3장

기하급수적 가치 창출을 위한 AI 에이전트 오케스트레이션

자율형 AI 에이전트 확산으로 기업 환경은 단일 에이전트 활용을 넘어, 멀티 에이전트를 연결·조율하는 오케스트레이션 역량이 성과를 좌우하는 단계로 진입하고 있다. 이에 따라 기업은 기존 업무에 AI를 덧붙이는 수준을 넘어, 인간–AI 협업 구조와 조직 역할을 재정의하고, 에이전트 중심의 프로세스로 전환해야 한다. 이 과정에서 3계층 기술 아키텍처, 통신 표준, 통제 인프라를 포함한 기술 기반과 함께, 소유권·책임·성과 측정이 명확한 거버넌스 설계가 AI 오케스트레이션 경쟁력의 핵심으로 부상하고 있다.

핵심 내용 요약 (Executive Summary)

왜 오케스트레이션이 핵심이 되는가

- 자율형 AI 에이전트가 기업 내 다양한 역할을 수행하며 멀티 에이전트 환경이 빠르게 확산
- 개별 에이전트 성능보다 여러 에이전트를 연결·조율하는 오케스트레이션 역량이 성과를 좌우
- AI 에이전트 오케스트레이션 시장은 2026년 85억 달러 → 2030년 350~450억 달러로 급성장 전망

(도입 전략과 조직의 변화) 단일 목적 에이전트에서 멀티 에이전트 시스템으로의 전환이 필수

- 기존 업무에 1)AI 에이전트를 덧붙이는 방식, 2)처음부터 AI 에이전틱 전제의 신규 설계, 3)프로세스 재설계 등 다양한 접근법 존재
- 직원 역할은 AI 사용자 → 에이전트 설계·조율·감독자(오케스트레이터)로 진화

(기술 인프라와 통제 메커니즘) 멀티 에이전트 확장을 위해 3계층 아키텍처가 필수

- ① 컨텍스트 계층: 지식, 데이터 → ② 온톨로지 에이전트 계층: 모듈화, 보안, 관측 가능성 → ③ 경험 계층: UI, 설명 가능성, 복구·되돌림
- 관리 플랫폼, 텔레메트리, 가드레일, 가디언 에이전트 등과 같은 통제 인프라가 전제 조건

(비즈니스 프로세스와 거버넌스 재설계) 업무의 모듈화와 에이전트 중심 프로세스 재편 필요

- 에이전트의 의사결정에 대한 소유권·책임 소재 명확화가 핵심 이슈
- 지속적 개선을 위한 설계 전략, 거버넌스·성과 측정 체계 구축이 경쟁력의 핵심

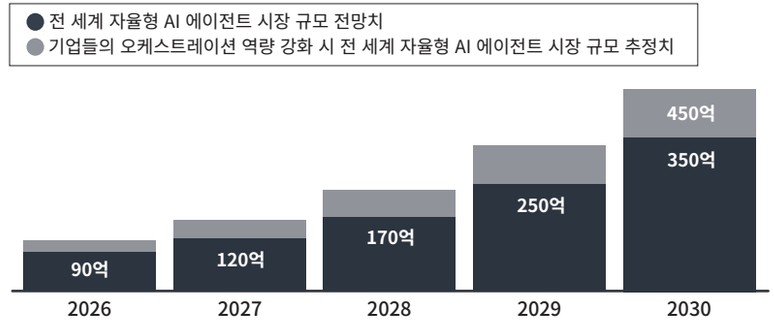
지능형 자동화를 위해서는 각기 다른 자율형 AI 에이전트 상호간 연결과 조율이 핵심이다. 에이전트간 협업을 가능하게 하는 오픈소스와 독점(proprietary) 통신규격(protocol)은 차세대 AI 자동화 생태계 내 주도권 경쟁을 좌우할 핵심 요소다.

다양한 AI 추론 엔진이 영역을 넘나들며 유기적으로 상호작용하는 멀티 에이전트 시스템이 확산하고 있다. 이에 따라 역할별 에이전트를 효과적으로 조율하는 에이전트 오케스트레이션(agent orchestration)의 중요성이 한층 부각되고 있다. 정교한 오케스트레이션은 멀티 에이전트 시스템이 사용자 요청을 해석하고, 업무 흐름을 설계하며, 작업을 위임 및 조정하고, 결과를 지속적으로 검증 및 개선하는 지능형 워크플로를 구현하기 위해 가장 중요하다.[1] 반대로 에이전트 조율 체계가 미흡할 경우, 멀티 에이전트가 지닌 잠재적 비즈니스 가치를 충분히 실현하기 어렵다.

시장 전망에 따르면 자율형 AI 에이전트 시장은 2026년 85억 달러까지 성장한 후 2030년에는 350억 달러 규모로 더욱 급격히 성장할 것으로 추산된다(그림 1).[2] 딜로이트는 기업들이 에이전트 오케스트레이션 역량을 정교화, 고도화하고, 이에 수반되는 과제와 리스크를 선제적으로 관리할 경우 시장 규모가 2030년까지 15~30% 추가 확대돼 최대 450억 달러까지 성장할 수 있다고 내다보고 있다. 그러나 한편에서는 현재 진행 중인 에이전틱 AI 프로젝트의 40% 이상이 예상치 못한 비용 부담, 확장 복잡성, 예기치 않은 리스크 등으로 인해 2027년 이전에 중단될 가능성도 제기된다.[3] 하지만 이러한 프로젝트는 잠재적 위험 요소를 사전에 해소할 경우 기업의 매출 성장을 크게 견인할 수 있는 기회 요인이 될 수 있다. 따라서 선제 대응이 무엇보다 중요하다.

