범정부 AI 공통기반 연계
광역 주도 기초 활용 행정 AI 플랫폼 구축 제안서

범정부 AI 공통기반 연계를 통한 GPU 비용 절감
광역자치단체는 AI 공통기반과 공통 데이터의 기반 구축
기초자치단체는 광역 제공 공통기반 활용 행정 및 대민 서비스 에이전트 개발 및 운영

제안일: 2026년 7월 2일
제안사: ㈜스캐터엑스

핵심 요약

광역이 중심이 되어 기초와 함께 활용하는
안전한 행정 AI 공통기반을 구축하는 사업입니다.

행정 AI 플랫폼 구축

행정망 기반
공동 활용 구조
공공 행정 AI 운영체계
단순 챗봇 도입 아님
특정 LLM 구매 사업 아님

Secure RAG

행정 데이터 수집
데이터 분류
전처리 | 검색 | 활용
보안 중심 관리
민감정보 탐지·마스킹
권한 기반 검색

Secure LLM 라우터

데이터 보안 등급 기반
사용자 권한 기반
LLM 처리 경로 자동 선택
모델 라우팅 정책
로그 관리
감사 관리

공개자료 | 내부자료 | 민감자료 | 개인정보 포함 자료

광역의 표준성과 보안 역량과 기초의 현장성과 자율성을 결합한 공동활용 AI 운영모델입니다.

광역자치단체 역할

AI 공통기반 제공　공통 데이터 제공

내부망 LLM　범정부 AI 공통기반 연계

Secure RAG　Secure LLM 라우터

데이터 카탈로그　공통 API

MCP 기반 데이터·도구 연계체계

보안정책　권한관리　로그·감사체계

AI 공통기반

기초자치단체 역할

민원, 복지, 시설, 주차

청소　지역행사　생활정보

AI 서비스 운영　부서별 에이전트

자체 데이터 등록　데이터 갱신

데이터 검수　데이터 관리 책임

광역 표준성　기초 자율성

행정 데이터 보안과 AI 활용을 동시에 실현하는 통합 안전 운영 체계를 구축하고자 합니다.



내부망과 범정부 기반, 글로벌 모델을 보안 등급에 따라 구분 활용하는 전략적 AI 운영 구조를 제안드립니다.

내부망 LLM

행정망 내부자료 처리

공문
내부 보고서
회의자료
민원자료
업무편람

비공개 정책자료
광역 통제 환경
보안 중심 처리

범정부 AI 공통기반

내부망 수준 보안
보안정책 충족
사용자 권한 관리

행정망 연동
감사 로그
전송 통제 기준
C/S 등급 처리 가능
대량 처리
피크 부하 대응
공통 행정기능 처리
내부망 LLM 보완
GPU 부담 완화
확장성 확보

글로벌 LLM API

외부 민간 서비스
최신 모델 성능 활용
0등급 공개 데이터
문안 작성
보도자료 표현 개선
홈페이지 공개정보 요약
외부 리서치
개인정보 제외
비공개자료 제외
내부 검토자료 제외

보안 중심 처리

확장성과 성능 활용

보안 등급에 따라 LLM을 지능적으로 분기하는 안전한 AI 운영 구조를 제안드립니다.



보안 등급 기반 LLM 라우팅

데이터 등급
첨부파일 포함 여부
사용자 권한
업무 유형
검색 결과 민감도
외부 전송 가능 여부

Secure LLM 라우터 판단

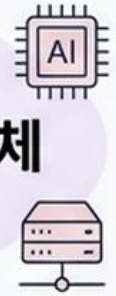
C등급	S등급	O등급
기밀 대외비 개인정보 원문	내부 업무자료 민감 행정자료	공개자료
광역 내부망 LLM	내부망 LLM 우선	2차 AI DLP 통과
범정부 AI 공통기반 제한 처리		
차단 격리 관리자 승인	정책 허용 시 범정부 AI 공통기반 병행	글로벌 LLM API 활용 가능

광역과 기초가 안전하게 AI를 공동 활용할 수 있는 실무적 기반을 구축합니다.



광역자치단체

- AI 공통기반 운영
- 데이터 표준 정립
- 보안정책 일관성
- 모델 라우팅 기준 통합
- 로그·감사체계 관리



기초자치단체

- 대규모 GPU 투자 불필요
- 광역 인프라 공동 활용
- 행정수요 맞춤 서비스
- AI 에이전트 운영

광역·기초 인프라 중복투자 절감	GPU 구매 및 운영 부담 완화	반복 행정업무 생산성 향상	민감정보 유출 위험 감소	AI 답변 신뢰도 및 감사 추적성 강화



- Secure RAG
- Secure LLM 라우터

- 근거문서 관리
- 출처 관리
- 기준일 관리
- 라우팅 이력 관리

- 행정망 환경 맞춤 적용
- 보안정책 반영

- 예산 여건 고려
- 단계적 협의·조정

사업 배경

생성형 AI는 지방행정의 일하는 방식을 혁신하고 보안 기반 위에서 행정의 본질적 역량을 강화합니다.

환경 변화



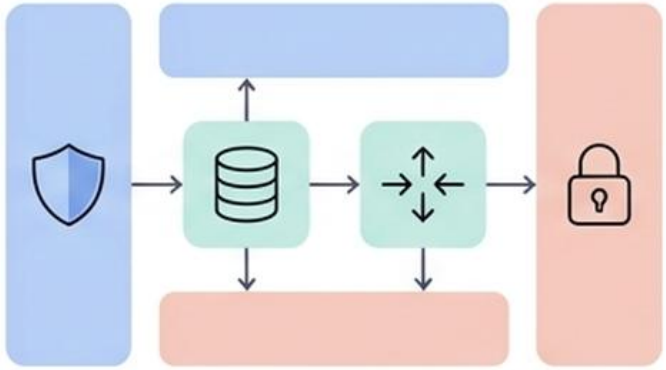
- 공문 작성
- 보고서·회의자료
- 보도자료
- 민원 답변
- 법령·지침 검토
- 정책 참고자료
- 행정업무 복잡화
- 주민 요구 세분화
- 참고자료 증가

생성형 AI 활용



- 지침·과거사례 검색
- 민원 답변 초안 작성
- 회의자료 요약
- 정책 쟁점 정리
- 정책 쟁점 정리
- 자료 탐색 시간 단축
- 초안 작성 효율화
- 판단 지원 도구

보안 기반 설계



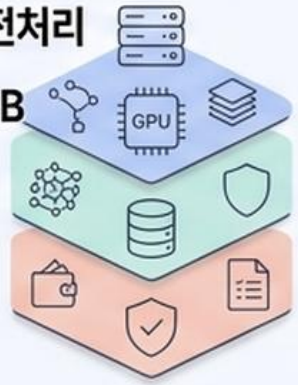
- 행정 데이터 분류
- 권한 기반 검색
- AI 처리 경로 설계
- Secure RAG
- Secure LLM 라우터
- 광역 내부망 LLM
- 범정부 AI 공통기반
- 글로벌 LLM API
- 행정혁신
- 보안책임 확보

광역 공통기반과 기초 특화 서비스의 역할 분담은 부담을 줄이면서 지방정부 전체의 AI 활용 수준을 균형 있게 높입니다.

개별 구축 부담

AI 플랫폼 복합 인프라

데이터 수집·전처리
임베딩·벡터DB
LLM 연계



권한관리
로그감사
DLP
모델 운영
서비스 관리

- 예산 부담
- 운영 인력 필요
- 보안정책 상이
- 데이터 표준 불일치

광역 역할

AI 공통기반

보안정책
데이터 표준
MCP
공통 API
Secure RAG
Secure LLM 라우터

안전한 기반 제공

기초 역할

민원 서비스



- 지역 특화 데이터
- AI 에이전트 운영
- 현장성 반영
- 서비스 신속 도입

인프라 부담 완화 | 자율성 유지 | 도입 속도 향상 | AI 활용 수준 균형 향상

광역 내부망 LLM과 범정부 AI 공통기반의 전략적 결합은 GPU 부담을 완화하면서 보안 기반 AI 처리를 가능하게 합니다.

GPU 부담 현실

고성능 GPU 가격 상승
수급 부담
전력
냉각
서버실 환경
저장장치

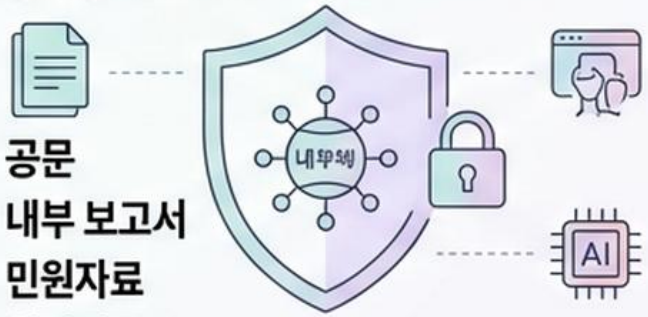


유지보수
보안점검

모델 운영인력
장애 대응체계
총소유비용 증가

내부망 필수 기반

행정망 내부자료

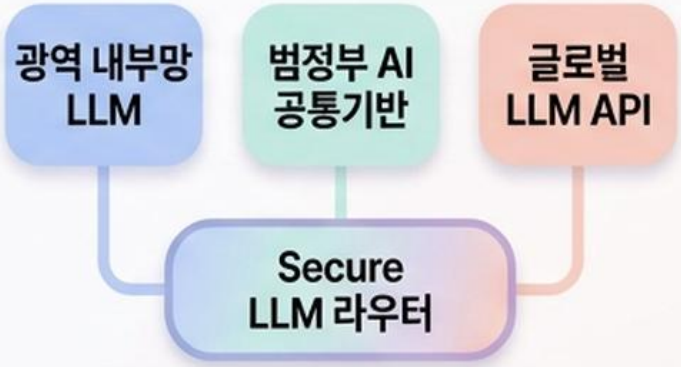


공문
내부 보고서
민원자료
회의자료
비공개 검토자료

외부 LLM 직접
전송 제한
비공개 검토자료

광역 내부망 LLM
GPU 기반 전처리
기본 기반 확보

효율적 자원 배분 구조



광역 내부망 LLM
범정부 AI 공통기반
글로벌 LLM API
대량 처리

공통 행정기능
고성능 모델 보완
GPU 구매 부담 완화
O등급 공개자료 활용

C/S 등급 정책·권한·감사 조건 처리

데이터 등급에 따른 통제형 활용 체계는 보안과 혁신을 동시에 달성하는 기반입니다.

데이터 등급 체계

C등급
(Classified, 기밀)

C등급 (Classified, 기밀)
유출 시 국가 안보나 주요 이익에 심각한 피해를 주는 정보
카주드: 국가 기밀, 핵심 국방 전략, 주요 외교 문서

S등급
(Sensitive, 민감)

S등급 (Sensitive, 민감)
유출 시 법적·재정적 손실 및 심각한 사회적 피해를 주는 정보
카주드: 대규모 개인정보, 핵심 연구개발(R&D) 기술, 재무 및 계약 정보

O등급
(Open, 공개)

O등급 (Open, 공개)
누구나 접근 가능한 공공 정보
카주즈: 홈페이지 안내문, 일반 홍보자료

글로벌 LLM 통제형 활용



행정망 데이터는 보안 등급과 권한 체계, 감사 기록 안에서 관리될 때 안전하게 AI에 활용될 수 있습니다.

행정망 데이터 자산



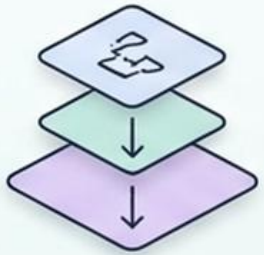


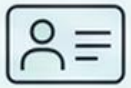




- 전자문서
- 업무보고자료
- 민원자료
- 신청·허가·점검자료
- 회의자료
- 공간정보
- 통계자료
- 내부 지침
- 업무편람
- 부서 내부 검토자료
- 권한 기반 열람 자료

권한·등급 통제









- 사용자 인증
- 소속기관 기반 권한관리
- 부서 기반 권한관리
- 직무 기반 권한관리
- 데이터별 접근권한
- 보안 등급 관리
- 검색 범위 제어
- 권한 없는 문서 차단
- 열람 권한 우회 방지

감사·추적 체계

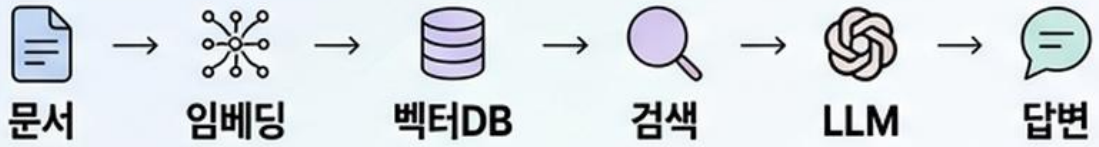




- 질문 기록
- 검색 문서 기록
- 보안 등급 판단 기록
- LLM 경로 선택 기록
- 외부 전송 여부 기록
- 응답 생성 근거 기록
- Secure RAG
- 2차 AI DLP
- Secure LLM 라우터
- 처리 이력 관리
- 사전 설계 기반 통제

기존 RAG와 일반 DLP의 한계를 보완하려면 데이터 전 과정과 LLM 경로를 통합 통제하는 구조가 필요합니다.

1 기존 방식 구조



- 임베딩 전 민감정보 제거 미흡
- 벡터DB 민감정보 포함 가능성
- 권한관리 미흡 시 검색 위험

부분 통제, 구조적 한계

패턴 기반 DLP

- 주민등록번호
- 전화번호
- 이메일
- 계좌번호

AI 기반 DLP

- 문맥 판단 가능
- 처리비용 증가
- 응답속도 부담
- 설명가능성 한계

부분식 구조적 한계

2 Secure RAG 구조



- 행정망 데이터 수집
- 명확한 민감정보 탐지, 마스킹
- 임베딩 전 차단
- 임베딩
- 벡터DB 적재
- 권한 기반 검색
- 검색 결과 재검증
- 질의 문맥 분석
- 보안 등급 재판단

3 Secure LLM 라우터 분기



- 민감자료 기본 경로
- 피크타임 등 조건부 활용
- 0등급 한정 활용

전 과정 통제 | **권한 기반 접근** | **보안 등급 분기** | **행정망 적용 안전성 확보**

사업 목적

광역자치단체 중심의 AI 공통기반은
지방정부 전체의 안전하고 일관된 AI 활용을 가능하게 합니다.

