. (미상). "Open WebUI (GitHub 저장소)". https://github.com/open-webui/open-webui (접속일 2026-10-08)
22. [S22] Datadog. (미상). "AI Agents Console (Product Preview)". https://www.datadoghq.com/product-preview/ai-agents-console/ (접속일 2026-10-08)
23. [S23] Langfuse 프로젝트. (미상). "Langfuse (GitHub 저장소)". https://github.com/langfuse/langfuse (접속일 2026-10-08)

함께 읽을 자료 (자사 공개 자료)

아래 [R] 번호는 본문의 같은 주제를 더 읽어 볼 수 있도록 안내하는 자사 공개 자료입니다. 본문 주장의 확인 근거인 [S] 번호와는 계열이 다르며, 외부 출처를 대신하지 않습니다.

1. [R1] 자사 공개 자료 (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)

용어	정의
감독용 에이전트 (guardian agent)	다른 에이전트의 행동을 감시하고 통제하는 에이전트
게이트웨이 (Gateway)	에이전트와 메신저, 또는 에이전트와 모델 사이를 중계하는 연결 구성 요소. 메신저 게이트웨이와 모델 게이트웨이

용어	정의
	가 있다
런타임 (runtime)	에이전트가 실제로 실행되는 엔진. 에이전트 정의·실행 기록·자격증명이 이곳에 저장된다
성격 (SOUL)	에이전트의 역할과 응답 말투를 적은 설정. 역할 템플릿을 고르면 채워진다
스킬 (Skill)	에이전트가 일하는 방법을 적은 문서와 그에 딸린 스크립트 묶음
스킬 마켓	부서가 만든 스킬과 에이전트를 사내에 올리고 내려받아 나눠 쓰는 저장소
예행 (dry-run)	실제로 기록하기 전에 어느 시스템의 어떤 항목에 무엇을 쓸지 먼저 보여 주는 시험 실행
온프레미스 (on-premises)	외부 클라우드가 아니라 조직이 직접 관리하는 서버에 설치해 쓰는 방식
자격증명 (Credential)	에이전트가 외부 시스템을 부를 때 쓰는 API 키·토큰·서비스 계정 파일 같은 비밀값
정기 업무 (크론, Cron)	정해진 시각에 자동으로 실행되도록 예약한 에이전트 작업과 그 전달 대상
쿠버네티스 (Kubernetes)	컨테이너를 여러 서버에 배치하고 운영하는 플랫폼. AAS의 다중 사용자 배포본이 이 위에서 돈다
프로파일 (Profile)	에이전트 한 명에 해당하는 설정 단위. 성격·모델·메신저 연결·스킬 목록을 따로 갖는다
화자 분리 (화자 구분)	녹음 속 목소리를 사람별로 나누고 목소리 지문으로 이름을 붙이는 처리
AI Agent (AI 에이전트)	사람이 맡긴 일을 여러 단계로 나누고 필요한 도구를 스스로 호출해 결과를 돌려주는 프로그램
API (Application Programming Interface)	프로그램끼리 정해진 형식으로 기능과 데이터를 주고받는 호출 창구. AAS는 설정을 바꿀 때 에이전트 플랫폼의 공식 API만 쓴다
APM (Application Performance Monitoring)	애플리케이션의 응답시간과 트랜잭션 처리를 추적해 성능 문제를 찾는 관제 도구
CLI (명령줄)	글자로 명령을 입력해 프로그램을 다루는 방식. 화면 없이 설정을 바꿀 때 쓴다
CRM (고객 관계 관리)	고객사·담당자·영업 기회 같은 고객 정보를 모아 관리하는 업무 시스템

용어	정의
Hermes Agent	AAS가 지금 연결하는 오픈소스 에이전트 플랫폼. 에이전트 프로세스를 실행하고 모델·메신저 게이트웨이를 잇는 런타임을 제공한다
HWP·HWPX	국내 공공기관이 주로 쓰는 한글 문서 형식. HWPX는 그 개방형 XML 형식이다
JWT (JSON Web Token)	로그인 정보와 만료일을 담아 주고받는 토큰 형식. AAS는 값 없이 만료일만 읽는다
LDAP (Lightweight Directory Access Protocol)	사내 계정 디렉터리를 조회·연동하는 규약
LiteLLM	여러 언어 모델을 하나의 창구로 묶어 중계하는 모델 게이트웨이. AAS는 이를 통해 모델별 응답 여부를 점검한다
MCP (Model Context Protocol)	에이전트가 외부 도구와 데이터를 일정한 규약으로 부르게 하는 공개 프로토콜
MLS (Multi-Level Security, 다층보안체계)	일률적인 망 분리 대신 데이터 중요도에 따라 보안 통제를 차등 적용하는 체계
N²SF (National Network Security Framework, 국가망 보안체계)	업무 정보를 기밀(C)·민감(S)·공개(O)로 나눠 통제를 달리하고, 그 범위 안에서 생성형 AI·외부 클라우드 활용 길을 연 국내 공공 보안 가이드라인
OCR (Optical Character Recognition, 문자 인식)	이미지·스캔 문서 속 글자를 읽어 텍스트로 바꾸는 기술. AAS 업무 에이전트는 조직 안 모델로 처리한다
OIDC (OpenID Connect, 표준 로그인)	사내 계정으로 여러 시스템에 로그인하게 하는 표준 인증 방식. AAS는 OIDC 그룹으로 사용자별 에이전트와 권한을 나눈다
SaaS (Software as a Service)	설치 없이 외부 클라우드에서 빌려 쓰는 소프트웨어 서비스
STT (Speech-to-Text, 음성 인식)	녹음된 말을 글로 받아 적는 기술. 화자 구분 회의록은 조직 안 GPU 서버에서 처리한다
WAS (Web Application Server)	웹 애플리케이션을 실행해 요청을 처리하는 서버



업무를 아는 사람이 AI Agent 를 만든다 — MSAP.ai AAS 소개 백서

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

© 2026 SMART CF, MSAP.ai. All rights reserved.