

# KB 지식 비타민

## AI 오케스트레이션을 통한 조직 내 AI 접근성 확대 전략

- AI가 조직 전체에 확산하지 못하는 이유
- AI 오케스트레이션 개요
- MCP와 AI 오케스트레이션
- AI 오케스트레이션 도입 로드맵
- 향후 전망 및 시사점

### < 요약 >

- 기술적 복잡성과 데이터의 품질 및 편향 문제, 통합된 인공지능(AI) 거버넌스 체계의 부재 등 복합적인 요인으로 인해 AI 모델이 조직 전반에서 폭넓게 활용되지 못하고 있음
  - 거대언어모델(Large Language Model, LLM) 기술이 인간 수준의 언어 이해와 생성 능력을 갖추며 다양한 벤치마크에서 인간 전문가에 근접하는 성능을 보여주면서 전 산업에 걸쳐 주목을 받고 있음
  - 그러나 여전히 최적 모델 선택, 환각(Hallucination) 현상에 따른 부정확한 답변, 그리고 기업 고유의 업무에 대한 기술적 진입장벽으로 인해 전사적 AI 활용에는 한계가 존재
- 다양한 구성 요소를 유기적으로 통합하고 조율하기 위한 AI 오케스트레이션(AI Orchestration) 등장
  - AI 오케스트레이션은 다양한 톨이나 모듈을 연결하고 조건에 따라 적절한 것을 선택적으로 호출하는 자동화된 판단 기능은 물론, 복잡한 요청을 하위 작업으로 분류하고 순차 실행하는 다단계 실행 기능과 사용자의 대화 이력이나 업무 흐름 상태를 기억하는 컨텍스트 유지 기능을 갖춘
  - AI 오케스트레이션 도입의 가장 큰 효과는 접근성 향상으로 기술 장벽을 제거하고 직관적 인터페이스 상에서 사용자별로 맞춤 대응함으로써 비개발 부서도 AI를 자유자재로 활용하여 조직 전체의 생산성과 디지털 역량을 향상시킬 수 있다는 것임
- AI 오케스트레이션에서 ‘모델 컨텍스트 프로토콜(Model Context Protocol, MCP)’은 AI 모델과 데이터 소스 및 도구 간의 상호작용을 표준화하여 조직 내 AI 접근성과 활용성을 향상시키는 핵심 요소로 부상
  - MCP는 LLM이 검색·데이터베이스·연산 등 외부 도구를 상황에 맞게 자동으로 선택하고 연동할 수 있도록 도와주는 에이전트 인터페이스 프로토콜로, 앤트로픽이 2024년 11월 오픈소스로 공개
  - 기존 워크플로우 기반 오케스트레이션과 비교해 AI 모델이 동적으로 워크플로우를 판단하고 필요에 따라 도구를 유연하게 호출하며, 상황에 따른 컨텍스트 변화를 추적하고 복수 시스템 간의 상태 정보를 연계하여 기능 추가 및 연동이 용이하다는 장점이 있음
  - 2025년 4월 현재까지 오픈AI, 마이크로소프트, 구글, 아마존 등 주요 AI 기업들이 자사 제품에 도입을 선언하면서 사실상 기술 표준(De facto standard)이 되고 있음
- 향후 전망 및 시사점
  - 금융권은 고유한 보안 요건과 도메인 특성으로 인해 일반적인 AI 오케스트레이션 구조만으로는 실질적인 적용에 한계가 존재하므로, AI 도입 초기부터 AI 오케스트레이션 전략을 적용하며 데이터 팀·IT 운영 팀·컴플라이언스 팀 등 다양한 부서 간의 유기적 협업을 이끌어내는 것이 중요
  - 직관적 사용과 반복 가능성에 초점을 맞춰 기능의 완성도보다 사용자 경험(UX) 중심으로 접근

## 1. AI가 조직 전체에 확산하지 못하는 이유

### ■ 챗GPT 등장을 기점으로 거대언어모델(Large Language Model, LLM)은 인간 수준의 언어 이해와 생성 능력을 갖춘 인공지능(AI) 기술로서 전 산업에 걸쳐 주목받고 있음

○ LLM은 이미 다양한 벤치마크에서 평균적인 인간 수준을 뛰어넘는 성능을 보여주고 있으며, 일부 고난도 평가에서도 인간 전문가에 근접하는 결과를 기록

[표 1] 고난도 평가 벤치마크

벤치마크	세부 내용
MMMU (Massive Multi-discipline Multimodal Understanding)	다양한 분야의 대학 수준 과제에 대해 멀티모달 <sup>1</sup> AI 모델을 평가하기 위해 설계된 새로운 벤치마크
GPQA (Graduate-level Google-Proof Q&A Benchmark)	물리학, 화학, 생물학 분야의 전문가들이 작성한 대학원 수준의 복잡한 문제들로 구성되어 AI 언어 모델의 고급 추론 능력을 평가하기 위해 설계된 벤치마크
SWE-bench	실제 소프트웨어 엔지니어링 문제를 다루는 언어 모델 평가 벤치마크로, 깃허브(GitHub)의 인기 파이썬 저장소에서 수집한 2,294 개의 이슈와 해당 풀 리퀘스트 <sup>2</sup> 로 구성됨. 모델이 주어진 문제를 해결하기 위해 코드베이스를 수정하고, 수정 내용이 단위 테스트를 통과하는지를 평가

자료: KB경영연구소

- 2025년 2월 7일 기준 GPT-4가 86.4%의 정확도를 기록하여 89.8%를 달성한 인간 전문가에 근접한 성능을 보임
- 2025년 4월 4일 기준 GPQA 다이아몬드(GPQA Diamond) 세트<sup>3</sup>에서는 제미니 2.5 프로(Gemini 2.5 Pro)가 80.3%, 클로드 3.7 소네트(Claude 3.7 Sonnet)가 75.3%를 달성하여 인간 전문가의 81.3%에 근접한 수치를 보였음
- 2025년 1월 10일 기준 SWE-벤치 베리파이드(SWE-bench Verified) 세트<sup>4</sup>에서 구글의 Learn-by-interact 모델이 60.2%의 성능을 달성하며 특정 문제에는 인간처럼 코드 작성이 가능하다고 여겨짐

○ 이러한 추세에 발맞춰 전 세계적으로 국가 차원의 투자 확대와 함께 기업의 AI 도입률이 빠르게 증가하고 AI에 대한 인식도 '일상적인 도구'로 변화하고 있음

<sup>1</sup> 텍스트, 이미지, 음성, 영상, 센서 등 여러 종류의 데이터 형태(Modality)를 동시에 이해하고 처리할 수 있는 능력

<sup>2</sup> 개발자가 깃허브 저장소(Repository)에서 코드 변경 사항을 제안하고, 이를 프로젝트에 반영해달라고 요청하는 방식

<sup>3</sup> 전문가 집단은 모두 맞추었지만, 비전문가 중에는 3분의 1 미만이 정답을 맞춘 세트

<sup>4</sup> 다수의 인간 평가자가 검토하여 확실히 해결 가능하다고 판단한 500개의 문제를 모아놓은 데이터세트로, 이론적으로는 100% 해결 가능한 SWE-벤치의 하위 집합

