

# AI 에이전트 시대의 공공AX와 데이터전략

---

AI 센트릭 데이터 — 접근 · 이해 · 상태 · 배치

이승현

# 이승현

(전) 디지털플랫폼정부위원회 인공지능플랫폼혁신국장

(현) 알파카랩 대표

(현) 라이너 AI 에반젤리스트

(현) 국민경제자문회의 AI경제정책자문단 위원

(현) 법무법인 린 공공AX 고문

(현) 한양대 ERICA AI for Humanity and Sustainability 겸임교수

(현) 가천대 스타트업칼리지 겸임교수

## 저 서

— AI 국부론 (2026.3)

— 공공AX (2026.4 공저)

## 최근 기 고

— AI 에이전트 시대의 국가전략 (KISDI, 2026.7)

— 국가 반도체·AI 인프라 투자의 리스크 진단과  
조건부 리밸런싱 전략 (ETRI, 2026.9)

# 오늘의 순서

세 부분 — 에이전트가 첫 고객이 되면 바뀌는 공공AX의 전제와 데이터의 설계 기준

## 1 | 에이전트 시대

사람 기준 제도가 깨지는 지점

챗봇과 에이전트, 9초에서 14시간으로  
빌더의 시대, 왜 AI만 다른가  
토큰 소비의 주체는 이미 에이전트  
루프·그래프, stateless와 stateful

## 2 | 공공AX

첫 고객은 정부 자신의 에이전트

AI 도입 ≠ AX  
4대 병목 — 기술이 아니라 제도  
문제제기자 중심 MVP·성과중심 발주  
세 개의 문 — 파이프·지능·망

## 3 | 데이터전략

AI 센트릭 데이터 — 4개 전환축

- ① 접근: 데이터셋 신청 → 등급 한 키
- ② 이해: readable → understandable
- ③ 상태: stateless → stateful
- ④ 배치: 클라우드 → 로컬+클라우드

