과학기술정보통신부

보도자료

대체불가 대한민국

보도시점 2026. 11. 6.(금) 11:00 (2026. 11. 6.(금) 석간) 배포 2026. 11. 5.(목) 14:00

과기정통부, 에이전틱 AI 이용 환경에서 제로트러스트를 적용할 수 있는 안내서 발간

【관련 국정과제】 23-4. AI시대를 지탱하는 견고한 디지털 보안·안전 체계 구축

과학기술정보통신부(부총리 겸 과학기술정보통신부 장관 배경훈, 이하 '과기정통부')와 한국인터넷진흥원(이하 'KISA')은 산·학·연 전문가들과 함께 **국내·외 주요 AI 보안·제로트러스트 가이드**를 분석하고 **수요·공급기관 대상 의견수렴**을 거쳐 **국내 기업들이 에이전틱 AI를 도입하고 운영하는 환경에서 제로트러스트를 적용**할 수 있는 **「에이전틱 AI 제로트러스트 안내서」**(이하 '안내서')**를 마련**하였다고 밝혔다.

최근 클라우드 이용 확대, AI 기반 업무 자동화 등 **기업의 업무환경이 빠르게 변화**하고 있다. 특히 **AI가 단순한 정보 분석·생성**을 넘어 **스스로 판단하고 도구를 활용해 업무를 수행**하는 **에이전틱 AI(Agentic AI)로 발전**하면서, 기존의 사용자·단말·서버뿐 아니라 **AI 에이전트가 접근**하는 **외부 서비스와의 상호작용**, **물리적 장치에 대한 명령 등**으로 **통제 대상이 확대**되고 있다.

이에 따라 정부는 **기존 보안체계**로는 대응하기 어려운 **에이전틱 AI의 자율성**과 높은 권한에서 비롯되는 **보안위협을 최소화**하고, **에이전틱 AI가 수반하는 고유 위협**(프롬프트 오염, 위임된 권한을 넘어선 자율 행동 등)에 대해 제로트러스트* 적용을 통해 예방·대응 할 수 있는 보안조치를 반영한 안내서를 마련했다.

* 정보시스템 등에 대한 접속 요구가 있을 때 네트워크가 이미 침해된 것으로 간주하여 **"절대 믿지 말고, 계속 검증하라(Never Trust, Always Verify)"**는 **보안 개념**

이번 안내서는 기업의 **제로트러스트 적용 절차 및 도입 방향**을 제시한 「**제로트러스트 가이드라인 2.0('24. 12.)**」을 토대로 기존 가이드라인에서 정의한 **'성숙도 모델*'**을 **에이전틱 AI 이용 환경에 맞게 확장하고 구체적인 적용 기준을 제시하는 방식으로 안내서를 고도화**하였다.

* 각 기업이 제로트러스트를 도입하고자 할 때 현재 기업 보안 수준을 진단·분석 후 목표를 설정하고 검증하는데 활용할 수 있도록 정의한 4단계 보안 분류체계

특히, **에이전트의 자율 행위**(입력 처리, 도구 호출, 작업 위임, 외부 통신 등)가 이루어지는 **여러 지점**에서 **해당 행위를 검증**하고 **정책을 집행**하며, **위험 수준**에 따라 **인간의 승인**이나 **사전에 승인된 정책을 적용**하도록 하였다. 또한 **조직이 현재 보안 수준을 자가 진단**하고 **우선순위**에 따라 **개선**할 수 있도록 **성숙도 단계별 실무 기준을 제시**하였다.

아울러, 에이전틱 AI 환경에서 제로트러스트를 도입할 때의 **고려사항**과 **단계별 도입·운영 절차** 및 관련 사항을 **자체 적용**할 수 있는 **제로트러스트 활용 예시** 등을 제시함으로써 기업이 에이전틱 AI 환경의 제로트러스트 **도입부터 운영·개선 단계**까지 **안내서**를 활용할 수 있도록 하였다.

안내서의 상세 내용은 **KISA 누리집**(www.kisa.or.kr)에서 **확인**할 수 있다.

과기정통부 임정규 정보보호네트워크정책관은 "**기업 업무에 AI 활용이 증가**하는 상황에서 **에이전틱 AI에 제로트러스트를 적용**할 수 있는 안내서가 나온 것은 시의적절하다"면서, "정부는 **제로트러스트 보안 모델 구축 사업**을 수행함과 동시에, **제로트러스트 적용 가이드** 등을 **지속적으로 발간**함으로써 제로트러스트의 **민간 자율 확산 기반**을 마련해 나가겠다"라고 말했다.

담당 부서	정보보호네트워크정책실 정보보호산업과	책임자	과 장	이종혁 (044-202-6450)
		담당자	사무관	이원규 (044-202-6451)
유관 기관	한국인터넷진흥원 AI보안기술팀	책임자	팀 장	이재형 (061-820-1550)
		담당자	책임연구원	이혜진 (061-820-1555)

대체불가 대한민국
내일을 만드는 과학기술 내삶을 채우는 디지털·AI
대한민국 정책브리핑
OPEN 출처표시 공공누리 공공저작물 자유이용허락
OPEN 인공지능 학습용 공공누리 공공저작물 자유이용허락