- 생성형 AI를 하나 이상의 직무에 사용한다고 응답한 기업 비율도 2023년 33%에서 2024년 71%로 2배 이상 증가
- 2024년 전 세계 기업의 인수합병(M&A), 민간 투자, 주식 공모 등을 포함한 AI 관련 총투자액은 2,523억 달러로 전년 대비 25.5% 증가
  - 미국의 AI 관련 민간 투자는 1,091억 달러로 2위 중국(93억 달러)의 12배, 3위 영국(45억 달러)의 24배에 달함
  - 생성형 AI 분야 민간 투자는 339억 달러로 전년 대비 18.7%, 2022년 대비 8.5배 이상 성장
- 각국 정부는 AI 기술 경쟁력을 확보하기 위해 대규모 투자 계획을 발표
  - 캐나다(24억 달러), 중국(475억 달러 규모의 반도체 펀드 조성), 프랑스(1,090억 유로), 인도(12억 5천 달러), 사우디아라비아[‘프로젝트 트랜센던스(Project Transcendence)’를 통해 1천억 달러]

○ 최근에는 범용인공지능(Artificial General Intelligence, AGI)에 가장 가까운 것으로 평가받는 중국 스타트업 모니카의 마누스(Manus)가 등장하며 향후 AI 에이전트가 나아갈 방향을 제시

- 마누스 AI는 멀티모달 입력을 실시간으로 통합하고 분석하여 인간처럼 상호작용하며 문제를 해결하는 고성능 AI 에이전트를 의미
  - 엔트로픽의 클로드 3.5 소네트를 기반으로 수십 개의 톨과 외부 시스템을 적용하여 멀티 에이전트 협업 시스템을 구축하며 단순한 질의응답을 넘어 복잡한 업무 수행이 가능

## ■ 그러나 대부분의 조직에서는 여전히 LLM의 최적 모델 선택, 부정확한 답변, 그리고 기술적 한계 등으로 인해 전사적으로 모든 직원이 AI를 직접 활용하는 데 한계가 있음

○ 많은 기업이 AI에 관심을 갖고 투자에 나서고 있지만, 조직 전반에서 폭넓게 활용되지 못하면서 AI 도입은 예상보다 더디게 진행되고 있음

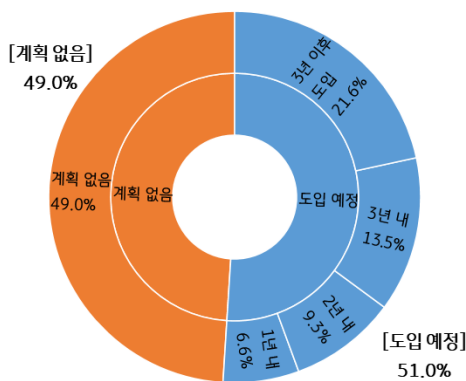
- 보스턴컨설팅그룹(BCG)의 글로벌 설문<sup>5</sup>에 따르면, 조사 대상 기업의 74%는 AI를 활용하여 아직까지 뚜렷한 가치를 실현하지 못하는 것으로 나타남
  - AI 파일럿 프로젝트와 개념 증명(PoC<sup>6</sup>)은 많지만 생산 단계로 연결되는 사례는 소수이며, 26%의 기업만이 PoC 단계를 넘어 스케일업(Scale Up, 사업 확장)할 역량을 갖춘 것으로 평가됨

<sup>5</sup> BCG, October 24, 2024, “AI Adoption in 2024: 74% of Companies Struggle to Achieve and Scale Value”

<sup>6</sup> Proof of Concept, 아이디어나 기술의 실현 가능성을 검증하는 절차

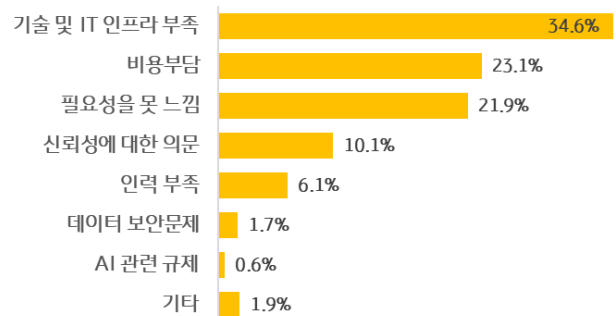
- 인사관리 전문 매체 《HR 인사이트(HR Insight)》의 설문조사에서는 전체 응답자의 36%만이 AI를 도입했거나 도입을 계획 중이라 답변<sup>7</sup>
  - AI를 도입하지 않았다고 답변한 응답자들은 가장 큰 이유로 ‘AI 활용 전략의 부재(22%)’를 꼽았고, ‘AI 도입 및 적용 비용(17%)’도 주요 장애물로 확인됨
- 대한상공회의소의 설문조사<sup>8</sup>에 따르면, 조사 대상 기업의 절반(49.0%) 정도는 아직 AI 도입 계획이 없다고 응답했으며, ‘기술 및 IT 인프라 부족(34.6%)’, ‘비용 부담(23.1%)’, ‘신뢰성에 대한 의문(10.1%)’ 등을 주된 이유로 꼽음

[그림 1] 향후 AI 도입 계획



자료: 대한상공회의소

[그림 2] AI 기술 미활용 이유



자료: 대한상공회의소

- **[최적 모델 선택의 어려움]** 기업들은 LLM 개발보다는 실질적 활용에 방점을 두고 있으나, 성능이 빠르게 개선되는 생태계에서 “가장 적합한 LLM을 언제, 어떻게 선택할 것인가”는 향후 AI 활용의 효율성과 지속 가능성을 좌우할 핵심 요인으로 부각
- 특히 금융과 같이 보안 요구 사항이 높은 산업에서는 온프레미스(On-premise)<sup>9</sup> 기반의 AI 운영이 요구되어 초기 진입장벽이 더욱 높음
  - 금융위원회는 2024년 8월 13일 발표한 ‘금융 분야 망 분리 개선 로드맵’에서 규제 샌드박스 특례 조치를 통해 예상되는 리스크에 대한 보안 대책 마련을 조건으로 금융회사의 생성형 AI 활용을 허용할 것임을 밝힘
- AI 모델 학습에 필요한 컴퓨팅 파워는 약 5개월마다, 데이터세트 크기는 약 8개월마다, 학습 전력 소비량은 매년 2배 증가

<sup>7</sup> 브런치스토리, 2024.6.29, “AI의 성공적 도입을 위한 조직관리”<sup>8</sup> 대한상공회의소, 2024, “국내 기업 AI 기술 활용 실태 조사”<sup>9</sup> 기업이나 조직이 자체 데이터센터나 서버실과 같은 물리적인 공간에 하드웨어와 소프트웨어를 직접 설치하고 관리

- **[데이터 품질 및 편향성]** LLM이 여전히 사실과 다른 정보를 생성하는 ‘환각(hallucination)’ 문제를 완전히 극복하지 못함에 따라 AI에 대한 신뢰가 아직 부족하며 데이터 편향에 대한 우려 역시 큰 장애 요소
  - AI의 부정확한 답변은 사용자의 신뢰도를 저하시킬 뿐 아니라 자동화 시스템 내 오남용 가능성을 높여 도입 속도를 떨어뜨리는 요인 중 하나
    - 특히 금융, 법률, 의료처럼 정합성과 정확성이 핵심인 산업에서는 환각 현상이 치명적인 오류로 이어질 수 있어 전사적 확산에 대한 장애물로 작용
  - 자사에 맞는 충분한 양의 고품질 데이터를 확보하지 못해 AI 모델 최적화에 어려움을 토로하는 기업들도 다수
- **[기술적 한계]** LLM은 웹 상의 방대한 텍스트, 문서, 코드 등을 기반으로 사전 학습하기 때문에 일반적인 언어 이해나 상식 습득에서는 우수한 성능을 보이지만, 기업의 고유한 업무 처리에는 어려움이 존재
  - 최대 입력 토큰<sup>10</sup>이 제한되어 있기 때문에 긴 문서를 처리해야 할 경우에는 별도의 전처리 로직이 필요
  - 문장과 섞여 있거나 행렬이 복잡하게 병합된 표에 대해서는 주변 텍스트와 혼동하는 등 인식이 떨어져 부정확한 응답을 생성할 수 있음
  - 동일한 질문에도 반복 요청 시 결과가 달라질 수 있어 한 가지 문제에 대해 항상 같은 결과를 기대하는 업무에서는 적용이 매우 제한됨
- **[명확한 비즈니스 성공 사례 부재 및 투자 성과의 불투명성]** AI 도입으로 일부 비용 절감과 매출 증대 효과가 나타나고 있지만, 향상되는 수준이 대부분 5~10% 미만에 머무는 등 아직 가치 창출 초기 단계를 벗어나지 못하고 있음
  - IBM의 설문조사<sup>11</sup>에 따르면, 조사 대상 기업 중 42%가 AI 활용 확대를 주저하는 요인으로 뚜렷한 재무적 타당성이나 성공 사례 부재를 언급
    - AI 도입으로 비용 절감이나 매출 증대가 얼마나 가능한지 명확하지 않으면 경영진의 설득이 어렵기 때문
  - AI를 핵심 전략과 연계하지 못하고 부서별 산발적 실험에 머무르는 경우, 가시적 성과가 적어 후속 투자가 위축되는 악순환이 발생하기도 함

