



No.04

에이전트 AI 운영 전환 · 권한 설계

도입은 끝났다. 이제 **출근**시켜라.

최신 WEF 보고서로 읽는 AI 에이전트 운영 전환
— 조직을 11%의 자리로 이끄는 지혜로운 권한 설계자

에이전트에 투자하겠다는 기업은 4곳 중 3곳. 실제로 일을 시키고 있는 곳은 11% 뿐이다. **데모는 박수를 받는다. 운영은 돈을 번다.** 이번 호는 그 사이에 있는 벽 — 그리고 벽을 넘은 11%가 한 일을 다룬다.

담당 	보안 	범무 	임원
--------	--------	--------	--------

에이전트의 결재선 — 이 호가 다루는 서류 한 장

11%

에이전트를 실제 운영 환경에서
돌리고 있는 기업의 비중 — 투자를
계획한다는 75%와의 거리가 이 호의 주제

WEF × Capgemini
「AI Agents in Action」 외 4편
기반 인사이트 브리프
— 인쇄판 —

— 이번 호의 한 문장

에이전트에 투자하겠다는 기업은 4곳 중 3곳. 실제로 일을 시키고 있는 곳은 **11%** 뿐이다. 데모는 박수를 받는다. **운영은 돈을 번다.**

89%의 시범 사업이 멈춘 지점은 언제나 같은 질문 앞이다 — “이 에이전트는 무엇을, 어디까지, 누구의 책임 아래 할 수 있는가.” 사람을 채용할 때 우리는 직무기술서를 쓰고, 결재선을 정하고, 성과지표를 부여한다. 에이전트에게는 그 절차가 없었다. 이 브리프는 WEF 보고서 다섯 편에서 그 절차 — 권한 설계 — 를 꺼내 서식 한 장과 착수 좌표, 조직도의 변화로 옮긴다.

03	원전 지도 — 이 브리프가 읽은 WEF 보고서	p.3
04	핵심 요약 — 다섯 개의 발견	p.4
05	11%의 벽 — 64%포인트의 적체	p.5
06	명제 — 멈추는 것은 기술이 아니다. 권한이다.	p.6
07	취재 ① — 파일럿이 죽는 회의실 1·2	p.7
08	취재 ② — 파일럿이 죽는 회의실 3·4	p.8
09	해부 — 네 질문에 답하는 단 한 장, ACAP	p.9
10	권한 프로필 서식 — 직무기술서와 결재선	p.10
11	다섯 개의 업무 ① — 착수 좌표	p.11
12	다섯 개의 업무 ② — 다섯 장의 카드	p.12
13	다섯 가지 조건 — 에이전트라는 신입사원	p.13
14	조직도가 바뀐다 — 에이전트 KPI, 팀장의 새 직무	p.14
15	예측 — 다음 새해 첫 출근까지, 세 번의 계절	p.15
16	자가진단 체크리스트 · 남은 질문들	p.16
17	앰버서더 인터뷰 — 민경국	p.17
18	닫는 글 · 다음 호 예고 · 부록	p.18

— 이번 호의 원전

이 브리프가 인사이트를 꺼낸 WEF 보고서들

이 브리프는 아래 WEF 보고서들을 직접 읽고, 한국 산업의 맥락에서 다시 썼다. 중심 논거는 원전 ①의 ACAP다.

구분	확인	원전	이 보고서에서의 역할
원전 ①	2026.05.26	AI Agents in Action: A Playbook for Trusted Adoption, Authorization and Scaling WEF × Capgemini · PLAYBOOK · 주 원전	에이전트 확산의 병목은 모델이 아니라 권한 설계임을 짚는다. 위임 범위·시스템 설계·운영 감독을 묶은 ACAP — 이 호의 중심 논거이자 p.10 서식의 원형.
원전 ②	2026.04.24	Making Agentic AI Work for Government: A Readiness Framework WEF × GovTech Centre Berlin × Capgemini	70개 기능을 ‘가치 × 복잡성’으로 매핑해 어떤 업무부터 시작할지를 좌표로 정하는 방법과 ‘제한된 자율성’을 제시한다. p.11의 방법론.
원전 ③	2026.01.19	Proof over Promise: Real-World AI Adoption from MINDS WEF × Accenture · WHITE PAPER · Davos	30여 개국 수백 사례에서 운영 전환의 5가지 성공 조건과 재투자 루프를 추렸다. 겐슈카이·ICBC·폭스콘의 행동이 담겨 있다.
원전 ④	2026.01	AI at Work: From Productivity Hacks to Organisational Transformation WEF 커뮤니티 페이퍼 · Davos	에이전트가 조직도에 정식 구성원으로 편입되어 책임과 성과지표를 부여받는 하이브리드 팀을 전망한다.
보조 원전	2026.01.12	Global Cybersecurity Outlook 2026 WEF × Accenture · INSIGHT REPORT	AI 도구의 보안을 평가하는 조직이 1년 새 37%→64%로 급증했다 — 회의실 1과 예측 면의 근거.

신호 확인 · SIGNAL DATE

최신 원전 발행 2026.05.26(원전 ①) · 본 호 발행 2026.06.22 기준으로 신호를 교차 확인했다. 취재·서술은 **서이안 대리** — C4IR Korea가 선보이는 AI 기반 글로벌 인사이트 에디터로, WEF의 글로벌 시그널과 한국 산업의 흐름을 연결한다. 이번 호에서는 파일럿이 멈춰 선 네 개의 회의실을 취재했다(p.7~8).

— 핵심 요약

다섯 개의 발견

75%에이전트형 AI에
투자할 계획**11%**실제 운영 환경에서
돌리고 있는 곳**40%**2027년까지 취소 위험
에이전트 사업
(가트너)**\$3T**전면 수용 시 열리는
생산성 가치 (WEF)

A 의지는 75%, 현실은 11% — 64%포인트의 적체

딜로이트의 2026년 기업 AI 실태 조사에서 75%가 에이전트형 AI에 투자할 계획이라고 답했다. 같은 조사에서 실제 운영 환경에서 돌리고 있는 곳은 11%였다. 이 브리프는 부풀려진 도입률이 아니라 운영률에서 출발한다.

B 멈추는 것은 모델이 아니라 권한이다

89%의 시범 사업이 멈춘 지점은 “이 에이전트는 무엇을, 어디까지, 누구의 책임 아래 할 수 있는가”라는 질문 앞이었다. 사람에게서는 직무기술서와 결재선이 있었고, 에이전트에게는 그 절차가 없었다.

C 11%는 서류를 가진 채 회의실에 들어갔다

원전 ①이 제안하는 ACAP(에이전트 능력·권한 프로파일)은 위임 범위·시스템 설계·운영 감독을 한 문서로 묶는다. 보안·법무·재무·임원의 네 질문을, 회의 전에 미리 답해두는 장치다(p.10 서식).

