
MSAP.ai

msap.ai

MSAP.ai AAS 제품 소개와 도입 방법

AI Agent 플랫폼에 연결되는 일반 사용자용 콘솔
도입 검토를 위한 7편 영상 시리즈

SERIES

7편 · 45장

DATE

2026-10



KEY INSIGHT

업무 담당자가 조직 안에서 에이전트를 만들고 지켜볼 화면이 있어야 에이전트가 업무에 자리 잡음

문제와 시장

1편

채팅 창구와 AI Agent 업무 정착 문제

탐재율과 정착률 차이 · 채팅 창구의 승인 기록 · 정기 업무 실패

2편

AI Agent 도구 시장 여섯 구분과 AAS 위치

만드는 도구와 지켜보는 도구 · 세 조건 교차표 · N²SF · 조건별 선택

제품과 화면

3편

AAS 정의와 Hermes Agent 연결 구조

담당자와 플랫폼의 역할 분담 · 계층별 읽기 · 변경 범위 · 사용자 네 부류

4편

AAS 콘솔 네 기능 묶음의 실제 화면

만들기 · 시키기 · 지켜보기 · 나누기 화면

업무 사례와 보안

5편

AAS 업무 에이전트 부서별 사례

10개 카테고리 카탈로그 · 명함 인식 · 공문 판독 · 화자 구분 회의록

6편

AAS 관측 기능과 보안 구조

Cron 헬스체크 · 값 없는 자격증명 점검 · 연결 구조 · 온프레미스 구성

도입 판단

7편

AAS 도입 판단과 파일럿 4단계

앞서는 항목과 부족한 항목 · 첫 유즈케이스 선정 · 역할별 파일럿 준비

PART 01

채팅 창구와 AI Agent 업무 정착 문제

탐재율과 정착률 차이 · 채팅 창구의 승인 기록 · 사람 없이 도는 정기 업무

도입 검토 관점

KEY INSIGHT

탑재는 공급사가 정하고 정착은 담당자가 정함 —

만들고 지켜볼 창구가 없으면 에이전트가 시험 단계에 머물

탑재는 빠르게 늘고 정착은 제자리

같은 시기 두 지표 비교

AI Agent 탑재 기업용 앱 — 2025년

5% 미만

AI Agent 탑재 기업용 앱 — 2026년 말 전망

40%

업무 기능 하나 기준 확대 적용 비율

10% 이하

조직 단위 응답: 시험 39% · 확대 23%

시험은 많지만 한 업무 기능에 넓게 쓰는 비율은

어느 기능에서도 10%를 넘지 않음

2027년 말까지 중단될 에이전트형 AI 프로젝트

40% 이상

중단 사유: 비용 증가 · 불분명한 사업 가치 ·

부족한 위험 통제

Gartner 2025-06-25

허가되지 않은 에이전트 행위 중 내부 정책 위반 비중

80% 이상

2028년까지 전망 — 정보 과다 공유 같은 내부 원인이

외부 공격보다 많음

Gartner 2025-06-11

KEY INSIGHT

승인이 "네" 한 줄로 끝나면 승인 당시 화면이 기록되지 않음 —
사고가 나면 에이전트의 역할 없이 담당자 판단 착오로 정리됨

항목	채팅 프로그램	에이전트 전용 콘솔
진행 단계	일반 메시지로 표시	현재 단계를 따로 표시
실행하려는 명령	본문에 섞임	실행 전 명령을 따로 표시
실행 승인	"네" 메시지 한 줄	승인 카드와 승인 이력
되물기	일반 질문 메시지	답이 필요한 항목을 따로 표시
정기 업무 결과	전달 대상 채널에만 도착	실행 기록과 실패 여부를 한 화면에서 조회

채팅 프로그램은 사람끼리 대화하려고 만든 도구

진행 단계 · 실행 승인 · 되물기가 모두 같은 말풍선으로 흘러감
→ 무엇을 보고 승인했는지가 기록에 남지 않음



설정도 여러 곳에 흩어짐

에이전트마다 반복하는 일

메신저 봇 등록과 토큰 복사

설정이 놓인 자리

설정 파일

서버 폴더

CLI

메신저 관리 화면

흩어진 설정

모델 · 스킬 · 정기 업무 · 봇 토큰

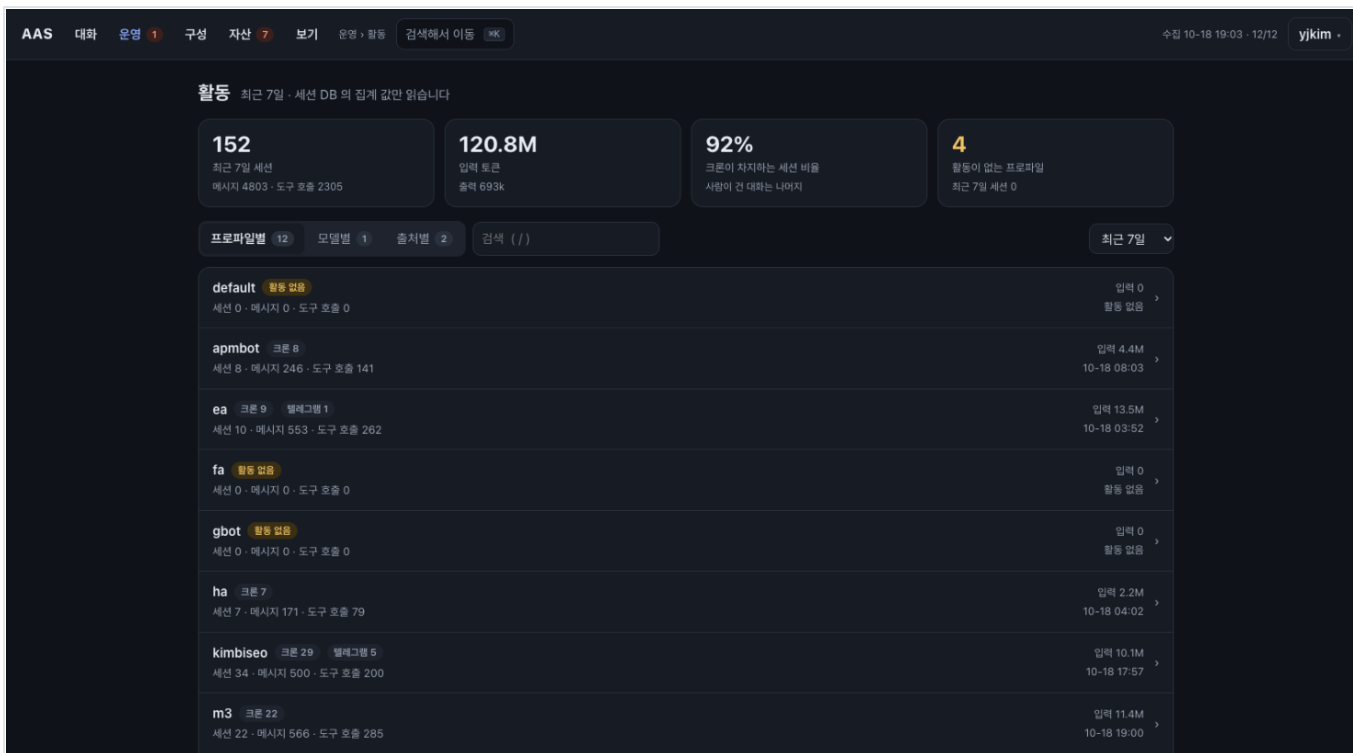
결과

동작이 바뀌어도 원인을 대화창에서 찾지 못함

KEY INSIGHT

실행의 대부분은 사람이 보지 않는 동안 일어남 —

전달 대상이 빈 작업의 실패는 결과를 기다리던 사람이 가장 늦게 발견함



화면 예시 — AAS 활동 화면(운영 설치본 화면 예시): 최근 7일 세션 152개, 정기 업무 비율 92%

채팅 창에 남는 대화는 사람이 시작한 8% 남짓 — 나머지는 결과 메시지로만 확인

92%

세션 152개 중 사람이 아니라
정기 업무가 시작한 비율

알림이 안 가는 작업이 생기는 세 조건

처음부터 전달 대상 없이 만든 작업
파일로만 저장하는 수집 작업에 혼함대화방 삭제 · 봇 제거로 대상이 사라진 작업
작업 목록에는 정상 등록으로 보임퇴사자 개인 대화방으로 남은 작업
담당자가 바뀐 뒤에도 알림이 옛 사람에게 감