<sup>10</sup> LLM이 언어를 처리하는 최소 단위

<sup>11</sup> IBM, 14 February, 2025, “The 5 biggest AI adoption challenges for 2025”

○ **[조직 문화 및 인적 요인]** 새로운 기술에 대한 구성원의 저항과 변화관리 실패도 중요한 문제

- 조직 구성원이 AI로 인해 일자리 위협을 느끼거나 출력 결과에 불신을 갖는 경우 활용이 제한될 수 있음
  - BCG의 설문조사<sup>12</sup>에서 조사 대상 기업들은 AI 도입 시 직면하는 어려움의 70%가 구성원과 프로세스 이슈에서 기인한다고 밝힘. 이는 변화관리, 협업 방식, 업무 재설계 등에 대한 준비 부족과 저항이 기술적 문제보다 더 큰 장애가 되고 있음을 의미

○ **[거버넌스, 규제 및 보안 우려]** 명확한 AI 거버넌스 체계의 부재에 따른 의사결정의 투명성 및 책임성 부족과 규제 준수 리스크에 대한 우려가 활용 확대를 저해할 수 있음

- 특히 금융과 같이 규제가 엄격한 산업에서는 AI 출력 결과에 대한 설명 가능성과 감시 대응 체계 미비 시 전사적 활용이 어려울 수 있음
- AI 활용에 따른 윤리적 책임 규정과 위험관리 체계(AI 거버넌스)가 마련되지 않으면 조직 내 신뢰 확보가 어려워지고, 이로 인해 일부 부서에서 도입을 꺼리게 되면서 활용 격차가 확대될 수 있음

■ **2022년 챗GPT 등장 이후 다양한 AI 서비스가 출현하고 기업이 AI를 적극 도입하고 있지만 여러 가지 복잡성과 제약이 존재. 따라서 성공적인 AI 도입을 위해 단순히 기술을 도입하는 차원을 넘어 조직 전반에 걸친 체계적이고 전략적인 접근이 필요**

○ 기업의 AI 활용도가 증가하면서 처리해야 할 데이터 양이 증가하고 업무 프로세스가 복잡해졌으며, 이로 인해 단일 AI 모델로는 산업 현장의 세분화되고 복잡한 업무를 효과적으로 해결하기 어렵다는 한계가 부각

## 2. AI 오케스트레이션 개요

■ **AI 오케스트레이션(AI Orchestration)은 다양한 AI 도구와 시스템을 통합해 복잡한 작업을 효율적으로 수행할 수 있도록 조율하는 프로세스를 의미**

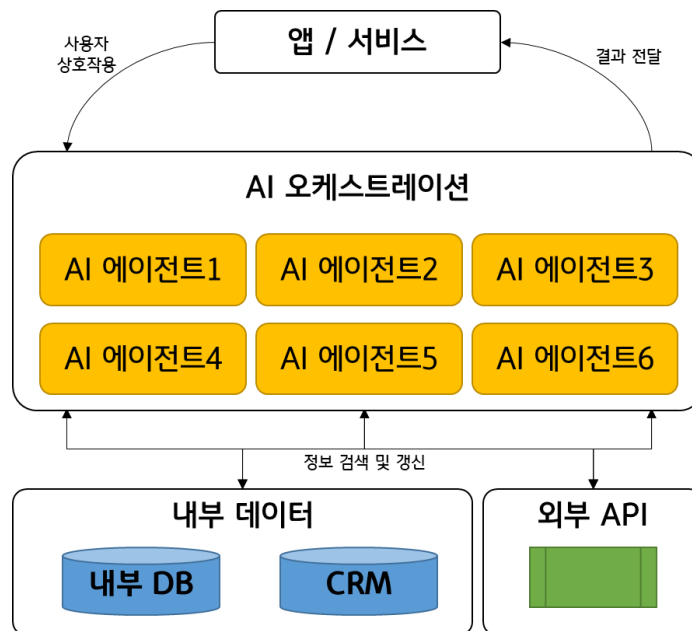
○ LLM을 중심으로 검색 시스템, 외부 애플리케이션 프로그래밍 인터페이스(API), 내부 데이터베이스, 워크플로우 자동화 도구 등 다양한 AI 구성 요소를 유기적으로 통합하고 조율하여 복잡한 작업을 자동화하는 기술적 접근 방식

- 기존에는 사용자가 직접 프롬프트를 작성하거나 단일 AI 모델을 수동으로 호출해야 했다면, AI 오케스트레이션은 여러 AI 모델의 기능이 순차적 혹은 병렬적으로 실행되는 구조를 자동화된 흐름으로 관리

<sup>12</sup> BCG, Ibid.

- 단일 AI 모델의 성능을 극대화하는 것이 아니라 여러 AI 모델의 기능을 유기적으로 통합해 실질적인 업무 자동화 및 보조 시스템을 구축하는 데 목적이 있음
  - 특히 금융과 같이 업무 단계가 복잡하고 규칙 기반의 해석이 필요한 산업에서는 다양한 AI 기능을 역할별로 분류함으로써 업무 정확성과 일관성을 확보 가능
- AI가 단순한 질의응답을 넘어 여러 단계에 걸친 복잡한 업무를 처리하는 데 필요한 검색, 계산, 질의응답, 문서 생성, 시스템 연동 등 다양한 기능을 인간의 개입 없이 자연스럽게 연결하는 것이 핵심
  - 예를 들어 LLM이 사용자의 질문을 이해하고 검색 시스템을 활용하여 관련 정보를 수집·요약·분석한 후 정형화된 보고서를 작성하는 일련의 과정을 자동으로 수행할 수 있음

[그림 3] AI 오케스트레이션 개념도



자료: 샌드버드(Sendbird), 연구자 재구성

- 최근 AI 오케스트레이션이 핵심 트렌드로 부상하는 것은 AI 기술을 유기적으로 결합해 복잡한 문제를 해결하고 업무 효율을 높이려 하는 기업의 수요가 급증하고 있기 때문. 특히 AI 에이전트의 등장과 장기간 지속된 불황으로 인한 생산성 향상 요구가 맞물리며 기업의 관심이 더욱 높아지고 있음

### [참고] AI 오케스트레이션과 AI 에이전트의 차이점

○ AI 오케스트레이션은 여러 AI 에이전트 혹은 다양한 AI 시스템을 하나의 목적을 위해 유기적으로 연결하고 통합하여 전체를 효과적으로 관리하는 개념