그림 1
기업들의 에이전트 오케스트레이션 역량 강화되면서 AI 에이전트 시장 확대 전망

(단위: 미달러)



참조: 모든 수치는 반올림 수치임.
출처: Deloitte analysis.

멀티 에이전트 시스템의 잠재력을 온전히 실현하기 위해 기업은 에이전트가 어느 수준까지 자율적으로 작동할 것인지에 대한 명확한 기준을 설정해야 한다. 상당수 기업이 가까운 시점에 이러한 기준을 본격적으로 수립하고 조율하기 시작할 것으로 전망된다. 동시에 에이전트간 상호운용성과 관리 역량을 핵심 전략 요소로 삼고, 이에 맞춰 업무 프로세스와 인재 운영 체계를 실질적으로 개편해야 멀티 에이전트 시대의 주도권을 확보할 수 있다.

멀티 에이전트 시스템을 기업 환경에 안착시키기 위한 지침

기업들이 에이전트 오케스트레이션을 강화하기 위한 본격적 의사결정을 추진하는 과정에서 다음의 세 가지 핵심 지침을 따르는 것이 바람직하다.

1. 단일 목적 에이전트에서 멀티 에이전트 시스템으로 전환

현재 기업은 특정 업무에 특화된 단일 목적 AI 에이전트를 활용해 여러 단계를 자율적으로 수행할 수 있는 수준에 이르렀다.[4] 그러나 최근 들어 에이전틱 AI는 단일 에이전트를 넘어 멀티 에이전트 시스템을 통해 훨씬 더 광범위하고 폭발적인 기업 가치를 창출할 수 있다는 인식이 확산되고 있다.[5] 그럼에도 불구하고, 다수의 기업에서 멀티 에이전트 기술을 실제 활용하는 수준은 여전히 미흡하다.

딜로이트가 미국 내 산업 전반의 리더 약 550명을 대상으로 실시한 '2025 테크 밸류 서베이'(2025 Tech Value Survey)에 따르면, 자사 조직의 기본적인 자동화 역량이 성숙 단계에 도달했다고 평가한 응답자는 80%에 달했다. 하지만 기본 자동화와 더불어 AI 에이전트 활용 역량까지 성숙 단계에 도달했다고 응답한 비율은 28%에 그쳤다. 또한 각 전략을 추진 중인 기업 가운데 기본 자동화만을 도입한 경우 45%가 3년 이내 플러스(+) 투자수익률(ROI) 달성을 기대한 반면, 자동화와 에이전트를 병행하는 경우 동일한 기간 내 플러스 투자수익률을 기대한 비율은 12%에 불과했다.[6] 이는 에이전틱 AI가 가치 창출의 잠재력은 크지만 실제 기업 현장에서 여전히 적용하기가 어렵고 결과의 불확실성도 크다는 점을 단적으로 보여준다.

그렇다면 이러한 격차를 보다 빠르게 줄이려면 어떻게 해야 할까? 이를 위한 첫 단계로 멀티 에이전트 도입을 위한 세 가지 접근 방식에 대한 전략적 검토가 필요하다(그림 2).[7]

그림 2
업무 복잡성, 기반 워크플로, 적용 기술을 반영한 에이전틱 AI 전략 사례

지능형 가상계층 (overlay, 기존 구조에 추가 기능을 겹쳐 적용)
명확히 정립된 기존 워크플로에 AI 에이전트를 겹쳐 적용하면 빠르게 실험적 도입을 실행할 수 있다.
· **장점:** 기존 레거시 시스템을 거의 방해하지 않고 적용할 수 있다. · **단점:** 통합, 비용 관리, 데이터 보안 등과 관련해 까다로운 해결과제가 발생할 수 있다.
처음부터 에이전틱 AI를 설계
모듈형 마이크로서비스 아키텍처를 기반으로 프로세스를 재설계함으로써, 특정 워크플로에 최적화된 맞춤형 AI 에이전트를 적용할 수 있다. 그 과정에서 에이전트 기능이 내재된 서비스형 소프트웨어(SaaS) 솔루션이나 특정 기능에 특화된 마켓플레이스 기반 에이전트를 활용해 구현 속도를 높이고 복잡성을 낮출 수 있다.
· **장점:** 실행 장벽을 낮출 수 있다. · **단점:** 혁신, 보안, 규제 준수가 솔루션 제공업체의 기술력과 운영 역량에 좌우되는 문제가 발생할 수 있다.
프로세스 재설계
자동화 난이도가 높거나 리스크가 큰 최우선순위 업무의 경우, 기존 프로세스를 재설계하고 AI 에이전트를 전략적으로 도입함으로써 업무 지능화와 운영 혁신을 동시에 달성할 수 있다.
· **장점:** 새로운 혁신적 활용사례를 만들 수 있다. · **단점:** 세심한 사전 계획과 단계적 실행이 필요하다.

출처: Deloitte analysis.

