

에이전트가 먼저다

민선 9 기 지방정부를 위한 벤더 중립형 행정 AI

에이전트 허브 전략 백서

핵심 메시지

성과는 에이전트가 만들고, 인프라는 그 에이전트를 뒷받침합니다.

발행: 스캐터엑스(ScatterX)

발행일: 2026 년 9 월

일러두기

이 백서는 두 층위의 독자를 염두에 두고 작성되었습니다.

Part 1 과 Part 2 는 왜 에이전트부터 시작해야 하는지에 대한 전략적 논거를 다룹니다. 지자체장님, 부단체장님, 기획조정실, 예산부서 관계자분들께서 우선 읽어주시면 좋을 부분입니다.

Part 3 부터 Part 6 까지는 에이전트의 구체적 기준, 데이터 처리 방식, 3 단계 도입 로드맵, 현장 운영 방식을 다룹니다. 정보화부서, 보안담당자, 사업 담당 주무관님께서 실무적으로 참고하시면 좋을 부분입니다.

각 Part 서두에는 해당 장을 우선 읽어주시면 좋을 독자를 안내해 두었습니다. 바쁘신 중에도 끝까지 읽어주신다면 더없이 감사하겠습니다.

발간사

성과는 구축이 아니라 사용에서 나옵니다

존경하는 공직자 여러분께 삼가 인사드립니다. 스캐터엑스(ScatterX) 대표이사 강명수입니다.

민선 9기 지방정부에 주어진 실질적인 시간은 4년이 아니라 그 절반에 가깝다고 생각합니다. 임기 전반기 2년 안에 행정 현장에서 체감할 수 있는 성과를 만들어내지 못한다면, 후반기는 새로운 사업을 벌이기보다 다음 선거를 준비하는 시기로 넘어갈 가능성이 큼니다. 인공지능(AI) 도입 역시 예외가 아니라고 조심스럽게 생각합니다. 지금 이 시점에 지방정부가 결정해야 할 것은 어떤 모델을 구축할 것인가가 아니라, 무엇으로 전반기 2년 안에 성과를 낼 것인가라는 질문이라고 믿습니다.

지난 수년간 적지 않은 지방자치단체에서 생성형 AI 행정비서 형태의 서비스를 도입해 주셨습니다. 그 덕분에 공직자 여러분께서는 이미 AI에게 문서 요약을 맡기고, 초안을 부탁하고, 자료를 찾아달라고 요청하는 경험을 쌓아 오셨습니다. 이는 대단히 소중한 자산이라고 생각합니다. 저희는 이 경험 위에 무엇을 더할 것인가가 앞으로 2년의 성패를 가른다고 보고 있습니다.

그런데 최근 현장에서 만나 뵈는 여러 담당자분들께서는 AI 도입을 검토하실 때 종종 대규모 지식그래프나 온톨로지 구축, 혹은 방대한 데이터 통합 플랫폼 구축과 같은 무거운 제안을 먼저 받으시는 경우가 많다고 말씀해 주셨습니다. 저희 스캐터엑스는 이러한 방식이 틀렸다고 감히 단정하지는 않습니다. 다만 지금 공공기관이 보유한 데이터의 정비 수준과 임기 내 성과가 필요한 시간적 제약을 함께 고려할 때, 그러한 접근이 다소 이르거나 무거울 수 있다는 말씀을 조심스럽게 드리고 싶습니다.

저희가 생각하는 순서는 이렇습니다. 먼저 공직자 여러분께서 실제로 매일 마주하시는 업무, 이를테면 민원 답변, 법령 검토, 보고서 작성, 회의록 정리와 같은 업무를 돕는

에이전트를 빠르게 만들어 드리고, 실제로 사용해 보시면서 무엇이 필요한지 함께 확인해 나가는 것입니다. 그 과정에서 어떤 에이전트에는 더 정확한 법령 데이터 연결이 필요하고, 어떤 에이전트에는 내부 행정망의 민감한 자료를 안전하게 다루는 보안 체계가 필요하다는 것이 자연스럽게 드러날 것입니다. 그때 비로소 필요한 만큼의 데이터 연결과 보안 인프라를 갖추어 나가는 것이 순서에 맞는다고 생각합니다.

이러한 이유로 이번 백서의 제목을 「에이전트가 먼저다」로 정하였습니다. 다소 단정적으로 들릴 수 있는 제목이오나, 저희가 드리고 싶은 말씀의 핵심을 가장 정직하게 담은 표현이라 여겨 이렇게 정하였습니다.

이 백서에서 저희는 특정 대규모언어모델(LLM)이나 특정 검색증강생성(RAG) 기술, 특정 데이터 플랫폼을 반드시 도입하셔야 한다고 권하지 않습니다. 오히려 그 반대য়ে 가깝습니다. 지금처럼 기술이 빠르게 변화하는 시기에 특정 기술을 미리 강제하는 방식은 자칫 특정 기업에 종속되는 결과로 이어질 수 있다고 우려합니다. 저희는 지방정부가 어떤 모델이든, 어떤 에이전트든 필요에 따라 안전하게 연결해 사용하실 수 있는 열린 구조를 제안드리고자 합니다.

또한 이러한 전환은 저희가 시스템을 납품해 드리는 것만으로 완성되지 않는다고 생각합니다. 공직자 여러분과 저희 스캐터엑스의 담당 인력이 현장에서 함께 만들고, 써 보고, 고치고, 때로는 과감히 접고, 잘 되는 것은 더 키워 나가는 공동의 과정이 반드시 필요하다고 믿습니다.

부족한 점이 많은 글이오나, 이 백서가 공직자 여러분의 소중한 시간을 헛되이 하지 않고 작으나마 현실적인 참고가 되기를 진심으로 바랍니다. 끝까지 읽어주셔서 미리 감사드립니다.

스캐터엑스 대표이사 강명수 올림

(핵심 메시지 재확인: 성과는 에이전트가 만들고, 인프라는 그 에이전트를 뒷받침합니다.)

Executive Summary — 의사결정자를 위한 8 개

메시지 요약

바쁘신 의사결정자 여러분을 위하여, 이 백서 전체의 핵심 내용을 8 개 문장으로 먼저 요약해 드립니다.

1. 민선 9 기 지방정부의 AI 성과는 임기 전반기 2 년 안에 나타나야 실효성이 있습니다.
2. 그 성과는 LLM 이나 데이터 플랫폼을 구축하는 것 자체에서 나오지 않으며, 공직자 여러분께서 실제로 사용하시는 에이전트에서 나온다고 판단합니다.
3. 구축형 시스템인지 SaaS 인지, 어떤 LLM 을 쓰는지, 어떤 RAG 기술을 쓰는지는 목적이 아니라 수단에 가깝습니다.
4. 특정 기업의 기술에 종속되지 않으시려면, 처음부터 여러 모델과 에이전트를 자유롭게 연결할 수 있는 벤더 중립형 구조로 설계하시는 편이 안전하다고 생각합니다.
5. 공직자용 에이전트는 AI 가 스스로 알아서 판단하는 자율적인 도구가 아니라, 공직자 여러분의 업무 처리 절차를 충실히 따르면서 깊이 있게 검토하는 도구여야 한다고 믿습니다.
6. 데이터는 그 성격에 따라 서로 다르게 다루어야 하며, 법령·지침처럼 이미 정리된 근거 데이터는 실시간으로 연결하고, 행정 운영 데이터는 정제하며, 현장·센서 데이터는 맥락을 더해 설명해야 한다고 생각합니다.
7. 이 백서에서 제시하는 1 단계부터 3 단계까지의 도입 로드맵은 미리 정해진 인프라 구축 일정표가 아니라, 실제로 효과가 검증된 에이전트가 필요로 하는 데이터와 보안 수준에 따라 자연스럽게 뒤따르는 결과라고 이해해 주시면 감사하겠습니다.
8. 이러한 전환은 시스템 납품만으로는 이루어지기 어려우며, 현장에 함께하는 인력과 지자체 공직자 여러분의 공동 운영을 통해서만 완성될 수 있다고 생각합니다.

Part 1. 왜 지금 에이전트부터 시작해야 하는가

(이 장은 지자체장님, 부단체장님, 기획조정실, 예산부서 관계자분들께서 우선 읽어주시면 감사하겠습니다.)

1.1. 민선 9 기 시간표와 AI 성과 압박

민선 9 기 지방정부는 2026 년 7 월 1 일 출범하였습니다. 이제 막 임기를 시작하신 단체장님들께서는 공약을 구체적인 사업으로 옮기는 일에 매진하고 계시리라 짐작됩니다. 실제로 화성특례시의 경우 출범과 함께 AI 전략과를 신설하고 78 개에 이르는 세부 사업을 추진하는 등, 여러 지자체에서 AI 를 핵심 시정 방향으로 삼는 움직임이 이미 본격화되고 있는 것으로 보입니다.

다만 이 시점에서 한 가지 조심스러운 말씀을 드리고 싶습니다. 지방정부의 임기는 4 년이지만, 실질적으로 새로운 사업의 성과를 주민들과 의회에 보여드릴 수 있는 시간은 그보다 훨씬 짧다는 점입니다. 통상적으로 임기 1 년 차는 조직을 정비하고 예산 편성 체계를 갖추는 데 상당한 시간이 소요됩니다. 2 년 차부터는 본격적인 사업 집행과 함께 가시적인 성과가 요구되기 시작합니다. 3 년 차에 접어들면 이미 다음 선거를 의식한 성과 정리와 홍보가 시작되며, 4 년 차는 사실상 선거 국면으로 접어들어 대규모 신규 사업을 추진하기 어려운 시기가 됩니다.