개별 구축 한계



기관별 AI 시스템 구축

예산 중복

인력 중복

보안정책 상이

데이터 기준 불일치

광역 공통기반



공통 인프라

보안정책

데이터 표준

MCP

공통 API

Secure RAG

Secure LLM 라우터

광역 중심 통합 운영

기대 효과



기초자치단체 공동 활용

대규모 인프라 부담 완화

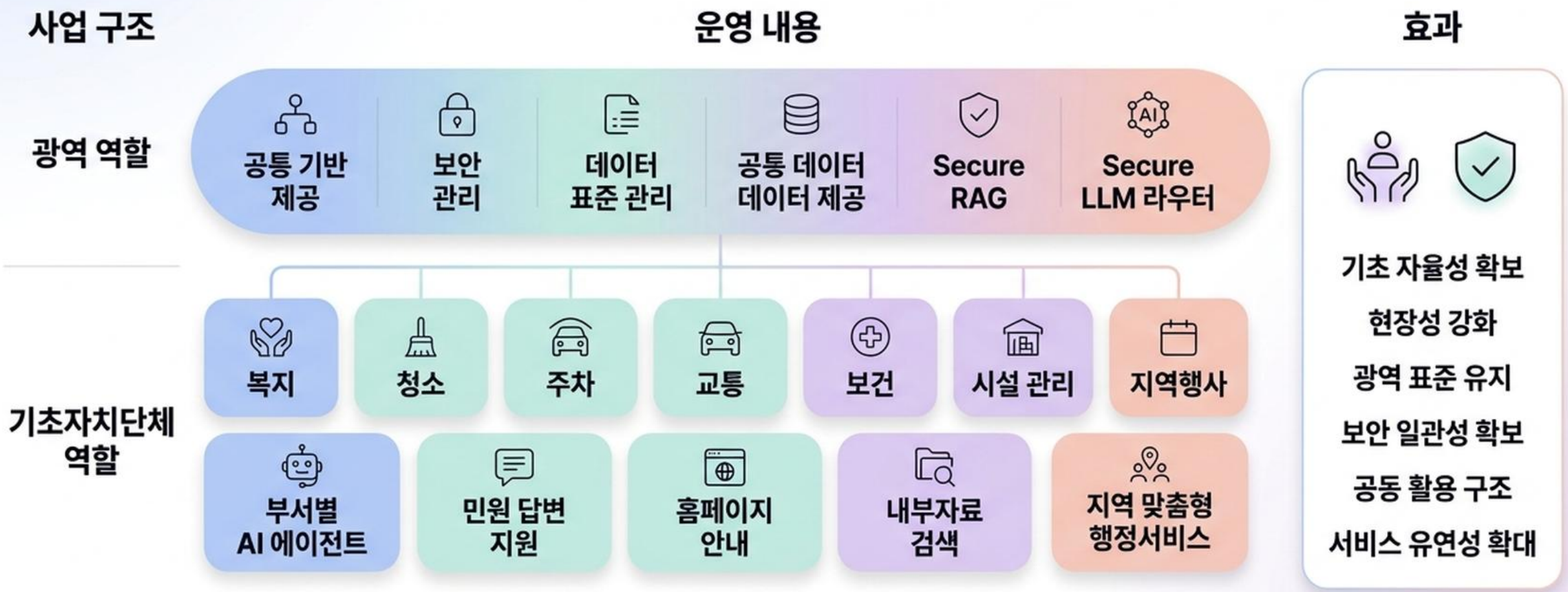
단계적 서비스 도입

AI 도입 격차 완화

행정망 데이터 신뢰성 향상

지방정부 전체 활용 기반 확보

광역 공통기반 위에서 기초자치단체는 지역 특성을 반영한 AI 서비스와 에이전트를 자율적으로 운영할 수 있습니다.



행정망 데이터는 수집부터 검색·활용까지
전 과정이 체계화될 때 안전한 지식자산으로 전환됩니다.

데이터 수집



업무시스템 데이터
행정망 데이터 통합 수집

전처리



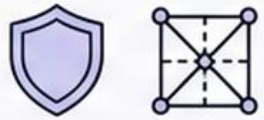
AI OCR
STT/TTS
데이터 정제
형식 표준화

데이터 카탈로그



출처 등록
소관부서
기준일
갱신주기
접근권한
보안 등급
메타데이터 관리

보안 및 임베딩



1차 패턴 DLP
보안 등급 분류
3072차원 임베딩
벡터DB 적재
권한 기반 검색
2차 AI DLP

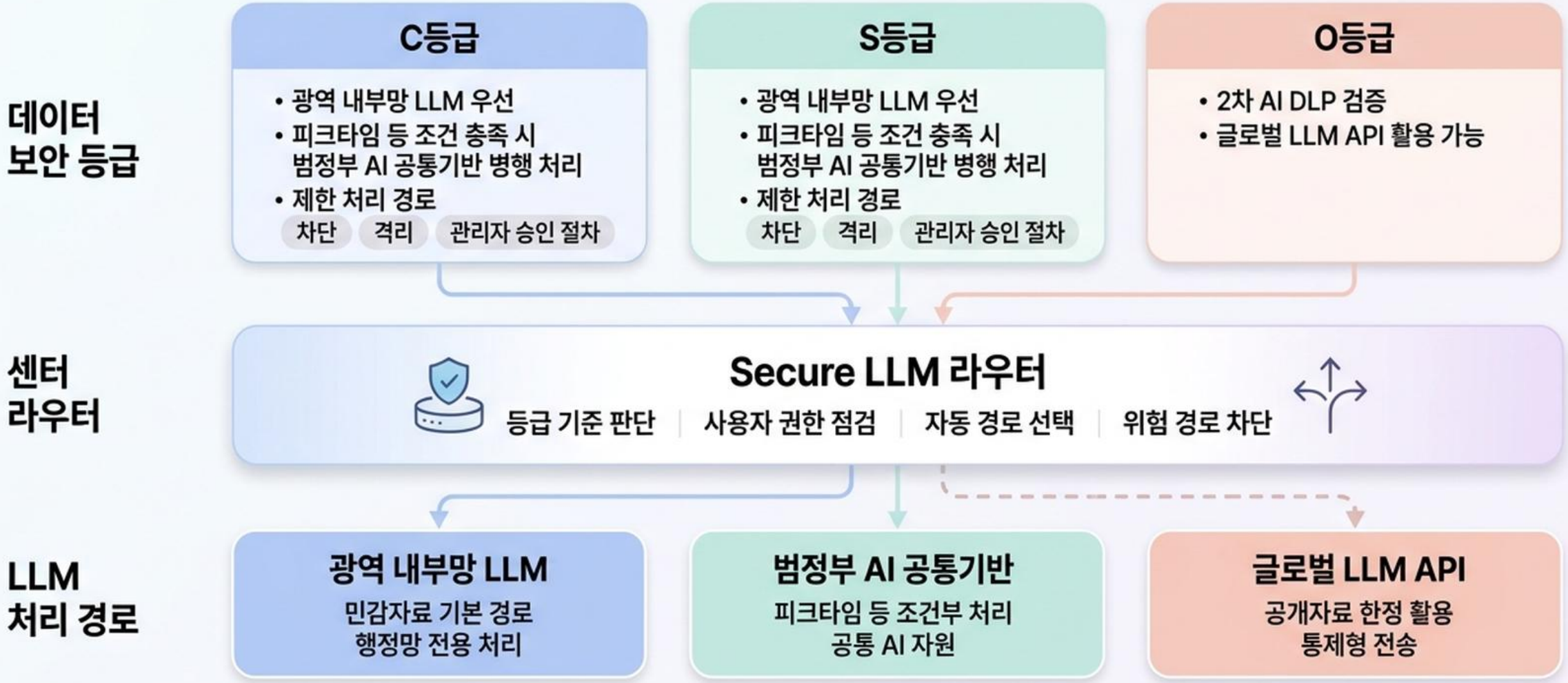
LLM 활용



근거자료 검색
출처 확인
기준일 확인
안전한 LLM 응답 활용
지식자산 전환

부서별 분산 자료 통합 보안·권한 적용 AI 활용 기반기반 확보

보안 등급 기반 자동 라우팅 체계는 안전성과 업무 연속성을 동시에 확보합니다.



개인정보 보호와 AI 활용성은 통제된 구조 안에서 균형 있게 운영되어야 합니다.

1. 균형의 필요성

보안을 이유로 전면 차단
행정혁신 기회 상실

균형 있는 운영체계

편의성 중심 외부 전송
공공기관 책임 위험

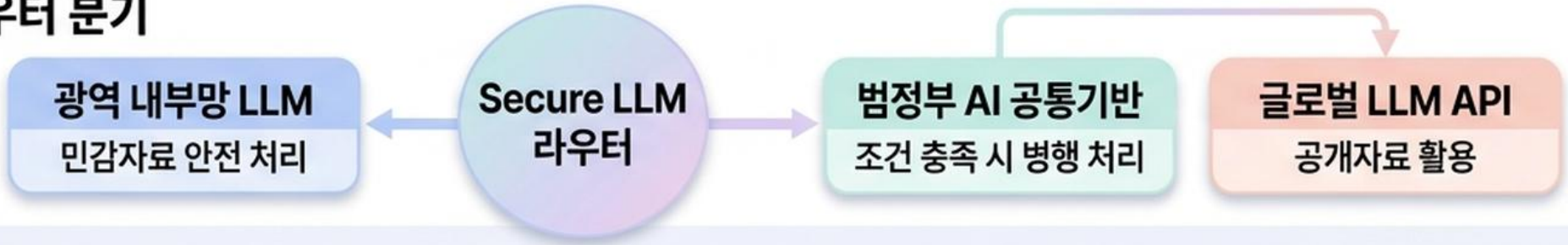
2. Secure RAG 구조

1차 패턴 DLP
개인정보 탐지 | 민감정보 탐지 | 임베딩 전 차단

→ 임베딩 → 권한 기반 검색 →

2차 AI DLP
문맥상 민감성 재검토

3. Secure LLM 라우터 분기



민감자료 행정망 내 처리 | 공개자료 최신 AI 활용 | 공공성과 효율성 동시 확보

광역 내부망 LLM을 중심으로 안정성과 확장성을 결합한 행정 AI 운영 기반을 마련합니다.

중심 AI 플랫폼

광역 내부망 LLM

- 행정망 내부자료 기본 경로
- 권한관리
- 장애 대응
- 데이터 보호
- 모델 교체 안정성
- 직접 통제 구조

보조 AI 플랫폼

범정부 AI 공통기반

- 행정망 내 공통 AI 자원
- 공통 기능 활용
- 처리량 보완
- 운영 부담 완화

GPU 비용 증가
운영 부담 증가
단독 처리 한계

내부망 LLM 중심 운영 | 범정부 AI 공통기반 연동 | 안정성과 확장성 결합

광역·기초 공동활용 구조는 중복투자를 줄이고 공공 AI의 효율성과 가치를 동시에 높입니다.

1. 중복투자 부담 요소

- 초기 구축비
- 운영비
- 모델 교체비 GPU 증설비
- 데이터 갱신비
- 보안점검비
- 사용자 교육비
- 기관별 개별 부담
- 예산 효율성 저하
- 서비스 품질 격차

2. 광역·기초 공동활용 구조

광역

- 공통 인프라 관리
- 보안체계 관리
- 표준 관리
- 범정부 AI 공통기반 연계

공동 활용 | 역할 분담 | 중복투자 절감

기초

- 개별 서비스 운영
- 선택적 확장
- 자체 데이터 활용
- 지역 특화 서비스

3. 기대 효과

GPU 직접 구매 부담 완화

- GPU 직접 구매 부담 완화
- 전국 단위 공통 AI 자원 연계
- 현장 서비스 효율 연결 안전한 협력 구조
- 공직자 업무 부담 경감
- 신속한 행정서비스
- 신속한 행정서비스
- 공공 가치 창출

중복투자 감소 | 운영 효율 향상 | 보안 유지 | 지속가능한 행정 AI 기반

사업 추진 전략

광역은 공통 기반과 보안을 책임지고
기초는 지역특화 서비스를 운영하는 역할 분담 구조로 추진합니다.

광역 역할

- 공통 인프라 제공
- 보안체계 관리
- 데이터 관리 기준
- LLM 운영 기준
- Secure RAG
- Secure LLM 라우터
- 내부망 LLM
- 범정부 AI 공통기반 연계
- 데이터 카탈로그
- 공통 API
- MCP 기반 연계체계
- 권한관리
- 감사체계

복합 인프라 특성

- 모델 라우팅
- 로그감사
- 권한관리
- 응답 생성
- 검색
- 전처리
- 데이터 수집

예산 중복 보안정책 불일치 | 데이터 품질 편차 운영인력 부담

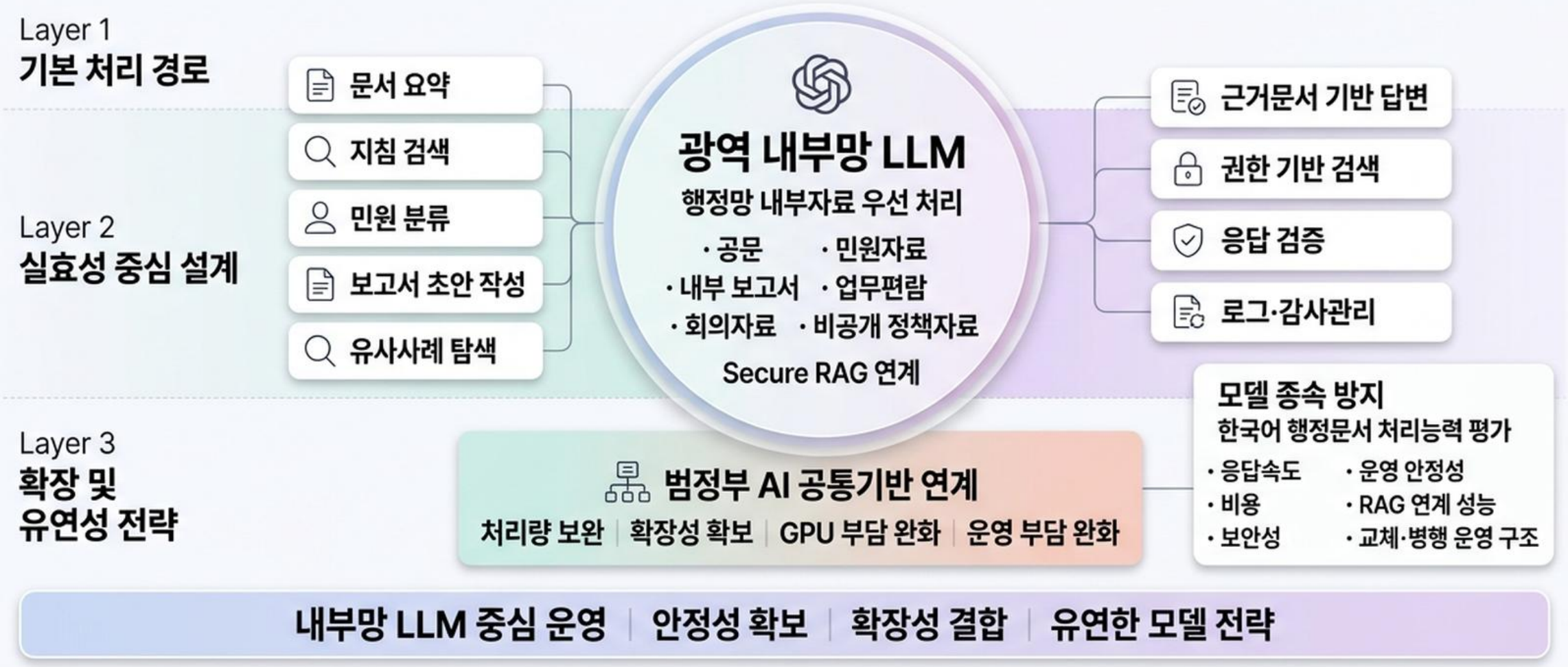
기초 역할 및 추진 방식

- 민원
- 복지
- 교통
- 환경
- 시설관리
- 지역행사
- 생활정보
- 부서별 AI 에이전트

- 선택형 참여
- 단계적 확산
- 공동 운영협의체 기반 운영

보안과 표준 책임 | 현장성과 자율성 반영 | 중복 구축 최소화 | 효율적 공동 활용 구조

내부망 LLM을 중심으로 하되 범정부 AI 공통기반을 연계하는 하이브리드 운영 전략을 적용합니다.