1

# 에이전트 시대

사람 기준 제도가 깨지는 지점

# 챗봇과 에이전트

묻고 답하면 끝나는 도구에서, 목표를 받아 스스로 도구를 쓰고 검증하는 주체로



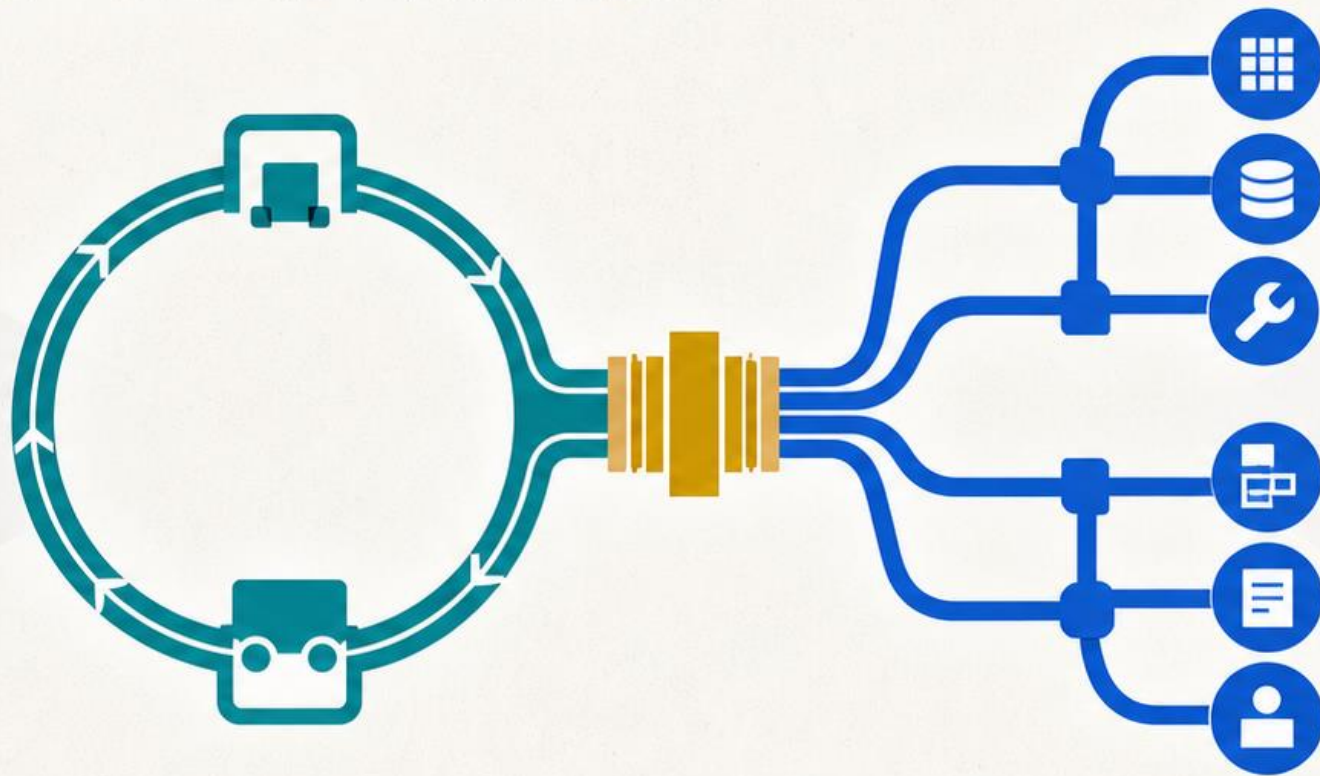
**에이전트 = 도구 사용 · 기억 · 계획 · 실행-검증 루프**

# 하네스 = 루프 엔지니어링 + 그래프 엔지니어링

에이전트를 굴리는 일은 두 가지 설계 — 얼마나 오래 돌리나, 무엇과 무엇을 잇나

루프 엔지니어링 —  
계획 → 실행 → 검증 → 수정의 반복 설계

- 언제 멈추고 언제 사람을 부르나
- 루프가 길수록 호출량과 상태가 커짐



그래프 엔지니어링 —  
도구 · 데이터 · 에이전트의 연결 구조

- 무엇을 어떤 순서로 부르나
- 공공에서는 그래프의 절반이 정부 데이터



## 사람의 역할 = 루프와 그래프의 설계

# 빌더의 시대

기획·구현·배포를 에이전트와 — 직접 만든 넷



## im-not-ai

AI가 쓴 한글 글 분류

GitHub ★4.6K · 글로벌 상위 0.03%

## OneGov

정부 부처 자료 통합검색 원원도우

50개 기관 · 문서 10만 건 이상

## PolicyBlind

정당 가린 정책 카드 → 공감 후 발의자 공개

policyblind.com · 법안 500장

## 국회 기록 MCP

법안 · 표결 · 회의록 · 검토보고서 연결

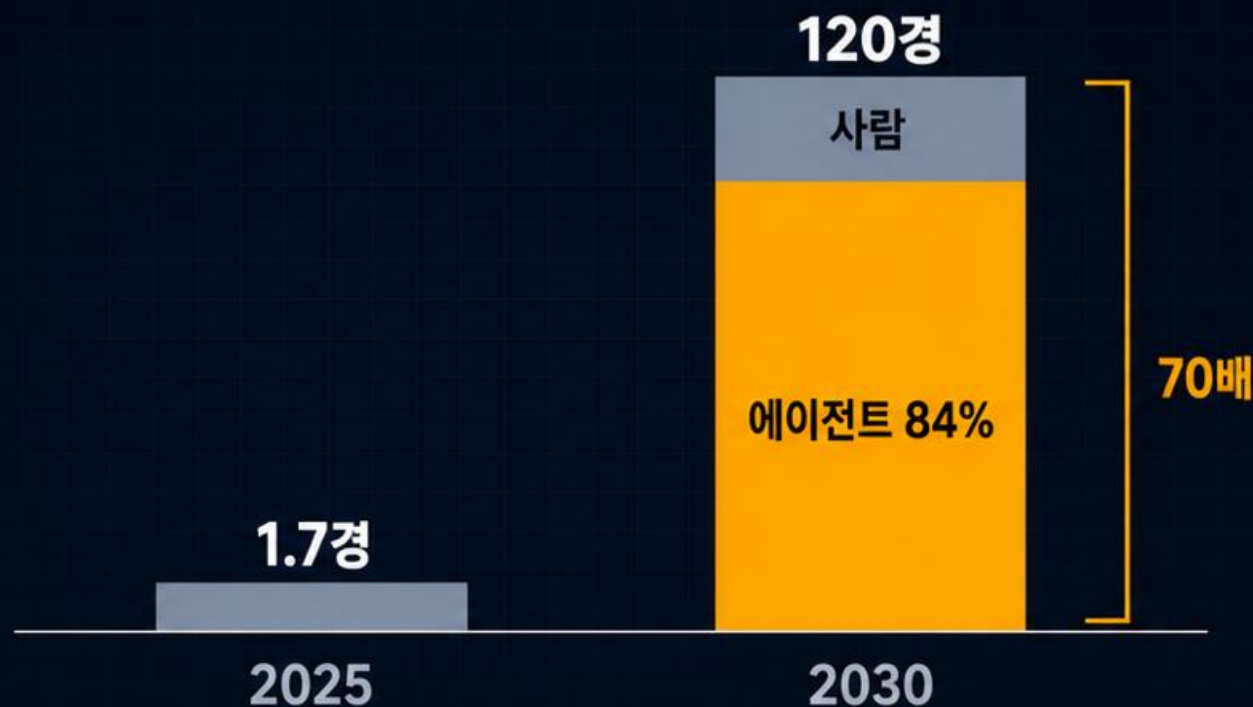
제1대~제22대



# 도구를 쓰는 시대 → 도구를 만드는 시대

# 토큰 소비의 주체, 이미 에이전트

루프 1회 = 수십~수백 호출 → 사람 기준 접근·한도 체계와 구조적 불일치



**14배**

6개월간 에이전트 토큰 증가율 — 사람은 2.8배

**일 7.3조**

에이전트 토큰, 7일 평균 — 사람 사용(1.4조)의 5배

**2026.2.6**

에이전트 토큰이 사람 토큰을 처음 추월한 날

프랑스 data.gouv.fr MCP 서버가 공개 며칠 만에  
트래픽으로 다운된 배경

같은 달, 한국 공공데이터포털의 운영계정 한도는  
여전히 사람 앱 기준 **일 10만 건**