이러한 시간표를 고려하면, 민선 9 기 지방정부에게 주어진 실질적인 AI 사업 추진 기간은 전반기 2 년, 즉 2026 년 하반기부터 2028 년까지라고 보는 것이 현실적이라고 생각합니다. 이 2 년 안에 공직자 여러분과 주민 여러분께서 체감하실 수 있는 성과를 만들어내지 못한다면, 후반기에는 관련 예산과 조직의 동력을 유지하기가 쉽지 않을 것으로 우려됩니다. 반대로 전반기 2 년 안에 분명한 성과를 보여드릴 수 있다면, 후반기 2 년은 그 성과를 다음 임기까지 이어가는 발판이 될 수 있을 것입니다.

바로 이 지점에서 AI 사업의 추진 방식에 대한 근본적인 고민이 필요하다고 생각합니다. 만약 첫해를 데이터 표준화와 시스템 설계에, 둘째 해를 인프라 구축에, 셋째 해를 시험 운영에 사용한다면, 정작 성과를 보여드려야 할 시점에는 아직 아무것도 실제로

사용되지 못하는 상황에 이를 수 있습니다. 저희 스캐터엑스는 이러한 우려를 여러 현장에서 직접 듣고 있습니다.

1.2. 기존 접근의 한계

지금까지 공공부문에 제안되어 온 AI 도입 방식에는, 저희가 감히 몇 가지 아쉬운 점이 있다고 조심스럽게 말씀드리고자 합니다.

첫째, 특정 대규모언어모델(LLM)이나 특정 검색증강생성(RAG) 기술, 특정 임베딩 모델, 전용 데이터 플랫폼을 처음부터 함께 도입하도록 안내드리는 방식입니다. 이러한 방식은 도입 초기에는 편리해 보일 수 있으나, 이후 더 뛰어난 모델이나 기술이 등장하더라도 기존 체계를 바꾸기 어려운 구조로 이어질 우려가 있습니다. 인공지능 기술은 최근 수년간 매우 빠르게 발전해 왔고, 앞으로도 그러할 것으로 예상됩니다. 특정 기업의 기술 체계에 처음부터 깊이 결합되는 방식은, 장기적으로 지방정부의 선택권을 제한하는 결과로 이어질 수 있다고 생각합니다.

둘째, 대규모 데이터 통합 플랫폼을 먼저 구축하려는 접근입니다. 여러 부서의 데이터를 한곳에 모으는 작업은 상당한 시간과 예산이 소요될 뿐 아니라, 완성되었을 때는 이미 최신 정보가 아닐 위험도 있습니다. 아울러 민감한 행정 정보를 별도의 저장소에 복제하는 과정에서 보안 관리의 책임 소재가 늘어나는 측면도 있습니다. 저희는 이러한 방식이 잘못되었다고 단정하지 않습니다. 다만 모든 데이터를 처음부터 한곳에 모아야만 AI를 활용할 수 있는 것은 아니라는 점을 말씀드리고 싶습니다.

셋째, 지식그래프나 온톨로지와 같은 정교한 개념 체계를 처음부터 설계하려는 접근입니다. 이러한 기술 자체는 학술적으로 훌륭하다고 생각합니다. 그러나 아직 공공기관의 데이터 상당수가 담당자 개인의 문서함에 비정형 형태로 흩어져 있는 현재 상황에서, 정교한 개념 체계부터 설계하는 방식은 적지 않은 예산과 시간을 필요로 합니다. 2023 년을 전후하여 널리 제안되었던 이러한 접근 방식들이, 지금의 에이전트 중심 기술 환경과 임기 2 년이라는 시간적 제약 속에서는 다소 무겁게 느껴질 수 있다고 조심스럽게 생각합니다.

1.3. 성과의 단위는 "구축 완료"가 아니라 "사용 중인 에이전트"입니다

저희가 가장 강조하여 말씀드리고 싶은 부분이 바로 이것입니다. AI 사업의 성과는 시스템 구축이 완료되었다는 보고서로 증명되지 않습니다. 실제로 공직자 여러분께서 매일 사용하고 계신지, 그로 인해 업무 시간이 줄었는지, 민원 답변의 품질이 나아졌는지로 증명된다고 생각합니다.

시범 사업, 즉 개념검증(PoC) 단계에서 좋은 결과를 보였다는 것과, 실제 업무 현장에서 꾸준히 사용되고 있다는 것은 전혀 다른 이야기입니다. 여러 공공기관에서 진행된 AI 시범 사업들이 보고서로는 성공적이었으나, 실제 업무에 정착하지 못한 사례를 저희도 여러 차례 접한 바 있습니다. 그 원인은 대체로 기술의 부족함보다는, 실제 업무 절차와 맞지 않았거나 현장의 피드백을 반영해 개선해 나갈 체계가 없었기 때문이었습니다.

그러므로 저희는 이번 백서를 통해 성과의 단위를 새롭게 제안드리고자 합니다. "몇 개의 시스템을 구축하였는가"가 아니라 "몇 개의 부서에서, 몇 명의 공직자께서, 어떤 업무에, 얼마나 자주 에이전트를 사용하고 계신가"를 성과의 기준으로 삼아야 한다고 생각합니다. 아울러 업무 시간이 얼마나 줄었는지, 민원 처리 과정에서 근거 누락이 얼마나 줄었는지, 반복되는 문의가 얼마나 감소하였는지와 같은 구체적인 지표로 성과를 확인해야 한다고 믿습니다.

이러한 이유로 저희는 이 백서의 제목을 「에이전트가 먼저다」로 정하였습니다. 무엇을 구축할 것인가를 먼저 정하지 마시고, 어떤 업무를 도와드릴 에이전트가 필요한지를 먼저 정하시기를 조심스럽게 제안드립니다. 그 에이전트가 실제로 사용되면서 어떤 데이터와 어떤 보안 체계가 더 필요한지가 자연스럽게 드러날 것이며, 그때 필요한 만큼의 기반을 갖추어 나가는 것이 임기 2 년이라는 시간 안에서 가장 현실적인 길이라고 생각합니다.

Part 2. 에이전트 퍼스트 전략과 공직자용 에이전트의 본질

(이 장은 의사결정자분들과 실무 담당자분들께서 함께 읽어주시면 좋은 내용입니다.)

2.1. 에이전트가 인프라 요구사항을 결정합니다

Part 1 에서 저희는 성과의 단위가 "구축 완료"가 아니라 "사용 중인 에이전트"여야 한다는 말씀을 드렸습니다. 그렇다면 실제로 무엇을 먼저 정하고, 무엇을 나중에 갖추어야 할지에 대해 조금 더 구체적으로 말씀드리고자 합니다.

저희가 제안드리는 순서는 다음과 같습니다.

먼저 어떤 업무에서 성과를 만들고자 하시는지를 정하시는 것이 출발점이라고 생각합니다. 예를 들어 "민원 답변 초안 작성에 드는 시간을 줄이겠다", "법령 검토 시 근거 누락을 줄이겠다"와 같이 구체적인 업무 성과를 먼저 정하시는 것입니다.

그다음으로, 그 성과를 만들어 낼 에이전트를 선정하시는 것이 두 번째 단계입니다. 이 에이전트가 어떤 절차로 업무를 도와드릴지, 어떤 결과물을 만들어 드릴지를 구체화하는 과정입니다.

세 번째로, 그 에이전트를 실제로 운영해 보면서 어떤 데이터가 필요한지, 그 데이터의 보안 등급은 어느 정도인지를 확인하시는 것입니다. 이 단계에 이르러야 비로소 "이 업무에는 최신 조례 데이터 연결이 필요하다", "이 업무에는 개인정보가 포함된 내부 자료를 다루어야 한다"는 것이 분명해집니다.

그리고 마지막으로, 그때 확인된 필요에 맞추어 필요한 만큼의 데이터 연결 방식과 보안 인프라를 갖추어 나가시는 것이 순서에 맞다고 생각합니다.

이 순서를 거꾸로 하시면, 즉 어떤 데이터가 필요할지 다 알 수 없는 상태에서 처음부터 모든 데이터를 모으는 대규모 플랫폼을 먼저 구축하려 하시면, 정작 그 플랫폼이 실제로 어떤 업무에 쓰일지 늦게 드러나는 경우가 많습니다. 저희는 이러한 순서의 역전이

그동안 여러 공공 AI 사업에서 성과가 늦어졌던 원인 중 하나라고 조심스럽게 생각합니다.

다시 말씀드리면, 인프라가 에이전트를 낳는 것이 아니라, 에이전트의 실제 필요가 인프라의 범위를 결정한다고 말씀드릴 수 있습니다. 이 원칙은 이후 Part 5 에서 말씀드릴 3 단계 도입 로드맵에서도 동일하게 적용됩니다. 그 로드맵은 미리 정해진 인프라 구축 일정표가 아니라, 먼저 적용해 본 에이전트가 요구하는 데이터와 보안 수준에 따라 자연스럽게 다음 단계의 필요성이 드러나는 과정임을 다시 한번 말씀드리고 싶습니다.

2.2. 공직자용 에이전트는 자유방임형 AI 가 아닙니다

이 백서에서 가장 오해받기 쉬운 표현이 "에이전트"라는 단어라고 생각합니다. 최근 언론과 여러 자료에서 소개되는 에이전트는 스스로 목표를 세우고, 스스로 판단하여, 스스로 시스템을 조작하는 자율적인 AI 로 그려지는 경우가 많습니다. 실제로 연합뉴스가 2026 년 7 월 보도한 내용에 따르면, 사이버보안 기업 소프트캠프의 배한국 대표는 AI 에이전트가 업무 시스템에 직접 접속하여 데이터를 읽고 쓰는 환경이 확산하면서, 보안의 초점이 차단에서 권한 관리로 옮겨가고 있다고 진단한 바 있습니다.