실패하지 않은 작업도 맞는 결과라는 보장은 없음

정상 종료된 작업도 엉뚱한 기간을 모으거나

빈 결과를 성공으로 보고할 수 있음

→ 결과 검증 주기를 따로 정함

KEY INSIGHT

세 원인 모두 담당자가 에이전트를 만들고 지켜볼 화면이 없다는 데서 나옴 —
도구를 고를 때 이 화면이 있는지가 첫 기준임

1

정착은 담당자가 정함

AI Agent 탑재 앱 40% 전망
업무 기능 기준 확대 적용은
10% 이하

탑재는 공급사, 정착은 업무를
아는 담당자가 정함

2

채팅 창구는 승인 근거 없음

승인이 "네" 한 줄로 끝남
모델 · 스킬 · 정기 업무 설정은
여러 곳에 흩어짐

무엇을 보고 승인했는지가
기록에 남지 않음

3

실행의 92%는 정기 업무

사람이 보지 않는 동안 실행됨
전달 대상이 없는 작업의 실패는
아무도 모름

결과를 기다리던 사람이
가장 늦게 발견함



필요한 것

만들기와 지켜보기를 한 화면에서 하는 콘솔

PART 02

AI Agent 도구 시장 여섯 구분과 AAS 위치

만드는 도구와 지켜보는 도구 · 조직 안 설치 조건 · 조건별 제품 선택

도구 선정 관점

KEY INSIGHT

제작 도구는 자사 실행 엔진이 전제이고 관측 도구는 운영자 · 보안팀용임 —
업무 담당자가 한 제품으로 둘을 다 하는 선택지가 없음

만들기

② 에이전트 · 워크플로 빌더

오픈소스, 개발자용

① 업무 담당자용 에이전트 빌더

상용, 공급사 런타임 일체형

③ 채팅 UI · 워크스페이스

대화 화면 중심, 플랫폼 운영 없음

④ 관제 · 거버넌스 도구

IT · 보안팀용, 만드는 화면 없음

⑤ 플랫폼 전용 콘솔

운영자 1인 전제

⑥ 조직 운영 콘솔

회사 경영 · 개발팀 은유

AAS

비어 있는 자리

업무 담당자가
만들고 지켜보기를
함께 하는 도구지켜
보기

← 운영자 · IT가 씀

업무 담당자가 씀 →

만드는 쪽 ① ② ③

상용 빌더는 공급사 실행 엔진과
한 묶음으로 들어옴

오픈소스 빌더는 개발자 지향,
채팅 UI는 실행 관측이 없음

지켜보는 쪽 ④ ⑤ ⑥

관제 도구와 플랫폼 콘솔은
운영자 · 보안팀이 보는 화면

AAS는 ⑤에서 출발해
①의 사용자인 부서 담당자를 겨냥

KEY INSIGHT

온프레미스 일체형은 쓰던 플랫폼에 붙지 않고 오픈소스 콘솔은 운영자 1인용임 —
망 분리 조직의 선택지가 플랫폼 교체 아니면 운영자용 화면뿐임

도구 구분	조직 안 설치	업무 담당자 사용	만들기	지켜보기	쓰던 플랫폼 연결
① 외부 클라우드 빌더	×	○	○	△ 분석 화면	×
① 온프레미스 일체형 플랫폼	○	○	○	△ 활동 기록	×
② 워크플로 빌더	○	△ 개발자 지향	○	△ 실행 기록	×
③ 채팅 UI	○	○	△	×	해당 없음
④ 관제 · 거버넌스	△	× IT · 보안팀	×	○	△
⑤ 플랫폼 전용 콘솔	○	△ 운영자 1인	○	△ 로그 수준	○
⑥ 조직 운영 콘솔	○	○	○	△	○
MSAP.ai AAS	○	○	△ 스크립트 스킬은 콘솔 밖 편집	○	○ Hermes Agent 1종

○ 제공 · △ 일부 제공 또는 제약 있음 · × 공식 자료에서 확인하지 못함

KEY INSIGHT

활용 범위는 공개 등급부터 넓어지고 기밀 등급은 분리가 유지됨 —
그 업무에서는 외부 클라우드 빌더가 기능과 관계없이 검토 대상에서 빠짐

N²SF(National Network Security Framework, 국가 망 보안체계) — 2025-01 가이드라인 초안, 6개 통제 영역

기밀 (C)



분리 유지

외부 서비스 활용이 가장 제한됨 — 기밀 등급 업무는 분리된 망에 남음

민감 (S)

조건부 검토

보안 대책을 갖춘 범위에서 활용 검토

공개 (O)

먼저 완화

망 분리 규제 완화를 먼저 적용 — 2026-03 공공기관 업무 PC 생성형 AI 실증 공모 시작

조직 안 설치가 필요한 기관의 두 가지 도입 방식

방식 A

온프레미스 일체형 플랫폼 신규 도입

빌더 · 런타임 · 스토어를 한 공급사가 제공

쓰던 플랫폼에서 옮기는 전환 비용 발생

방식 B — AAS 방식

오픈소스 에이전트 플랫폼 위에 콘솔만 추가

쓰던 플랫폼, 또는 조직 안에 새로 설치할 플랫폼에 연결

플랫폼은 그대로 두고 화면만 붙임

KEY INSIGHT

외부 클라우드를 쓸 수 있는 조직에는 글로벌 클라우드 빌더가 더 완성도 높음 —
AAS는 망 분리 조직과 오픈소스 플랫폼 보유 조직에 맞춤

외부 클라우드 사용 가능

Hermes
Agent
운영 · 계획

글로벌 클라우드
빌더 우선 검토

스크립트 스킴 제작 · 사내 마켓
관리자 통제 · 운영 이력에서 앞섬

오픈소스
플랫폼
없음

외부 클라우드 사용 불가

MSAP.ai AAS

쓰던 플랫폼 위에 콘솔 추가

한 사람만 운영하면
플랫폼 내장 대시보드나
오픈소스 웹 UI로 충분할 수 있음

온프레미스
일체형 플랫폼

빌더 · 런타임 · 스토어 일체
플랫폼 전환 비용 발생

도입 전 점검 질문

1

업무 데이터를 외부 클라우드에 둘 수 있는가
가능하면 글로벌 클라우드 빌더부터 검토

2

Hermes Agent를 운영하거나 도입할 계획인가
아니면 온프레미스 일체형 플랫폼과 비교

3

여러 사람이 각자 에이전트를 만들고
관리자가 전체를 봐야 하는가
한 사람 운영이면 콘솔 없이도 충분할 수 있음

4

마켓 결제와 부서별 비용 통제가
첫 도입의 필수 조건인가
필수라면 AAS의 현재 범위 밖

KEY INSIGHT

외부 클라우드를 쓸 수 없고 Hermes Agent를 쓰거나 쓸 계획이면 도입 검토 대상임 —
외부 클라우드를 쓸 수 있으면 글로벌 클라우드 빌더를 먼저 검토함

