

[기술 백서] 공직자가 체감하는 AI 만들기

지자체 AI 에이전트 구축 실무 가이드

정확한 공공데이터, 고성능 추론, 공직자 업무 흐름 재현을 기반으로 한 행정 AI 에이전트 설계 원칙과 단계별 실행 방법

Executive Summary

백서 작성 배경과 목적

전국 광역 및 기초자치단체에서 생성형 AI 도입이 활발히 논의되고 있으나, 실제 현장에서는 공직자 만족도가 낮고 실질적 업무 개선 효과가 미미한 사례가 반복되고 있습니다. 많은 지자체가 수십억 원을 투입해 AI 플랫폼을 구축했지만, 성능 부족, 외부 검색 미연동, 업무 맥락 부재로 인해 활용률이 저조하거나 사업이 중단되는 경우가 빈번합니다. 본 백서는 이러한 실패를 반복하지 않기 위해, 공직자의 실제 업무 흐름에 맞춘 AI 에이전트 구축 방법론을 제시합니다. 지자체 AI 정책 담당자와 정보화 담당자가 즉시 실행 가능한 단계별 가이드를 제공하며, 예산 낭비를 방지하고 공직자가 체감하는 성과를 만드는 것을 목표로 합니다.

공직자용 AI 에이전트의 정의

공직자용 AI 에이전트는 단순히 질문에 답하는 챗봇이 아니라, 공직자의 업무 사고 흐름을 따라 정보를 찾고, 판단을 보조하며, 행정 산출물을 생성하는 업무수행형

AI 입니다. 민원 분석, 정책 기획, 법령 검토, 보고서 작성 등 특정 행정 업무의 절차를 이해하고, 각 단계에서 필요한 데이터를 우선순위에 따라 제공하며, 공직자가 최종 판단과 검토만 하면 되도록 초안과 근거를 함께 제시합니다. 핵심은 공직자가 "어떤 순서로 생각하고, 어떤 자료를 먼저 보며, 어떤 형식으로 결과를 만드는가"를 AI 가 재현하는 것입니다. 이를 통해 반복 업무는 AI 에게 맡기고, 정책 판단과 주민 소통 같은 본질적 업무에 집중할 수 있는 환경을 조성합니다.

5 대 설계 원칙 요약

공직자용 AI 에이전트 구축의 핵심은 다섯 가지 설계 원칙입니다. 첫째, 정확한 데이터입니다. 법령, 조례, 통계, 공공데이터 등 공직자가 우선적으로 참고해야 하는 14 가지 티어 1 데이터를 정의하고, 출처가 명확하고 최신성이 보장된 정보만 AI 에 전달합니다. 둘째, 근거 기반 추론 성능입니다. 공직자 업무는 복잡한 판단과 비교 분석이 필요하므로, 글로벌 최상위 수준의 추론 모델을 활용하되 근거 없는 답변은 차단합니다. 셋째, 공직자 업무 사고 흐름의 재현입니다. 민원 처리, 정책 기획 등 실제 업무 절차를 단계별로 분석하고, AI 가 이를 따라 정보를 제시하고 초안을 생성하도록 설계합니다. 넷째, 보안·권한·개인정보 보호입니다. 데이터를 CSO(C 급·S 급·O 급) 3 단계로 분류하고, 등급에 따라 내부망 LLM 과 외부망 LLM 을 분리 운영하며, 개인정보는 자동 마스킹합니다. 다섯째, 근거 제시와 검토 가능한 책임 구조입니다. 모든 답변에 출처를 명시하고, 고위험 업무는 반드시 담당자 검토를 거치도록 설계하며, 오답 발생 시 정정 이력을 관리합니다.

4 단계 로드맵 요약

공직자용 AI 에이전트 구축은 4 단계 로드맵으로 진행합니다. 1 단계는 SaaS 형 AI 비서 즉시 도입입니다. 대규모 인프라 구축 없이 3 개월 내 파일럿 부서에 AI 비서를 제공하고, 사용자 반응을 확인하며 즉시 성과를 냅니다. 2 단계는 핵심 에이전트 발굴 및 검증입니다. 실무자 인터뷰를 통해 업무별 사고 흐름을 수집하고, 아이디어 도출, 정책 기획, 민원 분석, 법령 조회, 법적 가이드 등 5~10 개 에이전트를 설계해 배포한 후 활용 로그를 분석해 성과가 높은 에이전트를 선별합니다. 3 단계는 데이터·보안 체계

고도화입니다. 검색 API, MCP, 메타데이터 RAG 를 결합한 데이터 전달 체계를 구축하고, CSO 기반 보안 등급별 LLM 라우팅과 권한 관리 체계를 완성합니다. 4 단계는 전사 통합형 AI 플랫폼 구축입니다. 검증된 에이전트를 내재화하고, 내부망 LLM 과 외부망 LLM 을 하이브리드로 운영하며, 전 부서로 확산합니다. 각 단계마다 명확한 성과지표를 설정하고, 다음 단계로 넘어가는 조건을 사전에 정의합니다.

기대 효과 및 제언

본 백서의 방법론을 적용하면 지자체는 다섯 가지 핵심 효과를 얻을 수 있습니다. 예산 측면에서는 과잉 설계를 피하고 단계적 투자로 매몰 비용을 방지합니다. 신뢰 측면에서는 출처 기반 답변과 감사 대응력을 확보합니다. 업무 측면에서는 실시간 현행화와 반복 업무 경감으로 공직자가 본질 업무에 집중할 수 있습니다. 보안 측면에서는 CSO 등급별 통제와 개인정보 보호를 철저히 합니다. 미래 측면에서는 정제된 데이터 축적을 통해 지능형 행정의 기반을 마련합니다. 다만, AI 도입은 기술 도입이 아니라 조직 프로세스 재설계입니다. 성공을 위해서는 단체장의 의지, 실무 부서의 참여, 데이터 오너 지정, 지속적 평가와 개선 체계가 필수적입니다. 본 백서가 전국 지자체의 실질적인 AI 전환 길잡이가 되기를 기대합니다.

1 장. 왜 지금 공직자용 AI 에이전트인가

1.1 지자체 AI 도입의 현실: 성공과 실패 사례

전국 지자체의 AI 도입 현황을 보면 명암이 뚜렷합니다. 일부 광역자치단체는 생성형 AI 기반 행정 업무 지원 시스템을 도입하고 수백 종의 업무매뉴얼을 기반으로 RAG 체계를 구축하며, 내부 시스템과 연계해 정보 조회와 문서 작성을 지원하는 AI 에이전트 도입을 추진하고 있습니다. 반면 다른 지자체들은 내부망에 여러 LLM 을 도입했으나 외부 검색이 불가능하고 성능이 기대에 미치지 못해 단체장과 공직자의 불만이 높은

상황입니다. 또 다른 지자체는 내부망 LLM 성능 저하와 외부 검색 불가로 공직자 만족도가 낮아 개선 방안을 모색 중입니다. 일부 기초자치단체는 홈페이지 챗봇을 메타데이터 RAG 기반 실시간 검색 방식으로 검토하며 유지관리 편의성과 정확도 확보를 목표로 하고 있습니다. 성공 사례의 공통점은 명확합니다. 즉시 성과를 낼 수 있는 영역부터 시작하고, 공직자가 실제로 필요한 데이터를 우선 제공하며, 최신 정보 접근을 보장하는 구조입니다. 실패 사례는 대규모 인프라부터 구축하고, 성능 낮은 모델에 의존하며, 외부 검색을 차단한 경우입니다.

1.2 일반 챗봇은 왜 공직자 만족도가 낮은가

지자체가 도입한 많은 AI 챗봇이 활용률 저조로 사업이 중단되는 이유는 세 가지입니다. 첫째, LLM 추론 성능 부족입니다. 공직자 업무는 법령 해석, 정책 비교, 민원 쟁점 분석 등 복잡한 추론이 필요한데, 일부 국산 LLM 이나 제한적 모델은 글로벌 최상위 모델 대비 추론 능력이 현저히 낮아 정책 기획이나 법령 분석 같은 고난도 업무를 맡기기 어렵습니다. 둘째, 외부 검색 미연동입니다. 내부망 폐쇄 환경에서 최신 정책 사례, 타 지자체 조례, 언론 동향, 연구보고서 접근이 차단되면 AI 는 과거 데이터에 갇혀 시의성 있는 답변을 할 수 없습니다. 셋째, 업무 맥락 부재입니다. 단순 질의응답형 챗봇은 공직자가 "어떤 순서로 업무를 처리하는가"를 이해하지 못합니다. 민원 담당자는 민원 유형 분류, 관련 법령 확인, 유사 사례 검토, 회신 초안 작성 순서로 일하는데, 챗봇은 이 흐름을 모르고 단편적 정보만 제공하므로 실무에 바로 쓰기 어렵습니다. 결국 공직자는 AI 를 참고용 도구로만 보고 본격적으로 활용하지 않게 됩니다.

1.3 공직자용 AI 에이전트는 무엇이 다른가

공직자용 AI 에이전트는 세 가지 핵심 차별점을 갖습니다. 첫째, 데이터 전달 방식이 다릅니다. 일반 챗봇은 학습된 데이터나 크롤링한 정보를 무작위로 제공하지만, 공직자용 에이전트는 법령, 조례, 통계, 공공데이터 등 14 가지 티어 1 데이터를 정의하고, 검색 API→MCP→메타데이터 RAG 순으로 정확한 정보를 찾아 출처를 명시합니다. 둘째, 추론 방식이 다릅니다. 단순 검색이 아니라 공직자 업무에 필요한 고도의 추론 능력을 갖춘 최상위 LLM 을 활용하되, 근거 없는 답변은 "확인 필요"로

표시해 환각 현상을 차단합니다. 셋째, 업무 흐름 재현 방식이 다릅니다. 정책 기획자가 현황 분석→원인 파악→대안 비교→추진안 도출 순서로 생각하듯, AI 도 같은 절차를 따라 단계별로 정보를 제시하고 초안을 생성합니다. 이 세 가지 차별점이 결합되면, 공직자는 AI 를 단순 검색 도구가 아니라 업무 파트너로 인식하게 됩니다.

1.4 이 백서의 목적과 활용 방법

본 백서는 광역 및 기초자치단체의 AI 정책 담당자, 정보화 담당자를 주 독자로 합니다. 단체장과 기획실 간부는 Executive Summary 를 통해 핵심 방향을 파악하고, 실무 담당자는 4~7 장의 단계별 실행 가이드를 따라 즉시 사업을 추진할 수 있습니다. 부록의 체크리스트와 템플릿은 제안서 작성, 예산 산정, RFP 작성 시 바로 활용 가능합니다. 본 백서는 "읽는 문서"가 아니라 "쓰는 가이드"를 지향합니다.

2 장. 공직자용 AI 에이전트란 무엇인가

2.1 질의응답형 AI vs 업무수행형 AI

질의응답형 AI 는 사용자의 질문에 답을 제공하는 데 그칩니다. "청년 일자리 지원금 지급 기준은?"이라고 물으면 관련 법령 조문을 찾아 보여주는 수준입니다. 반면 업무수행형 AI 는 질문 의도를 파악하고, 공직자가 그 다음 해야 할 일까지 제시합니다. 같은 질문에 업무수행형 AI 는 법령 조문뿐 아니라 우리 지자체 조례, 신청 서식, 유사 사례, 예산 집행 현황, 타 지자체 비교까지 묶어서 제공하고, "신청 접수 시 확인해야 할 체크리스트"와 "민원 회신 초안"까지 함께 생성합니다. 핵심 차이는 AI 가 "정보 제공자"인가, "업무 보조자"인가입니다. 공직자용 에이전트는 후자를 지향합니다.

2.2 공직자 사고 흐름 기반 에이전트의 의미

공직자는 업무를 처리할 때 일정한 사고 흐름을 따릅니다. 정책 기획자는 문제 정의→현황 분석→원인 파악→대안 비교→추진안 도출→기대효과 정리 순서로 생각합니다. 민원 담당자는 민원 내용 파악→쟁점 도출→관련 법령 확인→유사 사례 검토→회신 방향 결정→초안 작성 순서로 일합니다. 공직자 사고 흐름 기반 에이전트는 이 절차를 AI가 재현하도록 설계하는 것입니다. AI는 공직자가 각 단계에서 필요한 자료를 순서대로 제시하고, 단계별 판단 포인트를 함께 알려주며, 최종 산출물(보고서, 회신문, 기획안)까지 생성합니다. 공직자는 AI가 제시한 흐름을 따라가며 검토하고 판단만 하면 됩니다. 이것이 사고 흐름 재현의 핵심입니다.

