정보보호 주간 R&D 기술·성과교류 계획(안)

('25.7.1.(화), 디지털보안팀)

□ 개요

○ (목적) 정보보호 R&D 성과를 공유하고, 혁신적 성과 창출을 위해 연구자 수요자가 함께 새로운 아이디어를 발굴하는 긍정환류 도모

- 2025 정보보호 주간 부대 행사로 연계(참고1 참조), 슬로건(AI 시대 보안으로 신뢰를 더하다)과 관련된 과제로 구성

* 대상 과제 네트워크·클라우드 보안(8개)+데이터·AI보안(9개)(참고2 참조)

○ (일시/장소) '25.7.10.(목) 10:00~18:00, 용산 로카우스 호텔 6층 플로리스홀

* 행사 진행은 온-오프라인 병행으로 추진

○ (참석자) 과제 연구책임자, 기술교류회 참관자, IITP 디지털보안팀 등

□ 프로그램(안)

○ 정보보호 R&D 방향성①, 정보보호 R&D 혁신성과 발표·전시②, 과제 중간 성과 공유 및 전문가 피어리뷰③, VC 투자 방향④ 등 4가지 세션으로 구성

세션	시간		주요 내용	비고
	10:00~10:05	5′	행사소개	IITP
	10:05~10:10	5′	인사말씀	과기부
1	10:10~10:30	20′	정보보호 R&D 추진방향	김창오 정보보안 PM
2	10:30~10:50	20′	이벤트 기반 실험시스템 구축을 통한 자동차 내·외부 아티팩트 수집 및 통합 분석 기술 개발	우사무엘(단국대)
	10:50~11:10	20′	AI·빅데이터 기반 사이버보안 오케스트레이션 및 자동대응 기술 개발	김태은(KISA)
	11:10~11:20	10′	커피 Break	
	11:20~11:40	20′	5G기반 선제적 위험대응을 위한 예측적 영상보안 핵심기술 개발	김건우(ETRI)
	11:40~12:00	20′	대용량 정형 데이터 대상 개인정보 가명익명처리 자동화 및 안전성 검증 기술개발	심기창(이지서티)
	12:00~13:30	90′	점심식사	-
3	13:30~14:10	40′	프라이버시 보호를 위한 고성능 머신언러닝 기술개발	구자동(에이아이딥)
	14:10~14:50	40′	자가진화형 AI 기반 사이버 공방 핵심원천기술 개발	문대성(ETRI)
	14:50~15:00	10′	커피 Break	
	15:00~15:40	40′	AI 역기능 억제를 위한 사이버 보안 특화 RAG 기반 sLLM 모델 개발 및 국민 체감형 실증 플랫폼 구축	김기홍(샌즈랩)
	15:40~16:20	40′	생성형 AI 보안 위협 대응 기술 개발	최대선(숭실대)
	16:20~16:30	10′	커피 Break	
4	16:30~17:00	30′	정보보호기업의 기술화사업화 및 투자유치 전략	VC
	17:00~17:10	10′	마무리	IITP
	17:10~17:50	40′	네트워킹 및 밋업	자율