범정부 AI 공통기반은 내부망 LLM과 역할을 분담하여 행정망 내 공통 AI 처리 자원으로 활용합니다.

개념 구분

범정부 AI 공통기반

- 행정망 내 공통 AI 처리 자원
- 내부망 LLM 준하는 보안 수준

글로벌 LLM API

- 외부 민간 서비스
- 공개자료 중심 활용

역할 분담 구조

광역 내부망 LLM

- 민감자료 기본 경로
- 통제 기반 처리

Secure LLM 라우터

범정부 AI 공통기반

- C/S 등급 조건부 처리
- 기관 보안정책 충족
- 사용자 권한 적용
- 전송 통제
- 감사로그 관리

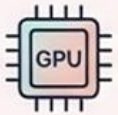
글로벌 LLM API

- O등급 한정 활용

전략적 활용 범위



- 대량 처리
- 피크 부하 대응
- 공통 행정기능 처리



- 고성능 모델 보완



- 비용 효율화
- GPU 직접 구매 부담 완화



- 분산 처리 구조
- 초기 설계 단계 통합 설계

내부망 중심 구조 | **병행·보완적 활용** | **보안 수준 차등 적용** | **운영 리스크 완화**

글로벌 LLM API는 공개 가능 데이터에 한해 Secure LLM 라우터 통제 아래 활용합니다.

활용 가능 영역

- O등급 공개 가능 데이터
- 홈페이지 공개자료
- 보도자료
- 공고문
- 일반 정책자료
- 대외 공개용 문안
- 공개 통계 설명
- 외부 리서치
- 2차 AI DLP 검증
- 데이터 최소화 절차

전송 차단 대상

- 개인정보
- 비공개 민원자료
- 내부 검토자료
- 감사·인사자료
- 비공개 정책 초안

- 행정망 내부자료 직접 전송 금지

자동 통제 구조



최신 AI 성능 활용 | 데이터 보호 책임 준수 | 통제형 활용 전략 | 보안과 혁신 균형

Secure RAG는 데이터 수집부터 LLM 전달까지 전 과정을 통제하는 생애주기 보안관리 체계입니다.

1



데이터 수집

원천 시스템 확인
문서 출처 확인
데이터 카탈로그 등록

소관부서
기준일
갱신주기
접근권한
보안 등급

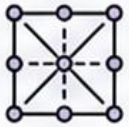
2



임베딩 전 보안 통제

1차 패턴 DLP
주민등록번호 탐지
연락처 탐지
계좌번호 탐지
이메일 탐지
카드번호 탐지
민감 키워드 탐지
마스킹
제외 , 격리

3



임베딩 및 저장

보안 등급 판단
임베딩 가능 여부 판단
3072차원 임베딩
벡터DB 분리 저장
기관 기준 분리
부서 기준 분리
업무 기준 분리
권한 기준 분리

4



검색 및 검증

권한 범위 내 검색
근거문서 제공
출처 제공
기준일 제공

2차 AI DLP
문맥 재검증
LLM 전달 가능
여부 판단

5

통합 통제

데이터 수집 통제
전처리 통제
임베딩 통제
검색 통제
LLM 전달 통제
응답 생성 통제
로그관리

정확도 향상 보안 유지 책임성 확보 공공기관 운영 기반

Secure LLM 라우터는 보안 등급과 권한을 기준으로 최적의 LLM 처리 경로를 자동 선택합니다.



데이터 우선 원칙 | 사용자 선택보다 등급 우선 | 안전한 대체 경로 제공 | 업무 연속성 확보

GPU 기반 전처리 서버는 비정형 행정 데이터를 Secure RAG로 연결하는 핵심 기반입니다.



단계별 구축과 검증을 통해 안전성과 확장성을 동시에 확보합니다.

Step 1



데이터 현황 진단

대상 시스템 분석

보안정책 점검

권한체계 점검

범정부 AI 공통기반 연계 조건 진단

Step 2



Secure RAG 통합 설계

Secure LLM 라우터 설계

내부망 LLM 설계

범정부 AI 공통기반 연계 설계

역할 분담 구조 확정

Step 3



데이터 카탈로그 구축

1차 DLP 적용

3072차원 임베딩

벡터DB 구축

검색 기능 구축

2차 AI DLP 적용

Secure RAG 시범 구축

Step 4



Secure LLM 라우터 검증

광역 내부망 LLM 처리 검증

범정부 AI 공통기반 병행 처리 검증

C/S/O 등급 기준 점검

비용 점검

성능 점검

보안로그 점검

관리자 승인 절차 점검

Step 5



기초자치단체 선택적 연계

개별 서비스 확산

AI 에이전트 확산

공동 운영 체계 확장

Step 6



O등급 공개자료 중심 글로벌 LLM API 통제형 연계

모델 교체

보안정책 보완

품질관리

비용 최적화

지속 고도화

단계적 확산, 통합 설계 기반 추진, 보안 검증 중심 운영, 지속적 개선 구조

핵심 구현 사항

데이터 카탈로그는 행정 AI 신뢰성과 데이터 거버넌스를 결정하는 핵심 기반입니다.

데이터 카탈로그

사업 목적



- 본 사업의 출발점
- 데이터 위치 관리
- 관리 주체 명확화
- 기준 시점 관리
- 접근 권한 정의
- 보안 등급 관리
- 체계적 등록·관리 기반

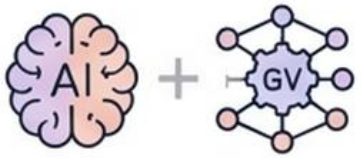
관리 체계

광역자치단체	기초자치단체
공통 데이터 카탈로그 기준 기준 마련	데이터 출처 관리 소관부서 관리 갱신주기 관리 공개 가능 여부 관리 민감정보 포함 여부 관리

문서 PDF 이미지 도면

표 음성 업무시스템 데이터

활용 및 효과



- 근거문서 제시
- 데이터 품질관리
- 기준일 표시
- 자료 폐기 관리
- 권한 기반 검색
- 자료 갱신 관리
- 데이터 품질관리
- 최신성 확보
- 정확성 확보
- 소관부서 명확성 확보
- 행정 데이터 거버넌스 핵심 요소

1차 패턴 DLP는 벡터DB 오염을 사전에 차단하는 행정 AI 보안의 핵심 통제 장치입니다.



탐지 대상

주민등록번호
외국인등록번호
전화번호
휴대전화번호
이메일
계좌번호
카드번호
주소
특정 민감 키워드
패턴 기반 식별 정보



적용 시점 및 위험

임베딩 이전 단계 탐지
벡터DB 적재 전 차단
수정 어려움 예방
검색·응답 노출 위험 차단
민감정보 임베딩 방지
사전 통제 체계 구축



처리 정책

정책 기반 처리
마스킹
임베딩 제외
격리
관리자 검토
금칙어 추가 관리
내부 문서 표기 관리
보안 등급 문구 관리
기관별 운영정책 수립

출력 필터가 아닌 사전 예방 통제 체계

보안 등급 분류는 Secure RAG와 Secure LLM 라우터를 연결하는 핵심 통제 기준입니다.

C/S/O 등급 체계

C등급

기밀자료, 대외비,
개인정보 원문,
감사 관련 자료,
인사 관련 자료,
보안 관련 자료,
외부 민간 LLM 전송 금지

S등급

내부 업무자료,
비공개 행정자료,
민감 민원자료,
내부망 LLM 우선 처리,
조건 충족 시 범정부 AI
공통기반 병행 처리

O등급

홈페이지 공개자료,
보도자료, 공고,
일반 정책자료,
2차 AI DLP 검증,
글로벌 LLM API
활용 검토

처리 경로 다이어그램



보안 등급 조정 기준

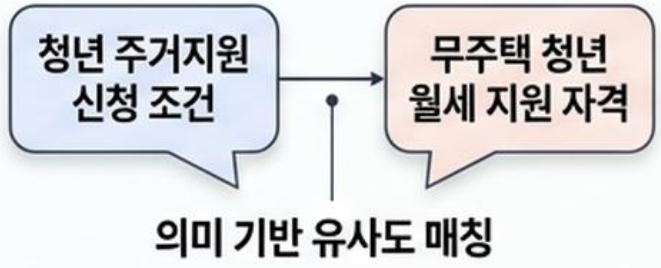


3072차원 데이터 임베딩은 행정문서 기반 AI 검색 정밀도를 높이는 핵심 기술입니다.

개념 설명

3072차원 데이터 임베딩

- 의미 기반 검색
- 고차원 벡터화
- 키워드 불일치 보완
- 문맥 이해 강화



수행 원칙

1차 패턴 DLP → 보안 등급 분류 → 임베딩 수행 → 벡터DB 저장

임베딩 허용 데이터만 벡터화
임베딩 모델 버전 관리
처리 일시 기록
원문 출처 관리
소관부서 관리
보안 등급 연계 관리

행정적 효과

행정적 효과

- 근거문서 신속 탐색
- 표현 차이 극복
- 의미 유사 자료 검색
- 실제 문서 기반 답변
- 업무 처리 속도 향상
- 답변 신뢰성 강화

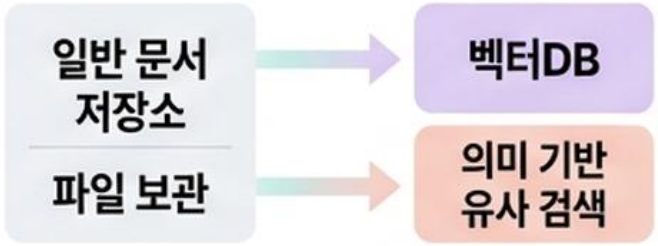
세부 알고리즘보다 행정적 효과 중심 설명

벡터DB는 보안과 권한이 반영된 의미 기반 행정 검색 인프라입니다.

개념

벡터DB는 전통 서장자료리부의
의미 기반 행정 검색 대프입니다.

- 임베딩된 행정자료 저장
- 의미 정보 기반 검색
- 유사 내용 신속 탐색
- 단순 파일 저장소와 차별화
- 보안 반영 검색 기반



구조 분리

광역·기초 분리 구조

- 광역 공통 벡터DB
- 공통 지침
- 공통 업무편람
- 공개자료
- 광역 표준 데이터
- 기초 개별 벡터DB
- 자체 행정자료
- 지역 특화 데이터

운영 원칙

많이 적재보다 정확한 적재
오래된 자료 관리
중복 자료 정비
기준일 명확화
소관부서 명확화
데이터 카탈로그 연계
갱신주기 관리
폐기정책 관리
권한관리 연계
AI 답변 품질 유지

안전성과 정확성 중심 운영

검색 엔진은 권한 기반 근거문서 탐색을 통해 책임 있는 AI 활용을 지원합니다.

+ 하이브리드 검색 구조

하이브리드 검색

키워드 검색

- 법령명 탐색
- 사업명 탐색
- 부서명 탐색
- 고시번호 탐색
- 명확 표현 검색

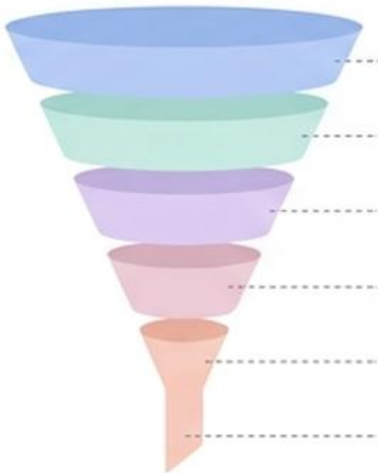
하이브리드 검색 결합

벡터 검색

- 의미 유사 문서 탐색
- 표현 차이 극복
- 문맥 기반 검색
- 유사 질의 대응

권한 연계 구조

권한 기반 검색



- 소속기관 반영
- 부서 반영
- 직무 반영
- 권한 반영
- 권한 없는 자료 제외
- AI 응답 근거 제한

검색 결과 제공 요소

검색 결과 구성

- 근거문서
- 출처
- 기준일
- 소관부서
- 근거 확인 후 문서 완성
- 담당자 최종 판단

책임 있는 AI 활용 기반

2차 AI DLP는 문맥 기반 재검증을 통해 민감정보 노출을 예방하는 핵심 통제 체계입니다.

개념 비교

2차 AI DLP

1차 패턴 DLP

- 주민등록번호 탐지
- 전화번호 탐지
- 계좌번호 탐지
- 정형 패턴 기반 탐지

2차 AI DLP

- 문장 의미 분석
- 조합 관계 판단
- 문맥 단위 재검증
- 비정형 민감성 판단

탐지 필요성 사례

민감정보 판단 사례

- 민원 내용
- 위치 정보
- 사건 경위
- 부서 내부 검토 의견

결합 시 민감정보 가능

- 문서 제목 비민감 표시
- 본문 비공개 검토자료

단순 패턴 방식 한계

동작 방식 및 등급 조정

검색 결과 → 2차 AI DLP 점검 → 보안 등급 재판단 → LLM 전달

- O등급 자료 재검토
- 내부 판단자료 포함 시 S등급 상향
- 민감 민원정보 재분류
- LLM 응답 생성 후 재검사
- 최종 출력 민감정보 점검

문맥 기반 보안 강화

Secure LLM 라우터는 보안 등급과 권한을 기반으로 최적의 처리 경로를 자동 결정하는 제어 장치입니다.