2.3 대표 에이전트 5 가지 예시

공직자용 AI 에이전트는 업무별로 특화됩니다. 첫째, 아이디어 도출 에이전트는 신규 사업 아이디어 발굴, 주민 체감형 서비스 개선안 도출 시 타 지자체 사례, 연구보고서, 언론 동향을 검색해 아이디어 카드를 생성합니다. 둘째, 정책 기획 에이전트는 정책 과제 정의→현황 분석→대안 비교→추진안 도출 흐름에 따라 정책기획서 초안을 작성하고, 법적 근거와 타 지자체 사례를 함께 제시합니다. 셋째, 민원 분석 자동화 에이전트는 민원 텍스트와 첨부 파일을 분석해 민원 유형 분류, 핵심 쟁점 추출, 관련 법령 검색, 회신 초안 생성까지 수행합니다. 넷째, 법령 조회 에이전트는 질문 의도에 맞는 법령·조례·지침을 찾아 조문 요지, 관련 조례, 해석상 유의점을 정리합니다. 다섯째, 법적 가이드 에이전트는 특정 행정행위의 법적 리스크, 실무상 유의사항, 분쟁 가능성을 점검하고 담당자 확인 필요 항목을 제시합니다. 이 5 가지는 가장 보편적인 에이전트이며, 지자체는 자체 수요에 따라 추가 에이전트를 설계할 수 있습니다.

2.4 공직자용 AI 에이전트의 적용 범위

공직자용 AI 에이전트는 거의 모든 부서에 적용 가능합니다. 기획 부서는 정책 기획, 사업계획서 작성, 타 지자체 사례 비교에 활용합니다. 민원 부서는 민원 분석, 회신 초안, 반복 민원 패턴 탐지에 활용합니다. 법무 부서는 법령 검토, 조례 충돌 감지, 감사 대응 자료 정리에 활용합니다. 홍보 부서는 보도자료 초안, 연설문 작성, SNS 여론 분석에 활용합니다. 복지 부서는 대상자 자격 안내, 신청 서식 정리, 유사 사례 검색에

활용합니다. 건설·환경 부서는 인허가 서류 검토, 기술 기준 확인, 민원 현장 분석에 활용합니다. 핵심은 부서별로 "어떤 업무가 반복적이고, 자료 조사가 많으며, 문서 작성이 필요한가"를 파악하면 에이전트 적용 영역을 찾을 수 있다는 점입니다.

3 장. 공직자용 AI 에이전트 구축 로드맵

3.1 전체 로드맵 개요

공직자용 AI 에이전트 구축은 단번에 완성되지 않습니다. 성공적인 도입을 위해서는 4 단계 로드맵을 따라 점진적으로 확장하는 전략이 필요합니다. 1 단계는 SaaS 형 AI 비서 즉시 도입으로 3 개월 내 파일럿 부서에서 즉시 성과를 냅니다. 2 단계는 핵심 에이전트 발굴 및 검증으로 6 개월간 부서 수요를 조사하고 활용 로그를 분석해 성과 높은 에이전트를 선별합니다. 3 단계는 데이터·보안 체계 고도화로 1 년간 검색 API, MCP, 메타데이터 RAG 를 결합한 데이터 전달 체계를 구축하고 CSO 기반 보안 체계를 완성합니다. 4 단계는 전사 통합형 AI 플랫폼 구축으로 2 년 차에 검증된 에이전트를 내재화하고 전 부서로 확산합니다. 각 단계는 명확한 성과지표를 갖추며, 다음 단계로 넘어가는 조건을 사전에 정의합니다. 이 로드맵의 핵심은 대규모 인프라 구축을 미루고, 공직자가 체감하는 성과부터 만드는 것입니다.

3.2 1 단계: SaaS 형 AI 비서 즉시 도입

1 단계의 목표는 대규모 예산과 긴 구축 기간 없이 3 개월 내 공직자가 AI 를 직접 체험하고 효과를 확인하는 것입니다. SaaS 형 AI 비서는 클라우드 기반으로 제공되므로 별도 서버 구축이 불필요하고, 계정 발급 즉시 사용 가능합니다. 파일럿 부서 30~50 명을 선정해 문서 작성, 자료 검색, 민원 분석 등 실제 업무에 AI 를 투입하고, 사용 로그와 만족도를 주간 단위로 측정합니다. 이 단계에서 중요한 것은 완벽한 시스템이 아니라 빠른 피드백입니다. 공직자들이 "AI 가 실제로 도움이 되는가"를 직접

경험하고, "어떤 업무에서 가장 효과적인가"를 파악합니다. 비용은 사용자 수 기준 월 구독료로 책정되며, 광역자치단체 기준 연간 5 천만~1 억 원 수준입니다. 이 단계의 성공 기준은 월 활성 사용자 30% 이상, 만족도 4.0/5.0 이상입니다. 이 기준을 충족하면 2 단계로 진행합니다.

3.3 2 단계: 핵심 에이전트 발굴 및 검증

1 단계에서 AI 효용을 확인한 후, 2 단계는 부서별로 진짜 필요한 에이전트가 무엇인지 찾는 과정입니다. 기획실, 민원실, 법무담당관, 홍보담당관 등 주요 부서와 워크숍을 진행하고, 실무자 인터뷰를 통해 "가장 시간이 오래 걸리는 업무", "반복적인 업무", "자료 조사가 많은 업무"를 파악합니다. 이를 바탕으로 아이디어 도출, 정책 기획, 민원 분석, 법령 조회, 법적 가이드 등 5~10 개 에이전트를 설계하고 배포합니다. 중요한 것은 각 에이전트마다 공직자의 업무 사고 흐름을 반영하는 것입니다. 예를 들어 정책 기획 에이전트는 문제 정의→현황 분석→대안 비교→추진안 도출 순서로 정보를 제시합니다. 배포 후 3 개월간 활용 로그를 분석해 사용 빈도, 정확도, 수정률, 만족도를 측정하고, 10 개 에이전트 중 5 개 이상이 주 1 회 이상 사용되면 성공으로 판단합니다. 이 단계에서는 구축형 전환 여부를 판단할 수 있는 충분한 데이터가 축적됩니다.

3.4 3 단계: 데이터·보안 체계 고도화

2 단계까지 SaaS 로 운영하며 에이전트 효용을 검증했다면, 3 단계는 본격적인 내재화 준비 단계입니다. 핵심은 데이터 전달 체계와 보안 체계를 완성하는 것입니다. 먼저 AI 데이터 전달 3 대 유형(정확하게 찾아주기, 만들어주기, 설명하기)을 구현합니다. "정확하게 찾아주기"는 검색 API→MCP→메타데이터 RAG 3 단계 전략으로 구성하며, 법령·조례·통계·언론 등 14 가지 티어 1 데이터를 우선순위에 따라 검색합니다. "정확하게 만들어주기"는 내부 시스템의 인허가 이력, 민원 처리 내역, 예산 데이터를 ETL 엔진으로 정제해 AI 가 이해 가능한 형태로 가공합니다. "정확하게 설명하기"는 센서 데이터에 운영 매뉴얼과 SOP 를 결합해 맥락을 부여합니다. 보안 체계는 CSO(C 급·S 급·O 급) 3 단계로 데이터를 분류하고, C 급은 내부망 LLM 만, S 급은 내부망 우선, O 급은 외부

LLM 허용으로 라우팅합니다. 이 단계의 성공 기준은 검색 정확도 85% 이상, 근거 누락률 5% 이하입니다.

3.5 4 단계: 전사 통합형 AI 플랫폼 구축

3 단계까지 데이터·보안 체계가 완성되면, 4 단계는 검증된 에이전트를 내재화하고 전 부서로 확산하는 단계입니다. SaaS 로 운영하던 에이전트 중 성과가 높은 5~10 개를 선별해 내부 플랫폼으로 이전하고, 내부망 LLM 과 외부망 LLM 을 하이브리드로 운영합니다. 내부망에는 민감정보 처리용 LLM 을 배치하고, 공개정보 기반 업무는 외부 고성능 LLM 을 활용합니다. 전 부서로 확산하며 부서별 특화 에이전트(건설·환경 부서용 인허가 검토 에이전트, 복지 부서용 대상자 안내 에이전트 등)를 추가 개발합니다. 이 단계의 목표는 공직자 1 인당 주 5 회 이상 AI 활용, 전체 만족도 4.5/5.0 이상입니다. 성공 시 AI 는 지자체의 일상적 업무 도구로 자리 잡습니다.

3.6 광역·기초자치단체별 추진 시나리오

광역자치단체는 공직자 수가 많고 예산 규모가 크므로 4 단계 로드맵을 2 년에 걸쳐 완주할 수 있습니다. 1 단계 3 개월, 2 단계 6 개월, 3 단계 1 년, 4 단계 이후 전 부서 확산 순서로 진행합니다. 기초자치단체는 공직자 수가 적고 예산이 제한적이므로 1~2 단계를 SaaS 로 1 년 이상 운영하며 효과를 검증한 후, 3~4 단계 진행 여부를 판단하는 것이 현실적입니다. 소규모 기초자치단체는 4 단계까지 가지 않고 SaaS 방식을 장기 유지하는 것도 합리적 선택입니다. 핵심은 조직 규모와 예산에 맞춰 유연하게 접근하되, 1 단계는 반드시 거치는 것입니다.

4 장. 1 단계 실행 가이드: SaaS 형 AI 비서 도입

4.1 왜 SaaS 부터 시작하는가

많은 지자체가 AI 도입 시 대규모 플랫폼 구축부터 시작해 실패합니다. 수십억 원을 투입해 1~2 년 구축 후 막상 사용해보니 성능이 기대에 못 미치거나, 공직자들이 사용법을 익히지 못해 활용률이 저조한 경우가 반복됩니다. SaaS 형 AI 비서는 이 위험을 최소화합니다. 첫째, 즉시 성과를 냅니다. 계약 후 1 주일 내 계정을 발급받고, 공직자들은 웹브라우저나 모바일 앱으로 즉시 사용 가능합니다. 문서 요약, 보고서 초안, 자료 검색 등 실제 업무에 투입하며 바로 효과를 체감합니다. 둘째, 위험을 최소화합니다. 대규모 투자 없이 월 구독료로 시작하므로, 효과가 없으면 계약 종료하면 됩니다. 매몰 비용이 거의 없습니다. 셋째, 사용자 반응을 확인합니다. 공직자들이 "어떤 업무에서 AI 를 많이 쓰는가", "어떤 기능이 부족한가"를 파악해 2 단계 에이전트 설계에 반영합니다. SaaS 는 검증 도구이자 학습 과정입니다.

4.2 도입 절차와 예산

SaaS 형 AI 비서 도입 절차는 5 단계입니다. 1 단계는 사업 계획 수립입니다. 파일럿 부서 선정, 예산 확보, 목표 설정을 진행합니다. 2 단계는 제안요청서(RFP) 작성 또는 조달 계약입니다. SaaS 서비스는 조달청 지정구매나 수의계약이 가능한 경우가 많으므로, 입찰 절차를 단축할 수 있습니다. 3 단계는 계약 및 계정 발급입니다. 계약 후 1 주일 내 파일럿 부서 공직자 계정을 발급받고, SSO(Single Sign-On) 연동을 설정합니다. 4 단계는 사용자 교육입니다. 2 시간 내외 온라인 교육으로 기본 사용법, 파일 업로드, 문서 작성, 검색 활용법을 안내합니다. 5 단계는 운영 및 모니터링입니다. 주간 단위로 사용 로그, 만족도, 오답 사례를 수집하고 개선합니다. 예산은 사용자 수에 비례합니다. 광역자치단체 공직자 6 천 명 기준 연간 5 천만~1 억 원, 기초자치단체 공직자 500 명 기준 연간 5 백만~1 천만 원 수준입니다. 무제한 사용 방식과 종량제 방식 중 선택 가능하며, 파일럿 단계에서는 무제한 방식이 사용자 부담을 줄입니다.

4.3 파일럿 부서 선정 기준

파일럿 부서는 AI 도입 성공을 좌우합니다. 잘못 선정하면 효과가 미미해 확산이 어렵습니다. 선정 기준은 세 가지입니다. 첫째, 문서 업무 비중이 높은 부서입니다. 보고서, 기획안, 민원 회신, 보도자료 등 문서 작성이 많은 부서일수록 AI 효과가 큼니다. 기획실, 홍보담당관, 민원실이 대표적입니다. 둘째, 혁신 의지가 있는 부서입니다. 부서장이나 팀장이 AI 활용에 적극적이고, 실무자들이 새로운 도구 학습에 거부감이 적은 부서를 선택합니다. 혁신 의지가 낮은 부서는 교육 후에도 활용률이 저조합니다. 셋째, 데이터 접근성이 좋은 부서입니다. 법령, 조례, 통계 등 공개 데이터를 많이 다루는 부서가 초기 성과를 내기 쉽습니다. 민감정보만 다루는 부서는 보안 제약이 많아 파일럿에 부적합합니다. 이 세 기준을 충족하는 부서 2~3 곳을 선정하고, 부서당 15~20 명 규모로 시작합니다.