- 단일 AI 에이전트가 아닌 다수의 에이전트와 도구를 활용해 복잡한 문제를 해결하는 전략

[표 2] AI 에이전트와 AI 오케스트레이션의 비교

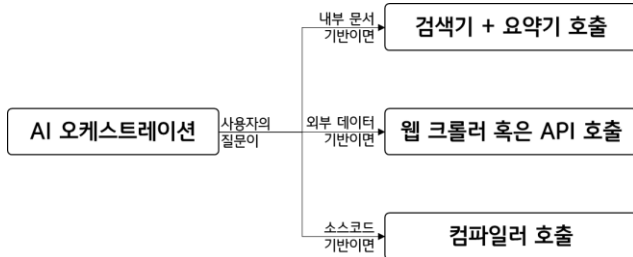
구분	AI 에이전트	AI 오케스트레이션
정의	특정 업무나 목적을 위해 자율적으로 작업을 계획하고 실행하는 단일 AI 시스템 혹은 소프트웨어	여러 AI 도구·시스템·에이전트를 통합하고 조율해 복잡한 작업을 효율적으로 수행하는 프로세스
기능 범위	주로 단일 목적에 특화되어 개별 업무를 처리	다양한 AI(에이전트, 모델, 도구 등)를 연결하고 관리해 대규모의 복합적 업무를 처리
구성 방식	단일 에이전트 혹은 챗봇 등이 여러 역할을 수행하거나 제한된 도구만을 활용	여러 에이전트와 AI 시스템이 각자 역할을 맡고, 오케스트레이터가 전체를 조율
확장성·유연성	과업의 복잡성이 증가하면 관리 및 유지보수가 어려움	새로운 AI 도구와 에이전트의 추가 및 교체가 용이하며, 대규모의 복합적 업무에 유연하게 대응 가능
예시	FAQ 챗봇, 단일 문서 요약 AI, 특정 업무 자동화 봇 등	고객 상담, 주문 관리, 물류, 데이터 분석 등 여러 AI가 협력하는 통합 고객 서비스 시스템

자료: KB경영연구소

- AI 오케스트레이션은 다양한 툴이나 모듈을 연결하고 조건에 따라 적절한 것을 선택으로 호출하는 자동화된 판단 기능은 물론, 복잡한 요청을 하위 작업으로 분류하고 순차 실행하는 다단계 실행 기능과 사용자의 대화 이력이나 업무 흐름을 기억하는 컨텍스트 유지 기능을 갖춘

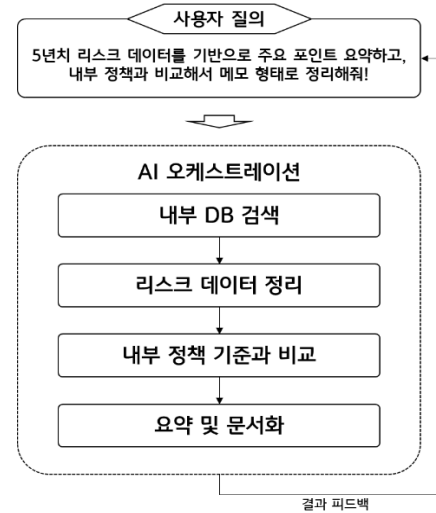
- [모듈 간 연결] LLM, 검색 툴, 분석기, 외부 API 등 다양한 AI 구성 요소를 마치 레고 블록처럼 조합해 통합적으로 관리
- [자동화된 판단] 단순한 일괄 실행이 아니라 조건에 따라 적절한 툴이나 모듈을 선택적으로 호출
- [다단계 실행] 사용자의 목적을 분석한 뒤 이를 하위 작업 단위로 분류하고 순차적으로 실행
  - 각 모듈을 연결함으로써 복잡한 작업도 단계별로 처리할 수 있음
    - 예를 들어 ‘LLM’이 사용자의 질문을 이해하고 ‘검색 시스템’을 활용해 관련 정보를 탐색하면, ‘요약 에이전트’에서 정리하고 최종적으로 ‘문서 자동 생성 에이전트’에서 결과물을 산출
    - 모듈이 연결되어 협업이 이루어짐으로써 단일 모델로는 불가능한 고차원 작업을 수행 가능

[그림 4] 자동화된 판단 흐름 예제



자료: KB경영연구소

[그림 5] 다단계 실행 예제



자료: KB경영연구소

○ **[컨텍스트 유지]** 하나의 질문에 하나의 응답을 제시하는 단순한 구조의 기존 AI 시스템은 복잡한 과정을 거쳐 결과가 도출되는 실무에서는 한계를 보이는 데 반해, AI 오케스트레이션은 사용자의 컨텍스트를 기억하여 작업 과정에 활용함으로써 이를 극복할 수 있음

- 사용자와의 대화 이력이나 워크플로우 내의 중간 상태를 기억하고 동일한 사용자 요청이라도 컨텍스트에 따라 적절히 해석
- 이전 응답 내용을 바탕으로 다음 액션을 판단
  - 예를 들어 “이 자료를 작년 기준으로 다시 정리해 줘”라고 요청할 경우, 이전에 어떤 보고서를 생성했는지 알아야 올바른 답변이 가능

■ AI 오케스트레이션은 기술적 전문성이 부족한 비즈니스 사용자가 직관적 인터페이스를 기반으로 복잡한 AI 기능을 활용할 수 있도록 지원하여 ‘AI의 민주화’를 촉진

○ 기존에는 LLM을 업무에 활용하려면 프롬프트 작성, API 호출, 코드 구성 등 일정 수준의 기술 역량이 요구되었으나, AI 오케스트레이션을 도입하면 복잡한 기술 처리 과정은 숨기고 사용자에게는 단순한 대화 인터페이스만을 제공함으로써 접근성 개선 효과를 기대할 수 있음

- **[기술적 장벽 제거]** 사용자가 더 이상 복잡한 명령어를 외우거나 API를 다룰 필요 없이 자연어로 요구 사항을 입력하면 결과가 출력되므로 비개발 부서도 AI를 일상적인 업무 도구로 활용할 수 있음

- **[직관적 인터페이스]** 사용자의 요청을 이해한 후 검색, 요약, 보고서 작성 등의 작업을 수행하기 위해 필요한 기능을 자동으로 연결 및 실행하므로 사용자는 무엇을 해야 하는지가 아니라 무엇을 원하는지 말하기만 하면 되는 구조
- **[사용자 맞춤 대응]** 콘텍스트를 저장하고 사용자 프로파일을 기반으로 작동하도록 설계되어 동일한 요청이라도 상황에 맞는 결과를 제공. 예를 들어 “최신 이슈를 정리해 줘”라는 요청에도 사용자 역할, 최근의 업무 흐름, 이전 문서 등을 반영해 개인화된 결과를 생성할 수 있음
- **[업무 프로세스 통합]** AI 기능이 기존의 업무 시스템에 통합되도록 설계되어 사용자는 인트라넷, 이메일, 문서 작성 툴 등 익숙한 플랫폼에서 자연스럽게 AI를 사용할 수 있음. 이에 따라 별도의 교육이나 플랫폼 전환 없이 AI 기능을 워크플로우에 내재화 가능

○ AI 오케스트레이션은 ‘AI를 활용하는 사람’의 범위를 확장하여 모든 조직 구성원이 AI와 협업할 수 있는 기반을 마련해 줌

- 복잡한 기술 처리 과정을 사용자 눈에 보이지 않도록 추상화함으로써 누구나 AI의 도움을 받을 수 있는 환경을 구현. 이는 AI를 활용해 조직 전체의 생산성과 디지털 역량을 향상하는 핵심 전략이 될 수 있음