2. 에이전트 오케스트레이션의 인간 계층(layer) 정립

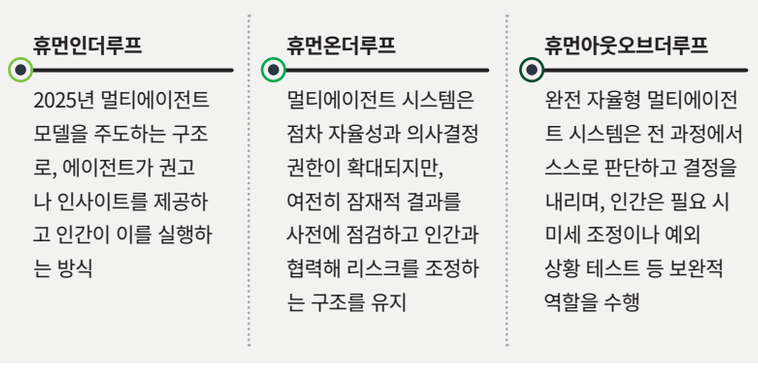
2025년 현재 기업들은 금융 투자 리서치나 중증 질환 의료 분야 등 특정 영역에서 비교적 단순하지만 실효성이 검증된 형태의 에이전트 오케스트레이션을 우선 도입하고 있다.[8] 이들 사례에서 AI 에이전트는 인간의 감독하에, 또는 별도의 '감독 에이전트'(supervisor agent)의 통제 아래 협업하며, 인간 전문가가 최종 의사결정을 내릴 수 있도록 인사이트를 제공하는 역할을 수행하고 있다. 반면 여러 사업 영역을 가로지르는 고난도·고자율 에이전트 오케스트레이션은 아직 일부 선도 기업들만 실행하고 있다.[9] 그러나 이러한 시도가 본격화될수록 기업은 에이전트의 자율성과 인간의 통제 사이에서 혁신, 리스크, 책임, 신뢰의 균형을 더욱 정교하게 조율해야 한다.

연구 결과에 따르면, 현재 멀티 에이전트 시스템은 인간이 직접 개입하는 휴먼인더루프(human in the loop) 구조에서 더 우수한 성과를 낸다. 이는 인간의 경험과 직관이 에이전트의 판단에 보완적으로 작용하며, 조직 특유의 미묘한 기대치와 의사결정 기준에 결을 맞추는 데 중요한 역할을 하기 때문이다.[10] 이에 따라 향후 12~18개월 내 휴먼인더루프 구조를 유지한 채 복잡한 에이전트 오케스트레이션의 실험적 도입을 본격 가속화하는 기업이 증가할 것으로 전망된다. 이 과정에서 기업은 의사결정의 신뢰도, 품질, 책임성을 높이기 위해, 인간의 판단을 에이전트 워크플로에 체계적으로 통합하는 프레임워크와 솔루션을 적극 도입할 가능성이 크다.[11]

아울러 업무 복잡성, 산업 특성, 워크플로 설계, 결과의 중요도에 따라 인간이 직접 개입하는 휴먼인더루프(human in the loop) 단계부터 인간이 감독만 하는 휴먼온더루프(human on the loop) 단계, 인간이 전혀 개입하지 않는 휴먼아웃오브더루프(human out of the loop) 단계까지 AI 에이전트의 자율성 스펙트럼이 점진적으로 정립될 것으로 예상된다(그림 3). 다만 인간 개입이 배제되는 방식 역시 지속적 모니터링이 반드시 필요하다. 인간이 개입 또는 감독하는 방식에서는 성과 추적, 오케스트레이션 시각화, 에이전트 활동 내역을 제공하는 플랫폼과 텔레메트리(telemetry)* 대시보드가 인간의 판단을 지원하는 핵심 인프라로 자리잡게 될 전망이다. 딜로이트는 2026년을 전후해 가장 선도적인 기업들이 휴먼온더루프 중심의 오케스트레이션 체계로 전환하기 위한 본격적인 기반 구축에 착수할 것으로 내다보고 있다.

* **텔레메트리(telemetry)**는 시스템·장비·소프트웨어의 상태와 동작 데이터를 실시간 또는 지속적으로 수집·전송·분석하는 기술과 데이터 체계를 의미한다. 사람이 직접 개입하지 않아도 자동으로 데이터를 수집하며, 지연 없이 실시간으로 상태·이상·성능을 파악하기 때문에, 관측 가능성(observability)의 핵심 구성요소로 작용한다.

그림 3
AI 에이전트 자율성의 점진적 발전 단계



출처: Deloitte analysis.

3. 산발적 AI 에이전트 확산의 통제

산발적 AI 에이전트 확산을 통제하는 것은 2026년을 기점으로 더욱 중대한 해결 과제로 부상할 전망이다. AI 에이전트는 매우 다양한 프로그래밍 언어, 프레임워크, 인프라, 통신규격을 기반으로 급속히 확산될 가능성이 크기 때문이다. 일부 에이전트는 텍스트·음성·이미지 등 다양한 정보 유형과 형식을 해석하는 멀티모달 역량과 함께 최고 수준의 지능을 구현해야 하는 복합적 과제에 직면하게 된다. 따라서 기업 내부를 넘어 디지털 인터페이스 상 에이전트간 협력 방식을 정의하는 새로운 표준을 수립하는 것이 시급한 과제로 떠올랐다. 현재로서는 미국 매사추세츠공과대학(MIT)의 '난다'(NANDA) 프로젝트와 같은 웹 기반 에이전트 통신규격 대표적 표준 사례로 꼽힌다.[12] 장기적으로는 이러한 기술 덕분에 기업 내·외부 네트워크를 아우르는 전략적 에이전트 오케스트레이션이 가능해져, 완전히 새로운 비즈니스 역량을 창출하는 기반이 될 것으로 기대된다.

이 같은 기술 환경의 변화 때문에 멀티 에이전트 상호운용성이 필수 요소이자 동시에 가장 어려운 과제로 부상하고 있다. 기업은 서로 다른 AI 에이전트를 하나의 통합 플랫폼에서 지시, 관측, 관리할 수 있는 방안을 점점 더 적극적으로 모색하게 될 가능성이 크다. 그러나 디지털 워크포스 운영에 대한 표준이 부재할 경우, AI 에이전트의 개발, 구성, 배포는 적절히 조율되지 못한 채 분산된 형태로 진행되기 쉽다. 이는 결국 성능 저하, 윤리 리스크, 사이버 보안 위협, 규제 컴플라이언스 문제 등 다양한 잠재적 위험과 비용 증가로 이어질 수 있다.