저희 스캐터엑스는 공직자 여러분께서 사용하실 에이전트가 이러한 방식으로 설계되어서는 안 된다고 분명히 말씀드리고 싶습니다. 행정 업무는 법령, 조례, 지침, 사무분장, 처리 기한, 그리고 감사 가능성이라는 명확한 절차와 책임 구조 안에서 이루어집니다. 공직자 여러분께서 어떤 민원을 처리하실 때, 머릿속으로 자유롭게 아무 생각이나 떠올리시는 것이 아니라, 관련 법령을 확인하시고, 유사한 선례를 찾아보시고, 담당 부서를 확인하시고, 기준일을 대조하시는 일정한 절차를 따르시는 것과 마찬가지로입니다.

그러므로 저희가 말씀드리는 공직자용 에이전트는, 공직자 여러분께서 실제로 밟으시는 이러한 업무 절차를 업무별로 충실히 옮겨 담은 체계에 가깝습니다. 예를 들어 민원 답변을 돕는 에이전트라면 다음과 같은 단계를 따르도록 설계하는 것이 바람직하다고 생각합니다.

먼저 민원의 요지를 파악하고, 개인정보가 포함되어 있는지 확인합니다. 다음으로 민원의 유형을 분류하고, 담당 부서의 후보를 확인합니다. 그다음으로 관련 법령과 조례를 검색하고, 내부 업무 매뉴얼을 확인합니다. 이어서 과거에 유사한 민원에 어떻게 답변하였는지 확인하고, 현재 시행 중인 기준이 맞는지 대조합니다. 마지막으로 답변이 가능한 범위와 추가로 확인이 필요한 사항을 구분하여 초안을 작성하고, 근거가 된 조항과 출처를 함께 표시합니다.

이처럼 각 단계에서 어떤 자료를 확인해야 하는지를 미리 지정해 드리는 것이 에이전트 설계의 핵심이라고 생각합니다. 이러한 지정 없이 AI 에게 그저 "민원에 답변해 줘"라고만 요청드리면, AI 는 그럴듯하지만 근거가 부족한 문장을 만들어 낼 위험이 있습니다. 반대로 업무 단계와 필요한 자료를 명확히 지정해 드리면, AI 는 공직자 여러분의 사고 과정을 충실히 따라가면서 답변을 만들어 낼 수 있습니다.

2.3. 추론은 충분하게, 접근과 실행은 통제해야 합니다

여기서 한 가지 중요한 구분을 말씀드리고자 합니다. 바로 "얼마나 깊이 생각하게 할 것인가"와 "무엇을 하도록 허락할 것인가"는 서로 다른 문제라는 점입니다.

먼저 얼마나 깊이 생각하게 할 것인가에 대해 말씀드리겠습니다. 법령 간 충돌 여부를 검토하는 업무, 인허가 신청 서류를 사전 검토하는 업무, 감사 지적 사항에 소명하는 업무와 같이 행정적 책임이 무거운 업무일수록, 에이전트가 더 많은 단계를 거쳐 더 깊이 검토하도록 허용해 드려야 한다고 생각합니다. 만약 비용을 절감하기 위해 에이전트가 검토할 수 있는 문서의 수나 검토 단계의 횟수를 지나치게 제한하신다면, 예외 조항을 놓치거나, 최신 개정 사항을 반영하지 못하거나, 반대되는 선례를 확인하지 못하는 위험이 커질 수 있습니다. 그러므로 저희는 고위험 업무일수록 오히려 더 성능이 뛰어난 모델과 더 충분한 검토 과정을 허용해 드리는 것이 바람직하다고 생각합니다.

다음으로 무엇을 하도록 허락할 것인가에 대해 말씀드리겠습니다. 이는 앞서 말씀드린 깊이 있는 생각과는 전혀 다른 차원의 문제입니다. 그리드지(Gridge)의 사내 AI 에이전트 도입 가이드에 따르면, AI 에이전트의 권한은 읽기, 작성, 삭제, 외부 전송, 결제, 권한 변경과 같이 항목별로 나누어 설계해야 하며, 각 권한의 기본값은 업무 수행에 필요한 최소한으로 제한하는 것이 원칙이라고 설명하고 있습니다. 아울러 되돌리기

어렵거나 금전 또는 개인정보에 영향을 주는 작업에는 반드시 사람의 승인과 감사 기록이 뒤따라야 한다고 강조하고 있습니다.

저희는 이 원칙이 공직자용 에이전트에도 그대로 적용되어야 한다고 생각합니다. 다만 공공 행정의 특성상 조금 더 세심하게 나누어 말씀드리고자 합니다.

에이전트가 자유롭게 수행해도 무리가 없다고 생각되는 일은 다음과 같습니다. 관련 법령과 조례를 검색하는 일, 과거 자료를 조회하고 비교하는 일, 문서를 요약하는 일, 초안을 작성하는 일, 검토 의견의 근거를 정리하는 일입니다.

반면 반드시 공직자 여러분의 확인과 승인을 거친 뒤에만 이루어져야 한다고 생각하는 일은 다음과 같습니다. 민원을 최종적으로 발송하는 일, 인허가의 허가 또는 불허를 결정하는 일, 예산을 집행하는 일, 내부 시스템에 결재를 올리는 일, 시스템의 자료를 직접 수정하는 일입니다.

정리하여 말씀드리면, 에이전트가 생각하고 검토하는 과정은 가능한 한 충분하고 깊이 있게 이루어지도록 허용해 드리되, 에이전트가 실제로 무엇을 실행할 수 있는지는 엄격하게 제한하고, 되돌리기 어려운 일일수록 공직자 여러분의 승인을 거치도록 설계해야 한다는 것입니다. 이 원칙을 한 문장으로 표현한다면 다음과 같습니다.

추론은 충분하게, 데이터 접근은 권한에 맞게, 실행은 승인 기반으로.

이 원칙은 이어지는 Part 3 에서 말씀드릴 공직자용 에이전트의 구체적인 기준, 그리고 Part 5 에서 말씀드릴 단계별 도입 로드맵 전반에 걸쳐 일관되게 적용되는 저희 스캐터엑스의 핵심 설계 철학임을 다시 한번 말씀드리고 싶습니다.

Part 3. 벤더 중립형 행정 AI 에이전트 허브

(이 장은 정보화부서, 보안담당자, 사업 담당 주무관님께서 실무적으로 참고해 주시면 좋을 내용입니다.)

3.1. 플랫폼의 본질은 소유가 아니라 연결에 있습니다

Part 1 과 Part 2 에서 저희는 에이전트를 먼저 정하고, 그 에이전트가 요구하는 만큼만 인프라를 갖추어 나가야 한다는 말씀을 드렸습니다. 이 원칙을 실제 플랫폼 구조로 옮기면 어떤 모습이 되어야 할지, 이번 장에서 조금 더 구체적으로 말씀드리고자 합니다.

저희 스캐터엑스가 제안드리는 플랫폼의 첫 번째 원칙은, 플랫폼의 가치가 무엇을 소유하고 있는가가 아니라 무엇을 안전하게 연결할 수 있는가에 있다는 것입니다. 지방정부가 굳이 모든 에이전트를 자체적으로 만들어야 할 필요는 없다고 생각합니다. 이미 좋은 기술을 보유한 기업이 적지 않고, 정부 차원에서도 관련 기반이 빠르게 마련되고 있기 때문입니다.

실제로 연합뉴스가 2026 년 6 월 24 일 보도한 내용에 따르면, 한국지능정보사회진흥원(NIA)은 같은 날 경기 고양시 킨텍스에서 열린 '2026 공공 AI 박람회' 부대행사로 '공공부문 AI 도입·활용 가이드 설명회'를 열고 범정부 AI 공통기반의 운영 현황과 활용법을 안내하였습니다. 이 공통기반을 이용하면 중앙부처와 지방자치단체가 GPU 서버를 별도로 구매하거나 임차하지 않고도 클라우드 방식으로 AI 모델과 개발 도구를 바로 사용할 수 있다고 전해집니다.

또한 보안뉴스가 보도한 내용에 따르면, 과학기술정보통신부와 행정안전부는 2025 년 11 월 24 일부터 '범정부 AI 공통기반' 서비스를 본격 개시하였으며, 이를 통해 그동안 보안 우려로 인터넷망에서만 사용할 수 있었던 민간 AI 기술을 정부 내부망에서도 안전하게 활용할 수 있게 되었다고 합니다. 디지털데일리 보도에 따르면 이 공통기반은 국가정보자원관리원 대구센터의 폐쇄형 환경에 구축되어 있으며, 한글에 특화된 중소형 언어모델과 7 종의 검색증강생성(RAG) API 를 서비스 형태로 각 부처와 지자체에 제공하고 있습니다. 아울러 지디넷코리아 보도에 따르면 정부는 여기서 한 걸음 더 나아가, 공무원 업무를 직접 지원하는 AI 에이전트 기능을 확대하고 최신 민간 AI 모델과 외부 데이터를 보다 유연하게 연동할 수 있는 체계로 확장할 계획이라고 전해집니다.

이러한 흐름은 저희가 이 백서에서 제안드리는 방향과 맥락을 같이 한다고 생각합니다. 지방정부의 AI 플랫폼은 어느 한 기업의 기술만으로 채워지는 닫힌 공간이 아니라,

범정부 AI 공통기반, 민간 AI 기업의 우수한 에이전트, 그리고 지자체 자체적으로 만든 에이전트가 함께 놓이는 열린 공간이어야 한다고 생각합니다.

