공공 AI 전환지원센터

2026-01
AX ISSUE BLENDER

Transformer 모델 혁신과 AI Full Stack 중심의 공공 AX 전략

NIA 한국지능정보사회진흥원

Transformer 모델 혁신과 AI Full Stack 중심의 공공 AX 전략

「 보고서 개요 」

○ Transformer 아키텍처의 등장('17, Google Brain) 이후 **Generative AI의 폭발적인 성장**이 가속화, **공공·행정 분야**에서도 **본격 확산**

※ **(에스토니아 정부)** X-Road 플랫폼에 AI 통합, 기관 데이터 연계 75% 자동화

※ **(덴마크 코펜하겐시)** AI 도시 관제로 행정 운영비 연 12% 절감

○ AI 서비스 특성에 따라, AI Transformation은 **기존 사업 모델, 수행 방식과는 다른 접근**으로의 **공공 서비스 구현과 운영**을 요구

※ **(구현 전략)** "사업 단위 납품" → "플랫폼 기반 서비스 설계"

※ **(운영 인프라)** "정적 시스템" → "동적 AI 파이프라인"

※ **(AI 솔루션)** "단순 자동화 도구" → "업무 지능화 파트너"

※ **(거버넌스)** "사후 규제" → "내재화된 책임 설계"

○ 성공적 AX는 **❶AX 대상·서비스, ❷AX 구현, ❸AX 운영·거버넌스**의 3요소가 **통합**할 때 비로소 작동

① AX 대상·서비스	↔	② AX 구현	↔	③ AX 운영·거버넌스
◆ **(방향)** 무엇을 AI로 전환할 것인가? (예: 업무, 서비스, 의사 결정, 프로세스, 고객 접점 등)		◆ **(방향)** 어떻게 AI를 구축·적용할 것인가? (예: 데이터, 모델, 인프라, 시스템, RAG, 에이전트 등)		◆ **(방향)** 어떻게 AI를 운영·관리할 것인가? (예: 보안, 모니터링, 품질, 책임성, 조직, ROI 등)

○ 본 보고서에서는 **총 7단계**로 구성된 **AI Full Stack 중심의 AX 방법론**을 제시하고, 그에 따른 **도입 전략**을 안내

※ **[단계]** 목표 정의(Define) → Data 정립(Discover) → Data 운영 방안 설계(Develop) → AX 투자 모델 수립(Design) → AI Full Stack 구성(Deploy) → 서비스 제공 채널 선택(Deliver) → AX 활용 진단·모니터링(Diagnose) → (환류)

○ 결론적으로 공공 AX는 단편적 AI 솔루션 도입이 아닌, **AI Full Stack**(인프라·데이터·모델·오케스트레이션·응용 등) 관점에서 **표준화, 종속 회피, 민첩 대응**이 가능한 방향으로의 접근이 핵심

□ **(Transformer 아키텍처의 등장)** **Transformer 아키텍처**는 **전역적 문맥 모델링***을 가능케 하는 **신경망 구조**를 채택함으로써, 현재 Generative AI의 폭발적 성장을 견인

* 문장을 읽을 때 모든 단어가 동시에 서로를 바라보며 문맥을 파악하는 구조로, 모든 위치 간의 관계를 동시에, 그리고 직접 계산함으로써 이해·예측 극대화

※ **(참고)** 기존 RNN이 앞부터 순서대로 읽는 "책 읽기"라면, Transformer는 페이지를 펼쳐놓고 "형광펜으로 관련 단어들을 동시에 밑줄" 긋는 방식

○ Google Brain 팀은 "Attention Is All You Need(2017)"를 통해 **Transformer 모델**을 제안, 현재 **대규모 언어 모델의 토대**로 작용

※ **(논문 핵심)** 어텐션(Attention) 메커니즘을 통해 RNN 등 기존 순차적 모델의 한계를 극복, 기계 번역과 자연어 처리 분야에서 성능을 혁신적으로 개선

○ 이는 이미 사회 전반에 도입, **혁신적 성과로 연결**되고 있으며, 다양한 산업뿐만 아니라 **공공·행정 분야**에서도 널리 활용 중

▸ **(에스토니아 정부)** X-Road 플랫폼에 AI 레이어를 통합, 정부 기관 간 데이터 연계 요청의 75%를 자동화

※ **(핵심 성과(체감도))** 한 명의 시민이 평균 3~5개 기관을 방문해야 했던 민원이 단일 창구에서 처리되었으며, 연간 행정비용 절감 규모가 GDP의 2% 해당 추산

▸ **(덴마크 코펜하겐시)** AI 도시 인프라 관제 시스템을 통해 신호등 최적화, 쓰레기 수거 경로 자동화, 노면 파손 예측 점검 일원화

※ **(핵심 성과(체감도))** 시 행정 운영비용을 연간 약 12% 절감, 시민 불편 신고 처리 속도를 기존 평균 72시간에서 약 8시간으로 단축

○ 특히 **공공 부문**에서는 **서비스의 구현 전략, 운영 인프라, AI 솔루션, 거버넌스** 등을 체계화하는 방식에서 다양한 변화 직면

▸ **(구현 전략)** "사업 단위 납품" → "**플랫폼 기반 서비스 설계**"

▸ **(운영 인프라)** "정적 시스템" → "**동적 AI 파이프라인**"

▸ **(AI 솔루션)** "단순 자동화 도구" → "**업무 지능화 파트너**"

▸ **(거버넌스)** "사후 규제" → "**내재화된 책임 설계**"

□ **(트렌드의 전환)** 이는 사용자로 하여금 **혁신(검색 편의, 업무 효율 향상)**을 유발하고 있으며, **데이터와 사람(활용)의 가치**는 더욱 중요

[트렌드 1] "검색에서 응답으로의 변화"

○ 기존 검색 엔진(Search Engine)은 질의어에 관련된 **웹사이트 링크 목록을 제공**하는 반면, 현재 환경(AX)에서는 **AI 에이전트**가 질문에 대한 **정확하고 구체적인 응답을 즉시 제공**

* **[AS-IS]** 검색어를 분석 및 웹페이지를 인덱싱해 우선순위 기반으로 나열 → **[TO-BE]** 자연어로 표현된 질문의 의도와 맥락을 이해하고, 복수의 정보원을 실시간으로 추론·종합하여 사용자 상황에 최적화된 응답을 즉시 생성

○ 이에 **"프롬프트 엔지니어링(Prompt Engineering)"**과 AI의 **작동 원리 및 한계**를 명확히 이해하는 것이 **핵심 역량**으로 부각

※ **(프롬프트 엔지니어링)** 대규모 언어 모델(LLM)에서 원하는 결과를 얻기 위해 지시문을 생성, 고품질 응답을 위해 지시문을 최적화하는 일련의 과정

[트렌드 2] "여러 명이 하던 일을 단 한 명이 수행"

○ 기존 여러 사람이 수행하던 복잡한 업무 프로세스, 대량의 반복 업무가 **AI 에이전트의 활용** 또는 **시스템의 통합**으로 인해 앞으로는 **한 명의 담당자만으로 해결** 가능

○ 민원 처리, 법·규제 대응, 소프트웨어 등 IT, 제조 공정 및 품질 관리 등 **산업의 전반을 아우르는 업무 영역**에 동일하게 적용

▸ **고객 서비스 센터 (Call Center)**

AX 이전 (N명)		AX 이후 (1명)	시사점
◆ 복수의 상담원이 단순/반복하여 문의 응대, 주문 접수 등	→	◆ AI 고객 서비스 센터가 90% 이상 문의 자동 처리 ◆ 1명의 관리자가 복잡한 경우 대응 및 총괄 관리	◆ AI가 수만 건의 정형화된 고객의 문의에 대응, 업무 효율 및 품질 개선

▶ 법률 및 규제 준수 (Legal & Compliance)

AX 이전 (N명)		AX 이후 (1명)	시사점
◆ 복수의 변호사 또는 직원이 수천 건의 계약서 검토 ◆ 법률 문서에서 특정 조항 수동 검색, 내부 규정 준수 여부 심사 등	→	◆ AI 기반 계약 검토 및 리스크 분석 솔루션 기반 검토, 이상 징후 자동 알림 ◆ 1명의 전문가가 AI 분석 결과 최종 승인 및 미비점 등을 보완	◆ AI가 대량의 비정형 텍스트 데이터(법률, 규제, 계약서 등)를 즉각 분석하는 등 필요 정보 추출 작업을 대체하여 인력 투입 최소화

▶ 소프트웨어 개발 및 IT 운영 (DevOps)

AX 이전 (N명)		AX 이후 (1명)	시사점
◆ 복수의 초급 개발자가 단순 코드 작성, 버그 수정, 테스트 Case 작성 등 S/W 엔지니어링 수행	→	◆ 생성형 AI 코딩 에이전트 (예: Code.i, CURSOR 등)가 코드 초안 생성 및 버그 요소 등을 제안 ◆ 1명의 고급 개발자가 최종 코드 검토 및 아키텍처 설계에 집중	◆ AI가 반복적이고 정형화된 프로그래밍 작업을 자동화, 인간 개발자는 더욱 창의적이며 복잡한 문제해결에 집중

▶ 제조 공정 및 품질관리 (Smart Factory)