현재의 IT 및 비즈니스 아키텍처를 형성한 클라우드와 마이크로서비스 등 과거 기술 진화 과정을 되짚어 보면 이러한 과제를 해결하는 데 도움이 되는 중요한 시사점을 얻을 수 있다. 과거 인터넷 보안 통신 프로토콜 HTTPS(HyperText Transfer Protocol Secure), 데이터 교환 형식 JSON(JavaScript Object Notation) 등 표준화된 통신규격, 명확한 서비스 연동규칙(API) 설계도, 도메인 특화 마이크로서비스는 상호운용성과 안정성, 시스템 소유권을 동시에 확보하는 기반이 됐다. 또한 서비스 레지스트리, 분산 추적, 중앙 로그 시스템은 기능 탐색, 오류 해결, 서비스 관리를 획기적으로 개선했다. 여기에 거버넌스 체계, 서비스 카탈로그, '제로 트러스트'(zero trust)* 보안 모델은 시스템 안정성을 확보하고 버

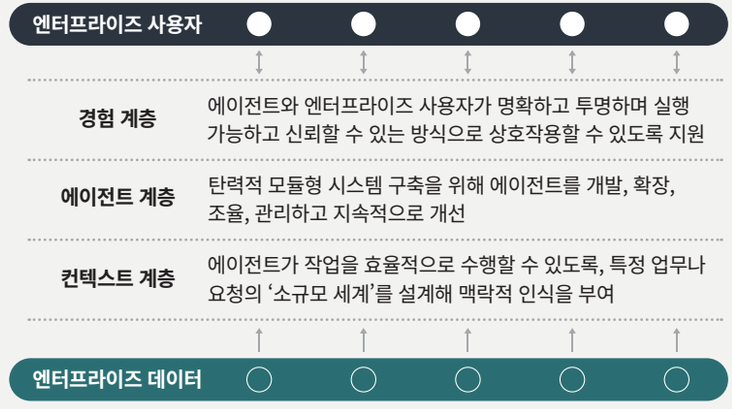
전 혼선을 방지하는 핵심 장치로 작용했다. 이러한 요소들은 회복탄력적이면서도 확장 가능한 멀티 에이전트 시스템을 구축하는 데 중요한 교훈을 제공할 수 있다.

* **제로 트러스트(zero trust)**는 내·외부를 불문하고 그 어떤 사용자·기기·시스템도 기본적으로 신뢰하지 않고, 매 접근마다 검증하는 보안 철학이자 아키텍처를 의미한다. △ 네트워크 내부라 하더라도 자동 신뢰하지 않고(never trust) △ 접속 시점뿐 아니라 사용 중에도 신원·상태·행위를 반복 검증하며(always verify) △ 필요한 만큼 필요한 시간 동안만 접근을 허용(least privilege)하는 등 3가지 핵심 원칙을 기반으로 한다.

다만 전문가들은 과거의 성공 공식을 답습하는 데 그쳐서는 안 된다고 지적한다. 멀티 에이전트 시대에는 기존 IT 아키텍처 위에 에이전트 전용의 새로운 계층을 추가하고, 이를 중심으로 업무 프로세스와 데이터, 보안, 거버넌스를 재설계하는 근본적 전환이 필요하다. 이는 AI 에이전트가 단순한 도구를 넘어 기업 운영 구조 자체를 재편하는 핵심 인프라로 진화하고 있음을 보여주는 신호로 해석된다.

회복탄력적이고 확장 가능한 멀티 에이전트 시스템을 위한 엔터프라이즈 아키텍처

그림 4



컨텍스트 계층

확장 가능한 AI 에이전트 아키텍처 구현에 핵심인 지식 엔지니어링 기반 계층이다. 컨텍스트 계층은 원천 데이터와 같이 다양한 비정형 데이터를 지식 그래프, 온톨로지, 도메인 분류 체계 등 거버넌스가 적용된 구조화된 지식 표현 형태로 변환해, 에이전트가 효과적으로 이해할 수 있는 '소규모 세계'(small world) 모델을 제공한다. 최적화된 컨텍스트 검색 기술은 에이전트가 필요한 정보를 정확하고 적시에 확보할 수 있도록 지원한다. 컨텍스트 정제(context shaping)는 불필요한 노이즈와 충돌 요소를 제거해 입력값의 품질을 높임으로써 에이전트의 정확도와 처리 효율을 동시에 향상시키는 역할을 수행한다.

에이전트 계층

컨텍스트 계층을 기반으로 실제 에이전트를 작동하는 핵심 계층으로, 안전성, 자율성, 상호운용성 등 중심 가치를 기반으로 설계된다. 에이전트 계층의 중심에는 새로운 기술을 유연하게 통합 및 확장할 수 있는 모듈형·조합형 아키텍처가 자리한다. 적합한 도구를 활용해 에이전트의 과도한 부하를 방지하며, 정교한 메모리를 활용해 사실·경험·절차 기반 기억을 균형 있게 적용함으로써 컨텍스트 인식 능력을 한층 고도화한다. 또한 에이전트 계층은 소형 특화 모델부터 대형 고성능 모델에 이르기까지 업무 성격에 맞는 최적의 AI 모델을 선택해 운용함으로써 오케스트레이션 성능을 극대화한다. 강력한 보안 체계와 고도화된 텔레메트리 기반의 관측 기능은 에이전트 활동의 보안성, 투명성, 신뢰성을 동시에 확보하는 기반으로 작용한다.

