LHRI-FOCUS
Land Housing Research Institute
vol.84
2026. 8. 18.

민감한 공공자료, 해외 AI에 맡겨도 될까

공공기관이 '자체 AI'를 준비해야 하는 이유

LH 토지주택연구원

LHRI-FOCUS

CONTENTS

민감한 공공자료, 해외 AI에 맡겨도 될까

공공기관이 '자체 AI'를 준비해야 하는 이유

이상훈 연구위원
icarus@lh.or.kr

※ 저자 이미지는 ChatGPT를 활용하여 제작된 캐리커처로, 실제 인물의 외형과 일부 차이가 있을 수 있습니다.

민감한 공공자료, 해외 AI에 맡겨도 될까

공공기관이 '자체 AI'를 준비해야 하는 이유

이상훈 연구위원

01

우리가 쓰는 AI, 정말 안전한가

AI는 이미 공공부문 깊숙이 들어와 있다

생성형 AI의 활용은 공공부문까지도 빠르게 확산되고 있다. 지난 10년간(2015~2024) 공공부문에서 체결된 AI 도입 계약만 무려 6,975건에 이른다.[1)]

정책적 움직임도 빠르다. 정부는 올해 AX(AI 전환, AI Transformation) 사업에 약 2조 4천억 원을 투입하며,[2)] 내부 문서를 스스로 학습해 담당자의 업무를 돕는 이른바 'AI 에이전트(AI Agent)' 도입도 본격화되고 있다. 상황이 이렇다 보니, "AI를 쓸 것이냐 말 것이냐"는 이미 지나간 질문이 되어 버렸다.

이제 필요한 질문은 "민감한 행정 자료를 어떻게 안전하게 다루면서 AI를 쓸 것이냐"이다.

자료가 어디로 가는지, 아무도 모른다

지금의 AI 이용 방식은 여러가지 문제들이 내재하고 있다. 이 중 하나가 담당자들이 개인적으로 외부 AI 서비스(GPT, 제미나이, 클로드 등)에 업무 자료를 그대로 입력하는 이른바 '섀도우 AI(Shadow AI)' 현상이다. 회의록을 요약하려고 참석자 발언을 그대로 붙여 넣거나, 보고서 초안을 다듬으려고 내부 자료를 통째로 올리는 일이 대표적이다.

물론 AI 회사들도 "사용자가 입력한 내용을 학습에 쓰지 않는다"고 약속한다. 그러나 그 자료가 정말 저장되지 않고 삭제되는지를 확인할 방법은 사실상 없다. 게다가 누가 언제 무엇을 입력했는지에 대한 기록도 조직에 남지 않기 때문에, 문제가 생겼을 때 경위를 되짚기조차 어렵다.

결국 AI 활용에서 중요한 문제는 '자료를 지금 어디서 처리하고 있고, 누가 통제하고 있는가'라는 물음이다. 이 통제력을 우리 스스로 갖는 것, 이것이 바로 AI 주권이다.

1) 소프트웨어정책연구소. (2026). 「2025년 공공부문 AI 도입현황 연구」

2) 제4회 과학기술관계장관회의(2026.1), KBS 등 뉴스보도

해외 AI는 언제든 멈출 수 있다

지금 우리가 쓰는 해외 AI는 그 나라 정부의 정책 한 번에 접속이 막힐 수 있는 서비스다. 실제로 미국은 국가안보를 이유로 첨단 반도체와 AI 기술의 수출을 지속적으로 통제해 왔다. 따라서 외부 AI는 언제든 "우리가 통제할 수 없는 이유로 멈출 수 있는 서비스"라는 전제 아래 써야 한다.

한 기관의 핵심 업무가 특정 해외 AI에 깊숙이 연결되어 있다고 가정해 보자. 그 접속이 어느 날 갑자기 끊긴다면 어떤 일이 벌어질까. 이는 단순한 시스템 장애로 끝나지 않는다. 행정은 지연되고, 업무는 공백에 빠지며, 급하게 다른 시스템으로 갈아타는 데에 막대한 비용이 든다. 여기에 이미 축적해 둔 프롬프트와 업무 절차, 연동 데이터까지 고려하면 특정 서비스에 발이 묶이는 부담도 결코 가볍지 않다.

그런데도 우리는 "AI 이용이 어느 날 갑자기 멈춘다면 어떻게 할 것인지, 활용된 자료는 안전할 것인지" 등에 대한 대비를 하지 않고 있다. 그래서 지금이라도 "앞으로도 계속 남의 AI를 빌려 쓸 것인가, 아니면 우리 것을 직접 갖출 것인가?"를 고민해야 한다.

이 물음에 답하기 위해 이 글에서는 먼저 다른 나라들의 대응을 살펴보고, 우리가 직접 AI를 갖출 수 있는 여건이 되었는지, 그리고 무엇을 어떻게 준비해야 하는지를 차례로 짚어 보고자 한다.

02
세계는 이미 움직이고 있다

같은 고민을 먼저 시작한 나라들의 접근은 크게 세 갈래다.
미국은 상용 AI를 쓰되 통제 장치를 촘촘히 두고,
싱가포르는 자체 개발과 글로벌 협력을 병행하며,
유럽은 데이터를 역내에 묶어 두는 방식을 택했다.

미국 : 적극 활용하되, 촘촘히 통제한다

미국은 시장에 나와 있는 좋은 AI를 적극 활용하고 있다. 대신 아주 촘촘한 감시망을 두었다. 요컨대 "쓰되, 아무렇게나 쓰지는 못하게 한다"는 것이 미국식 접근의 핵심이다.

백악관 예산관리국(OMB, Office of Manage-ment and Budget)은 연방기관이 AI를 쓸 때 반드시 위험관리 체계를 함께 갖추도록 의무화하고,[3] 연방 보안인증 제도인 FedRAMP (Federal Risk and Authorization Management

[사례] AI 접속이 끊길 수 있다는 것을 보여준 사건

미국 정부는 국가안보상 이유로 특정 고성능 AI 모델에 대한 외국인의 접근을 제한해 왔다. 실제로 오픈AI의 최신 모델 'GPT-5.6'도 출시 직전인 2026년 6월 접근 제한 조치가 요구되었다가, 약 한 달 뒤인 7월 8일에야 해제되었다. 한 나라의 정책 결정 하나로 다른 나라 이용자의 AI 접근권이 순식간에 좌우될 수 있다는 사실이 눈앞에서 드러난 사건이다. 공공기관이 외부 상용 AI를 쓸 때 반드시 대체 모델과 비상 전환 절차를 함께 준비해 두어야 하는 이유가 여기에 있다. [4]

3) NIST. (2024). Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (NIST AI 600-1).

4) axios.com (2026.7.8.) Trump administration lifts restrictions on OpenAI's GPT 5.6

Program, 연방 위험·인증 관리 프로그램)는 로그인·권한·접근 기록 관리 같은 기업급 보안 기능을 갖춘 AI 클라우드만 우선적으로 인정하는 방식을 택했다.