공공데이터포털 운영계정 한도 일 10만 건 = 사람 앱 기준 → 에이전트 몇 개로 소진

# 에이전트와 사람의 다른 데이터 호출

많이 · 빠르게 · 반복적으로 — 사람 기준 제도가 깨지는 세 지점



## 많이

에이전트의 방식 — 루프 1회 = 수십~수백 호출  
사람 기준 제도 — 운영계정 한도 일 10만 건

## 빠르게

에이전트의 방식 — 초 단위로 시도하고 검증  
사람 기준 제도 — 휴대폰 본인인증 · 화면 클릭

## 반복적으로

에이전트의 방식 — 같은 등급 데이터 수십 종을 연달아  
사람 기준 제도 — 데이터셋마다 활용신청 → 승인



사람 기준으로 설계된 접근·한도·신청 제도가 깨지는 지점 — 공공AX의 병목

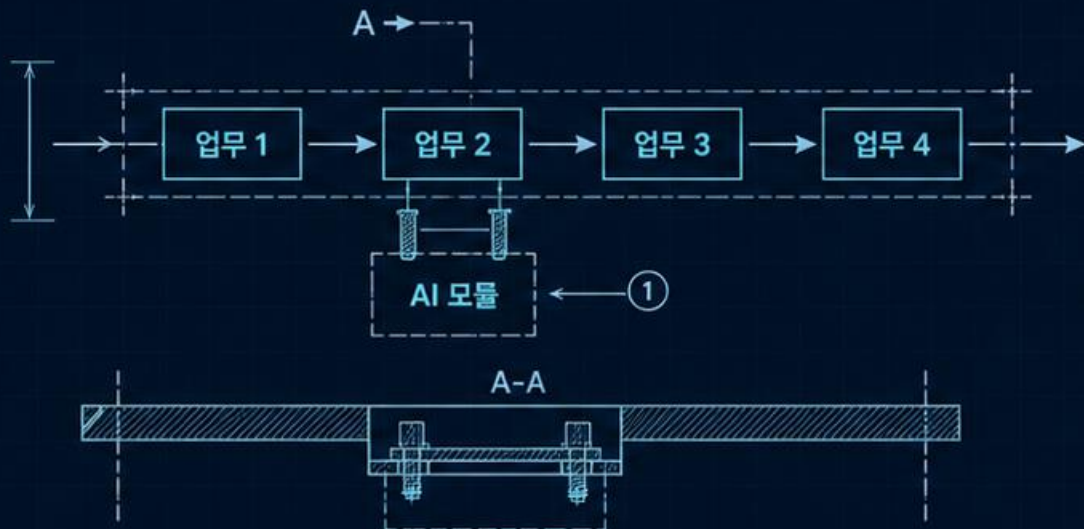
PART 2

# 공공AX

사람 기준 제도가 깨진 자리에서 시작

# AI 도입 ≠ AX

같은 토큰을 태워도 구조가 그대로면 도입, 구조를 다시 짜면 전환

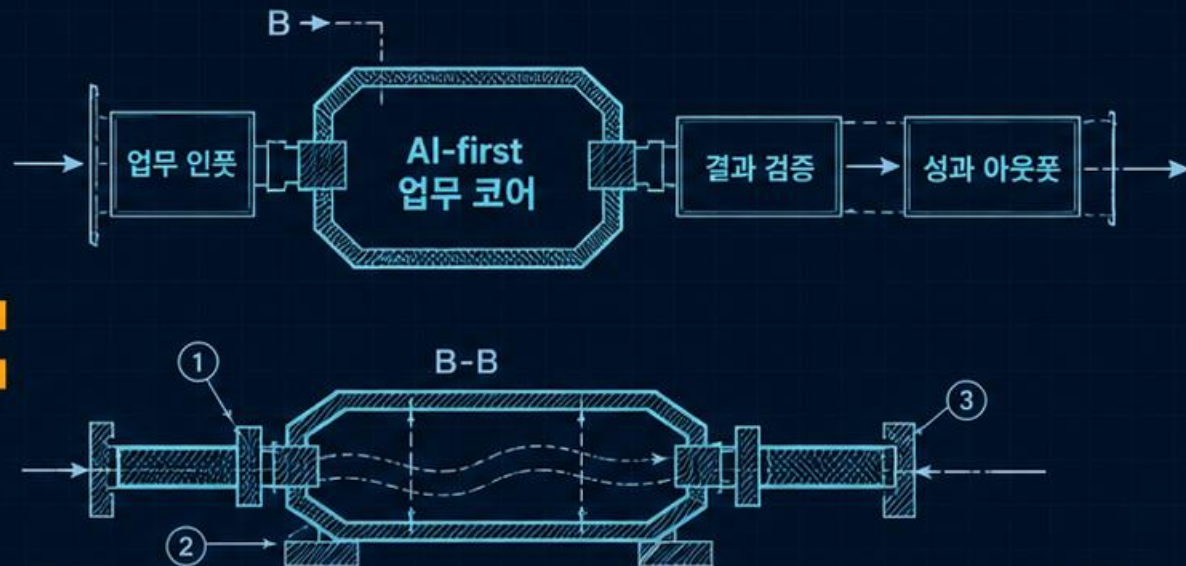


## AI 도입

기존 업무 + AI 부착  
개인 생산성 +10~20%  
무실패 → 무성과  
같은 토큰을 태우고, 구조는 그대로

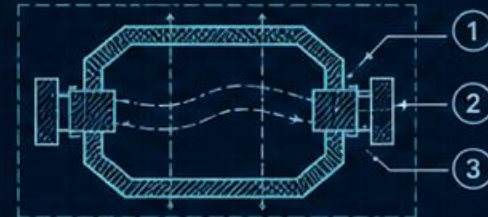


≠



## AX

업무 자체를 AI-first로 재설계  
처리시간 · 비용의 구조 절감  
관행과 충돌 = 리더십의 일  
사례 — 신청주의 → Push 행정



# AX의 전제 = 업무 재설계 — 붙이는 것이 아니라 다시 짜는 것

# 첫 고객: 민간이 아니라 정부 자신의 에이전트

공공데이터 개방(A)과 공공AX(B)가 한 몸인 이유 — B의 에이전트가 사용하는 A의 파이프

**A — 공공데이터 개방 — 포털 · API · 등급표**

**B — 공공AX — 규정 검토 · 사각지대 발굴 에이전트**

**B의 에이전트가 부르는 A의 파이프**

부처 사각지대 발굴 에이전트가 타 부처 데이터를 호출 —  
현재는 행정정보공동이용 승인 + API 건별 신청  
민간 개방 도구이기 전에 정부 내부 에이전트의 파이프