경험 계층

엔터프라이즈 사용자와 AI 에이전트를 연결하는 최전선 인터페이스 계층으로, 에이전트의 행동을 통제하고 방향을 교정하는 역할을 담당한다. 경험 계층은 에이전트의 상태 정보와 컨텍스트 데이터를 사용자에게 제공하고, 프롬프트 추천 기능과 이해하기 쉬운 결과 표시 방식을 통해 업무 검토와 의사결정을 지원한다. 또한 인간의 감독을 위한 직관적 제어 기능, 고도화된 피드백 체계, 에이전트의 사고 과정을 시각적으로 보여주는 설명 가능성 기능은 결과에 대한 투명성과 신뢰도를 크게 높이는 요소로 작용한다. 더 나아가 오류 발생이나 판단이 모호한 상황에서도 명확한 원인 설명과 복구 선택지를 제공함으로써 안정적 운영을 뒷받침하는 역할을 수행한다.

출처: Deloitte analysis.

멀티 에이전트 시스템을 조직에 안착시키기 위한 필수 요소

기업은 다음의 필수 요소를 고려해야 비즈니스 핵심 과제에 부합하는 기술적 기반을 구축할 수 있다.

1. 유연하고 확장 가능하며 안전한 통신규격

멀티 에이전트 환경에서는 에이전트 상호간뿐 아니라 에이전트와 외부 도구·플랫폼 간 표준화된 통신규격을 갖춰야 에이전트의 역량, 인사이트, 실행 결과에 대한 예측 가능한 메시지 교환이 가능해진다. 지난 1년간 구글(Google)의 A2A, 시스코(Cisco)가 주도하는 AGNTCY, 앤트로픽(Anthropic)의 MCP 등 여러 에이전트간 통신규격이 잇따라 등장하며, 서로 다른 프레임워크나 모델 위에서 구축된 에이전트간 협업 경쟁에 불이 붙었다.[13] 테크 기업들은 이 분야의 주도권을 확보하기 위해 파트너사뿐 아니라 고객사와 손잡고 생태계 구축에 속도를 내고 있다. 일부 통신규격은 금융 거래와 같은 특정 영역에서 신뢰 가능한 에이전트 상호운용성을 구현하는 방향으로 확장되고 있다.[14]

다만 통신규격간 과도한 경쟁은 자칫 특정 통신규격과 에이전트 생태계에 기업이 종속되는 '닫힌 정원'(walled garden) 구조를 초래할 수 있다.[15] 그러나 업계에서는 이르면 2026년을 기점으로 다수의 규격이 2~3개의 사실상 표준 규격으로 수렴될 가능성이 크다는 관측도 나온다. 이후 다른 테크 기업들은 경쟁력을 유지하기 위해 이들 핵심 표준에 맞춰 기술 전략을 재편할 수밖에 없을 것으로 보인다.

어떤 통신규격이 최종적으로 시장의 주도권을 확보할지는 기업의 멀티 에이전트 활용 방식, 산업 특성, 오케스트레이션 성숙도가 좌우할 전망이다. 예를 들어 표준 API와 테스트 및 시뮬레이션용 개발자 도구를 갖춘 경량 규격은 실험과 검증 단계에서 높은 효율성을 제공할 수 있다. 또한 공유 컨텍스트와 메모리를 기반으로 한 P2P(peer-to-peer)* 및 허브앤스포크(hub-and-spoke)** 방식의 에이전트 상호작용, 내장형 협상·위임·충돌 해결 기능 등을 다양한 오케스트레이션 장치로 활용할 수 있다. 더 나아가 에이전트 레지스트리를 통한 신뢰 기반 탐색과 작업 부하 분산, 비동기 메시징, 고처리량·저지연 통신, 체인형·중첩형 워크플로 지원은 대규모 에이전트 오케스트레이션의 확장을 뒷받침하는 핵심 요소로 작용한다. 또한 인증, 보안 메시징, 접근 통제 기능은 보안 리스크를 완화하는 역할을 하며, 에이전트간 메시지와 설명 정보는 감사 가능성과 오류 추적성을 확보하는 핵심 장치로 평가된다.

* **P2P(Peer-to-Peer)**는 중앙 서버를 거치지 않고, 네트워크에 참여한 각 노드(피어)가 서로 직접 연결돼 데이터·자원·서비스를 주고받는 분산형 네트워크 구조를 의미한다. 서버-클라이언트 구조가 아니라 참여자간 동등한 연결, 피어간 데이터 직접 전송 및 공유, 저장·연산·전송 부담을 네트워크 전체에 분산할 수 있다는 장점이 있다.

** **허브앤스포크(hub-and-spoke)**는 중앙의 허브(hub)가 주변에 연결된 지점, 즉 '스포크(spoke)'를 연결·조정·통제하는 구조로, 트래픽·업무·의사결정을 효율적으로 집약 및 분배하는 네트워크 모델을 의미한다. 중복을 제거하고 운영 일관성을 유지해 표준화와 효율성을 확보할 수 있는 장점이 있다.

2. 관리 플랫폼과 관측 도구

멀티 에이전트 시스템이 대규모로 확산되고 기업이 운영하는 AI 에이전트가 증가하면서, AI 에이전트가 결정을 내리고 업무를 수행하는 방식에 대한 통합적 관리와 이해가 필수 과제로 떠오르고 있다. 이를 위해 감독 기능 또는 '감독 에이전트'를 포함한 통합·확장형 오케스트레이션 플랫폼을 활용할 수 있다. 이러한 감독 에이전트는 요청 해석, 작업 분배, 접근 권한 부여 및 관리, 병렬 처리 및 다단계 프로세스 실행 등을 담당한다.[16] 업계에서는 이르면 향후 1년 내 테크 기업들이 새로운 관련 기능을 대거 출시할 것이라는 전망이 우세하다. 이를 활용하는 기업들은 이에 맞춰 오케스트레이션 플랫폼을 자체 구축할지, 외부 솔루션을 활용할지를 두고 전략적 판단이 필요하다. 예컨대 중앙 집중형 사내 플랫폼은 벤더 종속성을 줄이고 데이터와 에이전트에 대한 통제력을 높일 수 있는 반면, 상용(off-the-shelf) 플랫폼은 실험과 도입 속도를 높이고 혁신 비용을 보다 효율적으로 관리할 수 있다는 장점이 있다.