AX 이전 (N명)		AX 이후 (1명)	시사점
◆ 복수의 작업자가 육안으로 제품 불량 검사, 장비 가동 데이터 수기 기록 및 분석	→	◆ AI Vision 검사 시스템과 제조 데이터 분석 플랫폼이 실시간 불량 감지하고, 예측 정비 ◆ 1명의 통합 관제사가 전체 공정 모니터링 및 대응	◆ AI가 센서·카메라 데이터를 실시간 분석, 우수한 정밀도로 문제를 예측·해결하여 인력 감축 및 비용 절감

○ 이러한 **N:1 효율화**는 단순히 인력을 줄이는 것을 넘어, **"업무의 성격 자체를 변화"**시킴으로써, **업무의 재설계(혁신)를 유도**

※ **[기존 N명 역할]** 대량 및 다양한 유형의 업무를 반복적 수행으로 해결
[향후 1명 역할] AI 에이전트의 운영자(Supervisor), 기획자(Strategist)로 역할

[트렌드 3] "기존 전문가의 암묵지보다는 데이터가 핵심"

○ 문제해결의 관점에서, 과거에는 **전문가의 경험과 직관**에 의존하는 것이 추세였다면, 이제는 **데이터를 활용**하는 것이 핵심

▸ [AX 도입 前] 주로 "전문가의 암묵지(Tacit Knowledge)"에 의존

구분	전문가의 암묵지	정형/비정형 Data
문제해결	◆ 압도적으로 우세	◆ 각종 이유(데이터 수준, 분석·활용 수준 등)에 따라 제약적
강점	◆ 복잡·비정형적인 문제, 선례가 없는 새로운 상황에서 직관과 경험, 맥락적 이해를 통해 신속한 판단과 해결이 가능	◆ 정형화된 문제나 반복 작업에 대한 통계적, 규범적 해결
약점	◆ 경험에 의존하므로 객관성과 일관성이 부족, 전파 속도↓	◆ 데이터가 누락되거나 단절된 경우, 오류가 생성되어 문제해결에 한계 직면
시사점	◆ 암묵지(실력·경험)를 가진 전문가가 조직 핵심 문제를 해결	◆ 주로 사실 확인이나 결과의 기록 등 용도로 데이터를 사용

▸ [AX 도입 後] 높은 정확도를 위해 "데이터 + AI 솔루션"에 의존

구분	전문가의 암묵지 + 지시문 작성	정형/비정형 Data + AI 솔루션
문제해결	◆ 특정 영역(윤리·감성·창의적 문제해결의 영역)에서 필수	◆ 대부분 영역에서 우세 (빠르며, 정확한 문제해결 가능)
변화된 역할	◆ 非 데이터 영역의 통찰, AI 결과에 대한 최종 검토 및 책임, AI에 대한 지시문(Prompt) 작성	◆ 방대한 데이터와 암묵지의 형식화를 통해 학습하며, 정확하고 일관된 예측과 자동화된 해결책을 도출
새로운 강점	◆ 창의성, 윤리적 판단, 감성적 상호작용 등 AI가 모방하기 어려운 고차원적 문제 집중	◆ 처리 속도, 규모, 일관성에서 인간을 압도하며, 잠재적 위험 예측 등 어려운 패턴 분석·해결
시사점	◆ 암묵지를 가진 전문가는 20%의 복잡하고 새로운 문제에 집중	◆ AI 솔루션은 80% 가량의 문제를 빠르고 정확하게 해결

○ AX 시대에 문제해결의 승자를 선정한다면, **"데이터와 결합하여 명시화된 암묵지까지 보유하고 있는 AI 솔루션"**으로 귀결

※ **(참고)** AI는 기본적으로 전문가 암묵지(Tacit Knowledge)의 학습을 넘어, 이 중 핵심 정보의 패턴을 형식지(Explicit Knowledge)로 변환, LLM을 통해 비정형 데이터와 맥락까지 이해·통합하여 방안 제시

[트렌드 4] "온프레미스 → 클라우드로의 전환 가속화"

○ **Transformer 중심 AI 확산**은 단순한 소프트웨어 도입을 넘어, 공공·민간을 막론하고 **IT 인프라 운영 방식**의 **근본적 전환** 유도

※ **(연산 수요 폭증 및 탄력적 활용 요구)** 단일 LLM 추론(Inference)에 수십~수백 개의 GPU가 요구되고, 사용량의 변동성이 커 자원 활용의 탄력성 필요

※ **(Foundation Model의 API 化)** OpenAI, Google, Anthropic, Meta 등 주요 AI 기업들이 최신 Transformer 모델을 클라우드 API 형태로 제공하는 추세

※ **(참고)** "Anthropic의 'Claude 3'은 클라우드 API를 통해서만 제공", "OpenAI의 GPT-4를 포함한 주요 Foundation Model은 클라우드 API 형태로만 제공" 등

○ 크게 **'대규모 데이터 처리·저장 용이성', '고성능 컴퓨팅 자원 탄력성', 'AI/ML 개발 생태계 제공'**을 전환의 촉진 요소로 언급*

* **(참고문헌)** Magic Quadrant for Cloud AI Developer Services (Gartner, 2024), AI Index Report 2024 (Stanford University HAI, 2024) 등

▶ [요소 1] 대규모 데이터 처리 및 저장 용이성

온프레미스 한계	클라우드 이점	시사점
◆ 기관이 자체적으로 수십 페타바이트(PB)에 달하는 데이터 저장소와 이를 처리할 고성능 네트워크를 구축하고 유지는 데에 상당한 초기 투자(CAPEX) 비용과 관리 인력 필요	◆ CSP에서 제공하는 객체 저장소에 방대한 양의 데이터를 저렴하게 보관·관리 가능 ◆ 각종 방대한 데이터의 "수집-정제-전처리"를 위한 통합 관리 가능 제공	◆ AI 모델, 특히 LLM 모델은 대규모의 정형 및 비정형 데이터를 학습해야 높은 성능을 보장 ◆ 방대한 데이터의 양을 보관·처리하는 데 클라우드 최적

▶ [요소 2] 고성능 컴퓨팅 자원 확보의 탄력성

온프레미스 한계	클라우드 이점	시사점
◆ 고성능 GPU 서버를 구축하는 데는 높은 비용이 발생 ◆ 한 번 구축하게 되면 AI 모델의 학습 기간 외에는 자원이 유휴 상태가 되기 때문에 비효율이 극대화	◆ 클라우드는 필요할 때만 고성능 GPU/TPU 자원을 빌려 쓰는 것이 가능 (pay-as-you-go) ◆ 학습이 끝나면 즉시 반환할 수 있어 운영비용(OPEX)의 최적화가 가능	◆ AI 모델의 Training & Validation 과정은 막대한 연산 자원(GPU, TPU)을 필요로 하므로, 자원 활용 탄력성(Elasticity)이 매우 중요

▶ [요소 3] AI/ML 개발 생태계 제공

온프레미스 한계	클라우드 이점	시사점
◆ AI 시스템의 직접 구축(Build)이 필요하므로, 구축 업체 선정 및 계약, 이후 운영 유지보수 계약 체결 등 AI 전환에 상당한 시간 소요와 행정 업무가 수반 ◆ MLOps 사이클을 온프레미스에서 구현하려면 전문 인력, 인프라 구축 비용이 기하급수적으로 증가	◆ MLOps(Machine Learning Operations) 플랫폼, Pre-trained AI 모델 API, 데이터 라벨링 도구 등 AI 개발에 필요한 모든 도구와 서비스를 통합하여 제공 ◆ 클라우드는 전 주기를 관리형 서비스(Managed Service)로 제공해 조직이 인프라 관리 대신 AI 서비스 품질에 집중하도록 지원	◆ AI 시스템을 직접 '구축(Build)'하는 대신 클라우드 서비스를 '활용(Buy)'하여 AI 전환 속도를 획기적으로 개선

[트렌드 5] "AI도 중요하나, 사람이 AI를 잘 활용하는 것이 더욱 중요"

○ AI 솔루션은 AI를 활용하기 위한 **"도구이자 기초 기술"**이나, 서비스의 경쟁력과 혁신을 좌우하는 것은 AI 솔루션을 **문제 해결 상황에 어떻게 적용하여 활용**하는지에 따라 결정

▸ AI 솔루션은 필수 도구로, 학습·예측·분류·생성 등 업무에 적용

AI 솔루션 주요 기능	AI 솔루션 주요 특징
◆ **(학습(Learning))** 대규모 데이터로부터 패턴을 스스로 학습, 규칙 없이도 판단 ◆ **(예측(Prediction))** 과거 데이터 기반으로 미래 상태·수요·리스크를 사전에 산출 ◆ **(분류(Classification))** 민원·문서·이미지 등 비정형 데이터를 자동으로 범주화 ◆ **(생성(Generation))** 자연어를 기반으로 보고서, 민원 답변, 정책 초안 자동 작성	◆ **(범용성)** 단일 Foundation Model이 번역·요약·분류 등 복수 업무 동시 수행 ◆ **(확장성)** 클라우드 API 연동으로 추가 개발 없이 기능 고도화, 서비스 확장 ◆ **(자동화)** 반복적·규칙적 업무를 자율 수행해 인력을 고부가 업무로 재배치 ◆ **(학습 지속성)** 신규 데이터 투입으로 모델이 지속 개선되는 자기 발전 구조