1 정보보호 R&D 추진 방향 제시

- AI 기술의 일상화로 서비스·모델 등이 확산하는 시기에, 기반 기술로서 **정보보호 R&D가 나아가야 할 방향성** 등 제시

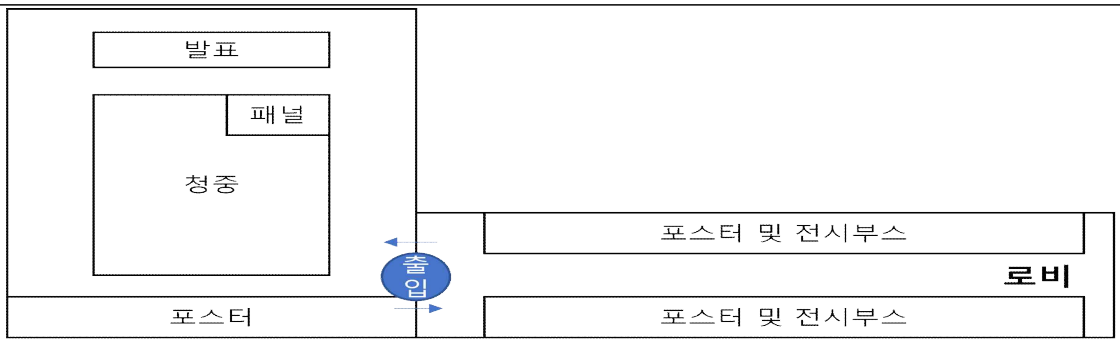
2 정보보호 혁신성과·우수사례 공유·부스 전시

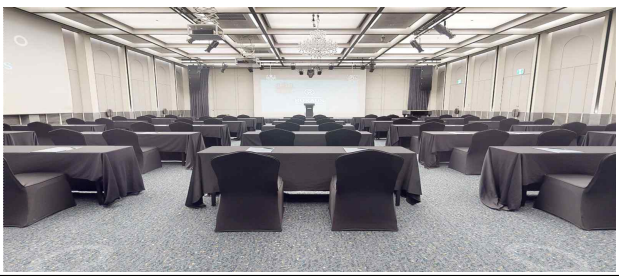
- 정보보호 분야에서 혁신적인 성과를 창출한 우수과제를 선정하여 **성과 발표, 시연** 및 **성과물 부스 내 전시** 등
- ①자율주행자동차 사고조사, 개인정보 삭제, EDR Chip-Swap, 자동차 디지털 포렌식 기술 등 성과 전시 및 상주 인원 대응[단국대]
- ②개인정보 가명·익명처리 자동화 및 안전성 검증 성과 부스 내 동영상 시연 및 질의 응답 시 상주 인원 대응[이지서티]
- ③프라이버시 보호를 위한 고성능 머신 언러닝 기술 부스 내 동영상 시연 및 질의 응답 시 상주 인원 대응[에이아이딥]
- ④딥페이크 탐지 서비스, LLM 필터 기술 등 시연 및 질의 응답 시 상주 인원 대응[샌즈랩]

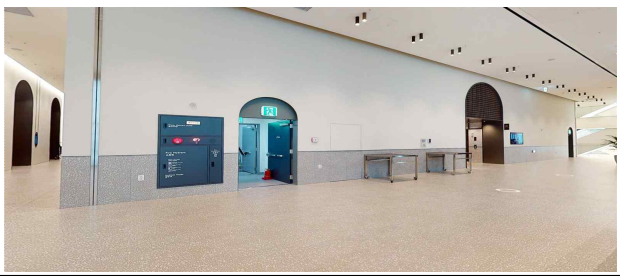
3 과제 중간 성과 공유 및 전문가 피어리뷰 추진

- 그간 추진 된 과제의 **중간 연구성과를 공유**하고, 피어리뷰를 통해 **연구성과·계획 토론 및 개선의견 제시**(발표(25분)+질의응답(15분))
- 과제 연구성과 등을 **포스터로 게재**, 메모함을 설치하여 행사 중 언제든 **자유롭게 피어리뷰어들이 의견 제시** 가능

* 현장 발표 제외 나머지 포스터 게재 및 온·오프라인 피어리뷰 13개 과제







4 VC, 투자자 등 정보보호 분야 투자유치 노하우 등 공유

- 연구개발 과제 등이 사업화, 성과, 기업 성장으로 연계되기 위한 실제 투자자 입장에서 바라보는 **투자유치 전략·노하우** 등 **공유**

□ 행사 홍보

○ 정보보호 주간 통합 행사 홍보(6.30~)

- 과기부 및 KISA 주관 통합 홍보 자료 배포(영상, 팜플렛 등)

○ IITP 기술성과교류회 별도 홍보(7.1~)

- 기술성과교류회 포스터 제작 후 학·협회 네트워킹을 활용하여 배포
- 주요 매체 지면 보도 추진 및 행사 관련 기획 기사 발간

참고1 2025 정보보호 주간(Week) 추진 기본계획(안)

□ 개 요

○ (목적) 기존 산업계, 학계 등이 **분산 운영** 중인 **정보보호 행사**를 **통합**한 '**정보보호 주간**'을 새롭게 운영하여 정보보호 정책·의지 홍보 강화