4.4 성과 측정 방법

파일럿 운영 3 개월 후 성과를 측정해 2 단계 진행 여부를 판단합니다. 성과지표는 네 가지입니다. 첫째, 사용률입니다. 월 활성 사용자(MAU) 비율을 측정합니다. 파일럿 부서 50 명 중 30 명 이상이 월 1 회 이상 사용하면 60% 사용률로, 목표는 30% 이상입니다. 사용 빈도도 중요합니다. 주 1 회 이상 사용하는 파워유저 비율이 20% 이상이면 성공입니다. 둘째, 만족도입니다. 월 1 회 설문조사로 "AI 가 업무에 도움이 되는가", "계속 사용하고 싶은가"를 5 점 척도로 측정합니다. 평균 4.0/5.0 이상이 목표입니다. 셋째, 업무 시간 단축입니다. 보고서 작성, 자료 검색, 민원 회신 작성 시간을 AI 사용 전후로 비교합니다. 평균 30% 이상 단축되면 효과가 있다고 판단합니다. 넷째, 문서 작성 건수입니다. AI 로 생성한 초안 건수를 집계합니다. 파일럿 부서 50 명이 월 100 건 이상 초안을 생성하면 실질적 활용이 이뤄진 것입니다. 이 네 지표를 종합해 70 점 이상이면 2 단계로 진행합니다.

4.5 주의사항과 리스크 관리

SaaS 형 AI 비서 도입 시 세 가지 리스크를 관리해야 합니다. 첫째, 개인정보 처리입니다. 공직자가 민원인 정보나 내부 민감 문서를 AI 에 업로드할 수 있습니다. 이를 방지하려면 사용 전 교육에서 "개인정보 포함 문서는 업로드 금지", "민감정보는 가명 처리 후 사용"

원칙을 명확히 안내합니다. SaaS 제공사가 개인정보 자동 마스킹 기능을 제공하는지 확인하고, 제공하지 않으면 내부 지침으로 통제합니다. 둘째, 오답 대응입니다. AI는 환각 현상으로 틀린 답을 생성할 수 있습니다. 공직자 교육에서 "AI 답변은 반드시 검토 후 사용", "법령·통계는 원문 확인 필수" 원칙을 강조합니다. 오답 사례가 발견되면 즉시 수집해 SaaS 제공사에 피드백하고, 전체 사용자에게 공유합니다. 셋째, 사용자 교육입니다. 공직자들이 AI 사용법을 익히지 못하면 활용률이 낮습니다. 교육은 2시간 온라인 강의 + 2주간 실습 지원 방식으로 진행하고, 부서별 파워유저 1~2 명을 지정해 동료 지원 체계를 만듭니다. 이 세 가지 리스크를 사전에 관리하면 파일럿 성공 확률이 크게 높아집니다.

5 장. 2 단계 실행 가이드: 핵심 에이전트 발굴

5.1 업무 중심 에이전트 설계 원칙

많은 지자체가 AI 에이전트를 설계할 때 "문서 요약 기능", "번역 기능", "이미지 생성 기능"처럼 기능을 나열하는 방식으로 접근합니다. 하지만 공직자는 기능이 아니라 업무를 합니다. 민원 담당자는 "민원을 어떻게 처리하는가"가 중요하지, "요약 기능이 있는가"가 중요한 것이 아닙니다. 업무 중심 에이전트 설계의 핵심은 공직자의 업무 절차를 먼저 파악하고, 그 절차에 맞춰 AI가 정보를 제시하고 초안을 생성하도록 만드는 것입니다. 예를 들어 정책 기획 에이전트는 "문서 작성 기능"이 아니라 "문제 정의→현황 분석→원인 파악→대안 비교→추진안 도출→기대효과 정리" 순서로 공직자를 안내하며, 각 단계에서 필요한 통계, 법령, 타 지자체 사례를 자동으로 검색해 제시합니다. 공직자는 AI가 제시한 흐름을 따라가며 판단하고, 최종 정책기획서 초안을 받습니다. 이것이 업무 중심 설계입니다. 기능 나열 방식은 공직자가 "AI를 어떻게 써야 할지"

고민하게 만들지만, 업무 중심 설계는 공직자가 "평소 하던 업무를 AI 와 함께" 하도록 만듭니다.

5.2 실무자 인터뷰 기반 사고 흐름 수집

공직자의 업무 사고 흐름을 파악하는 가장 확실한 방법은 실무자 인터뷰입니다. 인터뷰 대상은 부서별 경력 3~5 년 차 실무자가 적합합니다. 신규자는 업무 흐름이 아직 체화되지 않았고, 10 년 이상 경력자는 암묵지가 많아 언어화가 어렵습니다. 인터뷰 질문지는 다섯 가지 핵심 질문으로 구성합니다. 첫째, "이 업무를 시작할 때 가장 먼저 하는 일은 무엇인가?" 둘째, "어떤 자료를 먼저 찾아보는가?" 셋째, "가장 시간이 오래 걸리는 단계는 어디인가?" 넷째, "결재권자나 상급자가 가장 자주 지적하는 부분은 무엇인가?" 다섯째, "최종 결과물은 어떤 형식인가?" 이 다섯 질문에 대한 답변을 정리하면 업무 흐름도가 나옵니다. 예를 들어 민원 담당자 인터뷰 결과는 "민원 내용 파악→쟁점 도출→관련 법령 확인→유사 사례 검토→회신 방향 결정→초안 작성→상급자 검토" 순서로 정리됩니다. 이 흐름도를 바탕으로 민원 분석 에이전트를 설계하면, AI 는 공직자가 실제로 일하는 방식 그대로 정보를 제시합니다. 인터뷰는 부서당 2~3 명, 1 인당 1 시간 내외로 진행하며, 녹음 후 텍스트로 정리해 흐름도를 작성합니다.

5.3 에이전트 설계 워크숍 운영 방법

실무자 인터뷰로 업무 흐름을 수집했다면, 다음은 부서별 워크숍으로 에이전트 우선순위를 선정합니다. 워크숍은 부서별로 진행하며, 부서장, 팀장, 실무자 5~10 명이 참여합니다. 워크숍은 3 단계로 진행됩니다. 1 단계는 업무 목록 작성입니다. 부서에서 수행하는 모든 업무를 화이트보드에 나열합니다. 2 단계는 AI 적용 가능성 평가입니다. 각 업무를 "반복성(자주 하는가)", "자료 조사량(찾아볼 자료가 많은가)", "문서 작성량(결과물이 문서인가)" 세 기준으로 평가하고, 세 기준 모두 높은 업무를 선별합니다. 3 단계는 우선순위 투표입니다. 선별된 업무 중 참석자 투표로 상위 3~5 개를 최종 선정합니다. 워크숍 결과는 "부서별 에이전트 우선순위 목록"으로 정리됩니다. 예를 들어 기획실은 "정책 기획 에이전트", "타 지자체 사례 비교 에이전트",

"사업계획서 작성 에이전트" 순으로 선정하고, 민원실은 "민원 분석 에이전트", "민원 회신 초안 에이전트", "반복 민원 패턴 분석 에이전트" 순으로 선정합니다. 전체 부서 워크숍 결과를 종합하면 지자체 전체의 에이전트 우선순위가 도출됩니다.

5.4 에이전트별 입력·출력 구조 설계

에이전트 우선순위가 정해지면, 각 에이전트의 입력·출력 구조를 설계합니다. 구조 설계는 세 요소로 구성됩니다. 첫째, 입력 항목입니다. 공직자가 에이전트를 사용할 때 입력해야 할 정보를 정의합니다. 정책 기획 에이전트의 입력 항목은 "정책 과제명", "대상 주민", "예산 범위", "추진 기간", "계약조건"입니다. 민원 분석 에이전트의 입력 항목은 "민원 텍스트", "첨부 파일", "민원 유형"입니다. 입력 항목은 최소화해야 공직자 부담이 줄어듭니다. 둘째, 처리 단계입니다. 에이전트가 입력을 받은 후 어떤 순서로 작업하는지 정의합니다. 정책 기획 에이전트는 "문제 정의→현황 분석(통계 검색)→원인 파악→대안 생성(타 지자체 사례 검색)→대안 비교→추진안 도출→기대효과 정리" 순서로 처리합니다. 민원 분석 에이전트는 "민원 내용 파악→쟁점 도출→관련 법령 검색→유사 사례 검색→회신 방향 결정→초안 생성" 순서로 처리합니다. 처리 단계는 5.2 절에서 수집한 업무 흐름도를 그대로 반영합니다. 셋째, 출력 형식입니다. 에이전트가 최종적으로 제공하는 결과물 형식을 정의합니다. 정책 기획 에이전트는 "정책기획서 초안(HWP 또는 DOCX)", 민원 분석 에이전트는 "민원 회신문 초안(HWP)"을 출력합니다. 출력 형식은 공직자가 평소 사용하는 서식과 동일해야 수정이 쉽습니다.

5.5 성공 기준과 평가

에이전트를 배포한 후 3 개월간 성과를 측정해 성공 여부를 판단합니다. 평가 기준은 네 가지입니다. 첫째, 사용 빈도입니다. 해당 에이전트를 주 1 회 이상 사용하는 공직자 비율을 측정합니다. 목표는 대상 부서의 30% 이상입니다. 예를 들어 정책 기획 에이전트를 기획실 50 명에게 배포했다면, 15 명 이상이 주 1 회 이상 사용해야 성공입니다. 둘째, 정확도입니다. 에이전트가 생성한 초안의 정확도를 공직자 평가로 측정합니다. "AI 초안이 업무에 바로 활용 가능한가"를 5 점 척도로 평가해 평균 3.5 점

이상이면 성공입니다. 셋째, 수정률입니다. 공직자가 AI 초안을 받은 후 수정하는 비율을 측정합니다. 수정률 50% 이하(즉, 초안의 50% 이상을 그대로 사용)면 성공입니다. 수정률이 80% 이상이면 AI 초안의 실효성이 낮다는 의미입니다. 넷째, 만족도입니다. 월 1 회 설문조사로 "이 에이전트가 업무에 도움이 되는가"를 5 점 척도로 평가해 평균 4.0 점 이상이면 성공입니다. 이 네 기준을 종합해 70 점 이상인 에이전트는 3 단계에서 내재화 대상으로 선정하고, 50 점 이하인 에이전트는 개선하거나 폐기합니다.

6 장. 3 단계 실행 가이드: 데이터·보안 체계 구축

6.1 공직자 우선 데이터 전략

많은 지자체가 AI 도입 시 "데이터를 많이 모으면 성능이 좋아진다"고 생각해 무분별하게 데이터를 수집합니다. 하지만 공직자용 AI 에서 중요한 것은 데이터의 양이 아니라 정확성과 우선순위입니다. 공직자 우선 데이터 전략의 핵심은 세 가지입니다. 첫째, 공직자가 실제로 참고하는 데이터를 먼저 정의합니다. 법령, 조례, 통계, 공공데이터, 타 지자체 사례, 연구보고서, 언론 등 14 가지 티어 1 데이터를 우선순위로 설정합니다. 둘째, 출처가 명확한 데이터만 사용합니다. 정부기관, 공공기관, 학술기관, 언론사 등 공신력 있는 출처의 데이터만 AI 에 전달하고, 블로그나 개인 사이트 정보는 제외합니다. 셋째, 최신성을 보장합니다. 법령은 개정 여부를 실시간 확인하고, 통계는 최신 시점 데이터를 우선 제공하며, 조례는 시행일 기준으로 현행 조문만 검색합니다. 이 전략의 핵심은 특정 LLM 종속을 탈피하는 것입니다. 데이터 체계를 먼저 구축하면, LLM 은 언제든지 교체 가능합니다. 반대로 특정 LLM 에 종속되면, 해당 LLM 성능이 낮아도 교체가 어렵습니다. 데이터 중심 접근은 지속 가능한 AI 인프라의 기반입니다.

6.2 AI 데이터 전달 3 대 유형

광역 및 기초자치단체가 보유한 데이터는 성격에 따라 AI에 전달하는 방식이 달라야 합니다. 스캐터엑스는 이를 3대 유형으로 정의합니다. 첫째, 정확하게 찾아주기입니다. 법령, 조례, 통계, 공공데이터, 언론, 논문 등 이미 외부에 존재하는 정보를 검색해 AI에 전달하는 방식입니다. 검색 API, MCP, 메타데이터 RAG를 순차적으로 활용하며, 검색 성공 시점에 즉시 중단해 비용과 시간을 최적화합니다. 둘째, 정확하게 만들어주기입니다. 내부 시스템의 인허가 이력, 민원 처리 내역, 예산 집행 데이터, 계약 관리 DB 등 파편화된 정형 데이터를 ETL 엔진으로 추출·변환·적재해 AI가 이해 가능한 형태로 가공하는 방식입니다. 예를 들어 민원 관리 시스템, 예산 시스템, 인사 시스템의 데이터를 결합해 "부서별 민원 처리 현황과 예산 집행률 상관관계"를 분석 가능한 형태로 만듭니다. 셋째, 정확하게 설명하기입니다. 상수도 수압, 하수처리장 수질, 화재 감지 센서, CCTV 메타데이터 등 현장 센서 데이터는 단순 수치만으로는 AI가 의미를 파악하기 어렵습니다. 이를 설비 운영 매뉴얼, 비상 대응 SOP와 결합해 "수압 저하 시 조치 절차", "수질 이상 시 점검 항목"처럼 행정·기술적 맥락을 부여합니다. 이 3대 유형을 모두 구현해야 공직자용 AI 에이전트가 완성됩니다.

