

보도시점 2026. 7. 23.(목) 10:00
(2026. 7. 23.(목) 석간)

배포 2026. 7. 22.(수) 14:00

실행 중심의 에이전틱 AI 생태계 선점 본격 추진

- 관계부처 합동 「에이전틱 AI 이니셔티브」 마련
- 3대 추진 전략 : ① 에이전틱 AI 안전신뢰 선도 ② 개방형 에이전틱 AI 실행 기반 조성
③ 수요 중심의 에이전틱 AI 도입 촉진

【관련 국정과제】 21. 세계에서 AI를 가장 잘 쓰는 나라 구현

과학기술정보통신부(부총리 겸 과기정통부 장관 배경훈, 이하 ‘과기정통부’)는 7월 23일(목)에 개최된 제11회 과학기술관계장관회의에서 「에이전틱 AI 이니셔티브」를 발표했다고 밝혔다.

< 추진 배경 >

최근 AI는 목표에 따라 자율적이고 능동적으로 계획을 수립하고, 실행을 하는 ‘에이전틱 AI’로 급속히 진화하고 있다. 에이전틱 AI는 산업 생태계 전반의 수익 구조와 서비스 방식을 바꾸고, 개인의 생산성을 획기적으로 향상시켜 ‘1인 기업 시대’를 가능하게 하는 등 경제 구조를 재편하는 핵심 기술로 주목받고 있다.

<에이전틱 AI로 바뀌는 경제 모습>



이에 AI 경쟁의 축이 확대되고 있다. 기존에는 ‘누가 더 우수한 모델을 보유하였는가’였다면, 향후에는 ‘누가 더 많은 데이터, 시스템, 업무 흐름을 연결하고 실행하는가’도 경쟁력을 좌우할 핵심요소가 될 전망이다. 구글, OpenAI, 마이크로소프트 등 글로벌 빅테크는 자사의 프론티어 AI 모델을 기반으로 업무 소프트웨어·API·모델·클라우드 인프라를 포괄하는 실행 체계 선점 전략을 추진 중에 있으며, 중국은 자국 플랫폼과 공공·산업 데이터를 기반으로 통제형 실행 생태계를 구축하는 중이다.

우리나라는 세계 최고 수준의 디지털 인프라와 제조·금융·공공 등 탄탄한 산업 기반을 보유하고 있어 에이전틱 AI 확산에 유리한 여건을 갖추고 있다. 실행 생태계 중심으로 전환되는 AI 패러다임 전환을 기회로 삼아 우리나라가 에이전틱 AI 생태계를 선점할 수 있도록 동 이니셔티브가 마련되었다. 이번 이니셔티브는 ❶에이전틱 AI 안전·신뢰 선도, ❷개방형 에이전틱 AI 실행 기반 조성, ❸수요 중심의 에이전틱 AI 도입 촉진을 3대 추진 전략으로 제시하였으며, 구체적인 내용은 다음과 같다.

< 주요 추진 전략 >

❶ 에이전틱 AI 안전·신뢰 선도

에이전틱 AI는 외부 시스템과도 연동이 되고, 실제 실행까지 수행한다는 점에서 그 파급효과가 생성형 AI보다 크다. 특히, 권한 오남용, 보안 위협, 민감 데이터 유출 등 문제가 발생할 가능성도 있어 에이전틱 AI의 도입·활용에 있어서 안전·신뢰 확보는 필수적이다. 엔트로픽, OpenAI, 구글 등은 에이전트 기능 출시와 함께 권한 범위 제한, 로그 기록 관리 등 안전 기능을 설계 단계부터 반영하는 추세이다.

과기정통부는 에이전틱 AI 전주기에 적용 가능한 안전·신뢰 관리 체계를 확보한다. 이를 위해 개인정보·민감데이터 보호, AI 권한 관리, 목표 이탈 방지 등 에이전틱 AI 고유 위험 요소를 반영한 ‘에이전틱 AI 안전·신뢰 가이드라인’을 연내 마련한다.

또한, 에이전틱 AI의 성능 및 안전·신뢰성을 평가하기 위한 기반을 구축하고, AI 에이전트의 안전한 활용 및 행위 책임성 확보를 위해 ‘에이전틱 AI 얼라이언스’를 중심으로 AI 에이전트 신원확인 및 책임소재를 검토할 예정이다.

② 개방형 에이전틱 AI 실행 기반 조성

에이전틱 AI는 AI 모델이 외부 시스템·도구와 연결되어 실제 업무를 수행할 때 비로소 가치를 창출한다. 따라서 에이전틱 AI 시대의 경쟁력은 개방형 실행 생태계 구축 여부에 달려있다.

국내 환경에 맞는 AI 에이전트 도구, 유통 체계, 기술 및 모델을 확보한다. 국민이 일상이나 업무에서 반복 활용하는 생활 밀착형·고수요 AI 에이전트 서비스 및 도구 개발을 지원하고, 신뢰할 수 있는 AI 에이전트 유통을 위한 마켓플레이스도 지원한다.