### 3. MCP와 AI 오케스트레이션

■ AI 오케스트레이션에서 ‘모델 콘텍스트 프로토콜(Model Context Protocol, MCP)’은 AI 모델과 데이터 소스 및 도구 간의 상호작용을 표준화하여 조직 내 AI 접근성과 활용성을 크게 향상시키는 핵심 요소로 부상

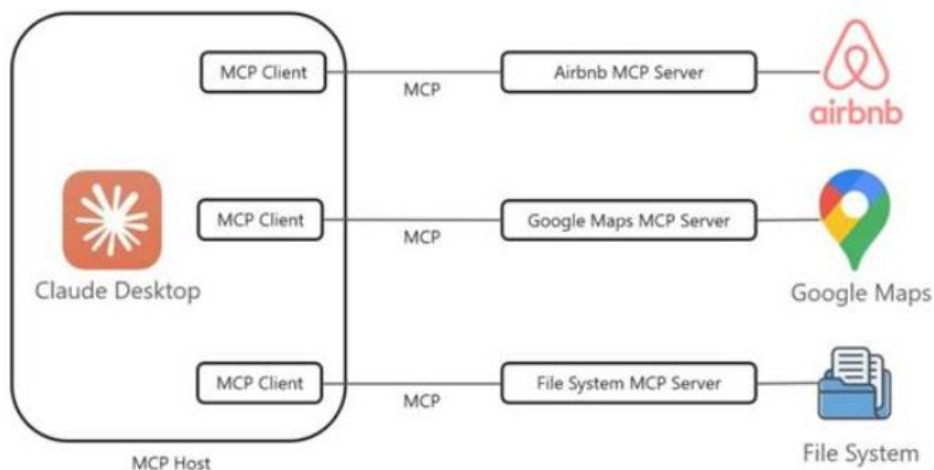
○ MCP는 LLM이 검색·데이터베이스·연산 등 외부 도구를 상황에 맞게 선택적으로 호출하고 연동할 수 있도록 도와주는 에이전트 인터페이스 프로토콜로, 앤트로픽이 2024년 11월 오픈소스로 공개

- USB-C 포트가 다양한 기기를 하나의 표준 단자로 연결하듯이 LLM과 콘텐츠 저장소, 비즈니스 애플리케이션, 개발 도구 등 여러 시스템을 단일한 방식으로 연결
- 이처럼 기존의 각기 다른 API 및 플러그인 방식을 통합해 AI 시스템이 필요한 콘텍스트와 데이터를 원활히 얻을 수 있게 함으로써 LLM이 ‘지능형 오케스트레이터’로서 기능할 수 있게 해줌
  - 특히 금융, 법률, 컨설팅과 같이 연속적 해석과 판단이 중요한 도메인<sup>13</sup>에서는 MCP가 없으면 실질적인 자동화가 어려움

<sup>13</sup> IT 및 AI 분야에서는 특정 데이터 소스나 모델이 작동하는 환경, 혹은 의료·금융·법률과 같은 산업·업무 분야를

- 복잡한 업무 요청도 AI가 자체적으로 판단하여 최적의 도구를 적절히 조합
  - 기존 LLM API는 단순한 질의응답 구조이기 때문에 컨텍스트 유지가 어렵고 업무 연속성이 낮다는 문제점을 안고 있는데, MCP를 적용하면 마치 업무 도우미처럼 AI가 일관된 컨텍스트로 업무 수행을 보조
    - MCP 개발 전에는 추가 도구를 활용해 컨텍스트 관리를 일부 지원했으나 개발과 유지보수가 어렵다는 단점이 존재
- 사용자가 엔트로픽의 클로드에 휴가 일정과 원하는 지역을 입력하고 사용자의 선호도를 감안해 최적의 여행 일정과 숙소를 검색해 제시해달라고 요청한 경우, MCP를 통한 AI는 3단계로 동작
- [1단계] AI 모델이 공항에서 숙소까지 거리와 예상 소요 시간 확인 등 외부 데이터가 필요함을 인식하고 MCP 클라이언트를 통해 구글 맵과 같은 적절한 MCP 서버에 접근 권한을 요청
  - [2단계] 사용자의 접근 권한 승인을 받아 MCP 표준 형식으로 요청을 전달하면, 서버는 구글 맵과 같은 외부 시스템에서 데이터를 가져와 포맷된 결과를 반환
  - [3단계] AI 모델은 이 정보를 받아 대화 컨텍스트에 통합하고 최종 응답을 생성

[그림 6] MCP를 통한 AI 모델-도구 상호작용 예시



자료: 《MIT 테크놀로지 리뷰(MIT Technology Review)》

- MCP는 개방성과 실용성이 결합된 기술 설계, 주요 기업의 전략적 선택, 복잡한 업무 환경 수용력이 결합되어 구현되며, AI 연결성 혁명을 이끄는 사실상의 기술 표준(De facto standard)으로 자리매김

의미하기도 함. 이 경우 해당 데이터의 특성, 분포, 컨텍스트를 포함하는 개념으로 사용됨

- 오픈AI, 마이크로소프트, 구글, 아마존 등이 자체 프로토콜 대신 MCP 도입을 선언하는 등 MCP는 기술적 우위성을 앞세워 주요 AI 기업과 플랫폼에서 채택되고 있음

[표 3] MCP 채택 기업

주요 기업	채택 사례
마이크로소프트	2025년 3월 19일, 코파일럿 스튜디오(Copilot Studio) 등에서 MCP 지원
오픈 AI	2025년 3월 27일, 자사의 에이전트 SDK에서 MCP 지원
아마존	2025년 4월 2일, 아마존웹서비스(AWS)에서 MCP 지원 발표
구글	2025년 4월 10일, 제미나이 SDK에서 MCP 지원 발표
네이버	MCP 지원 예정

자료: 《이데일리》

○ MCP의 핵심 기능은 여러 AI 시스템과 서비스를 중앙에서 통합 관리하며 리소스 할당, 워크플로우 관리, 정책 시행을 조정하는 데 있음

- **[컨텍스트 저장 및 공유]** 사용자의 입력, 이전 대화 내용, 실행 결과 등 다양한 정보 조각을 구조화된 형태로 저장한 후 호출되는 LLM이나 외부 도구에 해당 컨텍스트를 공유하여 중단 없는 의사결정 흐름을 구현
- **[에이전트 간 컨텍스트 연계]** 검색 시스템, 분석 에이전트, 요약 에이전트 등 복수의 AI 에이전트가 순차적으로 호출될 때 단계별 상태 정보를 넘겨받아 컨텍스트를 유지
- **[프롬프트 설계 자동화 및 일관성 확보]** 컨텍스트 정보를 기반으로 LLM 프롬프트를 자동 생성하거나 갱신함으로써 사용자 경험의 일관성을 확보
- **[의사결정 흐름 관리]** 사용자의 요청에 따라 필요한 AI 에이전트를 자동으로 호출하고 상황에 따라 다르게 흐름을 전환하여 복수의 모델과 시스템 간 실시간 연동 및 조건 기반 분기 실행<sup>14</sup> 자동화를 구현
- **[도구 선택 및 호출]** 질의에 따라 검색, 계산, 문서 조회, 모델 실행 등 필요한 외부 기능을 선택적으로 호출
- **[양방향 통신]** AI 모델과 데이터 소스 간의 양방향 통신을 통해 지속적으로 연결된 상태에서 정보 교환을 가능하게 함으로써 더 복잡하고 상호작용이 필요한 작업 처리를 지원