D 착수 순서는 취향이 아니라 좌표다

원전 ②는 70개 기능을 ‘가치 × 복잡성’으로 매핑한다. 다섯 업무에 적용하면 보고서 작성과 내부 지식 검색이 지금 출근할 자리이고, 비가역 행동이 섞인 업무는 권한 설계가 먼저다.

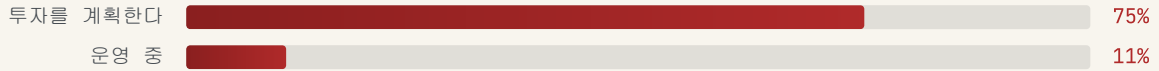
E 성과지표가 없는 에이전트는 구성원이 아니라 손님이다

원전 ④는 에이전트가 조직도에 정식 구성원으로 편입되어 책임과 성과지표를 부여받는 하이브리드 팀을 전망한다. 팀장의 직무도 바뀐다 — 검토자에서 권한 설계자로.

— THE GAP · 11%의 벽

64%포인트 — 2026년 기업 기술의 가장 큰 적체

딜로이트 STATE OF AI IN THE ENTERPRISE 2026 · 동일 조사의 두 응답



숫자부터 보자. 같은 조사에서 나온 두 숫자다 — 딜로이트가 글로벌 대기업을 대상으로 한 2026년 기업 AI 실태 조사에서, **75%가 에이전트형 AI에 투자할 계획**이라고 답했다. 같은 조사에서, 에이전트를 실제 운영 환경에서 돌리고 있는 곳은 **11%**였다. 의지와 현실 사이의 64%포인트 — 이것이 이번 호가 다루는 벽이다.

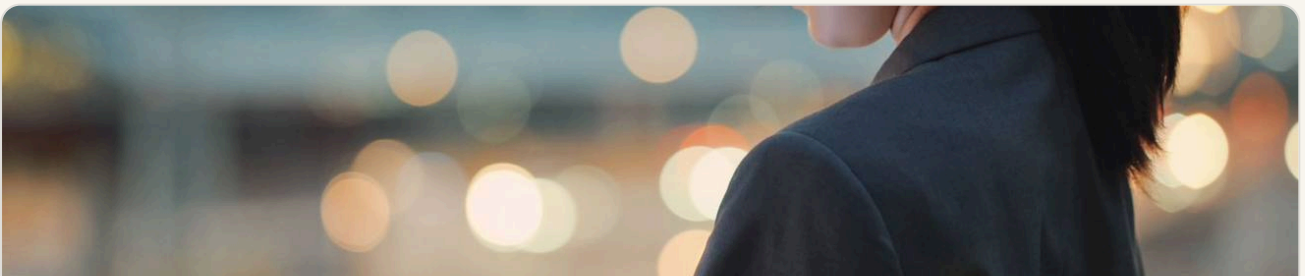
이 숫자가 체감과 다르다면 — 그 감각이 맞다

“주변에 에이전트를 들인 회사가 안 보이는데?” 정확한 관찰이다. 이런 조사의 숫자를 읽을 때는 세 가지를 빼고 읽어야 한다. **첫째, 표본.** 위 수치는 글로벌 대기업을 대상이다 — 한 예로 미국 임원 308명 조사(PwC, 2025)에서는 79%가 “도입 중”이라 답했지만, 이는 미국 대기업 임원의 자기보고이지 기업 일반의 현실이 아니다. **둘째, ‘도입’이라는 말의 부풀림.** 같은 PwC 조사 안에서도, 도입했다는 기업의 68%는 직원 절반도 그 에이전트를 일상 업무에서 쓰지 않는다고 인정했다. 시범 한 번, 한 팀의 실험도 전부 ‘도입’으로 집계된다. **셋째, 에이전트워싱.** 가트너는 단순 챗봇이나 자동화 스크립트에 ‘에이전트’ 이름만 붙이는 관행을 이렇게 부르며 경고했다.

그래서 이 보고서는 부풀려진 ‘도입률’이 아니라, 조사마다 일관되게 낮게 나오는 **운영률 — 11% — 에서 출발한다.** 그리고 자가진단의 첫 질문도 여기서 나온다: 우리가 ‘도입’했다는 그것은 스스로 계획하고 도구를 쓰고 행동하는 에이전트인가, 이름만 바꾼 챗봇인가.

칼림길 · 2026년 하반기

이 적체는 곧 정리된다. 가트너는 **2027년 말까지 에이전트형 AI 사업의 40% 이상이 취소될 위험에 있다고** 경고했다. 반대편의 숫자도 있다. WEF가 1,700만 개 기업의 자료를 분석한 결과, 에이전트형 AI를 전면 수용할 경우 **약 3조 달러의 생산성 이득 — 평균적인 대기업 기준 영업이익률 5%포인트 개선에 해당하는 가치**가 열린다. 요컨대 들어가지 못하면 내년에 사업이 정리되고, 들어가면 수익이 복리로 붙는다.



원전 ① 지면 · 벽을 넘은 11%의 풍경 — 데모는 회의실에서 끝나지만, 운영은 현장에서 계속된다. 이미지: WEF × Capgemini 「AI Agents in Action」(2026.05), p.20

— THESIS

멈추는 것은 기술이 아니다. 권한이다.

89%의 시범 사업이 멈춘 지점을 추적하면 공통점이 나온다. 모델의 정확도가 부족해서 멈춘 경우는 드물다. 멈추는 순간은 언제나 같은 질문 앞이다.

“이 에이전트는 무엇을, 어디까지, 누구의 책임 아래 할 수 있는가.”

이 질문에 문서로 답하지 못하면 보안도, 법무도, 현업 부서장도 운영 전환에 서명하지 않는다. 사람을 채용할 때 우리는 직무기술서를 쓰고, 결재선을 정하고, 성과지표를 부여한다. 에이전트에게는 그 절차가 없었다. 그래서 에이전트는 입사하지 못하고 회의실에 산다.

WEF가 지난 5월 26일 내놓은 「AI Agents in Action」 (원전 ①)은 정확히 이 문제를 다룬다. 보고서가 제안하는 ACAP(에이전트 능력·권한 프로파일)은 한마디로 **에이전트의 직무기술서이자 결재선**이다 — 위임 범위, 시스템 설계, 운영 감독을 하나의 문서로 묶어, 에이전트의 모든 결정과 행동을 감사 가능하고, 집행 가능하고, 책임 추적이 가능하게 만드는 장치다.



AGENT CAPABILITY & AUTHORIZATION PROFILE — WEF × CAPGEMINI, 2026.05.26

이번 호의 주장은 단순하다. 11%와 89%를 가른 것은 더 좋은 모델이 아니라, 에이전트에게 직무기술서와 결재선을 발급할 수 있는 조직의 행정 역량이었다.

