한국정보보호학회
Korea Institute of Information Security & Cryptology

2026년 한국정보보호학회 동계학술대회

CISC-W'26

Conference on Information Security and Cryptography Winter 2026

2026년 10월 28일(수)~30(금) | 여수 베네치아 호텔&스위트

주최·주관
한국정보보호학회

후원
과학기술정보통신부, 행정안전부, 한국인터넷진흥원, 한국전자통신연구원, 국가보안기술연구소, 한국과학기술정보연구원

기업·기관 후원
AWS, ICTK, KT, 네이버클라우드, 스마트엠투엠, 씨큐립톤, 유니스소프트, 유비벨록스, 쿤텍, 트리즈엔,
한국기계전기전자시험연구원, 한국보안인증, 한국시스템보증, 한국정보통신기술협회

대학후원
가천대 CPS보안연구센터, 가천대 대학원 정보보호학과, 가천대 스마트보안학과, 가천대 융합보안대학원 사업단,
강원대 데이터보안활용혁신융합대학 사업단, 강원대 융합보안학과, 고려대 AI보안연구소, 고려대 정보보호대학원,
고려대 정보보호대학원 EMSEC, 고려대세종 엣지클라우드데이터보안연구센터, 고려대세종 융합보안대학원,
고려대세종 정보보호특성화대학, 국민대 국방사이버전자전연구소, 국민대 글로컬랩 방산기술보호연구소,
국민대 정보보안암호수학과, 덕성여대 사이버보안연구실, 부산대 블록체인플랫폼연구센터,
부산대 제로트러스트 클라우드보안연구센터, 서울과학기술대 BK21 능동적 사이버보안 교육연구단,
서울과학기술대 암호 및 정보보호 연구실, 성신여대 융합보안공학연구소, 성신여대 융합보안전문대학원,
세종대 SysCore Lab., 세종대 정보보호특성화사업단, 숭실대 AI보안연구센터, 숭실대 AI안전성연구센터,
숭실대 사이버보안연구센터, 아주대 데이터보안활용융합사업단, 아주대 정보보호응용및보증연구실,
연세대 AI보안연구실, 연세대 CPS보안연구실, 인하대 컴퓨터공학과, 중앙대 데이터프라이버시연구센터,
중앙대 융합보안대학원 사업단, 한남대 고성능&보안컴퓨팅연구실, 한성대 융합보안학과,
한양대 임베디드보안 및 프라이버시 연구실@ERICA

위원회

학술대회장

한국정보보호학회 회장 김호원 (부산대학교)

조직위원회

- 조직위원장: 박영호 (세종사이버대학교)
- 조직위원: 이정현 (숭실대학교), 김우년 (국가보안기술연구소), 김건우 (한국전자통신연구원), 송중석 (한국과학기술정보연구원), 오진영 (한국인터넷진흥원)

운영위원회

- 운영위원장: 한동국 (국민대학교), 김환국 (국민대학교)
- 운영위원: 강동호 (한국전자통신연구원), 강봉호 (ICTK), 곽진 (아주대학교), 김영수 (고려대학교), 김우환 (국가보안기술연구소), 박기웅 (세종대학교), 박해룡 (한국인터넷진흥원), 박애선 (국방부), 방혁준 (쿤텍), 변동훈 (코나아이), 서승현 (한양대학교), 서정택 (가천대학교), 손경호 (강원대학교), 이봉수 (국가보안기술연구소), 이일구 (성신여자대학교), 이종현 (LIG D&A), 이주현 (777사령부), 이준 (한국과학기술정보연구원), 이창훈 (서울과학기술대학교), 임동혁 (알티스트), 정익래 (고려대학교), 조지훈 (삼성SDS), 조해현 (숭실대학교), 주범수 (프라이빗에이아이), 최윤호 (부산대학교), 한인성 (국방과학연구소)

프로그램 위원회

- 프로그램위원장: 최두호 (고려대학교)
- 프로그램위원: 강동호 (한국전자통신연구원), 한미란 (고려대학교), 김형식 (성균관대학교), 강민석 (한국과학기술원), 강아름 (배재대학교), 강유성 (한국전자통신연구원), 강정민 (고려대학교), 곽병일 (고려대학교), 곽진 (아주대학교), 구자훈 (고려대학교), 구형준 (성균관대학교), 권동현 (부산대학교), 권태경 (연세대학교), 권태웅 (한국과학기술정보연구원), 김도훈 (경기대학교), 김동우 (동국대학교), 김득훈 (아주대학교), 김범현 (한양대학교), 김병구 (한국전자통신연구원), 김수현 (순천향대학교), 김수형 (한국전자통신연구원), 김영수 (고려대학교), 김은영 (LIG D&A), 김정태 (한국전자통신연구원), 김종길 (이화여자대학교), 김종성 (국민대학교), 김준섭 (쿤텍), 김지윤 (경상국립대학교), 김진우 (충북대학교), 김태근 (고려대학교), 김태성 (충북대학교), 김현일 (조선대학교), 김형종 (서울여자대학교), 김효승 (한림대학교), 김희석 (고려대학교), 노희준 (인하대학교), 도경화 (서강대학교), 류권상 (국립공주대학교), 문영훈 (KT), 민무홍 (성균관대학교), 박기웅 (세종대학교), 박명서 (한성대학교), 박상욱 (한국전자통신연구원), 박승현 (한성대학교), 박정수 (강남대학교), 박종근 (한국전자통신연구원), 박종환 (상명대학교), 박철준 (경희대학교), 변진욱 (평택대학교), 서대희 (상명대학교), 서민혜 (덕성여자대학교), 서석충 (국민대학교), 서승현 (한양대학교), 서정택 (가천대학교), 서지원 (단국대학교), 서화정 (한성대학교), 성하영 (한국과학기술정보연구원), 손경호 (강원대학교), 송도경 (연세대학교)

위원회

송원준 (강원대학교)
신지호 (목원대학교)
오주형 (한국인터넷진흥원)
유지현 (광운대학교)
윤인수 (한국과학기술원)
윤택영 (단국대학교)
이근우 (국가보안기술연구소)
이동훈 (국가보안기술연구소)
이병영 (서울대학교)
이선우 (이화여자대학교)
이용준 (극동대학교)
이일구 (성신여자대학교)
이준 (한국과학기술정보연구원)
이태진 (가천대학교)
이현민 (한양대학교)
임재덕 (한국전자통신연구원)
장진수 (충남대학교)
전상훈 (수원대학교)
정성훈 (숙명여자대학교)
조금환 (고려대학교)
조효진 (연세대학교)
진범진 (아주대학교)
최선오 (전북대학교)
최윤호 (부산대학교)
한승훈 (숭실대학교)
황성재 (성균관대학교)
송현민 (단국대학교)
양대헌 (이화여자대학교)
우사이먼성일 (성균관대학교)
윤경국 (국립한국해양대학교)
윤종희 (영남대학교)
이경률 (국립목포대학교)
이덕규 (서원대학교)
이만희 (한남대학교)
이상만 (고려대학교)
이성재 (강원대학교)
이윤경 (한국전자통신연구원)
이종혁 (세종대학교)
이창훈 (서울과학기술대학교)
이학준 (국립금오공과대학교)
임송빈 (한국인터넷진흥원)
장대희 (경희대학교)
장항배 (중앙대학교)
전웅렬 (광주대학교)
정익래 (고려대학교)
조남수 (단국대학교)
주경호 (숭실대학교)
최대선 (숭실대학교)
최원석 (고려대학교)
최현우 (성신여자대학교)
홍득조 (전북대학교)
황현욱 (국가보안기술연구소)
신욱 (국가보안기술연구소)
오상학 (한양대학교)
유일선 (국민대학교)
윤명근 (국민대학교)
윤주범 (세종대학교)
이광수 (세종대학교)
이동재 (강원대학교)
이문규 (인하대학교)
이석준 (가천대학교)
이세영 (강원대학교)
이윤호 (서울과학기술대학교)
이종훈 (한국전자통신연구원)
이철호 (엔플러스랩)
이현우 (한국에너지공과대학교)
임을규 (한양대학교)
장준하 (공군사관학교)
전상훈 (국민대학교)
전유석 (고려대학교)
정혜야 (삼성물산)
조해현 (숭실대학교)
지승구 (한국인터넷진흥원)
최동현 (에스케이텔레콤)
최윤성 (부산교육대학교)
최현민 (단국대학교)
홍준호 (성신여자대학교)