○ 기존 워크플로우 기반 AI 오케스트레이션이 사전 정의된 순차적 프로세스에 따라 각 AI 시스템이 독립적으로 작동하는 반면, MCP 기반 오케스트레이션은 중앙집중식 제어 엔진이 모든 AI 시스템을 통합 관리하고 실시간으로 리소스와 작업을 조정

<sup>14</sup> 조건에 따라 프로그램의 실행 순서를 변경해 다른 명령을 실행할 수 있게 하는 기능

- 워크플로우 방식이 정해진 규칙에 따른 제한적 의사결정과 분절된 시스템 관리에 중점을 둔다면, MCP 방식은 상황 인식 기반의 동적 의사결정과 시스템 간 유기적 연계를 통해 보다 높은 효율성과 유연성을 제공
  - 전통적 오케스트레이션의 대표적인 예인 아파치 에어플로우(Apache Airflow)는 배치 작업 오케스트레이션<sup>15</sup>으로, 정해진 순서에 따라 명령어를 실행하며 컨텍스트 인식이나 실시간 사용자 요청에 대한 대응은 불가능
  - 또 다른 예로 쿠브플로우 파이프라인(Kubeflow Pipelines)은 AI 모델 학습 및 서빙 워크플로우를 쿠버네티스(Kubernetes)<sup>16</sup> 기반으로 관리하는 오케스트레이션으로, 반복적인 AI 실험에는 적합하나 유저-LLM-도구 상호작용 기반은 아님

[표 4] 전통적 오케스트레이션과의 차이점

구분	전통적 오케스트레이션	MCP 기반 AI 오케스트레이션
중심 대상	데이터 파이프라인·배치 작업	사용자 요청·LLM 중심 워크플로우
흐름 설계	사용자가 명시적으로 구성	사용자 입력을 기반으로 모델이 동적으로 판단
도구 호출	미리 연결된 API 고정	필요에 따라 유연하게 호출
컨텍스트 처리	상태 없음 혹은 배치 단위로 제한적	사용자·세션 중심의 컨텍스트 지속성 유지
상호 작용	없음(자동 스케줄 위주)	인간과 AI 간 실시간 상호작용 가능
확장성	유지보수 비용이 많이 듦	기능 추가 및 연동 용이

자료: KB경영연구소

## 4. AI 오케스트레이션 도입 로드맵

### ■ 조직 차원에서 AI 오케스트레이션을 효과적으로 도입하려면 전략·문화-인프라-파일럿-확산-개선의 흐름으로 이어지는 체계적인 단계별 접근 로드맵이 필요

○ [①전략 수립 및 목표 정의] 경영진의 적극적인 지원하에 AI 오케스트레이션의 비전과 목표를 명확히 설정

- 비즈니스 전략과 연계한 AI 활용 로드맵을 구축하여 AI 오케스트레이션을 통해 어떤 가치(비용 절감, 매출 향상, 고객 만족 등)를 창출할 것인지 정의

<sup>15</sup> 여러 배치 작업(일괄 처리 작업)을 조율·예약·실행하고 모니터링하는 프로세스로, 대규모 데이터 처리나 정기적인 시스템 작업이 필요한 기업 환경에서 핵심적 역할을 함

<sup>16</sup> 실행에 필요한 모든 파일을 포함한 전체 실행(runtime) 환경에서 애플리케이션을 패키징하고 격리할 수 있는 기술인 ‘컨테이너’를 활용한 애플리케이션의 배포·확장·관리를 자동화하는 오픈소스 오케스트레이션 플랫폼

- 이때 전사적 핵심 과제 중 AI로 재구상할 도메인과 업무 우선순위를 선정하는 것이 중요. 예를 들어 은행이라면 대출 심사, 고객 분석, 콜센터 등 파급 효과가 큰 영역부터 AI 오케스트레이션 적용 범위를 설정
    - 조직 내 AI 활용 수요 및 업무별 반복성과 데이터 접근성 평가
    - AI 오케스트레이션이 필요한 ‘반복적인 지식 기반의 업무’(리스크 리포트 작성, 법규 요약, 고객 FAQ 대응 등) 도출
  - 보안, 컴플라이언스, 개인정보 보호 등 기술적·법적 제약 사항을 진단하고 추후 성과 측정을 위한 핵심성과지표(KPI)를 수립
  - AI 오케스트레이션의 도입은 단순 기술 도입이 아닌 업무 방식의 혁신이므로, 초기부터 구성원과 프로세스 측면의 변화관리 계획을 함께 수립하는 것이 바람직
- [②데이터 및 기술 인프라 구축] AI 오케스트레이션의 기반이 되는 데이터 인프라와 플랫폼을 구축. 이때 향후 여러 AI 모델과 API를 한데 묶어 관리할 통합 아키텍처를 설계하는 것이 중요
- 데이터웨어하우스 구축, 데이터 정제 및 통합을 통해 조직의 데이터 자산을 활용하기 쉽게 구조화
  - 다양한 내외부 데이터 소스가 실시간으로 AI 모델에 공급되도록 데이터 파이프라인을 자동화하고 AI 모델 학습용 환경을 정비
  - 상용 솔루션 도입 혹은 내부 개발 등 목적에 맞는 오케스트레이션 플랫폼을 선정
  - 보안 및 거버넌스 요건을 충족시키기 위해 데이터 암호화, 접근 제어, 로그 감사 등 보안 체계를 인프라 구축 단계에서부터 반영
- [③최소 기능 제품(Minimum Viable Product, MVP) 구축 및 실험] 앞서 선정된 우선순위 업무 중 하나를 골라 파일럿 프로젝트를 수행
- LLM, 벡터 데이터베이스<sup>17</sup>, 검색 API와 간단한 인터페이스를 조합하고 핵심 기능에 집중한 소규모의 AI 오케스트레이션 환경을 설계
    - 예를 들어 콜센터 업무 혁신을 목표로 설정했다면 음성인식 AI, 상담 내용 요약 AI, 상담사 지원 챗봇 등을 오케스트레이션하여 콜센터 AI 어시스턴트를 개발
  - 프롬프트 최적화와 워크플로우 단순화 실험을 진행한 후 실사용자 피드백 수집 및 개선을 반복

<sup>17</sup> 데이터 객체의 수치적 표현인 벡터 형태로 정보를 저장하는 데이터베이스

- 파일럿 프로젝트의 목적은 조기에 가시적인 성공 사례를 만드는 것이므로, 처리 속도 20% 향상 등과 같은 명확한 목표 지표를 정하고 실행 결과를 계량적으로 평가하여 프로젝트의 성과를 입증
  - 파일럿 프로젝트 단계에서는 교차기능팀(Cross Function Team)을 구성하는 것이 중요
    - 현업 부서의 도메인 전문가, 데이터 사이언티스트, ML 엔지니어, IT 운영 담당자 등이 한 팀이 되어 업무 프로세스에 AI를 적용하는 흐름을 함께 설계
- [④전사 확산 및 스케일업] 파일럿 프로젝트를 통해 검증된 솔루션이나 교훈을 바탕으로 AI 오케스트레이션을 조직 전반으로 확산
- 파일럿 프로젝트 대상 업무를 정교화하여 본격적인 프로덕션 시스템으로 배포하고, 해당 분야에 AI 에이전트와 자동화 기능을 완전히 내재화하는 동시에 다른 우선순위 업무로 적용 범위를 넓혀 나감
    - 파일럿 프로젝트 결과를 바탕으로 부서별 요구 사항을 커스터마이징하고 고객 대응용, 규제 해석용, 회의록 요약용 등 업무별 워크플로우를 템플릿화
    - 데이터 흐름 · API 호출 · 모델 응답 검증 프로세스 설계 등의 거버넌스 및 보안 체계를 수립
    - 사내 메신저, 그룹웨어, 문서 시스템 연결 등 전사 업무 시스템과 통합
  - 전사 거버넌스 체계를 작동하여 표준화된 원칙과 모범 사례를 공유함으로써 중복 투자를 막고 모델 · 툴의 호환성과 일관성을 유지
  - 프롬프트 엔지니어링, 툴 체인 구성 등에 대한 조직 내부 교육과 변화 관리를 지속하여 새로운 AI 도구의 업무를 실제 업무에 활용하도록 유도하고 사용률을 제고
- [⑤지속적인 모니터링 및 개선] 도입된 AI 오케스트레이션이 최적의 성능을 발휘할 수 있도록 지속적으로 모니터링하고 개선
- 다수의 AI 모델과 시스템이 유기적으로 작동해야 하므로 개별 구성 요소의 성능 추적과 오류 대응 체계는 필수적
  - 사용 로그, 응답 품질, 오류 케이스 수집 등 지속적인 모니터링 체계를 수립
    - AI 모델의 정확도 저하나 데이터 드리프트<sup>18</sup>를 감지하기 위한 모니터링 대시보드를 운영하고, 성능 리포트와 경고 시스템을 구축