어떤 방식을 선택하든, 에이전트 오케스트레이션 플랫폼은 운영 지표 추적, 성능 개선, 비용 관리의 핵심 인프라로 자리 잡게 될 전망이다. 현재 일부 플랫폼은 지연 시간, 오류율, 토큰 사용량 등 에이전트 텔레메트리와 다양한 도구 인사이트를 통합 모니터링하는 기능을 개발하고 있다.[17] 가드레일(guardrail)* 평가와 이상 행동 감지 기능을 통해 리스크를 사전에 완화하는 시도도 확산하고 있다. 중장기적으로는 이러한 플랫폼에 계층화된 비즈니스 인사이트 제공과 추가적인 통제 메커니즘을 포함한 혁신적 기능이 추가될 수도 있다. 대표적으로 '가디언 에이전

트'(guardian agent)라는 새로운 유형의 에이전트는 스스로 업무를 수행하는 동시에, 다른 에이전트의 행동을 감독하며 위험 징후를 감지 및 관리하는 역할을 수행할 수 있는 차세대 통제 수단으로 주목받고 있다.[18]

아울러 내재화된 규제 컴플라이언스 기능 역시 에이전트 오케스트레이션 플랫폼의 필수 요소로 자리 잡을 전망이다. 유럽연합(EU)은 AI법(AI Act)에서 위험 평가, 투명성 확보 조치, 기술적 보호장치, 인간 감독 의무 등을 명확히 규정하고 있으며,[19] 이에 맞춰 EU의 표준화 기구들도 조화된(harmonized) 법적·기술적 표준을 마련하는 작업을 본격화하고 있다.[20]

* **가드레일(guardrail)**이란 시스템·AI·조직이 허용된 범위 안에서만 작동하도록 사전에 설정하는 규칙·제약·통제 장치를 의미한다. 문제가 발생한 뒤 조치하는 것이 아니라 발생하지 않도록 미리 제한하며, 무엇이 가능하고 무엇이 불가능한지 명확히 규정하고, 사람의 개입 없이도 지속적으로 작동한다.

3. 비즈니스 프로세스와 인력 구조의 변화

시장조사기관 가트너(Gartner®)는 기업용 소프트웨어 애플리케이션 중 에이전틱 AI가 탑재된 비율이 2024년 1% 미만에서 2028년에는 33%로 상승할 것으로 전망했다. 이후 2028년에 이르면 일상적 업무 의사결정의 최소 15%가 AI 에이전트를 통해 자율적으로 이뤄질 것으로 예상했다.[21] 이러한 변화에 대응하기 위해, 기업들은 2026년을 기점으로 기존 업무 흐름을 전면 재구상하고, 보다 구체적이고 독립적인 업무 모듈을 정의하는 작업에 본격 착수할 것으로 예상된다. 그 과정에서 업무의 중요도, 상호 의존성, 중요 업무의 예측 가능성, 목표로 하는 회복탄력성 수준이 어떤 유형의 에이전트 오케스트레이션이 필요한지를 결정하게 된다. 예를 들어 일부 업무 모듈은 한 에이전트의 산출물이 다음 에이전트의 입력값이 되는 순차형 협업 구조에 적합할 수 있으며, 다른 업무는 여러 에이전트가 병렬 또는 협업 방식으로 동시에 작동하는 구조가 더 큰 효과를 낼 수 있다.

또 하나의 핵심 변수는 인간과 멀티 에이전트 시스템 간 협업 방식이다. 전 세계 주요 기업의 최고인사책임자(CHRO) 200명을 대상으로 실시한 조사에 따르면, 응답자의 86%는 '디지털 노동력' 즉 지능적 업무를 수행하는 기술의 통합을 CHRO의 핵심 역할로 인식하는 것으로 나타났다.[22] 초기 협업 모델에서는 인간이 '에이전트 보스'로서 AI를 관리하거나, 에이전트와 나란히 협업하는 형태가 주를 이루고 있다.[23] 2026년에는 이러한 협업 모델이 더 많은 직무와 기능, 중요 업무 전반으로 확산될 것으로 전망된다.[24] 에이전트 오케스트레이션을 통해 업무 효율성을 극대화하고, 인간 고유의 강점과 협업이 더 큰 가치를 만들어낼 수 있도록 정밀한 업무의 재설계 작업이 본격화될 것으로 전망된다.