**원키 게이트웨이 = 에이전트 시대의 행정정보공동이용**

부처 간 데이터 호출을 사람의 승인 절차가 아니라 등급과 키로 —  
정부 에이전트가 첫 사용자

**민간 클라우드 정부 리전 = 국내 AIDC의 확정 수요**

18.4GW 계획의 앵커 테넌트 — S·C등급 정부 에이전트 수요가  
국내 CSP 리전에 들어가야 채워지는 캐파



**그 문을 가장 먼저 통과하는 주체는 민간 에이전트가 아니라 정부 자신의 에이전트**

# 그런데 불가능 — 4대 병목

기술 문제가 아니라 제도 문제, 열쇠는 부처별로 분산



## 01 · 예산

서버 예산 有 · 지능(토큰) 예산 無

소관 — 기재부

## 02 · 조달

AI 3개월 주기 vs 시스템 3~5년

소관 — 기재부 · 조달청 · 행안부

## 03 · 전문성

순환보직 — 축적 전 이동

소관 — 인사처 · 행안부

## 04 · 클라우드

사실상 부재 — 서버 임대 + SI

소관 — 행안부 · 과기정통부 · 국정원



기술 문제가 아니라 제도 문제 — 열쇠는 부처별로 분산, 단독 해결 불가

# 문제제기자 중심 MVP · 성과중심 발주

공공AX = 프로세스 혁신 · 테스트베드

## 시작 방식

### 문제제기자 중심 MVP —

현업이 문제를 정의하고  
에이전트로 2~4주 검증

### 성과중심 발주 —

기능 명세 대신  
처리시간 · 비용 · 오류율 목표

### 실패 허용 —

무실패 → 무성과에서  
벗어나는 예산 항목

문제  
도착

2~4주

## 전환 결과

### 프로세스 혁신 —

신청 → Push, 사람 검토 →  
규정기반 에이전트 검토

### 테스트베드 —

정부가 첫 고객 —  
국내 모델 · 서빙 ·  
에이전트의 확정 수요

### 데이터 파이프 —

에이전트가 부를 수 있는  
형태로 데이터를  
다시 여는 계기



공공AX는 예산 항목이 아니라 국내 AI 스택의 첫 확정 수요

# 병목의 공통분모

예산·조달·전문성·클라우드를 풀어도 남는 질문 하나

예산이 있어도 → 부를 데이터가 없으면 헛도는 토큰

조달이 빨라져도 → 데이터셋마다 신청이면 멈추는 에이전트

전문가가 있어도 → 사람용 구조(HWP·PDF)면 불가능한 환각 감사

클라우드가 생겨도 → 망 밖에 데이터가 없으면 멈추는 루프

# 데이터

에이전트를 향한 데이터 개방 여부



공공AX의 병목은 결국 데이터 — 3부, 데이터전략

# 3

## 데이터전략

AI 센트릭 데이터 — 접근 · 이해 · 상태 · 배치

# AI 센트릭 데이터(AI-centric Data)란

공개의 기준 고객이 바뀌면 설계 기준도 바뀌는 세 번째 단계



**AI 센트릭 데이터 = 에이전트를 기준 고객으로 설계된 데이터 — 따라오는 4개 전환축**

# S·C 등급 공공AX의 성립 조건 — 파이프 · 지능 · 망

세 조건을 동시에 열어야

## 1 파이프 —

데이터 쪽 조건 ·  
접근 등급표 ·  
키의 성격 ·  
Stateless로 열기

## 2 지능 —

기억의 조건 ·  
메모리 규정 ·  
에이전트 신원 ·  
Stateful로 쌓기

## 3 망 —

에이전트가 사는 곳 ·  
N2SF 3.0 ·  
내부망 vs 정부 리전 ·  
로컬 + 클라우드



