LG경영연구원

2024.10.

AI 에이전트, '자비스'가 온다

윤성재
sungjae2015@lgbr.co.kr

AI 에이전트가 단순한 대화 기능을 넘어 실제 작업 수행 능력까지 갖추며, AI 산업의 차세대 혁신 테마로 떠오르고 있다. 스마트폰, PC, 스마트홈 등 다양한 분야에 AI 에이전트의 도입이 확산되면서 사용자 경험에 혁신을 가져오고 있다. 특히 애플, 마이크로소프트 등 주요 기업들은 AI 에이전트를 자사 제품에 통합하면서 경쟁력을 높이고 있다. 로봇, 차량과 같은 물리적 움직임이 중요한 분야에서도 AI 에이전트의 활용이 활발하다.

그러나 AI 에이전트 도입에는 여전히 해결해야 할 과제가 남아있다. 높은 운영 비용과 AI의 안전성 문제가 대표적이다. 기업들은 이를 해결하기 위해 경량화 모델 개발과 AI 정렬 연구에 박차를 가하고 있다. AI 에이전트는 기술 혁신을 넘어 산업 전반에 걸친 패러다임의 변화를 예고하고 있다. AI 에이전트가 가져올 혁신과 미래 전망을 깊이 있게 살펴본다.

"자비스 깨어있나?"

"물론입니다."

"새 프로젝트 파일 만들어줘. 타이틀은 '마크2'."

"회사 데이터베이스에 저장할까요?"

2008년 개봉한 '아이언맨'의 한 장면이다. '자비스'는 주인공 토니 스타크의 작업을 보조하는 인공지능으로, 스타크의 지시를 즉시 이해하고 수행한다. 당시 먼 미래로 여겨졌던 이런 AI의 모습이 현실로 다가오고 있다. 올 상반기 다양한 AI 서비스와 제품이 등장하면서, 전문가들은 초거대언어모델(Large Language Model) 기반 'AI 에이전트'가 자비스와 같은 인공지능 비서를 실현하고 산업을 크게 변화시킬 것으로 예측하고 있다.

소프트웨어 산업의 Next Step, 'AI 에이전트'

최근 AI 업계를 중심으로 큰 주목을 받고 있는 AI 에이전트란, LLM이 중심이 되어 사람의 개입 없이도 특정 작업을 자율적으로 실행하는 지능형 시스템을 말한다. 단어 뜻 그대로, 대행자의 역할을 할 수 있는 AI인 것이다.

AI 에이전트는 기존의 AI 시스템과는 확연히 다른 세 가지 핵심 능력을 보유하고 있다.

첫째, 자율적 실행 능력이다. 사용자의 의도를 깊이 이해하고, 목표 달성을 위해 필요한 행동을 스스로 결정하고 실행한다. "다음 주 출장 준비해줘"라는 간단한 명령에 AI는 일정 확인, 예약, 준비물 목록 작성까지 모든 과정을 알아서 처리한다.

둘째, 다양한 도구와 리소스를 조합하여 실행할 수 있다. "최근 5년간 회사 재무 상태를 분석해줘"라는 요청에 AI는 데이터베이스 접근, 스프레드시트 작성, 그래프 생성, 보고서 작성 등 여러 도구를 활용해 작업을 완수한다.

셋째, 재귀적 실행 능력을 갖추고 있다. 결과의 품질을 높이기 위해 작업을 반복적으로 실행하고 개선한다. 마케팅 캠페

AI 에이전트의 3가지 특징

① 자율 실행 (Autonomous)	주어진 목표를 완수하기 위해 자율적으로 계획 수립 및 이행
② 조합 실행 (Combined)	웹 검색이나 외부 API 등 도구 조합 · 활용하여 작업 수행
③ 재귀 실행 (Recursive)	작업을 반복적으로 평가하고 수정하여 최적의 결과를 도출

인 기획 시 AI는 초안 작성, 과거 사례와의 비교 분석, 개선점 도출 및 수정을 반복하여 최상의 결과물을 만들어낸다.

즉 AI 에이전트는 사용자의 의도를 깊이 이해하고 어떤 작업을 수행해야 하는지 '자율적'으로 결정하고 여러 '도구'를 조합하여 '반복' 실행'한다. 기존의 ChatGPT와 같은 대화형 AI는 사용자의 질문이나 요청에 그럴 듯한 대답을 할 뿐이지만, AI 에이전트는 실제로 일을 하는 AI라고 볼 수 있다.