▸ 성공적인 AX를 위해서는 명확한 '목표 설정', '가치 수립' 중요

구분	AI 활용의 일반적인 방향성		AI 활용 혁신을 위한 구체적 방향성
목표	◆ 더욱 빠르고, 정확한 계산과 예측, 분류/식별 등을 달성	→	◆ **구체적 달성 목표 :** 특정 문제의 해결, 수익 증대, 비용 절감, 업무 효율 개선 등
가치	◆ 우수한 기술 수준을 바탕으로 선도적인 AI 서비스 제공 등	→	◆ **구체적 달성 가치 :** 특화 데이터 확보, 도메인 지식 축적, 사용자 경험 확보, 新 서비스 창출 등

○ 따라서 "기존 **알고리즘 중심**에서, **AI를 서비스에 통합·적용**하기 위한 **전략가·실행가 중심**으로의 패러다임 전환" 중요

※ **(AI 활용과 경험의 최적화)** 예로, 챗봇 서비스의 정확도 개선, 제조 공정의 불량률 감소 등의 혁신 목표는, 결국 AI 솔루션의 영향보다도 사용자(고객)에게 얼마나 더 나은 경험을 제공하는지에 대한 여부로 귀결

※ **(데이터와 도메인 지식의 결합)** 아무리 뛰어난 알고리즘이라도, 양질의 특화 데이터와 특정 산업 분야의 깊은 통찰력(도메인 지식) 없이는 혁신 한계

□ **(AI Transformation 정의와 구성요소)** 성공적 AX를 위한 추진 프레임워크는 **AX 대상과 구현, 운영 등 3단계의 계층**으로 수렴

※ **(참고)** OECD(2026)는 공공 부문의 AI 전환을 '정책·서비스 설계', 'AI 시스템 구현', '책임 있는 운영 및 거버넌스' 요소의 결합으로, Databricks(2025)는 '비즈니스 프로세스 혁신', '데이터·AI 플랫폼 구축', '거버넌스 및 운영체계' 등 요소의 조합으로 정의

① AX 대상·서비스	↔	② AX 구현	↔	③ AX 운영·거버넌스
◆ **(방향)** 무엇을 AI로 전환할 것인가? (예: 업무, 서비스, 의사결정, 프로세스, 고객 접점 등) ◆ **(구성요소)** - 고객 경험 - 운영 및 생산성 - 제품 및 서비스		◆ **(방향)** 어떻게 AI를 구축·적용할 것인가? (예: 데이터, 모델, 인프라, 시스템, RAG, 에이전트 등) ◆ **(구성요소)** - AI as a Service - AI Infra - AI Governance		◆ **(방향)** 어떻게 AI를 지속 운영·관리할 것인가? (예: 보안, 모니터링, 품질, 책임성, 조직, ROI 등) ◆ **(구성요소)** - Active Learning - MLOps - Compliance

① AX 대상·서비스

○ **'고객 경험(Customer Experience)'**이란 AI 활용을 통해 고객 **상호작용**과 **여정 전반**을 혁신하고, **극대화된 가치**와 **맞춤화된 경험을 제공**하는 요소로 정의

▶ **[대상·서비스 1] 개인화 추천 (초개인화: Hyper-personalization))**

· AI 추천 엔진을 통해 고객의 행동, 선호도, 맥락을 분석하여 상품, 콘텐츠, 서비스를 실시간으로 맞춤 제공

▶ **[대상·서비스 2] 지능형 고객 서비스**

· AI 챗봇, 음성 인식, 감정 분석 등 기능을 통해 365일 응대 및 빠르고 정확한 문제해결 제공 (콜센터 자동화, FAQ 자동 응답 등)

▶ **[대상·서비스 3] 수요 예측 및 가격 최적화**

· AI를 이용하여 시장 수요를 정확히 예측하고 동적 가격 책정(Dynamic Pricing)을 적용하여 고객 만족도와 수익을 동시 확보

○ **'운영 및 생산성(Operations & Productivity)'**이란 AI 활용을 통해 **기업 내부 프로세스의 효율성, 속도, 정확성을 혁신적으로 개선**하는 요소로 정의

▸ **[대상·서비스 1] 프로세스 자동화**

· RPA(로봇 프로세스 자동화)를 넘어 지능형 자동화를 도입, 의사결정이 필요한 복잡한 사무 업무까지 자동화

▸ **[대상·서비스 2] 공급망 및 제조 공정 최적화**

· AI 수요 예측, 재고 관리, 물류 경로 최적화, 제조 공정의 비전 검사를 통한 불량률 최소화 및 예지 보전(Predictive Maintenance)

▸ **[대상·서비스 3] 내부 지식 관리**

· 임직원의 방대한 암묵지(Tacit Knowledge)와 문서를 AI로 명시화하고, 검색이 가능하게 하여 업무 효율과 협업을 증진

○ **'제품 및 서비스(Products & Services)'**란 기존 제품과 서비스에 **AI 기능을 내재화**하거나, **AI 기반의 완전히 새로운 제품 또는 서비스를 창출**하는 요소로 정의

▸ **[대상·서비스 1] AI 기능 탑재**

· 기존 소프트웨어, 하드웨어, 앱 등에 AI 기능을 통합·탑재함으로써 사용자에게 새로운 가치 제공
(예: 지능형 검색 기능, AI 기반 디자인 보조 도구)

▸ **[대상·서비스 2] 생성형 AI 기반 비즈니스 모델 창출**

· Generative AI(생성형 AI)를 활용한 콘텐츠 생성, AI 기반 진단·분석 솔루션 등 이전에는 없었던 새로운 비즈니스 모델을 발굴

▸ **[대상·서비스 3] 데이터 기반 의사 결정**

· AI 분석을 바탕으로 얻은 깊은 통찰력(Insight)을 제품 개발 및 서비스 개선 주기에 반영하여 지속적인 혁신 동력으로 활용

② AX 구현

○ **'AI as a Service'**란 인프라, 서비스 요소, 응용 서비스와 같은 **AI 기능·자원**을 **클라우드 형태로 구현**, 사용자에게 **On-Demand 형식으로 제공**하는 서비스 방식을 의미

▸ **[구현 요소 1] 데이터 엔진 (Data Engine)**

· **(목적·구성)** AI 모델이 학습할 수 있는 양질의 데이터를 확보

· **(데이터 추출·수집)** 센서, 로그, 웹, DB 등 에서 데이터 추출·통합

· **(데이터 저장소)** 중앙 집중형으로, 대규모 데이터를 저장·관리

· **(데이터 전처리·거버넌스)** 데이터 정제·정규화 및 레이블링, 데이터의 품질, 보안, 윤리적 사용 등을 관리

▸ **[구현 요소 2] AI 모델 및 알고리즘**

· **(목적·구성)** 데이터에 숨겨진 패턴을 학습하여 추론·생성

· **(학습 모델)** 딥러닝, LLM, sLLM 등 데이터를 학습·내재화

· **(훈련 파이프라인)** 모델을 효율적으로 훈련하기 위한 컴퓨팅 자원(GPU 클러스터) 및 프로세스

· **(추론 엔진)** 학습 모델을 실제 서비스 환경에 배포, 실시간 예측

▸ **[구현 요소 3] 애플리케이션 및 인터페이스**

· **(목적·구성)** AI 모델의 성능을 실질적 가치나 사용자 경험으로 변환

· **(사용자 인터페이스)** AI 기능을 최종 사용자가 쉽게 사용하도록 연결하는 웹/앱 인터페이스 또는 타 시스템과 통신하는 API

· **(RAG)** 대규모 언어 모델(LLM)이 답변을 생성하기 전 외부 신뢰 데이터베이스에서 관련 정보를 찾아내고(검색), 이를 바탕으로 답변을 보강하여(증강) 정확하고 최신성을 갖춘 답변을 생성

· **(Lang Chain)** LLM 기반 애플리케이션과 RAG 파이프라인을 연계

○ **'AI Infra'**란 'AI as a Service'가 효율적·안정적으로 구동되는데 필요한 **AI 기반(AI Infrastructure)**을 말하는 것으로, **데이터와 모델을 지원하는 컴퓨팅 환경** 그 자체를 의미

▸ **[구현 요소 1] 고성능 컴퓨팅 자원**

· **(목적·구성)** 대규모 데이터와 복잡한 알고리즘을 빠르고 효율적으로 처리

· **(GPU/NPU)** AI 연산에 최적화된 그래픽 처리 장치(GPU) 또는 NPU(신경망 처리 장치) 클러스터

· **(고속 인터커넥트)** GPU와 서버 간에 데이터를 빠르게 주고받기 위한 고대역폭 네트워크

▸ **[구현 요소 2] 대규모 병렬 스토리지 (분산 환경)**

· **(목적·구성)** 대용량 데이터를 다수의 서버 및 사용자가 동시에 안정적으로 저장·처리하기 위한 고성능 저장 체계

· **(Data Fabric)** 하이브리드 및 멀티 클라우드 환경에서 분산된 데이터 자산을 통합, 관리, 활용하는 핵심적인 역할

· **(고성능 파일 시스템)** 병렬 컴퓨팅 자원이 동시에 데이터를 읽고 쓸 수 있도록 설계된 분산/병렬 파일 시스템

· **(객체 스토리지)** 대규모 비정형 데이터(이미지, 영상, 로그 등)를 객체(Object) 단위로 분산하여 저장·관리

▸ **[구현 요소 3] 클라우드 기반 운영 기술 (Operation)**

· **(목적·구성)** 인프라 자원의 탄력성, 민첩성, 안정성을 확보하고, AI 모델을 구축 및 배포

· **(가상화/컨테이너 기술)** 컴퓨팅 자원을 논리적으로 분할하고 관리하는 기술로, 효율적인 자원 배분과 확장성을 제공

· **(CI/CD(형상관리))** 소프트웨어의 개발·수정 후, 이를 자동으로 통합·검증·배포하는 개발·운영 자동화 체계

· **(클라우드 관리 시스템(CMS))** 온프레미스 자원과 퍼블릭 클라우드 자원을 통합 관리하고, 사용량에 따라 자원을 동적 할당

○ **'AI Governance'**란 AI 시스템의 **윤리성·투명성·안전성·책임성**을 확보하고, **법규**를 준수하며 서비스의 **목표를 달성**하는 데 필요한 **정책, 프로세스, 조직 구조** 등의 **체계**를 의미