판단 기준



라우팅 구조



Secure LLM 라우터

1 내부망 LLM
기본 처리 원칙

2 범정부 AI 공통기반
- 내부망 준하는 보안 수준
- 정책 조건 충족 시 C/S 등급 처리 가능

3 글로벌 LLM API
- O등급 공개 가능 데이터 중심
- 외부 전송 제한 적용

효과 및 통제



보안 사고 예방
- 외부 민간 LLM 전송 차단
- 자동 내부망 전환

업무 연속성 확보
- 단순 차단 지양
- 안진한 대체 경로 제시

감사 및 기록 관리
- 모든 판단 로그 기록
- 사후 감사 활용
- 정책 개선 반영

보안 강화와 업무 지속성 동시 확보

AI OCR·STT/TTS 기반 전처리는 비정형 행정데이터를 AI 활용 가능 자산으로 전환하는 핵심 기반입니다.

대상 데이터

비정형 데이터

- 스캔 문서
- 이미지
- 도면
- 표
- 손글씨
- 회의 녹취
- 민원 상담 음성
- 현장 점검 음성

텍스트화 필요

검색 · 임베딩 · DLP · RAG 활용 기반

기술 기능

AI OCR

- 이미지 텍스트 추출
- 도면 텍스트 인식
- 표 구조 인식
- 문서 레이아웃 인식
- 행정문서 검색 활용

STT

- 회의 음성 텍스트 변환
- 상담 음성 변환
- 민원 통화 변환
- 회의록 작성
- 민원 분류
- 주요 쟁점 정리

TTS

- 대민 안내 확장
- 정보 접근성 향상
- 음성 기반 행정서비스

보안 연계

개인정보 포함 가능성 높음

LLM 직접 전달 금지

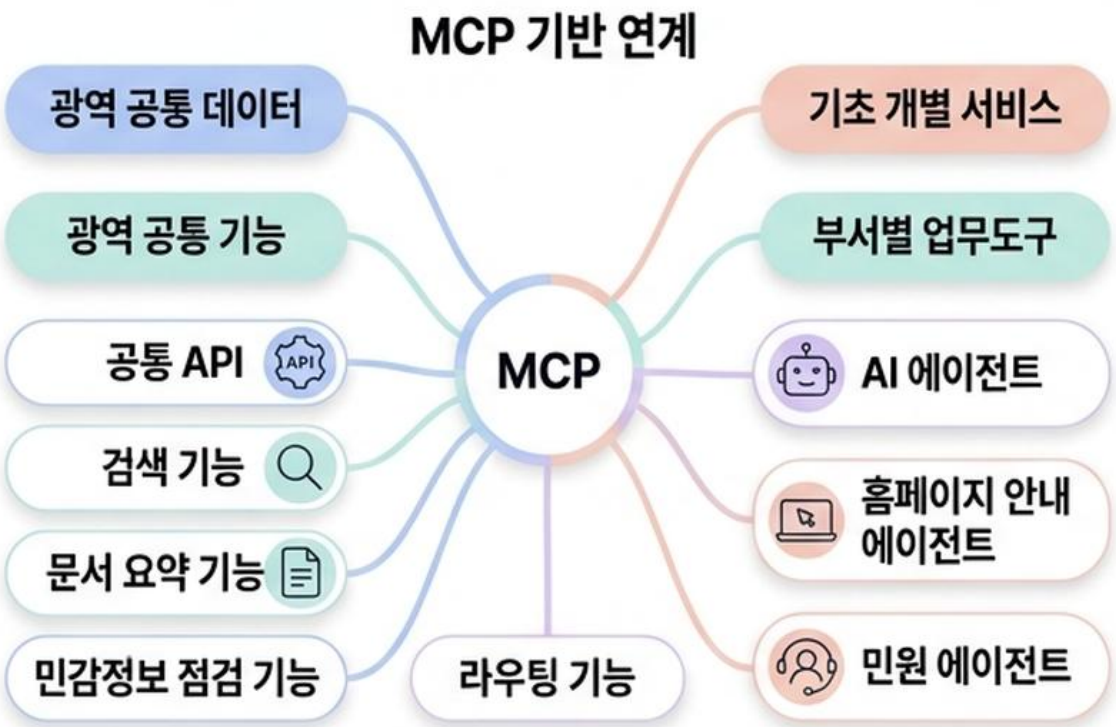
보안 보안통제 하 관리

1. 전처리 텍스트
2. 데이터 카탈로그 등록
3. 1차 DLP
4. 보안 등급 분류
5. 임베딩 가능 여부 판단
6. Secure RAG 편입

비정형 데이터의 안전한 AI 자산화

MCP 기반 연계는 광역 공통 기능과 기초 특화 서비스를 유연하게 연결하는 확장 구조입니다.

구조 개념



활용 시나리오

시나리오 1

- 홈페이지 안내 에이전트
- 광역 공통 정책자료 참조

표준화된 호출 구조

시나리오 2

- 부서별 민원 에이전트
- 자체 데이터 검색
- 광역 공통 업무편람 병행 검색

효과 및 튼영 원칙



효과

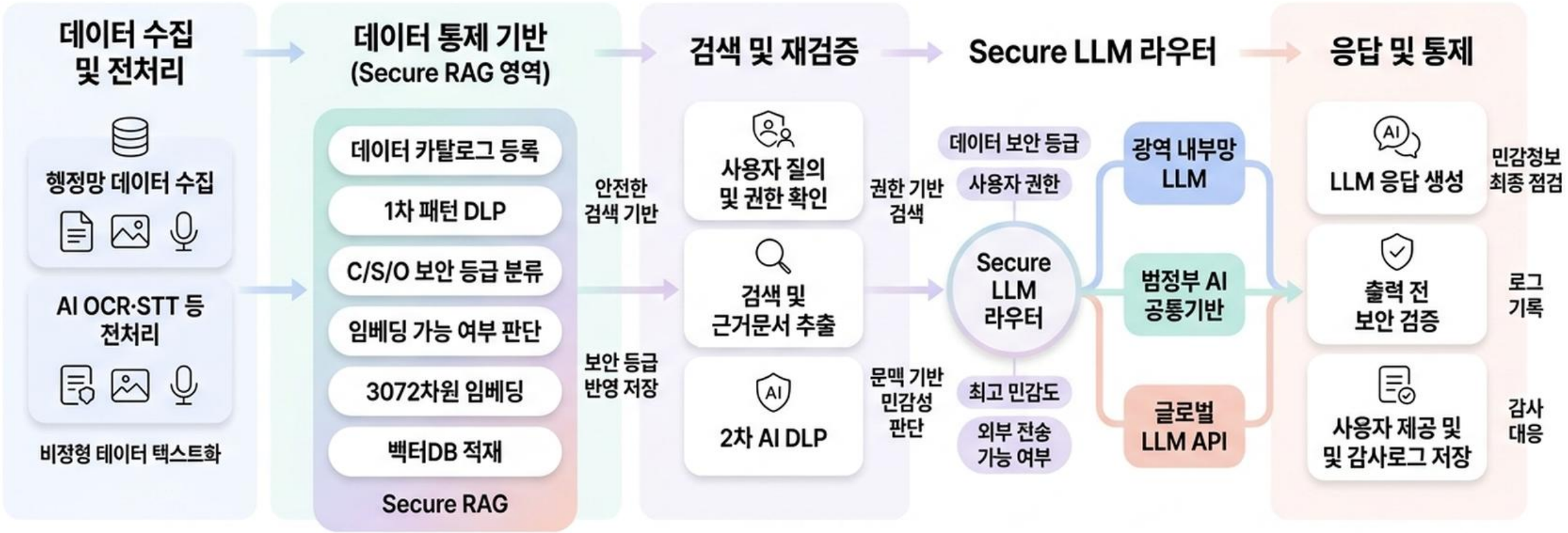
- 중복 개발 최소화
- 서비스 확장성 향상
- 공통 기능 안정 제공
- 지역 특화 서비스 구성

운영 원칙

- 권한관리 연계
- 보안 등급 반영
- 로그감사 체계 운영

확장성과 통제의 균형 구조

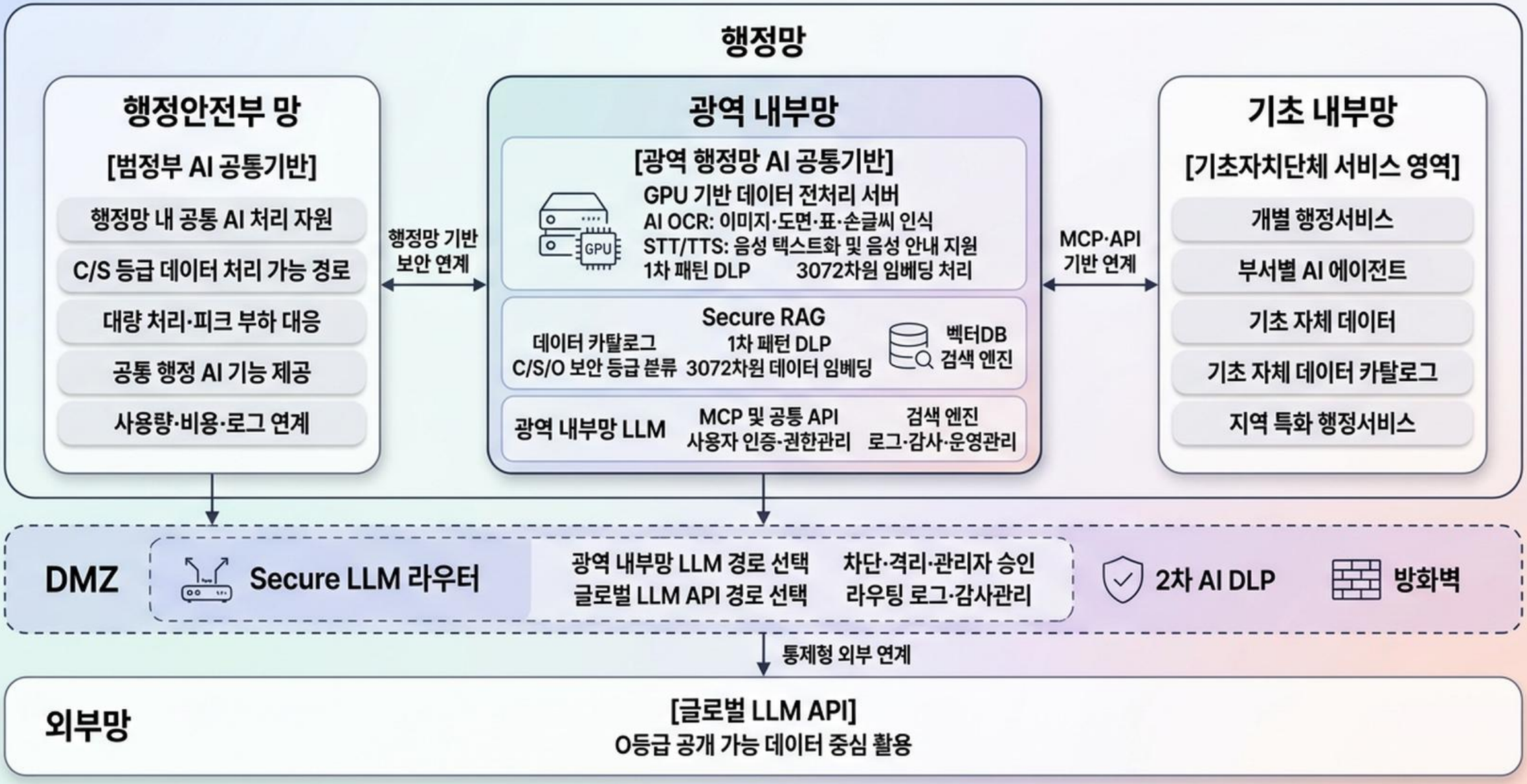
행정 데이터 수집부터 보안 등급 기반 LLM 응답까지 전 과정을 통합 통제하는 안전한 행정 AI 아키텍처입니다.



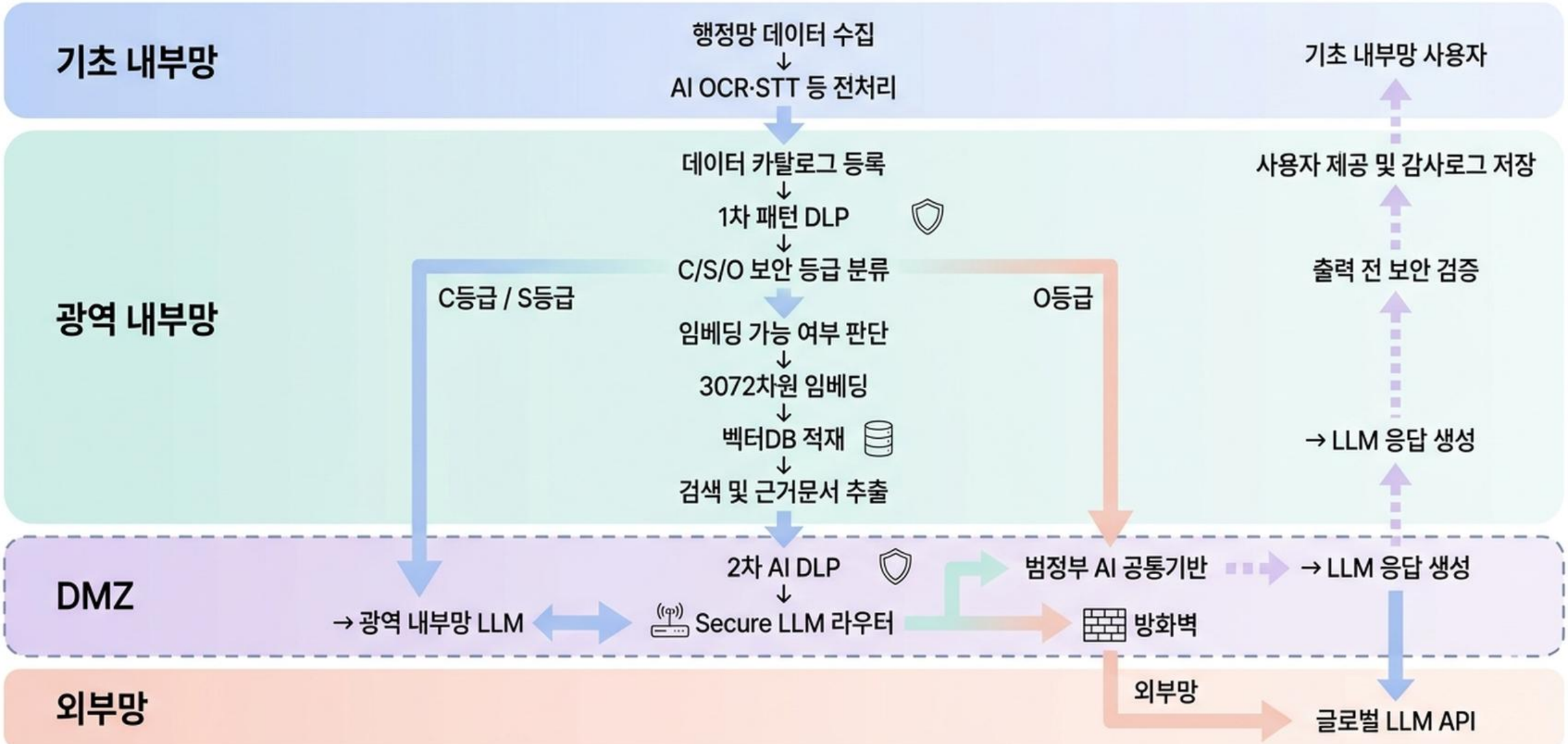
안전성 · 책임성 · 확장성 기반 광역·기초 통합 행정 AI 운영체계

구현 방안

전체 시스템 구성도


행정망
행정안전부 망
[범정부 AI 공통기반]
행정망 내 공통 AI 처리 자원
C/S 등급 데이터 처리 가능 경로
대량 처리·피크 부하 대응
공통 행정 AI 기능 제공
사용량·비용·로그 연계
행정망 기반
보안 연계
광역 내부망
[광역 행정망 AI 공통기반]
GPU
GPU 기반 데이터 전처리 서버
AI OCR: 이미지·도면·표·손글씨 인식
STT/TTS: 음성 텍스트화 및 음성 안내 지원
1차 패턴 DLP
3072차원 임베딩 처리
Secure RAG
데이터 카탈로그
C/S/O 보안 등급 분류
1차 패턴 DLP
3072차원 데이터 임베딩
벡터DB
검색 엔진
광역 내부망 LLM
MCP 및 공통 API
사용자 인증·권한관리
검색 엔진
로그·감사·운영관리
MCP·API
기반 연계
기초 내부망
[기초자치단체 서비스 영역]
개별 행정서비스
부서별 AI 에이전트
기초 자체 데이터
기초 자체 데이터 카탈로그
지역 특화 행정서비스
DMZ
Secure LLM 라우터
광역 내부망 LLM 경로 선택
글로벌 LLM API 경로 선택
차단·격리·관리자 승인
라우팅 로그·감사관리
2차 AI DLP
방화벽
통제형 외부 연계
외부망
[글로벌 LLM API]
O등급 공개 가능 데이터 중심 활용