이를 위해 저희가 제안드리는 구조는 두 가지입니다.

첫째는 공직자 여러분께서 매일 접속하시는 통합 업무화면입니다. 이 화면에서는 여러 에이전트가 마치 하나의 서비스처럼 자연스럽게 이용되어야 하며, 공직자 여러분께서 어느 기업의 기술인지를 일일이 신경 쓰지 않으셔도 되도록 설계하는 것이 바람직하다고 생각합니다.

둘째는 에이전트 카탈로그입니다. 이 카탈로그에는 스캐터엑스가 직접 만든 에이전트, 범정부 AI 공통기반에서 제공하는 에이전트, 다른 민간 기업이 만든 우수한 에이전트, 그리고 이웃한 다른 지자체가 먼저 만들어 검증한 에이전트가 함께 등록될 수 있습니다. 공직자 여러분께서는 이 카탈로그에서 필요한 에이전트를 부서와 업무에 맞게 선택하여 사용하시면 됩니다.

이렇게 설계하면 지방정부는 특정 기업의 기술에 얽매이지 않으면서도, 계속하여 등장하는 좋은 기술을 그때그때 안전하게 받아들이실 수 있습니다.

3.2. Secure Router: 통제의 실제 위치

여러 기업의 에이전트와 여러 종류의 인공지능 모델을 한곳에서 사용하시게 되면, 자연스럽게 "이 요청은 어디로 보내야 안전한가"라는 질문이 생기게 됩니다. 저희는 이 질문에 답하는 장치를 시큐어 라우터(Secure Router)라고 부르고 있습니다.

시큐어 라우터의 역할은 공직자 여러분의 질의를 받는 즉시 곧바로 어떤 모델에 전달하는 것이 아니라, 다음의 사항을 먼저 확인하는 것입니다.

먼저 질의를 요청하신 분이 어느 부서, 어떤 직무의 공직자이신지를 확인합니다. 다음으로 이 업무가 어떤 유형에 속하는지, 예를 들어 단순 문서 작성인지, 법령 검토인지, 개인정보가 포함될 가능성이 있는 민원 처리인지를 판단합니다. 이어서 함께 입력된 자료에 개인정보나 비공개 자료가 포함되어 있는지를 확인합니다. 이러한 확인을 거친 뒤에야 비로소 이 요청을 어느 처리 경로로 보낼지를 결정합니다.

처리 경로는 크게 다음과 같이 나뉠 수 있다고 생각합니다.

공개 자료를 다루는 단순한 업무는 서비스형(SaaS) 상용 AI 로 보내어 빠르게 처리할 수 있습니다. 법령이나 조례처럼 공식 근거가 필요한 업무는 범정부 AI 공통기반의 검색증강생성 기능과 연계하여 처리할 수 있습니다. 개인정보나 내부 비공개 자료가 포함된 업무는 반드시 내부망에 설치된 언어모델로 처리하도록 하여, 외부로 자료가 나가지 않도록 해야 합니다. 그리고 법령 간 충돌 검토나 복합적인 정책 검토와 같이 매우 높은 수준의 추론이 필요한 업무는, 자료를 안전하게 비식별화한 뒤 성능이 뛰어난 해외 언어모델의 추론 능력을 빌려 오는 방식도 고려할 수 있습니다.

이렇게 경로가 나뉜 뒤에는 반드시 처리 과정을 기록으로 남겨야 합니다. 누가, 언제, 어떤 업무로, 어떤 자료를 근거로, 어느 모델을 거쳐, 어떤 결과를 받으셨는지가 감사 기록으로 남아야 한다고 생각합니다. 이 기록은 나중에 감사나 민원 이의 제기 상황에서 행정 처리의 적법성을 소명하는 중요한 자료가 될 것입니다.

정리하여 말씀드리면, 시큐어 라우터는 여러 모델과 여러 에이전트를 자유롭게 사용하시면서도, 실제 통제는 한곳에서 일관되게 이루어지도록 하는 장치입니다. 이 장치가 있어야 비로소 "벤더 중립형"이라는 개방성과 "보안"이라는 안전성이 함께 지켜질 수 있다고 생각합니다.

3.3. 공직자용 에이전트가 갖추어야 할 열 가지 기준

지금까지 말씀드린 원칙들을 바탕으로, 저희는 공직자용 에이전트가 최소한으로 갖추어야 할 열 가지 기준을 정리해 보았습니다. 이 기준은 스캐터엑스가 자체적으로 만드는 에이전트뿐 아니라, 앞서 말씀드린 에이전트 카탈로그에 등록되는 모든 외부 에이전트에도 동일하게 적용하고자 하는 원칙입니다.

순번	기준	내용
1	보안 등급 판단	질의와 자료의 보안 등급, 사용자의 권한을 답변 생성에 앞서 먼저 확인함
2	공식 근거 기반	모델의 기억에 의존하지 않고 법령, 조례, 지침 등

		공식 자료를 근거로 답변함
3	시점 구분	시행일, 개정일, 폐지일을 인식하여 현재 기준과 과거 기준을 구분함
4	하이브리드 검색	의미 기반 검색과 정확한 단어·조항 검색을 함께 사용하여 정확도를 높임
5	데이터 출처 기록	답변의 근거가 된 문서의 출처, 작성 부서, 작성일을 함께 표시함
6	질의 명확화	기준일이나 지역, 목적이 불분명할 경우 짐작하여 답하지 않고 다시 확인을 요청함
7	자체 검증	답변을 생성한 뒤 근거의 충분성과 최신성을 스스로 점검하고, 근거가 부족하면 답변을 보류함
8	제한된 권한	검색, 요약, 비교, 초안 작성까지만 수행하며 시스템에 직접 반영하지 않음
9	사람의 최종 승인	민원 발송, 처분 결정, 결재 상신과 같은 행위는 반드시 담당 공직자의 승인을 거침
10	감사 기록	질의 내용, 참고한 자료, 사용된 모델, 처리 시각을 감사 기록으로 남김

이 열 가지 기준 가운데 어느 하나라도 충족하지 못하는 에이전트는, 아무리 답변이 유창하고 그럴듯하더라도 공직자 여러분께서 사용하시기에 적합하지 않다고 저희는 판단합니다. 반대로 이 기준을 충족하는 에이전트라면, 그것을 만든 곳이 저희 스캐터엑스이든, 범정부 AI 공통기반이든, 다른 민간 기업이든 관계없이 함께 사용하실 수 있어야 한다고 생각합니다.

이 기준은 다음 장에서 말씀드릴 데이터 처리 방식, 그리고 이어지는 3 단계 도입 로드맵 전반에 걸쳐 반복하여 적용되는 저희 스캐터엑스의 공통 원칙임을 말씀드립니다.

Part 4. 데이터 전략: 연결·정제·맥락화

(이 장은 정보화부서, 보안담당자, 사업 담당 주무관님께서 실무적으로 참고해 주시면 좋을 내용입니다.)

4.1. 데이터 플랫폼을 무조건 만들지는 않습니다

앞선 장에서 저희는 에이전트가 실제로 필요로 하는 만큼만 데이터 기반을 갖추어 나가야 한다고 말씀드렸습니다. 이번 장에서는 그 원칙을 조금 더 구체적으로, 공공 데이터의 성격별로 나누어 말씀드리고자 합니다.

저희는 지방정부가 보유하고 계신 데이터를 크게 세 가지 층위로 나누어 이해하는 것이 유용하다고 생각합니다.

첫 번째 층위는 법률, 시행령, 조례, 지침, 고시와 같이 행정 행위의 근거가 되는 제도·근거 데이터입니다. 두 번째 층위는 민원 접수, 인허가 처리, 예산 집행, 계약 관리와 같이 업무 시스템 안에서 만들어지는 행정 운영 데이터입니다. 세 번째 층위는 상수도 수압, 도로 상태, 대기질, 재난 신고와 같이 현장의 설비와 센서에서 발생하는 데이터입니다.

이 세 층위는 성격이 서로 다르기 때문에, 저희는 하나의 방식으로 모두를 다루려 하지 않으시기를 조심스럽게 권해 드립니다. 제도·근거 데이터는 이미 국가법령정보센터나 자치법규정보시스템처럼 공신력 있는 원천이 존재합니다. 이런 데이터까지 별도의 창고에 다시 옮겨 담으려 하시면, 오히려 최신성이 떨어지고 관리 부담만 늘어날 수 있습니다. 반면 행정 운영 데이터는 부서별 시스템에 흩어져 있고 형식도 제각각이어서, 정제하는 작업이 반드시 필요합니다. 그리고 현장·센서 데이터는 숫자만으로는 의미를 알기 어려워, 별도의 설명이 더해져야 비로소 행정적으로 쓸모가 있습니다.

그러므로 저희는 "데이터 플랫폼을 만들 것인가 말 것인가"라는 이분법 대신, "이 데이터는 연결해야 하는가, 정제해야 하는가, 맥락을 더해야 하는가"를 먼저 여쭙는 것이 옳다고 생각합니다.

4.2. 찾아야 하는 데이터 — MCP 와 메타데이터 검색증강생성

법령, 조례, 지침처럼 이미 공식적인 원천이 있는 데이터는, 별도로 모아두지 않으시고 필요한 순간에 정확히 찾아오시는 방식이 더 안전하다고 생각합니다. 이때 활용할 수 있는 기술이 모델맥락프로토콜(MCP, Model Context Protocol)입니다.