1

담당자 자리가 비어 있음

여섯 구분 가운데 업무 담당자가
만들고 지켜보는 도구는 없음

제작 도구는 자사 엔진 전제,
관측 도구는 운영자 · 보안팀용

2

네 조건을 함께 갖춘 구분 없음

조직 안 설치 · 담당자 사용 ·
만들기와 지켜보기 ·
쓰던 플랫폼 연결

일체형은 플랫폼 교체가 필요하고
오픈소스 콘솔은 운영자 1인용

3

기밀 등급은 분리 유지

N²SF 기밀 등급 업무에서는
외부 클라우드 빌더가
검토 대상에서 빠짐

조직 안 설치가 필요한 기관의
선택지는 일체형 또는 콘솔 추가



AAS가 맞는 조직

조건 1 외부 클라우드 사용 불가

+ 조건 2 Hermes Agent 운영 또는 도입 계획

PART 03

AAS 정의와 Hermes Agent 연결 구조

담당자와 플랫폼의 역할 분담 · 계층별 읽기 · 변경 범위 · 사용자 네 부류

제품 이해 관점

KEY INSIGHT

업무를 아는 사람이 직접 에이전트를 고침 —

업무 규칙이 바뀔 때마다 IT 개발 요청을 거치지 않아도 됨

MSAP.ai AAS

AI Agent 플랫폼에 연결되는 일반 사용자용 콘솔

부서 담당자가 정의하는 세 가지

누가

에이전트 · 프로필

성격 · 모델 · 메신저 연결

어떻게

스킬

업무 방법 · 순서 ·
사람 확인 조건

언제

정기 업무

실행 시각 · 주기 ·
결과 보낼 곳

실행은
플랫폼이 맡음

Hermes Agent

콘솔의 네 기능 묶음



만들기

에이전트 추가, 프로필 정의
스킬 판 관리, 정기 업무 등록

사키기

진행 단계 · 실행 승인 · 되묻기가
보이는 채팅
여러 에이전트에게 묻는 회의

지켜보기

정기 업무 실패 · 멈춤 · 알림 누락
자격증명 만료, 호출 관계

나누기

사내 스킬 마켓
사용자별 에이전트와 권한

KEY INSIGHT

AAS가 멈춰도 정기 업무는 플랫폼에서 계속 실행됨 —
콘솔을 붙이거나 떼어도 운영 중인 에이전트에 영향이 없음

Hermes Agent 계층

읽기 — 모든 계층에 닿음

변경 — 두 계층에만 닿음

런타임

게이트웨이 · 모델 연결

게이트웨이 상태
모델 연결

바꾸지 않음

플러그인 · 설정 · 버전 그대로

프로파일

에이전트 안의 업무 묶음

성격 · 모델 · 메신저
최근 활동

만들기 · 내보내기 · 삭제

성격 · 모델 변경

공식 API 경유

스킬 · 정기 업무

일하는 방법과 실행 일정

스킬 판 · 실행 일정
실패 · 알림 대상

스킬 문서 수정

정기 업무 등록 · 수정

MCP 서버 ·
외부 시스템

호출 관계
자격증명 이름 · 위치

바꾸지 않음

고객 환경에서 설정

조직 상황별 연결 방법

Hermes Agent 운영 중

바로 연결

운영 중인 정기 업무를 멈추지 않음

플랫폼 미정

함께 설치

Hermes Agent와 AAS를 조직 안에 함께 구성

다른 플랫폼 운영

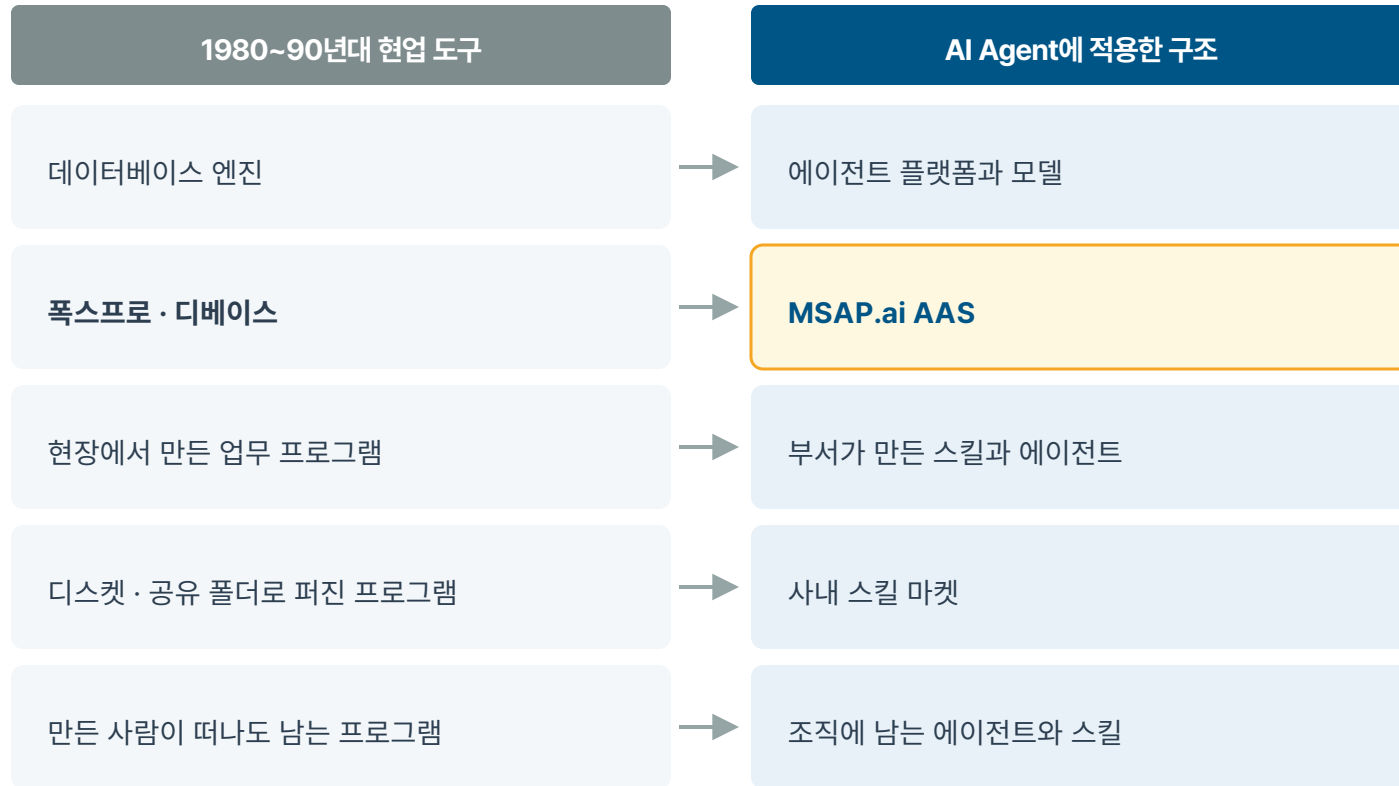
현재 연결 불가

두 번째 플랫폼 연결은 로드맵

MCP(Model Context Protocol) — 에이전트가 외부 도구를 일정한 규약으로 부르는 공개 프로토콜

KEY INSIGHT

어려운 부분은 엔진이, 업무 규칙은 담당자가 말을 때 현업 도구가 퍼짐 —
판 이력과 실패 관측이 있어야 만든 사람이 떠난 뒤에도 관리됨



Visual FoxPro는 2007년 개발 종료 — 현업이 업무 프로그램을 직접 만들던 대표 도구

선례가 남긴 관리 문제

누가 어떤 판을 쓰는지 모름

고칠 사람이 남지 않음

AAS의 대응

스킬 판 이력과 비교 · 되돌리기

마켓 패키지의 설치 위치 표시

정기 업무 실패 · 알람 누락 관측

만든 사람이 떠나도 판과 실행 상태가 남음

KEY INSIGHT

주 사용자는 부서 담당자이고 나머지 셋은 결과를 보거나 기반을 관리함 —
담당자가 늘어나도 플랫폼 설정은 IT 통제 아래 남음

 부서 담당자

주 사용자

하는 일

에이전트 추가, 프로필 만들기
정기 업무 예약, 채팅 지시

주 화면

내 에이전트 · 스킬 · 자동화 · 대화

 부서장 · 팀 리더

하는 일

팀 에이전트의 처리량과
실패 확인

주 화면

대시보드 · 오늘 볼 것 · 오피스

 IT · 플랫폼 관리자

하는 일

플랫폼 · 모델 · 자격증명 · 권한
사람별 에이전트 한도 관리

주 화면

사용자 · 권한 · 자격증명

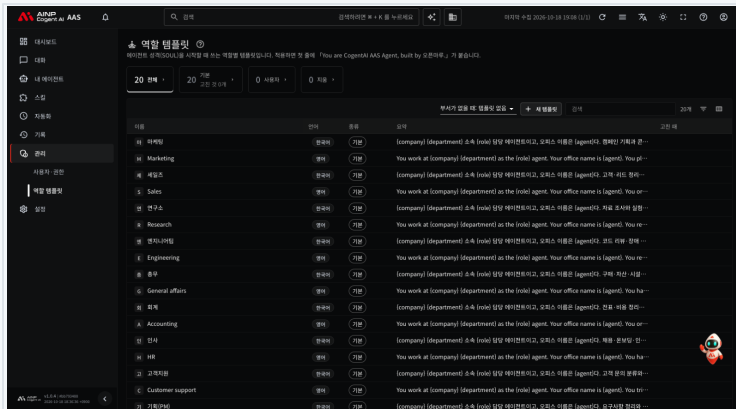
 보안 · 감사 담당

하는 일

외부 호출 대상과
변경 이력 점검

주 화면

흐름 · 변경 기록 · 활동



역할 템플릿 20종

마케팅 · 영업 · 연구소 · 엔지니어링 · 총무 · 회계 · 인사 · 고객지원 · 기획
한국어 · 영어 짝으로 제공

에이전트 성격(SOUL) 문서의 출발점 — 조직이 직접 추가할 수 있음

화면 예시 — 역할 템플릿 목록(쿠버네티스 배포본 v1.0.4)