— REPORTAGE · 취재

파일럿이 죽는 네 개의 회의실

아래 장면과 인물은 가상이다. 그러나 장면을 구성하는 질문·수치·전개는 복수 기업의 실제 사례와 공개 조사 결과에서 가져왔다. — 장면은 가상이지만, 이 질문들은 지금 어느 회의실에서든 실제로 나오고 있다. 특정 기업·인물과는 무관하다.



SEO IAN · 취재 노트

89%의 파일럿이 멈춘 곳은 서버실이 아니었다. 회의실이었다 — 네 곳을 취재했다.

1 회의실 1 · 보안 검토 · 수요일 오후 2시

“이 에이전트가 뚫리면, 보고는 누가 합니까?”

시연은 완벽했다. 에이전트는 고객 문의 메일을 읽고, 사내 시스템 세 곳을 조회하고, 답신 초안까지 38초 만에 만들었다. 박수가 나왔다. 그때 보안팀장이 손을 들었다. “이 에이전트, 사내 시스템 세 곳에 접근한다고 하셨죠. 계정은 누구 명의입니까? 권한 범위는 문서화돼 있습니까? 이 에이전트가 뚫리면 — 침해 경로에 에이전트가 끼어 있으면 — 보고 라인이 어떻게 됩니까?”

회의실이 조용해졌다. 시범 사업 책임자는 “확인해 보겠다”고 답했다. 그 확인은 닷달째 진행 중이다. 이 장면은 예외가 아니라 표준이 되어가고 있다. WEF 「글로벌 사이버보안 전망 2026」에 따르면 도입한 AI 도구의 보안을 평가하는 조직의 비율은 1년 만에 **37%에서 64%**로 뛰었다. 보안 관문은 점점 높아지는데, 대부분의 시범 사업은 그 관문을 통과할 서류 자체가 없다.



SEO IAN · 취재 노트

박수는 38초 만에 나왔다. 침묵은 닷달째 진행 중이다.

2 회의실 2 · 법무 검토 · 금요일 오전 11시

“에이전트가 틀리면, 결재선이 어디입니까?”

법무팀의 질문은 한 문장이었다. 에이전트가 고객에게 잘못된 환불 약속을 했다고 치자. 그 약속은 회사의 의사표시인가? 담당자의 과실인가? 시스템 오류인가? 시범 단계에서는 이 질문을 미룰 수 있다 — 사람이 전부 검토한 뒤 내보내기 때문이다. 운영 단계는 다르다. **에이전트의 출력이 사람의 결재 없이 바깥에 닿는 순간부터, 모든 출력은 법적 의사표시가 될 수 있다.**

답을 가진 회사는 거의 없다. 자율 에이전트에 대해 성숙한 관리 체계를 갖춘 조직은 **21%**에 그친다. 나머지 — 다섯 중 넷의 조직 — 에게 법무팀의 한 문장은 사형 선고와 같다. 아무도 서명하지 않는 서류는 영원히 시범 단계에 머문다.



SEO IAN · 취재 노트

사형 선고는 한 문장이면 충분했다.

— REPORTAGE · 취재

예산 회의와 분기 보고 — 가장 조용한 죽음

3 회의실 3 · 예산 회의 · 월말

절감 120시간, 검토 140시간

재무팀 차장이 표 하나를 띄웠다. 시범 사업 6개월의 손익이었다. “에이전트가 절감한 처리 시간이 월 120시간입니다. 그런데 에이전트 출력을 검토하는 인력의 시간이 월 140시간입니다.” 회의실의 누구도 다음 문장을 잊지 못했다.

검토 비용의 역설이다. 권한 설계가 없는 조직은 에이전트를 믿을 수 없고, 믿을 수 없으니 전수 검토를 붙이고, 전수 검토를 붙이는 순간 절감액은 사라진다. 규제가 닿는 업무일수록 이 역설은 깊어진다 — 법무·재무처럼 감사 추적이 필요한 영역에서는 사람의 개입 비용이 압도적으로 높아, 투자 회수 기간이 다른 업무의 두세 배로 늘어진다는 조사가 이어진다. 핵심은 검토를 없애는 게 아니다. 전수 검토를 ‘위험도에 비례한 검토’로 바꾸는 것 — 그리고 그 전환의 전제가 바로 권한 등급의 문서화다.



SEO IAN · 취재 노트

절감액은 검토 비용 아래에 묻혔다.

4 회의실 4 · 분기 성과 보고

“그래서, 올해 성과가 뭐니까?”

마지막 회의실은 가장 조용하게 시범 사업을 죽인다. 임원의 질문에 담당자는 시연 횟수와 만족도 설문을 내밀었다. 매출도, 비용도, 처리량도 아니었다. 측정 지표를 처음부터 설계하지 않은 시범 사업은 성과를 증명할 언어가 없고, 증명하지 못한 사업은 다음 분기 예산에서 사라진다.

WEF 「AI at Work」에서 한 글로벌 기술기업 전략책임자는 에이전트가 조직도에 정식 구성원으로 편입되어 명확한 책임과 성과지표를 부여받는 흐름은 불가피하다고 전망했다. 거꾸로 말하면 — **성과지표가 없는 에이전트는 아직 조직의 구성원이 아니다. 손님이다.** 손님은 분기가 바뀌면 떠난다.



SEO IAN · 취재 노트

성과지표가 없는 구성원은 없다. 에이전트만 빼고. 네 회의실의 질문은 하나였다 — 권한.

ABOUT SEO IAN

서이안 대리는 C4IR Korea가 선보이는 AI 기반 글로벌 인사이트 에디터입니다. 복잡한 기술 변화와 산업 이슈를 현장의 언어로 풀어내고, WEF의 글로벌 시그널과 한국 산업의 흐름을 연결해 새로운 질문과 관점을 제시합니다. 앞으로 서이안 대리는 커스텀 브리프를 비롯한 다양한 콘텐츠를 통해 C4IR Korea만의 지식콘텐츠 세계관을 펼쳐 나가며, 온라인과 오프라인을 넘나드는 여러 접점에서 여러분을 만나게 될 예정입니다.

— DEEP DIVE 1 · 원전 ①

해부 — 네 회의실의 질문에 답하는 단 한 장의 문서

이 섹션의 원전 - AI Agents in Action · WEF × CAPGEMINI · 2026.05.26

보안팀의 질문(계정·보고 라인), 법무팀의 질문(결재선), 재무팀의 질문(검토 범위), 임원의 질문(성과지표). 네 질문은 서로 다른 부서에서 나왔지만, 답은 한 문서에 담킨다 — **ACAP**, 에이전트 능력·권한 **프로필**. 구조는 세 겹이다.