6.3 티어 1 데이터 정의와 우선순위 설계

공직자가 업무에서 우선적으로 참고해야 하는 티어 1 데이터는 14가지입니다. 첫째, 법령입니다. 헌법, 법률, 대통령령, 총리령, 부령 등 국가법령정보센터의 모든 법령이 포함됩니다. 둘째, 조례입니다. 지자체가 제정한 조례, 규칙, 훈령 등 자치법규정보시스템의 모든 자치법규가 포함됩니다. 셋째, 지침입니다. 중앙부처와 지자체의 행정 지침, 예규, 고시, 공고가 포함됩니다. 넷째, 판례입니다. 대법원, 헌법재판소, 행정법원의 판례와 행정심판 재결례가 포함됩니다. 다섯째, 지자체 누리집입니다. 지자체 공식 홈페이지의 공지사항, 보도자료, 정책 안내, 사업 소개가 포함됩니다. 여섯째, 정부기관 누리집입니다. 중앙부처, 공공기관의 공식 홈페이지 공개 데이터가 포함됩니다. 일곱째, 공공데이터입니다. 공공데이터포털의 개방 데이터가 포함됩니다. 여덟째, 통계청 데이터입니다. KOSIS의 모든 공식 통계가 포함됩니다. 아홉째, 나라장터 데이터입니다. 입찰 공고, 계약 정보, 낙찰 내역이 포함됩니다. 열째,

정부 및 광역 산하 연구기관 보고서입니다. 국책연구기관, 광역자치단체 산하 연구원의 연구보고서와 정책 브리프가 포함됩니다. 열한째, 국내 논문입니다. 학술 DB 등재 논문이 포함됩니다. 열두째, 해외 논문입니다. 국제 학술 DB 논문이 포함됩니다. 열셋째, 국내 언론 기사입니다. 중앙지, 지역지, 전문지 기사가 포함됩니다. 열넷째, 해외 언론 기사입니다. 주요 해외 언론사 기사가 포함됩니다. 이 14 가지를 규범 데이터(법령·조례·지침·판례), 사실 데이터(누리집·공공데이터·통계·나라장터), 참고 데이터(연구보고서·논문·언론)로 계층화하고, 질문 유형별로 검색 우선순위를 설정합니다.

6.4 "정확하게 찾아주기" 3 단계 전략

"정확하게 찾아주기"는 AI 데이터 전달 3 대 유형 중 가장 기본이 되는 전략입니다. 핵심은 검색 API→MCP→메타데이터 RAG 순으로 실행하며, 검색 성공 시점에 즉시 중단하는 것입니다. 1 순위는 기존 검색 API 활용입니다. 구글, 네이버, 다음, 퍼플렉시티 등 상용 검색 API 와 국가법령정보센터, KOSIS, 공공데이터포털 등 공공 API 를 질문 유형에 따라 우선순위로 호출합니다. 법령 질문은 국가법령정보센터 API 를 먼저 호출하고, 통계 질문은 KOSIS API 를 먼저 호출합니다. 검색 결과는 메타데이터 필터링으로 출처 신뢰도, 최신성, 적용 범위를 기준으로 재정렬합니다. 검색 성공 시 2 순위는 실행하지 않고 즉시 LLM 에 전달합니다. 2 순위는 MCP 연동입니다. 검색 API 로 찾을 수 없는 내부 시스템 데이터나 특정 공공 DB 데이터를 MCP 로 실시간 조회합니다. 예를 들어 민원 관리 시스템의 유사 민원 사례, 나라장터의 최신 입찰 정보, 내부 예산 시스템의 집행 현황을 MCP 로 가져옵니다. MCP 는 보안 등급별 접근 통제를 적용하며, 사용자 부서와 권한을 확인한 후 데이터를 전달합니다. MCP 로도 찾지 못하면 3 순위로 이동합니다. 3 순위는 메타데이터 RAG 입니다. 검색 API 와 MCP 로 찾을 수 없는 내부 문서(업무 매뉴얼, 부서 FAQ, 과거 회신 사례, 결재 문서)를 메타데이터 RAG 로 검색합니다. 메타데이터 필터링(발행기관, 시행일, 보안등급, 효력상태)을 먼저 수행한 후 벡터 검색을 실행해 현행 유효 문서만 검색 대상으로 삼습니다. 이 3 단계 전략은 비용을 최소화하고 최신성을 보장하며 출처 신뢰도를 확보하는 가장 효율적인 방법입니다.

6.5 CSO 기반 보안 등급별 데이터 처리

공공 데이터는 보안 등급에 따라 AI 처리 방식이 달라야 합니다. 본 백서는 CSO(C 급·S 급·O 급) 3 단계 분류를 제안합니다. C 급은 비밀입니다. 국가안보, 외교, 수사, 개인 민감정보 등이 포함되며, 내부망 LLM 만 사용 가능합니다. 외부 LLM 전송은 절대 금지되며, 내부망에서도 권한자만 접근 가능합니다. S 급은 대외비입니다. 내부 검토 문서, 미확정 정책, 계약 협상 내역 등이 포함되며, 내부망 LLM 을 우선 사용하되 필요 시 범정부 공통 AI 를 보조로 활용합니다. 외부 LLM 사용 시 반드시 개인정보를 마스킹하고 민감 표현을 제거한 후 전송합니다. O 급은 공개입니다. 법령, 조례, 공공데이터, 보도자료, 공식 통계 등이 포함되며, 외부 고성능 LLM 사용이 허용됩니다. 이 등급 분류에 따라 LLM 라우팅이 자동으로 이뤄집니다. 공직자가 질문하면 시스템이 질문에 포함된 데이터의 보안 등급을 자동 판별하고, C 급 데이터가 포함되면 내부망 LLM 으로, O 급만 포함되면 외부 LLM 으로 라우팅합니다. 이 체계는 보안을 유지하면서도 최고 성능의 LLM 을 활용할 수 있는 균형점입니다.

6.6 개인정보 보호 및 권한 통제

CSO 등급 분류만으로는 개인정보 보호가 완벽하지 않습니다. 추가로 세 가지 장치가 필요합니다. 첫째, 자동 마스킹입니다. 공직자가 업로드한 문서나 입력한 텍스트에서 주민번호, 전화번호, 주소, 계좌번호, 이메일 등을 패턴 인식으로 자동 탐지해 마스킹 처리합니다. 마스킹된 데이터만 LLM 에 전달하고, 답변 생성 후 원본 정보를 재결합합니다. 둘째, 권한 기반 검색입니다. 공직자의 부서, 직급, 역할에 따라 접근 가능한 문서를 제한합니다. 예를 들어 복지과 주무관은 복지과 문서만 검색 가능하고, 타 부서 문서는 검색 결과에서 제외됩니다. 셋째, 감사 로그입니다. 누가 언제 어떤 문서를 검색했는지, 어떤 LLM 을 사용했는지, 어떤 답변을 받았는지 모두 기록합니다. 이상 접근(대량 문서 다운로드, 권한 밖 문서 접근 시도)은 자동 탐지해 관리자에게 알림을 보냅니다. 이 세 장치가 결합되면 공직자는 안심하고 AI 를 사용할 수 있습니다.

7 장. 4 단계 실행 가이드: AI 플랫폼 구축

7.1 SaaS vs 구축형 vs 하이브리드 비교

4 단계에서 지자체는 AI 플랫폼 구축 방식을 결정해야 합니다. 선택지는 세 가지입니다. 첫째, SaaS 방식입니다. 1~3 단계에서 사용하던 클라우드 기반 서비스를 계속 유지하는 방식입니다. 장점은 초기 투자 비용이 없고, 최신 LLM 을 자동으로 업데이트받으며, 유지보수 부담이 없다는 점입니다. 단점은 장기적으로 구독료가 누적되고, 내부 데이터 통제가 제한적이며, 서비스 제공사 정책 변경에 영향을 받는다는 점입니다. 둘째, 구축형 방식입니다. 내부망에 LLM 과 데이터 플랫폼을 직접 구축하는 방식입니다. 장점은 데이터 완전 통제, 장기 비용 절감, 커스터마이징 자유도가 높다는 점입니다. 단점은 초기 투자 비용이 크고(수억~수십억 원), 구축 기간이 길며(1~2 년), 전문 인력이 필요하고, LLM 업데이트를 직접 관리해야 한다는 점입니다. 셋째, 하이브리드 방식입니다. 민감정보는 내부망 LLM 로 처리하고, 공개정보는 외부 LLM 을 활용하는 방식입니다. 장점은 보안과 성능을 동시에 확보하고, 비용을 최적화하며, 유연한 운영이 가능하다는 점입니다. 단점은 설계 복잡도가 높고, 내부망·외부망 간 데이터 흐름 관리가 필요하다는 점입니다. 권장 방식은 하이브리드입니다. 광역자치단체는 하이브리드로 구축하고, 소규모 기초자치단체는 SaaS 를 장기 유지하는 것이 현실적입니다.

7.2 멀티 LLM 및 LLM 라우팅 구조

공직자용 AI 에이전트는 하나의 LLM 에 의존하지 않고, 여러 LLM 을 업무와 보안 등급에 따라 선택적으로 사용하는 멀티 LLM 구조가 효율적입니다. 멀티 LLM 의 핵심은 LLM 라우팅입니다. 라우팅은 두 가지 기준으로 이뤄집니다. 첫째, 보안 등급별 라우팅입니다. C 급 데이터가 포함된 질문은 내부망 LLM 으로만 처리합니다. S 급 데이터는 내부망 LLM 을 우선 사용하되, 성능이 필요한 경우 개인정보 마스킹 후 외부 LLM 을 사용합니다. O 급 데이터는 외부 고성능 LLM 을 자유롭게 사용합니다. 보안 등급은 질문

텍스트와 업로드 파일을 자동 분석해 판별하며, 불명확한 경우 공직자에게 등급 확인을 요청합니다. 둘째, 업무별 모델 선택입니다. 정책 기획, 법령 분석처럼 고도의 추론이 필요한 업무는 최상위 추론 모델(GPT, Claude, Gemini 등)을 사용합니다. 단순 안내, 요약, 번역은 경량 모델을 사용해 비용을 절감합니다. 민원 분석은 중간 수준 모델로 충분합니다. 업무별 모델 매핑은 5장에서 설계한 에이전트별 입력·출력 구조를 바탕으로 사전 정의합니다. 라우팅 규칙은 관리자 화면에서 조정 가능하며, 새로운 LLM 이 출시되면 성능 테스트 후 라우팅 테이블에 추가합니다. 멀티 LLM 구조는 특정 LLM 종속을 방지하고, 비용과 성능을 최적화하며, 기술 발전에 유연하게 대응할 수 있는 장점이 있습니다.

7.3 내부망·외부망 LLM 분리 운영

하이브리드 방식의 핵심은 내부망과 외부망 LLM 을 분리 운영하는 것입니다. 내부망 LLM 은 지자체 데이터센터 또는 전산실에 구축하며, 인터넷과 물리적으로 분리된 폐쇄망에서 운영합니다. 민감정보 처리 전용으로 사용하며, C 급·S 급 데이터만 처리합니다. 내부망 LLM 은 성능보다 보안과 안정성을 우선하므로, 검증된 오픈소스 LLM 이나 국산 LLM 을 사용합니다. 내부망에서는 외부 검색이 불가능하므로, 메타데이터 RAG 와 MCP 로 내부 시스템 데이터만 활용합니다. 외부망 LLM 은 클라우드 기반 API 로 사용하며, 인터넷 접속이 가능한 환경에서 운영합니다. 공개정보 처리 전용으로 사용하며, O 급 데이터만 처리합니다. 외부망 LLM 은 보안보다 성능을 우선하므로, 글로벌 최상위 LLM(GPT, Claude, Gemini 등)을 사용합니다. 외부망에서는 검색 API, MCP, 메타데이터 RAG 를 모두 활용해 최신 정보를 제공합니다. 내부망과 외부망 사이에는 데이터 전송 게이트웨이를 두고, S 급 데이터를 외부망으로 전송할 때 반드시 개인정보 마스킹과 민감 표현 제거를 거칩니다. 게이트웨이는 모든 전송 내역을 로그로 기록하며, 이상 전송(대량 데이터, 비인가 사용자)을 자동 차단합니다. 이 분리 운영 구조는 보안을 유지하면서도 최고 성능의 LLM 을 활용할 수 있는 현실적 방법입니다.