데이터 흐름도


기초 내부망
행정망 데이터 수집
AI OCR·STT 등 전처리
기초 내부망 사용자
광역 내부망
데이터 카탈로그 등록
1차 패턴 DLP
C/S/O 보안 등급 분류
C등급 / S등급
O등급
임베딩 가능 여부 판단
3072차원 임베딩
벡터DB 적재
검색 및 근거문서 추출
사용자 제공 및 감사로그 저장
출력 전 보안 검증
→ LLM 응답 생성
DMZ
2차 AI DLP
→ 광역 내부망 LLM
Secure LLM 라우터
범정부 AI 공통기반
방화벽
→ LLM 응답 생성
외부망
외부망
글로벌 LLM API

광역은 보안과 표준을 책임지고
기초는 지역 특화 서비스를 운영하는 구조로 설계되어야 합니다.

광역 AI 공통기반 구성 방안

데이터 관리	데이터 카탈로그 | 데이터 출처 관리 | 소관부서 관리 | 기준일 관리 갱신주기 관리 | 접근 권한 관리 | 보안 등급 관리
사전 보안	1차 패턴 DLP | 개인정보 탐지 | 고유식별정보 탐지 | 민감 키워드 탐지 | 마스킹
의미 검색	3072차원 임베딩 | 벡터DB | 행정문서 의미 기반 검색 환경 구축
검색 통제	검색 엔진 | 사용자 권한 내 근거문서 검색 | 출처 제공
문맥 보안	2차 AI DLP | 검색 결과 민감도 재검증 | 질의 문맥 분석
모델 분기	Secure LLM 라우터 | 보안 등급별 LLM 경로 자동 선택
AI 처리	내부망 LLM | 행정자료 기반 검색 | 요약 지원 | 작성 지원
공통 연계	MCP·공통 API | 기초 서비스 공통 기능 호출 | 에이전트 기능 연계
운영관리	로그 관리 | 감사 관리 | 정책관리 | 질의 이력 관리 | 검색 이력 관리 | 라우팅 이력 관리 | 응답 이력 관리 | 외부 전송 이력 관리



공통 인프라 | 보안 체계 | 데이터 기준 | LLM 운영 기준 | 전 과정 관리

광역 공통기반과 기초 서비스의 권한 기반 연계 구조로 안정적인 AI 행정체계를 구현합니다.

기초자치단체 개별 서비스 및 에이전트 연계 방안

광역 AI 공통기반

- 공통 데이터
- 공통 검색
- Secure LLM 라우터
- 내부망 LLM
- Secure RAG
- 범정부 AI 공통기반 연계
- MCP·공통 API
- 보안·감사 정책

MCP·API 기반 연계

기초자치단체

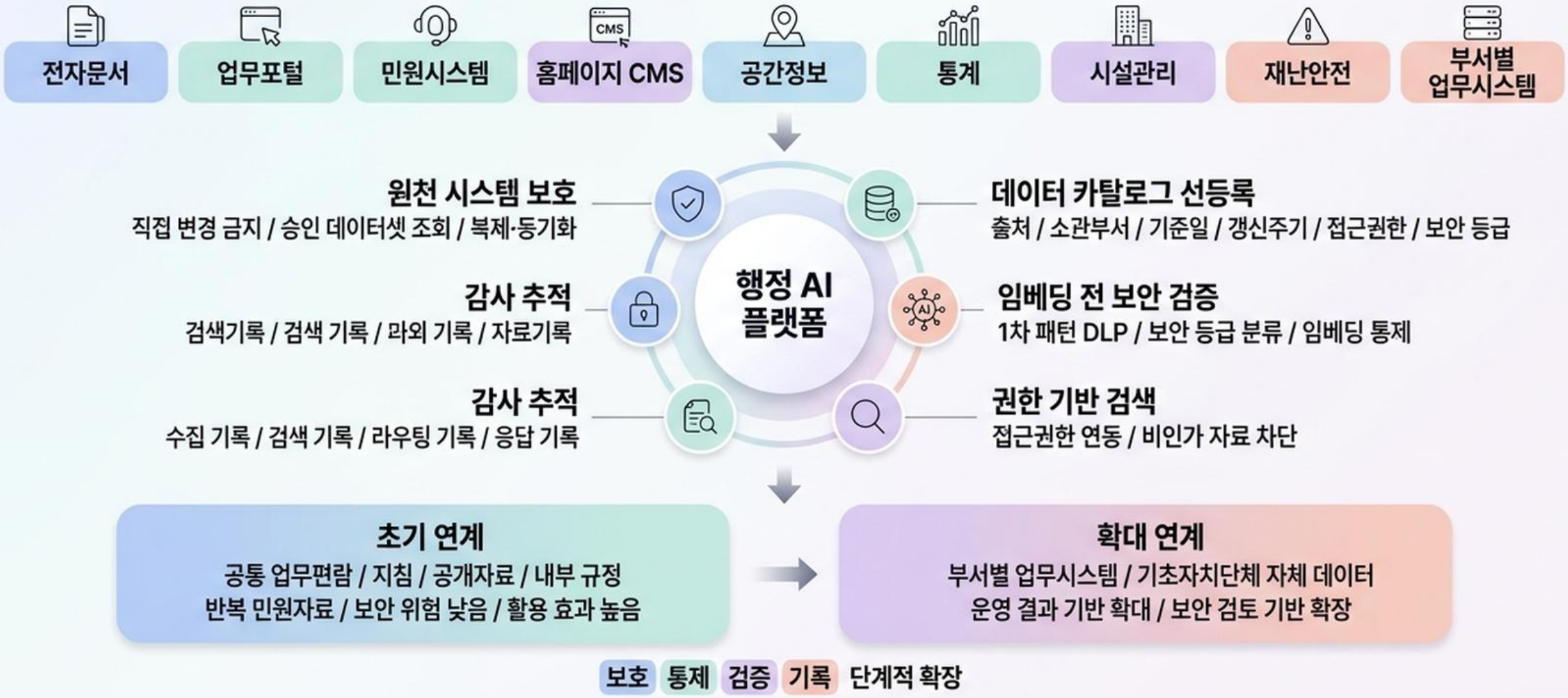
- 자체 행정서비스
- 자체 데이터 카탈로그
- 지역 특화 대민 서비스
- 부서별 AI 에이전트
- 자체 민원·생활정보 데이터
- 지역 특화 내부 업무 서비스

복지 청소 주차 교통
보건 시설
지역행사 생활민원

광역 공통 데이터 + 자체 데이터 결합	주민 안내 서비스 구성	정책자료 + 지역 행사·시설·민원 데이터 통합 검색	부서별 민원 에이전트 설계	광역 공통 업무편람 참조

정책 기초 데이터 관리 책임 존중 | 접근권한 기반 설계 | 권한·정책 기반 기능 제공 | 임의 통합 구조 아님

행정망 주요 시스템을 보호하면서 단계적으로 연계하는 구조로 안전한 행정 AI 환경을 구축합니다.



‘보안 등급과 권한, 정책 기준에 따라 최적의 LLM 경로를 안전하게 결정하는 체계입니다.’

사업 구조



Secure LLM 라우터

- 사용자 질의 기반 경로 결정
- 보안정책 반영
- 데이터 등급 고려
- 사용자 권한 기준 적용
- 외부 전송 가능 여부 판단



보안 통제 일관성



경로 자동 최적화



감사·로그 기반 책임성 확보

처리 흐름

사용자 질의 → 사용자 인증 및 권한 확인 → 첨부파일·검색 결과 보안 등급 확인 → 2차 AI DLP 문맥 검증 → 처리 목적 및 업무 유형 확인 → 내부망 LLM 가용성 확인 → 범정부 AI 공통기반 사용 가능성 확인 → 글로벌 LLM API 사용 가능성 확인 → 비용·부하·감사정책 확인 → 최종 LLM 경로 결정

보안 등급 기준

보안 등급	데이터 성격	기본 처리 방향	활용 가능한 LLM 경로
C등급	기밀자료, 대외비, 개인정보 원문, 감사·인사·보안자료	제한 처리, 관리자 승인, 4리 격리, 내부망 증심 처리	광역 내부망 LLM, 범정부 AI 공통기반
S등급	내부 업무자료, 비공개 행정자료, 민감 민원자료	내부망 LLM 우선, 정책상 허용 시 범정부 병행	광역 내부망 LLM, 범정부 AI 공통기반
O등급	공개자료, 홈페이지 자료, 보도자료, 일반 정책자료	2차 AI DLP 통과 후 외부 활용 가능	광역 내부망 LLM, 범정부 AI 공통기반, 글로벌 LLM API
예외·위험	등급 블영확, 고위험 질의, 민감정보 포함 가능성	차단, 마스킹, 관리자 승인	제한 처리

Secure RAG는 임베딩 이전 단계에서 보안을 통제하여 안전한 행정 AI 검색 기반을 구축하는 절차입니다.

처리 절차 흐름도



구성 요소 역할 표

절차	주요 역할
데이터 카탈로그	데이터 출처, 소관부서, 기준일, 갱신주기, 권한, 보안 등급 관리
1차 패턴 DLP	정형화된 개인정보와 민감 키워드 탐지
보안 등급 분류	C/S/O 등급에 따라 활용 가능 범위 결정
임베딩 판단	임베딩 허용 여부와 제한 처리 여부 결정
벡터DB 적재	권한·등급·기관별 분리 저장
검색	사용자 권한 내 근거문서 추출
2차 AI DLP	검색 결과와 질의의 문맥 기반 민감도 재검증
라우터 전달	최종 등급과 근거를 Secure LLM 라우터에 전달

핵심 원칙 인포그래픽

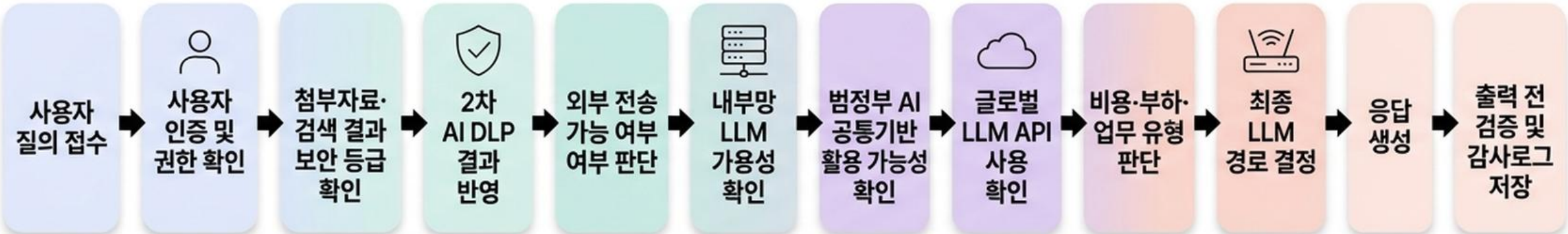
임베딩 이전 보안 통제

벡터DB 민감정보 최소화

검색 후 문맥 재검증

Secure LLM 라우터는 보안정책과 비용, 업무 연속성을 종합 고려하여 최적의 처리 경로를 결정하는 정책 기반 판단 체계입니다.

처리 절차 흐름도



종합 판단 기준

데이터 보안 등급	내부망 LLM 가용성
사용자 소속기관·부서·직무·권한	범정부 AI 공통기반 사용 가능 여부
검색 결과 중 최고 민감도	글로벌 LLM API 사용 가능 여부
비용 한도 및 사용량 정책	감사 대상 업무 여부

정책 기반 전환 원칙

- S등급 내부자료 포함 시 글로벌 LLM API 차단
- 광역 내부망 LLM 또는 범정부 AI 공통기반 전환
- O등급 공개자료 및 2차 AI DLP 통과 시 글로벌 LLM API 허용
- 차단이 아닌 안전 경로 선택

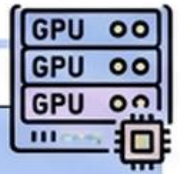
‘광역 내부망 LLM과 GPU 인프라는 행정 데이터 통제와 안정적 업무 처리를 위한 기본 처리 기반입니다.’