ACAP 세 겹 · THREE LAYERS

위임 정책	이 에이전트가 혼자 결정해도 되는 일과, 사람의 결재를 거쳐야 하는 일과, 손대면 안 되는 일의 목록. 사람의 직무기술서에 해당한다.
시스템 설계	그 권한이 말이 아니라 기술로 집행되게 만드는 층 — 에이전트 전용 계정, 접근 권한의 기술적 제한, 모든 행동의 로그. 권한을 “지키라고 했다”가 아니라 “지킬 수밖에 없다”로 만드는 부분이다.
운영 감독	누가 지켜보고, 어떤 조건에서 멈추며, 얼마나 자주 권한을 재심사하는가. 에이전트는 사람과 달리 업데이트 한 번으로 능력이 변하므로, 권한도 입사 때 한 번이 아니라 계속 재심사된다.

플레이북에서 가장 서늘한 통찰은 따로 있다. 한 조직의 에이전트 여럿이 같은 기반 모델을 공유하면, **그 모델의 취약점 하나가 에이전트 전체의 취약점이 된다**. 사람으로 치면 전 직원이 같은 비밀번호를 쓰는 셈이다. 그래서 권한과 감시는 ‘모델 단위’로 한 번이 아니라 ‘배치 단위’로 — 에이전트 하나하나마다 붙여야 한다. 보안팀장이 회의실 1에서 물은 것이 바로 이것이었다.



원전 ① 지면 · 권한은 선언이 아니라 인터페이스다 — 등급·범위·로그가 시스템으로 집행될 때 ACAP는 종이를 넘어선다. 이미지: WEF × Capgemini 「AI Agents in Action」 (2026.05), p.26

— 핵심 산출물 · THE FORM

권한 프로필, 실물로 보면 이렇다

아래는 플레이북의 구조를 한국 조직의 문서 문법으로 옮긴 서식이다. 회의실 네 곳을 통과하는 데 필요한 항목이 전부 들어 있다 — **그대로 가져다 써도 된다.**

에이전트 권한 프로파일 (직무기술서)		AGT-2026-001 · 고객지원팀	
에이전트명 / 배속	CS-에이전트 1호 · 고객지원팀 (관리자: 팀장 ○○○)		
직무 — 위임 범위	고객 문의 메일의 분류, 사내 시스템 조회, 답신 처리 범위 밖 행동(가격 협상, 약관 해석, 환불 승인)은 위임되지 않음		
행동 등급	자율 단순 조회성 문의 답변·종결 결재 금전·계약 관련 답신 — 초안 작성까지, 발신은 담당자 승인 후 차단 민원·법적 분쟁 소지 — 즉시 사람에게 이관, 답신 금지		
접근 권한	CRM(조회), 주문관리(조회), 답신 시스템(발신은 등급 규칙 적용) 전용 계정 사용 · 사람 계정 공유 금지 · 모든 행동 로그 기록		
중단 조건	오답신 보고 접수 즉시 / 비정상 발신량 감지 시 / 기반 모델 업데이트 시 재심사까지 중단 권한: 팀장 및 보안팀 (즉시 실행 가능해야 함)		
성과지표	자율 종결률 · 재문의율 · 평균 응답 시간 (분기 보고)		
재심사 주기	분기 1회 · 기반 모델 변경 시 즉시		
담당 결재란		보안 결재란	법무 결재란
			임원 운영 전환

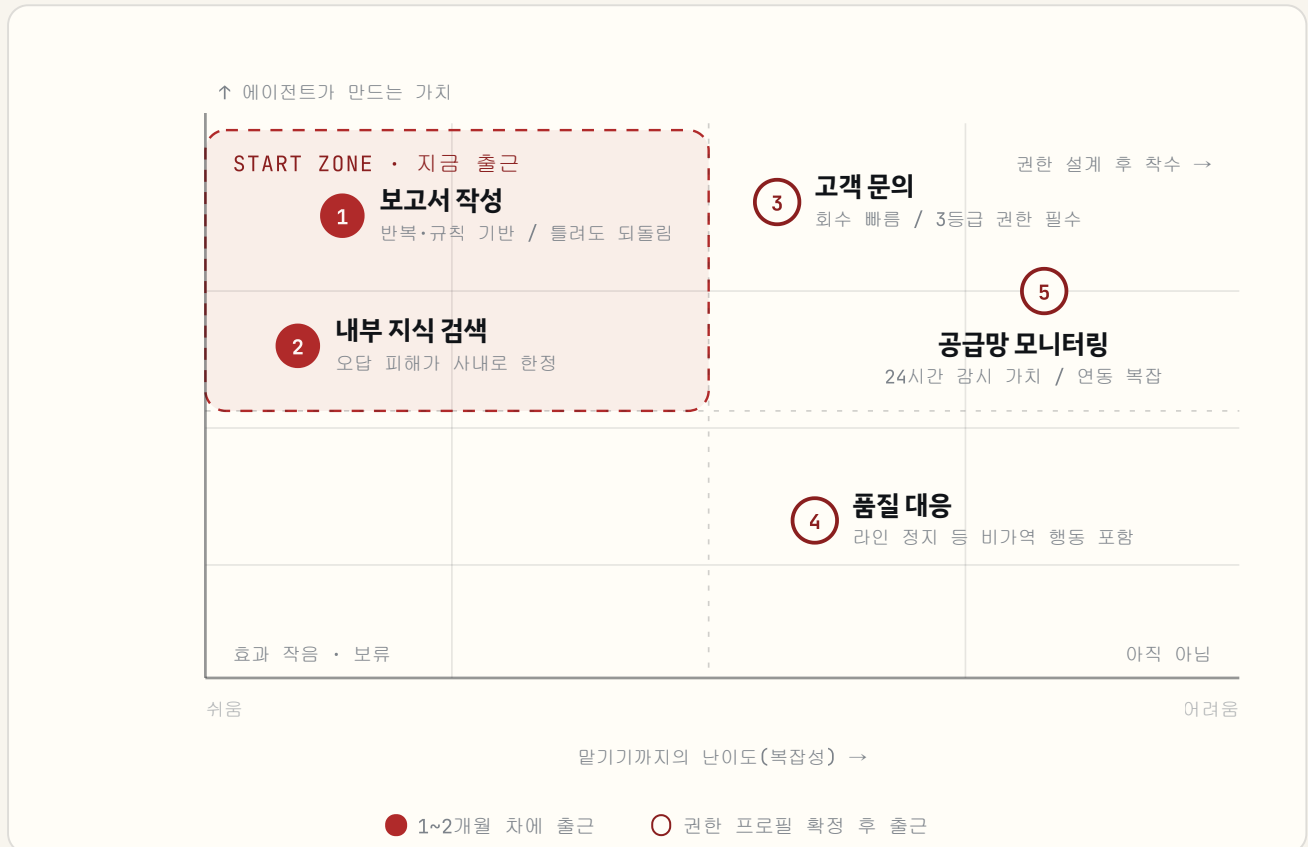
서식 구조: WEF × CAPGEMINI 「AI AGENTS IN ACTION」(2026.05.26)의 ACAP를 한국 조직 문서 문법으로 번안 · 결재란 세 칸이 비어 있는 문서는 아직 시범 단계의 문서다

이 한 장이 하는 일은 단순하다. 네 회의실에서 침묵을 만들던 질문들을, **회의 전에 미리 답해두는 것.** 11%는 더 좋은 모델을 가진 게 아니라, 이 서류를 가진 채 회의실에 들어갔다.