7.4 행정 문서 특화 임베딩과 검색 최적화

공공 행정 문서는 일반 문서와 구조가 다릅니다. 법령은 "장-절-조-항-호-목" 계층 구조를 가지며, 예산서는 셀 병합이 많고 표 안에 표가 있는 복잡한 형태입니다. 일반 임베딩 방식으로는 이런 문서의 의미를 정확히 파악하기 어렵습니다. 행정 문서 특화 임베딩의 핵심은 세 가지입니다. 첫째, 구조 보존 청킹입니다. 법령을 500 자 단위로 기계적으로 자르면 "제 1 항의 규정에도 불구하고 다음 각 호의 경우에는 예외로 한다"라는 문장 뒤에서 텍스트가 잘려 예외 조건을 놓칩니다. 구조 보존 청킹은 조문 단위로 텍스트를 분할하고, 각 조문마다 상위 제목(장, 절, 조)을 메타데이터로 붙입니다. 이렇게 하면 AI 가 법령의 단서 조항이나 예외 규정을 정확히 이해합니다. 둘째, 표 인식 최적화입니다. 예산서나 통계표는 셀 병합, 다단 헤더, 각주가 많습니다. 일반 OCR 은 이를 평면 텍스트로 변환해 의미가 소실됩니다. 표 인식 최적화는 표의 행·열 구조를 유지하고, 병합된 셀의 범위를 메타데이터로 기록하며, 각주와 본문을 구분해 저장합니다. 이렇게 하면 AI 가 "2026 년도 복지 예산 중 노인복지 비중"처럼 표의 특정 셀 값을 정확히 찾습니다. 셋째, 메타데이터 강화입니다. 문서 내용뿐 아니라 발행기관, 시행일, 개정일, 보안등급, 적용대상, 효력상태를 메타데이터로 함께 저장합니다. 검색 시 메타데이터 필터링을 먼저 수행해 현행 유효 문서만 검색 대상으로 삼습니다. 이 세 가지가 결합되면 행정 문서 검색 정확도가 일반 임베딩 대비 30% 이상 향상됩니다.

7.5 MCP 기반 시스템 연계

MCP(Model Context Protocol)는 AI 가 외부 시스템이나 데이터베이스에 실시간으로 접근할 수 있게 하는 표준 프로토콜입니다. 공직자용 AI 에이전트에서 MCP 는 내부 행정 시스템 연계에 필수적입니다. MCP 연계 대상은 세 가지입니다. 첫째, 내부 행정 시스템입니다. 서울, 온나라 같은 전자결재 시스템, 민원 관리 시스템, 예산 시스템, 인사 시스템과 MCP 로 연동해 실시간 데이터를 조회합니다. 예를 들어 공직자가 "우리 부서 올해 예산 집행률"을 물으면, MCP 가 예산 시스템에 접속해 최신 데이터를 가져옵니다. 둘째, 공공 DB 입니다. 나라장터, 사업자등록정보, 건축물대장 같은 공공 DB 와 MCP 로 연동해 최신 정보를 조회합니다. 셋째, IoT 플랫폼입니다. 상수도 수압, 대기질, CCTV 같은 실시간 센서 데이터를 MCP 로 가져와 AI 가 현장 상황을 파악합니다. MCP 연계 시 보안이 핵심입니다. CSO 등급별 접근 통제를 적용하고, 사용자 부서와 권한을 확인한 후에만 데이터를 전달합니다. MCP 호출은 모두 로그로 기록하며, 대량 조회나 비인가

접근은 자동 차단합니다. MCP 는 검색 API 와 메타데이터 RAG 로 찾을 수 없는 내부 실시간 데이터를 AI 에 전달하는 핵심 통로입니다.

7.6 에이전트 토큰 비용 최적화 전략

일부 지자체는 AI 에이전트 운영 중 토큰 비용이 폭증해 사업을 중단한 사례가 있습니다. 토큰 비용 최적화는 네 가지 전략으로 해결합니다. 첫째, 캐싱입니다. 같은 질문이 반복되면 LLM 을 다시 호출하지 않고 이전 답변을 재사용합니다. 법령 조문, 통계 같은 정적 정보는 캐싱 효과가 큼니다. 캐싱 기간은 데이터 유형별로 설정하며, 법령은 1 일, 통계는 1 주, 실시간 센서는 캐싱 없음으로 운영합니다. 둘째, 프롬프트 최적화입니다. 불필요하게 긴 프롬프트는 토큰을 낭비합니다. 에이전트별로 핵심 지시문만 포함하고, 반복되는 맥락 정보는 시스템 프롬프트로 분리합니다. 셋째, 검색 우선순위입니다. LLM 호출 전에 검색 API, MCP, 메타데이터 RAG 로 정보를 먼저 찾고, 찾은 정보만 LLM 에 전달합니다. 이렇게 하면 LLM 이 처리하는 토큰 양이 줄어듭니다. 넷째, 응답 길이 제한입니다. 에이전트별로 최대 응답 길이를 설정해 과도하게 긴 답변을 방지합니다. 민원 회신은 1,000 자, 정책 기획서는 3,000 자처럼 업무별로 적정 길이를 정의합니다. 이 네 전략을 적용하면 토큰 비용을 최적화 전 대비 50% 이상 절감할 수 있습니다.

8 장. 공직자용 AI 에이전트의 5 대 설계 원칙

8.1 정확한 데이터

공직자용 AI 에이전트의 첫 번째 설계 원칙은 정확한 데이터입니다. 행정에서는 잘못된 정보 하나가 민원 분쟁, 예산 오집행, 감사 지적으로 이어질 수 있으므로, 데이터의 정확성이 무엇보다 중요합니다. 정확한 데이터의 핵심은 세 가지입니다. 첫째,

공식성입니다. AI에 전달하는 데이터는 정부기관, 공공기관, 학술기관, 언론사 등 공신력 있는 출처에서 나온 것이어야 합니다. 블로그, 카페, 개인 사이트 정보는 제외합니다. 법령은 국가법령정보센터, 통계는 KOSIS, 조례는 자치법규정보시스템처럼 공식 출처만 사용합니다. 둘째, 최신성입니다. 법령은 개정 여부를 실시간 확인하고, 통계는 최신 시점 데이터를 우선 제공하며, 조례는 시행일 기준으로 현행 조문만 검색합니다. 과거 데이터를 최신으로 착각하는 것을 방지하기 위해, 모든 데이터에 시행일·발행일 메타데이터를 부착하고, 검색 시 현행 유효 데이터만 필터링합니다. 셋째, 출처 명확성입니다. AI 답변에는 반드시 출처를 명시합니다. "창녕군 재난지원금 지급 조례 제 5 조 제 2 항(시행 2026.3.1)"처럼 문서명, 조항, 시행일을 함께 표시합니다. 출처가 불명확한 정보는 "확인 필요"로 표시하고, 공식 출처 확인을 안내합니다. 이 세 가지가 지켜지면 공직자는 AI 답변을 신뢰하고 업무에 바로 활용할 수 있습니다.

8.2 근거 기반 추론 성능

공직자용 AI 에이전트의 두 번째 설계 원칙은 근거 기반 추론 성능입니다. 공직자 업무는 법령 해석, 정책 대안 비교, 민원 쟁점 분석처럼 고도의 추론이 필요합니다. 단순 검색만으로는 부족하고, 복잡한 맥락을 이해하고 판단을 보조하는 추론 능력이 필수적입니다. 근거 기반 추론의 핵심은 두 가지입니다. 첫째, 고성능 추론 모델입니다. 공직자 업무는 박사급 이상의 추론 역량이 필요하므로, 글로벌 최상위 LLM(GPT, Claude, Gemini 등)을 활용합니다. 국산 LLM이나 제한적 모델은 추론 능력이 현저히 낮아 정책 기획이나 법령 분석 같은 고난도 업무에 부적합합니다. 다만 고성능 모델은 비용이 높으므로, 7.2 절에서 설명한 업무별 모델 선택으로 비용을 최적화합니다. 둘째, 업무별 성능 기준입니다. 추론 성능은 업무별로 다르게 평가합니다. 법령 인용 정확도(조문 번호 일치율, 개정 반영 여부), 민원 답변 품질(사실관계 정확도, 누락 항목 탐지율), 문서 작성 실용성(공문체 적합도, 수정 필요 횟수), 표 인식 정확도(셀 병합 처리율, 표 안의 표 인식률), 추론 일관성(같은 질문 반복 시 답변 편차)을 측정합니다. 각 업무별로 목표 성능을 설정하고, 주기적으로 평가해 기준 미달 시 모델을 교체하거나 프롬프트를 개선합니다. 근거 기반 추론은 "좋은 모델을 쓴다"가 아니라 "공직자 업무에서 검증된 모델을 쓴다"는 의미입니다.

8.3 공직자 업무 사고 흐름의 재현

공직자용 AI 에이전트의 세 번째 설계 원칙은 공직자 업무 사고 흐름의 재현입니다. 공직자는 업무를 처리할 때 일정한 사고 흐름을 따릅니다. 정책 기획자는 문제 정의→현황 분석→원인 파악→대안 비교→추진안 도출 순서로 생각하고, 민원 담당자는 민원 내용 파악→쟁점 도출→관련 법령 확인→유사 사례 검토→회신 방향 결정→초안 작성 순서로 일합니다. AI 에이전트는 이 사고 흐름을 재현해야 공직자가 자연스럽게 사용할 수 있습니다. 사고 흐름 재현의 핵심은 두 가지입니다. 첫째, 업무 절차 복제입니다. 5 장에서 설명한 실무자 인터뷰와 워크숍으로 부서별·업무별 사고 흐름을 수집하고, 이를 에이전트 처리 단계로 구현합니다. AI 는 공직자가 각 단계에서 필요한 자료를 순서대로 제시하고, 다음 단계로 넘어가기 전 확인해야 할 체크리스트를 함께 알려줍니다. 둘째, 단계별 판단 지원입니다. AI 는 정보만 제시하는 것이 아니라, 각 단계에서 "어떤 점을 주의해야 하는가", "어떤 리스크가 있는가", "추가 확인이 필요한 사항은 무엇인가"를 함께 안내합니다. 공직자는 AI 가 제시한 흐름을 따라가며 판단하고, 최종 산출물을 받습니다. 사고 흐름 재현은 AI 를 단순 도구가 아니라 업무 파트너로 만드는 핵심입니다.

8.4 보안·권한·개인정보 보호

공직자용 AI 에이전트의 네 번째 설계 원칙은 보안·권한·개인정보 보호입니다. 공공 데이터는 민감정보를 포함하므로, 아무리 성능이 좋아도 보안이 취약하면 도입할 수 없습니다. 보안의 핵심은 세 가지입니다. 첫째, CSO 등급별 통제입니다. 데이터를 C 급(비밀), S 급(대외비), O 급(공개)으로 분류하고, 등급에 따라 내부망 LLM 과 외부망 LLM 을 분리 운영합니다. C 급은 내부망만, S 급은 내부망 우선, O 급은 외부망 허용으로 라우팅합니다. 등급 판별은 자동으로 이뤄지며, 불명확한 경우 공직자에게 확인을 요청합니다. 둘째, 권한 관리입니다. 공직자의 부서, 직급, 역할에 따라 접근 가능한 문서를 제한합니다. 복지과 주무관은 복지과 문서만 검색 가능하고, 타 부서 문서는 검색 결과에서 제외됩니다. 권한은 인사 시스템과 연동해 자동 업데이트되며, 퇴직자나 전출자는 즉시 접근이 차단됩니다. 셋째, 감사 추적입니다. 누가 언제 어떤 문서를 검색했는지, 어떤 LLM 을 사용했는지, 어떤 답변을 받았는지 모두 로그로 기록합니다.

이상 접근(대량 문서 다운로드, 권한 밖 문서 접근 시도)은 자동 탐지해 관리자에게 알림을 보냅니다. 감사 시 이 로그로 적법성을 입증할 수 있습니다.

8.5 근거 제시와 검토 가능한 책임 구조

공직자용 AI 에이전트의 다섯 번째 설계 원칙은 근거 제시와 검토 가능한 책임 구조입니다. 공공 행정은 모든 결정에 근거가 필요하고, 잘못된 결정은 책임 소재를 밝혀야 합니다. AI 답변도 마찬가지입니다. 근거와 책임의 핵심은 세 가지입니다. 첫째, 출처 표시입니다. AI 답변에는 반드시 출처를 명시합니다. "창녕군 재난지원금 지급 조례 제 5 조 제 2 항(시행 2026.3.1)"처럼 문서명, 조항, 시행일을 함께 표시하고, 가능하면 원문 링크도 제공합니다. 출처가 여러 개면 우선순위 순서로 나열하고, 각 출처의 신뢰도(공식 문서 > 보도자료 > 해설 기사)를 표시합니다. 둘째, 검토 체계입니다. 모든 업무를 AI 가 자동 처리하는 것이 아니라, 업무 성격에 따라 검토 단계를 다르게 설정합니다. 단순 안내(법령 조문 찾기, 통계 조회)는 AI 자동 응답 가능, 민원 회신은 담당자 검토 필수, 법령·예산·인사 같은 고위험 업무는 부서 책임자 검토 필수로 설정합니다. 검토 필수 업무는 AI 답변에 "담당자 검토 필요" 플래그를 붙이고, 검토 없이 사용하면 경고를 표시합니다. 셋째, 정정 이력입니다. AI 답변이 틀렸을 때 공직자가 수정한 내용을 기록하고, 같은 질문이 다시 들어오면 수정된 답변을 우선 제시합니다. 오답 사례는 주기적으로 수집해 모델 재학습이나 프롬프트 개선에 반영합니다. 근거 제시와 검토 체계는 AI 를 책임 있게 사용할 수 있는 안전장치입니다.