○ (기간/장소) '25. 7. 7.(월)~7. 11.(금) / 일자별 별도 장소

※ **제14회 정보보호의 날 '25.7.9.(수)**(매년 7월 둘째주 수요일, 법정기념일)

○ (슬로건안) **"AI 시대, 보안으로 신뢰를 더하다"**

○ (핵심 메시지) 정부 및 **정보보호 산업계, 학계, CISO 등** 이해관계자들이 '**원팀**'이 되어 '**AI 시대**'에 사이버보안이 **나아가야 할 방향** 제시

□ 정보보호 주간 "UNITED"

○ (구성) 사이버보안 관련 학계, 산업계, 기술개발 참여 기관, 인재 등 **사이버보안 생태계 참여자**들이 **요일별**로 **행사 구성**

- '정보보호의 날'에는 정부, 학계, 산업계, CISO, 지역 등 **생태계 참여자**들이 **모두 참여**하는 **정보보호 축제의 장**으로 운영

○ (주빈) 다가오는 AI 시대에 정보보호의 중요성을 강조하고 정부의 정보보호 지원 의지표명을 위해 **V 주관**(제한시 총리님) **행사**로 건의

※ 역대 참석자 : ('22) VIP, ('23) 국무총리, ('24) 과기정통부장관(V 서면 축전)

구분	Day1(7.7)	Day2(7.8)	Day3(7.9)	Day4(7.10)	Day5(7.11)
컨셉	University (학계)	Network (산업계, 글로벌)	Integrate (통합·조화)	Technology (기술)	Educate (인재양성)
내용	•정보보호학회 워크샵국	•CISO KOREA 2025차 •팀 시큐리티 코리아 발대식차 •CAMP 10주년 기념실	•정보보호의 날 기념식V •지자체 사이버보안 협의회 발대식장 •사이버보안 정책 포럼 세미나실	•R&D 사업성과 공유회과 •랜섬웨어 레질리언스 컨퍼런스국	•코드게이트 해킹방어대회실 •국제 해킹대회 출정식국 •정보보호 루키 Meet-Up Day과
주관	한국정보보호학회	CISO협의회, KISA	KISA, 지자체, KISIA	IITP, KISA	Codgate,, KITRI, KISA