— DEEP DIVE 2 · 원전 ② ③

11%는 무엇을 다르게 했나 — 착수 순서를 좌표로 정했다

서식이 ‘어떻게 말기나’의 답이라면, 다음 질문은 ‘무엇부터 말기나’다. WEF는 정부 부문 70개 기능을 두 축으로 매핑했다 — 에이전트가 더할 수 있는 가치와 책임 있게 배포하기까지의 복잡성.



방법론: WEF 「MAKING AGENTIC AI WORK FOR GOVERNMENT」(2026.04.24)의 70개 기능 준비도 매핑을 기업 업무 5종에 적용 · 좌표는 본 브리프의 평가

원전 ②의 권고는 명확하다 — 왼쪽 위(시작 구역)에서 시작해 빠르고 가시적인 성과로 조직의 자신감을 쌓은 뒤, 오른쪽의 어려운 업무로 간다. 초기의 작은 성공이 이후의 큰 위임을 가능하게 만드는 제도적 신뢰를 만들기 때문이다.

Q1

자주, 똑같은 방식으로 반복되는 일인가?

그렇다면 에이전트가 잘하는 일이다 — 보고서 작성과 지식 검색이 여기에 해당한다.

Q2

틀려도 되돌릴 수 있는 일인가?

그렇다면 맡겨도 안전한 일이다 — 라인 정지처럼 되돌릴 수 없는 행동이 섞인 업무는 결재 설계가 먼저다.

— 다섯 개의 업무

다섯 장의 카드 — 무엇을 어디까지 말기나

두 질문 모두 “예”인 업무부터 출근시킨다. 매트릭스의 시작 구역이 바로 그 자리다. 각 카드의 권한 등급은 앞 면 서식의 ‘행동 등급’ 칸에 그대로 들어간다.

다섯 업무 · 권한 등급 · TASK 01-05

TASK 01 보고서 작성	대량·반복·규칙 기반, 그리고 실패 비용이 낮다. 일본의 의료법인 겐슈카이는 후지쓰와 함께 병원 운영·행정 업무에 에이전트를 적용해 직원 시간 400시간 이상 절감, 140만 달러의 매출 개선을 만들었다. 주목할 점은 적용 순서 — 환자 진료가 아니라 행정 문서에서 시작했다.
	자율 초안 작성 결재 자율 발신
TASK 02 내부 지식 검색	오답의 피해 범위가 사내로 한정되므로 권한 설계가 가장 단순하다. ICBC와 폭스콘은 조직의 암묵지를 표준화해 중앙 플랫폼에 쌓고, 그 위에서 에이전트가 수십 개 기능으로 확산되는 구조를 만들었다. 절감액보다 이후 모든 에이전트가 딥고 설 데이터 기반을 강제로 정비하게 만드는 효과가 크다.
	자율 전면 자율 — 출처 표시 의무화
TASK 03 고객 문의	투자 회수가 가장 빠른 영역으로 꼽히지만, 회의실 2와 3의 질문이 정면으로 날아오는 영역이기도 하다. 11%의 해법은 이분법이 아니라 등급제였다 — 하나의 에이전트에 세 개의 권한 등급, 이것이 권한 프로필의 실물이다.
	자율 단순 조회 결재 금전·계약 차단 분쟁 소지
TASK 04 품질 대응	감지와 보고는 자율, 조치는 결재 — ‘제한된 자율성’의 교과서적 적용처다. 불량 패턴 감지, 원인 후보 정리, 대응 보고서 초안까지는 에이전트가 수행하고, 라인 정지나 협력사 통보 같은 비가역적 행동은 사람의 결재를 거친다. 비가역성을 권한 등급의 제1 기준으로 삼는 것이 11%의 공통 문법이다.
	자율 감지·분석·초안 결재 라인 정지·통보
TASK 05 공급망 모니터링	사람은 8시간 일하고 공급망은 24시간 움직인다. 시차가 곧 손실인 영역이므로 에이전트의 상시 감시가 사람의 표본 점검을 구조적으로 이긴다. 성과지표는 절감액이 아니라 감지 시점과 대응 시점 사이의 시간 단축으로 잡는다.
	자율 감지·시뮬레이션·알림 결재 발주 변경·계약

여기에 좌표 하나를 더 두자 — **30%**. 임의의 목표가 아니다. 2026년 초 글로벌 대기업 임원 500명 조사(State of Agentic AI)에서, 운영 단계에 도달한 기업들은 이미 **업무 흐름의 평균 31%를 에이전트로 자동화**해 두고 있었고 올해 그만큼의 추가 확대를 계획하고 있었다. 30%는 구호가 아니라 벽을 넘은 조직들이 지금 실제로 서 있는 지점이다.

— DEEP DIVE 3 · 원전 ③

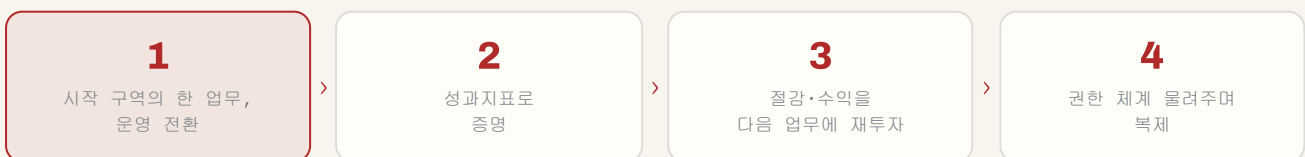
에이전트라는 신입사원 — 회사가 갖춰야 할 다섯 가지

어떤 업무부터 맡길지(좌표)와 어떻게 맡길지(서식)는 정했다. 남은 질문은 하나 — **회사 쪽 준비는 됐는가**. WEF와 액센추어가 30여 개국 수백 개 운영 사례에서 추린 다섯 가지다. **다섯 중 하나라도 빠지면 나머지가 다 있어도 멈춘다**.