<sup>18</sup> 머신러닝 모델을 트레이닝하는 데 사용되는 입력 데이터의 통계적 속성이 시간이 경과함에 따라 변하는 현상. 예를

- 주기적으로 AI 모델의 재학습과 튜닝을 수행하고, AI 기술 개선 속도에 맞춰 구성 요소를 교체하거나 추가하여 최신 상태로 고도화
- 사용자 피드백 루프를 만들어 현업 부서가 제안하는 개선점을 반영하고, 필요 시에는 인증 절차나 권한 관리 등을 조정하는 거버넌스 업데이트도 병행
- 보안 측면에서는 정기적인 취약점 점검과 개인정보 보호 조치를 지속적으로 강화

## 5. 향후 전망 및 시사점

### ■ AI 오케스트레이션은 향후 기업의 AI 활용도를 획기적으로 높이고 업무 방식을 재편할 핵심 기술로 자리매김할 전망

○ 기업의 생산성 향상과 비용 효율성 개선에 중요한 역할을 수행하면서 관련 시장도 빠르게 성장할 전망

- 스와미 시바수브라마니안(Swami Sivasubramanian) 아마존웹서비스 AI 및 데이터 담당 부사장은 “임원들이 AI 사용 비용을 신경 쓰기 시작하는 만큼 2025년은 생산성을 증명하는 해가 될 것”이라며, “AI 오케스트레이션은 AI 에이전트를 최적화해 정확성과 생산성을 5배 높이는 방법에 대한 해결책”이라 강조
- 시장조사기관 얼라이드 마켓 리서치(AMR)에 따르면, 글로벌 AI 오케스트레이션 시장의 규모는 2031년까지 연평균 21.5% 성장하여 약 352억 달러에 이를 전망

### ■ [AI가 ‘당연한 도구’가 되는 시대] 기존에는 개별 부서에서 산발적으로 AI를 적용하는 수준에 그쳤다면, 향후에는 조직 구성원 모두가 일상적으로 AI를 활용하는 환경이 보편화될 전망

○ AI 오케스트레이션을 통해 데이터와 AI 모델이 중앙에서 통합 관리되면 AI 관련 복잡한 기술을 모르는 현업 부서에서도 필요한 기능을 활용할 수 있게 됨

- 사실상 모든 직원이 AI 도구를 활용하게 되면 AI는 지금의 엑셀이나 이메일처럼 업무의 기본 툴로 인식되어 생산성 향상과 전문 역량 강화가 동시에 이루어질 것으로 기대
- 이러한 변화를 선도하기 위해 금융회사는 내부 AI 서비스 포털이나 AI 마켓 플레이스를 구축하고 조직 구성원의 AI 접근성을 극대화하는 노력이 필요

---

들어 알고리즘 트레이딩에서 과거 시장 데이터에 의해 훈련된 모델은 갑작스러운 경제 상황이나 정책 변경으로 인해 주가 및 거래 패턴의 변동이 발생하여 모델의 예측 정확도가 떨어질 수 있음. 이러한 변화는 점진적이거나 갑작스럽게 나타날 수 있으며, 고객 행동의 변화, 환경 조건의 변화, 데이터 수집 방법의 수정과 같은 다양한 요인에 의해 발생 가능

## ■ [멀티에이전트와 자율적 프로세스의 부상] AI 오케스트레이션이 발전하면 AI 에이전트들이 서로 협력하여 업무를 자율적으로 수행하는 수준에 이르게 될 전망

○ 단일 LLM 중심 구조에서 다중 AI 에이전트 구조로 전환이 진행 중인 가운데, 에이전트 간 협업을 통한 자율적 판단 및 분기 실행이 가능해짐

- 현재는 주로 사용자가 정한 흐름에 따라 각 모델의 기능별 협업이 이뤄지나, 향후에는 상위 오케스트레이션 AI가 스스로 계획을 세워 관련 에이전트를 호출하고 업무를 완수하는 자율적 AI 오케스트레이터가 등장할 가능성이 높음
  - 맥킨지앤컴퍼니에 따르면, 궁극적으로 행동 계획 수립, 의사결정, 다른 툴·에이전트 활용까지 자율적으로 수행하는 방향으로 진화할 전망
  - 예를 들어 금융업의 경우 기업대출 상담이 접수되면 ‘AI 딜 매니저’가 서류 수집 에이전트, 신용평가 에이전트, 담보평가 에이전트 등을 호출해 프로세스를 진행하고, 인간 직원은 최종 승인만 하는 고도의 자동화를 실현 가능

○ 금융회사 입장에서 AI 오케스트레이션의 진화는 업무 프로세스 설계 패러다임의 전환을 의미하며, 이러한 지능형 프로세스 자동화가 가져올 혁신에 대비해 테스트베드 마련과 내부 역량 강화를 서둘러야 할 것임

- 규칙 기반 로봇 프로세스 자동화(RPA)를 넘어 AI 기반 자동 의사결정이 가능해지므로 업무 프로세스를 고객 맞춤형으로 보다 유연하게 재구성할 수 있음
  - 예를 들어 대출심사 프로세스의 경우 획일적 기준이 아니라 AI가 자체 판단하여 필요한 경우 일부 단계를 건너뛰고 고객에게 다른 경로를 제시하는 등 유연한 프로세스 구현이 가능해짐

[표 5] 실제 활용 시나리오

부서	활용 사례	설명
고객센터	LLM 과 고객 데이터베이스 연동 상담	고객 질문을 분석하여 MCP 가 필요한 도구(DB 조회, 규정 검색 등)를 호출한 후 답변을 생성
리스크 관리	모델 결과 해석 도우미	AI 모델이 산출한 복잡한 결과를 LLM 이 자연어로 설명
WM·자산관리	포트폴리오 설명 및 비교	투자자의 포트폴리오를 분석해 MCP 가 필요한 도구를 활용하여 맞춤형 설명을 제공
마케팅	타겟 고객별 문구 생성	LLM 이 타겟 고객에게 적합한 이메일 및 메시지 문구를 자동 생성

자료: KB경영연구소

■ [맞춤형 서비스를 통한 경쟁력 강화] 단편적 AI 활용이 아닌 전사적 AI 통합 운영은 향후 고객 서비스 혁신과 내부 효율화, 리스크 관리 고도화의 필수 요건으로, 금융권의 경쟁 구도 재편의 동인이 될 전망