▶ **[구현 요소 1] 정책 및 규정**

· **(목적·구성)** AI 기술 사용이 규정에 부합하도록 법적 책임 준수

· **(윤리·책임 원칙)** AI 시스템 편향성(Bias) 방지, 공정성, 투명성, AI 결정에 대한 인간의 책임 소재를 명확히 하는 상위 원칙

· **(데이터 거버넌스)** AI 학습 데이터의 수집·저장·사용에 관한 규칙과 개인정보 보호법(GDPR 등), 품질 요구사항 등을 포함

· **(배포 정책·프로세스)** 모델의 문서화 의무, 버전 관리, 모델 성능테스트 기준, 모델을 운영 환경에 배포하기 위한 승인 프로세스 등을 규정

▶ **[구현 요소 2] 조직 및 역할**

· **(목적·구성)** AI 시스템의 기획·개발·운영·폐기 등 전 주기에 걸쳐 누가 무엇을 책임지고 결정하는지를 명확히 설정

· **(AI 윤리 위원회 또는 위원장)** AI 프로젝트의 윤리적 위험을 평가하고 주요 의사 결정을 감독하는 최고 의사결정 기구

· **(AI Owner 및 책임자)** 특정 AI 서비스나 모델에 대한 궁극적 책임을 갖고, 규정 준수 및 성능 유지 관리를 담당하는 주체

· **(내부 감사 및 규정 준수팀)** AI 시스템을 둘러싼 정책과 외부 법규를 준수하고 있는지를 정기적으로 검토·감사

▸ **[구현 요소 3] 운영 프로세스**

· **(목적·구성)** AI에 의한 보안 공격에서 지속 AI 활용을 모니터링

· **(AI 공격 유형 및 단계별 보안 원칙)** 생애주기 단계별* 주요 공격 유형과 보안 원칙·기법을 정의

* 데이터 수집·전처리 – 모델 학습 – 검증·배포 – 운영·추론 – 모니터링·폐기

· **(모니터링 및 감사 시스템)** 배포된 AI 모델의 성능 저하(Drift), 데이터 품질 변화, 윤리적 편향 발생 여부를 실시간 추적·경고하는 MLOps 시스템

· **(위험 평가 프레임워크)** AI 프로젝트에 착수하기 전 잠재적인 위험(기술적·윤리적·법적)을 체계적으로 식별하고 그 위험 수준에 따라 관리 방안을 정의

③ AX 운영·거버넌스

○ **'Active Learning(능동적 학습)'**이란 AI 모델의 성능을 효율적으로 개선하기 위해 **가장 가치 있는 데이터를 선별**하여 **레이블링하고 학습하는 프로세스**를 의미

▸ **[운영 요소 1] 불확실성 측정**

· **(목적·구성)** 최대 학습 효과를 위해 레이블링 대상을 효율적 선택

· **(최소 신뢰도)** 모델이 예측한 클래스 중 신뢰도가 낮은 데이터 선택

· **(엔트로피 측정)** 예측 확률 분포의 불확실성 정도를 정량화하는 엔트로피를 사용, 모든 가능한 클래스에 걸쳐 예측이 얼마나 고르게 분산되어 있는지를 측정

· **(경계 거리 측정)** 가장 확신하는 두 개의 클래스 간의 신뢰도 차이(Margin)가 가장 작은 데이터를 선택

▸ **[운영 요소 2] 전문가 피드백 루프**

· **(목적·구성)** 정확도·품질을 보장하고, 모델 성능을 빠르게 향상

· **(데이터 선별 및 라우팅)** 모델의 불확실성을 기반으로 가장 가치 있는 데이터를 식별하고, 해당 데이터를 레이블링 작업 목적으로 전문가에게 전달

· **(레이블링·검증 인터페이스)** 도메인 전문가가 선별된 데이터에 정확하고 일관된 레이블을 부여, 필요시 기존 레이블을 검증

· **(재학습·통합)** 전문가로부터 레이블을 부여받아 품질이 보장된 새로운 데이터를 기존의 학습 데이터셋에 통합하고, 모델을 재학습하여 성능 개선 후 운영 환경에 배포

▸ **[운영 요소 3] 데이터 Pool 관리**

· **(목적·구성)** 학습 데이터셋의 일관성을 유지하며, 데이터가 모델에 미치는 영향 측정

· **(데이터 저장소 계층화)** 데이터의 상태(원천, 미가공, 레이블링 완료)에 따른 접근 속도와 비용 효율성을 최적화

· **(데이터 추적 및 버전 관리)** 모델의 재현성(Reproducibility)을 보장 및 Active Learning의 효과를 측정, 오류 발생 시 원인 파악

· **(Active Learning 효과 측정)** 비용 대비 얼마나 효율적으로 모델 성능을 개선했는지를 정량적으로 평가하고 추적

○ ‘Machine Learning Operations(MLOps)’란 AI 모델의 **개발부터 배포, 운영, 모니터링까지의 전 과정**을 자동화하고 표준화하여 AI 서비스의 **안정성과 효율성을 확보**하는 체계를 의미

▸ **[운영 요소 1] 자동화된 파이프라인**

· **(목적·구성)** 모델 업데이트·배포에 필요한 시간, 오류를 최소화

- **(데이터 파이프라인)** 데이터를 수집·전처리, 그 특징을 엔지니어링하여 모델 훈련에 적합한 형태로 변환하는 과정을 자동화
- **(모델 훈련 파이프라인)** 모델 훈련 과정을 반복, 확장이 가능하도록 자동화하며, 최적의 모델을 선택하고 관리
- **(모델 배포 및 추론 파이프라인)** 새로운 모델을 안정적으로 서비스에 투입하고, 모델의 추론 결과를 최종 사용자에게 전달하는 과정을 자동화

▶ **[운영 요소 2] 모델 모니터링**

- **(목적·구성)** 모델이 운영 과정에서 지속하여 정확히 동작하고, 그 안정성을 유지
- **(성능 지표 모니터링)** 다양한 소스(센서, 로그, DB) 데이터 추출·통합
- **(데이터 저장소)** 중앙 집중형으로, 대규모 데이터를 저장·관리
- **(데이터 전처리·거버넌스)** 데이터 정제·정규화 및 레이블링, 데이터의 품질, 보안, 윤리적 사용 등을 관리

▶ **[운영 요소 3] 모델 레지스트리**

- **(목적·구성)** 모델 재현성을 보장하고, 필요시 특정 버전으로 회복
- **(데이터 수집·검증)** 모델 학습에 사용된 원본 데이터의 출처, 버전, 수집 시점, 라이선스 정보를 모델 메타데이터에 등록하여 모델-데이터 간 연계 추적성(Model-Data Lineage)을 확보
- **(데이터 및 특징 모니터링)** 모델 성능 저하의 주범인 데이터 드리프트(Data Drift)나 데이터 스큐(Data Skew) 발생 여부를 조기에 감지·대응
- **(이상 탐지 및 경고 시스템)** 잠재적인 문제를 조기 발견하고, 문제 발생 시 신속한 개입과 조치를 가능하게 하여 서비스의 중단을 방지

○ **'Compliance(법규 준수)'**란 AI 시스템이 관련 **법률, 규정, 윤리 기준, 내부 정책을 준수**하도록 해 **법적·윤리적 위험을 최소화**

▸ **[운영 요소 1] 개인정보 보호**

· **(목적·구성)** 데이터 개인정보 보호 법규(예: GDPR 등) 준수

· **(Anonymization 및 비식별화 기술)** 마스킹 및 암호화, 차분 프라이버시, 가명 정보 처리 등이 포함

· **(접근통제 및 감사 로그)** 역할 기반 접근 제어, API 게이트웨이 및 인증, 접근 감사 로그 등이 포함

· **(프라이버시 영향 평가)** DPIA(Data Protection Impact Assessment) 수행, 명시적 동의 및 철회, 법규 준수 매핑

▸ **[운영 요소 2] 공정성 및 편향성 감사**

· **(목적·구성)** AI 시스템의 사회적 책임을 이행, 윤리적 위험 방지

· **(보호 속성 식별·정의)** 민감 속성 식별과 데이터 세그먼트 정의

· **(공정성 지표 측정 및 평가)** 공정성 목표가 실제로 달성되고 있는지 객관적 수치로 확인하고 편향의 정도를 측정

· **(편향 완화 및 재학습 루프)** 발견된 편향을 제거하거나 줄여 공정한 모델을 만들고, 해당 상태를 교정·관리 및 지속화

▸ **[운영 요소 3] 설명 가능성 및 투명성 확보**

· **(목적·구성)** 사용자에게 신뢰를 제공, 규제 기관의 요구사항 충족

· **(AI 모델의 블랙박스(Black Box) 특성 해소)** 로컬 설명 기법, 글로벌 설명 기법, 인과 관계 분석 등으로 문제해결

· **(모델 문서화 및 지식 관리)** 모델 카드, 데이터 계보 기록, 결정 추론 기록 등이 포함

· **(사용자 대상 설명 인터페이스)** 쉬운 언어 사용, 설명 제공 채널 운영, 피드백 및 이의 제기 창구 운영 등이 해당

□ (AI Full Stack 중심 공공 AX 방법론) AX의 3개 요소를 고려, 공공 부문의 성공적 AX를 위한 7단계(7D) 공공 AX 전략 제시