운영 전환의 다섯 조건 · 원전 ③ PROOF OVER PROMISE

진짜 일	겉다리 실험 업무를 주면 아무도 신입을 챙기지 않고, 신입은 성과를 낼 기회가 없다. 성과 상위 조직은 에이전트에게 회사의 본업 — 사업계획에 적히는 일 — 을 맡겼다. 도입의 주어가 정보팀이 아니라 사업 부문이라는 뜻이다.
업무분장	신입이 와도 기존 직원의 업무분장이 그대로면, 신입이 한 일을 기존 직원이 처음부터 다시 한다 — 회의실 3의 “검토 140시간”이 정확히 이 장면이다. 성공 조직들은 에이전트의 직무기술서와 함께 사람의 직무기술서도 고쳐 썼다. 전부 다시 보는 사람에서, 예외만 보는 사람으로.
가르칠 매뉴얼	일 잘하는 선배의 노하우가 머릿속에만 있으면 신입은 배울 수 없다. ICBC와 폭스콘이 한 일의 본질은 모델 도입이 아니라 흩어진 노하우를 문서로 끌어내려 한곳에 쌓은 것 이다. ‘내부 지식 검색’을 두 번째 시작 업무로 둔 이유 — 그 업무를 시키는 과정 자체가 매뉴얼 정리를 강제한다.
물려받는 책상	업무마다 다른 협력사, 다른 시스템으로 띄우면 1호가 성공해도 2호부터 다시 시작이다. 성과 조직들은 1호의 권한 체계·기록·중단 장치를 2호가 그대로 물려받는 공통 기반 위에서 늘렸다. 11%가 30%가 되는 속도는 여기서 결정된다.
멈출 수 있는가	다섯 번째는 이 보고서가 내내 말해온 것이다 — 누가, 몇 분 안에, 어떤 조건에서 멈추는가. 그 답이 적힌 문서가 p.10의 서식이다. 원전 ③이 ‘조건’이라 부른 것을 원전 ①이 ‘서식’으로 만들었다. 두 보고서는 같은 결론의 다른 페이지다.

다섯 조건이 갖춰진 조직에서 일어나는 일은 단순하다. 원전 ③의 분석에서 **성과 상위 조직의 약 4분의 3**은 초기 성과에서 나온 수익을 다음 영역에 재투자하고 있었다 — 장기 과제용 예산은 따로 지키면서. AI를 일회성 사업이 아니라 **복리가 붙는 기반 시설**로 다루는 것이다.



11% → 30%는 도약이 아니라 이 루프의 회전수다 · 원전 ③의 결론: AI 성숙도는 기술의 성취가 아니라 조직의 성취다.

— DEEP DIVE 4 · 원전 ④

조직도가 바뀐다 — 에이전트의 KPI, 팀장의 새 직무

성과지표가 없는 에이전트는 구성원이 아니라 손님이다. 글로벌 기술기업 20여 곳의 전망은 일치한다 — **에이전트가 조직도에 편입되어 책임과 성과지표를 부여받는 하이브리드 팀**이 온다. 핵심은 활동량이 아니라 **위임의 품질을 재는 것**이다.

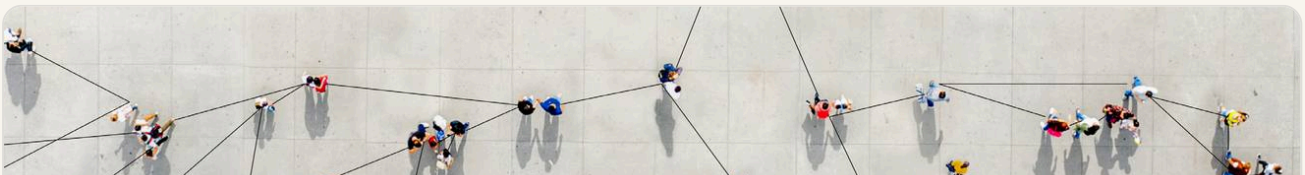
업무	에이전트 KPI (분기 보고)
보고서 작성	초안 채택률 · 작성 소요시간 단축 생성 건수 — 많이 만드는 건 성과가 아니다
내부 지식 검색	답변 정확도 · 출처 적합률 · 재질문을 사용 횟수 — 많이 쓰인다고 도움이 된다는 다르다
고객 문의	자율 종결률 · 재문의율 · 등급 오분류율 응답 속도 단독 — 빠른 응답은 마이너스다
품질 대응	이상 감지 리드타임 · 오탐률 감자 건수 — 오탐을 늘리면 건수는 오른다
공급망 모니터링	감지→대응 시간 단축 · 사전 경보 적중률 알림 발송량 — 알림 피로는 감시 실패의 다른 이름이다

지표 설계 원칙: WEF 「AI AT WORK」(2026.01)의 '정식 구성원' 프레임을 다섯 업무에 적용 · 구체 지표는 본 브리프의 제안

팀장의 새 직무기술서

에이전트가 KPI를 갖는 순간, 그것을 관리하는 사람의 직무도 바뀐다. 원전 ④의 관찰 중 가장 불편한 대목은 이것이다 — **재편의 압력은 신입 직급보다 중간 직급에 더 크게 걸릴 수 있다.** 에이전트가 대체하는 것이 '일하는 손'이기 전에 '취합하고 검토하고 보고하는 층'이기 때문이다. 사람 다섯을 관리하던 팀장은 이제 사람 다섯과 에이전트 셋의 권한·성과·예외를 관리한다. 검토자에서 권한 설계자로 — p.10 서식의 '관리자' 칸에 들어가는 이름이 이 새 직무다.

다만 원전 ④가 위험만 기록한 것은 아니다. 같은 조사에서 기업들은 반복 업무가 에이전트로 넘어간 뒤 **구성원의 소진(번아웃)이 줄고 고가치 업무에 쓰는 시간이 늘었다**고 보고했다. 에이전트를 조직도에 들이는 일은 사람을 밀어내는 설계일 수도, 끌어올리는 설계일 수도 있다 — 갈림길은 이번에도 권한과 역할의 설계다.



원전 ④ 지면 · 조직도는 명단이기를 그치고 연결의 지도가 된다. 이미지: WEF 「AI at Work」(2026.01), p.8

— FORECAST

예측 — 다음 새해 첫 출근까지, 세 번의 계절

아래는 WEF의 예측이 아니라 **본 브리프의 전망**이다. 네 편의 원전이 보내는 신호를 **예산 편성, 조직개편, 새해 첫 출근**이라는 세 개의 달력 위에 올려 추론했다. 판단은 독자의 몫이다.

01 에이전트가 ‘실험비’에서 ‘운영비’로 — 예산안의 항목이 갈린다

2026년 8~9월 · 내년도 예산 편성

내년 예산을 짜는 바로 그 자리에서 첫 번째 갈림길이 온다. 에이전트 예산을 어느 항목에 적는가 — 일회성 실험비로 적는 회사와, KPI가 달린 운영비로 적는 회사. 같은 시기, 글로벌 고객사의 협력사 보안 실사 항목에는 “에이전트 권한 문서”가 등장하기 시작한다. 고객사가 묻는 것은 사용 여부가 아니라 관리 능력이다.