그러나 특별히 민감한 분야에서는 방식이 달라진다. 국방부와 에너지부가 대표적이다. 이런 경우에는 자체 AI를 두고 쓴다. 미국은 자료의 민감도에 따라 두 개의 트랙을 병행하는 셈이다. 국방부는 외부와 단절된 기밀망 안에서만 돌아가는 폐쇄형 AI를 채택했다. 에너지부 역시 국립연구소의 연구 데이터가 유출되지 않도록 하는 폐쇄형 AI 플랫폼을 구축하고 있다.

싱가포르 : 스스로 만들되, 세계와 손잡는다

싱가포르 정부는 「국가 AI 전략 2.0(National AI Strategy 2.0)」을 발표하며 자체 AI 모델 육성에 힘을 쏟고 있다. 그 대표적인 결실이 바로 동남아시아 언어와 문화에 특화된 오픈소스 모델 'SEA-LION' 구축이다.

다른 한편으로는 글로벌 빅테크와 손을 잡았다. 최근 싱가포르는 OpenAI의 아시아 거점 유치와 Google Gemini의 공공행정 활용 협력을 발표한 바 있다.[5)]

이는 자립과 개방을 동시에 추구하는 전략이다. "모든 AI 하드웨어를 국가 안에서 만든다"는 물리적 자급자족을 고집하지 않는 대신, "꼭 필요한 기술은 갖되, 나머지는 세계와 협력한다"는 균형 잡힌 접근을 채택한 것이다. 자립과 개방을 대립이 아니라 조합으로 본 셈이다.

[사례] AI 싱가포르(AISG)가 개발한 SEA-LION

동남아시아의 다양한 언어와 문화적 맥락을 이해하도록 만들어진 오픈소스 대형 언어모델(LLM, Large Language Model) 제품군이다. 이는 모든 AI 인프라를 자국에서 만들려는 물리적 자급자족보다, 국가 맞춤형 활용과 글로벌 협력에 초점을 맞춘 사례이다.

AI SINGAPORE

SEA-LION

출처 : https://sea-lion.ai/

유럽 : 법으로 데이터 주권을 지킨다

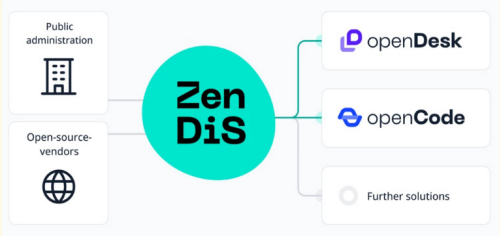
유럽연합은 법으로 강력한 규제선을 그었다. AI법(AI Act)과 일반 개인정보 보호 규정(GDPR, General Data Protection Regulation)이 그 대표적인 장치다. 이 두 법을 통해 EU는 위험도가 높은 AI에 대해 책임성 확보, 투명성 제공, 인간의 직접 감독 등의 의무를 부과하고 있다.

한편, 미국 빅테크에 대한 의존을 줄이기 위해 유럽은 자체 도구 개발에도 나서고 있다. 독일은 개방형 협업·문서 도구 'OpenDesk'를 자체 개발했고, 프랑스도 비슷한 성격의 'LaSuite'로 대응하고 있다. 유럽의 AI 기업들 역시 자체 AI 모델과 솔루션을 만들고 있다. 대표적으로 프랑스의 Mistral AI와 독일의 SAP가 유럽 기업용 AI 솔루션 개발에 협력하는 흐름이 형성되고 있다.

5) Smart Nation Singapore (2023) National AI Strategy 2.0 / AI Singapore (2025)

[사례] 독일 openDesk

openDesk는 독일이 공공행정의 디지털 주권(Digital Sovereignty)을 지키기 위해 개발한 개방형 협업·오피스 소프트웨어 묶음이다. 연방 정부 산하의 디지털 주권 센터(ZenDiS, Zentrum für Digitale Souveränität)가 개발을 주도하고 있으며, 국제형사재판소(ICC)를 비롯한 유럽 여러 공공기관이 도입해 주목받는 사례이다.



출처 : https://www.opendesk.eu

한국 : 추격자에서 벗어날 때가 됐다

한국의 전자정부 역량은 이미 세계 최고 수준이다. 그러나 AI의 원천기술로 들어가면 상황이 달라진다. GPU(Graphics Processing Unit, AI 학습·추론용 반도체) 같은 핵심 인프라나 대형 언어모델의 근간 기술은 해외 빅테크에 크게 의존하고 있다.

서두에서 말한 것처럼 외부 클라우드에 공공 AI를 계속 얹어 두면 나중에는 서비스를 바꾸고 싶어도 바꾸기 어려운 이른바 '운영 종속' 상황에 빠질 위험이 있다.

물론 아무런 대비도 안 하고 있는 것은 아니다. 정부는 이미 K-클라우드, 소버린 클라우드(Sovereign Cloud, 자국 법의 적용만 받는 클라우드), 그리고 독자적인 파운데이션 모델 확보 사업(이른바 '독파모')을 추진하고 있다. 금융과 제조업을 중심으로 사내 폐쇄망 AI 도입도 눈에 띄게 빨라지고 있다.

문제는 AI 주권의 확보 방향과 속도다. 이제는 남을 따라가는 '빠른 추격자(Fast Follower)'가 아니라, 스스로의 기반을 먼저 갖추는 '선도자(First Mover)'로 방향을 틀 때다.

그렇다면 우리 손으로 AI를 갖춘다는 것이 과연 현실적으로 가능한 일일까. 다음 장에서는 이 질문을 성능과 비용의 두 축에서 짚어 본다.