번호	상장	논문번호	논문명	저자/소속
1	과기부 장관상	142	Talking-Head 생성 악용 방지를 위한 음성-이미지 정렬 교란 기반 음성 보호 기법	김다인, 김동현, 김승민, 최대선(숭실대학교)
2	행안부 장관상	190	공공기관의 효율적인 국가망보안체계(N²SF) 도입을 위한 의사결정 프레임워크	이찬형(한국전자통신연구원), 김효빈(성신여자대학교), 유광민, 황주하, 박기웅(세종대학교)
3	학회 최우수논문상	135	HAETAE 서명 구현에서 NTT 영역 계수별 곱셈에 대한 상관 전력 분석 공격	이광용, 안경덕, 하재철(호서대학교)
4	학회 최우수논문상	207	Hiworks Messenger의 Socket.IO 기반 통신 프로토콜 역공학을 통한 메신저 데이터 획득	신민석, 김한결, 최종윤, 박명서(한성대학교)
5	학회 최우수논문상	263	제조 이상 탐지의 제품 간 이전에 따른 순위 성능과 판정 오류 분석: MoECLIP과 CNN 비교	김나현, 최대호(서울과학기술대학교), 조재익(Lewis University), 이창훈(서울과학기술대학교)
6	KISA 원장상	9	메시지 기반 데이터센터 전송 암호화의 키 교환 개선	남재호, 강준혁, 권태경(서울대학교)
7	KISA 원장상	175	침해된 CSMS 환경에서 OCPP 2.1 충전 프로파일 보호를 위한 FROST 기반 승인 기법	김태우, Lelisa Adeba Jilcha, 곽진(아주대학교)
8	KISA 원장상	336	이더리움 분산 밸리데이터 QBFT 라운드 타이머의 마감 내 비잔틴 내성 분석	지영빈, 이세영(강원대학교)
9	ETRI 원장상	305	IEEE 802.11 표준 WiFi PQC 마이그레이션을 위한 PQC-PAKE 연구	한윤선, 서석충(국민대학교)
10	ETRI 원장상	8	SeqSQLi: Sequential SQL Injection WAF Bypass via Deep Reinforcement Learning	Roby Firnando Yusuf, Abhishek Chaudhary, 최선오(전북대학교)
11	ETRI 원장상	93	재전송 공격 방지 가능한 블록체인 기반 익명 자격 증명 시스템 설계	탁지원, 임준호, 정익래(고려대학교)
12	NSR 소장상	115	ATLAS 기반 에이전틱 AI 맞춤형 공격 시나리오 자동 생성 프레임워크	정연수, 이주영, 이태진(가천대학교)
13	NSR 소장상	178	비디오 인식 모델에 대한 적대적 공격 벤치마킹	김지윤, 노다영, 서영재, 이상현, 우다현, 주경호(숭실대학교)
14	NSR 소장상	406	역방향 추적 기반 Android intent 취약점 분석 기법	안효빈, 신정헌, 방예현, 배준영, 김민석, 권민준, 배진석, 나웅재, 김주원, 장정안(KISA 화이트햇 스쿨)
15	KISTI 원장상	210	반사실적 인종 조작으로 본 VLM 공정성 평가에서 이산적 일관성 판단의 한계	신은재, Al-Sharabati Abdulrahman, Abuhmed Tamer, 우사이먼성일(성균관대학교)
16	KISTI 원장상	255	컴파일 시점 계측에서 링크 시점 우선순위 해석을 통한 외부 함수 호출 식별	한규상, 강민주, 박정우, 배연주, 김정수, 전승호(가천대학교)
17	KISTI 원장상	139	Android-CDS: 단일 모바일 단말 내 보안 도메인 간 파일 전송 통제를 위한 설계	이용재, 이여민, 김수빈, 박정수(강남대학교)
18	학회 우수논문상	158	Beyond the Sequence: Evaluating Traffic Features for Encrypted LLM Topic Inference	Alif Wicaksana Ramadhan, Anak Agung Ngurah Dharmawangsa, 신다윗, Thi-Thu-Huong Le, 김호원(부산대학교)
19	학회 우수논문상	155	확률론적 HAETAE 대상 오류 주입 기반 키 복구 공격	최기훈, 한재승, 한동국(국민대학교)
20	학회 우수논문상	356	Ollama GUI의 사용자 행위별 디지털 포렌식 아티팩트 분석	김영진, 최대호, 조민정, 김역, 손기욱, 이창훈(서울과학기술대학교)