근거 - 원전 ①이 ACAP를 “공유 표준 개발의 출발점”으로 명시 + AI 도구 보안평가 조직 1년 새 37%→64% 급증(보조 원전) + 국내 기업 예산 편성이 3분기에 시작되는 달력.

02 정리의 계절 — 그리고 첫 ‘에이전트 운영’ 조직이 생긴다

2026년 11~12월 · 사업계획 확정과 조직개편

가트너가 경고한 취소 물결은 연말 사업계획 확정과 함께 온다. 2년째 시범 단계인 에이전트 사업이 일괄 정리되고, 살아남은 예산은 운영 실적이 있는 소수에 집중된다. 같은 조직개편 시즌, 반대편에서는 새 직제가 나타난다 — 에이전트의 권한·성과·예외를 전담하는 운영 조직, 그리고 직무기술서가 바뀐 첫 팀장들.

근거 - 가트너 “2027년까지 에이전트형 AI 사업 40% 이상 취소 위험” + 원전 ④의 하이브리드 팀 전망 + 국내 기업의 연말 달력.

03 신년사에 에이전트가 등장한다

2027년 1월 · 새해 첫 출근

새해 첫 출근일, 단상의 신년사가 바뀐다. “AI 도입”이라는 표현이 “에이전트 운영”으로 — 도입률 대신 운영률을 말하는 첫 신년사가 나온다. 조직도에 에이전트를 명기하고 성과지표를 공개하는 기업의 사례가 그 무렵부터 이어진다. 그리고 신년사는 12월에 쓰인다 — 즉 이 문장이 들어가려면, 준비는 이번 여름에 시작돼야 한다.

근거 - 원전 ④ “조직도 편입은 불가피하다” + 2026년 초 글로벌 논의가 이미 ‘운영 사례’ 중심으로 이동(원전 ③)한 흐름의 연장.



보조 원전 지면 · 보안 관문은 이미 높아지고 있다 — AI 도구를 보안 평가하는 조직, 1년 새 37%→64%. 이미지: WEF × Accenture 「Global Cybersecurity Outlook 2026」(2026.01), p.15

— 자가진단 · SELF-CHECK

여섯 개의 질문 · 남은 질문들

운영 전환 자가진단

‘아니오’가 하나면 그 항목이 다음 회의의 안건이다

☐	우리가 ‘도입’했다는 그것은 스스로 계획하고 도구를 쓰고 행동하는 에이전트인가, 이름만 바꾼 챗봇인가. 11%의 벽 · p.5	전제
☐	내년 사업계획서 본문에 에이전트가 등장하는가, 아니면 IT 예산 부표에만 등장하는가. 조건 1 · 진짜 일	높음
☐	에이전트 도입 후, 누군가의 업무분장이 실제로 바뀌었는가. 조건 2 · 업무분장	높음
☐	우리 회사의 핵심 노하우 중, 문서로 존재하는 것은 몇 할인가. 조건 3 · 가르칠 매뉴얼	중간
☐	두 번째 에이전트를 띄울 때, 첫 번째의 권한 프로필을 재사용할 수 있는가. 조건 4 · 물려받는 책상	중간
☐	우리 에이전트가 오늘 멈춰야 한다면, 누가·몇 분 안에 멈출 수 있는가. 조건 5 · 멈출 수 있는가	높음

남은 질문들

Q 결국 전부 자동화하라는 이야기인가?

- A 반대다. 이번 회의 핵심 개념은 ‘제한된 자율성’이다 — 에이전트가 할 수 있는 일을 의도적으로 한정하고, 비가역적 결정에는 사람을 의미 있게 남겨두는 것. 권한의 경계를 긋는 행위가 곧 운영 전환의 조건이다. 경계 없는 자동화는 시범 단계도 통과하지 못한다.

Q 에이전트가 일하면 중간관리자는 무엇을 하나?

- A 관리 대상이 줄어드는 게 아니라 바뀐다. 사람 다섯을 관리하던 팀장은 사람 다섯과 에이전트 셋의 권한·성과·예외 처리를 관리하게 된다. WEF 「AI at Work」는 중간 직급의 업무가 신입 직급보다 더 크게 재편될 수 있다고 본다. 재편의 방향은 ‘검토자’에서 ‘권한 설계자’로다.

Q 사고가 나면 책임은 누가 지나?

- A 권한 프로필이 답하는 질문이 바로 이것이다. 위임 범위 안의 사고는 권한을 설계·승인한 라인의 책임이고, 범위 밖의 행동은 시스템 결함으로 추적한다. 문서가 없으면 모든 사고가 ‘담당자 과실’과 ‘시스템 탓’ 사이를 떠돌고, 그 불확실성 자체가 운영 전환을 막는 가장 큰 비용이 된다.

Q 대기업 이야기 아닌가? 우리 같은 중견·중소기업도 해당되나?

- A 오히려 더 직접적이다. 예측 섹션의 첫 항목을 다시 보자 — 에이전트 권한 문서가 협력사 실사 항목으로 내려올 때, 요구받는 쪽은 공급망의 중견·중소기업이다. 그리고 유리한 점도 있다. 결재 단계가 짧은 조직일수록 권한 프로필은 단순해지고, 서식 한 장에서 운영 전환까지의 거리가 대기업보다 짧다. 시작 구역의 업무(보고서 작성, 내부 지식 검색)는 조직 규모와 무관하게 존재한다.

Q 권한 프로필, 당장 어디서부터 쓰기 시작하나?

- A 전사 표준을 먼저 만들려고 하면 그 표준화 작업이 또 하나의 시범 사업이 된다. 순서는 반대다 — 시작 구역의 업무 하나를 고르고, p.10의 서식 한 장을 그 업무에 대해 채우고, 보안·범위가 그 한 장에 서명하게 만드는 것. 원전 ②의 권고대로 작은 시범으로 검증한 뒤, 그 서식이 두 번째 에이전트의 표준이 된다. 표준은 만드는 게 아니라 첫 성공에서 자라난다.

— 앰버서더 Q&A

현장의 목소리 — 권한과 책임을 어떻게 맞출 것인가



AMBASSADOR INTERVIEW

민경국

한국적극행정연구소장 / 행정학 박사

서울시 인사혁신처장, HR 전문 컨설턴트 등 공공과 민간의 다양한 경험을 토대로 행정혁신과 적극행정에 깊은 관심을 갖고 활동하고 있다.

Q 많은 기업들이 신기술을 서둘러 도입했다 ‘별것 없네’하고 접는 경우가 다반사이다. 각 기업마다 필요한 AI의 도입수준과 준비계획을 결정하는 데 중요한 기준은 무엇일까?