## 세 조건 모두 같은 열쇠 — C/S/O 등급

# 한국의 좌표 — AI-Ready 도달, Agent-Ready 공백

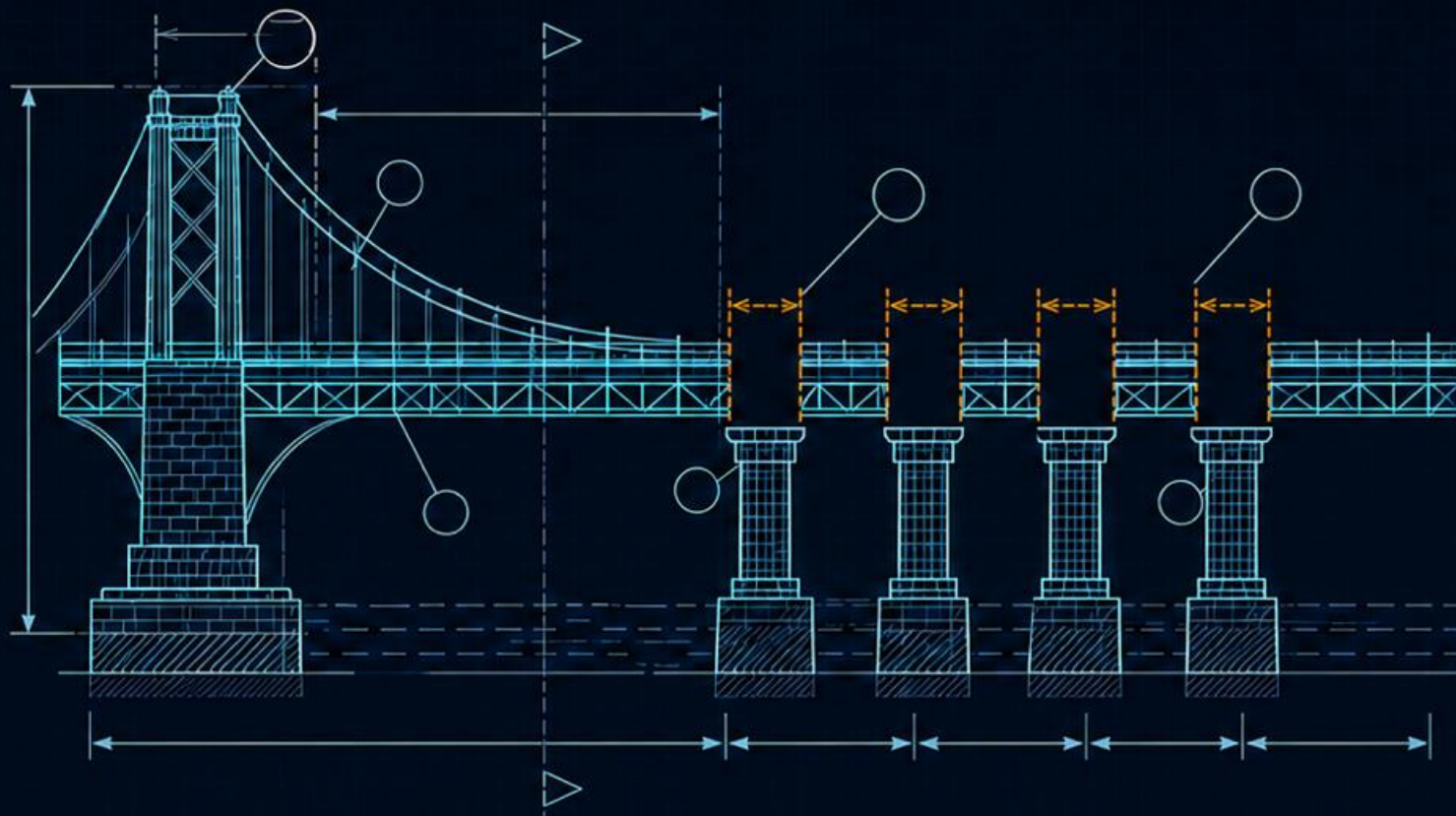
2026년 추진 사항과 남은 네 공백 → 네 개의 전환축

## 2026년 추진 사항

**5.28 데이터 관계장관회의**  
AI·고가치 데이터 Top 100,  
AI-Ready 품질관리, 공공누리  
AI유형 신설, 소재정보 단일창구  
(원·윈도우), 국가데이터기본법(가칭)

**8.3 AI 기반 공공데이터포털 시범**  
자연어 질의·추천,  
정부 통합 로그인 Any-ID,  
쿼시머리·큐레이션

**거버넌스**  
국가데이터처 승격(2025.9),  
국가데이터최고책임자 지정(2026.2)



## 공백 4가지 → 전환축

|                                    |      |
|------------------------------------|------|
| 무게 접근 ·<br>에이전트 신원 ·<br>에이전트 기준 한도 | ① 접근 |
| 기계가독 라이선스 ·<br>런타임 메타데이터           | ② 이해 |
| 메모리 ·<br>궤적의 규정 부재                 | ③ 상태 |
| 내부망 vs 리전,<br>배치 원칙 부재             | ④ 배치 |



원·윈도우는 있고 원키는 없음 — 접근·이해·상태·배치의 네 전환

# 전환① 접근 — 키의 유무가 아니라 키의 성격

식별(identification)용 키는 에이전트와 양립, 허가(authorization)용 키는 비양립

|         | 식별용 키 — 미국 api.data.gov | 허가용 키 — 한국 공공데이터포털      |
|---------|-------------------------|-------------------------|
| 발급 조건   | 이메일 입력, 즉시 발급           | 회원가입 + 휴대폰 본인인증 (PC 전용) |
| 키의 주체   | 앱 · 프로젝트 · 에이전트         | 신원이 확인된 개인              |
| 목적      | 레이트리미트 · 통계 · 남용 차단     | 이 사람의 이 데이터 사용 허가 여부    |
| 신청 단위   | 1회 발급, 참여 기관 API 전체 재사용 | 데이터셋마다 활용신청 → 승인        |
| 에이전트 양립 | 양립 — 식별자 전달로 충분         | 비양립 — 본인인증 · 클릭은 사람만    |



한국 포털의 키가 묻는 것: "누구인가"가 아니라  
"이 사람에게 이 데이터를 허가하는가" — 에이전트는 통과할 수 없는 문

# 전환① 접근 — 미국은 원키, 프랑스는 노키

신청 단위가 데이터셋이 아닌 구조



## 미국 — 원키

api.data.gov: 가입 즉시 키 1개, 참여 기관 API 전체에 재사용 — GovInfo·NASA·FEC 등

GSA가 연방 데이터 MCP 서버 목록(센서스·USAspending 등)을 공식 큐레이션

2026 MCP 서버·에이전트 해커톤 — 전 정부 직원 대상, 기관 데이터를 에이전트에 연결

## 프랑스 — 노키

mcp.data.gouv.fr (2026.2.25 공개): 접근 제한 없는 공개 인스턴스, 읽기 전용

약 7만4천 데이터셋 · 39만 파일이 대상 (2026.7)