KEY INSIGHT

AAS를 붙이거나 떼어도 운영 중인 에이전트는 그대로 둬 —
도입 위험이 콘솔 범위 안에 머물

1

담당자가 정의함

에이전트 · 스킬 · 정기 업무는
부서 담당자가 정의하고
실행은 Hermes Agent가 맡음

폭스프로 · 디베이스와 같은
현업 도구의 역할 분담

2

플랫폼을 고치지 않음

읽기는 모든 계층
변경은 프로파일과
스킬 · 정기 업무까지만

런타임의 플러그인 · 설정 ·
버전은 그대로 둬

3

역할별로 다른 화면

부서 담당자 · 부서장 ·
IT 관리자 · 보안 담당이
같은 데이터를 봄

플랫폼 설정은 IT 통제 아래
남음



담당자가 얻는 것

업무 규칙이 바뀔 때마다 IT 개발 요청을 거치지 않아도 됨

PART 04

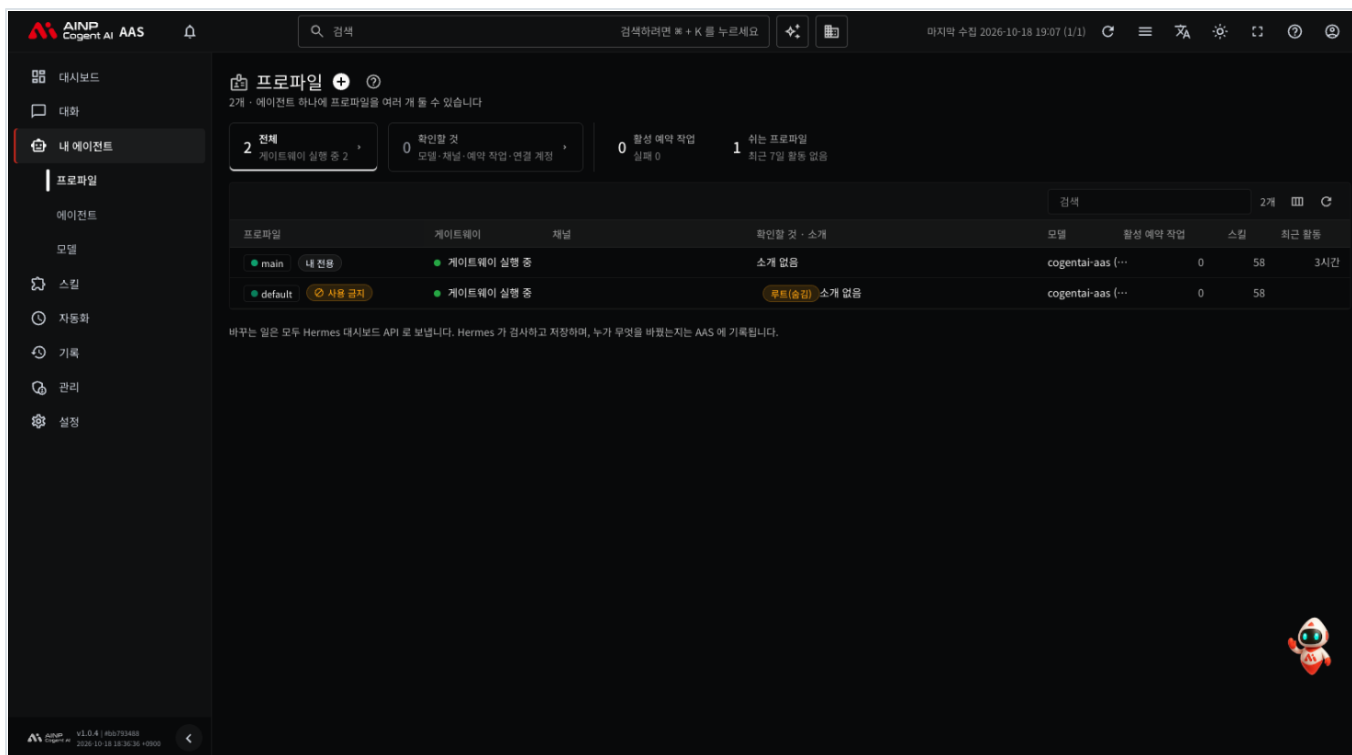
AAS 콘솔 네 기능 묶음의 실제 화면

에이전트 · 스킬 만들기 · 채팅으로 시키기 · 첫 화면으로 지켜보기 · 사내 마켓으로 나누기

부서 담당자 관점

KEY INSIGHT

잘 만든 업무 구성은 나눠 쓰되 자격증명은 사람 사이로 옮겨 가지 않음 —
복제 · 가져오기에서 비밀값(.env)이 복사되지 않음



화면 예시 — 프로파일 목록(쿠버네티스 배포본 v1.0.4): 게이트웨이 상태 · 주 모델 · 정기 업무 · 스킬 수

주 모델은 LiteLLM 게이트웨이에서 실제로 응답하는 모델 가운데서만 선택

에이전트 총 — 사람마다 받는 실행 단위

이름만 주고 추가, 사용자당 기본 3개 한도
관리자가 사람마다 한도 조정, 소유권 이전
30일 미사용 · OIDC 그룹 이탈 시 자동 멈춤
멈춤 동안 데이터 보존, 행 메뉴에서 다시 시작
OIDC(OpenID Connect) — 사내 표준 로그인

프로파일 총 — 에이전트 안의 업무 묶음

성격 · 설정 · 비밀값 · 스킬 · MCP · 정기 업무 ·
메신저 연결 · 모델을 프로파일마다 따로 가짐

새 프로파일: 기존 프로파일 복제, 또는
다른 에이전트에서 가져오기(스킬 제외 선택 가능)



비밀값은 복사되지 않아 담당자가 새로 넣음

삭제는 보관본 내보내기 성공 + 이름 다시 입력 후

KEY INSIGHT

문서로 끝나는 스킬은 담당자가 직접 고침 —
스크립트가 필요한 스킬은 아직 개발 인력의 손을 거침

스킬	위치	출처	태그	설명	예약 작업	스크립트	MCP	URL
A airtable	main	Hermes 기본	자동화·도구 지식·데이터	Airtable REST API via curl. Records CRUD, filters, upserts.	0	0	0	2
A apple-notes	main	Hermes 기본	자동화·도구	Manage Apple Notes via memo CLI: create, search, edit.	0	0	0	0
A apple-reminders	main	Hermes 기본	자동화·도구	Apple Reminders via remindctl: add, list, complete.	0	0	0	0
A architecture-diagram	main	Hermes 기본	디자인 이미지 생성	Dark-themed SVG architecture/cloud/infra diagrams as ...	0	0	0	1
A arxiv	main	Hermes 기본	지식·데이터 학습·안내	Search arXiv papers by keyword, author, category, or ID.	0	1	0	4
A ascii-video	main	Hermes 기본	자동화·도구	ASCII video: convert video/audio to colored ASCII MP4/...	0	0	0	2
B baoyu-infographic	main	Hermes 기본	디자인 이미지 생성	Infographics: 21 layouts x 21 styles (信息图, 可视化).	0	0	0	2
B blocked-page-recovery	main	Hermes 기본	자동화·도구	Use when a fetch fails: 403/429, paypal, WAF, bot wall.	0	1	0	3
B box	main	Hermes 기본	자동화·도구 지식·데이터	Box manages cloud files, sharing, search, and metadata.	0	0	0	5
C claude-code	main	Hermes 기본	개발 절차 코드 품질	Delegate coding to Claude Code CLI (features, PRs).	0	0	0	1
C claude-design	main	Hermes 기본	디자인	Design one-off HTML artifacts (landing, deck, prototype).	0	0	0	0
C codebase-inspection	main	Hermes 기본	코드 품질	Inspect codebases w/ pygount: LOC, languages, ratios.	0	0	0	0
C codex	main	Hermes 기본	코드 품질 개발 절차	Delegate coding to OpenAI Codex CLI (features, PRs).	0	0	0	1
C competitor-news-monitor	main	Hermes 기본	지식·데이터 자동화·도구	Watch named companies for material news: cited digests.	0	0	0	0
C computer-use	main	Hermes 기본	자동화·도구	Drive the desktop background first; escalate on signal.	0	0	0	1
D design-md	main	Hermes 기본	문서·글쓰기 API·구조	Author/validate/export Google's DESIGN.md token spec...	0	0	0	1

화면 예시 — 기본 스킬 58개 AI 태그 분류: 자동화 · 도구 28, 개발 절차 12, 문서 · 글쓰기 11 ...

스킬 = 에이전트가 일하는 방법을 적은 문서, 저장할 때마다 판이 남음

편집기

미리 보기 · 임시 저장 · 저장 메모

저장 전 바뀐 줄 확인

판 비교 · 되돌리기

동시 수정 충돌 시 저장 차단

스킬 목록

정기 업무 · 스크립트 · MCP · 외부 URL 호출 수

"호출 대상" 거르기로 계정 교체 전

영향받는 스킬 찾기

⚠️ 남은 제약

스크립트 파일은 콘솔에서 읽기만 가능 — 플랫폼에

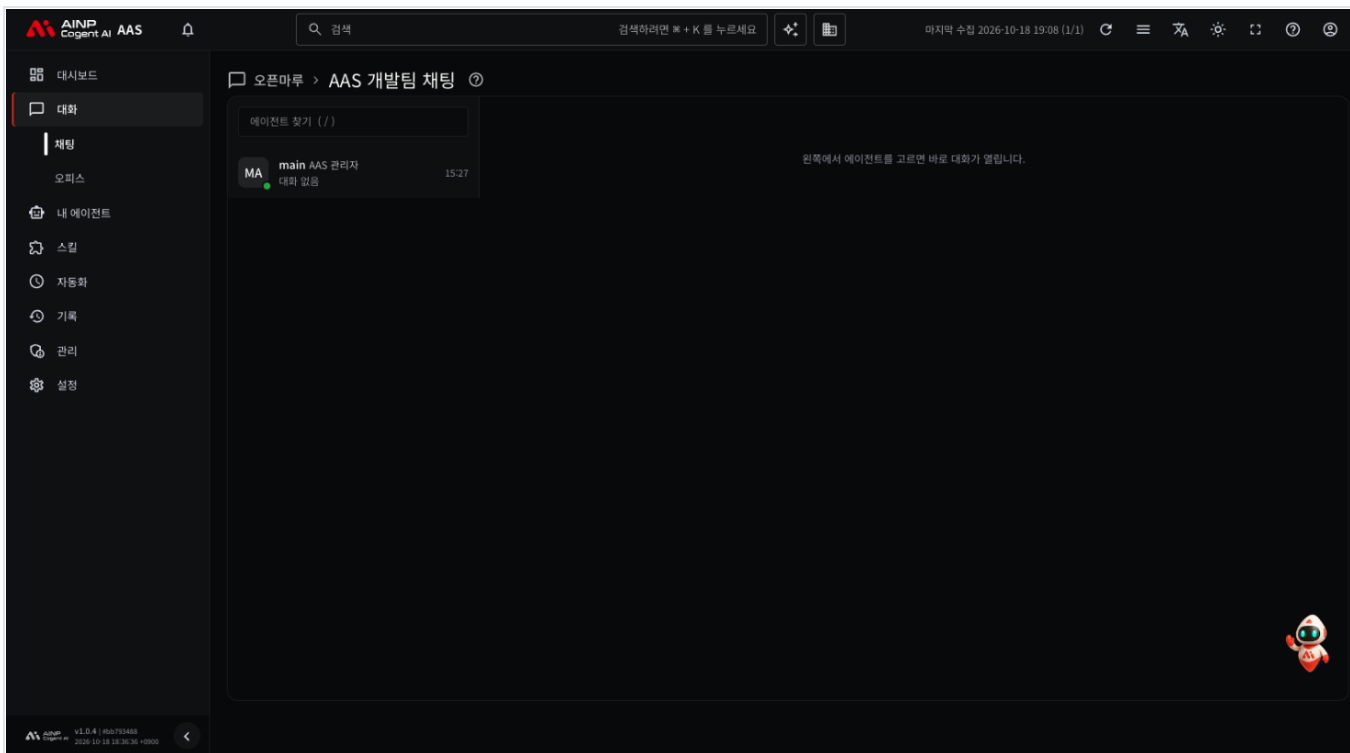
스크립트 저장 공식 API가 없음

에이전트가 고친 스킬의 검토 규칙은 조직이 정함

KEY INSIGHT

명령마다 사람의 승인이 대화 기록 안에 남음 —

봇 등록과 토큰 복사 없이 콘솔 로그인만으로 에이전트와 대화함



화면 예시 — 팀 채팅(쿠버네티스 배포본 v1.0.4)

지난 대화 목록에는 메신저 · CLI · 정기 업무에서 시작한 세션도 함께 보임

채팅에 나오는 카드

진행 단계

상태 · 부른 도구 · 추론(접힌 상태)