(최)우수논문상

번호	상장	논문번호	논문명	저자/소속
21	학회 우수논문상	157	인테그랄 키 복구에서 허용 키 차분의 정확한 특성화: ARKST 반례와 완전성 검증	이명규, 신한범(고려대학교), 권동근(국립군산대학교), 석병진(한성대학교), 이동재(강원대학교), 홍득조(전북대학교), 성재철(서울시립대학교), 홍석희(스마트엠투엠)
22	학회 우수논문상	46	LIFT-Guard: 상용 LLM 서비스를 위한 맥락 특화형 탈옥 공격 및 경량 방어	오주엽, 조항범, 최영락, 오준호, 박찬민, 손현기, 윤명근(국민대학교)
23	학회 우수논문상	173	Android 환경에서 Vault 애플리케이션 Photo Vault Lock – PhotoGuard의 암호화된 파일 복호화 연구	박승현, 조동후, 박세준, 김종성(국민대학교)
24	학회 우수논문상	197	동형암호 기반의 프라이버시 보존 차량 디지털 포렌식 기법	하상우, 김도현, 최현민, 조성제(단국대학교)
25	학회 우수논문상	259	Double Guessing Attack에 안전한 1라운드 saPAKE 프로토콜	황리교, 신채연, 황정연(성신여자대학교)
26	학회 우수논문상	182	국가 망 보안체계 정보서비스 모델 3의 등급 라벨 생애주기 통제 부재와 경계 중심 대응 아키텍처	유광민, 황주하(세종대학교), 이찬형(한국전자통신연구원), 김효빈(성신여자대학교), 박기웅(세종대학교)
27	학회 우수논문상	85	RAG 기반 LLM에서의 Prompt Injection 방어를 위한 Perplexity-Heuristic 결합 다층 탐지 알고리즘	김민준, 김성신(숭실대학교)
28	학회 우수논문상	174	다중 에이전트 LLM 시스템 내 반복 위임에 따른 KpqC 오버헤드 분석	유진, 정인수, 김득훈, 곽진(아주대학교)
29	학회 우수논문상	53	MCP-CAT: MCP 버전 및 전송 방식을 고려한 서버 적합성 테스트 자동화	김아인, 이승수(인천대학교)
30	학회 우수논문상	6	Windows 패치 분석을 위한 바이너리 디핑	이동준, 윤인수(한국과학기술원)
31	학회 우수논문상	244	NoClue 애플리케이션을 통해 은닉된 데이터 추출 방안 연구	박유진, 안현종, 박세준, 김종성(국민대학교)
32	학회 우수논문상	127	얼굴 검출 Source Hijacking과 신원 특징 교란을 결합한 얼굴 교체 선제 방어 기법	김세빈, 김동현, 최대선(숭실대학교)
33	학회 우수논문상	177	학습 데이터 추출 공격 완화를 위한 술어 유형 기반 SIEM 로그 비식별 기법 분석	남장우, 레리사 아데바 질차, 김득훈, 곽진(아주대학교)
34	학회 우수논문상	325	RFC 9124 보안 요구사항 기반 SUIT 구현체의 보안 동작 자동 평가 방안 제안	가진섭, 박미리, 서정택(가천대학교)
35	학회 우수논문상	334	TPM 원격 증명을 위한 기준 상태 전이 승인 검증 기법 제안	이성은, 박미리(가천대학교), 박춘서(한국전자통신연구원), 서정택(가천대학교)
36	학회 우수논문상	225	마스크 후보 확률을 이용한 코드워드 마스킹 HQC의 재실행 부채널 분석	이주원, 정상윤, 김희석(고려대학교)
37	학회 우수논문상	313	비지도 클러스터링을 활용한 FTL 상태 피드백 기반 SSD 펌웨어 퍼징 기법	김진세, 전희도, 최원석(고려대학교)
38	학회 우수논문상	152	단일 오류 주입을 이용한 무인비행체 MAVLink 인증 처리 경로 취약성 분석 및 대응 기법	박수진, 신원근, 배대현, 신한범(고려대학교), 이인섭(한국과학기술원), 홍석희(스마트엠투엠), 김희석(고려대학교)
39	학회 우수논문상	140	국방 전술 통신을 위한 O-RAN Near-RT RIC 내 DoS 공격의 PPS 및 연결 상태 분석	이현지, 유현수, 김환국(국민대학교)
40	학회 우수논문상	350	K-RMF 적용 무기체계 연구개발사업을 위한 리눅스 서버 자동화 점검도구 구현	노승일, 조한별(국방기술품질원)
41	학회 우수논문상	340	2라운드 PQC aPAKE 프로토콜의 설계 및 성능 분석	황리교, 백채원, 김민지(성신여자대학교), 신지선(세종대학교), 황정연(성신여자대학교)

번호	상장	논문번호	논문명	저자/소속
42	학회 우수논문상	267	OCPP JSON Schema 기반 세분화 변이 메시지 생성 및 퍼징 분석	최민식(아우토크립트)
43	학회 우수논문상	204	대규모 언어모델에서 안전 지시 유도 거절과 기준선 거절의 은닉 표현 비교 연구	정준, 선민준, 권태경(연세대학교)
44	학회 우수논문상	91	차량 네트워크에서 메시지 크기와 세그먼트 수에 따른 Cumulative MAC과 Compound MAC의 성능 비교	이동구, 김정훈, 변진욱(평택대학교)
45	학회 우수논문상	318	정상 근거 중복이 유사도 기반 RAG 오염 방어에 미치는 영향	김성엽, 유진호(상명대학교)
46	학회 우수논문상	379	컴패니언 보드 주도 vtable 기반 임베디드 펌웨어 핫패칭	하태욱, 장진수(충남대학교)
47	학회 우수논문상	61	AI 에이전트의 오픈소스 패키지 설치 행위 분석 연구	김송혜, 유지현(광운대학교)
48	학회 우수논문상	56	머신 언러닝 모델의 탐지 가능성 완화를 위한 내부 표현 정렬 프레임워크	김현옥, 김상민, 이병천, 박형준(중앙대학교), 박성우(덕성여자대학교), 이미영, 노승민(중앙대학교)
49	학회 우수논문상	250	정말 Apple 일까?: 숨겨진 자격증명 필드와 대규모 무료 호스팅 피싱의 탐지 사각지대	김도연, 박제만(경희대학교)
50	학회 우수논문상	219	t-SNI를 만족하는 효율적인 고차 Keccak 마스킹 구조의 설계와 안전성 증명	안현준, 한재승, 한동국(국민대학교)
51	학회 우수논문상	191	마이크로컨트롤러에서의 Falcon 서명을 위한 96비트 고정소수점 연산 설계	김영범(국민대학교), 신원근, 박태윤(고려대학교), 신동현, 이재석(국민대학교), 김희석(고려대학교), 서석충(국민대학교)
52	학회 우수논문상	332	비인가 도구 호출을 동반하지 않는 LLM 에이전트 공격의 다중 모델 분석	김유민, 박지민, 목정현, 이석준(가천대학교)
53	학회 우수논문상	52	FoundDef: Frozen Pre-trained Encoder 기반 얼굴 교체 딥페이크 능동 방어 기법	유하늘, 류권상(국립공주대학교)
54	학회 우수논문상	362	양자내성암호 전환을 위한 암호 자산 식별 도구 cdxgen의 한계 분석	김예찬, 최아영, 김예진, 김동현, 김동찬(국민대학교)
55	학회 우수논문상	213	금융권 SaaS 망분리 완화에 따른 생성형 AI 내장 SaaS의 보안규율 적용에 관한 연구 – 내부업무망 SaaS 망분리 예외와 생성형 AI 보안규율의 연계 및 재평가를 중심으로 –	김은서, 안시은, 홍준호(성신여자대학교)
56	학회 우수논문상	217	CVE-ATM 증거 그래프를 활용한 TARA 공격경로 생성 및 분석 방안	박준호, 김찬민, 이상욱(한국자동차연구원)
57	학회 우수논문상	88	TLS 1.3 이종 PQC 인증서 체인의 역할별 서명 배치 비용 분석	허문선, 조수빈, 안종범, 김민서, 서화정(한성대학교)

프로그램 일정표

2026년 10월 28일(수)