DINUM 회고(2026.7.28): 특정 모델에 종속되지 않는 중립 서버 — 새 데이터 개방이 아니라 접근 방식의 변경



원키든 노키든 — 한 번 받은 키(또는 무키)로 등급 전체를 부르는 구조

# 전환① 접근 — 제안: 같은 등급이면 한 번

원키 · 노키 게이트웨이 = 등급별로 한 키



## 함께 바뀌어야 하는 것

- 신청 단위: 데이터셋 → 등급
- 키의 주체에 에이전트 추가 — 위임한 사람·기관, 범위, 만료
- 한도의 기준: 사람 앱 → 에이전트 트래픽(ttl · cacheScope)

## 한국 연결 — 지금 어디까지

- One-Window(5.28 데이터 관계장관회의) — 데이터가 어디 있는지 찾는 단일창구
- Any-ID(8.3 공공데이터포털 시범) — 정부 서비스 통합 로그인, 사람 한 명의 신원까지
- 남은 한 칸 = 원키 — 에이전트가 누구의 위임으로 접근하는지, 아직 없음
- 국가데이터기본법 제정 = 접근 원칙을 법에 못 박을 기회



**C/S/O 전체를 키 하나로가 아니라, 등급별로 한 키 — O 무키 · S 식별 · C 인가**

# 전환② 이해 — 환각의 원인은 데이터 구조

모델이 아니라 구조 — 사람용으로 설계된 데이터를 에이전트가 확률적으로 재구성 → 환각 · 감사 불능



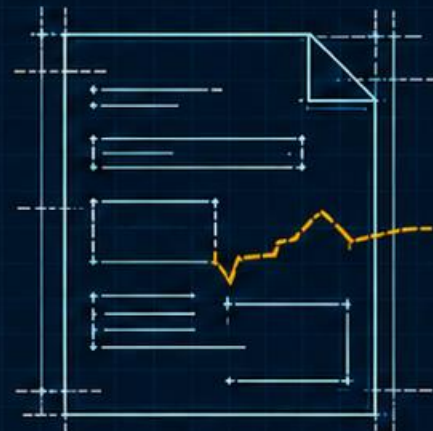
**사람 검토용 구조**  
HWP · PDF · FHIR



**파편화 · 맥락 빈곤**  
근거와 결론이 끊김



**확률적 재구성**  
벡터 RAG로 이어 붙임



**환각 · 사후 감사 불능**  
어디서 틀렸는지 추적 불가

## MedBeads (arXiv, 2026.5)

EMR · FHIR = 사람의 검토·행정에 최적화된 구조 —  
에이전트는 파편을 벡터 RAG로 재구성, 여기가 환각의 근본 원인

**처방: 인과로 링크된 불변 이벤트 그래프(Merkle DAG)**

## 행정 데이터에 적용하면

HWP · PDF 안의 규정 · 판단 근거를 개체 · 규정 · 인과 · 시점으로 링크  
기존 표준(공통표준용어 · 개방표준)을 그래프로 연결 —  
새 표준이 아니라 연결

**readable(읽힘)과 understandable(이해됨)은 다른 문제**

# 전환② 이해 — 영국: 공개 ≠ AI 준비도

GDS · DSIT 「정부 데이터셋의 AI 준비 가이드라인」(2026.1)과 국가데이터도서관



## 가이드라인의 4대 축

기술 최적화 — 구조·포맷·배포 방식  
데이터·메타데이터 품질 — 문서화·출처·일관성  
조직·인프라 맥락 — 사람·프로세스·데이터 성숙도  
법·보안·윤리 컴플라이언스 — 데이터셋 단위의 명시적 판단

**가이드라인 자체의 명시:** 데이터의 가용성이나 공개가 곧  
AI 준비도는 아님 — 자체 평가 체크리스트·액션플랜 포함

## 국가데이터도서관(NDL)

1억 파운드 이상·5개 킥스타터(에너지요금 지원·장기질환자  
취업·성인돌봄 수급·기업 법률 AI·기후데이터)  
— 2026.1 진행 보고

## GDS × 국립기록보관소 법령데이터

데이터 성숙도 진단 → MCP로 노출 → 40명 해커톤 검증.  
초기 증거: MCP가 AI 출력 품질에 유의미한 차이  
(2026.6, 알파 단계 진입)



# 영국은 "열었는가"가 아니라 "이해되는가"를 기준으로 삼기 시작

# 전환② 이해 — 제안: 런타임에 읽히는 것까지가 개방

readable에서 understandable로 가는 네 가지

## readable → understandable

런타임 메타데이터 3종 — 기계가독 라이선스(공공누리 AI유형을 필드로) · 신선도(ttl) · 접근등급(C/S/O)

스키마 · 코드북 · 단위 정의 — 컬럼의 의미 · 단위 · 코드표를 데이터와 함께 배포, 공통표준용어에 연결

국가 MCP 서버 — 카탈로그 검색 → 데이터 조회 → 분석 도구. 정부 공식 등재 · 모델 중립 — 프랑스 · 미국 GSA 방식

한국판 AI-ready 데이터 기준 — 영국 4대 축 참조, 자체 평가 체크리스트 — AI-Ready 품질관리(5.28)에 연결



메타데이터 세 줄 부재 → 에이전트가 써도 되는지 · 최신인지 · 어느 등급인지 모르는 상태

# 전환③ 상태 — 파이프는 Stateless

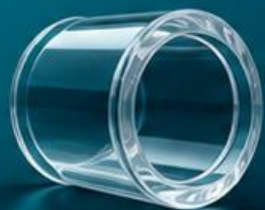
MCP 2026.7 스펙 — 세션 제거, 호출 단위 무상태



얇고 넓게 —  
아무나 붙었다 떨어질 수 있게

키 · 등급 · 메타데이터만 실어 보냄

호출은 버려도 되는 것



파이프는 얇게 — 연결은 버려도 되는 것

# 전환③ 상태 — 지능은 Stateful

기억을 1급 아키텍처 자산으로 — 2026년 상반기 빅테크의 '세션을 넘는 기억' 제품화



사실 · 기준정보 — 조직 · 코드 · 기준 금액

사건 · 처리 이력 — 비식별 패턴 · 결정 궤적

지시 · SOP · 조례 해석 — 반복 판단의 근거

과업 · 진행 중 민원 — 상태 · 다음 단계



파이프는 Stateless, 지능은 Stateful — 호출은 버려도 궤적은 남긴다

# 전환③ 상태 — 제안: 기억을 자산으로

메모리 스토어 · 에이전트 신원 · 개인정보 한계 — 열린 파이프(무기), 쌓이는 기억(해자)