승인

실행하려는 명령 — 실행 전 사람 승인

되물기

질문마다 한 장 — 빠진 조건 채우기

회의 탭

한 메시지를 여러 에이전트에게 동시에 보냄

여러 설치본의 에이전트가 한 방에서 답함

나온 할 일은 칸반 카드로 이어짐

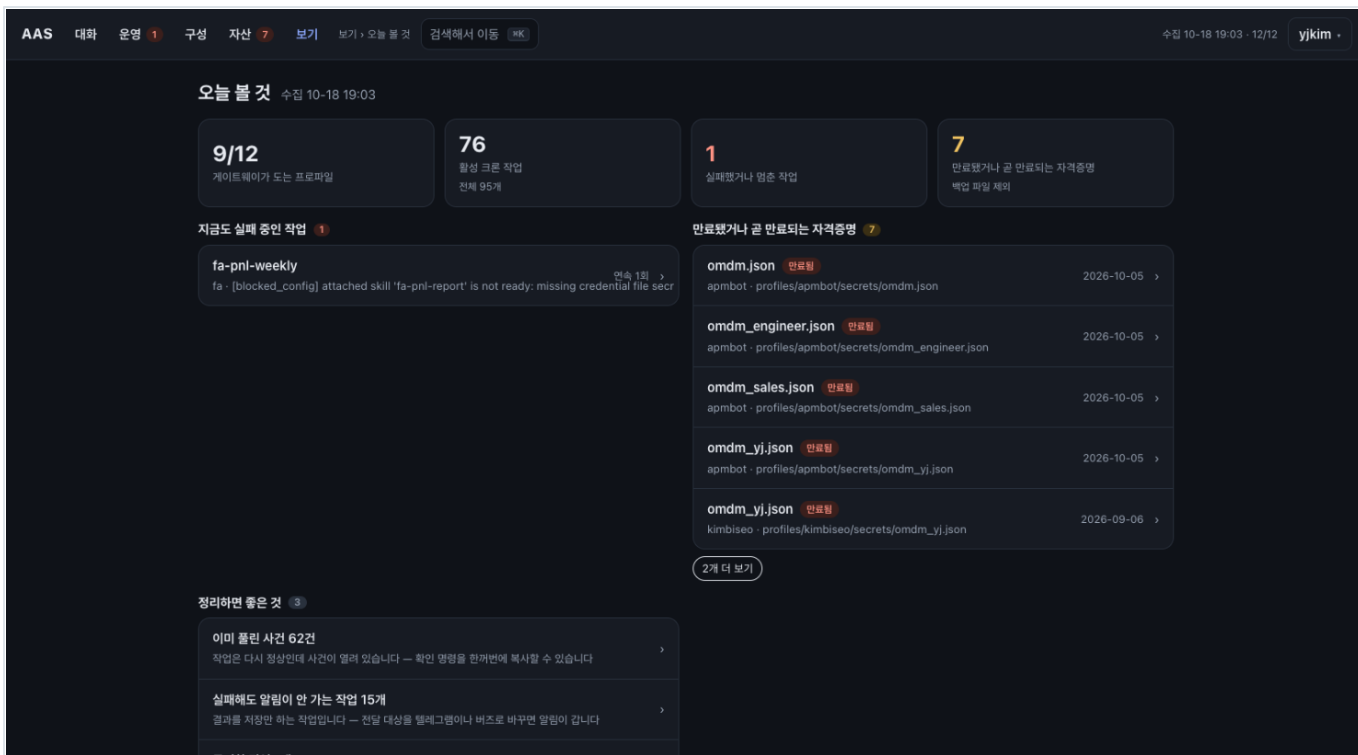


파일럿 단계에서는 회의방을 조직 안 설치본으로 한정

외부 에이전트 연결은 별도 보안 검토

KEY INSIGHT

게이트웨이가 꺼진 프로파일의 정기 업무는 실패로도 기록되지 않음 —
9/12 같은 실행 상태가 실패 건수만큼 중요한 신호임



화면 예시 — 첫 화면 "오늘 볼 것"(운영 설치본)

아래 묶음: 답을 기다리는 대화 · 지금도 실패 중 · 문제 있는 프로파일 · 만료 자격증명

게이트웨이 실행

9/12

활성 정기 업무

76

지금도 실패 중

1

만료 · 임박 자격증명

7

정리하면 좋은 것: 이미 풀린 사건 62 · 알림 안 가는 작업 15



하루 두 번 요약 알림 — 08:30 · 18:30

수집 성공 12/12 · 신규 실패 0 · 지금도 실패 1

이미 풀림 62 · 멈춤 0 · 알림 없음 15

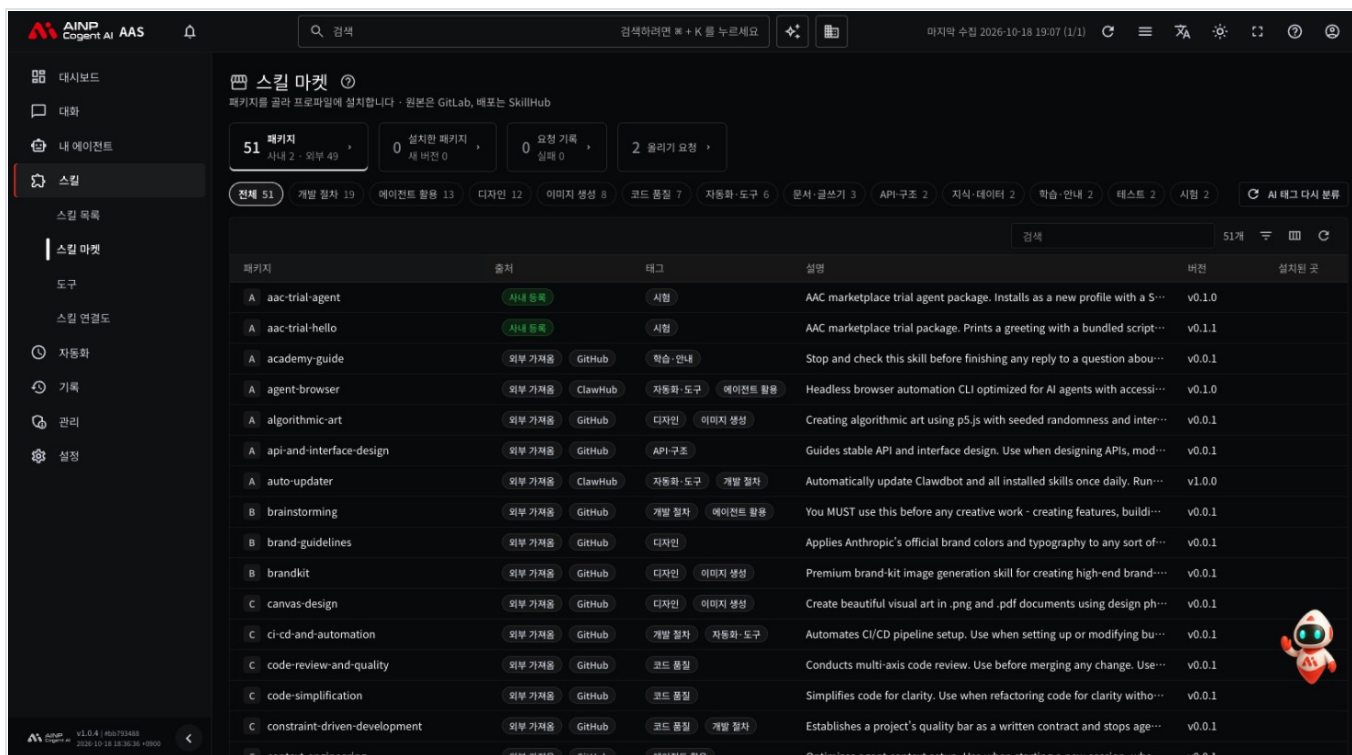
실패가 0건이어도 요약을 보냄

요약이 오지 않으면 수집 · 발송 이상 신호

알림 예시는 운영 설치본 기준

KEY INSIGHT

배포 경로가 마켓 하나로 모이고 에이전트가 사람 단위로 관리됨 —
퇴사자 에이전트는 멈추고 데이터는 남아 후임자에게 넘길 수 있음



화면 예시 — 사내 스킬 마켓 패키지 51개(사내 등록 2 · 외부에서 가져옴 49)

원본은 사내 GitLab, 배포는 SkillHub — 부서가 만든 스킬을 다른 부서가 설치

설치 범위

스킬 패키지 → 기존 프로파일에 설치
에이전트 패키지 → 새 프로파일로 설치
설치 기록에 실패한 요청까지 남김

사람 단위 에이전트 관리

OIDC(사내 표준 로그인) 그룹 연동
사용자당 에이전트 기본 3개
그룹 이탈 · 30일 미사용 → 자동 멈춤, 데이터 보존
행 메뉴에서 다시 시작

! 아직 부족한 것

부서 단위 권한과 부서별 비용 할당
→ 운영 규칙으로 보완

KEY INSIGHT

네 묶음 모두 사람의 확인과 기록을 화면에 남김 —

담당자가 바뀌어도 무엇을 왜 바꿨는지 추적됨



만들기

에이전트와 업무별 프로필
스킬 판 이력 · 비교 · 되돌리기(복제 · 가져오기 모두 해당)
(복제 · 가져오기 모두 해당)

시키기

승인 카드 · 되묻기 카드가
있는 팀 채팅
여러 에이전트에게 묻는 회의 탭명령마다 승인이
대화 기록 안에 남음

지켜보기

첫 화면 "오늘 볼 것"
하루 두 번 요약 알림게이트웨이 실행 상태가
실패 건수만큼 중요함

나누기

사내 스킬 마켓
사람 단위 에이전트 관리퇴사자 에이전트는 멈추고
데이터는 후임자에게 넘김

한 콘솔에 네 묶음

업무 담당자가 IT 도움 없이 고치고 확인함

PART 05

AAS 업무 에이전트 부서별 사례

10개 카테고리 카탈로그 · 명함 · 공문 · 회의록 처리 방식 · 부서별 활용 장면

현업 부서 관점

KEY INSIGHT

세 카테고리는 사람이 보낸 사진 · 파일 · 녹음으로 시작하고 일곱은 정기 업무 중심임 —
정기 업무가 많은 업무일수록 실패 감시가 운영의 중심이 됨