MCP 는 인공지능이 여러 시스템의 데이터와 기능을 표준화된 방식으로 호출할 수 있도록 하는 기술입니다. 이미 여러 공공기관에서 이러한 방식을 실제로 도입하고 있습니다. 한국지방정부신문 보도에 따르면 서울특별시는 2026 년 7 월 14 일 '서울 실시간 도시데이터 MCP' 시범 서비스를 공개하며 공공데이터 분야 최초로 MCP 서비스를 도입하였습니다. 오세훈 서울시장은 이를 두고 AI 가 인터넷의 일반 정보가 아니라 서울시의 실시간 공공데이터를 기반으로 답변하도록 하여 정확성과 신뢰성을 높이려는 것이라고 밝힌 것으로 전해집니다. 또한 아이데일리뉴스 보도에 따르면 한국산업인력공단은 2026 년 8 월 국가자격시험, 해외취업, 국가직무능력표준 관련 공공데이터를 생성형 AI 가 직접 호출할 수 있도록 하는 'HRDKorea MCP' 서비스를 가동하였으며, 개방된 229 개 오픈 API 가운데 핵심 60 여 개를 MCP 방식으로 전환하여 24 시간 서비스하고 있다고 합니다.

이러한 사례들은 저희가 이 백서에서 말씀드리는 방향, 즉 데이터를 옮겨 담기보다 있는 곳에서 실시간으로 불러오는 방식이 이미 여러 공공기관에서 현실화되고 있음을 보여준다고 생각합니다.

다만 아직 모든 데이터가 MCP 나 오픈 API 형태로 준비되어 있지는 않습니다. 지자체 홈페이지의 안내문이나 소규모 기관의 고시문처럼 API 가 갖추어지지 않은 자료도 많습니다. 이런 경우에는 저희가 메타데이터 검색증강생성이라고 부르는 방식을 제안드립니다. 이는 홈페이지의 메뉴 구조나 법령 사이트의 분류 체계를 그대로 활용하면서, 문서마다 발행 기관, 담당 부서, 시행일, 문서 유형과 같은 정보를 함께 저장해 두는 방식입니다. 이렇게 해두면 검색 시점에 이러한 정보를 기준으로 먼저

범위를 좁힌 뒤 검색할 수 있어, 이미 폐지된 지침이나 관련 없는 부서의 자료가 답변에 섞여 들어가는 것을 상당 부분 막을 수 있습니다.

아울러 저희는 이러한 자료의 변경 여부를 주기적으로 확인하는 별도의 점검 기능을 함께 두시기를 권해 드립니다. 법령이나 조례가 개정되면 그 사실이 가능한 한 빨리 반영되어야 하기 때문입니다. 그리고 답변을 생성할 때에는 "현재 기준"과 "질의하신 시점 당시의 기준"을 구분하여 안내해 드리는 기능도 함께 갖추어야 한다고 생각합니다. 예를 들어 2024 년에 체결된 계약에 관하여 여쭙신다면, 지금 시행 중인 규정이 아니라 당시 유효했던 규정을 기준으로 답변드려야 행정적으로 올바르기 때문입니다.

4.3. 만들어야 하는 데이터 — 목적에 맞게 정제된 행정 운영 데이터

법령이나 조례와 달리, 민원 접수 이력, 인허가 처리 내역, 예산 집행 내역, 계약 관리 자료와 같은 행정 운영 데이터는 사정이 다릅니다. 이러한 데이터는 이미 지자체 내부에 존재하지만, 그 자체로는 AI 가 바로 활용하기 어려운 경우가 많습니다.

예를 들어 조직 개편으로 부서 이름이 바뀌었는데 옛 명칭이 자료에 그대로 남아 있거나, 같은 사업인데 부서마다 사업명을 조금씩 다르게 입력해 두었거나, 같은 항목인데 시스템마다 코드 체계가 달라 서로 연결하기 어려운 경우가 적지 않습니다. 이런 상태로는 "우리 시의 청년 일자리 예산과 실제 취업률 사이에 어떤 관계가 있는가"와 같은 질문에 AI 가 답을 드리기 어렵습니다.

그러므로 이러한 데이터에는 정제 작업이 반드시 필요하다고 생각합니다. 옛 부서명을 현재 조직 기준으로 통일하고, 중복되거나 비어 있는 값을 정리하고, 개인정보가 포함된 항목은 미리 구분해 두는 작업입니다. 다만 이 작업을 모든 부서의 모든 데이터를 대상으로 한꺼번에 진행하실 필요는 없다고 생각합니다. 앞서 말씀드린 원칙대로, 실제로 어떤 에이전트가 이 데이터를 필요로 하는지가 먼저 확인된 뒤에, 그 업무에 필요한 범위만큼만 정제해 나가시는 것이 예산과 시간 모두를 아끼는 길이라고 생각합니다.

4.4. 설명해야 하는 데이터 — 현장과 센서 데이터의 맥락화

마지막으로 도로, 상수도, 대기질, 재난 신고와 같이 현장에서 발생하는 데이터에 대하여 말씀드리고자 합니다. 행정안전부의 2026 년도 재난안전 연구개발사업 시행계획에 따르면, 정부는 사물인터넷(IoT) 센서로 수집한 데이터를 기반으로 인공지능 모델을 개발하고 이를 현장의 소형 기기에 탑재하는 사업을 단계적으로 추진하고 있습니다. 이처럼 현장 데이터를 수집하는 기반은 이미 여러 지자체에서 마련되어 가고 있습니다.

다만 이러한 수치 데이터는 그 자체만으로는 행정적인 의미를 갖기 어렵습니다. 예를 들어 어느 지점의 수압이 평소보다 낮게 측정되었다는 수치만으로는, 이것이 시설 점검이 필요한 상황인지, 단순한 사용량 변화인지 AI 가 판단하기 어렵습니다. 이 수치가 의미를 가지려면 해당 시설의 정상 범위, 과거의 평균값, 인근 지역의 민원 이력, 그리고 이상 상황 발생 시의 표준 대응 절차와 함께 놓여야 합니다.

그러므로 저희는 현장·센서 데이터를 다루실 때에는, 수치 자료 자체를 저장하는 것에 그치지 않고, 그 수치를 해석하는 데 필요한 매뉴얼과 기준을 함께 연결해 두시기를 권해 드립니다. 아울러 위치 정보를 함께 다루셔야 하는 경우가 많으므로, 주소 체계를 표준화하여 지도 정보와 연결하는 작업도 함께 고려하셔야 합니다. 이렇게 준비된 데이터라야 비로소 AI 가 "이 지역은 최근 신고가 잦았던 구간이니 우선 점검이 필요합니다"와 같이, 단순한 수치 나열을 넘어선 행정적 설명을 도와드릴 수 있다고 생각합니다.

정리하여 말씀드리면

이번 장에서 말씀드린 세 가지 방식을 한 문장으로 정리하면 다음과 같습니다.

찾아야 할 데이터는 있는 곳에서 안전하게 연결하고, 만들어야 할 데이터는 필요한 범위만큼 정제하며, 설명해야 할 데이터는 기준과 맥락을 더하여 이해할 수 있게 합니다.

이 세 가지 방식 가운데 무엇을, 언제, 어느 범위까지 적용할 것인가는 앞서 Part 2 에서 말씀드린 원칙과 마찬가지로, 결국 어떤 에이전트를 먼저 도입하시는가에 따라

자연스럽게 정해진다고 생각합니다. 이어지는 Part 5에서는 이러한 데이터 전략이 실제 3 단계 도입 로드맵 속에서 어떻게 순서대로 펼쳐지는지를 말씀드리겠습니다.

Part 5. 3 단계 도입 로드맵 — 왜 인프라가 뒤따라오는가

(이 장은 정보화부서, 보안담당자, 사업 담당 주무관님께서 실무적으로 참고해 주시면 좋을 내용입니다.)

5.1. 이 로드맵은 인프라 일정표가 아닙니다

이제부터 말씀드릴 1 단계, 2 단계, 3 단계는 언뜻 보면 첫해에는 SaaS 를, 둘째 해에는 MCP 연동을, 셋째 해에는 구축형 시스템을 순서대로 만들어 나가는 전형적인 연차별 인프라 구축표처럼 보일 수 있습니다. 그러나 저희가 진짜 말씀드리고 싶은 인과관계는 이와 정반대에 가깝습니다.

Part 2 에서 저희는 "에이전트가 인프라 요구사항을 결정한다"는 원칙을 말씀드린 바 있습니다. 이 로드맵은 바로 그 원칙이 시간의 흐름 속에서 어떻게 구현되는지를 보여드리는 것입니다. 다시 말씀드리면, 저희가 1 년 차에 인프라 구축 계획을 미리 세워두고 그 계획표대로 밀어붙이는 것이 아니라, 1 년 차에 먼저 적용해 본 에이전트들이 실제로 사용되면서 "이 업무에는 최신 조레 데이터가 실시간으로 연결되어야 정확도가 올라간다"거나 "이 업무에는 내부 결재 문서를 안전하게 열람할 수 있어야 한다"는 필요가 현장에서 자연스럽게 드러나고, 그 드러난 필요를 뒤따라 2 년 차, 3 년 차의 인프라가 갖추어지는 것입니다.