참고2 정보보호 기술·성과 교류회 참석 과제 등

□ 대상 과제(정보보호핵심원천 17개) 현장 발표과제

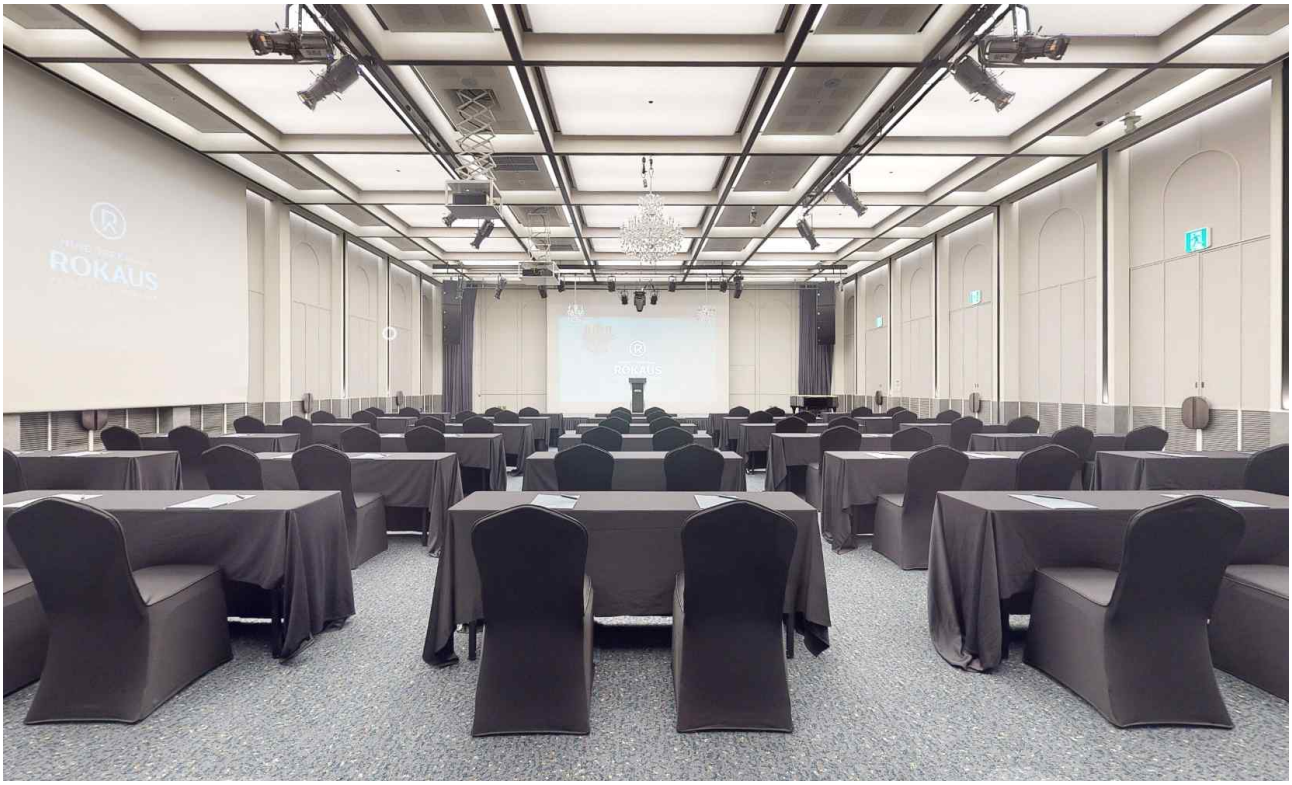
- 데이터·AI보안 과제협의체(9개)

No	과제명	주관기관 (연구책임자)	연구기간
1	하드웨어 중심 신뢰계산기반과 분산 데이터보호 박스를 위한 표준 프로토콜 개발	고려대학교 (이중희)	'21.4~'26.12
2	프라이버시 보호를 위한 고성능 머신 언러닝 기술 개발	에이아이딥 (구자동)	'24.6~'27.12
3	AI 역기능 억제를 위한 사이버 보안 특화 RAG 기반 sLLM 모델 개발 및 국민 체감형 실증 플랫폼 구축	샌즈랩 (김기홍)	'24.4~'27.12
4	자가진화형 AI 기반 사이버 공방 핵심원천기술 개발	ETRI (문대성)	'22.4~'27.12
5	미래컴퓨팅 환경에 대비한 계산 복잡도 기반 암호 안전성 검증 기술개발	ETRI (강유성)	'19.4~'26.12
6	안전한 다자간 데이터 결합을 위한 프라이버시 보존형 다자간 비밀연산 기술개발	중앙대학교 (이형태)	'24.4~'29.12
7	생성형 AI 보안 위협 대응 기술 개발	숭실대학교 (최대선)	'24.4~'27.12
8	AIM : AI 기반 차세대 보안 정보관리기법적용 Cognitive Intelligence 및 Secure-오픈 프레임워크(S-OFW) 기술 개발	차의과학대학교 (한현욱)	'19.4~'26.12
9	내용기반 중요정보 분류 및 등급별 보안서비스 기술 개발	고려대학교 (허준범)	'22.4~'27.12