03
직접 만든 AI, 이제는 쓸 만하다

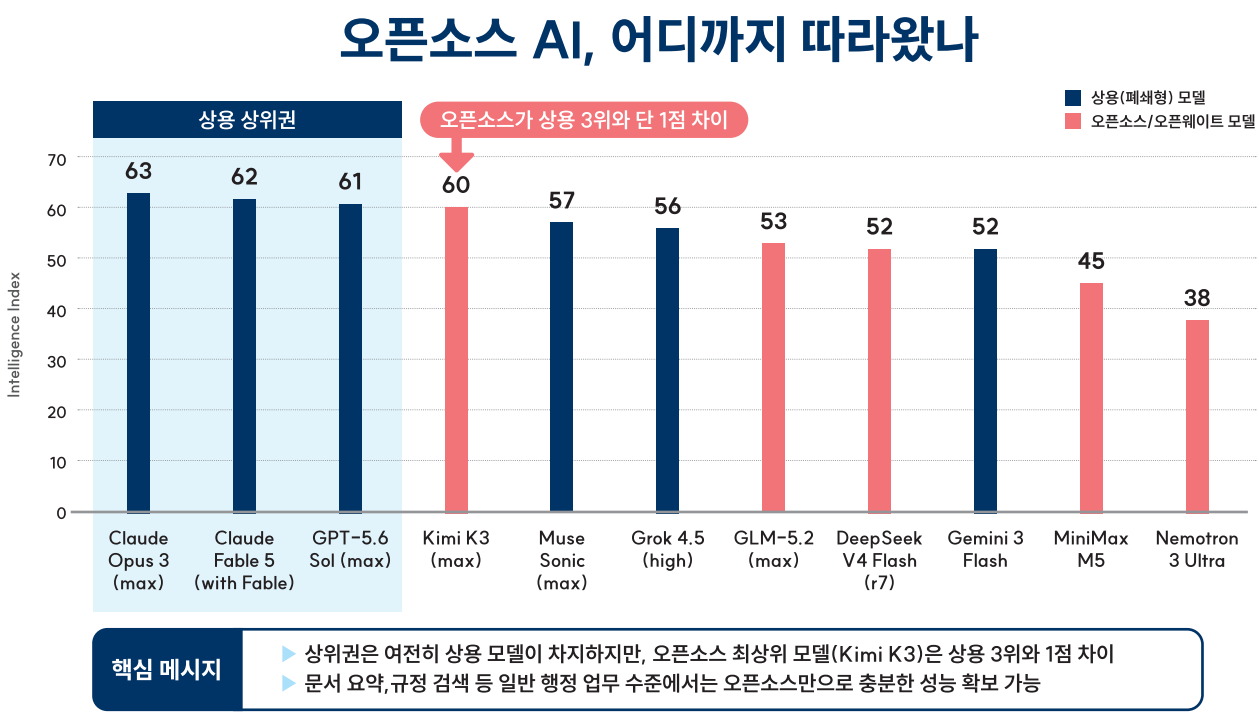
이 지점에서 자연스레 떠오르는 질문이 있다. "우리가 직접 만든 AI도 쓸만 할까? 비용은 감당할 만할까?" 하는 것이다. 결론부터 말하자면 이 두 걱정 모두에 대해 상당히 안심할 수 있는 시점에 와 있다.

오픈소스 AI, 성능은 이미 상용급이다

몇 년 전만 해도 무료로 공개된 오픈소스 AI는 유료 상용 AI에 비해 답변 수준이 떨어졌다. 그러나 최근에는 상황이 많이 달라졌다. 새로 공개된 오픈소스 모델들이 일반 행정 업무에서 요구되는 수준을 이미 넘어서고 있다. 특히 문서 요약, 규정 검색, 회의록 정리처럼 반복적인 행정 업무에서는 그 효과가 여러 실증을 통해 이미 확인되었다.

오래 쓸수록 직접 구축이 유리하다

비용 문제도 중요한 관건이다. 외부 AI를 빌려 쓰는 방식과 우리가 직접 구축하는 방식, 과연 어느 쪽이 더 저렴할까. 결론부터 말하자면 사용량이



주1) 세로축의 점수는 Artificial Analysis Intelligence Index로, MMLU·GPQA·MATH 등 복수 지표를 종합한 상대 점수(100점 만점 기준)임
주2) 상용 폐쇄형 모델(Claude Opus, Claude Fable5, GPT Sol)이 최상위권에 있으나 오픈웨이트, 오픈소스 모델,(Kimi K3, GLM-5.2, DeepSeek V4, MiniMAX)들도 상위권에 다수 진입한 점에 주목
주3) 벤치마크 결과는 시점과 산정 방식에 따라 순위가 달라질 수 있음

그림-1 오픈소스 AI, 어디까지 따라왔나 - 주요 LLM 성능 비교

출처 : ArtificialAnalysis.ai, 2026.8.12.

많을수록 직접 구축이 유리해진다.

외부 API(Application Programming Interface, 응용 프로그램 인터페이스) 방식은 처음에 드는 돈이 적다. 그러나 쓰면 쓸수록 호출 요금이 눈덩이처럼 쌓여 시간이 갈수록 운영비가 급격히 불어난다. 반면 직접 구축하는 방식은 처음에는 서버 구매 등으로 큰돈이 들지만, 그 이후로는 대부분 고정비 위주로 유지된다.

가상 시나리오를 하나 만들어 보자. 직원 3,000명이 하루에 30번, 연간 250일 AI를 쓴다고 가정한다. 이때 5년간 드는 TCO(Total Cost of Ownership, 총소유비용)는 외부 API 방식이 약 66.5억 원, 직접 구축 방식이 약 52.5억 원 수준으로 추정된다. 두 방식의 비용은 약 2.8년째에 역전되고, 그 이후로는 격차가 계속 벌어진다.

여기에 앞서 짚었던 접근 중단 위험이나 요금 인상 가능성까지 생각하면, 직접 구축이 갖는 전략적 가치는 단순한 비용 비교보다 훨씬 크다.

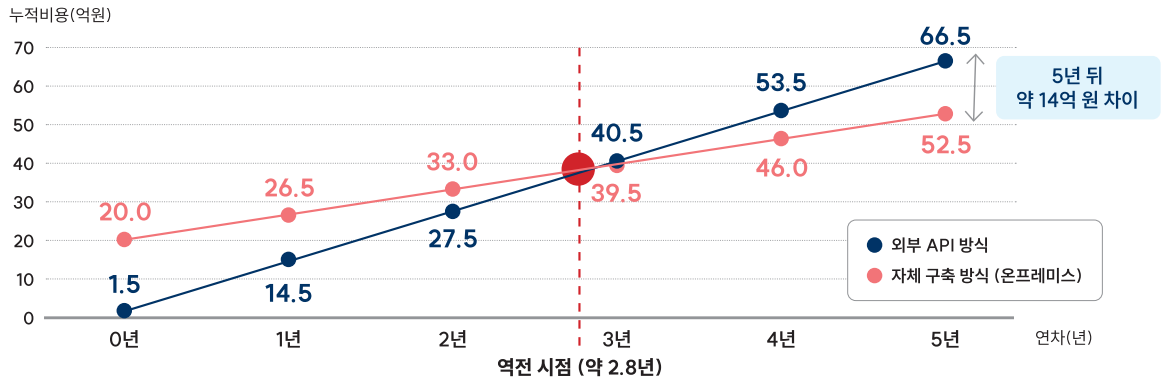
자체 AI, 이렇게 구성된다

기관 안에 자체 AI를 갖춘다는 것은 성능 좋은 모델 파일 하나를 사 오는 일과는 거리가 멀다. 여러 요소가 하나의 시스템처럼 맞물려 돌아가야 비로소 쓸 만한 AI가 된다.