AI 에이전트의 기대효과

많은 AI 전문가들은 AI 에이전트가 생성형 AI의 자연스러운 진화 형태로 AI 산업을 넘어 다양한 산업 분야에 큰 영향을 미칠 것으로 기대한다. 예를 들어 게이츠 재단 포트폴리오의 35%를 AI에 투자한 빌 게이츠도 AI 에이전트의 파급력에 주목하고 있다. "에이전트는 단순히 컴퓨터와의 상호작용 방식을 바꾸는 것뿐만 아니라 소프트웨어 산업 전체를 뒤흔들 것이다."라고 말했을 정도다. 그렇다면 왜 AI 에이전트가 AI 기술 발전에 있어 중요한 이정표로 인식되는 것일까? 그 이유는 다음과 같다.

- **기능성의 비약적 확장:** AI 에이전트는 단순 대화를 넘어 복잡한 작업을 수행할 수 있어, AI의 실용성과 적용 범위를 크게 확대할 수 있음.
- **인간–AI 상호작용의 질적 변화:** 더 자연스럽고 효율적인 인간–AI 협업이 가능해, 일상생활과 업무에 더 깊이 통합할 수 있음.
- **AI의 자율성 증대:** 인간의 적은 개입만으로도 큰 생산성 향상이 가능함.
- **문제 해결 능력의 향상:** 조합 실행, 재귀 실행을 통해 복잡한 문제를 다각도로 분석하고 해결하여 실질적 가치를 높임.
- **기술 융합의 촉진:** AI 에이전트는 다양한 기술들을 통합하여 사용하므로, 여러 기술 분야의 발전을 가속할 수 있음.
- **새로운 산업과 서비스의 창출:** 기존 AI보다 폭넓은 활용 범위로 인해 새로운 비즈니스 모델과 서비스를 창출할 수 있음.

스마트폰 산업, 최전선으로 부상

AI 에이전트가 가장 적극적으로 적용되는 곳은 디바이스 산업인데, 특히 스마트폰 산업에서 두드러진다. 최근 몇 년간 스마트폰 산업은 하드웨어 혁신이 한계에 이르며 기기 교체 주기 장기화로 수익성이 악화했고, 이에 대응하고자 신기술 적용에 적극 나선 것으로 보인다. 애플, 삼성, 화웨이 등 대부분의 스마트폰 제조사들은 AI 기능을 앞다투어 장착하며 AI 에이전트 내재화의 초석을 다지고 있다. 이 중 애플은 특히 주목할 만하다.

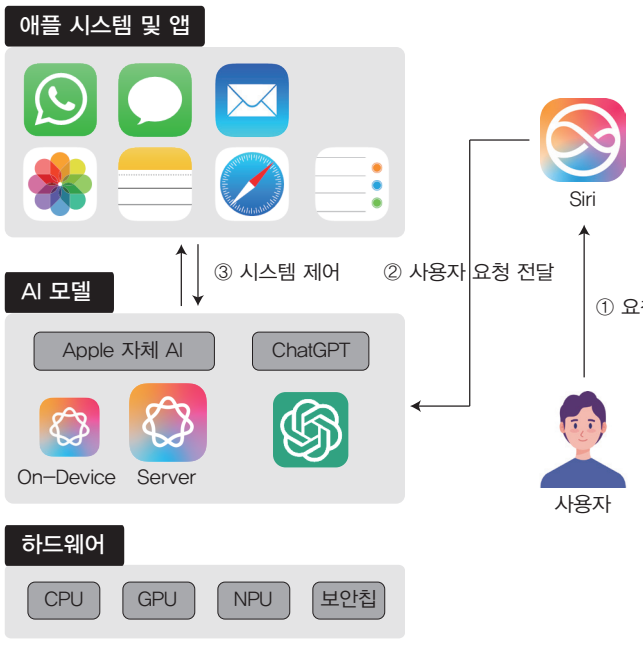
AI 에이전트는 기존의 AI 기능이 수행하는 작업보다 훨씬 복잡하고 다양한 것들을 수행해야 하는 만큼, 고도의 기술이 필요하다. 이에 애플은 스마트폰을 구성하는 두 개의 축인 ①소프트웨어(AI를 결합한 iOS)와 ②하드웨어(스마트폰 칩)를 AI 중심으로 특화하여 온디

바이스 AI 에이전트의 첫 발을 내디뎠다.