9 장. 핵심 업무별 에이전트 설계 상세

9.1 아이디어 도출 에이전트

아이디어 도출 에이전트는 신규 사업 발굴, 주민 체감형 서비스 개선, 공모사업 대응 시 활용됩니다. 입력 항목은 "주제", "대상 주민", "지역 특성", "예산 범위", "추진

기간"입니다. 사고 흐름은 5 단계로 구성됩니다. 1 단계는 주제 분해입니다. "청년 유출 문제"를 입력하면 일자리, 주거, 문화, 교통, 정주여건으로 세분화합니다. 2 단계는 유사 정책 사례 수집입니다. 검색 API 로 타 지자체, 중앙부처, 해외 사례를 검색합니다. 3 단계는 지역 데이터 결합입니다. 통계청, 공공데이터에서 인구, 산업, 민원 데이터를 가져와 지역 여건을 반영합니다. 4 단계는 아이디어 생성입니다. 단기형, 중기형, 저예산형, 상징형으로 구분해 3~5 개 아이디어를 제시합니다. 5 단계는 실행 가능성 평가입니다. 법적 근거, 예산 부담, 부서 협업 필요도를 점검합니다. 출력 형식은 "아이디어 카드(제목, 핵심 내용, 기대효과, 예산 수준, 참고 사례)"입니다. 차별화 포인트는 근거 없는 창의성이 아니라 데이터 기반 기획 아이디어를 낸다는 점입니다.

9.2 정책 기획 에이전트

정책 기획 에이전트는 신규 정책 기획서, 사업계획서 작성 시 활용됩니다. 입력 항목은 "정책 과제명", "대상 주민", "예산 범위", "추진 기간", "제약조건"입니다. 사고 흐름은 7 단계로 구성됩니다. 1 단계는 정책 과제 정의입니다. 문제 상황, 대상, 시급성을 정리합니다. 2 단계는 현황 분석입니다. 통계청, 공공데이터에서 관련 통계를 검색하고, 민원 현황, 언론 보도를 분석합니다. 3 단계는 원인 분석입니다. 구조적 원인, 제도적 원인, 실행상 원인을 구분합니다. 4 단계는 정책 대안 생성입니다. 타 지자체 사례, 연구보고서를 검색해 대안 1, 2, 3 을 생성합니다. 5 단계는 대안 비교입니다. 효과성, 실현 가능성, 예산성, 주민 수용성을 기준으로 비교표를 만듭니다. 6 단계는 추진안 도출입니다. 최적안을 선정하고 추진 전략을 정리합니다. 7 단계는 문서 작성입니다. 정책기획서 초안(정책 과제명, 추진 배경, 현황 및 문제점, 정책 목표, 추진 전략, 세부 과제, 기대 효과, 법적 근거, 재정 검토)을 HWP 또는 DOCX 로 출력합니다. 차별화 포인트는 정책 논리 구조("왜→무엇→어떻게→효과")를 자동으로 만든다는 점입니다.

9.3 민원 분석 자동화 에이전트

민원 분석 자동화 에이전트는 국민신문고 등 민원 접수 시 활용됩니다. 입력 항목은 "민원 텍스트", "첨부 파일"입니다. 사고 흐름은 6 단계로 구성됩니다. 1 단계는 민원 유형 분류입니다. 단순 문의, 불만, 제도 건의, 반복 민원, 집단 민원으로 분류합니다.

2 단계는 핵심 쟁점 추출입니다. 장소, 시점, 요구사항, 갈등 요인을 파악합니다. 3 단계는 관련 근거 검색입니다. 법령 조회 시스템으로 관련 법령·조례·지침을 검색하고, 메타데이터 RAG 로 과거 유사 민원 처리 사례를 찾습니다. 4 단계는 회신 방향 결정입니다. 수용 가능, 불가, 추가 안내, 부서 이관으로 판단합니다. 5 단계는 회신 초안 작성입니다. 민원회신체로 초안을 생성하고, 근거 조문과 처리기한을 명시합니다. 6 단계는 분석 리포트 생성입니다. 민원 요약, 민원 유형, 핵심 요구사항, 관련 근거, 회신 초안, 추가 확인 필요사항, 유사 민원 여부를 정리합니다. 출력 형식은 "민원 분석 리포트(HWP)"입니다. 차별화 포인트는 민원 처리 보조뿐 아니라 반복 민원 패턴 탐지까지 한다는 점입니다.

9.4 법령 조회 에이전트

법령 조회 에이전트는 관련 법령·조례·지침 탐색 시 활용됩니다. 입력 항목은 "질문 텍스트"입니다. 사고 흐름은 5 단계로 구성됩니다. 1 단계는 질문 유형 판별입니다. 인허가, 복지, 인사, 계약, 행정절차 등으로 분류합니다. 2 단계는 핵심 법적 쟁점 도출입니다. 질문에서 법적으로 중요한 키워드를 추출합니다. 3 단계는 관련 법령 후보군 검색입니다. 국가법령정보센터 API 로 법령을 검색하고, 자치법규정보시스템 API 로 조례를 검색합니다. 4 단계는 조문 수준 매칭입니다. 법령 전체가 아니라 질문과 관련된 특정 조문을 찾습니다. 5 단계는 관련 조례·지침 연결입니다. 상위 법령과 연결된 지자체 조례, 중앙부처 지침을 함께 제시합니다. 출력 형식은 "법령 검토 리포트(적용 가능 법령, 관련 조문 요지, 관련 조례/지침, 해석상 유의점, 추가 확인 필요사항)"입니다. 차별화 포인트는 법령을 보여주는 도구가 아니라 질문에 맞는 법적 근거 후보군을 정리하는 도구라는 점입니다. 다만 정확한 법령·자치법규 조문 조회는 법령 조회 시스템 비서가 국가법령정보센터·자치법규정보시스템 공식 데이터로 더 정확하게 수행하므로, 복잡한 법령 질의는 해당 비서 활용을 권장합니다.

9.5 법적 가이드 에이전트

법적 가이드 에이전트는 특정 행정행위의 법적 리스크 점검 시 활용됩니다. 입력 항목은 "사안 개요"입니다. 사고 흐름은 6 단계로 구성됩니다. 1 단계는 사안 요약입니다.

행정행위의 핵심 내용을 정리합니다. 2 단계는 법적 쟁점 도출입니다. 법적으로 문제가 될 수 있는 부분을 파악합니다. 3 단계는 관련 법령·판례·유권해석 검색입니다. 법령 조회 시스템으로 관련 법령을 찾고, 판례 DB 에서 유사 사례를 검색합니다. 4 단계는 가능 해석 범위 제시입니다. 법령 해석에 여지가 있는 경우 여러 해석을 제시합니다. 5 단계는 실무상 리스크 정리입니다. 분쟁 가능성, 감사 지적 가능성, 민원 발생 가능성을 점검합니다. 6 단계는 검토 메모 작성입니다. 담당자가 확인해야 할 항목을 체크리스트로 정리합니다. 출력 형식은 "법적 검토 가이드(사안 개요, 관련 법적 쟁점, 적용 가능 법령, 실무상 유의점, 분쟁·감사 리스크, 추가 확인 필요사항, 담당부서 검토 의견 초안)"입니다. 차별화 포인트는 결론을 단정하지 않고 "어디가 위험한지, 무엇을 더 확인해야 하는지"를 알려준다는 점입니다.

10 장. 운영관리와 성과평가

10.1 운영 조직과 역할 분담

공직자용 AI 에이전트는 도입 후 지속적 운영과 개선이 필수적입니다. 운영 조직은 세 층위로 구성됩니다. 첫째, AI 정책팀입니다. 기획조정실 또는 디지털정책과 소속으로, AI 전략 수립, 예산 확보, 성과 평가, 대외 협력을 담당합니다. 둘째, 정보화팀입니다. 정보통신과 또는 정보화담당관 소속으로, 시스템 운영, 보안 관리, 장애 대응, 사용자 지원을 담당합니다. 셋째, 부서별 데이터 오너입니다. 각 부서에서 1~2 명을 지정해 부서 내 AI 활용 촉진, 오답 사례 수집, 에이전트 개선 요구사항 전달을 담당합니다. 이 세 층위가 협력해야 AI 에이전트가 지속적으로 개선됩니다. 역할 분담이 불명확하면 아무도 책임지지 않아 시스템이 방치됩니다.

10.2 성과지표 설계

AI 에이전트의 성과는 네 가지 지표로 측정합니다. 첫째, 사용률입니다. 월 활성 사용자(MAU) 비율과 주 1 회 이상 사용하는 파워유저 비율을 측정합니다. 목표는 전체 공직자의 30% 이상이 월 1 회 이상 사용, 10% 이상이 주 1 회 이상 사용입니다. 둘째, 정확도입니다. AI 답변의 정확도를 공직자 평가로 측정합니다. "AI 답변이 업무에 바로 활용 가능한가"를 5 점 척도로 평가해 평균 3.5 점 이상이 목표입니다. 법령 인용 정확도, 통계 수치 정확도는 별도로 측정합니다. 셋째, 업무 효율입니다. 보고서 작성 시간, 자료 검색 시간, 민원 회신 작성 시간을 AI 사용 전후로 비교합니다. 평균 30% 이상 단축이 목표입니다. 넷째, 만족도입니다. 월 1 회 설문조사로 "AI 가 업무에 도움이 되는가", "계속 사용하고 싶은가"를 5 점 척도로 측정합니다. 평균 4.0 점 이상이 목표입니다. 이 네 지표를 종합해 AI 에이전트의 성과를 평가하고, 목표 미달 시 개선 계획을 수립합니다.

10.3 정확도, 만족도, 업무효율 측정

정확도는 두 가지 방법으로 측정합니다. 첫째, 공직자 평가입니다. AI 답변을 받은 공직자가 "정확도" 항목을 5 점 척도로 평가합니다. 평가는 선택 사항이지만, 평가 참여율을 높이기 위해 간편 평가 버튼(👍👎)을 제공합니다. 둘째, 오답 사례 수집입니다. 공직자가 "이 답변이 틀렸다"고 신고하면 오답 사례로 기록하고, 주기적으로 분석해 오답률을 계산합니다. 만족도는 월 1 회 온라인 설문조사로 측정합니다. 설문 대상은 AI 를 1 회 이상 사용한 공직자이며, 5 분 내외로 완료 가능한 간단한 설문지를 사용합니다. 업무효율은 사용 로그 분석과 사용자 자가 평가를 결합합니다. AI 가 문서 초안을 생성한 시간, 공직자가 수정에 소요한 시간을 로그로 기록하고, 공직자에게 "AI 사용 전 대비 시간이 얼마나 단축되었는가"를 설문조사합니다. 평가 주기는 월 1 회이며, 결과는 AI 정책팀과 정보화팀이 공유하고 개선 과제를 도출합니다.

10.4 지속 개선 체계

AI 에이전트는 한 번 구축하고 끝나는 것이 아니라 지속적으로 개선해야 합니다. 개선 체계는 네 가지입니다. 첫째, 오답 수집입니다. 공직자가 신고한 오답 사례를 주기적으로

수집하고, 오답 원인을 분석합니다. 데이터 오류, 프롬프트 문제, 모델 한계로 구분해 원인별 대응 방안을 수립합니다. 둘째, 재학습입니다. 오답 사례를 바탕으로 프롬프트를 수정하거나, 메타데이터 RAG의 검색 우선순위를 조정합니다. 필요 시 에이전트 처리 단계를 재설계합니다. 셋째, 모델 교체 기준입니다. 특정 LLM의 성능이 지속적으로 목표에 미달하면 다른 LLM으로 교체합니다. 교체 기준은 "3개월 연속 정확도 3.5점 미만" 또는 "오답률 20% 이상"입니다. 넷째, 피드백 반영입니다. 부서별 데이터 오ner가 수집한 개선 요구사항을 월 1회 검토 회의에서 논의하고, 우선순위가 높은 요구사항부터 반영합니다. 이 네 가지 체계가 작동하면 AI 에이전트는 시간이 갈수록 정확도와 만족도가 높아집니다.

11 장. 지자체 적용 시 고려사항

11.1 예산, 조달, 계약 방식

AI 에이전트 도입 시 예산과 계약 방식은 세 가지입니다. 첫째, SaaS 구독료입니다.