먼저 최신 자료를 찾아와 답하게 하는 RAG (Retrieval-Augmented Generation, 검색 증강 생성) 기술이 붙어야 한다. 이는 '오픈북 시험'에 비유할 수 있는데, 모델이 답하기 전에 기관 내부 문서를 먼저 찾아본 뒤 그 내용을 근거로 답하게 하는 방식이다. 다음으로 누가 어떤 자료에

외부 API vs 자체 구축 – 5년 뒤 비용은 이렇게 갈린다

직원 3,000명·1일 30회·연 250일 (연 2,250만 회 호출) 기준 가상 시나리오



핵심 메시지

- ▶ 초기에는 외부 API가 저렴하지만, 사용량이 늘수록 비용이 급증해 **약 3년차에 역전**
- ▶ 5년 이상 장기 관점에서는 자체 구축이 **약 14억 원가량의 절감 효과**

※ 가상 시나리오이며, 실제 금액은 모델 단가 • 환율 • 사용량 • 장비 견적 등에 따라 변동될 수 있음

주1) 단가 가정 : 호출당 입력 2,000토큰·출력 1,000토큰, 환율 1,400원/달러, 발간 시점의 주요 상용 API 공개 요율 적용
주2) 본 TCO는 예산 검토를 위한 가상 시나리오이며, 실제 금액은 모델 단가·환율·사용자 수·토큰량·GPU 견적·전력 단가·유지보수 범위·재학습 주기·감가상각 방식에 따라 크게 변동될 수 있음

그림-2 빌려 쓰는 AI vs 직접 만든 AI - 5년 뒤 비용은 이렇게 갈린다

출처 : 저자 작성, 가상 시나리오에 기반한 추정 차트

표-1 빌려 쓸 때와 직접 만들 때의 5년 총비용 비교 (가상 시나리오, 단위: 억 원)

출처 : 저자 작성, 사용자 3,000명·1일 30회·연 250일 가정

구분	항목	빌려 쓰는 방식 (외부 API)	직접 만드는 방식 (온프레미스)	비고
초기비용	서버·장비 구축	0.5억	15.0억	온프레미스는 GPU서버·스토리지·네트워크 포함
	모델 튜닝·검색 연동(RAG)	1.0억	5.0억	오픈소스 모델 튜닝, 내부 문서 검색·권한 연계 포함
운영비용 (연간)	이용료 또는 장비 유지보수	12.0억/년	2.0억/년	빌려 쓸 때는 사업자 요금·사용량(토큰)에 따라 변동
	전력·냉각·관제 시스템	0.0억/년	1.5억/년	사업자가 부담(빌려 쓸 때) / 자체 부담(직접 구축)
	전담 운영 인력	1.0억/년	3.0억/년	운영·보안관제 담당 인력
5년 누적	**총 비용**	**66.5억**	**52.5억**	**직접 구축 시 약 14억 원(21.1%) 절감**

주1) 산식 : 빌려 쓰는 방식 = 초기 1.5억 + 연 13.0억 × 5년 / 직접 만드는 방식 = 초기 20.0억 + 연 6.5억 × 5년
주2) 손익분기 시점은 약 2.8년이며, 이후로는 격차가 계속 벌어짐
주3) 사용 규모 : 직원 3,000명 × 1일 30회 × 연 250일 = 연 2,250만 회 호출 기준
주4) 실제 금액은 모델 단가·환율·사용자 수·사용량·장비 견적·전력 단가·유지보수 범위·재학습 주기에 따라 크게 변동될 수 있음

접근할 수 있는지를 관리하는 권한 체계가 필요하다. 여기에 위험한 질문을 걸러 주는 보안 필터, 기관 특유의 문체까지 반영하는 파인튜닝(Fine-tuning, 특정 분야 자료로 모델을 추가 학습시키는 작업)이 함께 어우러져야 한다.

도입 전, 반드시 챙겨야 할 네 가지

온프레미스 LLM을 도입하려면 다음 네 가지 전제조건을 함께 챙겨야 한다.

첫째, GPU 확보와 공급망 리스크의 사전 점검이다. 고성능 GPU는 수요가 집중되는 전략

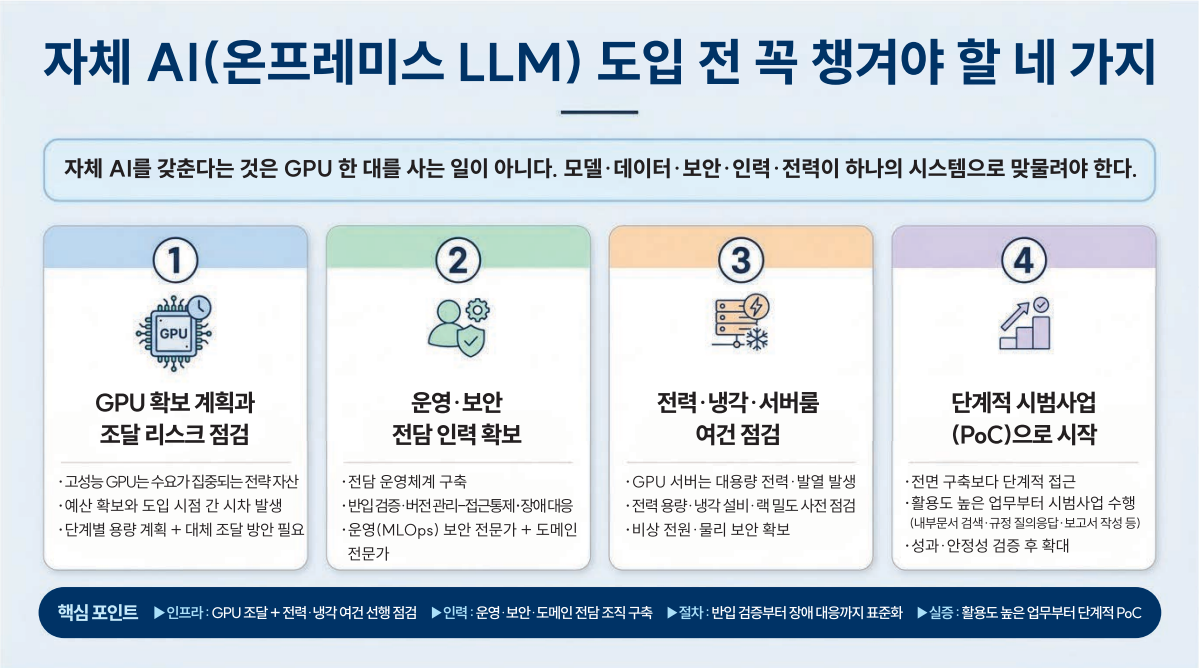


그림-3 직접 만든 AI(온프레미스 LLM) 도입 전 준비사항 네 가지

출처 : 생성형 AI로 작성

자산으로, 예산 확보 시점과 실제 도입 시점 사이에 시차가 발생한다. 따라서 단계별 용량 계획과 대체 조달 방안을 함께 마련해 두어야 한다.

둘째, 전담 운영 인력을 확보해야 한다. 모델 반입 검증·버전 관리·접근통제·장애 대응을 담당하는 MLOps(Machine Learning Operations, 머신러닝 운영) 인력, 보안관제 인력, 그리고 업무부서의 도메인 전문가가 함께 참여하는 전담 운영체계가 필요하다.

셋째, 전력·냉각·서버룸 환경을 선행 점검해야 한다. GPU 서버는 전력 사용량과 발열이 매우 크다. 기존 전산실의 전력 용량, 냉각 설비, 랙 밀도, 비상 전원, 물리보안 환경을 사전에 검토해야 도입 이후의 예상치 못한 병목을 피할 수 있다.