	구두트랙1	구두트랙2	구두트랙3	구두트랙4	구두트랙5	구두트랙6	포스터세션	부대행사
시간/장소	부라노 I (3F)	부라노 II (3F)	부라노 III (3F)	카프리 I (2F)	카프리 II (2F)	카프리 III (2F)	컨벤션센터 (3F)	페스타 (3F)
10:00~	참가자등록 (컨벤션센터 앞(3F))							
11:00~12:00	좌장: 권태경 (연세대)	좌장: 구자훈 (고려대)	좌장: 서승현 (한양대)	좌장: 한재승 (국민대)	좌장: 서화정 (한성대)	좌장: 김득훈 (아주대)		
	(1-A) [AI보안] AI에이전트 보안 I	(1-B) 소프트웨어보안 I	(1-C) 로봇/ 자율이동체 보안 I	(1-D) 부채널분석/ 대응 I	(1-E) PQC 및 PQC전환 I	(1-F) 네트워크/ 클라우드 보안 I		
12:00~13:00	중식							
13:00~14:00	좌장: 임정환 (쿤텍)	좌장: 황병희 (KTC)	좌장: 이규호 (LIG D&A)	좌장: 김한빛 (국가보안기술연구소)	좌장: 김병구 (한국전자통신연구원)	좌장: 권태웅 (한국과학기술정보연구원)	좌장: 곽병일 (고려대)	
	(2-A) [AI보안] AI에이전트 보안 II	(2-B) 소프트웨어보안 II	(2-C) 산업/우주/국방보안 I	(2-D) 부채널분석/ 대응 II	(2-E) PQC 및 PQC전환 II	(2-F) 네트워크/ 클라우드 보안 II	Poster Session I [AI보안]	
14:00~14:10	휴식							ETRI 양자워크숍 (Open Session)
14:10~15:10	좌장: 성하영 (한국과학기술정보연구원)	좌장: 윤영태 (국가보안기술연구소)	좌장: 강준기 (국가보안기술연구소)	좌장: 이봉수 (국가보안기술연구소)	좌장: 이동훈 (국가보안기술연구소)	좌장: 유지현 (광운대)	좌장: 이재승 (국가보안기술연구소)	
	(3-A) [AI보안] AI에이전트 검증 및 평가 I	(3-B) 취약점분석 I	(3-C) 산업/우주/국방보안 II	(3-D) HW가속 보안	(3-E) 암호이론 및 구현 I	(3-F) 블록체인/암호화폐 I	Poster Session II [시스템보안]	
15:10~15:20	휴식							
15:20~16:20	좌장: 문종철 (씨크랩)	좌장: 신영찬 (국가보안기술연구소)	좌장: 강봉호 (ICTK)	좌장: 배선하 (국가보안기술연구소)	좌장: 박명서 (한성대)	좌장: 배병철 (국가보안기술연구소)	좌장: 석우진 (한국과학기술정보연구원)	
	(4-A) [AI보안] AI에이전트 취약점 분석 I	(4-B) 취약점분석 II	(4-C) 자동차보안 I	(4-D) 정보보호 표준/정책/ 평가 I	(4-E) 개인정보보호/ 데이터보안 I	(4-F) 사이버위협 인텔리전스 I	Poster Session III [암호/융합보안]	
16:20~16:30	휴식							
16:30~17:30	좌장: 노희준 (인하대)	좌장: 김준섭 (쿤텍)	좌장: 김정태 (한국전자통신연구원)	좌장: 방지호 (KTC)	좌장: 김영수 (고려대)	좌장: 이진용 (한국전자통신연구원)		
	(5-A) [AI보안] LLM탈옥/ 프롬프트 인젝션 방어 I	(5-B) 시스템보안 I	(5-C) [AI보안] 딥페이크 탐지/방어 I	(5-D) 공급망 보안	(5-E) 개인정보보호/ 데이터보안 II	(5-F) 오류주입분석		
17:30~	석식							

프로그램 일정표

2026년 10월 29일(목)

	구두트랙1	구두트랙2	구두트랙3	구두트랙4	구두트랙5	구두트랙6	신진연구자 소개, 키노트, 개회식, 초청 및 특별강연	부대행사
시간/장소	부라노 I (3F)	부라노 II (3F)	부라노 III (3F)	카프리 I (2F)	카프리 II (2F)	카프리 III (2F)	컨벤션센터 (3F)	페스타 (3F)
09:00~	참가자등록 (컨벤션센터 앞(3F))							ETRI 양자워크숍 (Closed Session)
09:20~10:20	좌장: 진승헌 (한국전자통신연구원)	좌장: 이상만 (고려대)	좌장: 박승환 (국방방첩본부)	좌장: 이주현 (777 사령부)	좌장: 이현정 (한국시스템보증)	좌장: 박애선 (국방보안지원단)		
	(6-A) [AI보안] AI에이전트 보안 III	(6-B) [AI보안] AI에이전트 취약점 분석 II	(6-C) 로봇/ 자율이동체 보안 II	(6-D) 부채널분석/ 대응 III	(6-E) PQC 및 PQC전환 III	(6-F) 네트워크/ 클라우드 보안 III		
10:20~10:30	휴식							
10:30~11:30	좌장: 주범수 (프라이빗에이아이)	좌장: 강동호 (한국전자통신연구원)	좌장: 이윤경 (한국전자통신연구원)	좌장: 장상운 (국가보안기술연구소)	좌장: 구본욱 (국가보안기술연구소)	좌장: 이석준 (가천대)		가천대학교 AI융합보안대학원 워크숍
	(7-A) [AI보안] AI에이전트 검증 및 평가 II	(7-B) 소프트웨어보안 III	(7-C) 산업/우주/국방보안 III	(7-D) 정보보호 표준/정책/ 평가 II	(7-E) 암호이론 및 구현 II	(7-F) 블록체인/암호화폐 II		
11:30~11:40	휴식							
11:40~12:40	좌장: 박해룡 (한국인터넷진흥원)	좌장: 한인성 (국방과학연구소)	좌장: 한상윤 (국가보안기술연구소)	좌장: 김익균 (한국전자통신연구원)	좌장: 김희석 (고려대)	좌장: 문대성 (한국전자통신연구원)	신진연구자 소개 세션 좌장: 이윤경 (한국전자통신연구원)	
	(8-A) [AI보안] LLM탈옥/ 프롬프트 인젝션 방어 II	(8-B) 취약점분석 III	(8-C) 자동차보안 II	(8-D) 시스템보안 II	(8-E) [AI보안] 딥페이크 탐지/방어 II	(8-F) 사이버위협 인텔리전스 II	박소현 교수(성신여대), 전소은 교수(성신여대) 유지현 교수(광운대), 양훈민 교수(고려대), 최현민 교수(단국대), 진범진 교수(아주대)	
12:40~13:40	중식							
13:40~14:10	키노트 / 장소 : 컨벤션센터(3F) 주제 : 방산보안의 미래 / 연사 : 이승영 본부장(LIG D&A) / 좌장 : 하재철 교수(호서대)							
14:10~14:20	휴식							IITP 기술성과교류회
14:20~15:40	개회식 컨벤션센터(3F)							
	사회: 운영위원장 한동국(국민대), 김환국(국민대) 국민의례 내빈소개 개회사 : 한국정보보호학회 회장 김호원 행사보고(프로그램위원장 최두호(고려대), 한미란(고려대), 김형식(성균관대)) (최)우수논문 및 우수심사위원 시상 경품추첨							
15:40~16:00	휴식							
16:00~16:30	초청강연 I / 장소 : 컨벤션센터(3F) 주제 : 보안특화 AI 모델 개발 전략 / 연사 : 김진휘 전무(네이버 보안특화AI PI) / 좌장 : 서정택 교수(가천대)							
16:30~16:40	휴식							
16:40~17:10	특별강연 / 장소 : 컨벤션센터(3F) 연사 : 위성일 교수(울산과학기술원) – USENIX Security 2026, Internet Defence Prize / 좌장 : 최두호 교수(고려대)							
17:10~17:20	휴식							
17:20~17:50	초청강연 II / 장소 : 컨벤션센터(3F) 주제 : 2027년 사이버보안 R&D 기획방향 / 연사 : 조학수 PM(정보통신기획평가원) / 좌장 : 이임영 교수(순천향대)							
17:50~18:10	글로벌 탑티어 대학 파견 프로그램 소개(IITP)							
18:10~	만찬							