아울러 기업은 2026년부터 기존 직무가 멀티 에이전트 시스템을 통해 어떻게 더 높은 부가가치를 창출할 수 있는지도 본격적으로 재탐색하기 시작할 것이다.[25] 인간은 보다 창의적인 프롬프트 설계, 문제 해결 과정에서의 방향 제시, 전략적 의사결정 지원 등 에이전트를 조율하고 유도하는 역할에 집중하게 될 것이다. 동시에 기업들은 에이전트 훈련, 오케

스트레이션, 감독, 거버넌스를 담당할 새로운 인적 역량 개발과 책임 범위의 정립에도 속도를 낼 것으로 보인다.[26] 이에 맞춰 맞춤형 교육 프로그램 도입과 함께, 인간과 디지털 노동력을 동시에 관리할 수 있는 리더 양성이 중요 과제로 부상하고 있다. 이는 멀티 에이전트 기반 의사결정의 품질, 책임성, 회복탄력성을 제고하는 동시에, 인간 고유의 역량을 극대화하는 핵심 전략으로 평가된다.[27]

2026년, 에이전트 오케스트레이션의 변곡점

에이전트 오케스트레이션은 향후 지능형 자율기업(intelligent enterprise)* 시대를 규정하는 핵심 요인이 될 것이다. 2026년을 기점으로 기업은 멀티 에이전트 시스템을 본격적으로 확장할 것이며, 이로 인해 IT 환경과 비즈니스 운영 여건이 한층 복잡해질 것이다. 에이전트간 통신규격 역시 실험 용이성, 유연성, 확장성, 보안성을 갖춘 소수의 표준 중심으로 재편될 가능성이 크다. 기업의 업무 프로세스는 내부 구축 에이전트는 물론 SaaS 및 제3자 공급업체가 제공하는 에이전트를 기반으로 점차 모듈화된 구조로 재설계될 것으로 보인다. 이와 동시에 인간 근로자의 역할도 변화하며, 멀티 에이전트 시스템과의 효과적인 협업을 지원하는 새롭게 변형된 직무가 본격적으로 등장하기 시작할 전망이다.

* **지능형 자율기업(intelligent enterprise)**은 AI, 빅데이터, 사물인터넷(IoT) 등 첨단 기술을 활용해 데이터 기반의 실시간 의사결정, 업무 자동화 및 최적화, 사용자 맞춤형 서비스 제공을 통해 혁신을 이끌고 빠르게 변화하는 시장에 적응하며 성장하는 기업을 뜻한다.

다만 기업과 기술 공급업체 모두가 변화의 방향을 주도적으로 설계하고, 과감하게 실행해야 이러한 전환을 순조롭게 이행할 수 있다.

1. 멀티 에이전트 시스템을 도입하려는 기업이 해결해야 할 필수 과제

1) 소유권과 책임 소재 정립

기업은 자사의 AI 에이전트 비전, 전략, 실행 전반을 총괄할 최고책임자(C 레벨)를 정해야 하며, 이에 상응하는 인센티브와 책임 구조도 수립해야 한다. 일반적으로 전략적 기술 혁신과 디지털 전환을 주도하는 최고기술책임자(CTO)나 최고디지털책임자(CDO)가 해당 역할을 담당하는 것이 가장 자연스럽지만, 경우에 따라서는 기술·사업·리스크 관리를 통합적으로 아우르는 전사적 기능 조직이 더 큰 시너지를 낼 수도 있다.

2) 단기적 도입을 넘어 지속적 발전을 위한 설계 전략

AI 에이전트와 오케스트레이션 기술은 매우 빠른 속도로 발전하고 있으므로, 모듈형 '플러그 앤 플레이'(plug-and-play)* 방식의 오케스트레이션 프레임워크는 유연성, 비용 효율성, 혁신 역량을 동시에 높이는 핵심 수단으로 주목받고 있다. 이러한 구조는 기존 시스템 아키텍처에 대한 충격을 최소화하면서도 새로운 기술을 신속히 흡수할 수 있는 기반을 제공한다.

* **플러그 앤 플레이(plug-and-play)**는 별도의 복잡한 설정이나 전문 지식 없이 연결만 하면 즉시 작동하도록 설계된 기술·제품·시스템 특성을 의미한다. 연결 즉시 장치와 소프트웨어를 자동 감지하고, 설치·설정·튜닝이 최소화돼 즉시 사용이 가능하며, 저마찰 UX를 제공해 사용자의 진입 장벽을 크게 낮춘다. 마우스와 키보드 등 USB 장치와 계정 생성 후 즉시 사용할 수 있는 클라우드 등이 이에 해당한다.

3) 멀티 에이전트 오케스트레이션의 규모 확대 전 엄격한 스트레스 테스트 선행

실제 기업 환경에서는 불완전한 데이터, 상충하는 목표, 악의적 공격 시나리오 등 다양한 리스크가 동시에 발생한다. 통제된 환경에서 이러한 복합 리스크를 반영한 시뮬레이션을 수행하면, 규모를 확대하기에 앞서 잠재적인 실패 지점을 조기에 발견하고 보호 장치를 강화할 수 있다.

4) 신중한 거버넌스 수립 및 성과 측정

AI 에이전트 거버넌스는 대규모 확장 시 에이전트 오케스트레이션이 안전하고, 규제를 준수하며, 신뢰할 수 있는 방식으로 작동하도록 보장하는 핵심 장치다. 이를 위해 에이전트의 역할을 명확히 설정하고, 책임 범위를 정의하며, 오류 발생 시 우회 경로(fallback route)와 감독 체계를 설계하는 것이 필수적이다. 이는 오남용을 방지하고 감사 가능성을 확보하며 궁극적으로 신뢰를 구축하는 토대가 된다. 기업은 기술적 준비와 더불어 에이전트 오케스트레이션이 실제 어떠한 방식으로 가치를 창출하는지를 보여주는 성과 지표를 명확히 정의하고 지속적으로 추적할 필요가 있다. 이러한 성과 지표에는 의사결정 속도 개선, 고객 경험 향상, 혁신 속도 제고 등을 포함할 수 있다.

2. 멀티 에이전트 시대에 대비하는 기술 공급업체의 전략적 과제

1) 상호운용성을 전제로 한 설계

단순히 에이전트간 통신 표준을 준수하는 수준을 넘어, 솔루션 자체를 모듈형 구조로 설계하고 에이전트가 상호 의도와 행동 맥락을 이해할 수 있도록 구현해야 원활한 협업과 조율이 가능해진다.