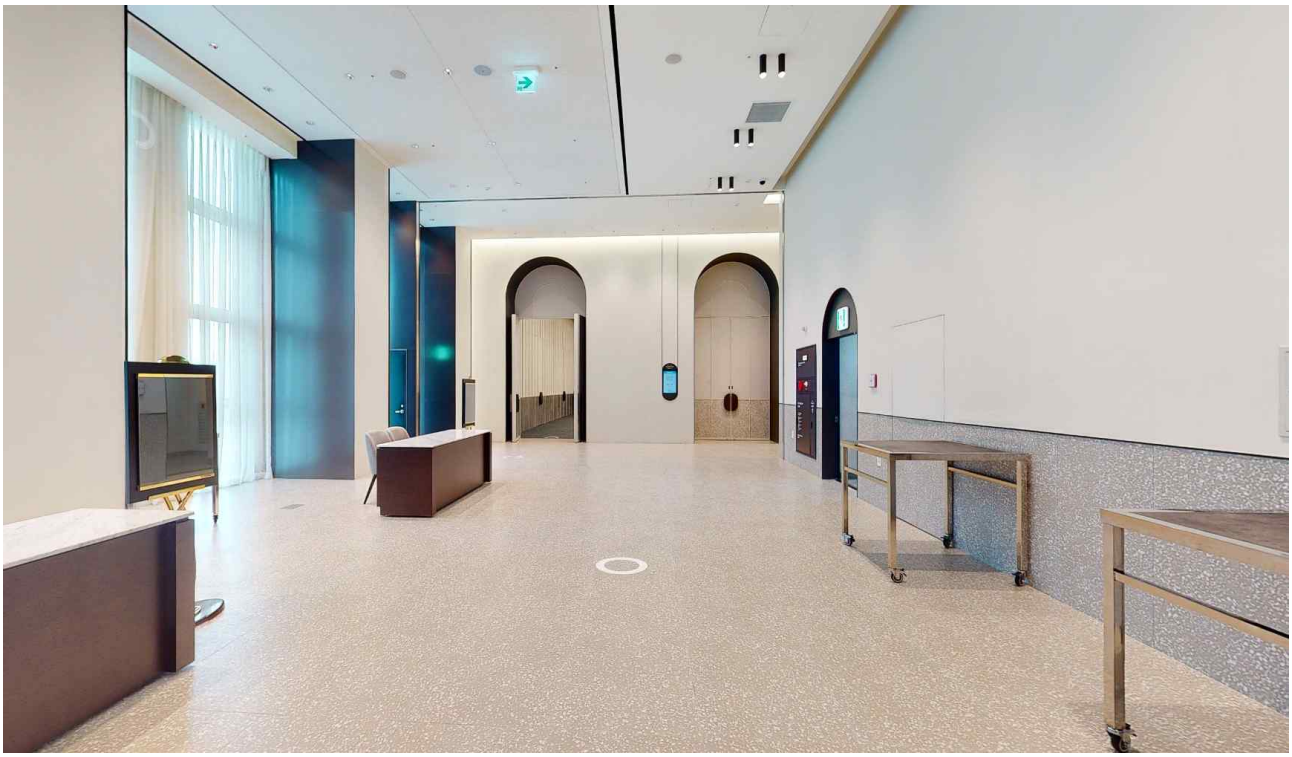
- 네트워크 · 클라우드보안 과제협의체(8개)

No	과제명	주관기관 (연구책임자)	연구기간
1	프라이버시 보존형 내부 보안정보의 보안관제 연계·활용기술 개발	ETRI (강동호)	'24.6~'26.12
2	5G특화망·유·무선 통합환경에서 네트워크 슬라이싱 기반서비스의 보안 리질리언스 기술 개발	ETRI (김정태)	'24.6~'27.12
3	다크웹 은닉서비스 식별 및 근원지 추적기술 개발	㈜에스투더블유 (윤창훈)	'22.4~'25.12
4	5G+ 기반 6G 이동통신 정보보안 기술 연구	국민대학교 (이옥연)	'20.4~'27.12
5	특화망·기업망 통합보안을 위한 5G 특화망 보안 기술개발	ETRI (이종훈)	'24.4~'27.12
6	양자보안 기반 5G 특화망 기기 식별 기술 및 시험검증 기술개발	TTA (전숙현)	'24.4~'29.12
7	클라우드 기반 사이버 훈련장 구축 기술 및 사이버 훈련 시나리오 기술 언어(K-SDL) 개발	코어시큐리티 (주한익)	'24.6~'27.12
8	안전한 클라우드 네이티브 환경을 위한 클라우드 심층방어 보안 프레임워크 기술 개발	㈜SGA솔루션즈 (최영철)	'24.4~'27.12

참고3 행사장소(용산 프리미어 로카우스 호텔 플로리스 홀)



[행사장 내부]



[행사장 외부 로비]

[행사장 오시는길 – 용산구 한강대로23길 25]