1~2 단계는 SaaS 방식으로 진행하며, 사용자 수 기준 월 구독료를 지급합니다.

광역자치단체 공직자 6천 명 기준 연간 5천만~1억 원, 기초자치단체 공직자 500명 기준 연간 5백만~1천만 원 수준입니다. 계약은 조달청 지정구매나 수의계약이 가능한 경우가 많으므로, 입찰 절차를 단축할 수 있습니다. 둘째, 구축형 사업비입니다.

3~4 단계는 구축형으로 진행하며, 데이터 플랫폼, 메타데이터 RAG, LLM 라우팅 시스템, 보안 체계 구축 비용이 필요합니다. 광역자치단체 기준 5~10억 원, 기초자치단체 기준 2~5억 원 수준입니다. 계약은 제안요청서(RFP) 작성 후 경쟁입찰 방식으로 진행합니다.

셋째, 유지보수비입니다. 구축 후 연간 유지보수비는 구축비의 10~15% 수준입니다.

조달 방식은 조달청 등록 제품은 지정구매, 미등록 제품은 제안요청 후 입찰로 진행합니다. 예산 확보는 전년도 하반기에 차년도 예산에 반영하며, 긴급 도입이 필요한 경우 예비비나 추경으로 확보합니다.

11.2 조직문화와 사용자 수용성

AI 에이전트 도입의 가장 큰 장애물은 기술이 아니라 조직문화입니다. 공직자들이 AI 사용을 거부하거나 소극적으로 대응하면 아무리 좋은 시스템도 무용지물입니다. 저항 요인은 세 가지입니다. 첫째, 새로운 도구 학습 부담입니다. 기존 업무 방식에 익숙한 공직자들은 AI 사용법을 배우는 것 자체를 부담스러워합니다. 둘째, AI 신뢰 부족입니다. "AI가 틀린 답을 주면 어떡하나", "AI에 의존하면 내 능력이 떨어지는 것 아닌가" 같은 우려가 있습니다. 셋째, 일자리 불안입니다. "AI가 내 일을 대체하는 것 아닌가"라는 두려움이 있습니다. 이를 극복하는 방법은 네 가지입니다. 첫째, 교육 프로그램입니다. 2시간 온라인 강의 + 2주간 실습 지원으로 사용법을 익히게 하고, 부서별 파워유저를 지정해 동료 지원 체계를 만듭니다. 둘째, 성공 사례 공유입니다. 파일럿 부서의 성공 사례를 전 부서에 공유해 AI 효용을 체감하게 합니다. 셋째, 인센티브입니다. AI 활용 우수 부서·개인을 선정해 포상하거나, 업무 평가에 반영합니다. 넷째, 일자리 불안 해소입니다. "AI는 반복 업무를 줄여 공직자가 정책 기획, 주민 소통 같은 본질 업무에 집중하게 한다"는 메시지를 지속적으로 전달합니다.

11.3 부서별 우선 도입 영역

모든 부서에 동시 도입하기보다, 효과가 큰 부서부터 단계적으로 확산하는 것이 현실적입니다. 우선 도입 부서는 네 가지입니다. 첫째, 기획 부서입니다. 정책 기획, 사업계획서 작성, 타 지자체 사례 비교 업무가 많아 AI 효과가 큼니다. 기획조정실, 기획예산담당관이 해당됩니다. 둘째, 민원 부서입니다. 민원 분석, 회신 초안, 반복 민원 패턴 탐지 업무가 많아 AI 효과가 큼니다. 민원봉사과, 종합민원실이 해당됩니다. 셋째, 법무 부서입니다. 법령 검토, 조례 충돌 감지, 감사 대응 자료 정리 업무가 많아 AI 효과가 큼니다. 법무담당관, 자치법규담당관이 해당됩니다. 넷째, 홍보 부서입니다. 보도자료 초안, 연설문 작성, SNS 여론 분석 업무가 많아 AI 효과가 큼니다. 홍보담당관, 소통기획관이 해당됩니다. 이 네 부서에서 성과를 내면, 복지·건설·환경 등 타 부서로 확산이 쉽습니다.

11.4 인프라 우선 접근의 실패 사례와 대안

일부 지자체는 AI 도입 시 대규모 데이터 플랫폼이나 온톨로지 구축부터 시작해 실패했습니다. 실패 원인은 네 가지입니다. 첫째, 기초 데이터 부재입니다. 공공기관 데이터는 대부분 공직자 PC 속 비정형 문서로 흩어져 있어, 온톨로지를 설계할 기초 데이터 자체가 부족합니다. 둘째, 행정 도메인 이해 부족입니다. 외부 IT 기업이 단기 인터뷰만으로 복잡한 행정 업무를 이해하고 온톨로지를 설계하기 어렵습니다. 셋째, 과잉 설계로 인한 예산·시간 낭비입니다. 수십억 원을 투입해 1~2 년 구축했지만, 막상 사용해보니 공직자 업무와 맞지 않아 활용률이 저조합니다. 넷째, 생성형 AI 시대에 맞지 않는 과거 접근입니다. 2009 년경 빅데이터 붐 당시 설계 방식을 그대로 적용해 현재 LLM 이 소화하기 어려운 구조로 만들어집니다. 대안은 메타데이터 RAG 입니다. 새로운 온톨로지를 처음부터 설계하지 않고, 이미 잘 정리된 정부·지자체 홈페이지 구조를 메타데이터로 활용합니다. 검색 API→MCP→메타데이터 RAG 3 단계 전략으로 비용을 최소화하고 최신성을 보장하며, 실무 에이전트를 먼저 운영하며 데이터를 축적한 후 향후 필요 시 상향식 온톨로지를 구성합니다. 인프라 우선이 아니라 성과 우선, 데이터 우선 접근이 핵심입니다.

12 장. 결론 및 제언

12.1 공직자용 AI 에이전트 구축의 핵심 메시지

본 백서는 전국 광역 및 기초자치단체가 공직자용 AI 에이전트를 성공적으로 구축하기 위한 실무 가이드를 제시했습니다. 핵심 메시지는 다섯 가지입니다. 첫째, 5 대 설계 원칙입니다. 정확한 데이터, 근거 기반 추론 성능, 공직자 업무 사고 흐름의 재현, 보안·권한·개인정보 보호, 근거 제시와 검토 가능한 책임 구조가 반드시 지켜져야 합니다. 이 중 하나라도 빠지면 공직자용 AI 에이전트로 완성되지 않습니다. 둘째, 4 단계 로드맵입니다. SaaS 형 AI 비서 즉시 도입(1 단계) → 핵심 에이전트 발굴 및 검증(2 단계) → 데이터·보안 체계 고도화(3 단계) → 전사 통합형 AI 플랫폼 구축(4 단계) 순서로 점진적으로 확장해야 위험을 최소화하고 성과를 극대화할 수 있습니다. 셋째, 데이터

중심 접근입니다. 특정 LLM 에 종속되지 않고, 공직자가 우선적으로 참고해야 하는 14 가지 티어 1 데이터를 정의하고, 검색 API→MCP→메타데이터 RAG 3 단계 전략으로 정확한 정보를 찾아 AI 에 전달하는 것이 핵심입니다. 넷째, 업무 중심 에이전트 설계입니다. 기능 나열이 아니라 공직자의 업무 사고 흐름을 재현하는 에이전트를 만들어야 공직자가 자연스럽게 사용합니다. 다섯째, 성과 우선 접근입니다. 대규모 인프라 구축을 미루고, 공직자가 체감하는 성과부터 만들어야 조직 내 확산이 가능합니다. 이 다섯 가지를 지키면 지자체는 예산 낭비 없이 공직자가 진짜 쓰는 AI 를 만들 수 있습니다.

12.2 지자체 AI 전환의 방향

공직자용 AI 에이전트 도입은 단순한 기술 도입이 아니라 지자체 AI 전환의 출발점입니다. 지자체 AI 전환의 방향은 세 가지입니다. 첫째, 데이터 중심입니다. AI 모델은 계속 발전하고 교체되지만, 데이터는 조직의 자산으로 축적됩니다. 따라서 특정 LLM 에 종속되지 않고, 데이터 체계를 먼저 구축하는 것이 지속 가능한 AI 인프라의 기반입니다. 공직자 우선 데이터 전략, AI 데이터 전달 3 대 유형, 메타데이터 RAG 는 모두 데이터 중심 접근의 구체적 방법입니다. 둘째, 실행 우선입니다. 완벽한 계획을 세우고 대규모 인프라를 구축하는 방식은 실패 위험이 큼니다. SaaS 로 빠르게 시작하고, 파일럿 부서에서 성과를 내며, 사용자 반응을 확인한 후 단계적으로 확장하는 방식이 현실적입니다. 실행하며 배우고, 배우며 개선하는 애자일 방식이 AI 도입에 적합합니다. 셋째, 단계적 확장입니다. 한 번에 모든 부서, 모든 업무에 AI 를 도입하려 하지 말고, 효과가 큰 부서와 업무부터 시작해 성공 사례를 만들고, 이를 바탕으로 전 부서로 확산하는 것이 조직 수용성을 높이는 방법입니다. 이 세 가지 방향을 따르면 지자체는 AI 전환을 안정적으로 추진할 수 있습니다.

12.3 향후 과제

공직자용 AI 에이전트가 전국 지자체에 확산되기 위해서는 세 가지 과제가 남아 있습니다. 첫째, 표준화입니다. 현재는 각 지자체가 개별적으로 AI 를 도입하고 있어 중복 투자가 발생하고 있습니다. 행정안전부나 지방자치단체 협의체 차원에서 공직자용

AI 에이전트의 표준 아키텍처, 표준 에이전트, 표준 데이터 체계를 정립하면 지자체들이 더 효율적으로 도입할 수 있습니다. 특히 법령 조회, 통계 조회, 민원 분석 같은 공통 업무는 표준 에이전트로 개발해 전국 지자체가 공유하는 것이 바람직합니다. 둘째, 광역-기초 협력입니다. 광역자치단체가 AI 플랫폼을 구축하고, 관할 기초자치단체가 이를 공동 활용하는 방식이 예산 효율성을 높입니다. 광역자치단체는 데이터 플랫폼, 메타데이터 RAG, LLM 라우팅 시스템을 구축하고, 기초자치단체는 자체 에이전트만 추가 개발하는 구조가 가능합니다. 이를 위해서는 광역-기초 간 협약, 비용 분담, 운영 체계 마련이 필요합니다. 셋째, 생태계 조성입니다. 공공 AI 시장이 활성화되려면 우수한 AI 기업이 공공 시장에 진입할 수 있어야 합니다. 조달청 등록 절차 간소화, 중소 AI 기업 우대, 성과 기반 계약 방식 도입 등 제도 개선이 필요합니다. 또한 지자체 AI 담당자들이 정보를 공유하고 협력할 수 있는 네트워크(예: 전국 지자체 AI 협의회)를 구성하면 시행착오를 줄이고 우수 사례를 빠르게 확산할 수 있습니다. 이 세 과제가 해결되면 공직자용 AI 에이전트는 전국 지자체의 표준 업무 도구로 자리 잡을 것입니다. 본 백서가 그 출발점이 되기를 기대합니다.

부록

부록 1. 공직자 우선 티어 1 데이터 정의안

공직자가 업무에서 우선적으로 참고해야 하는 티어 1 데이터는 14 가지입니다.

1. **법령**: 헌법, 법률, 대통령령, 총리령, 부령 등 국가법령정보센터의 모든 법령
2. **조례**: 지자체 조례, 규칙, 훈령 등 자치법규정보시스템의 모든 자치법규
3. **지침**: 중앙부처와 지자체의 행정 지침, 예규, 고시, 공고
4. **판례**: 대법원, 헌법재판소, 행정법원 판례 및 행정심판 재결례
5. **지자체 누리집**: 지자체 공식 홈페이지의 공지사항, 보도자료, 정책 안내, 사업 소개
6. **정부기관 누리집**: 중앙부처, 공공기관의 공식 홈페이지 공개 데이터

7. **공공데이터**: 공공데이터포털의 개방 데이터
8. **통계청 데이터**: KOSIS 의 모든 공식 통계
9. **나라장터 데이터**: 입찰 공고, 계약 정보, 낙찰 내역
10. **정부 및 광역 산하 연구기관 보고서**: 국책연구기관, 광역자치단체 산하 연구원의 연구보고서 및 정책 브리프
11. **국내 논문**: 학술 DB 등재 논문
12. **해외 논문**: 국제 학술 DB 논문
13. **국내 언론 기사**: 중앙지, 지역지, 전문지 기사
14. **해외 언론 기사**: 주요 해외 언론사 기사

이 14 가지는 규범 데이터(1~4), 사실 데이터(5~9), 참고 데이터(10~14)로 계층화하며, 질문 유형별로 검색 우선순위를 설정합니다.