이러한 순서는 실제로 정부 차원의 AI 전환 기본계획에서도 확인되는 흐름이라고 생각합니다. 연합뉴스와 전자신문이 2026 년 3 월 19 일 보도한 내용에 따르면, 조달청은 '공공조달 AI 전환 기본계획'을 마련하면서 데이터 규모와 소요 비용, 보안성에 따라 자체 시스템 또는 범정부 AI 플랫폼 가운데 적합한 방식을 선택하여 AI 서비스를

개발하겠다고 밝혔습니다. 아울러 개별 AI 시스템을 구축하는 과정에서 데이터의 공유와 활용이 가능하도록 정비와 품질관리 체계를 함께 마련하겠다고 전해집니다. 이는 처음부터 모든 데이터와 인프라를 갖춘 뒤 서비스를 시작하는 방식이 아니라, 서비스별 특성에 맞추어 필요한 만큼의 기반을 그때그때 마련해 나가는 접근이라는 점에서 저희가 제안드리는 방향과 같은 맥락에 있다고 생각합니다.

그러므로 이어지는 1 단계부터 3 단계까지의 설명을 읽으실 때에는, 이를 "반드시 지켜야 할 구축 일정"이 아니라 "먼저 적용한 에이전트가 요구하게 될 가능성이 높은 인프라의 자연스러운 순서"로 이해해 주시기를 부탁드립니다. 어떤 지자체에서는 1 단계 에이전트만으로도 상당 기간 충분한 성과를 거두실 수 있고, 또 어떤 지자체에서는 필요에 따라 2 단계와 3 단계를 동시에 준비하실 수도 있습니다. 중요한 것은 순서 자체가 아니라, 각 단계로 넘어가는 이유가 인프라 담당 부서의 계획이 아니라 현장에서 사용 중인 에이전트의 실제 요구에서 비롯되어야 한다는 점입니다.

5.2. 1 단계 — SaaS 화면형 에이전트: 먼저 쓰게 만듭니다

민선 9 기의 실질적 성과 창출 기간이 전반기 2 년이라는 점을 다시 상기하면, 1 단계의 목표는 분명합니다. 별도의 구축 기간 없이, 가능한 한 빠르게 공직자 여러분께서 실제로 손에 쥐고 사용해 보실 수 있는 에이전트를 제공해 드리는 것입니다.

이 단계에서 저희가 우선적으로 제안드리는 에이전트는 다음과 같습니다. 보도자료 초안을 작성해 드리는 에이전트, 각종 인사말과 축사의 초안을 작성해 드리는 에이전트, 정기 보고서나 결과보고서의 틀을 잡아 드리는 에이전트, 회의 녹취나 메모를 바탕으로 회의록을 요약해 드리는 에이전트, 그리고 이미 공개되어 있는 법령과 조례를 검색해 드리는 에이전트입니다. 이러한 업무들은 공통적으로 개인정보나 내부 비공개 자료를 다루지 않으면서도, 공직자 여러분의 문서 작성 시간을 상당히 줄여드릴 수 있는 업무라는 특징이 있습니다.

이 단계에서는 반드시 지켜야 할 제한 기준을 명확히 안내해 드려야 한다고 생각합니다. 가장 중요한 원칙은 개인정보나 내부 비공개 자료를 입력하지 않으시도록 하는 것입니다. 이 단계의 에이전트는 대부분 서비스형(SaaS) 상용 AI 를 활용하기 때문에, 자료가 외부로 전달될 가능성을 원천적으로 차단해야 합니다. 이를 위해 화면 안에 입력

전 안내 문구를 표시하거나, 개인정보로 의심되는 문자열이 입력될 경우 자동으로 감지하여 경고해 드리는 기능을 함께 갖추시기를 권해 드립니다.

이 단계의 성과는 다음과 같은 지표로 확인하실 수 있다고 생각합니다. 몇 개 부서에서, 몇 명의 공직자께서 실제로 매주 접속하여 사용하고 계신지, 문서 초안 작성에 소요되는 평균 시간이 도입 전과 비교하여 얼마나 줄었는지, 그리고 공직자 여러분께서 직접 응답해 주시는 만족도 조사 결과가 어떠한지입니다. 이러한 지표들은 다음 단계로 넘어갈 필요성을 판단하는 근거가 되기도 합니다. 예를 들어 법령 검색 에이전트를 사용하시는 과정에서 "이 조례가 최근에 개정되었는지 확실히 알고 싶다"거나 "우리 부서의 과거 유사 사례와 비교해 보고 싶다"는 요구가 반복하여 나타난다면, 이는 곧 2 단계로 넘어갈 시점이 되었다는 신호로 볼 수 있습니다.

5.3. 2 단계 — MCP·메타데이터 검색증강생성형 에이전트: 근거를 갖추게 만듭니다

1 단계에서 문서 작성의 편의를 경험하신 공직자 여러분께서는, 자연스럽게 "이 답변의 근거가 정확한가", "지금 기준으로 맞는 내용인가"를 확인하고 싶어 하시게 됩니다. 이러한 요구에 응답하는 것이 2 단계의 목표입니다.

이 단계에서 저희가 제안드리는 에이전트는 다음과 같습니다. 법령과 조례의 개정 여부를 확인하며 검토 의견을 작성해 드리는 에이전트, 민원 답변의 근거가 되는 법적 조항과 지침을 함께 찾아 정리해 드리는 에이전트, 그리고 복지 제도나 생활 민원에 대하여 최신 기준으로 안내해 드리는 에이전트입니다. 이러한 업무들의 공통점은 Part 4 에서 말씀드린 대로, 답변의 정확성이 곧 법령의 시행일과 개정 이력에 달려 있다는 점입니다.

이 단계에서는 Part 4 에서 말씀드린 MCP 와 메타데이터 검색증강생성 기술이 핵심적인 역할을 합니다. MCP 연동이 가능한 데이터, 예를 들어 국가법령정보센터나 자치법규정보시스템, 혹은 서울특별시의 실시간 도시데이터 MCP 사례처럼 공공기관이 표준화된 방식으로 개방한 데이터는 직접 실시간으로 호출하도록 연결합니다. 아직 API 가 갖추어지지 않은 홈페이지 게시물이나 소규모 고시문은 메타데이터를 함께 저장하는 방식으로 정리하고, 정기적인 변경 감시를 통해 현행화합니다.

이 단계에서 지켜야 할 제한 기준으로는, 답변에 반드시 근거 조항과 시행일, 자료의 출처를 함께 표시하도록 하는 것을 첫 번째로 꼽고 싶습니다. 아울러 근거를 찾지 못하였거나 근거가 상충되는 경우에는 짐작하여 답변하지 않고, 확인이 필요하다는 점을 솔직히 안내하도록 설계해야 합니다. 이 단계에서도 여전히 개인정보가 포함된 내부 자료는 다루지 않으며, 공개된 법령·조례·지침과 이미 익명화된 통계성 자료의 범위 안에서 운영하는 것을 원칙으로 삼아야 한다고 생각합니다.

이 단계의 성과는 다음과 같은 지표로 확인하실 수 있습니다. 법령 검토나 민원 답변 과정에서 근거 누락이나 오류로 인해 재작업이 발생한 건수가 얼마나 줄었는지, 답변에 포함된 근거 조항의 정확도가 담당자 확인 결과 얼마나 되는지, 그리고 동일한 문의에 대하여 여러 담당자가 서로 다른 답변을 드리는 사례가 얼마나 줄었는지입니다. 만약 이 단계에서 "내부 결재 문서나 회의 자료까지 함께 검토할 수 있다면 더 정확한 판단이 가능하겠다"는 요구가 현장에서 반복된다면, 이는 3 단계로 넘어갈 시점이 임박했다는 신호라고 생각합니다.

5.4. 3 단계 — 구축형 시큐어 에이전트: 내부 데이터까지 안전하게 확장합니다

2 단계까지는 대체로 공개된 자료를 중심으로 에이전트를 운영해 드릴 수 있습니다. 그러나 인허가 신청 서류를 사전 검토하거나, 감사 지적 사항에 소명 자료를 준비하거나, 부서 내부의 회의와 결재 이력을 바탕으로 판단을 도와드리는 업무에 이르면, 불가피하게 개인정보와 비공개 내부 자료를 다루어야 하는 상황에 이르게 됩니다. 이러한 업무를 안전하게 지원해 드리기 위한 것이 3 단계, 즉 구축형 시큐어 에이전트입니다.

이 단계에서 저희가 제안드리는 에이전트는 다음과 같습니다. 인허가 신청 서류를 사전에 검토하여 누락된 요건을 안내해 드리는 에이전트, 감사 지적 사항에 대한 소명 자료를 관련 규정과 과거 사례를 근거로 준비해 드리는 에이전트, 부서 내부의 회의와 보고 이력을 바탕으로 의사결정을 보좌해 드리는 내부 회의비서 에이전트, 그리고 과거의 재난·안전 데이터와 현장 센서 데이터를 결합하여 위험 징후를 예측해 드리는 에이전트입니다.

이러한 업무는 반드시 지자체 내부망 또는 이에 준하는 폐쇄형 환경에서, 국가정보원의 AI 보안 가이드북 기준에 부합하는 방식으로 처리되어야 한다고 생각합니다. 아울러 이 단계에서만 가능해지는 몇 가지 기준을 말씀드리고자 합니다. 첫째, 내부 결재 문서와 부서 간 협조 공문을 열람 권한 범위 안에서 검색할 수 있어야 합니다. 다만 이는 어디까지나 검색과 요약에 한정되며, 문서를 직접 수정하거나 결재를 상신하는 행위는 Part 2 에서 말씀드린 대로 반드시 사람의 승인을 거쳐야 합니다. 둘째, 개인정보가 포함된 자료를 다룰 때에는 재식별이 가능한 정보를 분리하여 저장하고, 실제 업무 처리에 필요한 최소한의 범위 안에서만 다시 결합하여 볼 수 있도록 하는 재식별화 통제 절차를 갖추어야 합니다. 셋째, 이 단계에서 이루어지는 모든 조회와 처리는 예외 없이 감사 기록으로 남아야 하며, 그 기록은 담당자 본인은 물론 감사부서에서도 확인할 수 있어야 합니다.