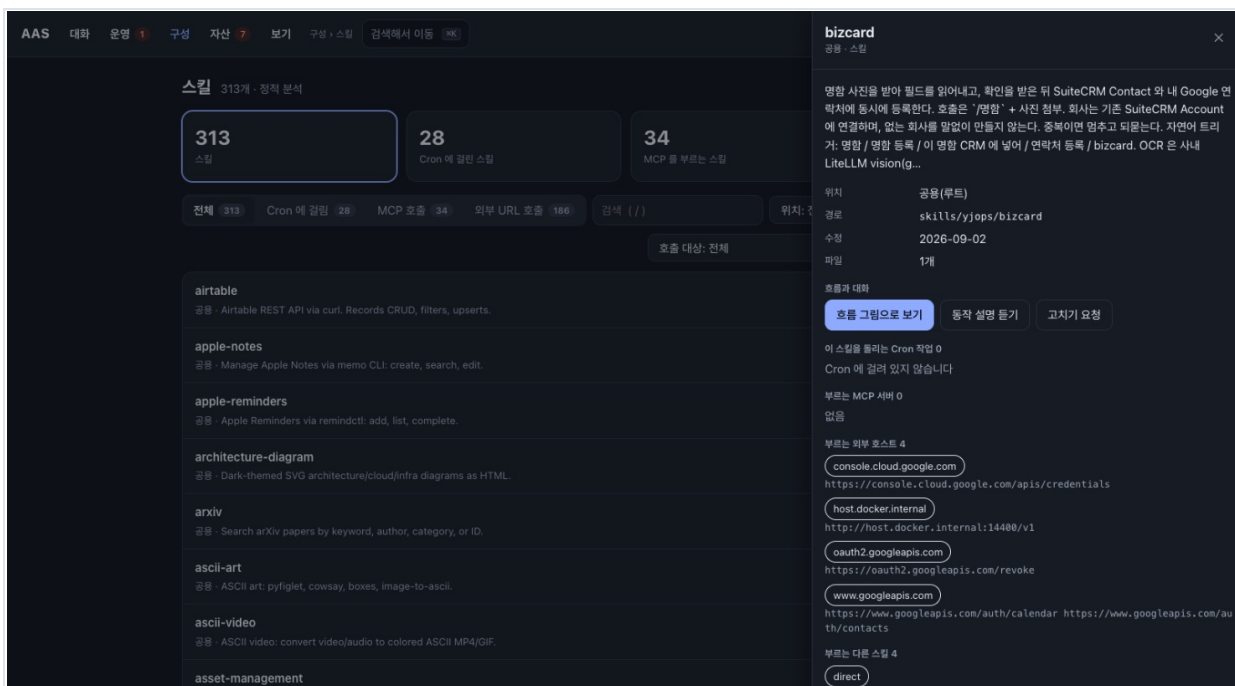
카테고리	대표 유즈케이스	담당 에이전트	주된 시작 신호
1 문서 · OCR	명함 → CRM 연락처, PDF · 스캔 판독	영업 · 비서	사진 · 파일 첨부 사람이 보낸 입력으로 시작
2 공공 문서 · 서식	HWP · HWPX 인식, 서식 채우기, 기안문, 법령 인용 확인	공공	첨부 · 대화 · 정기
3 음성 · 회의	화자 구분 회의록 → 지시사항 → 할 일	비서	녹음 · 음성
4 영업 · CRM	영업기회 등록, 일 · 주 · 월 영업 보고, 무활동 딜 점검	영업	정기 · 대화
5 마케팅 · 지표	웹 · 검색 · 유튜브 지표 보고, 이상 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 점검 보고, 장애 1차 조사	APM	정기 · 대화
9 리서치 · 콘텐츠	기술 조사, 백서 · 장표 제작	리서치	대화 · 정기
10 개인 비서	아침 브리핑, 휴가자 안내, 리마인더	비서	정기 · 음성

화면 예시 — 운영 설치본: 업무 에이전트 11개 · 스킬 313개. 연결 시스템(CRM · 위키 · 드라이브 등)은 고객 환경에 맞춰 설정

KEY INSIGHT

판독 정확도 대신 기록 전 확인으로 잘못된 등록을 막음 —

중복 고객사가 하나 생기면 이후 영업 집계가 모두 어긋남



화면 예시 — 명함 인식 스킬 상세(운영 설치본)



판독은 조직 안 AI 게이트웨이의 비전 모델

고객 이름 · 휴대전화가 담긴 이미지가 외부 OCR로 나가지 않음

1

등록 전 예행(dry-run) 확인

어느 시스템에 무엇을 쓸지 먼저 보여 줌

2

중복이면 멈춤

같은 사람이 있으면 멈추고 갱신 여부를 되물음

3

없는 회사는 만들지 않음

새 고객사 등록은 사람이 결정

기록처 3곳: CRM 연락처 · 연락처 · 위키 명함집(회사 · 이름)



파일럿 후보로서의 특성

반복량 많음 — 행사마다 수십 장

사람 확인 1회 · 연결 시스템 3곳

KEY INSIGHT

두 업무 모두 외부 OCR · STT 없이 끝남 —

기밀 등급 업무가 남은 기관에서도 같은 구성으로 실행할 수 있음

공문 판독 · 서식 채우기

중앙부처형 · 지자체형 각 10개 업무

HWP · HWPX · PDF · DOCX → 마크다운 변환 → 요약

문서 변환 MCP 도구 서버가 처리



스캔본은 CPU 오프라인 OCR

한국어 모델, 외부 API 키 불필요



공공서식 빈칸 구조 분석 → 채운 값을 먼저 보여 줌

→ 사람이 확인한 뒤 저장

기안문 · 보고서 HWPX 생성

법령 인용 확인

법령 조회 API 키가 없으면 추측하지 않고 멈춤

화자 구분 회의록

조직 안 GPU 서버에서 처리

STT

음성 → 글자

화자 분리

말한 사람 구분

실명화

목소리 지문

템플릿

부서별 양식

STT(Speech-to-Text, 음성 인식) · 근거가 없으면 이름 대신 "미확인"으로 표시

지시사항

지시 · 근거 · 기한

→ 지시 원장
(D · F 번호로 추적)

액션 아이템

항목 · 담당 · 기한

→ 칸반 체크박스
30분 주기 정기 업무가
체크 결과를 거둬 감

원본 음성 보관이 실패하면 위키에 올리지 않음

회의록과 원본 음성이 짝으로 남아야 나중에
화자 실명과 지시 근거를 다시 확인할 수 있음

KEY INSIGHT

프로파일 · 스킬 · 정기 업무 · 결과물이 조직 시스템에 저장됨 —
 퇴사 · 부서 통합 · 지사 확산 때 일하는 방식이 구성째 넘어감

부서	시작 신호 → 에이전트가 하는 일	사람이 판단하는 단계
경영	주간 회의 녹음 → 회의록 · 지시 원장 · 칸반 할 일	화자 실명 확정, 완료 체크
영업	명함 사진 · 매일 정기 실행 → CRM 등록, 무활동 · 퇴사자 담당 딜 보고	등록 전 확인, 딜 재배정
인사	04:00 정기 실행 → 이력서 점수와 근거	채용 판단 전부
IT 운영	"어제 15시 응답 지연" 질문 → 지표 조사 · 원인 후보	부담 큰 수집과 쓰기 도구 실행 지시
공공	HWP 공문 첨부 → 요약 · 서식 채우기	채운 값 확인 후 저장

에이전트가 반복 작업을 하고 판단은 사람에게 남김

부서마다 사람이 확인하는 단계가 절차 안에 한 번 이상 있음



KEY INSIGHT

판독 정확도보다 기록 전 확인이 잘못된 등록을 막음 —
사람 확인 단계가 이미 있는 업무가 첫 적용 대상으로 알맞음

1

기록 전에 사람이 확인

예행 결과를 먼저 보여 주고
사람이 승인해야 기록함

명함 중복이면 멈추고,
서식은 채운 값을 먼저 보여 줌

2

조직 안에서 처리

비전 모델 · 오프라인 OCR ·
GPU STT로 문서와 음성이
조직 밖으로 나가지 않음

기밀 등급 업무가 남은 기관도
같은 구성으로 실행

3

구성은 조직에 남음

프로파일 · 스킬 · 정기 업무 ·
결과물이 퇴사 뒤에도
후임자에게 넘어감

부서 통합 · 지사 확산 때도
구성재 옮김



첫 적용 대상

명함 인식과 공문 판독은 결과 확인이 쉬운 업무임

PART 06

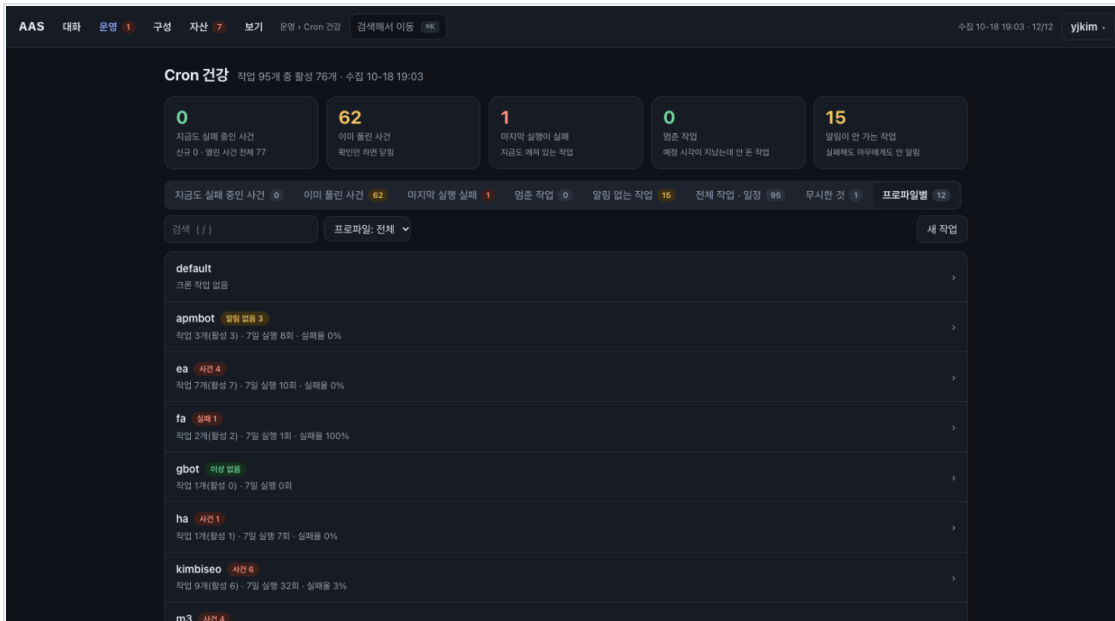
AAS 관측 기능과 보안 구조

Cron 헬스체크 · 값 없는 자격증명 점검 · 읽기 전용 연결과 온프레미스 구성

IT · 보안 검토 관점

KEY INSIGHT

읽지 못한 프로파일은 0건이 아니라 "수집 실패"로 표시됨 —
0이라는 숫자를 믿을 수 있어야 운영 판단을 내릴 수 있음



화면 예시 — Cron 헬스체크 프로파일별 보기(운영 설치본)