## 공동기반 메모리 스토어

기관 공통 레이어 · 사실/사건/지시/과업  
4분류 · 버전 대체 규칙 · 감사 로그

## 에이전트 신원

위임한 사람 · 기관, 범위, 만료 —  
전환①의 키 주체 확장과 같은 객체

## 무기 개방과 기억 해자의 비충돌

파이프를 무기로 열어도 남는 차별화 — 누가 무엇을 했고  
무엇을 배웠는지는 게이트웨이가 아닌 메모리 스토어에 축적 /  
개방은 파이프의 일, 경쟁력은 기억의 일

## 개인정보 한계

자산화 대상은 규정 · 비식별 이력 ·  
기준정보 / 민원 원문은 제외 ·  
보존기한 · HITL



# 열린 파이프에서 생기는 차별화 — 기억

# 전환④ 배치 — 내부망 vs 정부 리전

에이전트가 사는 곳 — 격리의 단위는 선(물리망)이 아닌 인가(ATO)

## 내부망 배치

망 안에서는 루프 가능 · 모델 소급 부담 없음  
외부 실시간 웹 · 내부망에 없는 도구 사용 불가  
갱신은 사업 단위 — 뒤처지는 모델 세대

## 정부 리전 — 미국 GovCloud

CSP 자체 리전에 정부가 인가 경계를 긋는 구조  
2026.7.28 승인표: Claude 4.8 Opus · Claude 5 Sonnet · GPT 5.4 · Nemotron 3 · Grok 4.3  
완전 폐쇄 옵션은 별도(GDC air-gapped)

|        | 미국                        | 한국                          |
|--------|---------------------------|-----------------------------|
| 격리의 단위 | 인가 경계 + 논리 격리 (CSP 자체 리전) | 물리망 + 정부 데이터센터 상면 (PPP 존)   |
| 경계 정책  | 통제된 연결                    | 선으로 단절, 연결은 예외              |
| 갱신     | 상시 인가 파이프라인, 분기 단위        | 사업 단위 (1차 2025 → 2차 2026.8) |



둘 중 하나가 아닌 둘 다 — 데이터 등급이 정하는 위치

# 전환④ 배치 — 프랑스 Albert API, 한 점점의 멀티탭

DINUM의 OpenGateLLM 인스턴스 — 오픈웨이트와 상용 모델을 단일 게이트웨이로, 로컬과 클라우드를 한 점점에서

## 구조

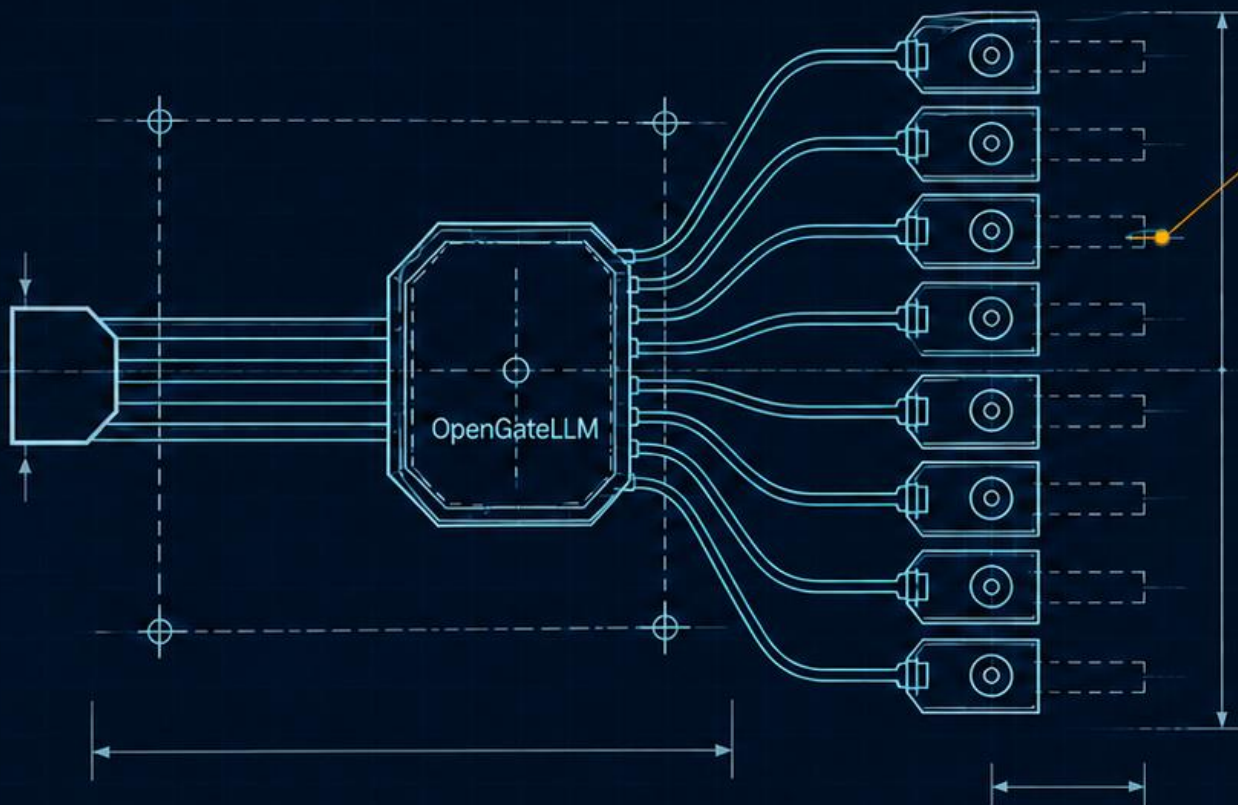
OpenGateLLM — 프랑스 정부가 개발한 오픈소스,  
Albert API는 그 DINUM 인스턴스