넷째, 처음부터 전면 구축하기보다 단계적 실증을 추진해야 한다. 내부문서 검색, 규정 질의응답, 보고서 작성 지원처럼 활용도 높은 업무부터 PoC (Proof of Concept, 개념 증명) 를 수행하고, 성과와 안정성을 검증한 뒤 단계적으로 확대하는 것이 합리적이다.

04
이제, 우리가 준비할 차례다

남의 AI를 빌려 쓰는 시대는 저물고 있다. 이제 필요한 것은 필요한 순간, 우리 손으로 쓸 수 있는 AI다. 데이터 주권과 업무 연속성을 지키는 다섯 가지 과제, 지금 준비하지 않으면 다음 기회는 오지 않는다.

AI 주권은 '쓸 수 있는 권리'를 지키는 일이다

공공 AI의 진정한 경쟁력은 가장 최신 모델을 가장 먼저 도입하는 데 있지 않다. 어떤 상황에서도 흔들리지 않고, 필요할 때 우리 손으로 쓸 수 있는 체계를 갖추는 데 있다. 그것이 바로 AI 주권이다.

직접 만든 AI가 모든 문제의 해법은 아니다. 그러나 민감 데이터와 기관 고유의 지식 자산 영역에서는 데이터 주권과 기술 자립을 확보하는 실질적 수단이 된다.

향후 공공부문은 인증·전용 클라우드와 직접 만든 AI를 업무 등급별로 조합하는 하이브리드 전략으로 보안성·비용 예측성·자립성을 확보해야 한다. 즉, 공개 가능한 업무는 인증 클라우드로, 민감·폐쇄망 업무는 자체 구축으로 이원화하는 방식이다. 여기에 기관의 CIO(최고정보책임자, Chief Information Officer)·정보보호 담당관이 통제하고, 시범사업을 거쳐 표준화로 안착하는 단계별 추진이 필요하다.

제대로 안착시키려면 다섯 가지가 필요하다

공공 AI가 제대로 안착되기 위해서는 기술만이 아니라 제도와 거버넌스가 함께 갖춰져야 한다. 이를 위한 과제는 다음 다섯 가지이며, 실행 순서를 고려해 배치했다.

첫째, 데이터 거버넌스부터 세워야 한다. 내부 문서를 어디까지 AI 학습에 쓸 것인지, 개인정보는 어떻게 비식별화할 것인지에 대한 기준을 먼저 세워야 한다. 이 기준 없이는 어떤 AI를 도입해도 통제가 무너진다.

둘째, 공공 AI 전용 가이드라인이 필요하다. 어떤 모델을 어떻게 반입할지, 어떤 로그를 얼마나 보존할지 등 세부 기준을 담아야 한다. 데이터 거버넌스가 원칙을 정한다면, 가이드라인은 그 원칙을 실무 절차로 옮긴다.

셋째, 운영을 표준화해야 한다. 폐쇄망 안에서 AI를 배포하고, 버전을 관리하며, 장애에 대응하는 표준 절차와 전담 조직이 필요하다.

넷째, 공공에 특화된 평가체계를 마련해야 한다. 단순한 정확도만이 아니라 답변에 근거가 잘 붙는지, 보안 필터가 제대로 작동하는지 같은 공공 업무 특유의 지표로 AI를 평가해야 한다.

다섯째, 업무 연속성을 확보해야 한다. 외부 AI가 갑작스레 멈춰도 흔들리지 않도록 대체 모델·백업 시스템·전환 절차를 미리 갖춰야 한다. 특정 해외 모델에 지나치게 의존하는 상황은 반드시 피해야 한다.

이 다섯 과제는 원칙(①) → 절차(②) → 실행(③) → 검증(④) → 지속가능성(⑤)의 순서로 이어지며, 어느 하나라도 빠지면 나머지가 흔들린다.

하이브리드 전략, LH라면 이렇게 그려진다

이런 전환이 어떻게 현실화될 수 있을까. 한국토지주택공사(LH)의 보안 환경을 예시로 그림을 그려 보면 훨씬 선명해진다.

LH는 이미 보안을 위해 두 가지 PC 환경을 나눠 운영하고 있다. 하나는 인터넷이 되는 물리 PC, 다른 하나는 인터넷이 아예 차단된 채 내부 업무망에만 접속하는 가상 PC다. 그런데 AI 활용의 관점에서 보면 이 두 환경 모두에서 묘한 문제가 발생한다.

물리 PC 쪽부터 보자. 이곳에서는 직원들이 ChatGPT, Gemini, Claude 같은 외부 상용 AI에 각자 접속해 사용할 수 있다. 문제는 어떤 자료가 어디로 흘러 들어가는지 통제할 방법이 마땅치 않다는 점이다.

반면 가상 PC 쪽은 정반대의 문제를 안고 있다. 인터넷 자체가 차단되어 있어 AI를 아예 쓸 수가 없다. 결국 민감한 자료를 다루는 업무에서 오히려 AI의 도움을 받지 못하는 아이러니가 벌어진다. 그러다 보니 담당자들은 업무 효율을 위해 개인 휴대전화나 개인 PC로 우회하게 된다.

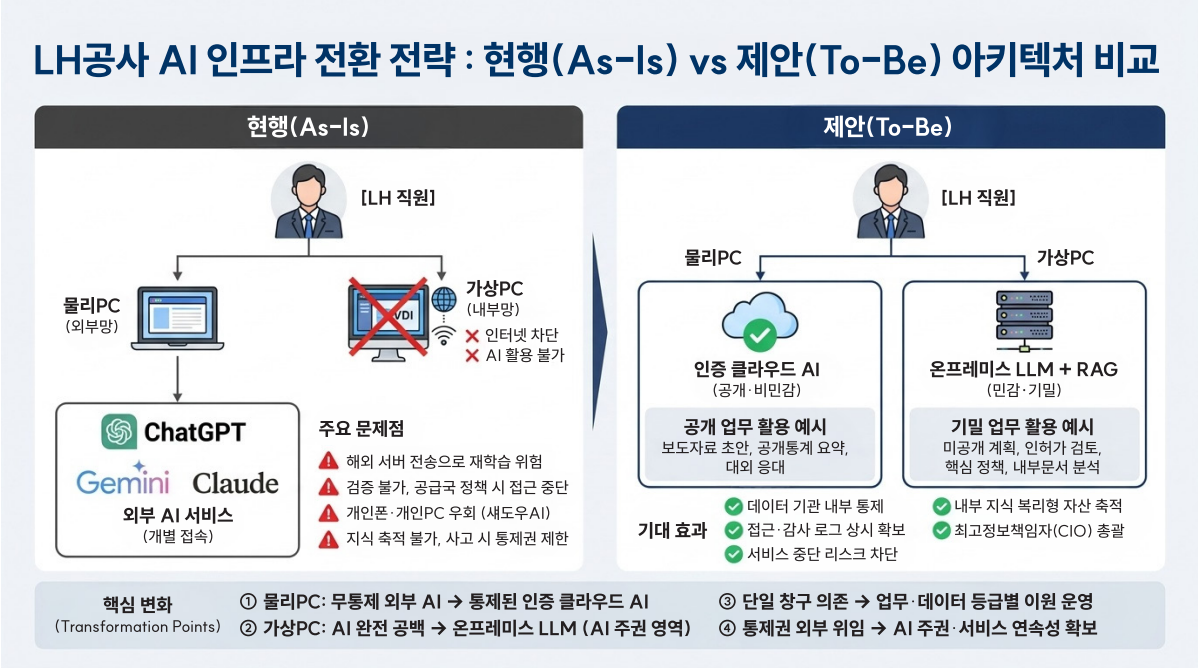


그림-4 LH의 AI 사용 환경, 이렇게 바뀔 수 있다

출처 : 생성형 AI로 작성

앞서 언급한 섀도우 AI의 유혹에 자연스럽게 노출되는 것이다.