정기 업무 95개(활성 76) · 이미 풀림 62

알림 안 가는 작업 15 · 수집 12/12

같은 오류 문자열을 묶어 공통 원인 후보 제시 — 판단과 수정은 운영자

화면 구분

판정 기준

사람이 할 일

● 지금도 실패 중

열린 기록 +
마지막 실행도 실패

원인 조사와 조치

● 이미 풀린 것

열린 기록 +
마지막 실행 성공

확인 명령으로 기록 정리
실행은 운영자

● 마지막 실행 실패

최근 실행 결과가 실패

다음 실행 전 점검

● 멈춘 작업

예정 시각이 지났는데
실행 기록 없음

일정 · 게이트웨이 확인

● 알림이 안 가는 작업

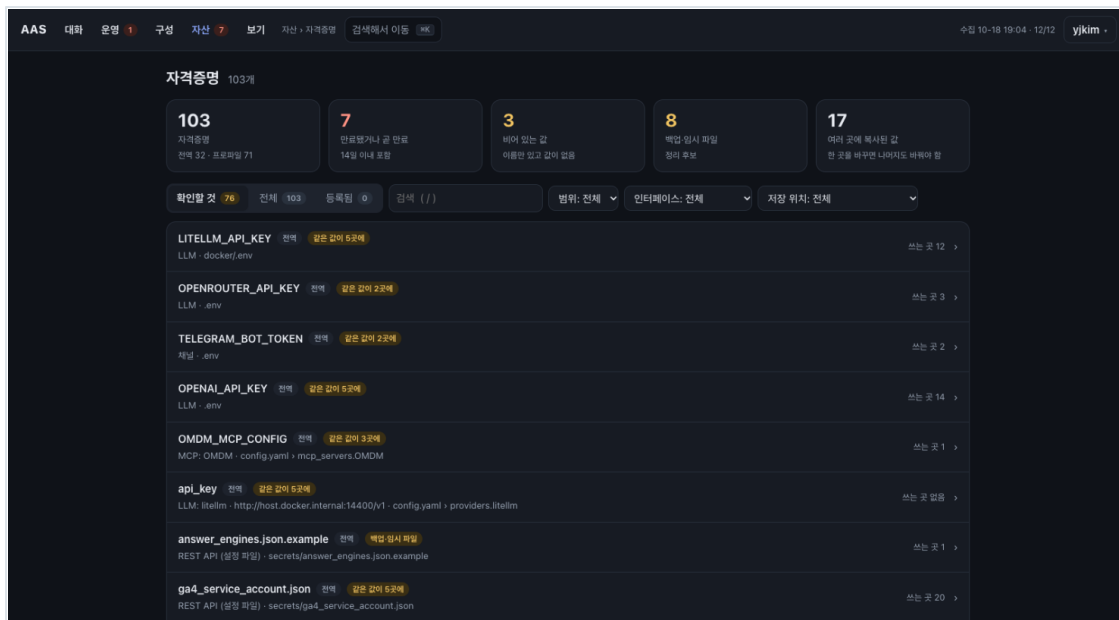
전달 대상 없음

전달 대상 지정
여부 결정

KEY INSIGHT

토큰을 바꾸기 전에 멈출 스킬과 정기 업무를 미리 찾음 —
점검 화면이 또 하나의 비밀값 노출 경로가 되지 않음

자격증명 점검



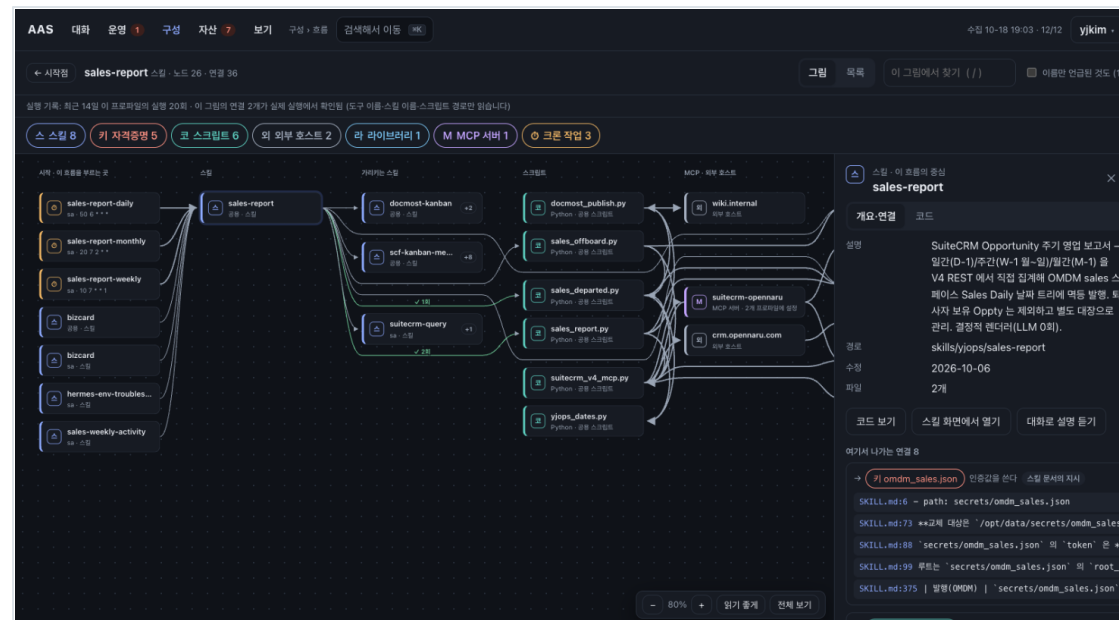
화면 예시 — 103개 중 만료(임박) 7 · 빈 값 3 · 백업 · 임시 파일 8 · 여러 곳에 복사 17

만료일은 토큰 정보로, 중복은 값 해시 비교로 판정 → "같은 값이 N곳에"로만 표시

모델 게이트웨이 카: 같은 값 5곳 · 쓰는 곳 12

→ 교체 전에 확인할 영향 범위

호출 관계 그림(흐름)



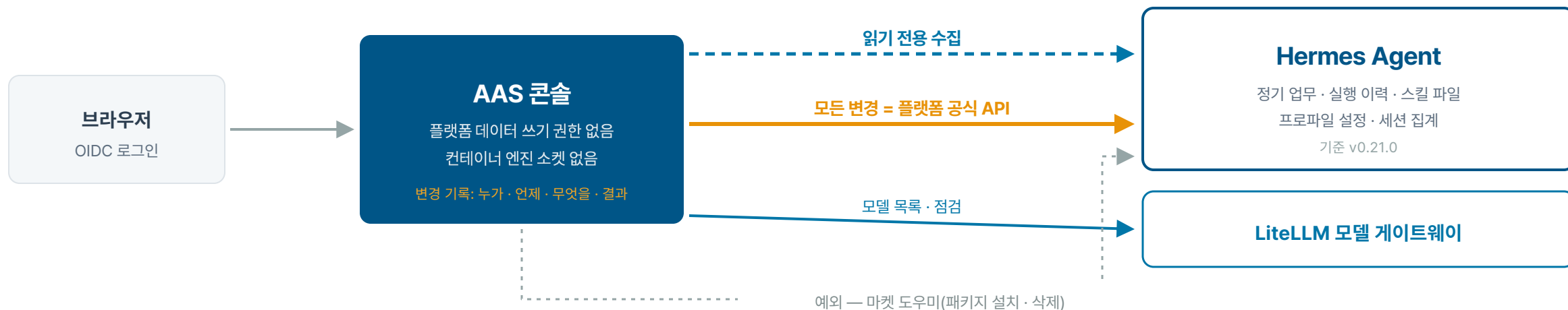
화면 예시 — 영업 보고 스킬의 흐름: 정기 업무 → 스킬 → 스크립트 → MCP 서버 · 외부 호스트

선마다 근거 파일 · 줄: 크론 설정 · 코드에서 확인 · 스킬 문서의 지시 ·
실행에서만 보임(실행 횟수 표시)