애플은 소프트웨어 측면의 AI 경쟁에 뒤처진 듯 보였으나, 실제로는 혁신적 기술을 조용히 준비 중이었다. 지난 4월 애플은 '페럿-UI'와 'ReALM'이라는 두 가지 핵심 AI 기술을 공개했다. 페럿-UI는 화면의 모든 요소를 이해하고 조작할 수 있으며, ReALM은 대화 맥락과 백그라운드 작업까지 고려해 모호한 명령도 정확히 실행한다. 이러한 기술 개발의 결실은 WWDC 2024에서 선보인 새로운 AI 에이전트로 나타났다. 애플은 AI 비서 '시리'와 자체 AI 모델인 '애플 인텔리전스'를 결합해, 사용자 경험을 근본적으로 변화시키는 포괄적 AI 시스템을 구축했다. 이 AI 에이전트는 사용자의 음성 명령만으로 개인 정보와 맥락을 이해하여 복잡한 작업을 자율 실행할 수 있다. 예를 들어, 사용자가 친구에게서 이메일 주소가 담긴 스크린샷을 메시지로 받았을 때, "시리, 이 주소를 연락처에 저장해줘"라고 명령하면 시리가 화면을 인식하고 내용을 해석하여 이를 처리한다. 페럿-UI의 화면 요소 이해 능력과 ReALM의 맥락 파악 기술이 실제 제품에 구현된 사례다.

한편, 애플은 이러한 AI 에이전트 기능들을 기기에 탑재하기 위해 하드웨어 기술 개발에도 심혈을 기울이고 있다. 파라미터 크기가 최소 수십억 개에 달하는 생성형 AI 모델을 기기에 탑재하려면, 메모리, 특히 RAM 문제를 해결해야 한다. 이에 애플은 RAM뿐만 아니라 플래시 메모리를 사용해 AI 모델의 데이터를 저장하는 기술을 개발했다. 또한 애플 칩에서 실행될 때 생성형 AI의 추론 지연 시간을 최소화하면서 메모리 소비를 크게 줄이는 기술도 선보였다. 차세대 프로세서 'A18 프로'에는 AI 연산 성능 강화를 위해 6개의 GPU 코어를 탑재하는 등 향후 큰 변화를 예고했다.

애플 인텔리전스 아키텍처



애플은 음성 비서 Siri와 애플 인텔리전스를 결합하여, AI 에이전트 시스템을 구성하고 있다. 예를 들어, ① 사용자가 Siri에게 새로운 일정을 추가해달라고 요청하면 ② Siri는 이 요청을 애플 인텔리전스에 보내고 ③애플 인텔리전스는 일정 앱에 접근하여 사용자가 요청한 일정을 추가한다. 이 과정에서 GPU, NPU 등의 AI 하드웨어가 시스템을 뒷받침한다.

PC에서도 AI 에이전트 탑재 활발

한편, PC 산업에서는 마이크로소프트가 '코파일럿+PC' 프로젝트를 통해 AI 에이전트 도입의 선두에 섰다. 이는 단순한 기능 추가를 넘어 PC 사용 경험을 근본적으로 변화시키려는 시도다. 예를 들어, 코파일럿은 기기 내 AI 기반의 실시간 번역을 제공하는 '라이브 캡션' 기능으로 PC에서 재생되는 모든 오디오, 비디오에 자막을 생성할 수 있다. 또한 게임 플레이 중에는 실시간 가상 코치 역할을 맡아 음성으로 조언하기도 한다. 이처럼 코파일럿은 사용자의 상황을 정확히 파악하고 맞춤형으로 도와주는 '디지털 비서' 역할을 수행한다. 또한 이러한 AI 기능을 기기에 결합하기 위해 코파일럿+PC에 신경망 처리 장치(NPU, Neural Processing Unit)를 탑재하는 등 하드웨어 성능 고도화에 나섰다. 마이크로소프트는 이러한 AI 기술 개발을 바탕으로 'Window OS와 AI 에이전트의 결합을 통한 새로운 고객 경험 제공'을 비전으로 제시하고 있다.