2026년 10월 30일(금)

	구두트랙1	구두트랙2	구두트랙3	구두트랙4	구두트랙5	구두트랙6	부대행사
시간/장소	부라노 I (3F)	부라노 II (3F)	부라노 III (3F)	카프리 I (2F)	카프리 II (2F)	카프리 III (2F)	페스타 (3F)
09:00~	참가자 등록 (부라노 I, II, III 앞(3F))						자동차 및 무인이동체연구회 세미나
09:20~10:20	좌장: 권혁찬 (한국전자통신연구원)	좌장: 김수현 (순천향대)	좌장: 공준진 (웨이브피아)	좌장: 강유성 (한국전자통신연구원)	좌장: 김준섭 (한국인터넷진흥원)	좌장: 이원혁 (한국과학기술정보연구원)	
	(9-A) [AI보안] AI에이전트 보안 IV	(9-B) [AI보안] AI에이전트 취약점 분석 III	(9-C) 산업/우주/국방보안 IV	(9-D) 부채널분석/대응 IV	(9-E) PQC 및 PQC전환 IV	(9-F) 네트워크/ 클라우드 보안 IV	
10:20~10:30	휴식						
10:30~11:30	좌장: 김수형 (한국전자통신연구원)	좌장: 이은경 (국가보안기술연구소)	좌장: 김종성 (국민대)	좌장: 박상욱 (한국전자통신연구원)	좌장: 전승호 (가천대)	좌장: 이수미 (금융보안원)	
	(10-A) [AI보안] AI에이전트 검증 및 평가 III	(10-B) 소프트웨어보안 IV	(10-C) [AI보안] 딥페이크 탐지/방어 III	(10-D) 콘텐츠/저작권 보안	(10-E) 취약점분석 IV	(10-F) 인증 및 ID관리	
11:30~	중식						
12:00~18:00	글로컬랩 방산기술보호연구소 워크숍 (14:00~16:00)						

구두발표 세션

2026년 10월 28일(수)

세션	논문번호	논문제목(저자/소속)
11:00~12:00 (1-A) [AI보안] AI에이전트 보안 I 좌장: 권태경 (연세대)	131	DRSS: 초장기 실행 보안 에이전트를 위한 이중 레일 컨텍스트 가상화 아낙 아궁 느구라 다마왕사, 신다윗, 조재한, 장현진, 레티투흐엉, 김호원(부산대학교)
	176	LLM 에이전트의 암호화 문맥 주입 공격에 대한 복호화 경계 가드 배치 연구 구진서, 송현민(단국대학교)
	286	간접 프롬프트 인젝션 환경에서 AI 에이전트의 위험도 기반 도구 실행 통제 정책 설계 및 평가 방안 연구 장은정, 홍준호(성신여자대학교)
	282	AI 에이전트의 최소 권한 정책 생성 및 적용 연구 동향 양수민, 전유석(고려대학교)
11:00~12:00 (1-B) 소프트웨어보안 I 좌장: 구자훈 (고려대)	6	Windows 패치 분석을 위한 바이너리 디핑 이동준, 윤인수(한국과학기술원)
	53	MCP-CAT: MCP 버전 및 전송 방식을 고려한 서버 적합성 테스트 자동화 김아인, 이승수(인천대학교)
	255	컴파일 시점 계측에서 링크 시점 우선순위 해석을 통한 외부 함수 호출 식별 한규상, 강민주, 박정우, 배연주, 김정수, 전승호(가천대학교)
	20	TensorShield 오픈소스 구현체의 비대칭 컴파일 옵션 분석 및 성능 영향 평가 박정현, 이승광(단국대학교)
11:00~12:00 (1-C) 로봇/자율이동체 보안 I 좌장: 서승현 (한양대)	252	ROS 2 콜백 시간 특성 기반 실시간 이상탐지 기법 이예진, 유준수(전북대학교)
	321	MMS-UWB 거리 단축 공격에 대한 하드웨어 클럭 오차 기반 탐지 기법 김지민, 김주언, 최원석(고려대학교)
	24	CAMEO: ROS 2 Callback 단위 보안을 위한 중재 및 집행 오버레이 최윤서, 이승수(인천대학교)
	202	ROS 2에서 세밀한 데이터 의존성 추적을 위한 프로세스 간 태그 연계 기법 김서준, 오현영(가천대학교)
11:00~12:00 (1-D) 부채널분석/대응 I 좌장: 한재승 (국민대)	135	HAETAE 서명 구현에서 NTT 영역 계수별 곱셈에 대한 상관 전력 분석 공격 이광용, 안경덕, 하재철(호서대학교)
	253	라즈베리파이 2B 대상 상관 전자파 분석을 위한 전처리 파라미터 선정과 필요 전처리 수준 송윤우, 문채윤, 한동국(국민대학교)
	284	결합확률분포 기반 블라인드 부채널 분석의 중간값 확률 재표현을 통한 라운드 간 확장 오성빈, 김주환, 한동국(국민대학교)
	293	단일 파형 수평 전력 분석을 통한 SLH-DSA-SHA2 키 생성 안전성 분석 민진용, 오성빈, 한동국(국민대학교)

2026년 10월 28일(수)

세션	논문번호	논문제목(저자/소속)
11:00~12:00 (1-E) PQC 및 PQC전환 I 좌장: 서화정 (한성대)	88	TLS 1.3 이종 PQC 인증서 체인에서 역할별 서명 알고리즘 배치가 성능에 미치는 영향 분석 허문선, 조수빈, 안종범, 김민서, 서화정(한성대학교)
	137	K-LMS: 한국 암호 프리미티브를 이용한 Leighton–Micali 서명의 설계·구현·평가 강희주, 형유림, 김하경, 정수민(한성대학교), 조항신(독립 연구자), 서화정(한성대학교)
	149	AIMer v3 서명 기법의 고정 덧셈 체인 기반 유한체 역원 최적화 이승원, 송민호, 엄시우, 조수빈, 김민서, 서화정(한성대학교)
	303	GPU 환경에서 SDitH 병렬 최적화 연구 김동천, 서석충(국민대학교)
11:00~12:00 (1-F) 네트워크/클라우드 보안 I 좌장: 김득훈 (아주대)	25	AURORA: 클라우드 네이티브 환경을 위한 IAM 기반 리소스 접근 제어 자동화 프레임워크 김민경, 이승수(인천대학교)
	96	자격증명 흐름과 자원 접근을 연결하는 CloudTrail 침해 조사 그래프 강인석(창원대학교), 서장훈(홍익대학교), 정준식(연세대학교), 박기웅(세종대학교)
	10	공공기관 IaaS 전환을 위한 N2SF 기반 보안준비도 예비 평가모델 연구: MITRE ATT&CK T1078.004 기반 가상 사례 최지연, 원유재(충남대학교)
	265	CloudTrail 관측 공백 환경에서 AWS 인프라 상태 변화 기반 그래프 추적 모델 강인석(창원대학교), 서장훈(홍익대학교), 정준식(연세대학교), 박기웅(세종대학교)