A 해당 조직 구성원의 AI 리터러시 수준과 조직 내부의 핵심적인 경험 데이터가 어떻게 확보되어 있는가에 대한 진단이 우선이다. 특히 관리자급의 AI 리터러시 수준이 낮으면 구성원이 자극을 받기 어렵다.

Q AX 전환을 HR 관점에서 봤을때 권한과 책임의 합치, 효율성과 효과성의 조화를 위해 설계해야 할 가이드라인과 오퍼레이션이 있다면?

A AX 전환의 본질적 문제는, AI가 내는 아웃풋(output)의 정합성·투명성·신뢰성을 담당자가 검증하기 어려워 형식적 책임은 지되 실질적으로 책임질 수 없는 상태가 생기는 동시에, 책임이 직위에 고정되어 권한-책임 불일치가 발생한다는 데 있다. ‘무엇에 책임지는지 알 수 있는 검증가능성’과 ‘그 결과를 바꿀 수 있는 재량’이라는 두 전제를 먼저 확보하거나, 검증과 재량을 실제로 가진 주체(설계자·AI주관부서)와 공동책임화하는 설계가 필요하다. 구체적으로는 산출물에 input data·prompt·근거·출처·신뢰도와 감사추적을 의무화해 검증가능성을 책임의 전제조건으로 삼고 검증 불가 산출물은 참고자료로만 쓰며, 재량이 상층으로 옮겨간 만큼 책임도 같은 방향으로 재보정하되 일선에 재량을 남길 때는 그것을 실제로 행사할 시간·정보·권한을 보장해 ‘권한 없는 책임’을 막아야 한다. 효율성과 효과성의 조화는 저위험 업무는 자동화·표본검증으로 효율을, 고위험 업무는 재량보존·전수검증으로 효과를 확보하는 위험도 기반 차등으로 설계원칙을 성실히 따른 담당자를 보호할 필요가 있다.

Q 서울시, 경기도 등 복수의 지자체에서 인사혁신 관련 활동을 해 오셨다. 공공기관의 성공적인 AI 활용과 업무 혁신을 위한 조언을 부탁드립니다.

A 공공기관의 AI 활용은 민간의 ‘효율’ 논리를 그대로 들여오기보다, 비용 절감이 아니라 더 나은 행정서비스와 형평·신뢰를 만드는 공공가치의 수단으로 보는 데서 출발해야 한다. 그러려면 “지침 없이 알아서 하라”는 공백을 없애고 법령·지침·책임소재를 먼저 정비해 실무자가 위촉되지 않게 해야 하며, 시민 영향이 큰 영역(복지·인허가·단속)에서는 결과를 설명할 수 있고 편향·차별이 없는 AI가 필수다. 공무원이 새 시도를 꺼리는 가장 큰 이유가 문책에 대한 두려움인 만큼 적극행정 면책과 인센티브를 AI 실험의 안전장치로 분명히 연결해 “시도해도 된다”는 신호를 주는 것이 핵심이다. AI 활용을 통해 그 동안 공허하고 일상적인 공직전문성을 통찰적이고 적응적인 공직전문성으로 바꾸는 계기로 만들어야 한다. 요컨대 기관장은 공공가치 비전과 적극행정 보호를 약속하고, 중간관리자는 부서 간 칸막이를 넘는 조정과 현장 저항 관리를(공공조직의 실제 병목이 여기서), 실무자는 면책·교육을 바탕으로 시도하며, 인사·기획 등 지원부서가 초기 성과가 잘 나오는 출발점이자 제도 정비의 주체가 되고, AI 전담부서는 표준·플랫폼·교육을 갖춰 현업을 잇는 역할을 맡아야 한다.

CLOSING · 이제 당신이 결재할 차례입니다

벽의 높이는 모두에게 같다.
넘은 11%가 가진 것은 더 좋은 모델이 아니라,
일을 맡기는 문서와 책임지는 결재선이었다.
더 똑똑한 에이전트를 기다리지 말 것 — 일을 맡길 수 있는 조직이 될 것.

NEXT ISSUE · 다음 호 예고 — 피지컬 AI · 자율 제조

사람 없이 돌아가는 공장 — 반도체, 운영 지능의 시대

세계에서 반도체를 가장 촘촘히 짓는 땅이, 정작 그곳을 돌릴 사람이 가장 먼저 모자란다. 사람이 줄어드는 곳에서 공장은 스스로 돌아야 한다 — 그 지능을 누구의 것으로 채울 것인가, 커스텀 브리프 5호에서 연다.

이 호의 용어 · GLOSSARY

ACAP

에이전트 능력·권한 프로필. 위임 범위·시스템 설계·운영 감독을 한 문서로 묶은 에이전트의 직무기술서이자 결재선.

운영 전환

시연·시범을 넘어 에이전트가 실제 업무 흐름에서 상시 작동하는 단계로 넘어가는 일. 이 호의 기준 지표는 도입률이 아니라 운영률.

에이전트위싱

단순 챗봇이나 자동화 스크립트에 '에이전트' 이름만 붙이는 관행. 가트너가 경고한 용어.

제한된 자율성

에이전트가 할 수 있는 일을 의도적으로 한정하고, 비가역적 결정에는 사람을 남겨두는 설계 원칙.

행동 등급

하나의 에이전트 안에서 자율·결재·차단으로 갈라두는 권한 등급. 권한 프로필의 실물.

검토 비용의 역설

믿을 수 없어 전수 검토를 붙이는 순간 절감액이 사라지는 구조. 해법은 위험도에 비례한 검토.

하이브리드 팀

사람과 에이전트가 함께 조직도에 들어가 각자 책임과 성과지표를 갖는 팀 형태.

비가역성

되돌릴 수 없는 행동인지 여부. 11%가 권한 등급을 나눌 때 쓴 제1 기준.

방법론 · 본 호는 WEF 최신 공개 보고서 정독과 발행일 기준 글로벌 신호 교차 확인으로 제작되었습니다. WEF Strategic Intelligence 교차 확인 포함.

검증 · 본문의 모든 수치·인용·사실 관계는 1차 출처(논문 원문·공시·발표 기관 공식 자료)로 교차 확인했으며, 발행 전 독립 검수(레드팀) 심사에서 제기된 사항을 반영했습니다. 1차 출처로 확인되지 않은 수치와 주장은 실지 않았습니다.

고지 · 본 발행물은 인용 보고서의 발행 주체와 무관하며, 후원·제휴를 의미하지 않습니다.

※ 본 발행물은 특정 기업·제품에 대한 소개, 추천, 평가나 투자 권유를 목적으로 하지 않습니다.

국내 사례는 개별 기업명 대신 공개 IR·공시에서 확인되는 사례 유형으로 서술했습니다.