또한, AI 모델-추론-에이전트-도구 등 AI 핵심 요소를 통합 관리하는 AI OS 핵심 기술을 개발한다. 특히 에이전틱 AI는 멀티에이전트 협업, 도구 활용, 반복 호출 등으로 높은 연산 자원을 요구하는 만큼 토큰 효율 기반 실행 운영 기술 확보를 추진한다.

아울러, 국산 AI 모델의 에이전틱 AI 성능 강화를 위해 GPU와 에이전틱 데이터를 지원할 예정이다. 이를 통해 서비스 개발 기업이 다양한 AI 모델을 목적에 맞게 선택·활용할 수 있는 환경을 조성할 계획이다.

③ 수요 중심의 에이전틱 AI 도입 촉진

에이전틱 AI는 복합적인 업무를 자율적으로 수행할 수 있어 생산성 향상과 업무 혁신을 가져올 수 있다. 국민과 산업 현장에서 체감할 수 있는 수요 중심의 에이전틱 AI 도입을 촉진한다.

‘모두의 AI 프로젝트’를 통해 국민 누구나 AI 에이전트를 활용할 수 있는 기반을 마련하고, 장기적으로 모든 국민이 자신만의 AI 에이전트로 일상과 경제활동 전반에서 새로운 가치를 창출할 수 있도록 한다.

또한, AI 파운데이션 모델 기업, 인프라 기업, AI 서비스 개발사, 수요 기업 등 AI 가치사슬 전반이 참여하는 ‘AI 에이전트 플래그십 프로젝트’를 추진하여 우리나라 주요 산업 분야의 에이전틱 AI 서비스 개발·실증을 지원한다.

<AI 에이전트 플래그십 프로젝트(안)>



기업의 AI 에이전트 개발·도입 역량을 강화하기 위해 도입 진단, 위험 관리, 운영 체계 수립 등 전문 컨설팅을 지원하고, 혁신 AI 에이전트 기술을 보유한 스타트업의 사업화도 지원한다.

아울러, 에이전틱 AI의 자율 실행, 멀티에이전트 특성을 고려해 ICT 규제 샌드박스를 활용한 실증 기회를 확대하고, 실증 결과를 기반으로 증거 기반의 에이전틱 AI 친화적 제도 개선을 단계적으로 추진한다.

< 향후 계획 >

과기정통부는 지난 4월 기술개발부터 산업 적용, 생태계 조성 및 안전·신뢰 확보까지 전 주기를 아우르는 국가 협력 플랫폼으로서 ‘에이전틱 AI 얼라이언스’를 출범시킨 바가 있다. 이번 이니셔티브의 실행력을 뒷받침하기 위해 ‘에이전틱 AI 얼라이언스’를 중심으로 정책 세부 내용을 구체화하고, 빠르게 변화하는 기술 환경에 발맞추어 무빙타겟 방식으로 정책을 추진해 나갈 계획이다.

배경훈 부총리 겸 과기정통부 장관은 “에이전틱 AI는 단순한 기술 혁신을 넘어 일하는 방식과 경제·사회 전반의 변화를 이끄는 새로운 전환점이 될 것”이라며, “우리 국민과 기업이 에이전틱 AI 시대에 기회를 확보하고 새로운 가치를 창출할 수 있도록 안전·신뢰 기반의 에이전틱 AI 생태계를 조성해 나가겠다”라고 강조했다.

붙임. 「에이전틱 AI 이니셔티브」 요약
 별첨. 「에이전틱 AI 이니셔티브」 전체본

담당 부서	인공지능정책기획관 디지털인재양성과	책임자	과 장	백병수 (044-202-6370)
		담당자	사무관	박수현 (044-202-6373)



내일을 만드는 과학기술
 내일을 채우는 디지털·AI

대한민국
 정책브리핑



□ 추진 배경

- 최근 AI는 자율·능동적 의사결정 및 실행이 가능한 ‘에이전틱 AI’로 급속히 진화 중으로, AI 경쟁의 축이 모델 성능에서 실행구조로 전환 중
 - ※ 빅테크는 자사 프론티어 AI를 기반으로 업무 소프트웨어·API·모델·클라우드 인프라를 포괄하는 실행 운영 체계 선점 전략을 추진
- 에이전틱 AI는 산업 생태계 전반의 수익 구조와 서비스 방식을 재편할 것으로 기대되며, 개인의 생산성*을 획기적으로 향상
 - * AI 기술의 발전으로 직원을 고용하지 않고도 기업 수준의 성과와 수익을 창출하는 1인 기업가 ‘솔로프리너’ 부상(美 1인 창업자 비율 ‘20년 24.5% → ‘25년 36%, Carta)
- 한편, 에이전틱 AI는 多 연산 자원 필요* 및 권한 오남용, 보안 위협, 민감 데이터 유출 등 문제가 존재하여 대응 필요
 - * 앤트로픽은 멀티에이전트 시스템이 일반챗봇 대비 약 15배 더 많은 토큰 소비 분석(‘25.6월)
 - ※ OpenAI, 앤트로픽, 구글 등 글로벌 기업은 에이전트 기능 출시와 함께 권한 범위 제한, 로그 기록 의무화 등 안전 대응 강화 추세