운영 방향

광역 내부망 LLM 기본 처리 경로

- 공문
- 내부 보고서
- 회의자료
- 민원자료
- 비공개 정책자료
- 부서별 업무편람
- Secure RAG 기반 처리

GPU 활용 / 영역 표



활용 영역	주요 내용
3072차원 임베딩	행정문서 의미 검색을 위한 고차원 벡터화
AI OCR	이미지, 도면, 표, 손글씨 텍스트 인식
STT	회의, 상담, 민원 음성 텍스트화
TTS	행정 안내 및 접근성 향상 서비스 지원
1차 패턴 DLP	대량 문서의 개인정보·민감정보 탐지
내부망 LLM	내부자료 기반 요약, 검색, 초안 작성

운영 전략

- 특정 모델 장기 종속 방지
- 한국어 행정문서 처리능력 기준 평가
  - 응답속도, 보안성
  - 운영 안정성, 비용 효율성
- 주기적 평가 및 교체·병행 운영 가능 구조
- 범정부 AI 공통기반과 역할 분담

광역 내부망 LLM	범정부 AI 공통기반
• 상시 업무 처리 • 행정 데이터 통제	• 대량 처리 • 피크 부하 대응 • 공통 행정 기능 • 고성능 모델 보완

범정부 AI 공통기반은 광역 내부망 LLM과 함께 설계되어야 하는 행정망 내 핵심 AI 처리 자원입니다

연계 흐름 다이어그램



통제 항목

사용자 인증정보 연계	기관·부서·직무 기반 권한 확인	C/S/O 등급 정보 전달
질의·응답 로그 저장	전송 데이터 범위 관리 관리	사용 모델 및 처리 경로 기록
비용·사용량 계량	관리자 승인 및 예외 처리 이력 관리	장애 발생 시 내부망 LLM 우회처리

활용 분야 표

활용 분야	활용 방식
C등급 제한 처리	관리자 승인, 요약본 기반 제한 처리, 내부망 준용 처리
S등급 내부자료 처리	내부망 LLM과 병행 또는 보조 처리
대량 문서 요약	내부망 GPU 부하 완화
공통 행정기능	여러 지자체가 공통으로 활용 가능한 기능 처리
피크 부하 대응	사용량 급증 시 보조 연산 자원 활용
모델 교차검증	광역 내부망 LLM 응답과 비교·검증

행정망 내 공통 AI 자원 | Secure LLM 라우터 통제 연동 | 로그·감사 기반 운영

글로벌 LLM API는 공개 가능 데이터에 한해 통제적으로 활용하는 외부 연계 자원입니다.

활용 흐름

O등급 공개 가능 질의

↓

→ 2차 AI DLP 검증

↓

Secure LLM 라우터 승인

↓

→ 필요 최소 데이터 전송

↓

글로벌 LLM API 응답 수신

↓

→ 출력 전 보안 검증

↓

사용자 제공 및 로그 저장

활용 가능 업무

- 공개자료 기반 문안 작성
- 보도자료 문체 개선
- 홈페이지 공개정보 요약
- 공개 정책자료 비교
- 외부 리서치
- 공개 통계 설명
- 번역·요약·표현 개선

전송 제외 대상

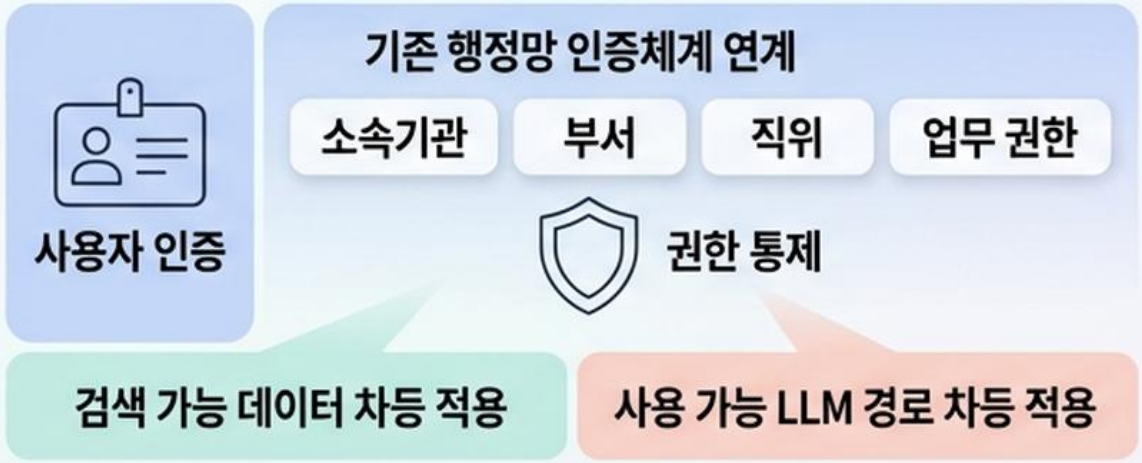
- C등급 전체
- S등급 내부자료
- 개인정보 원문
- 비공개 민원자료
- 내부 검토자료
- 감사·인사·보안자료
- 비공개 정책 초안
- 권한 없는 자료
- 2차 AI DLP에서 민감성이 확인된 자료

통제 원칙

- 차단 대상 아님
- 통제 대상
- Secure LLM 라우터 연계
- 2차 AI DLP 기반 검증
- 외부 전송 위험 관리

행정 AI 플랫폼은 사용자 편의성과 책임 있는 운영체계를 동시에 갖추어야 합니다.

인증·권한관리 구조



권한관리 기준 표

구분	관리 내용
사용자 권한	소속기관, 부서, 직무, 직위, 업무권한 기반 접근 제어
데이터 권한	소관부서, 공개범위, 보안 등급, 열람 가능 사용자 관리
검색 권한	권한 없는 문서는 검색 결과에서 제외
모델 사용 권한	글로벌 LLM API 사용 가능 여부, 범정부 AI 공통기반 공통기반 사용 가능 여부 관리
관리자 권한	데이터 등록, 등급 변경, 예외 승인, 정책 변경 이력 관리

로그·감사 항목



데이터 수집 이력
데이터 카탈로그 등록·수정 이력
DLP 탐지·마스킹·차단 이력
보안 등급 분류 및 변경 이력
임베딩 모델 버전과 재색인 이력
사용자 질의 및 첨부파일 처리 이력



검색 문서와 유사도 이력
2차 AI DLP 판단 결과
LLM 라우팅 경로와 판단 사유
범정부 AI 공통기반 사용 이력
글로벌 LLM API 외부 전송 이력
LLM 응답 및 출력 전 검증 결과
관리자 승인·예외 처리 이력

통제 원칙

범정부 AI 공통기반	행정망 내 공통 AI 처리 경로
글로벌 LLM API	O등급 공개 가능 데이터 중심 외부 민간 LLM 경로
경로별 구분 기록	감사 가능 구조

광역 내부망 LLM과 범정부 AI 공통기반을 초기 단계부터 병행 설계·검증하는 것이 핵심입니다.

1단계

통합 기획·진단

광역 AI 기반과
범정부 AI 공통기반
공동 고려

- 목표 아키텍처 수립
  - 현황 분석서
  - 데이터 분류 기준
  - 목표 구성도
  - 연계 전략

2단계

광역 AI 공통기반 및 및 범정부 연계 동시 설계

- Secure RAG
- Secure LLM 라우터
- 내부망 LLM
- 범정부 AI 공통기반 연계 구조

- 상세 설계서
  - 라우팅 정책
- 보안정책
  - 연계 인터페이스

3단계

Secure RAG 시범 구축

- 데이터 카탈로그
- 1차 DLP
  - C/S/O 분류
  - 임베딩
  - 벡터DB
  - 검색
  - 2차 AI DLP
- Secure RAG PoC
- 데이터 흐름도
- 검색 검증 결과

4단계

Secure LLM 라우터 및 이중 처리 경로 검증

- 광역 내부망 LLM
- 범정부 AI 공통기반
- 라우팅 PoC
- C/S/O 등급별 처리 결과
- 감사로그

- 기초 자체 데이터 개별 서비스
- AI 에이전트
- 기초 서비스 연계 결과
- 기관별 권한체계
  - 사용량 대시보드

5단계

광역 내부망 LLM·범정부 AI 공통기반 병행 운영

- C/S 등급 데이터 처리 정책 검증
- 병행 운영 결과
- 성능·비용 비교
- 보안 점검 결과

7단계

- O등급 공개 가능 데이터 중심 글로벌 LLM 활용
  - 외부 전송 통제 정책
  - API 사용량 관리
  - 로그 체계

8단계

운영 안정화 및 지속 고도화

- 모델 교체
- 성능평가
- 보안정책 보완
- 비용 최적화

- 글로벌 LLM API 통제형 연계

- 운영보고서
  - 개선계획
  - 성과지표
  - 고도화 계획

병행 설계 | **역할 분담** | **비용 효율성 검증** | **보안성 검증**

예산 산정 방법론

본 사업 예산은 장비 구매가 아닌 광역·기초 공동활용 행정 AI 플랫폼 구축 관점에서 편성해야 합니다.

예산 편성 구조

광역 내부망 AI기반 구축비

- 내부망 LLM
- GPU 기반 전처리 서버
- 저장소
- 운영환경
- 보안장비 연계

Secure RAG 구축비

- 데이터 카탈로그
- 1차 패턴 DLP
- 3072차원 임베딩
- 벡터DB
- 검색 엔진
- 근거문서 표시 기능

기초자치단체 확산 지원비

- 기초별 데이터 연계
- 개별 서비스 구성
- AI 에이전트 운영
- 사용자 교육
- 운영 지원 비용

글로벌 LLM API 통제형 활용 비용

- O등급 공개 가능 데이터
- 사용량 기반 관리

주요 구성 항목

Secure LLM 라우터 구축비

- 보안 등급 기반 LLM 경로 선택
- 내부망 LLM 연계
- 범정부 AI 공통기반 연계
- 글로벌 LLM API 연계
- 라우팅 로그
- 정책관리 기능

글로벌 LLM API 통제형 활용 비용

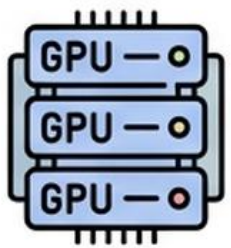
- O등급 공개 가능 데이터
- 사용량 기반 관리
- 비용관리
- 장애 대응
- 로그 연계 비용

예산 관리 방향

- 광역 AI 공통기반과 범정부 AI 공통기반 병행 고려
- 공동 활용 구조 전제
- 단계적 확산 구조
- 운영비와 확산비 분리 관리

GPU 기반 전처리와 내부망 LLM 인프라는 본 사업의 핵심 기본 인프라입니다.

인프라 구성



- RTX 5090급 GPU 기반 전처리 서버
- 내부망 LLM 운영 서버
- 저장장치
- 네트워크 구성
- 보안장비 연계
- 백업 및 장애 대응 환경

비용 항목 표

세부 항목	주요 내용	예산 성격
GPU 전처리 서버	OCR, STT/TTS, 임베딩, DLP 처리	초기 구축비
내부망 LLM 서버	내부자료 기반 질의응답, 요약, 초안 작성	초기 구축비·증설비
저장장치	원문, 전처리 결과, 벡터DB, 로그 저장	초기 구축비·증설비
백업·복구 환경	장애 대응, 데이터 보호	초기 구축비·운영비
운영 모니터링	GPU 사용량, 응답속도, 장애 상태 관리	구축비·운영비

산정 기준 원칙

- 문서 임베딩량
- OCR 대상 이미지·도면 수
- STT 처리 시간
- 동시 사용자 수
- 평균 질의량
- 피크 시간대 처리량

- 단순 장비 단가 기준 산정 지양
- 범정부 AI 공통기반 병행 활용 구조
- 단계적 증설 방식

Secure RAG 구축은 행정 데이터를 안전하게 검색·활용하기 위한 핵심 기반 투자입니다.

구성 범위



세부 항목 표

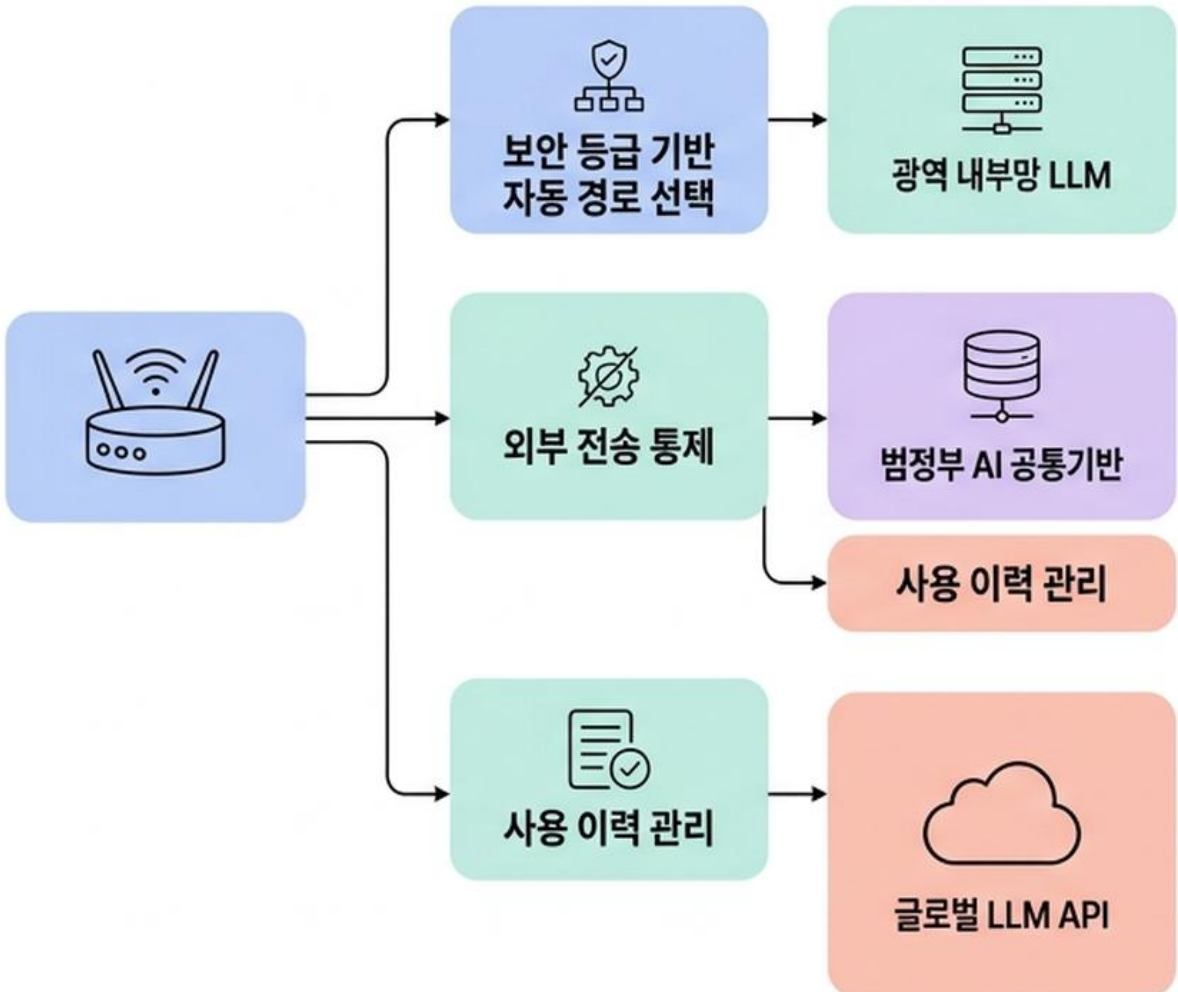
세부 항목	주요 내용	예산 성격
데이터 카탈로그	데이터 목록화, 메타데이터, 소관부서, 기준일, 권한 관리	구축비
1차 패턴 DLP	개인정보·민감정보 탐지, 마스킹, 제외 처리	구축비·고도화비
보안 등급 분류	C/S/O 등급 기준 적용 및 정책관리	구축비
임베딩 체계	3072차원 임베딩, 모델 버전관리, 재색인	구축비·운영비
벡터DB	광역 공통·기초 개별 영역, 권한별 인덱스 관리	구축비·증설비
검색 엔진	키워드·벡터 하이브리드 검색, 근거문서 표시	구축비
2차 AI DLP	문맥 기반 민감도 재검증, 등급 상향 판단	구축비·운영비
로그·감사	검색·DLP·임베딩·응답 처리 이력 관리	구축비·운영비

예산 관리 방향

- 초기 구축비와 연차별 고도화비 구분
- 데이터 증가 대응
- 보안정책 변경 대응
- 임베딩 모델 교체
- 검색 정확도 개선
- 검색 정확도 개선
- 부서별 특화 요구 반영

Secure LLM 라우터는 보안 등급 기반 경로 선택과 사용 이력 관리를 담당하는 핵심 제어 체계입니다.