2026년 10월 28일(수)

세션	논문번호	논문제목(저자/소속)
13:00~14:00 (2-A) [AI보안] AI에이전트 보안 II 좌장: 임정환 (쿤텍)	174	다중 에이전트 LLM 시스템 내 반복 위임에 따른 KpqC 오버헤드 분석 유진, 정인수, 김득훈, 곽진(아주대학교)
	335	원격 MCP 서비스 종료 시 권한 회수의 구조적 한계 및 종료 판정 기준 정립 양승권, 김미소(중부대학교), 정원재(고려대학교), 박소은(숙명여자대학교)
	72	LLM 데이터 에이전트의 DB 연결 신원 소실과 사용자 신원 바인딩 기반 접근제어 김영하, 백남균(덕성여자대학교)
	222	멀티 에이전트 시스템의 보안 위협 확산 방지를 위한 게이트웨이 통신 통제 기법 손재현, 차훈영, 이소이, 권태경(연세대학교)
13:00~14:00 (2-B) 소프트웨어보안 II 좌장: 황병희 (KTC)	313	비지도 클러스터링을 활용한 FTL 상태 피드백 기반 SSD 펌웨어 퍼징 기법 김진세, 전희도, 최원석(고려대학교)
	341	소스 문맥 결합 기반 크래시 중복 제거 기법 제안 김현성, 서정규, 서정택(가천대학교)
	379	컴패니언 보드 주도 vtable 기반 임베디드 펌웨어 핫패칭 하태욱, 장진수(충남대학교)
	145	부분 실행 흔적 기반 미래 행동 예측 정우진, 최원석(고려대학교)
13:00~14:00 (2-C) 산업/우주/국방보안 I 좌장: 이규호 (LIG D&A)	263	제조 이상 탐지의 제품 간 이전에 따른 순위 성능과 판정 오류 분석: MoECLIP과 CNN 비교 김나현, 최대호, 조재익, 이창훈(서울과학기술대학교)
	342	산업제어시스템의 시퀀스 간 시간적 관계를 반영한 IS-GAF 기반 비지도 이상탐지 모델 제안 서정규, 이주현, 서정택(가천대학교)
	172	산업용 압축기 원격 모니터링 및 유지보수 시스템의 공개 취약점 기반 공격표면 분석 주승환(한화파워 주식회사)
	150	S7comm 프로토콜 기반 가상 수처리 공정 설계 및 사이버 공격 탐지 모델 개발을 위한 데이터셋 구축 이혜강, 전원준, 기한결, 하재철(호서대학교)
13:00~14:00 (2-D) 부채널분석/대응 II 좌장: 김한빛 (국가보안기술연구소)	295	SHAKE 기반 SLH-DSA의 비밀키 시드 복구를 위한 상관전력분석 이민정, 오충연, 한동국(국민대학교)
	156	SHA-2 기반 SLH-DSA 대상 상관 전력 분석 장진욱, 김재효, 한동국(국민대학교)
	166	HAETAE 전자 서명에 대한 프로파일링 기반 부채널 분석 한이소, 정상윤, 김희석(고려대학교)
	237	Adaptive Successive Narrowing: 전자파 부채널 평가를 위한 효율적인 프로브 위치 선별 기법 김재효, 김주환, 한동국(국민대학교)

2026년 10월 28일(수)

세션	논문번호	논문제목(저자/소속)
(2-E) PQC 및 PQC전환 II 좌장: 김병구 (한국전자통신연구원)	305	IEEE 802.11 표준 WiFi PQC 마이그레이션을 위한 PQC-PAKE 연구 한윤선, 서석충(국민대학교)
	87	장거리 네트워크 환경에서 양자내성암호 기반 TLS 1.3의 성능 분석 송보연(한국과학기술정보연구원), 김종현(고려대학교), 박종환(상명대학교), 석우진, 이원혁(한국과학기술정보연구원)
	340	2라운드 PQC aPAKE 프로토콜의 설계 및 성능 분석 황리교, 백채원, 김민지(성신여자대학교), 신지선(세종대학교), 황정연(성신여자대학교)
	44	QUIC에서 KpqC 키 캡슐화 메커니즘 검증 및 성능 분석 백동규(과학기술연합대학원대학교), 이종헌, 이유석(한국전자통신연구원), 강유성(과학기술연합대학원대학교/한국전자통신연구원)
13:00~14:00 (2-F) 네트워크/클라우드 보안 II 좌장: 권태웅 (한국과학기술정보연구원)	158	시퀀스를 넘어: 암호화된 LLM 트래픽의 주제 추론을 위한 특징 평가 Alif Wicaksana Ramadhan, Anak Agung Ngurah Dharmawangsa, 신다윗, Thi-Thu-Huong Le, 김호원(부산대학교)
	326	암호화 트래픽 대상 클라이언트 핑거프린트 통제 기반 이상 탐지 성능 편향 분석 방안 제안 지일환, 이주현, 서정택(가천대학교)
	268	KubePhScope: K8s 임시 컨테이너 정책의 API 전이 집행 완전성 검증 프레임워크 김서연, 최민서, 윤지환, 박도현(한국인터넷진흥원 Best of The Best), 이현정(코스콤)
	269	Kubernetes 공격 경로의 ServiceAccount 인증 관계 판정 방식 제안 최민서, 김서연, 박도현, 윤지환(한국인터넷진흥원 Best of The Best), 이현정(코스콤)

2026년 10월 28일(수)