이 단계의 성과는 다음과 같은 지표로 확인하실 수 있습니다. 인허가 사전 검토 단계에서 서류 보완 요청 횟수가 얼마나 줄었는지, 감사 소명 자료를 준비하는 데 걸리는 시간이 얼마나 단축되었는지, 그리고 재난·안전 분야에서 사전 경보를 통해 실제 피해를 예방한 사례가 있는지입니다. 이러한 지표들은 단순히 시스템이 구축되었다는 사실이 아니라, Part 1 에서 말씀드린 대로 "사용 중인 에이전트"가 실제로 행정의 위험과 부담을 줄여드리고 있다는 것을 보여드리는 근거가 될 것입니다.

정리하여 말씀드리면, 1 단계는 공직자 여러분께서 AI 를 편하게 손에 쥐어 보시는 단계이고, 2 단계는 그 AI 가 믿을 수 있는 근거를 갖추어 가는 단계이며, 3 단계는 그 신뢰를 바탕으로 더 무거운 책임이 따르는 업무까지 안전하게 확장해 나가는 단계입니다. 어느 단계이든 그 다음 단계로 넘어가야 하는 이유는 미리 짜인 일정표가 아니라, 앞선 단계에서 실제로 사용되어 온 에이전트가 현장에서 보내온 신호에서 비롯되어야 한다는 점을 다시 한번 강조하여 말씀드리고 싶습니다.

Part 6. 공공형 FDE 운영 모델

(이 장은 실무 담당자분들과 경영진께서 함께 읽어주시면 좋은 내용입니다.)

6.1. 에이전트는 납품하는 것이 아니라 현장에서 함께 길러내는 것입니다

지금까지 저희는 에이전트를 먼저 정하고, 그에 맞추어 데이터와 보안 체계를 갖추어야 한다는 말씀을 여러 차례 드렸습니다. 그런데 이 원칙을 실행에 옮기는 방식, 즉 "누가, 어떻게" 에이전트를 만들고 운영할 것인가에 대해서도 조심스러운 제언을 드리고자 합니다.

전통적인 시스템통합(SI) 방식은 요구사항을 정의하고, 설계하고, 개발하고, 검수받고, 납품하는 절차를 따릅니다. 이 방식은 요구사항이 처음부터 명확한 시스템, 예를 들어 행정정보시스템이나 회계 시스템을 구축할 때에는 오랫동안 효과적으로 작동해 왔습니다. 그러나 에이전트는 사정이 다르다고 생각합니다. 에이전트가 실제로 잘 작동하는지는 설계도만 보아서는 알기 어렵고, 실제 업무 현장에서 공직자 여러분께서 사용해 보시면서 예상치 못한 예외 상황과 표현의 차이, 판단 기준의 미묘한 차이를 계속 발견하고 반영해 나가야 비로소 쓸모 있는 수준에 이르기 때문입니다.

이러한 어려움은 비단 공공부문만의 문제가 아닙니다. IT 시장 조사기관 가트너의 2025 년 보고서에 따르면 기업의 AI 프로젝트 가운데 약 60 퍼센트가 개념검증(PoC) 단계에서 중단되는 것으로 나타났으며, 이러한 경향은 2026 년에도 크게 달라지지 않은 것으로 전해집니다. 처음부터 완성된 형태로 요구사항을 정의하여 납품받는 방식으로는, 실제 업무에 정착하기까지 필요한 반복적인 개선의 기회를 충분히 갖기 어렵다는 것이 그 배경으로 지목되고 있습니다.

이러한 문제의식 속에서 최근 몇 년 사이 새롭게 주목받는 방식이 바로 현장 밀착형 엔지니어(FDE, Forward Deployed Engineer) 운영 모델입니다. 이 개념을 처음 체계화한 곳은 미국의 데이터 분석 기업 팔란티어(Palantir)로 알려져 있으며, 회사 설립 초기부터 고객의 현장에 엔지니어를 직접 배치하여 설정부터 맞춤 구현까지 담당하게 하는 방식을 운영해 온 것으로 전해집니다. 이러한 흐름은 이후 다른 기업으로도

확산되었습니다. 삼성 SDS 의 인사이트 보고서에 따르면 2026 년 3 월 액센추어와 마이크로소프트가 수천 명 규모의 AI 엔지니어를 동원하는 현장 밀착형 엔지니어링 조직을 구성하겠다고 밝히는 등, 2026 년 상반기 들어 여러 글로벌 기업이 비슷한 방향으로 조직을 재편하는 움직임을 보인 것으로 전해집니다. 아울러 이 보고서는 AI 도입에 있어 시스템 성능뿐 아니라 데이터 접근 권한, 보안, 책임 소재와 같은 거버넌스 측면이 함께 중요해지고 있다고 지적하고 있습니다.

저희 스캐터엑스가 이 백서를 통해 제안드리고자 하는 것도 이와 같은 방향입니다. 저희는 지방정부에 에이전트라는 완성품을 납품해 드리는 회사가 아니라, 공직자 여러분과 함께 현장에서 에이전트를 길러 나가는 동반자가 되고자 합니다.

6.2. FDE 의 역할과 지자체와의 공동 운영 구조

저희가 말씀드리는 공공형 FDE 는, 저희 스캐터엑스의 담당 인력이 지자체 현장에 상주하거나 정기적으로 방문하여, 공직자 여러분과 함께 다음과 같은 순환 과정을 반복해 나가는 역할을 의미합니다.

먼저 업무 발굴 단계입니다. 어느 부서의 어떤 업무에서 반복적인 부담이나 처리 지연이 발생하고 있는지를 공직자 여러분과 함께 대화하며 찾아 나가는 과정입니다. 이 단계에서는 저희가 먼저 기술을 제안드리기보다, 공직자 여러분의 불편함을 먼저 여쭙는 것을 원칙으로 삼고자 합니다.

다음은 절차화 단계입니다. 발굴된 업무를 공직자 여러분께서 실제로 어떤 순서로 처리하고 계신지 상세히 여쭙고, 그 절차를 에이전트가 따라갈 수 있는 단계별 지침으로 옮겨 담는 과정입니다.

세 번째는 데이터 식별 단계입니다. 이 절차를 수행하는 데 필요한 자료가 무엇인지, 그 자료를 어디에서 어떻게 가져올 수 있는지, 그리고 그 자료의 보안 등급은 어느 정도인지를 함께 확인하는 과정입니다. Part 4 에서 말씀드린 원칙에 따라, 필요한 만큼만 연결하거나 정제하는 방식을 택합니다.

네 번째는 프로토타입 제작 단계입니다. 완성된 형태가 아니라, 담당 부서에서 곧바로 시험해 보실 수 있는 초기 형태의 에이전트를 빠르게 만들어 드리는 과정입니다.

다섯 번째는 현장 적용 단계입니다. 실제 업무 환경에서 담당 공직자 여러분께서 며칠에서 몇 주간 직접 사용해 보시며 성능과 편의성을 확인하시는 과정입니다.

여섯 번째는 개선 단계입니다. 현장에서 확인된 부족한 점, 놓친 예외 상황, 어색한 표현들을 저희 FDE 인력이 신속하게 반영하여 다시 제공해 드리는 과정입니다. 이 개선 과정은 한 번으로 끝나지 않고 여러 차례 반복됩니다.

마지막으로 판단 단계입니다. 이 에이전트를 계속 사용할 것인지, 다른 부서로 확산할 것인지, 사용 빈도가 낮아 더 이상 유지할 실익이 적다고 판단되면 과감히 접을 것인지, 혹은 사용량과 중요도가 매우 높아져 지자체 자체의 구축형 시스템으로 전환할 필요가 있는지를 공직자 여러분과 함께 판단하는 과정입니다.

이 순환 과정에서 저희가 특히 강조하여 말씀드리고 싶은 부분은 "폐기"라는 선택지도 정당한 결과로 받아들여야 한다는 점입니다. 모든 에이전트가 성공적으로 확산되지는 않을 수 있습니다. 실제로 사용 빈도가 낮거나 효과가 뚜렷하지 않다면, 이를 솔직하게 인정하고 다른 업무로 자원을 옮기는 것이 예산을 아끼고 신뢰를 지키는 길이라고 생각합니다.

6.3. 2027년부터 2028년까지의 실행 계획

Part 1에서 말씀드린 대로, 민선 9기 지방정부의 실질적인 성과 창출 기간은 2026년 하반기부터 2028년까지의 약 2년으로 보는 것이 현실적이라고 생각합니다. 이 기간 동안 저희가 제안드리는 우선순위는 다음과 같습니다.

2027년은 내부 업무의 성과를 먼저 보여드리는 시기로 삼으시기를 권해 드립니다. 시민들께 직접 노출되지 않는 내부 업무에서 먼저 에이전트를 적용해 보시면, 실패하더라도 그 여파가 크지 않으면서도 공직자 여러분의 체감 효과는 빠르게 확인하실 수 있습니다. 이 시기에 쌓인 경험과 신뢰가 2028년의 확산을 위한 기반이 됩니다.

2028년은 이러한 내부 성과를 바탕으로, 시민 여러분께서 직접 체감하실 수 있는 서비스로 넓혀 가시는 시기로 삼으시기를 권해 드립니다. 아울러 2027년 한 해 동안 특히 사용 빈도가 높고 중요도가 큰 것으로 확인된 에이전트에 대해서는, 이 시점부터

지자체 자체의 구축형 시스템으로 전환하는 것을 검토하시는 것이 바람직하다고 생각합니다.

