

글로벌 인공지능 기업의 사이버보안 프로젝트 대응 관련 산학연 전문가와 간담회

- AI 기업, 정보보호학회 및 산업계, AI 보안전문가와 '미토스' 등 AI 모델의 사이버보안 활용 관련 국내 영향과 향후 대응방안 등 논의

과학기술정보통신부(부총리 겸 과학기술정보통신부장관 배경훈, 이하 “과기정통부”)는 5월 8일(금) 글로벌 인공지능 기업의 사이버보안 프로젝트 관련 대응방안을 논의하기 위해 산학연 전문가들과 간담회를 개최하였다고 밝혔다.

최근 美 엔트로픽과 오픈에이아이사는 고성능 보안역량을 보유한 자사의 최신 AI 모델을 파트너사에 제공하는 프로젝트를 가동하여 주목을 받고 있다.

- ※ 【엔트로픽】 Mythos 기반 'Project Glasswing' 프로젝트(26.4), 【오픈AI】 GPT-5.5-Cyber 기반 'Trusted Access for Cyber' 프로젝트(26.2)

이에 과기정통부는 전국 CISO(약 3만여 개사)를 대상으로 지난 4월 14일 보안 대비태세 점검을 요청한 데 이어, 지난 4월 30일에는 'AI 기반 사이버공격 대비 기업 대응 요령 및 CEO 행동 수칙' 을 추가로 배포한 바 있다.

이번 간담회는 고성능 AI 모델에 대한 보안영향과 향후 대응방안에 대해 각 분야 전문가의 의견을 충분히 청취하고자 마련된 것으로,

SKT, 업스테이지, 모티프테크놀로지스 등 독자 파운데이션 모델 개발 참여기업과 주요 AI 기업, 한국정보보호학회장을 비롯한 AI 보안 분야 학계 전문가, 한국정보보호산업협회장을 비롯한 주요 정보보호기업 대표, 주요 기업 CISO 등이 참여하여 각자 분야에서의 AI 모델의 영향과 향후 대응방안에 대한 다양한 의견을 개진하였다.

참석자들은 AI 보안모델의 영향에 대해 사이버보안 분야에 상당한 변화를 줄 것이라는 견해와, 과대평가된 측면이 있어 우려가 과도하다는 의견 등

평가는 엇갈렸으나, 미토스 등 고성능 AI 기반 사이버보안 서비스의 등장에 따라 민관이 함께 머리를 맞대고 장단기 대응방안을 모색해야 할 시점이라는 점에는 의견이 일치하였다.

특히, 참석자들은 글로벌 인공지능 기업의 사이버보안 프로젝트 참여 등을 통한 정보비대칭 해소 노력과 함께, AI로 인한 사이버 위협을 AI 보안역량 강화로 대응하기 위해 민관이 합심하여 AI 보안주권을 확립하는 일이 무엇보다 중요하다고 강조하였다.

배경훈 부총리는 “이번 이슈로 인해 우리 사회 정보보호 패러다임도 이제 AI기반 보안으로 대전환을 더 늦추기 어려운 상황이다” 라며, “국내 AI 보안 특화 모델 개발을 추진하는 한편, 사회 전 분야에 제로트러스트 철학의 확산, 양자보안 등 원천적인 방어체계 확립 등 관련 대응방안을 각 분야 전문가와 함께 조속히 마련하겠다” 고 밝혔다.

담당 부서	정보보호네트워크정책관 정보보호산업과	책임자 담당자
-------	------------------------	------------

내일을 만드는 과학기술
내 삶을 채우는 디지털·AI