여기서 흥미로운 점 하나를 짚어야 한다. LH의 가상 PC 환경은 이미 인터넷과 완전히 격리된 폐쇄망 조건을 갖추고 있다. 사실 자체 AI를 구축할 때 가장 어렵고 비용이 많이 드는 부분이 바로 이 폐쇄망을 만드는 일이다. 그런데 LH는 이미 그 조건을 절반 이상 갖추고 있는 셈이다.

따라서 방향은 이렇게 정리할 수 있다. 물리 PC 쪽에서는 공개된 자료 기반의 대민업무 등에 인증받은 클라우드 AI를 활용하도록 정돈한다. 가상 PC 쪽에서는 비공개 내부 자료를 활용한 업무를 자체 구축 AI로 채운다. 이렇게 하면 기존 보안체계는 그대로 유지하면서도, 업무 영역별로 알맞은 AI 지원을 제공할 수 있는 구조가 완성된다.

AI는 반복을, 사람은 판단을

AI 도입은 개인의 업무 방식뿐 아니라 조직의 직무 설계 자체를 다시 그리는 계기가 된다.

그동안 반복되던 업무들은 AI가 상당 부분을 자동화할 수 있다. 그 결과 담당자의 업무 비중은 자연스럽게 이동한다. 자료를 모으고 정리하는 단계에서, 결과를 검토하고 정책적 파급효과와 법적 책임, 윤리적 타당성을 판단해 최종적으로 결정하는 단계로 옮겨가는 것이다.

결국 이 과정에서 AI는 반복과 처리를 전담하고, 사람은 판단하고 책임지는 구도로 변화할 것이다. 이러한 역할 변화는 자연스럽게 조직 운영의 재정비도 요구하게 된다.

재설계된 운영구조 속에서 AI는 시간이 지날수록 점점 더 큰 가치를 만들어 낸다. 내부망에 축적되는 문서와 지식이 늘어날수록 답변의 정확도와 맥락 이해도가 함께 높아지기 때문이다. 이른바 '지식 복리형 엔진'의 성격을 지니는 것이다.

여기에 더해 조직의 경험과 노하우가 AI에 쌓인다는 것은 인사이동이나 퇴직으로 인해 조직의 지식이 끊어지는 것을 완화한다는 뜻이기도 하다. 따라서 자체 AI의 구축은 기관의 지적 자산을 안정적으로 이어갈 수 있는 통로가 되는 셈이다.

공공기관, 이제 수요자가 아니라 검증자다

마지막으로 짚을 것은 공공기관 스스로의 역할 변화다. 공공기관은 그동안 주로 IT 서비스를 구매해 쓰는 수요자 역할에 머물러 왔다. 그러나 AI 시대에는 그 역할이 한 단계 확장될 필요가 있다.

이유는 분명하다. 방대한 내부 문서와 정책 데이터를 이미 보유하고 있는 공공기관은, 폐쇄망 AI를 실증하기에 어느 조직보다도 유리한 조건을 갖추고 있기 때문이다. 전력 효율은 어떤지, 보안 격리는 잘 되는지, 실제 업무에 얼마나 유용한지 등을 공공기관이 먼저 검증해 낸다면, 다른 기관들이 참고할 수 있는 '표준 공공 AI 모델'을 정립하는 계기가 될 수 있다. ✦

부록 이 글을 읽을 때 알아두면 좋은 용어

AI 주권 (AI Sovereignty)
한 국가나 기관이 AI를 '필요할 때, 원하는 방식으로' 쓸 수 있는 권리다. 단순히 좋은 AI를 만드는 것이 아니라, 외부의 정책이나 서비스 중단에 흔들리지 않고 데이터와 모델을 스스로 통제할 수 있는 상태를 뜻한다. 공공 영역에서는 특히 서비스 연속성과 데이터 관할권이 핵심이다.

생성형 AI (Generative AI)
글, 그림, 코드, 음성 등을 새로 만들어 내는 AI다. 기존 AI가 주로 '분류'나 '예측'을 했다면, 생성형 AI는 사람처럼 새로운 결과물을 만들어 낸다. 챗지피티, 클로드, 제미나이가 대표 사례다.

LLM (Large Language Model, 거대 언어 모델)
방대한 양의 문서를 학습해 사람의 언어를 이해하고 생성하는 모델이다. 생성형 AI의 '두뇌'에 해당한다. 파라미터(매개변수) 수가 클수록 표현력이 풍부한 편이지만, 그만큼 운영에 필요한 자원도 커진다.

오픈소스 AI (Open Source AI)
설계도(모델 가중치·코드)가 공개된 AI다. 누구나 내려받아 자신의 서버에서 돌릴 수 있고, 필요에 맞게 고쳐 쓸 수도 있다. 대표적으로 라마(Llama), 미스트랄(Mistral), 큐원(Qwen) 계열이 있다. 공공기관이 '직접 갖추는 AI'를 만들 때 출발점이 된다.

상용 AI (Commercial AI)
민간 기업이 서비스 형태로 제공하는 AI다. 챗지피티, 클로드, 제미나이가 여기 속한다. 성능은 우수하지만 데이터가 외부 서버로 전송되고, 요금·약관·서비스 지속 여부를 사용자가 결정할 수 없다.

온프레미스 (On-Premises)
AI 모델과 데이터를 외부 클라우드가 아닌 기관 내부의 서버에 두고 운영하는 방식이다. 은행 금고에 비유할 수 있다. 자료를 밖으로 내보내지 않고 내부에서만 다루기 때문에 보안 통제가 강하다. 대신 서버·전력·인력을 스스로 마련해야 한다.

클라우드 AI (Cloud AI)
외부 사업자의 데이터센터에 있는 AI를 인터넷으로 이용하는 방식이다. 초기 투자 없이 바로 쓸 수 있어 편리하지만, 자료가 외부로 나가는 구조라 보안 등급이 높은 업무에는 제약이 있다.

인증 클라우드 AI
정부가 정한 보안 기준(예: 클라우드보안인증 CSAP)을 통과한 클라우드 서비스에서 제공되는 AI다. 일반 상용 AI보다 통제 수준이 높아 공공기관의 준민감 업무에 활용할 수 있다.