오픈웨이트 · 상용 모델을 하나의 점점에서 구동,  
OpenAI 호환 규약 — 기존 도구 그대로 연결

RAG · OCR · 분류 · 벡터화를  
공동 기능으로 제공

주권 호스팅 — Outscale, 이후 Nubo(정부 클라우드)  
SecNumCloud 인증

DINUM 표현: 행정을 위한 "멀티탭(multiprise)"



1만 명

8개 부처 공무원 시험  
(2025.10~, 8개월) —  
Albert API 위에 올린  
Assistant IA, 2026  
일반화 검토

## 교훈

초기 챗봇(Albert France  
Services)은 현 형태로  
일반화하지 않기로(2026.1) —  
살아남은 것은 챗봇이 아닌  
게이트웨이



게이트웨이가 모델의 위치를 추상화 — 로컬이든 클라우드든 한 점점, 한 규약

# 전환④ 배치 — 제안: 등급이 라우팅

원키 게이트웨이의 두 번째 역할 = 라우터



같은 에이전트, 과업의 등급에 따라 양쪽 왕복 — 배치를 사람이 아닌 등급이 결정

## 클라우드

민간 클라우드 정부 리전 · 프론티어 모델

O · S 등급 / 외부 웹 · 외부 도구 / 대규모 추론 · 최신 모델

## 로컬

내부망 · sLLM · 온디바이스

C 등급 · 개인정보 / 상시 루프 · 저지연 / 상면 · 소급 부담 없음

## 한국 현황

공통기반 2차(2026.8.10, 66억 · 180일): AI 게이트웨이 · MCP 연계 · 행정망-인터넷망 연계 최소 1개 검증 → 리전에 올라갈 세입자 플랫폼의 선행

PPP 존 ≠ 정부 리전 — 처방은 CSP 자체 리전 + CSAP + N2SF 3.0 인가 경계, 공통기반이 그 첫 세입자



# 클라우드나 로컬이냐가 아닌, 라우팅 주체는 등급

# 등급 축 하나로 네 문을 함께

접근 · 이해 · 상태 · 배치 — 네 가지 전환의 기준은 모두 같은 C/S/O 등급



기준을 따로 두면 —  
사업 네 개, 창구 네 개

등급 축 하나로 묶으면 —  
게이트웨이 하나

| 등급 | ① 접근 — 어떤 키로      | ② 이해 — 무엇을 붙여       | ③ 상태 — 기억은 어디까지        | ④ 배치 — 어디서 돌리나               |
|----|-------------------|---------------------|------------------------|------------------------------|
| O  | 무키 — 신청 없이 열람     | 라이선스 · 갱신주기 · 등급 표시 | 대화 이력까지 자산으로           | 민간 클라우드 정부 리전<br>+ 과도기 PPP 존 |
| S  | 식별 키 하나로 전부       | + 항목 설명 · 코드북       | 비식별 처리 후 보관            | 민간 클라우드 정부 리전<br>+ 과도기 PPP 존 |
| C  | 인가 키 하나 — 범위 · 만료 | + 인가 범위 · 감사 기록     | 보관 제한 ·<br>사람 확인(HITL) | 내부망 로컬 · 소형 AI               |



네 개의 사업이 아니라 하나의 게이트웨이 — 열쇠는 등급

# 무엇을 바꿀 것인가 — KPI와 로드맵

기존 모델 소급 부담 없음



## 등급별 키 전환율

데이터셋 신청 → 등급 키로 옮겨간 비율

## MCP 카탈로그 커버리지

정부 공식 MCP 서버로 닿는 데이터셋 비중

## 에이전트 트래픽 비중

포털 호출 중 에이전트 키의 몫

## 메모리 스토어 적용 업무

기억 레이어 위에서 도는 행정 업무 수

1

### 2026 하반기

KOSIS MCP 파일럿 · O등급 무키 실증 · 정부 MCP 공식 등재

2

### 2027 상반기

국가데이터기본법에 등급별 접근 원칙(키·식별·인가) 명문화 · 공공누리 SI유형 메타데이터화

3

### 2027 하반기

범정부 원키 게이트웨이 가동(등급별 한 키) · 에이전트 기준 한도 · 캐시 체계

4

### 2028

행정 궤적 로그 표준 · 공공 AgentOps · 부처·지자체 메모리 레이어 시범(HITL · 감사)



병행 과제: N2SF 2.0 · 민간 클라우드 정부 리전 제도화(2027)

공개는 무키, 그 위는 등급별 원키.

readable을 넘어 understandable로.

파이프는 Stateless로 열고, 지능은 Stateful로 쌓는다.

배치는 등급이 정한다.

그리고 그 첫 고객은, 정부 자신의 에이전트다.