- 금융권에서 AI 오케스트레이션 활용이 성숙 단계에 접어들면, 고객에게 보다 개인화되고 일관된 경험을 제공 가능
  - AI들이 여러 채널과 접점에서 수집된 고객 데이터를 통합하여 이를 기반으로 실시간으로 최적의 상품 추천이나 의사소통 전략을 도출 가능
- AI 통합 활용은 매출 성장과 고객 서비스 혁신으로 직결되어 AI를 효과적으로 조율하여 활용하는 금융회사는 그렇지 않은 경쟁사 대비 비용 구조와 고객 만족도 면에서 크게 앞서나갈 수 있음
  - 예를 들어 24시간, 주 7일 무중단 운영이 가능한 AI 에이전트를 적재적소에 배치해 운영 탄력성과 비용 효율성 향상을 도모할 수 있음
- 혁신적인 빅테크나 핀테크 기업, 대형 IT 기업이 우수한 AI 오케스트레이션 능력을 앞세워 금융 서비스 영역을 침투할 것을 대비해 전통적 금융회사는 디지털 경쟁력 확보 차원에서 AI 오케스트레이션 역량 확보가 필수
- 업무 특성과 리스크 기준에 따라 커스터마이징된 AI 에이전트 및 워크플로우 설계 역량이 기업 경쟁력으로 연결될 것으로 예상되면서 금융 특화 AI 오케스트레이션 프레임워크의 조기 개발 및 내재화가 전략적 우선 과제로 부상
  - 금융권은 고유한 규제 및 보안 요건과 도메인 특성으로 인해 일반적인 AI 오케스트레이션 구조만으로는 실질적인 적용에 한계가 존재
    - 예를 들어 민감한 고객 정보 보호, 실시간 리스크 판단, 컴플라이언스 이슈 등은 AI 오케스트레이션 구조 설계 단계부터 금융 환경에 최적화된 아키텍처를 요구
  - 데이터는 비정형 문서와 정형 데이터가 혼합된 형태로 존재하며 업무 또한 규정 해석, 투자 보고서 작성, 내부 정책 비교 등 다단계 분석과 판단이 요구되는 복합적인 작업이 다수
    - 도메인 지식 기반의 콘텍스트 유지 구조, 내부 규정 연동 모듈, 보안 감사 기능이 통합된 금융 특화 AI 오케스트레이션 구조가 필요

■ AI 오케스트레이션을 기업에 성공적으로 안착시키기 위해서는 도입 시 기술적 이슈뿐만 아니라 조직 문화, 데이터 인프라, 거버넌스 등 다양한 요소를 종합적으로 고려해야 함

○ 전사적 AI 활용을 위해서는 AI 오케스트레이션 전략 수립이 선행되어야 하며, AI 도입 초기부터 AI 오케스트레이션 전략 적용을 검토할 필요

- AI가 파일럿 수준의 기술 시연에 머무르지 않고 조직 전체로 확산하기 위해서는 다양한 AI 구성 요소를 통합하고 업무 흐름에 자연스럽게 연결하는 AI 오케스트레이션 체계 구축이 선행되어야 함

- AI 오케스트레이션을 활용하지 않고 LLM만 도입할 경우, 부서 간 AI 활용 역량 격차가 확대되고 기술 낭비로 이어질 수 있으며 전사적 AI 생산성 향상을 기대하기 어려움

- AI 프로젝트 초기 단계에서부터 단순 모델 테스트와 별도로 “이 모델이 어떤 업무 흐름 속에서 어떤 톨과 연계될 것인가”의 관점에서 AI 오케스트레이션 설계가 필요

- 이는 추후 전사적 확산 시 발생할 수 있는 재설계 비용과 중복 개발을 최소화하며 업무 자동화 체계로의 자연스러운 확장을 지원

○ AI 오케스트레이션 전략은 현업 부서의 접근성과 활용성을 높이는 데 초점을 맞춰 수립해야 함

- AI 오케스트레이션은 기술 도입 자체보다 실무에서 얼마나 쉽게, 반복적으로 활용하는지가 성공의 핵심인 만큼, 초기 전략 수립 시 기능의 완성도보다는 직관적 사용성과 반복 가능성에 초점을 맞춘 설계가 요구됨

- 고도화된 시스템보다는 작고 단순하더라도 실사용 빈도가 높은 기능부터 우선적으로 도입하고 점진적으로 확장하는 것이 효과적

- 기존의 기술 중심 접근에서 사용자 경험(UX) 중심 접근으로의 전환이 필요

- 자주 쓰일수록 사용자 피드백과 데이터가 쌓여 개선의 여지가 명확해지고 유지보수가 용이

○ 현업 부서와 기술 팀 간의 원활한 협업 문화도 뒷받침되어야 함

- 데이터 팀은 AI가 활용할 수 있는 내부 지식 구조와 벡터 데이터베이스 설계를 담당하고, IT 운영 팀은 API 연동과 실행 환경을 구축하며, 컴플라이언스 팀은 개인정보 보호 및 규제 준수 가이드라인을 제공하는 등 다양한 부서 간의 유기적 협업을 이끌어내는 것이 중요

- AI 오케스트레이션을 실질적인 업무 프로세스에 반영하려면 현업 부서 업무 흐름을 가장 잘 아는 담당자와 이를 구현할 수 있는 기술 인력 간의 유기적 협업이 필요

- 단순 인터뷰나 요건 수집이 아니라 워크플로우 단계별로 참여 기반의 공동 설계가 필요

<연구위원 최승우(sw.choi@kbf.com) ☎2073-5709>

### <참고문헌>

#### [국내 문헌]

- 대한상공회의소, 2024.8.29, “국내 기업 AI 기술 활용 실태 조사”.
- IBM, 2025.1.23, “AI 오케스트레이션이란 무엇인가요?”.
- 브런치스토리, 2024.6.29, “AI의 성공적 도입을 위한 조직관리”.
- 《디지털 투데이》, 2025.4.9, “적과의 동침도?...AI 에이전트 기술 'MCP' 겨냥 연대 확산”.
- 《이데일리》, 2025.4.13, “AI의 손발이 생겼다... MCP, 차세대 AI 연결 표준으로 부상”.
- 《테크데일리》, 2024.8.13, “금융권 망분리 규제 완화 개인정보 활용 확대...생성형 AI도 허용”.
- 《튜링포스트코리아》, 2025.3.21, “FOD#92: 'AI 오케스트레이션'의 해 - 개발자 커뮤니티를 향한 오픈AI와 앤쓰로픽”.
- 《ZDNet Korea》, 2025.1.1, “'AI와 AI가 협업하는 시대'...새해 핵심 트렌드 'AI 오케스트레이션’”.

#### [해외 문헌]

- BCG, 2024.10.24, “AI Adoption in 2024: 74% of Companies Struggle to Achieve and Scale Value”.
- Conor Bronsdon, 2025.2.7, “How MMLU Benchmarks Test the Limits of AI Language Models”.
- Ian Heining, 2025.2.5, “AI orchestration: A beginner’s guide for 2025”.
- IBM, 2025.2.14, “The 5 biggest AI adoption challenges for 2025”.
- Lang Wang, 2025.3.30, “Is MCP Set to Revolutionize AI Integration? Navigating Developer Hurdles and Investor Opportunities”.
- Stanford University, 2025.4.8, “AI Index Report 2025”.
- Zankar Desai, 2025.3.19, “Introducing Model Context Protocol (MCP) in Copilot Studio: Simplified Integration with AI Apps and Agents”.

#### [홈페이지]

- GPQA Benchmark, 검색일: 2025년 4월 13일,  
<https://www.vals.ai/benchmarks/gpqa-04-04-2025>
- SWE-bench, 검색일: 2025년 4월 13일,  
<https://www.swebench.com/#test>