한계: 변수로 조립한 주소, 스크립트가 부르는 스크립트는 빠질 수 있음

KEY INSIGHT

도입해도 플랫폼의 플러그인 · 설정 · 버전이 바뀌지 않음 —
운영 중인 정기 업무를 멈추지 않고 콘솔을 붙일 수 있음



경로	하는 일과 범위
읽기	정기 업무 정의 · 실행 이력 · 스킬 파일 · 프로파일 설정 · 세션 집계 — 대화 본문과 호출 인자 값은 읽지 않음
변경	정기 업무 · 스킬 문서 · 프로파일 · 비밀값 넣기 → 플랫폼이 검사 · 저장, 거절 문구는 화면에 그대로 표시
예외 두 가지	마켓 패키지 설치(플랫폼 자신의 설치 명령) · 마켓 스킬 패키지 삭제(AAS가 설치했다고 기록한 폴더 하나)
한계	플랫폼 대시보드 · CLI로 직접 바꾼 내용은 AAS 기록에 없음 → 플랫폼 직접 접근을 IT 관리자로 한정

KEY INSIGHT

다섯 원칙 중 넷은 콘솔이 하지 않는 일을 정함 —

값을 흘리거나 틀린 0을 보여 주는 위험을 기능 단계에서 없앴

설계 원칙

보안 담당이 확인하는 방법

- | 설계 원칙 | 보안 담당이 확인하는 방법 |
|-----------------------------|--------------------------------------|
| 1 플랫폼을 고치지 않음 | 도입 전후 플러그인 · 설정 · 버전 비교 |
| 2 변경 경로는 공식 API 하나 | 거절 문구가 그대로 뜨는지,
스크립트 화면에 고치기가 없는지 |
| 3 비밀값을 화면 · 로그 · 기록에 남기지 않음 | 비밀값 탭에 "있음"만 보이는지 |
| 4 못 읽은 것을 0건이라 하지 않음 | "수집 실패" 표시,
요약의 수집 성공 프로파일 수 |
| 5 흐름 그림을 사람이 그리지 않음 | 선마다 근거 줄과 근거 종류 |

설치

파이썬 표준 라이브러리 + 외부 패키지 2개, 빌드 없는 화면

→ 반입한 컨테이너 이미지만으로 기동

단일 서버 또는 쿠버네티스 배포본

조직 경계 안

AAS 콘솔

Hermes Agent

LiteLLM

조직 안 모델

음성 인식(GPU)

OCR

사내 스킬 마켓

조직 계정(OIDC)

모델 · 음성 인식 · OCR이 조직 안에서 끝남



기밀 등급 설치본은

같은 망 안에 별도 콘솔로 분리

KEY INSIGHT

세 항목 모두 보안 담당이 설치본을 열어 직접 확인할 수 있음 —
검토를 실제 화면으로 끝낼 수 있음

1

실패 상태를 나눠 보여 줌

지금도 실패 중 · 이미 풀림 ·
멈춤 · 알림 없음

못 읽은 프로파일은
0건이 아니라 "수집 실패"

2

비밀값 없이 점검

자격증명은 이름 · 위치 ·
쓰는 곳만 표시
호출 관계는 근거 줄과 함께

토큰 교체 전에 멈춤 스킵과
정기 업무를 미리 찾음

3

변경 경로는 하나

읽기 전용 수집 + 공식 API
모델 · 음성 인식 · OCR은
조직 안에서 처리

예외는 마켓 패키지
설치 · 삭제 두 가지



도입했을 때 플랫폼 쪽 변화

플랫폼의 플러그인 · 설정 · 버전이 바뀌지 않음

PART 07

AAS 도입 판단과 파일럿 4단계

앞서는 항목과 부족한 항목 · 첫 유즈케이스 선정 · 역할별 준비

의사결정권자 관점

KEY INSIGHT

강점은 사람이 보지 않는 동안의 실행을 드러내는 쪽에 몰려 있음 —

부족한 항목이 첫 유즈케이스에 걸리는지 먼저 확인해야 도입 범위를 정할 수 있음

앞서는 항목 6

정기 업무 건강 감시

관측

실행 근거가 붙은 호출 관계 그림

관측

값 없는 자격증명 점검

관측

쓰던 플랫폼 위에 없는 방식

만들기와 지켜보기가 한 화면

업무 에이전트 카탈로그 동봉

부족한 항목 5

→ 대응

두 번째 플랫폼 연결 없음

→ 로드맵 3

마켓 결제 없음

→ 로드맵 2

스크립트 스킬 콘솔 편집 불가

→ 스크립트는 IT, 스킬 문서는 부서 담당이 맡음

비용 자동 정지 · 부서별 할당 없음

→ LiteLLM 기별 예산 한도로 보완

그룹 · 부서 권한 미흡

→ 부서별 에이전트 소유자 지정

앞섬은 "다른 제품에 없음"이 아니라 "공식 자료에서 전면에 내세운 곳을 확인하지 못함" — 실제 화면으로 비교 필요

KEY INSIGHT

명함 인식과 공문 판독은 결과 확인이 쉽고 사람 확인이 이미 절차에 있음 —
우리가 먼저 업무 하나를 골라야 비용 · 가치 · 위험을 셀 수 있음

후보 업무	반복량과 시간대 병목	결과 확인 용이성	사람 확인 단계	연결 시스템 수 적을수록 좋음	외부 반출 없음
영업 명함 인식	○	○	○	△ 3곳	○
경영 화자 구분 회의록	○	△ 참석자 확인	○	△ 3곳 드라이브 · 위키 · 채팅	○
공공 공문 판독 · 서식 채우기	○	○	○	○ 1곳	○
IT 인프라 정기 점검 보고	○	○	△	○ 1곳	○



선택 규칙

○가 가장 많은 후보 가운데 연결 시스템 수가 가장 적은 하나 → 나머지는 확산 목록

KEY INSIGHT

넘어가는 조건을 미리 정해 두면 언제 넓히고 언제 멈출지가 분명해짐 —
중단 사유인 불분명한 가치와 위험 통제 부족을 단계마다 걸러 냄

① 첫 유즈케이스 확정

하는 일 · 산출물
선정 매트릭스
사람 확인 단계
성공 판정 기준

넘어가는 조건

부서장과 IT · 보안 담당이
범위에 합의

② 조직 안 설치와 연결

하는 일 · 산출물
설치 구성 기록
OIDC 연동
연결 프로파일

넘어가는 조건

조직 안 모델로 실행되고
결과가 연결 시스템에 기록됨

③ 지켜보기

하는 일 · 산출물
Cron 헬스체크 · 자격증명 ·
알림 대상 정기 점검

넘어가는 조건

성공 판정 기준 충족
알림이 안 가는 작업 0개
수집 실패가 남으면 미충족

④ 사내 마켓 확산

하는 일 · 산출물
판정을 통과한 스킬을
패키지로 배포

넘어가는 조건

설치 부서에서도
③ 기준을 다시 충족

⑤ 단계 뒤 판단

계속

성공 판정 기준 충족

확대

알림 · 만료 0 유지 + 같은 업무 요청 부서

중단 → 다음 후보

오류가 줄지 않거나 확인 시간 > 수작업

끝낸 프로파일은 보관본을 내보낸 뒤 삭제 — 잊힌 정기 업무가 남지 않음

KEY INSIGHT

세 역할 중 하나라도 늦으면 파일럿이 설치만 되거나 보안 검토에서 멈춤 —
우리가 먼저 업무 하나 · 기준 하나 · 책임자 한 명을 정해야 다음 결정의 근거가 생김

 부서 담당자

- 월간 건수와 물리는 시각
- 현재 처리 시간과 판정 방법
- 사람 확인 단계와 확인자
- 기록 시스템, 보안 등급

들고 올 것: 성공 판정 기준 초안

 IT 관리자

- 설치 환경(서버 · 쿠버네티스)과 망 구성
- OIDC 공급자와 참여 그룹
- 연결할 Hermes Agent 설치본
- 조직 안 모델 · STT · OCR
- 연결 시스템 계정

 보안 담당

- 업무 정보 등급(C · S · O)
- 외부 호스트 목록과 호출 관계
- 자격증명 보관 위치와 교체 책임자
- 변경 · 실행 · 승인 기록의
보관 위치와 열람 권한

외부 사업자와 진행할 때는 운영 결과(확인 주기 · 담당 · 제출 형식)를 과업으로 적음

 파일럿 대상 확정 회의 안건

1 첫 유즈케이스 확정

2 사람 확인 단계 · 성공 기준

3 설치 환경과 연결 범위

4 보안 검토 범위와 담당자

5 계속 · 확대 · 중단 책임자

KEY INSIGHT

업무 하나 · 기준 하나 · 책임자 한 명이 정해지면 파일럿을 시작할 수 있음 —
넘어가는 조건이 계속 · 확대 · 중단 판단의 근거가 됨

1

부족한 항목 확인

부족한 다섯 항목이
첫 업무에 걸리는지 확인

두 번째 플랫폼 · 마켓 결제 ·
부서별 비용 할당 등

2

첫 유즈케이스 선정

반복량 · 결과 확인 용이성 ·
연결 시스템 수로 좁힘

명함 · 회의록 · 공문 가운데
하나로 시작

3

넘어가는 조건 지정

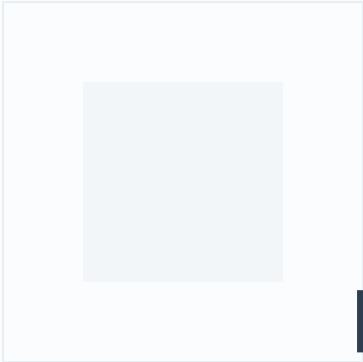
단계별 넘어가는 조건과
계속 · 확대 · 중단
판단 책임자 지정

단계 구분 기준은
넘어가는 조건임



확정 회의 참석

부서 담당자 · IT 관리자 · 보안 담당이 함께 참석



NEXT STEP

MSAP.ai AAS 파일럿의 첫 유즈케이스 결정



명함 · 회의록 · 공문 가운데 하나로 시작하는 4단계 도입

의사결정권자의 다음 행동

MSAP.ai

msap.ai

<https://www.msap.ai/>

hello@msap.ai

02-6953-5427

