[기조강연IV]

[생성형 AI 시대의 사이버보안]

국가보안기술연구소 류승진

경력

'24년 1월 – 현재	정보처리학회 데이터보안 및 프라이버시 연구회 운영위원
'22년 1월 – 현재	정보보호학회 AI보안연구회 운영위원
'22년 1월 – 현재	국가보안기술연구소 인공지능보안실장
'13년 12월 – 현재	국가보안기술연구소 연구원

발표내용

생성형 AI의 활용이 급격히 확대됨에 따라, AI 보안의 중요성 또한 크게 부각되고 있다. 본 발표에서는 AI 시스템 자체의 보안(Security for AI)과AI를 악용한 허위·조작 정보 대응 기술을 중점적으로 살펴보고자 한다. 먼저 AI 시스템의 취약점(특히, OWASP Top 10 for LLM Applications에서 제시한 대표적 위협을 중심으로)을 살펴보고, 이에 대한 대응 기술을 간단히 소개한다. 이어서 딥페이크를 비롯한 AI 생성 콘텐츠의 악용 사례와 이를 방어하기 위한 대응 기술을 검토하며 발표를 마무리하고자 한다.