세션	논문번호	논문제목(저자/소속)
14:10~15:10 (3-A) [AI보안] AI에이전트 검증 및 평가 I 좌장: 성하영 (한국과학기술정보연구원)	79	동적 정책 집행 기반 LLM 에이전트의 방어의 보안-유용성 한계 분석: AgentDojo 기반 DRIFT 평가 하유경, 나현식, 최대선(숭실대학교)
	324	사이버보안 에이전트의 반복 샘플링에서 정답 생성과 최빈 답 선택의 간극 신다윗, 아궁, 아마다, 울란, 함단, 정회광, 한승민, 김호원(부산대학교)
	196	8B LLM의 도구 사용 실패 분석: 형식 준수, 행동 선택 및 실행 종료 신다윗, 안드로, 아리프, 조재한, 이창율, 하업준, 흐엉, 김호원(부산대학교)
	228	멀티에이전트 시스템의 재승인 경계 조합에 대한 보안성 평가 결과 비교 연구 차원제(국립창원대학교), 송유래, 레리사 아데바 질차, 곽진(아주대학교)
14:10~15:10 (3-B) 취약점분석 I 좌장: 윤영태 (국가보안기술연구소)	173	Android 환경에서 Vault 애플리케이션 Photo Vault Lock - PhotoGuard의 암호화된 파일 복호화 연구 박승현, 조동후, 박세준, 김종성(국민대학교)
	244	NoClue 애플리케이션을 통해 은닉된 데이터 추출 방안 연구 박유진, 안현종, 박세준, 김종성(국민대학교)
	235	iOS 환경에서의 커넥티드 카 애플리케이션 마이현대 아티팩트 분석 연구 신관용, 박진철, 김현준, 박세준, 김종성(국민대학교)
	248	안드로이드 환경에서 내비게이션 애플리케이션 'Mappy'의 위치정보 데이터 구조 분석 박주연, 이용진, 김현준, 김종성(국민대학교)
14:10~15:10 (3-C) 산업/우주/국방보안 II 좌장: 강준기 (국가보안기술연구소)	330	S-100 ECDIS 수심 산출에서 검증 판정 미집행 탐지를 위한 조항 집행 검사 기법 제안 박미리, 이주현, 서정택(가천대학교)
	134	CCSDS SDLS PICS 기반 NASA CryptoLib 적합성 분석 이시하(과학기술연합대학교대학원), 조성민, 김영호, 이윤경, 김정녀(한국전자통신연구원)
	35	ECDIS 환경에서 PBFT와 Merkle Tree를 활용한 ENC 복구 프레임워크 이수왕, 김지윤(경상국립대학교)
	84	SAR 위성영상 기반 선박 추적 및 해상 경계 침범 조기경보 시스템 박민석, 류이노, 마흐무드 부헤드마, 유준수(전북대학교)
14:10~15:10 (3-D) HW가속 보안 좌장: 이봉수 (국가보안기술연구소)	191	마이크로컨트롤러에서의 Falcon 서명을 위한96비트 고정소수점 연산 설계 김영범(국민대학교), 신원근, 박태윤(고려대학교), 신동현, 이재석(국민대학교), 김희석(고려대학교), 서석충(국민대학교)
	304	Full-Radix MPI 가속을 위한 Ibex RISC-V 명령어 확장 구현 및 비교 김민기, 서석충(국민대학교)
	180	ARM Cortex-M4에서 HQC 다항식 곱셈의 1차 마스킹과 비용 분석 장지훈, 김규상, 김인성, 박수진, 박현주(고려대학교), 김수리(성신여자대학교), 권동근(국립군산대학교), 홍석희(스마트엠투엠)
	247	RISC-V 프로세서 기반 경량 AES 명령어 확장 구조 우상원, 김민재, 화정환, 정영준, 박현, 최필주(국립부경대학교)

2026년 10월 28일(수)

세션	논문번호	논문제목(저자/소속)
14:10~15:10 (3-E) 암호이론 및 구현 I 좌장: 이동훈 (국가보안기술연구소)	157	인테그랄 키 복구에서 허용 키 차분의 정확한 특성화: ARKST 반례와 완전성 검증 이명규, 신한범(고려대학교), 권동근(국립군산대학교), 석병진(한성대학교), 이동재(강원대학교), 홍득조(전북대학교), 성재철(서울시립대학교), 홍석희(스마트엠투엠)
	377	16라운드 블록암호 Marvin에 대한 차분 공격 박건우, 권혁태, 송원우, 김남일, 백승준, 김종성(국민대학교)
	277	LWE 및 MLWE 문제에 대한 하이브리드 양자 알고리즘 연구 동향 분석 안재만, 김영수, 최두호(고려대학교)
	312	심층 신경망에 구현된 국내 블록암호의 실수입력 거동 분석 김의재, 서화정(한성대학교)
14:10~15:10 (3-F) 블록체인/암호화폐 I 좌장: 유지현 (광운대)	93	재전송 공격 방지 가능한 블록체인 기반 익명 자격 증명 시스템 설계 탁지원, 임준호, 정익래(고려대학교)
	130	선택적 누락 공격 탐지를 위한 감사 주기 적응형 앵커 배치 기법 유현지, 유승우, 김수현(순천향대학교)
	336	이더리움 분산 밸리데이터 QBFT 라운드 타이머의 마감 내 비잔틴 내성 분석 지영빈, 이세영(강원대학교)
	29	이더리움 실행 클라이언트 간 실행 불일치 탐지 안건희, 윤인수(한국과학기술원)

2026년 10월 28일(수)

세션	논문번호	논문제목(저자/소속)
15:20~16:20 (4-A) [AI보안] AI에이전트 취약점 분석 I 좌장: 문종철 (씨크랩)	212	코딩 에이전트의 권한 및 제어 설정 취약점 사례 분석 김경민(서울여자대학교), 우용운(아주대학교), 이재균(성균관대학교), 안종범(한성대학교), 손서영(충남대학교), 신제원, 허준하(명지대학교), 이소영(광운대학교)
	61	AI 에이전트의 오픈소스 패키지 설치 행위 분석 연구 김송혜, 유지현(광운대학교)
	243	MCP 도구 설명 오염의 에이전트 간 전파와 세션 간 잔존 분석 김서이, 이일구(성신여자대학교)
	315	MCP 관리 API의 접근통제 취약점 분석 및 검증연구: Dify MCP 사례 이준용, 이현규, 김누리한, 강정민(고려대학교)
15:20~16:20 (4-B) 취약점분석 II 좌장: 신영찬 (국가보안기술연구소)	356	Ollama GUI의 사용자 행위별 디지털 포렌식 아티팩트 분석 김영진, 최대호, 조민정, 김역, 손기욱, 이창훈(서울과학기술대학교)
	359	갤럭시 AI 전사 아티팩트 포렌식 분석 연구 김성우, 최대호, 조민정, 김역, 손기욱, 이창훈(서울과학기술대학교)
	133	LLM 기반 PowerShell 포렌식 분석의 구조화 근거 보고 평가: RAG 및 RAFT 조건 비교 최성지, 신상욱(국립부경대학교)
	283	국가안보 관점에서 바라본 디지털 포렌식 기술 연구 최종윤, 김대환, 신민석, 김한결, 박명서(한성대학교)
15:20~16:20 (4-C) 자동차보안 I 좌장: 강봉호 (ICTK)	175	침해된 CSMS 환경에서 OCPP 2.1 충전 프로파일 보호를 위한 FROST 기반 승인 기법 김태우, 레리사 아데바 질차, 곽진(아주대학교)
	91	차량 네트워크에서 메시지 크기와 세그먼트 수에 따른 Cumulative MAC과 Compound MAC의 성능 비교 이동구, 김정훈, 변진욱(평택대학교)
	141	LinkPrinT: CCS 충전 통신의 SLAC 감쇠 프로파일을 이용한 물리계층 신호 주입 탐지 기법 박유희, 최원석(고려대학교)
	267	OCPP JSON Schema 기반 세분화 변이 메시지 생성 및 퍼징 분석 최민식(아우토크립트)
15:20~16:20 (4-D) 정보보호 표준/정책/평가 I 좌장: 배선하 (국가보안기술연구소)	190	공공기관의 효율적인 국가망보안체계(N²SF) 도입을 위한 의사결정 프레임워크 이찬형(한국전자통신연구원), 김효빈(성신여자대학교), 유광민, 황주하, 박기웅(세종대학교)
	182	국가 망 보안체계 정보서비스 모델3의 등급 라벨 생애주기 통제 부재와 경계 중심 대응 아키텍처 유광민, 황주하(세종대학교), 이찬형(한국전자통신연구원), 김효빈(성신여자대학교), 박기웅(세종대학교)
	294	N2SF 기반 국가 · 공공기관 데이터의 양자내성암호 전환 프레임워크 박도윤, 형유림, 서화정(한성대학교)
	129	N2SF 위협모델링 방법에 관한 연구 이승창, 박민재(한전KDN), 이동연, 김경훈, 이철호(엔플러스랩)