부록 2. AI 데이터 전달 3 대 유형 상세

광역 및 기초자치단체가 보유한 데이터를 AI 에 전달하는 방식은 데이터 성격에 따라 3 가지로 구분됩니다.

1. 정확하게 찾아주기

- **대상**: 법령, 조례, 통계, 공공데이터, 언론, 논문 등 외부에 존재하는 정보
- **방법**: 검색 API → MCP → 메타데이터 RAG 순으로 실행하며, 검색 성공 시점에 즉시 중단
- **핵심**: 비용 최소화, 최신성 보장, 출처 신뢰도 확보

2. 정확하게 만들어주기

- **대상**: 인허가 이력, 민원 처리 내역, 예산 집행 데이터, 계약 관리 DB 등 내부 시스템의 파편화된 정형 데이터
- **방법**: ETL 엔진으로 추출·변환·적재해 AI 가 이해 가능한 형태로 가공

- **핵심:** 내부 시스템 간 데이터 결합, 분석 가능한 형태로 정제

3. 정확하게 설명하기

- **대상:** 상수도 수압, 하수처리장 수질, 화재 감지 센서, CCTV 메타데이터 등 현장 센서 데이터
- **방법:** 센서 수치 데이터에 설비 운영 매뉴얼, 비상 대응 SOP 를 결합해 행정·기술적 맥락 부여
- **핵심:** 단순 수치를 의미 있는 정보로 변환

이 3 대 유형을 모두 구현해야 공직자용 AI 에이전트가 완성됩니다.

부록 3. 업무 유형별 데이터 우선순위 매트릭스

공직자의 질문 유형에 따라 검색 우선순위가 달라집니다.

질문 유형	1 순위	2 순위	3 순위
법령형	국가법령정보센터	자치법규정보시스템	행정규칙·지침
통계형	KOSIS	공공데이터포털	지자체 공식 통계
정책형	타 지자체 사례	연구보고서	해외 사례 기사
민원형	내부 FAQ/회신사례	관련 법령/조례	누리집 공지
사업·조달형	나라장터	공고문	관련 지침
언론 동향형	국내 언론	해외 언론	연구기관 분석

검색은 1 순위부터 순차 실행하며, 성공 시점에 즉시 중단합니다. 검색 결과는 메타데이터 필터링(출처 신뢰도, 최신성, 적용 범위)으로 재정렬합니다.

부록 4. 대표 에이전트별 입력·출력 구조 예시

1. 아이디어 도출 에이전트

- 입력: 주제, 대상 주민, 지역 특성, 예산 범위, 추진 기간
- 출력: 아이디어 카드(제목, 핵심 내용, 기대효과, 예산 수준, 참고 사례)

2. 정책 기획 에이전트

- 입력: 정책 과제명, 대상 주민, 예산 범위, 추진 기간, 제약조건
- 출력: 정책기획서 초안(HWP/DOCX) - 추진 배경, 현황 및 문제점, 정책 목표, 추진 전략, 세부 과제, 기대 효과, 법적 근거, 재정 검토

3. 민원 분석 자동화 에이전트

- 입력: 민원 텍스트, 첨부 파일
- 출력: 민원 분석 리포트(민원 요약, 민원 유형, 핵심 요구사항, 관련 근거, 회신 초안, 추가 확인 필요사항)

4. 법령 조회 에이전트

- 입력: 질문 텍스트
- 출력: 법령 검토 리포트(적용 가능 법령, 관련 조문 요지, 관련 조례/지침, 해석상 유의점, 추가 확인 필요사항)

5. 법적 가이드 에이전트

- 입력: 사안 개요
- 출력: 법적 검토 가이드(사안 개요, 관련 법적 쟁점, 적용 가능 법령, 실무상 유의점, 분쟁·감사 리스크, 추가 확인 필요사항)

부록 5. 지자체 도입 체크리스트

1 단계: SaaS 형 AI 비서 도입 (3 개월)

- [] 사업 계획 수립 (파일럿 부서 선정, 예산 확보, 목표 설정)
- [] 제안요청서 작성 또는 조달 계약
- [] 계약 및 계정 발급
- [] 사용자 교육 (2 시간 온라인 + 2 주 실습)
- [] 주간 사용 로그 및 만족도 수집
- [] 3 개월 후 성과 평가 (사용률 30% 이상, 만족도 4.0/5.0 이상)

2 단계: 핵심 에이전트 발굴 (6 개월)

- [] 부서별 워크숍 진행 (5~10 개 에이전트 우선순위 선정)
- [] 실무자 인터뷰 (업무 흐름 수집)
- [] 에이전트 설계 (입력·출력 구조)
- [] 에이전트 배포
- [] 3 개월 활용 로그 분석
- [] 성과 평가 (10 개 중 5 개 이상 주 1 회 이상 사용)

3 단계: 데이터·보안 체계 고도화 (1 년)

- [] AI 데이터 전달 3 대 유형 구현
- [] 티어 1 데이터 14 가지 정의
- [] 검색 API·MCP·메타데이터 RAG 구축
- [] CSO 등급별 보안 체계 구축
- [] 성과 평가 (검색 정확도 85% 이상, 근거 누락률 5% 이하)

4 단계: 전사 통합형 AI 플랫폼 구축 (2 년 차)

- [] 검증된 에이전트 내재화
- [] 내부망·외부망 LLM 하이브리드 운영
- [] 전 부서 확산
- [] 성과 평가 (1 인당 주 5 회 이상 사용, 만족도 4.5/5.0 이상)

부록 6. 사업 제안서 작성 가이드

제안서 필수 항목

15. 사업 개요: 배경, 목적, 필요성
16. 현황 분석: 지자체 AI 도입 현황, 문제점
17. 추진 방안: 4 단계 로드맵, 단계별 추진 내용
18. 기대 효과: 예산 절감, 업무 효율, 주민 만족도 향상
19. 소요 예산: 단계별 예산 산정 근거
20. 추진 일정: 단계별 추진 기간 및 마일스톤
21. 성과지표: 사용률, 정확도, 만족도, 업무 효율
22. 위험 관리: 예상 리스크 및 대응 방안

작성 요령

- 1 단계 SaaS 도입부터 시작하는 단계적 접근 강조
 - 타 지자체 실패 사례(대규모 인프라 우선 구축)와 차별화
 - 구체적 수치 제시 (예산, 인원, 기간, 성과지표)
 - 부록 7~10 의 템플릿 활용
-
-

부록 7. 예산 산정 기준 예시

SaaS 구독료 (1~2 단계)

- 광역자치단체 (공직자 6 천 명): 연간 5 천만~1 억 원
- 기초자치단체 (공직자 500 명): 연간 5 백만~1 천만 원
- 산정 기준: 사용자 수 × 월 구독료

구축형 사업비 (3~4 단계)

- 광역자치단체: 5~10 억 원

- 기초자치단체: 2~5 억 원
- 포함 항목: 데이터 플랫폼, 메타데이터 RAG, LLM 라우팅, 보안 체계, 에이전트 개발

유지보수비 (구축 후 연간)

- 구축비의 10~15%
- 예: 구축비 5 억 원 → 연간 유지보수비 5 천만~7 천 5 백만 원

기타 비용

- 사용자 교육: 1 회당 100~200 만 원
 - 컨설팅: 500 만~1 천만 원
-

부록 8. RFP 필수 항목 체크리스트

기술 요구사항

- [] 멀티 LLM 지원 (3 개 이상 LLM 선택 가능)
- [] CSO 등급별 LLM 라우팅
- [] 메타데이터 RAG 구현
- [] 검색 API·MCP 연동
- [] 개인정보 자동 마스킹
- [] 권한 기반 검색 통제
- [] 감사 로그 기록

기능 요구사항

- [] 5 개 이상 에이전트 제공
- [] 문서 업로드 (hwp, docx, pdf, xlsx 등)
- [] 문서 다운로드 (HWP, Word, PPT)
- [] 출처 명시 기능

- [] 사용 로그 분석

보안 요구사항

- [] 국정원 AI 보안 가이드 2.0 준수
- [] 개인정보 처리 방침 제시
- [] 데이터 암호화 (전송·저장)
- [] 접근 권한 관리
- [] 백업 및 복구 체계

운영 요구사항

- [] 사용자 교육 프로그램
 - [] 기술 지원 체계 (응답 시간 명시)
 - [] 정기 성과 보고
 - [] 오답 개선 체계
-

부록 9. CSO 기반 보안 운영 정책 예시

데이터 등급 분류

- **C 급 (비밀):** 국가안보, 외교, 수사, 개인 민감정보
- 처리 방식: 내부망 LLM 만 사용
- 접근 권한: 권한자만
- 외부 전송: 절대 금지
- **S 급 (대외비):** 내부 검토 문서, 미확정 정책, 계약 협상
- 처리 방식: 내부망 LLM 우선, 필요 시 마스킹 후 외부 LLM
- 접근 권한: 해당 부서만
- 외부 전송: 개인정보 마스킹 필수
- **O 급 (공개):** 법령, 조례, 공공데이터, 보도자료, 공식 통계

- 처리 방식: 외부 고성능 LLM 허용
- 접근 권한: 전체 공직자
- 외부 전송: 제한 없음

권한 관리

- 부서별 문서 접근 제한 (복지과는 복지과 문서만)
- 직급별 검색 범위 제한
- 인사 시스템 연동 자동 업데이트
- 퇴직·전출자 즉시 차단

감사 로그

- 사용자, 시간, 질문, 검색 문서, 사용 LLM, 답변 기록
- 이상 접근 자동 탐지 (대량 다운로드, 권한 밖 문서)
- 로그 보관 기간: 3 년

부록 10. 성과지표 설계 템플릿

지표	정의	측정 방법	목표	평가 주기
사용률	월 활성 사용자 비율	로그 분석	30% 이상	월 1 회
파워유저 비율	주 1 회 이상 사용자	로그 분석	10% 이상	월 1 회
정확도	AI 답변 정확도	사용자 평가	3.5/5.0 이상	월 1 회
업무 효율	작업 시간 단축률	로그+설문	30% 이상	분기 1 회
만족도	전반적 만족도	설문조사	4.0/5.0 이상	월 1 회
오답률	오답 사례 비율	신고 건수	5% 이하	월 1 회

측정 도구

- 사용 로그 자동 수집
- 월 1 회 온라인 설문조사 (5 분 내외)
- 오답 신고 버튼

개선 기준

- 3 개월 연속 목표 미달 시 개선 계획 수립
 - 오답률 20% 이상 시 모델 교체 검토
-

부록 11. 타 지자체 도입 사례 요약

광역자치단체 A

- 생성형 AI 기반 업무 지원 시스템 도입
- 270 종 업무매뉴얼 기반 RAG 구축
- 내부 시스템 연계 추진
- 성과: 문서 작성 지원, 정보 조회 효율화

광역자치단체 B

- 내부망 LLM 4 개 도입
- 외부 검색 미연동으로 만족도 저조
- 개선 방안 모색 중

광역자치단체 C

- 내부망 LLM 성능 저하
- 외부 검색 불가로 활용률 낮음
- 개선 방안 검토 중

기초자치단체 D

- 홈페이지 챗봇 메타데이터 RAG 방식 검토
- 실시간 검색 구조로 유지관리 편의성 목표

공통 시사점

- 외부 검색 연동이 만족도에 결정적
 - 고성능 LLM 활용이 중요
 - SaaS 우선 도입이 위험 최소화
-

부록 12. FAQ: 자주 묻는 질문과 답변

Q1. AI 에이전트 도입에 얼마나 걸리나요?

A. SaaS 방식은 계약 후 1 주일 내 사용 가능. 구축형은 1~2 년 소요.

Q2. 예산은 얼마나 필요한가요?

A. SaaS 는 연간 5 백만~1 억 원, 구축형은 2~10 억 원 (규모별 차이)

Q3. 어떤 부서부터 도입하면 좋나요?

A. 기획, 민원, 법무, 홍보 부서가 효과 큼니다.

Q4. 개인정보 유출 위험은 없나요?

A. CSO 등급별 통제, 자동 마스킹, 권한 관리로 보호합니다.

Q5. 기존 시스템과 연동되나요?

A. MCP 로 서울, 온나라 등 내부 시스템 연동 가능합니다.

Q6. AI 답변이 틀리면 어떻게 하나요?

A. 오답 신고 후 개선 반영. 고위험 업무는 담당자 검토 필수입니다.

Q7. 특정 LLM 에 종속되나요?

A. 멀티 LLM 구조로 언제든지 모델 교체 가능합니다.

Q8. 공직자들이 사용법을 익힐 수 있을까요?

A. 2 시간 교육으로 기본 사용 가능. 부서별 파워유저가 동료 지원합니다.

Q9. 구축 후 유지보수는 어떻게 하나요?

A. 연간 구축비의 10~15% 유지보수비로 시스템 관리, 오답 개선, 모델 업데이트를 진행합니다.

Q10. 다른 지자체 사례를 볼 수 있나요?

A. 부록 11 참조. 추가 문의는 솔루션사업팀으로 연락 바랍니다.