※ **(참고)** AWS CEO 맷 가먼은 "AI가 실제 서비스의 가치를 만들고 있는가? 아니면 일하는 방식을 바꾸고 있는가?"의 질문을 통해 AI 혁신보다 운영과 통제를, 단순 도입보다 지속 가능성 확보를 강조 (AWS re:Invent 2025, '25.12)

AI Full Stack 중심 AI 공공 AX 도입 프레임워크

◈ **(정의)** 공공 AX 추진 시 의사결정자가 단계별로 마주해야 할 7개 핵심 질문(Guiding Question)과 방향을 절차로 표현한 추진 프레임워크

◈ **(목적)** AI 솔루션 도입 중심이 아닌, 공공 서비스의 가치와 효율성을 극대화할 수 있도록 체계적인 실행 경로를 제시

◈ **(단계)** Define→Discover→Develop→Design→Deploy→Deliver→Diagnose

도입 단계 (7D)		핵심 질문	설명·키워드
목표 정의 (Define)	→	◆ 대국민을 대상으로 어떤 공공 서비스를 제공할 것인가?	◆ 공공 서비스의 목적·대상 도출 ※ *Identity, Objective, User/Scope*
Data 정립 (Discover)	→	◆ 어떤 Data를 활용하여 공공 서비스를 운영할 것인가?	◆ 공공 서비스를 위한 Data 선정 ※ *Metadata*
Data 운영 방안 설계 (Develop)	→	◆ 어떻게 Data를 축적·관리할 것인가?	◆ Data의 지속적 축적과 관리, 보안 방안 설계 ※ *Data Architecture, Knowledge Base*
AX 투자 모델 수립 (Design)	→	◆ AX 사업의 비용을 어떻게 조달·집행할 것인가?	◆ AX 구축과 운영 지출 계획 수립 ※ *CAPEX(선투자) & OPEX(운영비)*
AI Full Stack 구성 (Deploy)	→	◆ AX Framework를 어떻게 표준화할 것인가?	◆ 특정 업체·모델에 종속되지 않는, 최적화 아키텍처 정립 ※ *AI Full Stack, LLMOps*
서비스 제공 채널 선택 (Deliver)	→	◆ 대국민 대상 어떠한 채널을 통해 서비스를 제공할 것인가?	◆ 대국민이 쉽고, 빠르게 접근할 수 있는 애플리케이션 선정 ※ *옴니채널, 사용자 경험, 포용적 접근*
AX 활용 진단·모니터링 (Diagnose)	→	◆ AX 이후 운영·관리는 어떻게 할 것인가?	◆ 성능, 비용, 준법·윤리 등에 대한 상시 진단 및 환류 체계 구현 ※ *Performance, Cost, Compliance*

[단계 1] 목표 정의 : 어떤 공공 서비스를 제공할 것인가?

○ **(주요 현황)** 정부·공공기관은 **폭넓은 분야**에서 AI 서비스 제공 중

· **(민원·상담 서비스)** 법률 상담, 민원 상담, 국세 상담 등

· **(보건·복지 서비스)** 임신 예측, 질병 진단, 학습 지원 등

· **(교통·재난/안전 서비스)** 교통 최적화, 보이스피싱 탐지 등

○ **(주요 이슈)** 다만, 챗봇·고객센터 등 **정형화된 답변 기능**에 국한되는 경우가 많고, **학습·운영 데이터의 품질**도 상당 부분 미흡

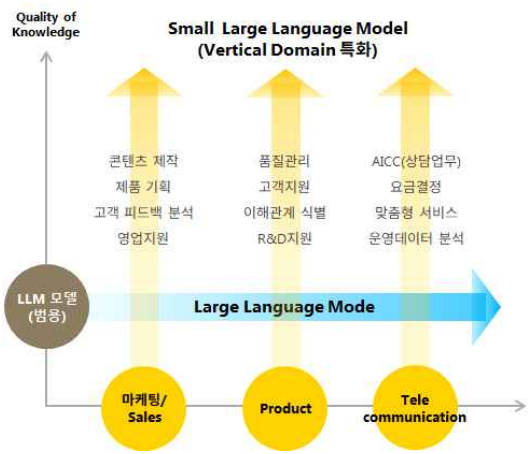
· **(서비스)** 단순 FAQ 응답·민원 안내 등 저난도·반복 업무에 편중, 결정·예측 분석 등 고부가가치 영역으로의 확장 제한

· **(데이터)** 비정형·이기종 데이터의 혼재, 양질의 데이터 부족 및 낮은 학습 수준 등으로 학습·운영 데이터의 신뢰성 저하

○ **(접근 전략 : 구체적 서비스·기능 발굴 및 목표 명확화)** 범용적 접근보다는 **특정 목표**와 이를 달성하기 위한 **구체적인 문제해결 중심**의 **서비스·기능 발굴**에 초점

▸ **(방안 1)** 범용분야에서도 **특정 영역·기능 발굴**에 집중(Vertical AI)하며, 모델 측면에서도 **sLLM(소형 언어 모델) 고려** 검토

< [참고] LLM vs Small LLM(sLLM) 비교 >



sLLM이 Vertical AI에 적합한 이유

- **(빠른 속도)** 경량화 구조로 속도↑, 특정 작업의 Fine-tuning 유리
- **(전문성 향상)** 특정 도메인을 집중 학습 → 문맥을 더 정확히 파악
- **(비용 효율 우수)** 모델 크기가 작아 학습 및 서버 운영비용이 저렴하며, CPU만으로도 추론 가능

※ **(참고)** 거대 언어 모델(LLM) 소개 (SK Tech Summit 2023, '23)

▸ (방안 2) 서비스에 관한 **정체성**과 **목표 설정, 대상 수립, 달성 방안** 등을 **구체화**할 수 있는 다양한 **방법론 활용** 고려

< [참고] 서비스 구체화 방법론 사례(안) >

방향 지표	역할	방법론
정체성 (Identity)	◆ 핵심 가치 도출	◆ 파괴적 혁신(Disruptive Innovation) ◆ TRIZ
목표 (Objective)	◆ 정체성을 실현할 수 있는 측정이 가능한 목표	◆ Root Cause Analysis ◆ Design Thinking
대상 (User/Scope)	◆ 서비스 제공의 주체와 범위	◆ 페르소나 기법 ◆ Analytic Hierarchy Process
달성 방안 (Initiative)	◆ 목표 달성을 위한 구체적인 방법·도구	◆ Agile 기법 ◆ Minimum Viable Product ◆ Proof of Concept

[단계 2] Data 정립 : 어떤 Data를 활용하여 서비스를 운영할 것인가?

○ **(주요 현황)** 공공 서비스의 운영 데이터는 크게 3가지로 분류할 수 있으며, 정부는 **공공 데이터의 발굴·통합·활용**을 위한 노력 지속

· **(행정 데이터)** 법령에 따라 업무를 수행 과정에 발생하는 데이터

※ **(개인 식별 데이터)** 주민등록, 세금 납부 기록, 의료보험, 국민연금, 교육 등

※ **(업무 처리 데이터)** 민원 신청 및 처리, 인허가, 복지, 출입국 등

· **(시설·인프라 데이터)** 도시 운영, 국민 안전과 관련하여 발생하는 실시간 또는 정기적인 데이터

※ **(실시간 데이터)** 차량 흐름, CCTV 영상, 환경 정보 수집, 재난 감지 등

※ **(SOC·시설 데이터)** 도로, 상하수도, 전력망, 가스 등 도시 인프라 상태 정보

· **(국민 참여 데이터)** 국민의 활동·피드백을 통해 생성되는 데이터

※ **(민원 및 피드백)** 온라인 민원, 상담 기록, 설문 결과 등

※ **(이동/활동 데이터)** 통신 데이터, 대중교통 이용, 출입 등

○ **(주요 이슈)** 정부·공공의 노력에도 불구하고, **데이터의 파편화** 및 **표준화 체계 미흡, 현행 법·제도의 허점** 등으로 최적의 Data를 관리·활용하는 데 애로

· **(품질·활용성)** 비표준화, 기관별 파편화, 실시간 데이터 등 한계

· **(법·규제 한계)** 개인정보 보호-활용 간 충돌, 익명화·가명화 제약

· **(거버넌스 및 역량 문제)** 데이터 소유 기관과 관리 책임 분산, 순환보직 등 조직 내 이슈로 인한 전문 인력(데이터 사이언티스트, 개발자 등) 양성 제약 등

○ **(접근 전략 : 메타데이터 중심 데이터 정의 및 설계·관리 체계화)** 서비스 **목적을 고려한 데이터 구성, 메타데이터 최적화 설계** 등으로 데이터의 검색·활용·이해·관리 효율을 극대화

▸ **(방안 1)** 서비스의 운영 목적을 우선으로 고려하여, 구체적인 데이터 구성과 표준화 추진

▸ **(방안 2)** 데이터별 비식별화 기법, 암호체계 적용 등 법·규제 대응

▸ **(방안 3)** 메타데이터의 최적화 설계가 핵심으로, 이때 주요 단계·절차의 기획을 통해 서비스 데이터의 메타데이터 지침* 마련 중요

* **(주요 요소)** 메타데이터 설계 목적 정의, 식별, 요소 분류, 표준 스키마 선정, PoC, 모델링 검토 및 검증, 운영·관리 방안 수립 등

메타데이터(Metadata)란?