하이브리드 전략 (Hybrid Strategy)
모든 업무를 하나의 AI로 처리하지 않고, 자료의 민감도에 따라 클라우드 AI와 온프레미스 AI를 나눠 쓰는 방식이다. 공개·비민감 업무는 외부 AI로 빠르게, 민감·기밀 업무는 내부 AI로 안전하게 처리한다.

RAG (Retrieval-Augmented Generation, 검색 증강 생성)
AI가 답을 만들기 전에 기관 내부 문서를 먼저 찾아본 뒤 그 내용을 근거로 답하게 하는 기술이다. '오픈북 시험'에 비유할 수 있다. 모델을 새로 학습시키지 않아도 최신 규정이나 내부 자료를 반영할 수 있어, 공공기관에서 특히 유용하다.

파인튜닝 (Fine-tuning)
이미 학습된 모델에 특정 분야의 자료를 추가로 학습시켜 그 분야에 맞게 조정하는 작업이다. RAG가 '자료를 찾아 답하는' 방식이라면, 파인튜닝은 '모델 자체를 그 분야 전문가로 다시 훈련'하는 방식이다.

섀도우 AI (Shadow AI)
기관의 공식 승인 없이 직원이 개인 판단으로 외부 AI를 업무에 사용하는 현상이다. 편리함 때문에 널리 퍼지지만, 내부 자료가 외부 서버로 흘러가도 조직이 파악하기 어렵다. 데이터 통제권을 잃는 가장 흔한 경로다.

에어갭 (Air-gap, 망 분리)
외부 인터넷과 물리적으로 끊어 놓은 폐쇄망을 말한다. 자료가 외부로 나갈 통로 자체가 없기 때문에 보안 수준이 매우 높다. LH의 가상 PC 환경이 여기에 해당한다.

FedRAMP (Federal Risk and Authorization Management Program)
미국 연방정부가 클라우드 서비스의 보안을 심사·인증하는 제도다. 공공기관이 클라우드 AI를 쓰려면 이 인증을 통과한 서비스만 사용할 수 있다. 한국의 CSAP와 성격이 비슷하다.

AI법 (EU AI Act)
유럽연합이 2024년 확정한 세계 최초의 포괄적 AI 규제법이다. AI를 위험 등급으로 나누고, 고위험 AI에는 투명성·감독 의무를 강하게 부여한다. 공공서비스에 AI를 쓸 때도 엄격한 기준을 적용한다.

GDPR (General Data Protection Regulation, 유럽 일반개인정보보호법)
유럽연합의 개인정보 보호법이다. 개인 자료가 어디에 저장되고 누구에게 넘어가는지를 엄격하게 통제한다. 유럽 각국이 자체 AI 인프라(소버린 클라우드)를 키우는 배경 중 하나다.

소버린 클라우드 (Sovereign Cloud)
자국 영토 안에 두고, 자국 법의 적용만 받는 클라우드 인프라다. 자료의 국외 이동을 원천 차단한다는 점에서 '데이터 주권'을 지키는 수단이다. 프랑스의 Bleu·S3ns, 독일의 Delos Cloud 등이 대표적인 사례다.

TCO (Total Cost of Ownership, 총소유비용)
어떤 시스템을 도입해 운영할 때 5년, 10년 등 일정 기간에 들어가는 모든 비용을 합산한 값이다. 초기 구축비뿐 아니라 전력·유지보수·인건비까지 포함한다. 클라우드 AI와 온프레미스 AI의 경제성을 비교할 때 사용된다.

GPU (Graphics Processing Unit)
원래 그래픽 처리를 위한 반도체였지만, 지금은 AI 학습·추론에 없어서는 안 될 핵심 장비다. LLM을 자체 운영하려면 고성능 GPU가 다수 필요하고, 전력·냉각 인프라도 함께 갖춰야 한다.

거버넌스 (Governance)
AI를 언제·어디서·누구의 책임으로 쓸지 정하는 조직 내 규칙과 의사결정 체계다. 기술 그 자체보다 오히려 이 부분이 흔들리면 AI 도입이 실패한다. 가이드라인, 평가 체계, 로그 관리 등이 모두 포함된다.

참고 자료

- 소프트웨어정책연구소. (2026).「2025년 공공부문 AI 도입현황 연구」
- 디지털플랫폼정부위원회·한국지능정보사회진흥원. (2025).「공공부문 초거대 AI 도입·활용 가이드라인 2.0」
- NIST. (2024). Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (NIST AI 600-1)
- Office of Management and Budget. (2024). M-24-10: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence.
- FedRAMP. (2025). AI Prioritization. https://www.fedramp.gov/ai/
- Anthropic. (2026). Statement on the US government directive to suspend access to Fable 5 and Mythos 5.
- axios.com. (2026.7.8), Scoop: Trump administration lifts restrictions on OpenAI's GPT 5.6, https://www.axios.com/2026/07/08/openai-gpt-trump-ban-lifted
- The Verge. (2026). Inside the fight over Claude Mythos 5.
- Business Insider. (2026). Anthropic's new models were restricted by the US. Europe's top AI startup has been waiting for this moment.
- Smart Nation Singapore. (2023). National AI Strategy 2.0. https://www.smartnation.gov.sg/initiatives/national-ai-strategy/
- AI Singapore. (2025). SEA-LION: Southeast Asian Languages in One Network. https://sea-lion.ai/
- CNBC (2026.5.19.) Singapore inks AI deals with Google, OpenAI as ChatGPT-maker commits $234 million to local ecosystem
- European Commission. (2024). AI Act
- Meta AI. (2024). Introducing Llama 3.1: Our most capable models to date.
- Mistral AI. (2024). Large Enough: Mistral Large 2.
- Anthropic. (2025). How we built our multi-agent research system.
- OpenAI. (2026). API Pricing: GPT-5.6. https://openai.com/api/pricing/(2026.6.16.기준)
- NVIDIA. (2025). NVIDIA H200 Tensor Core GPU Specifications.
- Lewis, P. et al. (2020). Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks. NeurIPS 2020.

편집인 최상희 선임연구위원(urban@lh.or.kr)