⇒ 산업 전반의 AI 서비스 혁신을 촉진하는 동시에, 에이전틱 AI의 안전·신뢰성을 보장할 수 있는 방향으로 국가 차원의 전략 마련 필요

□ 추진 방향

비전

실행 기반 중심의 에이전틱 AI 생태계 선점으로,
AI 글로벌 3대 강국(G3) 도약

추진목표

- ① (안전·신뢰) 자율실행, 외부연계 확대에 대응한 안전·신뢰 관리체계 구축
- ② (실행기반) 국내환경에 맞는 도구·기술·AI모델 확보로 실행 생태계 경쟁력 확보
- ③ (도입촉진) 산업·사회 확산으로 생산성 혁신 및 국민 체감형 수요 창출

□ 주요 추진과제

① (안전·신뢰) 에이전틱 AI 안전·신뢰 선도

- 자율적 도구 권한 통제, 멀티 에이전트 간 책임 귀속, 인간 감독 체계 등 에이전틱 AI 고유 위험 요소를 반영한 ‘안전·신뢰 가이드라인’ 마련(~26년)
- 에이전틱 AI의 성능·안전·신뢰성 평가 체계 및 기반(데이터셋, 시나리오, 벤치마크 도구 등) 구축(~26년~) 및 샌드박스(검증) 환경 지원(~27년~)
- AI 에이전트의 안전한 활용 및 행위 책임성 확보를 위해 신원확인·관리 방안 및 책임소재 검토 * 에이전틱 AI 얼라이언스 중심 논의

② (실행 기반) 개방형 에이전틱 AI 실행 기반 조성

- 국민이 일상생활이나 업무 전반에서 반복 활용되는 생활밀착형·고수요 AI 에이전트 서비스 및 도구 지원(~26년~)
- 신뢰할 수 있는 AI 에이전트 서비스·도구의 안전한 연결·유통을 위해 민간의 AI 에이전트 마켓플레이스 지원(~26년~)
- 자원 최적화 등 AI OS* 핵심 기술 개발, 장기 맥락 계획·자기수정 및 멀티 에이전트 오케스트레이션 등 에이전틱 AI 기술 경쟁력 강화
* AI 핵심요소(모델·추론·에이전트·도구)를 통합 관리해 자원 최적화 및 보안 기반 자율 서비스 실행을 지원하는 시스템

- 국내 AI 모델의 에이전틱 AI 성능 강화를 위해 GPU 및 데이터 지원(~27년~)

③ (도입 촉진) 수요 중심의 에이전틱 AI 도입 촉진

- 민간 기업 주도로 범용 AI 챗봇 및 국민 수요·선호 기반 AI 에이전트 연계 ‘특화 서비스’를 함께 제공하는 모두의 AI 프로젝트 추진(~26년~)
- 누구나 AI 에이전트를 개발·운영해 일상 업무를 혁신하고, 1인 창업을 할 수 있도록 인프라 비용(바우처) 지원(~27년~)

- 주요 산업* 분야 대상 AI 가치사슬 전체와 연계한 대형 컨소시엄**을 구성하여 에이전틱 AI 서비스 개발·실증 지원

* (예시) 미디어, 물류, 핀테크, 에듀테크, 리걸테크, 에너지, 에그리테크, 헬스케어, 바이오, 건축 등 에이전틱 AI 도입의 효과성 및 글로벌 확장성이 높은 분야 중심으로 선정 예정

** AI 파운데이션 모델·AI 서비스 개발사·인프라 기업·수요기업 등

- 기업이 AI 에이전트를 자체 개발·운영할 수 있도록 도입 진단, 위험관리, 운영 체계 수립 등 전문가 컨설팅 지원('27년~)
- 산업별 수요·서비스 유형 및 기업 현황을 종합, 'AI 에이전트 산업 지도'를 구축, 서비스 발굴·실증·확산과 연계('26년~)
- 기존 규제로 실증이 어려운* AI 에이전트 서비스에 대해 ICT 규제 샌드박스 연계를 통해 실증 기회를 확대('26년~)

* AI 에이전트는 멀티에이전트 연쇄 작동, 자율적 의사결정 등 기존 규제 프레임으로 대응이 어려워 전 주기적 규제 실험 인프라 필요

□ 향후 계획

- 민·관 합동 에이전틱 AI 얼라이언스('26.4월 발족, 280여개 기업 참여를 중심으로 정책 세부 내용 구체화('26.하반기))

< 에이전틱 AI Alliance 분과 구성(안) >