◈ **(정의)** "데이터에 관한 데이터(Data about Data)"로, 데이터 자체가 아니라, 그 데이터를 설명·식별·관리하기 위한 부가 정보를 의미

◈ **(활용 목적)** 데이터의 검색(Findability), 활용(Usability), 이해(Understandability), 관리(Manageability) 등 측면에서 매우 유리

◈ **(비유)** 도서관의 도서 카드와 유사한 개념으로, 책(데이터) 자체가 아닌, 책의 제목, 저자, 출판일, 분류 번호, 소장 위치 등을 기록한 정보

◈ **(예시)** 사진 파일을 예로 든다면, 사진 이미지는 데이터에, 해당 사진의 촬영 일시, 해상도, 파일 형식 등의 정보는 메타데이터에 해당

< [참고] 메타데이터 설계 절차 및 방법론(안) >

단계	절차	설명
(1단계) 분석 및 범위 정의	목표 정의	◆ 메타데이터 설계의 목적을 명확히 설정 (예: 응답 효율화, 품질 관리, 데이터 연계)
	범위 확정	◆ 메타데이터를 관리할 데이터 종류와 관리 수준을 결정 (예: 행정 데이터, 시설 및 인프라 데이터, 국민 참여 데이터)
	메타데이터 식별	◆ 데이터 생산자(연계 기관)와 소비자 (AI 개발자, 국민)의 요구사항을 분석하여 필요한 메타데이터 요소를 식별
(2단계) 모델링 및 표준화	메타데이터 요소 분류	◆ 목적에 따라 분류, 구조화 - 기술(Descriptive): 제목, 저자, 키워드 - 관리(Administrative): 데이터 소유자, 갱신 주기, 보안 등급 - 구조(Structural): 파일 형식, 데이터 관계
	표준 스키마 선정	◆ 국제 표준(예: Dublin Core, ISO 11179) 또는 국내 표준을 참고하여 요소별 데이터 형식, 길이, 필수 여부를 정의
	분류 및 용어 표준화	◆ 데이터의 주제 및 내용 분류를 위한 표준 분류 체계와 표준 용어를 정의하여 일관된 응답을 가능
(3단계) PoC 기반 검증	Proof of Concept	◆ AI Full Stack 기반 PoC 수행
	모델링 검토 및 검증	◆ 설계된 모델이 정의된 목표와 요구사항을 충족하는지, PoC 시스템과 연계에 논리적으로 타당한지 검토
	운영 및 관리 방안	◆ 메타데이터의 주기적인 갱신, 변경 관리, 품질 관리에 대한 운영 조직 및 프로세스를 수립

※ **(참고)** OAK 확장형 리포지터리 운영을 위한 연구데이터의 메타데이터 지침 (노지현, 2020)

[단계 3] Data 운영 방안 설계 : 어떻게 Data를 축적·관리할 것인가?

○ **(주요 현황)** 공공은 주로 **기관별**로 **데이터를 보유·관리**하는 상황

· 기관별 방대한 데이터를 보유하고 있으며, 고유의 데이터 관리 포털 등을 통해 관리·개방, 독립적 AI 원칙 등을 수립해 준수

○ **(주요 이슈)** **클라우드, 품질, 활용·보호, 구조화** 등 관점의 이슈 존재

· **(클라우드)** 외산 의존도, 통합 부재(기관별 Silo 심화), 표준 미비

· **(품질)** 저품질 데이터 만연, 자동화 부족, 설명이 가능한 AI 제약

· **(활용·보호)** 개인정보 침해 우려 등으로 인한 보수적 운영, AI 윤리·법규 준수 자동화 부재 등 한계 직면

· **(구조화)** Knowledge Base의 개념과 역할, 목적 등이 불분명하며, 온톨로지 및 지식 그래프 미적용, 임베딩 전략 부재 등 구조화 차원에서도 이슈 존재

○ **(접근 전략 : 데이터 아키텍처 설계 및 Knowledge Base 구조화)** **데이터 아키텍처(Data Architecture)**의 체계적 설계를 통한 AX의 작동 기반인 데이터의 **자주성·품질·보호**를 동시 확보

▸ **(방안 1) 데이터 아키텍처(Data Architecture)**의 체계적 설계를 통해 AX 작동 기반인 데이터의 **자주성·품질·보호**를 동시 확보

※ **(소버린 클라우드)** 논리적·물리적 통합 요소 및 메타데이터 기반 운영

※ **(AI 친화적 품질)** DB 품질 관리 자동화 및 스키마 개선, 설명 가능성(XAI) 지원, 지식기반 품질 검증 체계 확보

※ **(활용·보호 균형)** 보안·접근통제, 가명화 DB, AI 윤리 등 자동 준수 여부 측정

▸ **(방안 2) 구조화된 지식저장소(Knowledge Base)의 구성·운영 방안**을 확립하고, **온톨로지 모델링, 지식 그래프** 등 활용 고려

※ 구조화된 Knowledge Base가 없는 경우, AI 서비스의 도입 효과(성과·품질 등)가 사용자의 기대 수준보다 낮아진다는 연구 결과* 도출

* **(참고)** A Generative AI-driven Metadata Modelling Approach (M Bagchi, 2024)

< [참고] 공통 표준 데이터 아키텍처 방향(안) >

핵심과제	방법	주요 구성
소버린 클라우드	공공 데이터 주권의 자주성 보장	◆ **(논리적 통합)** 분산 Key-Value 저장소 ◆ **(물리적 통합)** 소버린 클라우드 기반 Data Lake, Warehouse, Fabric ◆ **(메타데이터 관리·저장소)** Data의 위치, 구조, 의미 관리
	의미론적 데이터 통합 및 Knowledge Base 적용	◆ **(온톨로지 모델링)** 계층적 관계 및 규칙 ◆ **(의미적 연결)** 분산된 Data 간 논리적 추론 및 통합 ◆ **(지식 그래프)** 복잡한 행정 관계 시각화
AI 친화적 품질 확보	DB 품질 관리 자동화 및 스키마 개선	◆ **(품질 표준)** 학습 데이터의 필수 기준 ◆ **(정제 프로세스)** 적재(ETL/ELT) 중 이상 탐지 로직 구현 ◆ **(버전 관리)** 모델의 재현성, 투명성 확보
	지식기반 품질 검증 및 설명 가능성 (XAI) 지원	◆ **(규칙 기반 품질 검증)** 규정, 제약 조건 반영 ◆ **(XAI(설명가능한AI))** 데이터의 근거, 연결 ◆ **(표준 용어 구축)** 인식의 통일성 확보
활용과 보호의 균형 달성	보안 및 접근통제 강화, 가명화 DB 구축	◆ **(개인정보 자동 비식별화)** 가명화/익명화 자동 변환 수행 ◆ **(가명 정보 분리)** 원본 민감 정보와 일반 정보 분리, 가명 처리된 민감 정보만 분석용 활용, 데이터 처리 이력 감시
	접근 규칙 기반 제어 및 AI 윤리 지식 통합	◆ **(지식기반 접근 제어)** Data가 가진 민감성 속성과 활용 목적에 따른 접근 제어 ◆ **(AI 윤리/법규 적용)** AI 모델 운영 시 자동으로 규정 준수 여부 확인

[단계 4] AX 투자 모델 수립 : 사업 비용을 어떻게 조달·집행할 것인가?

○ **(주요 현황)** 공공 AX 사업은 주로 **정부(중앙 및 지자체) 예산**을 통해 **조달·집행**되며, 성격에 따라 민관 협력 형태로도 진행

· **(비용 조달)** 정부 출연금, 민간 분담금, 추경 예산 등으로 구성

· **(사업 규모)** 사업 건 단위 기준 약 수십억~수백억 원 규모 산정

○ **(주요 이슈)** 정부·공공 모두 AX 사업의 특성을 반영하지 못하는 **기존 조달 체계**와 **사업 방식(직접 구현, On-Premise)**을 여전히 추구

· **(AX 속도와의 격차)** 지속적인 고도화, 지식화, 추가 학습이 필수인 특성을 반영하지 못해 ISP 의무화, SI 방식 의존

· **(예산 확보 불확실·비효율성)** 예산 심의 과정에서 보류·삭감 확률이 높고, 아직 OPEX(운영비)보다 CAPEX(자본비) 예산 강조

○ **(접근 전략 : AX 특성을 고려한 유연화된 방식 채택)** **동적 수요**에의 대응형 전략인 **OPEX 중심 투자, FinOps 중심 운영체계** 채택

▸ **(방안 1)** 단년도 **일회성 구축비(CAPEX) 중심**의 전통적 IT 기반 사업 방식에서, AX 특성에 부합하는 **운영·사용 기반(OPEX) 중심**의 **동적 투자 모델**로 점진적 전환 **(조달 방식 다각화)**