편집장 양홍석 수석연구원(h.yang@lh.or.kr) **발행인** 김용운 **발행처** LH 토지주택연구원

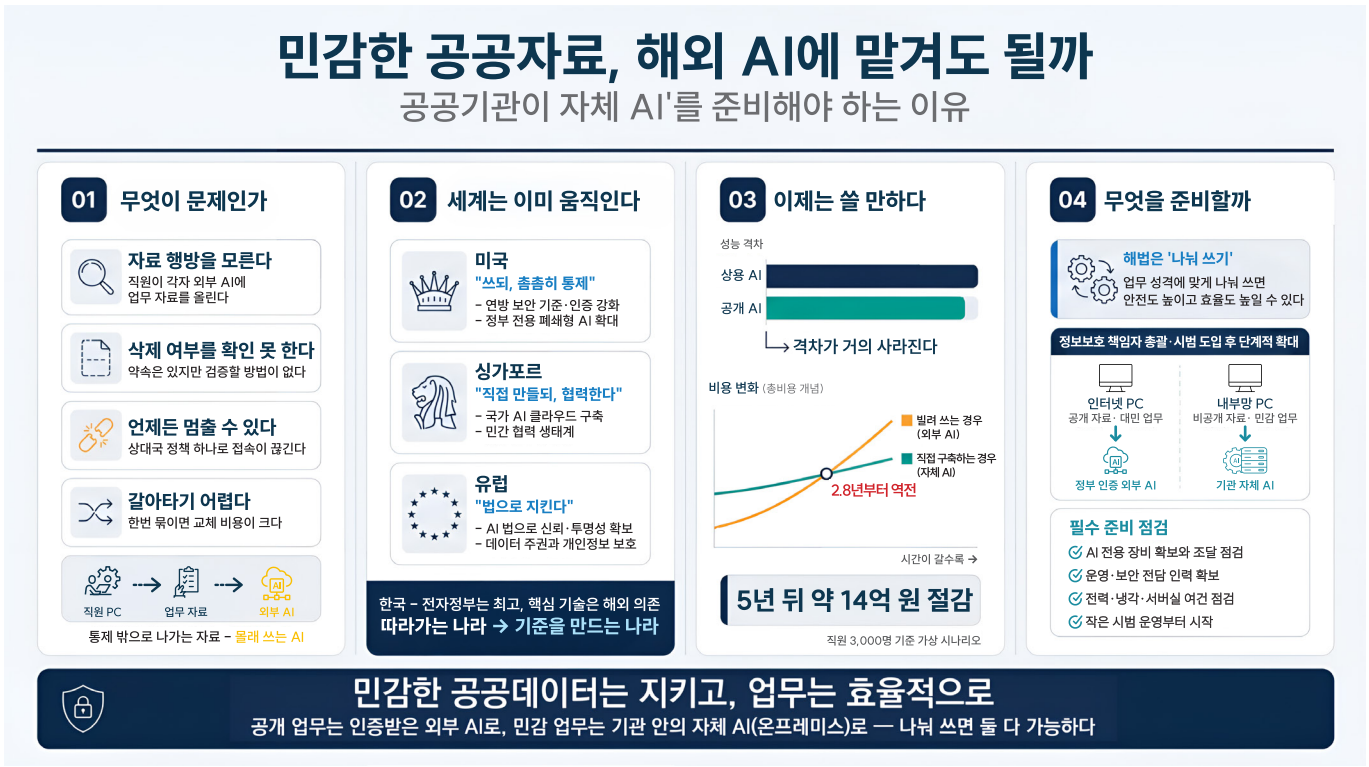
LHRI-FOCUS
vol.84_2026. 8. 18.

민감한 공공자료, 해외 AI에 맡겨도 될까

공공기관이 '자체 AI'를 준비해야 하는 이유

이상훈 연구위원

- 정부와 공공기관의 생성형 AI 활용이 빠르게 확산되고 있으나, 민감한 행정 자료의 안전한 처리 방안은 여전히 미해결 과제
- 해외 AI에 대한 의존이 지속될 경우, 상대국의 정책 변화 한 번으로 서비스가 중단되거나 자료의 유출 경로조차 파악하기 어려운 상황이 발생할 우려
- 공공 AI의 핵심은 최신 모델의 선제적 도입이 아니라, 필요한 순간 우리 손으로 활용할 수 있는 체계, 즉 'AI 주권'의 확보에 있음
- 모든 업무를 자체 AI로 전환하기보다는, 공개 업무는 외부 AI를 활용하고 민감 업무는 기관 내부에서 직접 운영하는 이원화 전략이 현실적 대안
- 최근 무료 공개 AI가 상용 수준까지 발전하면서, 장기적으로는 직접 구축이 비용 면에서도 더 유리해지는 국면에 진입



2025 _ 2026 LHRI-FOCUS

호수	제목	대표저자	발간일
62	• 비주택 리모델링 사업의 동향과 추진여건	송상훈 연구위원 박윤재 연구원	2025.09.01
63	• 해외국가를 통해 본 미래도시의 공간혁신 방향 • 도시혁신·공간문화를 이끄는 LH의 시대적 소명	윤정란 연구위원 김주진 연구위원	2025.09.29
64	• 2030 청년 1인가구가 원하는 집은?	정소이 연구위원	2025.10.27
65	• 공동주택 주차난, 오토발렛이 해법이 될 수 있을까?	배연희 책임연구원	2025.11.17
66	• 지방이 답이다. : 독일 히든 챔피언에서 찾은 지역균형발전 해법	이삼수 팀장	2025. 11. 24
67	• 속도와 사업성을 키운 도심공공주택복합사업 시즌2 : 규제완화 성과와 남은 과제들	김옥연 연구위원	2025.12. 24
68	• "왜 화성에는 탐사를 넘어 도시가 논의되는가"	김명인 책임연구원 손희주 책임연구원	2026.01.19
69	• 일본 도시정비사업의 재개발회사 역할 및 시사점	임정민 연구위원	2026.01.19
70	• 고령인구 천만시대 돌봄·의료·일자리·주거 연계 전략 제언	최상희 선임연구위원 김경미, 이봉조 책임연구원	2026.01.26
71	• 공공분양주택 완전정복+(PLUS) 신혼부부라면 반드시 알아야 할 청약 기본상식	이훈 책임연구원	2026.02.09
72	• 은퇴자 마을에 살려면 얼마가 필요할까?	정연우 연구위원	2026.02.23
73	• 로봇 경비원?	남성훈, 양홍석 수석연구원	2026.03.09
74	• 취임 이후 9개월, 대통령 부동산 메시지	양홍석 수석연구원	2026.03.23
75	• 공공분양 맞아? 84타입의 반전	손희주, 박민국 책임연구원, 김남정 연구위원	2026.04.06
76	• 도시의 나무들이 품고 있던 탄소 120만 톤, 6년의 추적 끝에 밝혀 내다	이은엽 연구위원, 이정민 실장, 김영민 전임연구원	2026.04.20
77	• AI·반도체가 키운 전력난, SMR이 답이 될까	이정민 실장, 이은엽 연구위원, 최종수 연구위원, 김명인 책임연구원	2026.05.04
78	• 세상에 이런 집이?	최상희 선임연구위원, 이정은, 박민국 책임연구원, 최대식 연구위원	2026.05.04
79	• 우리는 정말 균형발전을 하고 있나	정창무 원장 , 한혜숙 차장, 손희주 책임연구원	2026.06.08
80	• 땅은 국가가, 집은 국민이	최상희 선임연구위원, 김경미 책임연구원, 장진혁 책임연구원	2026.06.15
81	• 반세기가 흘러도 늙지 않는 신도시	이영환 연구위원, 임정민 연구위원	2026.07.06
82	• 빈집을 다시 보다	문준경 수석연구원	2026.07.20
83	• 땅속 배관, 덜 파고 더 안전하게 묻다	이수규 수석연구원, 윤정원 책임연구원, 박종배 선임연구위원	2026.08.03

※ 제목을 클릭하면 해당 호수의 포커스를 보실 수 있습니다.

LH 토지주택연구원