PC 제조사나 OS 개발사뿐만 아니라 스타트업들도 이 흐름에 가세했다. 'Adept AI'가 PC 에이전트를 추진한하는 대표적인 기업이다. Adept AI는 2022년 9월, PC 화면 이해 및 작업 수행에 특화된 ACT-1과 이를 활용한 PC 에이전트 데모 영상을 공개했다. 이 영상에서 ACT-1은 "새 고객 정보를 CRM에 추가하고, 그의 올 예상 매출을 계산해줘"라는 복잡한 명령을 척척 해냈다. 이는 마치 숙련된 비서가 옆에서 일하는 듯한 경험을 선사한다.

PC를 직접 제어하는 ACT-1의 비결은 재귀 실행이다. ACT-1은 주어진 사용자의 명령을 완수하기 위해 행동-관찰 패턴을 반복한다. 예를 들어, 특정 엑셀 파일 내에서 기존 데이터를 활용해 새로운 열을 만드는 작업을 요청한 경우, ACT-1은 새로운 열에 수식을 입력한다. 그리고 이것이 사용자의 명령에 부합하는 새로운 열인지 검토한 후에, 그렇지 않은 경우 이를 바로잡고자 다시 수식을 입력한다. 이러한 PC 에이전트의 재귀 실행은 사용자의 개입 없이 원하는 성과를 끌어내는 데에 핵심적인 역할을 한다.

새로운 플랫폼 생태계 형성 가능성도 제기

공개된 여러 사례에서 볼 수 있듯이, 디바이스와 AI 에이전트의 결합은 사람과 기기 간의 상호작용 방식에 큰 변화를 일으킬 수 있다. 사용자의 의도를 이해하고 기기 내 다양한 애플리케이션을 자율적으로 실행할 수 있는 AI 에이전트의 특성을 고려하여, AI에 기반한 운영체제를 이야기하는 전문가도 나타났다. 오픈AI 연구원이었던 안드레 카파시(Andrej

Karpathy)는 'LLM OS'라는 개념을 제시했다. LLM이 PC의 운영체제로 활용될 수 있다고 전망한 것이다.

단기적으로는 AI 에이전트 시스템의 불안정성으로 인해 기존 운영체제를 완전히 대체하기보다는 운영체제와 사용자 사이에서 명령어를 더욱 종합적, 효율적으로 이행시키는 새로운 계층(Layer)으로서 작동할 전망이다. 국내 AI 기업 업스테이지의 김성훈 CEO는 "AI가 Intelligent Layer라는 OS 상위 계층으로 자리 잡아, 모든 작업의 기반이 될 것"으로 예상했다. AI 에이전트가 형성하는 'Intelligent Layer'는 복잡한 작업을 간단한 자연어 명령만으로 수행할 수 있는 새로운 경험을 제공할 수 있다.

이러한 변화는 새로운 플랫폼 생태계의 형성으로 이어질 공산이 크다. 과거 OS가 다양한 프로그램 및 서비스 개발의 플랫폼 역할을 했다면, 앞으로는 AI 에이전트가 새로운 생태계의 기반이 될 수 있기 때문이다. 이 생태계에서는 AI 에이전트가 활용할 수 있는 다양한 도구, 서비스, 그리고 데이터 소스가 중요한 요소가 될 것이다. 예를 들면, 의료 분야의 특화 데이터베이스, AI 에이전트의 금융 거래를 위한 보안 시스템, 개인의 선호에 최적화한 맞춤형 디자인 도구와 같은 특색 있는 상품들이 이 새로운 시장의 핵심이 될 수 있다.

더 나아가, AI 에이전트와 소통하는 방식도 혁명적으로 바뀔 수 있다. 애플의 '비전 프로'처럼 손짓만으로 AI와 대화하거나, 일론 머스크의 '뉴럴링크' 프로젝트가 현실화한다면 생각만으로 명령을 내리는 날이 올 지도 모른다.

이러한 변화는 기술 업계 전반에 새로운 도전과 기회를 제시한다. 소프트웨어 개발자, 하드웨어 제조사, 서비스 기업들은 이 새로운 생태계에서 치열한 자리다툼을 벌이게 될 것이다. 지금과는 완전히 다른 모습으로 진화한 디지털 라이프도 상상해볼 수 있다.