※ **(조달 방식 다각화 전략)** ① 분리발주 채택, ② SaaS 직구매·구독형 방식 도입, ③ 클라우드 마켓플레이스 활용 등

전략	주요 내용 및 효과
분리발주	◆ **(내용)** 인프라(GPU·클라우드), 모델·플랫폼, 데이터 구축, 운영·고도화 등의 영역을 분리하여 발주 ◆ **(효과)** 영역별 전문기업 참여 확대, 특정 SI 종속 회피
SaaS 직구매·구독형 조달	◆ **(내용)** SaaS 직접 구매 채널 확대(디지털 서비스 전문 계약제도 활용 등) 및 사용량 과금(Pay-per-use) 방식 도입 ◆ **(효과)** 별도 구축 없이 즉시 활용 가능한 유연성 확보
클라우드 마켓플레이스	◆ **(내용)** 공공 클라우드 마켓플레이스를 통한 신속 조달 추진 ◆ **(효과)** 사전 검증된 솔루션 재사용성 확보, 중복 구축 방지

▸ **(방안 2) FinOps* 도입** 전략을 채택, **AX 특성인 실시간 변동성 (토큰 사용량, API 호출량)**에 대응할 수 있도록 각종 정책 추진

* **(개념)** "Finance + DevOps + AI Operations"의 결합을 의미하는 개념으로, AI 자원의 동적 사용·비용·가치 수준을 상시 가시화·최적화하는 운영체계를 의미

목적 구분	주요 내용 및 도구·지표
가시화 (Inform)	◆ **(내용)** 기관별 AX 비용 가시화 대시보드 구축 및 토큰·호출·GPU 등 사용량을 실시간 모니터링 ◆ **(도구·지표)** 대시보드, Cost per Token, Cost per Query
최적화 (Optimize)	◆ **(내용)** 모델 라우팅·캐싱·프롬프트 최적화 등 기술적 최적화 루틴 표준화 ◆ **(도구·지표)** Chargeback/Showback, Budget Alert
운영 (Operate)	◆ **(내용)** 부서·서비스 단위 비용 배분(Chargeback) 체계를 도입, 일정 기준에서 알림 등을 제공해 무분별한 사용 억제 ◆ **(도구·지표)** Model Cascading, Semantic Caching

< [참고] AX 도입 비용의 변화 추이 (민간 기준) >

구분	CAPEX (자본비용)	OPEX (운영비용)	비율 추이
AX 도입 초기·전환 시점 (1~2년)	◆ PoC 비용 ◆ AI Full Stack 개발 (API 연계 등 일부) ◆ 장기 사용을 위한 클라우드 선납 계약금	◆ 클라우드 컴퓨팅 사용료 (On-Demand) ◆ AI 모델 미세 조정 인건비 (Managed Service)	◆ CAPEX:OPEX = 50:50
AX 성숙·운영 시점 (3년 이후)	◆ 보안 강화 및 지식재산(IP) 등 추가 인프라 등	◆ 클라우드 컴퓨팅 사용료 (약정 계약 전환) ◆ AI 모델 미세 조정 인건비 (Managed Service)	◆ CAPEX:OPEX = 30:70 (OPEX 비중 우위: 70% 이상)

[단계 5] AI Full Stack 구성 : Framework를 어떻게 표준화할 것인가?

○ **(주요 현황) 국산의 AI 기술력**은 지속 높아지고 있으며, 인프라, 모델, 응용 등 **다양한 계층**에서 **공공 분문 AI 도입·전환 노력**

· **(계층별 현황)** 외산 중심 GPU·클라우드 도입(인프라 계층), 국산 LLM 모델이 등장하며 주로 PoC 단계에 집중(모델 계층), 공공 챗봇 및 콜센터 AI 도입 확산(응용 계층) 등 현상

· **(생태계 현황)** 국산 AI 칩, LLM, 플랫폼의 민간 기술 성숙도가 빠르게 향상되고 있으나, 공공 도입 사례는 여전히 부족

○ **(주요 이슈)** 다만, AI 도입이 **일부 계층에 편중**되는 현상과 **외산 종속, 중복 구축, 구축 후 방치** 등의 이슈가 지속 발생

· **(계층 편중)** 모델·응용 계층 외 영역에서는 공백이 발생(인프라·데이터·운영)하고 있어 다양한 계층의 균형 투자 부재 시급

· **(외산·벤더 종속)** 단일 SI·벤더 통합 발주 등으로 여전히 종속

· **(기관별 중복 구축)** 기관마다 개별로 유사 기술을 구축함에 따라, 동일·유사 서비스가 구현되어 막대한 중복 투자 발생

· **(운영·진화 체계 부재)** LLMOps 표준 부재, 단년도 구축형 예산 등은 구축은 했으나 결국 활용되지 못하는 문제로 연결

○ **(접근 전략 : 공공 AI Full Stack* 체계 정립)** 단일 시스템이 아닌 **계층 구조·인터페이스 표준**이 될 수 있는 **공통 설계도** 마련

* **(AI Full Stack)** AI가 실제로 작동하는 데 필요한 인프라·데이터·모델·운영·응용까지의 모든 기술 계층을 빠짐없이 포괄하는 통합 체계를 의미

▸ **(방안) AI의 모든 계층을 포괄적으로 활용**하되, 특정 업체에 종속되지 않는 **Plug-in 방식**으로 구성하여 급변하는 **AI 기술 환경에 민첩·예측 가능**하게 대응하는 표준 아키텍처 정립

※ ① 5계층 참조 아키텍처 정립, ② API 기반 Plug-in 구성, ③ LLMOps 표준 마련으로 상시 운영·진화 체계 확보

방안	주요 방향 및 요소
5계층 참조 아키텍처 정립	◆ **(인프라)** GPU 자원 확보, 소버린 클라우드 적용, 국산 AI 칩 활용 ◆ **(데이터)** 메타데이터 표준 적용, Vector DB 도입 ◆ **(모델)** LLM Gateway·Router 표준화, 민감도·복잡도별 모델 자동 분기 구조 정립, 국산 sLLM 검토 ◆ **(오케스트레이션)** RAG 표준 적용, MCP 어댑터 활용, 가드레일 도입 ◆ **(응용)** 표준 UX 컴포넌트 라이브러리, 옴니채널 게이트웨이 표준화
API 기반 Plug-in 구성	◆ **(LLM Gateway·Router)** OpenAI 호환 API 등 표준 인터페이스 채택 및 요청 특성별 자동 분기 (예 : 민감→내부 sLLM, 복잡→대형 LLM, 단순→경량 모델) ◆ **(MCP 표준)** 행정정보시스템·DB·문서저장소를 표준 어댑터로 연결함으로써, 한 번 만든 어댑터를 모든 기관 재사용 ◆ **(MSA 적용)** 임베딩·검색·생성·평가·로깅을 독립 서비스화
LLMOps 표준 마련 기반 상시 운영·진화 체계 강화	◆ **(프롬프트 버전 관리)** Git 기반 형상 관리, A/B 테스트, 롤백 ◆ **(평가셋 운영)** 도메인별 표준 평가 데이터, 자동 회귀 테스트 ◆ **(가드레일)** 사전·사후 필터, 출처 검증 ◆ **(관측·모니터링)** 추적, 품질 지표, 드리프트 감지 ◆ **(예측 가능성)** 비용 예측 모델, 성능-비용 Trade-off 매트릭스 ◆ **(지속 개선)** 피드백 → 평가셋 보강 → 모델 개선 자동 사이클

[단계 6] 서비스 제공 채널 선택 : 어떠한 채널로 서비스를 제공할 것인가?

○ **(주요 현황)** 부처·공공은 다양한 **채널(정부24, 국민 비서 등)**을 운영 중이며, **LLM 챗봇 전환, 음성 서비스(AI 상담) 도입 확산** 추세

○ **(주요 이슈)** **채널 중복, 신규 채널 선호, 신뢰도 미흡** 등이 주 이슈

· **(채널 중복)** 기관별 챗봇·앱 서비스의 목적·대상이 매우 유사

· **(신규 채널 구축 관성)** 기존 채널보다는 신규 채널 구축 경향

· **(취약계층 배제)** 취약계층의 AI 채널 접근성은 여전히 미흡

· **(채널 신뢰 미흡)** AI 답변 진위, 책임 소재 등 이슈 존재

○ **(접근 전략 : 옴니채널 통합 및 포용적 채널로 접근)** 새 채널을 만드는 것이 아니라, **국민이 이미 쓰는 채널에 AI를 얹고, 디지털 취약계층을 포용**하는 전략 채택

▸ **(방안 1)** 기존 공공 서비스 앱 혹은 민간 플랫폼(카카오, 네이버 등)에 **통합(Embed)**하여 **사용자 경험(UX)의 일관성을 유지**

구분	주요 내용
(1순위) 국민 친숙 민간 채널 활용	◆ **(내용)** 카카오톡 채널 및 플러스 친구, 네이버 앱, 토스 등 민간 메신저 플랫폼 활용 ◆ **(특징)** 신규 앱 다운로드·회원가입 부담 없이 즉시 접근
(2순위) 공공 통합 채널 우선 활용	◆ **(내용)** 정부24(통합 행정 포털), 국민 비서(맞춤 알림·상담) 활용 ◆ **(특징)** 기관별 별도 채널 신설 전 기존 공공 채널 우선 검토
(3순위) 기관 자체 채널 보완	◆ **(내용)** 기관 자체 채널 등이 있다면, 고려 아래 자체 채널 보완 전략 채택 ◆ **(특징)** 기관 홈페이지·앱은 심층 업무·전문 영역에 한정

▸ **(방안 2)** 공공 부문의 특성을 반영, **포용적 접근성**과 **신뢰성·책무성·투명성 확보**를 위한 **UX 반영**

구분	주요 내용
포용적 접근성	◆ **(음성 채널 지원)** 콜센터 AI 상담사, 시각·문해 약자 지원 ◆ **(오프라인 창구 연계)** 디지털 채널에서 해결이 안 될 시 창구 예약·연계 서비스 자동화 ◆ **(다국어 지원)** 외국인 대상 영어·중국어·베트남어 등 외국어 지원 ◆ **(수어·점자·고대비 UI)** 「장애인 차별금지법」, 웹 접근성 지침 준수 ◆ **(대리 지원 서비스)** 가족·대리인 보조 접근 기능 (위임 인증 기반)
신뢰성·책무성·투명성	◆ **(답변 근거 표시)** 출처 문서·법령·조항 명시, 클릭 시 원문 확인 ◆ **(사람 상담 전환)** "상담사 연결" 버튼 상시 노출, 맥락 이관 자동화 ◆ **(AI 고지)** AI 응대임을 명확 고지 (투명성 제고) ◆ **(신뢰도 차등 표시)** 공식 답변과 참고 답변을 구분하여 명시 ◆ **(불확실성 명시)** "이 부분은 정확하지 않을 수 있습니다."

