



국가AI전략위원회, '해커 울리는 AI시대를 연다' 『동형암호 기반 LLM과 AI데이터 보호』 세미나 개최

- 보안특위, 동형암호 분야 세계적 권위자 서울대 천정희 교수 초청 발제
- 데이터는 '유출'되도 '피해'는 '제로', 동형암호 상용화 방안 심층 논의

국가인공지능전략위원회 (위원장 이재명 대통령, 이하 '위원회')는 4월 9일 (목) 오전 10시, 보안특위 주관으로 서울대 천정희 교수를 초청하여 「동형암호 기반 LLM과 AI 데이터 보호」라는 주제로 세미나를 개최했다.

발제는 세계 최초로 상용화 가능한 동형암호(Homomorphic Encryption) 알고리즘을 개발한('17) 세계적 동형암호 분야 권위자 서울대 천정희 교수가 맡았다.

지난해 SKT, 롯데카드 등 연이은 정보유출 사태에 이어 최근 국민 일상 정보를 도맡아 처리하는 AI에이전트 활용이 급격히 확산되면서 사이버 보안 위협은 그 어느때 보다 가중되고 있다. 이번 세미나는 고도화되는 모든 해킹 공격을 막아내는 것은 더 이상 불가능하다는 현실을 직시하고, 방어에만 몰두하던 과거의 '해킹 방지'에서 벗어나, 데이터가 탈취되더라도 '실질적 피해를 차단'하는 차세대 보안 전략을 모색하기 위해 마련되었다.

세미나에서는 암호화된 상태에서 복호화 없이도 연산을 수행할 수 있게 하는 동형암호 기술에 대한 소개와 함께, 지난 10여 년간 연산속도 10억배 이상 향상 등 동형암호 기술의 발전 상황과 생성형 AI 분야 적용 사례, 나아가 동형암호 기술 활용을 통한 국내 데이터 주권 확보와 소버린 AI 구현 방안, 그리고 이를 뒷받침 할 국내 법·제도 개선 제언 등이 소개되었다.

관련 보안특위 위원들뿐만 아니라 국방분과 위원, 그리고 국정원, 과기정통부, 개인정보보호위원회, 한국인터넷진흥원 등 AI·데이터 보안 정책을

담당하는 정부부처 및 유관기관 관계자들도 대거 참석했으며 참석자들은 암호화된 상태로 AI를 학습하고 추론하는 동형암호 기술이 정보 보호와 AI 산업 발전을 동시에 달성할 수 있는 핵심 열쇠라는 데 공감했다.

이원태 보안특위 위원장은 “AI에이전트 시대 국민들이 일상에서 그 혜택을 안심하고 누리기 위해서는 '내 데이터가 안전하게 보호된다'는 확실한 신뢰가 전제되어야 한다”며, “오늘 소개된 동형암호 기술은 AI에이전트 시대 공공·의료·금융 등 사회 전반의 AI 서비스 질을 획기적으로 끌어올리는데 기여할 든든한 기반 기술이 될 것”이라고 평가했다.

임문영 부위원장은 “보안은 AI시대 본질이며, 국가 AI 경쟁력은 이제 단순한 모델 성능을 넘어, 데이터를 얼마나 안전하게 통제하고 지켜낼 수 있는지에 달렸다”며, “오늘 제언된 동형암호와 같은 새로운 보안 기술 정책이 공공과 민간 영역에 신속히 적용·확산될 수 있도록 관계 부처와 적극 협력해 나가겠다”고 밝혔다.

※ 유튜브 생중계 링크: <https://www.youtube.com/live/j7QmCiowz7k>

담당 부서	국가인공지능전략위원회 AI데이터·규제혁신팀	책임자	팀 장	유경태 (02-2224-4131)
		담당자	사무관	강영근 (02-2224-4138)

내일을 만드는 과학기술
내 삶을 채우는 디지털·AI

대한민국
정책브리핑