핵심 역할 다이어그램



세부 항목 표

세부 항목	주요 내용	예산 성격
라우팅 정책 엔진	C/S/O 등급, 사용자 권한, 업무 유형 기반 경로 판단	구축비
내부망 LLM 연계	광역 내부망 LLM 호출 및 응답 처리	구축비
범정부 AI 공통기반 연계	행정망 내 공통 AI 처리 자원 연계	구축비·운영비
글로벌 LLM API 연계	O등급 공개자료 중심 외부 LLM API 통제형 연계	구축비·사용량 기반 비용
차단·우회 처리	외부 전송 차단, 내부망 전환, 관리자 승인	구축비
비용관리	모델별 사용량, API 비용, 한도 관리	구축비·운영비
감사로그	라우팅 사유, 사용 모델, 외부 전송 여부 기록	구축비·운영비
정책관리 화면	관리자 정책 설정, 예외 승인, 이력 조회	구축비

설계 원칙

- 특정 LLM 종속 구조 지양
- 내부망 LLM 교체 대응
- 정책 기반 유연 연계
- 글로벌 LLM API 변경 대응
- 범정부 AI 공통기반 기능 변화 대응

데이터 카탈로그와 벡터DB는 Secure RAG의 저장·관리 핵심 기반입니다.

핵심 개념

데이터 카탈로그

- 데이터 출처 관리
- 메타데이터 관리
- 소관부서
- 기준일
- 권한 관리

벡터DB

- 의미 기반 검색
- 권한 기반 필터링
- 보안 등급별 인덱스
- 광역 공통 영역
- 기초 개별 영역

예산 고려 요소

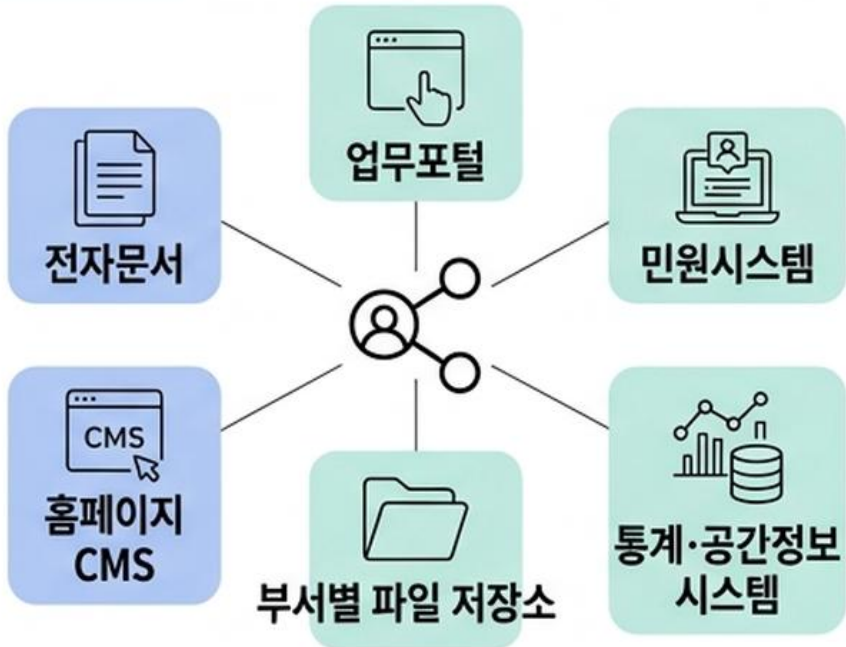
- 데이터 원천 시스템 수
- 수집 대상 문서량
- 이미지·도면·음성 등 비정형 데이터 규모
- 광역 공통 데이터와 기초 개별 데이터 분리 방식
- 보안 등급별 인덱스 분리 필요성
- 재색인 주기
- 백업·복구 요구 수준
- 데이터 갱신 및 폐기 정책

확장 전략

- 검색 성능
- 동시 사용자 수
- 권한 기반 필터링 성능
- 장애 대응 구조
- 백타시용에수 항상
- 검색기반 아터및 정보
- 초기 핵심 데이터셋 중심 구축
- 활용도 기반 단계적 확장
- 검색량 기준 증설

행정망 시스템 연계와 전처리는 데이터 활용 효과와 보안 통제를 동시에 좌우하는 기반입니다.

연계 대상



세부 항목 표

세부 항목	주요 내용	예산 성격
시스템 연계 분석	대상 시스템 조사, 데이터 구조 분석, 권한체계 확인	구축비
수집 인터페이스	API, 배치, 파일 연계, DB 연계 등	구축비
데이터 정제	중복 제거, 형식 변환, 오류 보정	구축비·운영비
OCR 전처리	스캔 문서, 이미지, 도면, 표, 손글씨 인식	구축비·운영비
STT 전처리	회의·상담·민원 음성 텍스트화	운영비
품질검증	추출 정확도, 누락, 최신성 점검	운영비

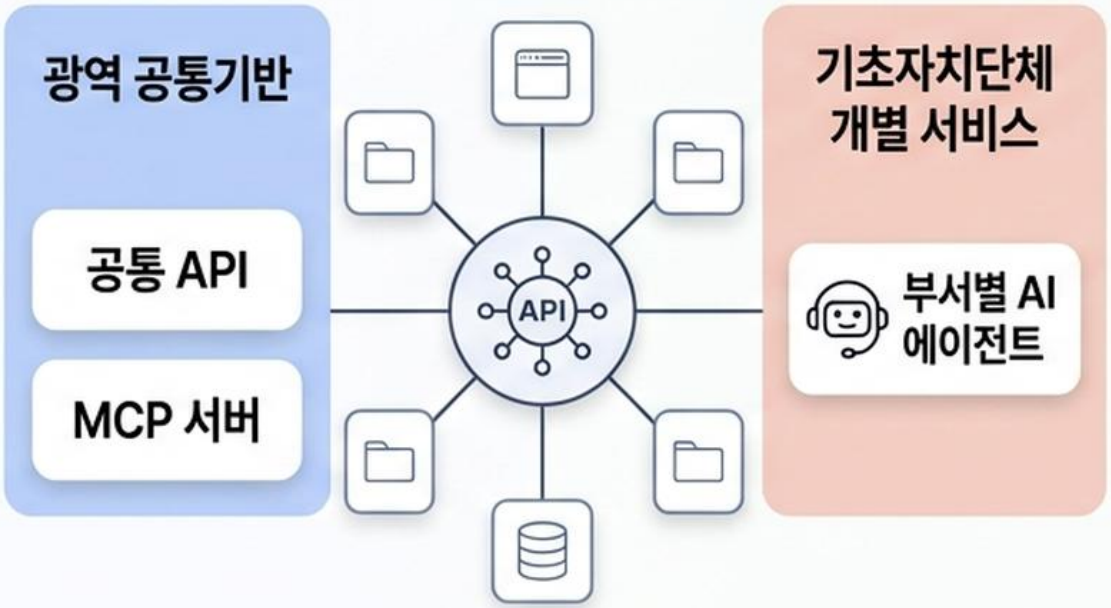
추진 원칙

- 원천 시스템 종류별 차등 설계
- 데이터 구조별 연계 방식 분리
- 보안정책 반영 구조
- 업무효과 높은 자료료 우선
- 보안위험 관리 용이 자료 우선
- 단계적 연계 추진

MCP와 공통 API는 광역·기초 공동활용을 가능하게 하는 서비스 확장 기반입니다.

역할 구조

공통 기능 호출 구조 | 중복 개발 최소화 | 서비스 확산 기반



주요 비용 항목

공통 API 설계 및 개발

MCP 서버 구성

데이터·도구·에이전트
호출 권한관리

기초자치단체별 서비스 연계

API 사용량 관리

장애 모니터링

연계 로그 및 감사관리

개발자·운영자용 문서화

설계 방향·효과

표준화된 연계 구조

광역	공통 기능 안정적 제공
기초	자체 서비스에서 필요한 기능 호출

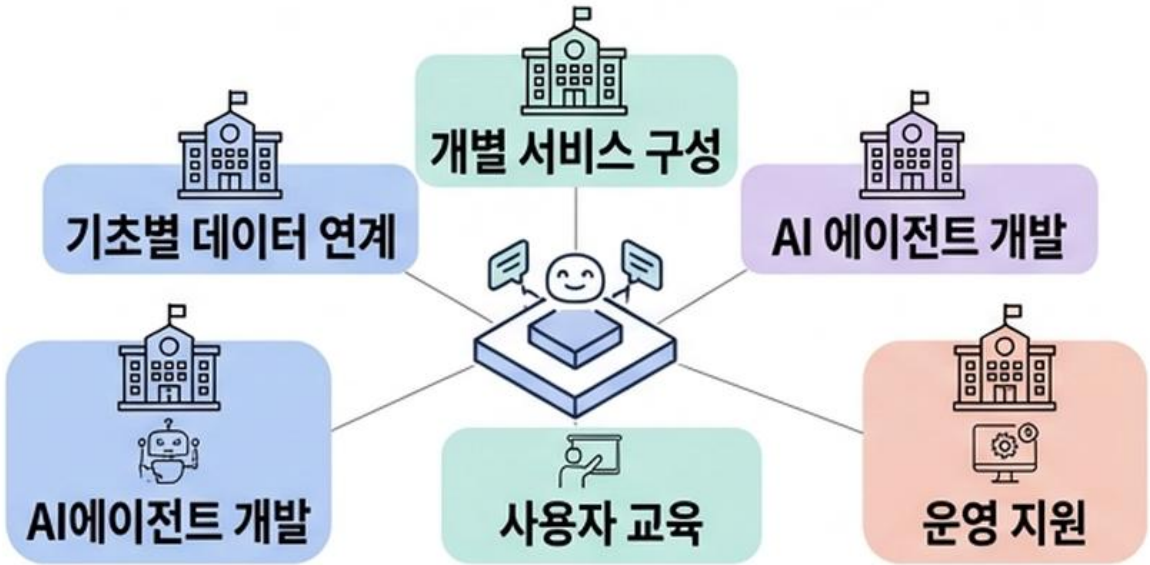
서비스 중복 개발 감소

확산 속도 향상

운영 효율성 확보

‘기초자치단체 확산은 기관별 여건을 고려한 선택형 모델로 추진하는 것이 바람직합니다.’

지원 범위



세부 항목

세부 항목	주요 내용
기초별 현황 진단	데이터 보유 현황, 업무 수요, 보안정책 검토
자체 데이터 구축	기초별 문서·민원·지역자료 카탈로그화
개별 서비스 연계	민원, 복지, 교통, 환경, 홈페이지 안내 등
AI 에이전트 구성	부서별·업무별 에이전트 템플릿 적용
사용자 교육	공직자 AI 활용교육, 보안교육, 답변 검수교육
운영 지원	장애 대응, 서비스 개선, 품질 점검

예산 모델 방향

- 참여 기초자치단체 수 기준 산정
- 구축 서비스 수 반영
- 연계 시스템 수 반영
- 자체 데이터 규모 반영

기본형	확장형	고도화형
선택형 확산 모델	단계적 참여 구조	운영 지속성 확보

범정부 AI 공통기반과 글로벌 LLM API 비용은 성격을 구분하여 통제적으로 관리해야 합니다.

비용 구분 구조

범정부 AI 공통기반

행정망 내 공통 AI 처리 자원
- 광역 내부망 LLM 병행·보완 활용

- 사용량
- 처리량
- 모델 종류
- 응답 시간
- 대량 처리 여부

글로벌 LLM API

O등급 공개 가능 데이터 중심
외부 민간 LLM

- 질의량
- 토큰 사용량
- 호출 모델
- 사용자 수

관리 방식 방식 표

구분	활용 범위	비용 관리 방식
범정부 AI 공통기반	C/S/O 등급 중 정책상 허용된 데이터 처리	행정망 내 사용량·처리량 기반 관리
글로벌 LLM API	O등급 공개 가능 데이터 중심	API 호출량·토큰 사용량 기반 관리

비용 관리 원칙

- 내부망 LLM과 범정부 AI 공통기반 역할 사전 정의
- C/S 등급 데이터 글로벌 LLM API 전송 금지
- O등급 데이터 2차 AI DLP 통과 시에만 글로벌 LLM API 사용
- 기관별·부서별·서비스별 월간 사용량 한도 설정
- 범정부 AI 공통기반 사용 비용과 자체 GPU 증설 비용 정기 비교
- 모델별 사용량, 응답속도, 비용 대비 효과 정기 점검

AI 플랫폼은 구축 이후에도 지속적인 운영·유지관리와 고도화가 필요합니다.

운영·유지관리 표

구분	주요 내용	예산 성격
시스템 운영	서버, 저장소, 네트워크, 모니터링	운영비
보안 점검	DLP 정책 점검, 접근권한 점검, 로그감사	운영비
데이터 관리	카탈로그 갱신, 폐기, 재색인, 품질검증	운영비
모델 관리	LLM·임베딩 모델 성능평가, 교체, 튜닝	운영비·고도화비
범정부 연계 관리	사용량 점검, 비용 비교, 장애 대응	운영비
사용자 지원	교육, 문의 대응, 부서별 활용 지원	운영비
서비스 개선	신규 기능 추가, 에이전트 고도화, API 확장	고도화비

고도화 영역

- 데이터 갱신
- 임베딩 재색인
- 보안정책 변경
- 모델 교체
- 성능 개선
- 장애 대응

형상관리 핵심





임베딩 모델 버전 기록
모델 교체 시점 기록
교체 사유 기록
재색인 완료 일시 기록
성능 비교 데이터 관리
답변 생성 기준 사후 추적 가능 구조



예산은 통합 설계부터 시범 검증과 확산까지 단계별 성과에 따라 집행하는 것이 바람직합니다.