2) 신뢰 개념의 근본적 재정의

이제 단순히 인사이트를 전달하는 것만으로는 충분하지 않으며, AI 에이전트의 산출물을 인간이 이해하고 검증할 수 있어야만 신뢰를 바탕으로 AI 에이전트의 도입을 확대할 수 있다. 에이전트에 디지털 아이덴티티를 부여하는 등 새로운 보안 메커니즘 장치를 구축해야, 신뢰 가능한 멀티 에이전트 시스템을 구축 및 운영할 수 있다.

3) 거버넌스를 설계 단계부터 내재화

고객사가 인적 가치, 조직 정책, 규제 요건 부합 여부 등을 중요시함에 따라, 이를 선제적으로 학습하고 반영하는 것이 향후 솔루션의 경쟁력을 좌우할 핵심 요소로 작용할 것이다. 이에 따라 차세대 솔루션에는 에이전트 모니터링 기능, 고도화된 거버넌스 체계, 윤리적 가드레일이 기본 구성 요소로 탑재돼야 한다. 이러한 방향으로 발전하는 AI 에이전트는 컴플라이언스와 실효성을 동시에 갖출 수 있다.

4) 생태계 확장

산업 전반에서 통신규격, 신뢰 체계, 거버넌스 표준을 정립하려면 산업 차원의 연합과 동맹을 지속적으로 구축 및 강화하는 노력이 필수적이다. 최근에는 플랫폼을 넘나드는 혁신적 오케스트레이션 다수의 툴이 급부상하고 있는데, 이는 기존 강자와 신생 기업 모두에게 인수합병(M&A), 전략적 제휴, 공동 협업을 통해 시장 입지를 강화할 수 있는 새로운 기회로 작용할 전망이다.[28]

Korean Perspectives

멀티 에이전트 시대의
핵심 경쟁력은 오케스트레이션이다

멀티 에이전트 시스템의 확산으로 한국 기업들은 단순한 AI 도입 단계를 넘어, 기업 운영체계 전반을 재설계해야 하는 상황에 직면했다. 이제 경쟁의 초점은 개별적으로 성능이 좋은 AI 에이전트를 얼마나 많이 보유했는가가 아니라, 서로 다른 에이전트를 어떻게 조율하고 통제하며 신뢰 가능한 방식으로 실행에 유기적으로 연결하느냐로 이동하고 있다. 실제로 에이전트 오케스트레이션 역량이 부족할 경우, 기술적 잠재력과 무관하게 비용 증가, 확장 실패, 리스크 누적으로 프로젝트가 중단될 가능성이 높아진다.

이러한 맥락에서 한국 기업이 가장 먼저 정립해야 할 것은 기술이 아니라 자율성의 경계와 책임 구조다. 멀티 에이전트 환경에서는 인간이 언제 개입하고, 감독하며, 완전히 위임할 것인지에 대한 기준이 명확하지 않으면 오히려 의사결정의 품질과 속도가 모두 저하될 수 있다. 따라서 단기적으로는 휴먼 인 더 루프(human-in-the-loop) 구조를 유지하며 신뢰와 학습을 축적하고, 중장기적으로 휴먼 온 더 루프(human-on-the-loop)로의 점진적 전환을 염두에 둔 설계가 현실적인 선택이 된다.

도입 전략 역시 일률적일 수 없다. 기존 업무에 에이전트를 덧붙이는 방식은 빠른 실험에는 유리하지만, 통합·보안·비용 관리 측면에서 복잡성을 빠르게 증폭시킨다. 반대로 장기 경쟁력을 확보하려면 업무를 보다 세분화된 모듈 단위로 재구성하고, 에이전트가 이해할 수 있는 컨텍스트 기반 구조(지식 체계, 온톨로지, 데이터 맥락)를 선제적으로 정비해야 한다. 멀티 에이전트의 성능은 결국 모델보다 기업 고유의 맥락 정보 품질에 의해 좌우되기 때문이다.

에이전트 수가 늘어날수록 통제의 중요성은 기하급수적으로 커진다. 관측 가능한 텔레메트리, 명확한 가드레일, 오류 발생 시 되돌림과 우회 경로를 포함한 복구 메커니즘은 선택 사항이 아니라 엔터프라이즈급 필수 인프라다. 특히 자율성이 높아질수록 사용자 인터페이스(UI)의 역할은 줄어들지 않고 오히려 강화된다. 에이전트의 판단 근거를 설명하고, 실행 이력을 추적하며, 인간이 개입해야 할 시점을 명확히 보여주는 경험 설계 없이는 조직 내부의 신뢰를 확보하기 어렵다.

또 하나 간과하기 쉬운 부분은 인력과 조직의 변화다. 멀티 에이전트 환경에서 직원은 더 이상 단순한 시스템 사용자가 아니라, 에이전트를 설계·조율·감독하는 오케스트레이터로 역할이 이동한다. 이는 교육, 직무 정의, 성과 평가 방식의 변화를 동시에 요구하며, 이를 뒷받침하지 못하는 조직은 기술을 도입하고도 실제 성과를 얻지 못할 가능성이 크다.

결국 멀티 에이전트 시대에 한국 기업의 승부처는 기술 도입 속도가 아니라, 에이전트를 중심으로 한 운영 모델과 거버넌스를 얼마나 일관성 있게 재설계했는가에 있다. 에이전트 오케스트레이션은 IT 프로젝트가 아니라, 지능형 기업으로 전환하기 위한 경영 구조의 문제다. 이 인식을 얼마나 빨리 받아들이느냐가 2026년 이후 성과 격차를 가르는 결정적 변수가 될 것이다.

정창모 파트너
한국 딜로이트 그룹
One AI 파트너