인공지능이 로봇을 만날 때

올해 3월, 'Figure AI'라는 휴머노이드 로봇 스타트업이 화제를 모았다. 이 회사의 로봇 Figure-1이 오픈AI의 GPT-4와 결합해 놀라운 능력을 선보인 것이다. Figure-1은 GPT-4(V)의 멀티모달(음성, 텍스트 등 여러 감각 정보를 처리하는 능력)을 기반으로 눈앞의 상황과 사용자의 요청을 종합적으로 이해하고, 이를 완수하기 위해 계획을 세운 뒤 실제 로봇의 움직임으로 실행하는 과정을 거친다. AI 에이전트가 휴머노이드 로봇과 결합해, 과거에는 불가능했던 높은 수준의 언어 이해와 더불어 사람의 개입 없이 적합한 행동을 자율적

으로 수행하는 놀라운 일이 일어난 것이다.

Figure-1 데모 영상은 GPT-4의 물리적 환경을 이해하는 능력과 Figure AI의 Order2Action(자연어 명령으로 움직임 제어) 능력이 결합한 것을 보여주었다. 예를 들어, 영상 속 연구원이 "먹을 것 좀 있을까?"라고 질문하면, Figure-1에 내장된 오픈AI의 STT(Speech-to-Text) 모델인 Whisper가 텍스트로 변환한다. 그리고 GPT-4는 멀티모달 능력을 기반으로 주변 환경 이미지를 텍스트로 변환하여 이해하고, 사용자의 질문과 조합하여 적절한 답변과 작업 계획(로봇의 움직임 제어)을 만든다. 마지막으로 이 작업 계획을 Figure AI의 자체 모델이 전달받아 로봇의 움직임으로 재해석하여 최종적으로 연구원의 질문에 적합한 행동을 한다.

스스로 작업 계획을 생성하고 이를 실제 물리적 움직임에 옮기는 'AI 에이전트적(Agentic)' 특성은 스마트홈 분야에서도 빠르게 적용되고 있다. LG전자의 'Q9'은 단순한 음성 명령을 넘어 복잡한 상황 판단까지 가능하다. "오늘 날씨 알려주고 날씨에 맞게 에어컨 온도 설정해줘"와 같은 복합적인 요청도 능숙히 처리한다. 더 나아가 집 안의 환경을 실시간으로 모니터링하며 맞춤형 서비스를 제공한다. 이는 단순한 기기 제어를 넘어 '디지털 집사'의 역할을 하는 셈이다.

모빌리티 산업 역시 AI 에이전트 결합 시도가 활발하다. 독일 완성차 업체 폭스바겐의 경우, 오픈AI의 ChatGPT와 엔비디아의 드라이브 IX 기술을 바탕으로 IDA 음성 어시스턴트를 개발, 탑재했다. IDA 어시스턴트는 ChatGPT를 적용한 만큼, 인포테인먼트나 내비게이션, 실내 온도 조절 시스템 등 차량 제어를 넘어 사용자와 일상적인 대화도 가능하다. 이와 같은 차량 내 AI 에이전트 탑재 시도는 BMW, 벤츠, 푸조 등에서도 이뤄지고 있으며, 현대차는 포티투닷과 차세대 AI 인포테인먼트 시스템을 구축하며 AI 모빌리티에 대한 열망을 내비치고 있다. 차량이 점차 '바퀴 달린 생활공간'으로 인식되면서, 자동차 업계는 고객 경험 향상을 위 해 SDV(Software Defined Vehicle)를 넘어 AIDV(AI Defined Vehicle) 시대를 향한 준비 에 박차를 가하고 있다.

AI 에이전트, 넘어야 할 장애물도 많아

AI 에이전트는 사람과 하드웨어 간의 상호작용에 큰 발전을 가져오고 있다. 그러나 상호작용을 넘어 실세계에서의 물리적인 움직임을 만들어내려면, 여전히 방대한 3D 시뮬레이

션 데이터를 기반으로 한 강화학습이 필수적이다. 예를 들어 로봇에게는 인간의 상식적 추론 능력과 연계한 동작 제어 능력이 없다. 그래서 일상적인 행동 하나하나도 유사한 상황을 수천 번 반복 학습해야만 간신히 흉내 낼 수 있다. 최근 쏟아지는 휴머노이드 AI 에이전트의 데모 영상을 보면 여전히 대부분의 로봇들이 엉거주춤한 걸음걸이를 보여주는데, 그것이 물리적 동작에 대한 강화학습이 얼마나 중요한지 보여주는 대목이다. 다양한 상황에서 물리적 작업을 하려면 더 많은 실세계 데이터를 기반으로 고도화가 필요한 상황이다.