단계별 집행 구조



집행 원칙·효과

대규모 일괄 집행 지양 시범검증 후 확산	광역 기반 확보	범정부 AI 공통기반 병행 운영	기초 단계적 참여 구조	안정적 확산	재정효율성 확보

예산 항목은 인프라부터 확산과 운영까지 기능별로 구분하여 체계적으로 관리해야 합니다.

예산 항목 표

구분	주요 내용	예산 성격
인프라	GPU 전처리 서버, 내부망 LLM 운영환경	초기 구축비
Secure RAG	카탈로그, DLP, 임베딩, 벡터DB, 검색	초기 구축비·고도화비
LLM 라우터	보안 등급 기반 모델 분기, 로그, 정책관리	초기 구축비
범정부 연계	행정망 내 범정부 AI 공통기반 연계	구 구축비·사용량 관리비
연계	행정망 시스템, MCP, 공통 API	구축비·확산비
기초 확산	기초별 서비스, 에이전트, 자체 데이터 구축 지원	확산비
운영	유지관리, 보안 점검, 모델 교체, 사용자 지원	운영비
글로벌 LLM	0등급 공개자료 중심 API 활용	사용량 기반 비용

집행 논리 구조



광역자치단체	자체 AI 기반 확보	범정부 AI 공통기반 초기 활용
기초자치단체	안정적 공통기반 활용	행정수요 맞춤 단계적 확장

기대 효과

‘광역 공통 플랫폼 기반 공동활용 구조는 AI 인프라 중복투자를 줄이고 GPU 부담을 완화합니다.’

중복투자 절감 구조

광역 공통 인프라

- GPU
- 내부망 LLM
- 데이터 카탈로그
- DLP
- 임베딩
- 벡터DB
- 검색 엔진
- LLM 라우터
- 권한관리
- 로그·감사



기초자치단체

- 별도 대규모 인프라 구축 불필요
- 자체 데이터 활용
- 지역 특화 서비스
- AI 에이전트 운영

광역

- 공통 인프라 제공
- 표준·보안정책 통합

기초

- 서비스 운영
- 행정수요 맞춤 적용

GPU 부담 완화 구조

- 고성능 GPU 가격 상승
- 수급 부담
- 전력·냉각
- 운영인력

- 광역 내부망 LLM 기본 구축
- 범정부 AI 공통기반 연동
- 대량 처리



- 범정부 AI 공통기반 연동
  - 대량 처리
  - 피크 부하 대응
  - 공통 행정기능
  - 고성능 모델 보완

- 자체 GPU 전면 확보 구조 지양
- 단계적 확장

기대 효과

- 재정 효율성 확보
- 중복 구축 방지
- 보안 정책 표준화
- 단계적 인프라 증설
- 확장성 확보

내부망 LLM 중심의 안전한 운영과 범정부 AI 공통기반 연계는 보안성과 비용 효율성을 동시에 확보합니다.

안전 운영 구조

내부망 LLM 중심 안전 운영

- 공문
- 내부 보고서
- 회의자료
- 민원자료
- 비공개 정책자료
- 감사·인사 자료

→ Secure RAG

- 카탈로그 등록
- 1차 패턴 DLP
- 보안 등급 분류
- 임베딩 판단
- 권한 기반 검색
- 2차 AI DLP

내부망 LLM 기본 처리 경로

- 처리 단계 추적 가능
- 근거문서 기반 응답
- 모델 경로 확인 가능

범정부 AI 공통기반 연계 활용

행정망 내 공통 AI 처리 자원

공통 앵해되VI 처리자원

- 대량 문서시 요약
- 공통 행정기능 처리
- 사용량 급증 시 부하 분산
- 모델 교차검증
- 내부망 LLM 성능 보완

Secure LLM 라우터 판단

C/S 등급 정책상 허용 범위 검토

↓

- 데이터 등급
- 업무 유형
- 비용
- 처리 부하
- 보안정책

종합 효과

- 보안성 확보
- 비용 효율성 확보
- 연산 자원 부담 완화
- 운영 투명성 강화
- 행정 AI 신뢰성 확보

'최신 글로벌 LLM 성능을 통제된 범위 내에서 활용하여 행정업무 생산성을 향상시킵니다.'

통제형 글로벌 LLM 활용

글로벌 LLM
- 문서 작성
- 요약
- 번역
- 자료 조사
- 표현 개선

O등급 공개 가능 데이터
- 홈페이지 공개자료
- 보도자료
- 공고문
- 대외 공개용 문안
- 일반 정책자료
- 외부 리서치



Secure LLM 라우터
- 보안 등급 확인
- 2차 AI DLP 결과 확인

C/S 등급 자료
- 외부 전송 금지
- 광역 내부망 LLM 전환
- 범정부 AI 공통기반 전환

최신 AI 성능 활용

내부 행정자료 보호

내부 행정자료 보호

보안 통제

행정문서 검색·요약·작성 생산성 향상

법령 | 조례 | 예규 | 지침 | 업무편람

가사용 | 감사사례 | 질의회신 | 과거 보고서

Secure RAG 기반 검색
- 권한 범위 내 검색
- 근거문서 제시
- 출처 표시
- 기준일 표시

공문 초안
보고서 초안
보도자료 초안
회의자료 초안
정책 검토자료 초안

자료 탐색 시간 감소
검토·판단 시간 확대
반복 업무 부담 완화

운영 원칙

AI 결과는 초안

최종 문서는 담당자 검토

내부 결재 절차 준수

통제된 활용

보안 우선 적용

책임 있는 운영

Secure RAG와 Secure LLM 라우터는 민원 품질을 높이면서 개인정보 유출 위험을 줄입니다.

민원 처리 지원

민원 분석 및 답변 초안 지원

- 반복 질의
- 유사 민원
- 관련 규정 확인
- 우사 민원
- 부서 배정
- 답변 초안 작성

- 민원 유형 분류
- 관련 지침 검색
- 기존 답변 사례 검색
- 담당자 판단 지원

개인정보 포함 민원 → 1차 패턴 DLP 점검 2차 AI DLP 점검 → 내부망 LLM 처리 / 범정부 AI 공통기반 처리

공개 가능 일반 안내 → 2차 AI DLP 점검 → 글로벌 LLM 문안 개선 활용 가능

AI 답변

- 담당자 검토용 초안
- 공식 입장 아님

보안 통제 구조

개인정보 및 민감정보 보호 구조

임베딩 전 1차 패턴 DLP

- 정형 개인정보 탐지

검색 후 2차 AI DLP

- 문맥상 민감성 재검증

Secure LLM 라우터

- 최종 보안 등급 판단
- 글로벌 LLM API 전송 가능 여부 판단
- C/S 등급 행정망 내 처리

데이터 수집 → 전처리 → 임베딩 → 검색 → LLM 전달 → 응답 출력 → 로그 저장

전 과정 보안통제

기대 효과

기대 효과

- 민원 처리 품질 개선
- 답변 일관성 강화
- 보안 사고 예방
- 개인정보 보호 강화
- 운영 투명성 확보

보안 등급 기반 LLM 라우팅과 근거 중심 응답 구조는 업무 연속성과 신뢰도를 동시에 확보합니다.

보안 등급별 라우팅 구조

Secure LLM 라우터

차단 중심 정책 지양
안전한 대체 경로 탐색

보안 통제



C등급
광역 내부망 LLM
범정부 AI 공통기반
차단 | 격리
관리자 승인 | 제한 처리

S등급
광역 내부망 LLM
범정부 AI 공통기반

O등급
2차 AI DLP 검증
글로벌 LLM API 활용 가능

보안과 업무 효율 동시 고려
정책 기반 자동 경로 선택

업무 연속성 효과

사용자 업무 중단 최소화

우회 사용 감소

복잡한 모델 선택 기준 자동화

정책 기반 경로 결정

공직자
모델 세부 기준 숙지 불필요

안전 경로 자동 선택

업무 연속성 향상

검거 기반·출즌·일 제공



법령 | 조례
지침 | 업무편람
통계자료
정책자료



근거문서 기반 검색

문서명 | 출처 | 기준일
관련 조항 | 최신성 확인 안내

맹목적 수용 방지

설명가능성 강화

행정 책임성 강화

전 과정 로그·감사 체계와 광역·기초 역할 분담 구조는 책임성과 지속가능성을 강화합니다.

감사 추적 구조

- 질문 이력
- 검색 문서 이력
- 보안 등급 판단 이력
- LLM 경로 선택 이력
- 범정부 AI 공통기반 사용 이력
- 글로벌 LLM API 전송 이력

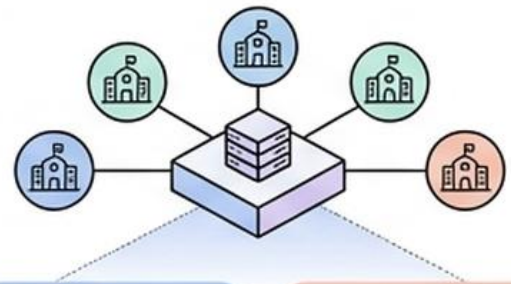


형상관리 기반 책임성

- 모델 교체 이력
- 임베딩 재색인 이력
- 정책 변경 이력
- 재색인 완료 시점 기록
- 성능 비교 데이터 기록

과거 답변 생성 기준 추적 가능
책임 있는 운영
사후 감사 대응 가능

기초자량단체 AI 역량 강화



광역

- Secure RAG
- Secure LLM 라우터
- MCP
- 공통 API
- 보안정책
- 데이터 표준 제공

기초

- 자체 데이터 관리
- 지역 특화 서비스 운영
  - 복지정보 안내
  - 지역행사 안내
  - 부서별 업무지원
  - 내부자료 검색
  - 대민 홈페이지 안내

대규모 인프라 부담 없음
단계적 서비스 확장
AI 활용 역량 향상
지방정부 AI 생태계 성장

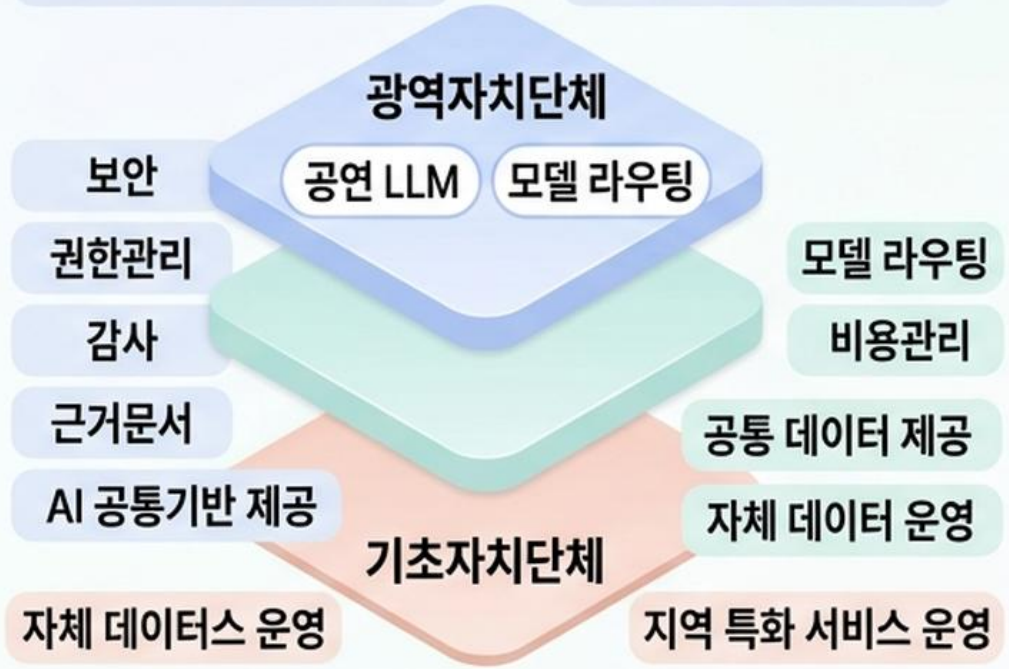
결론

지방정부 행정 AI는 단일 모델 도입이 아닌 보안·권한·감사를 포함한 공통 플랫폼 방식으로 구축해야 합니다.

플랫폼 구축 방향

단일 챗봇 중심 접근 지양
특정 LLM 단독 도입 지양

공통 플랫폼 방식



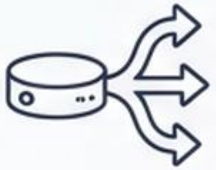
역할 분담 구조

Secure RAG와 Secure LLM 라우터의 필요성



Secure RAG

- 행정 데이터 안전 검색
- 권한 기반 검색
- 근거문서 기반 응답



Secure LLM 라우터

- 보안 등급 기반 경로 분기
- 광역 내부망 LLM
- 범정부 AI 공통기반
- 글로벌 LLM API

활용성과 보안성 동시 확보

보안 등급 기반 라우팅의 전략적 가치

- C/S/O 등급 구분
- 민감자료
- 행정망 내 안전 경로 처리
- 공개 가능 자료
- 글로벌 LLM 최신 성능 활용
- 범정부 AI 공통기반
- 행정망 내 공통 AI 처리 자원
- GPU 구매 부담 완화
- 처리 성능 확보
- 확장성 확보

광역 주도·기초 공동활용 모델은 중복투자를 줄이면서 자율성과 표준을 동시에 확보하는 구조입니다.

공동활용 구조

광역
- Secure RAG
- Secure LLM 라우터
- MCP
- 공통 API
- 보안정책
- 데이터 표준

공통 기반 위 자율 운영
- 중복 인프라 구축 방지
- 표준 일관성 유지

기초

공통 기반 위 자율 운영
- 중복 인프라 구축 방지
- 표준 일관성 유지

기초

기초
- 자체 데이터 관리
- 지역 특화 서비스

기초
- 민원 안내
- 복지 정보 안내
- 업무 지원 서비스

기대 효과

- 중복투자 절감
- 보안정책 일관성
- 데이터 관리 기준 통일
- 서비스 확장성 확보
- 운영 효율성 향상

지속가능성

광역 → 기반 안정적 제공

기초 → 단계적 서비스 확장

공유

- 대규모 인프라 부담 감소
- AI 활용 역량 향상
- 지방정부 AI 생태계 성장

본 제안은 각 광역자치단체의 행정망 환경, 보안정책, 예산 여건,
기초자치단체 참여 방식에 따라 세부 조정이 필요합니다.

따라서 우선 데이터 현황, 대상 시스템, 보안 등급 기준, 범정부 AI 공통기반 연계 조건,
기초자치단체 확산 범위를 함께 검토하는 사전 협의가 필요합니다.

스캐터엑스는 광역·기초자치단체가 안전하고 실효성 있는 행정 AI 플랫폼을 단계적으로
구축하실 수 있도록, 귀 기관의 여건에 맞춘 세부 추진 방안을 정중히 협의드리고자 합니다.

(주)스캐터엑스 솔루션사업부 최규호 본부장

010-2907-8929 kyuho.choi@scatterx.io