이를 표로 정리해 드리면 다음과 같습니다.

시기	우선순위	예시 업무 영역	핵심 목표
2027 년	내부 업무 성과형 에이전트	민원 답변 초안 작성, 법령·조례 검토 지원, 보고서·회의록 정리, 반복 문의 응대 지원	공직자 체감 효과 확보, FDE 공동 운영 체계 정착, 사용 데이터 축적
2028 년	시민 체감형·구축형 전환 에이전트	복지 대상자 안내, 인허가 사전 상담, 재난·안전 현장 대응 지원, 2027 년 검증된 고빈도 에이전트의 구축형 전환	시민 체감 서비스 확산, 안정적 운영 체계로의 이행, 임기 후반기 성과 기반 마련

이 표는 고정된 사업 목록이 아니라, 저희 스캐터엑스가 여러 지자체 현장에서 함께
확인해 나가고자 하는 우선순위의 방향입니다. 실제로 어떤 업무를 먼저 다룰 것인가는
각 지자체의 여건과 공직자 여러분의 의견에 따라 함께 조정되어야 한다고 생각합니다.

정리하여 말씀드리면, 저희가 제안드리는 공공형 FDE 운영 모델의 핵심은 시스템을
납품해 드리고 자리를 떠나는 것이 아니라, 성과가 확인될 때까지, 그리고 그 이후의
안정적인 운영까지 공직자 여러분과 함께하는 것입니다. 이러한 동반의 과정이야말로,
이 백서의 제목이기도 한 「에이전트가 먼저다」라는 원칙을 실제 행정 현장에서
완성하는 마지막 조각이라고 생각합니다.

에이전트가 먼저다

민선 9 기 지방정부를 위한 벤더 중립형 행정 AI 에이전트 허브 전략 백서

결론

첫 2 년의 성과가 다음 4 년을 결정합니다

이 백서를 통하여 저희 스캐터엑스가 드리고 싶었던 말씀은 크게 세 가지로 정리될 수 있다고 생각합니다.

첫째, 에이전트가 먼저입니다. 민선 9 기 지방정부에 실질적으로 주어진 시간은 임기 전반기 2 년에 가깝습니다. 이 시간 안에 성과를 보여드리기 위해서는, 무엇을 구축할 것인가를 먼저 정하는 방식이 아니라, 어떤 업무를 도와드릴 에이전트가 필요한지를 먼저 정하는 방식이 옳다고 생각합니다. 그 에이전트를 실제로 사용해 보시는 과정에서 어떤 데이터와 어떤 보안 수준이 필요한지가 자연스럽게 드러나며, 그때 필요한 만큼의 인프라를 갖추어 나가는 것이 순서에 맞는다고 믿습니다. 인프라가 에이전트를 낳는 것이 아니라, 에이전트의 실제 필요가 인프라의 범위를 결정한다는 원칙을 다시 한번 말씀드립니다.

둘째, 벤더 중립성입니다. 인공지능 기술은 앞으로도 빠르게 변화할 것으로 예상됩니다. 특정 기업의 대규모언어모델이나 특정 데이터 플랫폼에 처음부터 깊이 결합되는 방식은, 장기적으로 지방정부의 선택권을 제한하는 결과로 이어질 수 있습니다. 저희는 지방정부가 범정부 AI 공통기반, 여러 민간 기업의 에이전트, 그리고 자체 개발 에이전트를 상황에 맞게 자유롭게 연결하여 사용하시는 열린 구조를 제안드렸습니다.

이러한 개방성이 시큐어 라우터를 통한 일관된 통제와 함께 이루어질 때, 비로소 안전하면서도 지속 가능한 AI 활용이 가능하다고 생각합니다.

셋째, 공직자 여러분과 현장 밀착형 인력의 공동 운영입니다. 아무리 훌륭한 에이전트라 하더라도 납품과 동시에 완성되는 것은 아니라고 생각합니다. 현장의 업무 절차는 부서마다, 시기마다 조금씩 다르며, 실제로 사용해 보아야만 드러나는 세부적인 개선 사항이 반드시 있기 마련입니다. 그러므로 시스템을 전달해 드리는 것에서 그치지 않고, 현장에 함께하며 공직자 여러분과 지속적으로 다듬어 나가는 운영 방식이 반드시 뒤따라야 한다고 믿습니다.

이 세 가지 원칙은 결국 하나의 문장으로 모인다고 생각합니다.

성과는 에이전트가 만들고, 인프라는 그 에이전트를 뒷받침합니다.

민선 9 기 지방정부의 첫 2 년이 어떻게 채워지느냐에 따라, 남은 임기와 그 이후의 신뢰가 크게 달라질 것이라 생각합니다. 저희 스캐터엑스는 이 소중한 시간을 함께 만들어 가는 든든한 동반자가 되고자 합니다. 부족한 백서를 끝까지 읽어주신 공직자 여러분께 다시 한번 깊이 감사드립니다.

부록

부록 1. 공직자용 에이전트 10 대 체크리스트

순번	체크 항목	확인 내용
1	보안 등급 판단	질의·자료의 보안 등급과 사용자 권한을 답변 생성 전에 확인하는가
2	공식 근거 기반	법령·조례·지침 등 공식 자료를 근거로 답변하는가
3	시점 구분	시행일·개정일·폐지일을 인식하여 현재/과거 기준을

		구분하는가
4	하이브리드 검색	의미 기반 검색과 정확한 조항 검색을 함께 사용하는가
5	데이터 출처 기록	근거 문서의 출처, 작성 부서, 작성일을 표시하는가
6	질의 명확화	기준일·지역·목적이 불분명하면 짐작하지 않고 재확인을 요청하는가
7	자체 검증	답변 생성 후 근거의 충분성·최신성을 스스로 점검하는가
8	제한된 권한	검색·요약·비교·초안 작성까지만 수행하고 시스템에 직접 반영하지 않는가
9	사람의 최종 승인	민원 발송·처분 결정·결재 상신은 담당 공직자의 승인을 거치는가
10	감사 기록	질의·근거자료·사용 모델·처리 시각이 감사 기록으로 남는가

부록 2. 3 단계 로드맵 요약표

단계	시기	핵심 내용
1 단계 (도입기)	1 차년도	SaaS 기반 통합 업무화면 보급, 공직자 AI 협업 문화 조성
2 단계 (고도화기)	2 차년도	메타데이터 RAG·MCP 연동을 통한 데이터 실시간 호출 체계 구축
3 단계 (안정화기)	3 차년도	시큐어 RAG·시큐어 라우터 기반 완성형 플랫폼, 필요

		시 구축형 전환
--	--	----------

부록 3. 2027~2028 추천 에이전트 목록 (예시)

- 민원 답변 초안 작성 에이전트
- 법령·조례 검토 지원 에이전트
- 인허가 사전 검토 지원 에이전트
- 회의록 요약·정리 에이전트
- 예산·계약 문서 검토 지원 에이전트
- 재난·시설 이상 징후 설명 에이전트

(위 목록은 예시이며, 실제 도입 순서는 각 지자체의 업무 우선순위와 부서별 수요 조사에 따라 정해지는 것이 바람직합니다.)

부록 4. 용어 정리

용어	설명
LLM (대규모언어모델)	대량의 텍스트로 학습되어 자연어를 이해·생성하는 인공지능 모델
RAG (검색증강생성)	외부 문서를 검색하여 그 내용을 근거로 답변을 생성하는 방식
Metadata RAG (메타데이터 RAG)	문서의 발행기관·시행일·유형 등 메타데이터를 활용해 검색 범위를 좁히는 RAG 방식
MCP (모델맥락프로토콜)	AI 가 여러 시스템의 데이터·기능을 표준화된 방식으로 실시간 호출하는 기술
Secure Router (시큐어 라우터)	사용자·업무유형·데이터 등급에 따라 요청을 적절한 처리 경로로 분기하고 기록하는 장치
FDE (현장 밀착형 운영 인력)	현장에 파견되어 공직자와 함께 에이전트를 점검·개선하는 운영 인력
Time-Aware RAG (시점 인식 RAG)	시행일·개정일을 인식하여 현재 기준과 당시 기준을 구분해 답변하는 RAG 방식
Self-RAG (자체 검증 RAG)	답변 생성 후 근거의 충분성과 최신성을

부록 5. 참고문헌 및 출처 안내

- 국가정보원 국가인공지능안보센터(2025.12.10 배포). 「AI 보안 가이드북」.
- 인용 부분: Part 3 시큐어 라우터, Part 5 3 단계 도입 로드맵

- 연합뉴스(2026.6.24). 한국지능정보사회진흥원(NIA) '2026 공공 AI 박람회' 부대행사 '공공부문 AI 도입·활용 가이드 설명회' 관련 보도
- 보안뉴스·디지털데일리·지디넷코리아. 과학기술정보통신부·행정안전부 '범정부 AI 공통기반' 서비스 개시(2025.11.24) 관련 보도
- 한국지방정부신문(2026.7.14). 서울특별시 '서울 실시간 도시데이터 MCP' 시범 서비스 공개 관련 보도
- 아이데일리뉴스(2026.8). 한국산업인력공단 'HRDKorea MCP' 서비스 가동 관련 보도
- 연합뉴스(2026.7). 소프트캠프 배환국 대표, AI 에이전트 권한 관리 관련 진단 보도
- 그리드지(Gridge). 사내 AI 에이전트 도입 가이드 (권한 항목별 설계 원칙 관련)
- 행정안전부. 2026 년도 재난안전 연구개발사업 시행계획 (IoT 센서 기반 AI 모델 개발 관련)
- 스캐터엑스 기업부설연구소 내부 기술자료