AI 에이전트는 최근 생성 AI로 큰 변혁기를 맞이한 AI 산업에서 기반 모델(Foundation Model)을 넘어선 차세대 혁신 테마로 큰 주목을 받고 있다. 하지만 여느 기술과 마찬가지로 한계점도 존재한다.

첫째, AI 에이전트의 구동은 아직 비용효율적이지 않다. AI 에이전트는 사용자의 명령을 완수하기 위해 작업 수행 계획을 작성하거나 여러 도구를 실행하면서 여러 번 모델을 실행시켜야 하기 때문이다. 따라서 대화형 AI가 질문-대답 형태로 처리하던 기존 방식 대비 수배에서 수십 배의 운영 비용이 발생한다.

AI 모델 개발 기업들은 이를 일찍이 알아차리고, 최근 경량화 모델을 앞다퉈 출시하고 있다. 오픈AI는 7월 19일 GPT-4o 모델을 경량화한 GPT-4o Mini 모델을 공개했다. GPT-4o Mini의 API 이용료는 기존 경량 모델인 GPT-3.5 Turbo보다도 입력은 70% 출력은 60% 저렴하다. 구글도 Gemini-1.5 Ultra 공개에 앞서 Gemini-1.5 Flash를 공개했다. 이는 기존 Gemini-1.5 Pro 모델을 경량화한 것으로, 속도와 비용 측면에서 모두 크게 개선된 모델이다. Anthropic 역시 자사 최고 모델인 Claude 3.5 Opus를 공개하기 이전에 Claude 3.5 Sonnet을 출시했다. 이는 AI 에이전트가 대중화되었을 때, 서버 구동 비용 폭증에 대비해 경량 모델에 집중하는 것으로 해석할 수 있다.

둘째, AI 에이전트는 아직 위험하다. AI 에이전트가 특정 작업의 전 과정을 관장하여 인간의 개입이 적고 편리해지는 만큼, AI의 선택권이 커진다. 따라서 아직 AI 학계가 해결하지 못한 환각 현상이나 정렬 문제로 인해 위험 부담이 커진다. AI에서 정렬(Alignment)이란, AI 시스템을 인간이 의도한 목표, 선호도 또는 윤리적 원칙에 맞게 조정하는 것을 말한다. 만약 인간이 선한 의도에서 내린 명령을 AI가 잘못 해석하고 폭력적인 행동을 실행에 옮긴다면 예상치 못한 참사가 발생할 여지가 크다.

이는 AI가 어떤 사고방식으로 작동하는지 파악할 수 없는 현재, AI 비용 문제보다 심각하게 받아들일 사안이기도 하다. AI 업계와 학계는 이를 미연에 방지하기 위해 정렬 문제를

진지하게 받아들이고, 해결에 활발한 연구를 펼치고 있다. 아직 생성형 AI가 생각하는 방식을 인간이 정확히 이해하지는 못하지만, 인간의 가치관에 알맞은 생각을 하도록 '정렬'시키고자 노력하고 있다.

AI 에이전트의 등장은 단순한 기술 혁신을 넘어 산업 전반에 걸친 패러다임 전환을 예고하고 있다. 향후 스마트폰, PC, 스마트홈, 자동차 등 다양한 분야에서 AI 에이전트의 도입을 가속화한다면, 사용자 경험의 획기적 개선과 산업 구조의 근본적인 변화도 가능하다.

AI 에이전트가 열어갈 미래는 기회와 도전이 공존하는 복합적인 모습을 띨 것이다. 기업들은 AI 에이전트를 활용한 새로운 비즈니스 모델을 구축하고, 기존 제품과 서비스를 혁신할 기회를 얻게 될 것이다. 동시에 개인정보 보호, 윤리적 의사결정, 일자리 변화 등 사회적 차원의 새로운 과제에 직면하게 될 것이다. 따라서 AI 에이전트 시대를 대비하기 위해서는 기술 개발과 더불어 법 · 제도 정비, 윤리 가이드라인 수립, 교육 시스템 재편 등 다각적인 준비가 필요하다. LG경영연구원