

# 『IITP 테크&퓨처 인사이트 콘서트 × IT 메가비전 2026』 계획안 ( IITP Tech & Future Insight Concert × IT Mega-vision 2026 )

( '26. 6. 30(화), 디지털보안팀 )

## □ 개 요

- (행사명) “IITP 테크&퓨처 인사이트 콘서트 × IT 메가비전 2026”  
 - 주최·후원 : IITP 및 전자신문사 / 과학기술정보통신부 등
- (일시·장소) '26.9.16(수), 서울드래곤시티 그랜드볼룸 한라홀

## □ 구 성(안)

### ○ 프로그램 안

일정	시간	구분	프로그램	기타
구분		IITP 테크&퓨처 인사이트 콘서트 × IT 메가비전 2026 <sup>(300명)</sup>		
09:30~10:00	30'	등록		
10:00~10:08	08'	개회	오프닝 영상, 개회선언 및 내빈소개	사회자
10:08~10:20	12'		주요 내빈 인사 말씀 및 축사	IITP, 과방위 등
10:20~11:20	60'	기조강연	(강연1, 기업) AI시대 사이버전의 공격자와 방어자 (강연2, 대학) AI 대전환, K-Cyber Security	기획 중
11:20~11:50	30'	정책좌담	국가 AI보안 경쟁력 확보를 위한 K-Cyber Security 전략	
11:50~13:00	70'	오찬		
		Track① (IITP 테크&퓨처 인사이트 콘서트, 150명)		Track② (전자신문사 IT 메가비전, 300명)
13:00~14:30	90'	■ 공급망·인프라 보안 영역 : 3개 발표		■ AI 보안 영역 : 3개 발표
14:30~14:45	15'	휴식		휴식
14:45~16:15	90'	■ 데이터·양자 보안 영역 : 3개 발표		■ AI 보안 영역 : 3개 발표
16:15~		폐회·정리		

※ 오후 Track ①, ② (공급망·인프라 보안 / 데이터·양자 보안 / AI 보안 주제로 발표자 신청을 받고 있습니다.

( ~ 7.10.(금)까지 이메일 신청 부탁드립니다. ( [ces@kisia.or.kr](mailto:ces@kisia.or.kr) )

□ **오후 발표 주제 (안)**

○ **[Track①] 공급망·인프라 보안 (13:00~14:30)**

영역	<ul style="list-style-type: none"> <li>SW 공급망, 오픈소스, 클라우드, 데이터센터 및 국가정보통신망의 신뢰성 확보를 위한 공급망·인프라 보호 기술 분야</li> </ul>
운영목적	<ul style="list-style-type: none"> <li>공급망 공격 증가와 국가 핵심기반시설 대상 사이버위협에 대응하기 위한 핵심 보안기술 성과를 공유하고 디지털 인프라의 안정성 확보 방안 제공</li> </ul>
기술분야	<ul style="list-style-type: none"> <li>(SBOM) SW를 구성하는 모든 요소를 목록화하여 공급망 내 취약점과 보안 위험을 체계적으로 관리하는 기술</li> <li>(제로트러스트) 사용자와 기기를 신뢰하지 않고 지속적인 인증과 검증을 통해 접근을 통제하는 보안 모델</li> <li>(클라우드 보안) 클라우드 환경의 데이터와 서비스, 인프라를 보호하여 안전한 디지털 운영을 지원하는 기술</li> <li>(오픈소스 보안) 오픈소스 SW의 취약점과 악성코드 위험을 탐지·관리하여 SW공급망의 안전성을 확보하는 기술</li> <li>(인프라 보호) 네트워크와 서버 등 핵심 정보통신 인프라의 안정성과 가용성을 보장하기 위한 보안 기술</li> </ul>

○ **[Track①] 데이터·양자 보안 (14:45~16:15)**

영역	<ul style="list-style-type: none"> <li>양자컴퓨팅 시대 도래에 대비한 차세대 암호기술과 데이터 보호 기술 분야로서 양자 내성암호(PQC), 동형암호, 영지식증명, 프라이버시 보호 기술 등을 포함</li> </ul>
운영목적	<ul style="list-style-type: none"> <li>미래 보안환경 변화에 선제적으로 대응하기 위한 암호 원천기술 확보 및 데이터 활용·보호 기술의 발전 방향 공유</li> </ul>
기술분야	<ul style="list-style-type: none"> <li>(양자내성암호) 미래 양자컴퓨터의 공격에도 안전한 암호체계를 구현하기 위해 개발된 차세대 암호기술</li> <li>(동형암호) 데이터를 복호화하지 않은 상태에서 연산이 가능하도록 하여 개인정보를 안전하게 활용하는 암호기술</li> <li>(개인정보보호) 개인정보의 수집·이용·저장 과정에서 유출과 오남용을 방지하여 정보주체의 권리를 보호하는 기술</li> <li>(데이터 신뢰성) 데이터의 무결성과 정확성, 진위 여부를 검증하여 신뢰할 수 있는 데이터 활용 환경을 제공하는 기술</li> <li>(영지식증명) 정보의 내용을 공개하지 않고도 해당 정보를 보유하고 있음을 증명할 수 있는 암호기술</li> </ul>

○ **[Track②] AI 보안 (13:00~16:15)**

영역	<ul style="list-style-type: none"> <li>생성형 AI, LLM, AI 에이전트 등 인공지능 기술의 확산에 따라 발생하는 신규 보안위협에 대응하고, AI를 활용하여 사이버 공격을 탐지·분석·예측하는 지능형 보안기술 분야</li> </ul>
운영목적	<ul style="list-style-type: none"> <li>AI 기반 사이버위협 대응기술과 AI 자체의 안전성 확보 기술을 공유함으로써 국내 AI 보안 기술 경쟁력 강화 및 산업 적용 확산 기반 마련</li> </ul>
기술분야	<ul style="list-style-type: none"> <li>(AI 에이전트 보안) 자율적으로 의사결정을 수행하는 AI 에이전트의 권한 오남용과 보안 위험을 통제하는 기술</li> <li>(생성형 AI 보안) 생성형 AI의 정보유출·악용, 프롬프트 공격 등의 위험을 방지하여 안전한 AI 활용 구축 기술</li> <li>(LLM 보안) 대규모 언어모델의 취약점과 데이터 유출 위험을 분석·방어하여 신뢰성을 확보하는 기술</li> <li>(AI기반 위협탐지) 인공지능을 활용하여 사이버 공격과 이상행위를 실시간으로 탐지·예측하는 보안 기술</li> <li>(AI 취약점 분석) AI 모델과 시스템의 보안 취약점을 식별·평가하여 안전성과 신뢰성을 강화하는 기술</li> </ul>