[단계 7] AX 활용 진단·모니터링 : 이후 운영·관리는 어떻게 할 것인가?

○ **(주요 현황)** 대부분 기관이 구축 완료 시점을 **사업 종료로 인식**하고 있으며, 이에 따라 **모니터링** 및 **상시 운영체계 미정착**

· 일부 기관에서는 대시보드 등을 운영하고 있으나, 성능과 비용, 준법, 조직 등에 대한 통합적 진단·모니터링 역할은 미흡

○ **(주요 이슈)** AI 서비스 도입 이후 **진단·모니터링에 관한 거버넌스**(모니터링 및 진단, 피드백, 개선 등 절차)는 매우 미흡한 현실

· **(관리 미흡)** 사업 종료 후 모니터링을 위한 담당자 지속 변경

· **(통합 진단 체계 부재)** 성능, 비용, 준법 등 요소를 각 부서가 개별적으로 관리하며, 상시적 진단 체계 등이 부재

· **(환류 거버넌스 미비)** 모니터링 결과가 서비스 개선으로 연결되지 않는 경우가 많고, 정확한 개선 단계의 파악에도 한계

○ **(접근 전략 : 환류 거버넌스 마련 및 상시 진단 체계 구축)** AI 서비스 구축 이후 **전주기 차원의 환류·개선 거버넌스 마련**

▸ **(방안 1) 환류 목적·경로 명확화** 기반의 **환류 거버넌스 마련**

진단 결과	환류 위치 단계	조치
데이터 품질 저하	③ Data 운영 방안 설계 (Develop)	◆ 데이터 정제 ◆ Knowledge Base 갱신
비용 급증 및 ROI 저하	④ AX 투자 모델 수립 (Design)	◆ 모델 라우팅 조정 ◆ CAPEX·OPEX 재설계
모델 성능 한계	⑤ AI Full Stack 구성 (Deploy)	◆ 모델 교체 ◆ 파인튜닝·RAG 개선
채널 만족도 저하	⑥ 서비스 제공 채널 선택 (Deliver)	◆ UX 개선 ◆ 채널 재배치
법규 위반 위험	거버넌스 전반	◆ 정책·가드레일 강화

▸ **(방안 2) 성능, 비용, 준법·윤리, AI 전담 조직** 등 주요 구성 요소에 대한 **상시 진단 체계** 구축

구분	목적	검토 지표
성능 (Performance)	◆ AI 서비스가 의도된 가치를 제대로 전달하고 있는가를 측정	◆ 정확도 (Accuracy) ◆ 환각률 (Hallucination Rate) ◆ 지연시간 (Latency) ◆ 사용자 만족도 (CSAT·NPS) ◆ 활용률 (Adoption Rate) 등
비용 (Cost)	◆ AI 서비스 운영에 투입되는 재정 자원과 그 효율성을 측정	◆ OPEX 추세 ◆ 호출 당 단가 (Cost per Query) ◆ 토큰 사용량 (Token Usage) ◆ GPU 사용률 ◆ ROI (투자 대비 효과) 등
준법·윤리 (Compliance)	◆ AI 서비스가 법규·윤리·사회적 책무를 준수하는가를 측정	◆ 개인정보 보호 ◆ AI 기본법 준수 ◆ 편향성·차별 ◆ AI 영향 평가 ◆ 보안 사고 등
AI 전담 조직 (Organization)	◆ AX 전 주기(기획, 구축, 운영, 감사, 진화)를 통합 관리·담당하는 전담 조직의 구성·기능을 측정	◆ 조직 구성 (AI 운영위원회, 실무협의체, 운영팀 등) ◆ 구성 직군 (전략·기획, 기술, 운영·서비스, 평가 직군 등)

[참고] 「AI Full Stack AX 도입 프레임워크」 환류 체계

◈ **(환류 개요)** 총 7단계의 절차는 마지막 단계인 **"Diagnose"** 수행 결과에 따라 적정 단계로 환류, 지속적으로 피드백(Feedback)되며 개선·고도화

※ **(7단계)** ① Define → ② Discover → ③ Develop → ④ Design → ⑤ Deploy → ⑥ Deliver → ⑦ Diagnose

□ **(결론 및 시사점)** 공공에 최적화된 **AX 절차**를 **제안**하며, 전주기 차원의 **통합** 및 **지속적 환류 체계**를 바탕으로 성공적 AX 기대

○ **(Transformer 모델로 AI 혁신)** '17년 6월, Google Brain 팀이 **Transformer 모델**을 제안, 현재 **대규모 언어 모델의 토대**로 작용

※ **(정보 혁신)** 사용자 검색 후 답변 도출 → AI 에이전트가 알아서 응답 제시

※ **(업무 혁신)** 기존 N명의 역할을 1명이 대체함으로써 업무 효율화 극대화

※ **(가치 혁신)** AI 솔루션도 중요하나, 사람이 어떻게 AI를 활용하는가가 핵심

○ **(AX 정의 & 구성요소)** ① **AX 대상·서비스**, ② **AX 구현**, ③ **AX 운영·거버넌스** 등 3요소가 성공적 AX를 위한 핵심으로 언급

※ **(AX 대상·서비스)** 무엇을 AI로 전환할 것인가? (예: 업무, 서비스, 프로세스)

※ **(AX 구현)** 어떻게 AI를 구축·적용할 것인가? (예: 데이터, 모델, 인프라, 에이전트)

※ **(AX 운영·거버넌스)** 어떻게 AI를 지속 운영·관리할 것인가? (예: 품질, 모니터링)

○ **(AI Full Stack 중심 공공 AX 방법론)** 공공 부문의 성공적 AX를 위한 전략으로, **7단계**의 **AI Full Stack 전환 방법론** 제안

도입 단계	주요 내용 (핵심 질문)
목표 정의	◆ 공공 서비스의 목적·대상 도출 (어떤 서비스를 제공할지)
Data 정립	◆ 공공 서비스 Data 선정 (어떤 Data를 활용할지)
Data 운영 방안 설계	◆ Data 축적·관리, 보안 방안 설계 (어떻게 Data를 축적·관리할지)
AX 투자 모델 수립	◆ 구축·운영 지출 계획 수립 (비용을 어떻게 조달·집행할지)
AI Full Stack 구성	◆ 최적화 아키텍처 구현 (AX Framework를 어떻게 표준화할지)
서비스 채널 선택	◆ 국민 친화적 채널 선정 (어느 채널로 서비스를 제공할지)
AX 진단·모니터링	◆ 상시 진단 및 환류 체계 구현 (운영·관리는 어떻게 할지)

☞ **(종합 시사점)** AI 공공 서비스의 가치 제고를 위한 **통합적·지속적 관점**의 **운영·개선 및 고도화 사이클(환류 체계)**이 핵심

▸ **(프레임워크)** 의사결정자가 마주할 **핵심 질문**이자 **도구**로 활용

▸ **(통합·순환 체계)** 단순한 절차가 아닌, ⑦ Diagnose → ③~⑥ **단계로 환류**되는 **자기 개선(Self-improving)** 체계로 적극 활용 기대

세상의 혁신은 과거 “정보화(IX)”부터 시작해 “디지털 전환(DX)”으로 이어져 현재는 “인공지능 전환(AX)”에 이르렀습니다.

「AX ISSUE BLENDER」 series는 이에 발 빠르게 국내외 공공 AX 관련 주요 현황과 사례, 이슈를 진단·분석하고, 나아가 최적의 추진 전략을 모색하기 위해 한국지능정보사회진흥원(NIA) “공공AI전환지원센터”에서 기획·작성·발간하는 보고서입니다.

「AX ISSUE BLENDER」는 공공 AX의 핵심 요소인 기술, 조직 문화, 데이터, 인적 역량, 제도 및 거버넌스 등 다각도의 이슈를 조합·융합해 (Blending) 유의미한 통찰(Insight)을 제공한다는 의미를 지닙니다.

2026-01 AX ISSUE BLENDER

발 행	2026년 5월
발 행 인	김 형 철
기 획	한국지능정보사회진흥원 공공AI전환지원센터 김원확 센터장, whkim@nia.or.kr
작성 · 자문	메가존클라우드 Product Build 유동일 리더, dongyu@megazone.co.kr 한국지능정보사회진흥원 공공AI전환지원센터 이상준 책임, sjlee@nia.or.kr
온라인 출처	www.nia.or.kr