2026년 10월 28일(수)

세션	논문번호	논문제목(저자/소속)
15:20~16:20 (4-E) 개인정보보호/ 데이터보안 I 좌장: 박명서 (한성대)	73	연합학습에서 글로벌 모델 업데이트 보호를 위한 분산형 AGKA에 관한 연구 김기환, 김수현, 이임영(순천향대학교)
	98	스마트 팩토리 연합학습을 위한 Non-IID 데이터 처리 및 성능 분석 어윤규, 고성노, 이재원, 정은수(청주대학교)
	373	Non-IID 연합학습에서 오탐 고착 완화를 위한 양방향 이력 가중 집계 김주빈, 진규정, 임호현, 이세영(강원대학교)
	320	연합학습 환경에서 CNN 모델 배포 시 무결성 평가 방안 연구 오성택, 백남균(덕성여자대학교)
15:20~16:20 (4-F) 사이버위협 인텔리전스 I 좌장: 배병철 (국가보안기술연구소)	8	SeqSQLi: Sequential SQL Injection WAF Bypass via Deep Reinforcement Learning Roby Firnando Yusuf, Abhishek Chaudhary, 최선오(전북대학교)
	57	내부자 위협 탐지를 위한 개인별 시계열 표현의 다중 활용과 편차 기반 선별 최영아, 이수빈, 김진(시큐레이어 R&D 센터)
	70	클래스 불균형 환경에서의 성능 향상을 위한 그래프 생성 증강 모델 오영재, 서창호(국립공주대학교), 정수용(한국과학기술정보연구원)
	203	CCTV 기반 물리보안을 위한 이상행동 벤치마크 제안 송다은, 김형식(성균관대학교)

구두발표 세션

2026년 10월 28일(수)

세션	논문번호	논문제목(저자/소속)
16:30~17:30 (5-A) [AI보안] LLM탈옥/프롬프트 인젝션 방어 I 좌장: 노희준 (인하대)	46	LIFT-Guard: 상용 LLM 서비스를 위한 맥락 특화형 탈옥 공격 및 방어 오주엽, 조항범, 최영락, 오준호, 박찬민, 손현기, 윤명근(국민대학교)
	85	RAG 기반 LLM에서의 Prompt Injection 방어를 위한 Perplexity-Heuristic 결합 다층 탐지 알고리즘 김민준, 김성신(숭실대학교)
	55	한글 표기 변형을 이용한 대규모 언어모델 안전정렬 우회 가능성 분석: 이해도·순응도 분리 측정과 유효 우회율 강창협, 조용엽, 전규현, 김현우, 손주환(스틸리언)
	204	대규모 언어모델에서 안전 지시 유도 거절과 기준선 거절의 은닉 표현 비교 연구 정준, 선민준, 권태경(연세대학교)
16:30~17:30 (5-B) 시스템보안 I 좌장: 김준섭 (쿤텍)	58	커널 BPF struct_ops 확장의 위임 경계: 검증 책임 분산에 대한 위협 모델 김현우, 강창협, 조용엽, 전규현, 손주환(스틸리언)
	136	eBPF를 이용한 리눅스 상 난수 앵커 기반 암호 연산 실시간 탐지 정수민, 형유림, 김하경, 강희주, 서화정(한성대학교)
	240	독립 하드웨어를 이용한 Linux 커널 Credential 무결성 감시 기법 천현우, 김재현, 한승훈(숭실대학교)
	32	시스템 프로비넌스 기반 이상 탐지 기술의 동향 및 분석 김건호, 유동운, 정재영, 최윤호(부산대학교)
16:30~17:30 (5-C) [AI보안] 딥페이크 탐지/방어 I 좌장: 김정태 (한국전자통신연구원)	142	Talking-Head 생성 악용 방지를 위한 음성-이미지 정렬 교란 기반 음성 보호 기법 김다인, 김동현, 김승민, 최대선(숭실대학교)
	127	얼굴 검출 Source Hijacking과 신원 특징 교란을 결합한 얼굴 교체 선제 방어 기법 김세빈, 김동현, 최대선(숭실대학교)
	178	비디오 인식 모델에 대한 적대적 공격 벤치마킹 김지윤, 노다영, 서영재, 이상현, 우다현, 주경호(숭실대학교)
	210	반사실적 인종 조작으로 본 VLM 공정성 평가에서 이산적 일관성 판단의 한계 신은재, Abdulrahman Al-Sharabati, Tamer Abuhmed, 우사이먼성일(성균관대학교)
16:30~17:30 (5-D) 공급망 보안 좌장: 방지호 (KTC)	223	금융권 클라우드서비스 제공자 안전성 평가와 보안보증 제도의 요구사항 매핑 분석 최주섭, 안성현, 장지현(금융보안원)
	213	금융권 SaaS 망분리 완화에 따른 생성형 AI 내장 SaaS의 보안규율 적용에 관한 연구 – 내부업무망 SaaS 망분리 예외와 생성형 AI 보안규율의 연계 및 재평가를 중심으로 – 김은서, 안시은, 홍준호(성신여자대학교)
	272	반복적인 차량 엣지 AI 통신을 위한 컨텍스트 결합 인증 모델의 보안 요구사항 및 검증 김관우, 이학준(국립금오공과대학교)

2026년 10월 28일(수)

세션	논문번호	논문제목(저자/소속)
16:30~17:30 (5-E) 개인정보보호/ 데이터보안 II 좌장: 김영수 (고려대)	177	학습 데이터 추출 공격 완화를 위한 술어 유형 기반 SIEM 로그 비식별 기법 분석 남장우, 레리사 아데바 질차, 김득훈, 곽진(아주대학교)
	215	LLM 개인정보 마스킹의 프롬프트 민감 출처 근거화 함단 아자니, 신다윗, 레티투흐엉 , 물야사리 울란 실바니, 김호원(부산대학교)
	12	Aging Noise Schedule의 프라이버시-유틸리티 트레이드오프 검증 김민관, 홍성제, 최현민(단국대학교)
	18	전자정부프레임워크 환경에서 JDBC 프록시와 결정론적 추적 식별자(Trace ID)를 활용한 개인정보 접속기록 감사 및 이상탐지 시스템 최재봉, 류재철(충남대학교)
16:30~17:30 (5-F) 오류주입분석 좌장: 이진용 (한국전자통신연구원)	155	확률론적 HAETAE 대상 오류 주입 기반 키 복구 공격 최기훈, 한재승, 한동국(국민대학교)
	152	단일 오류 주입을 이용한 무인비행체 MAVLink 인증 처리 경로 취약성 분석 및 대응 기법 박수진, 신원근, 배대현, 신한범(고려대학교), 이인섭(한국과학기술원), 홍석희(스마트엠투엠), 김희석(고려대학교)
	236	SMAUG-T HWT 오류 주입을 통한 공유키 복구 김정현, 최기훈, 한동국(국민대학교)
	106	탐색 모델과 활용 모델을 이용한 딥러닝 기반 오류 파라미터 조사 방안 김주환, 한동국(국민대학교)

구두발표 세션

2026년 10월 29일(목)

세션	논문번호	논문제목(저자/소속)
09:20~10:20 (6-A) [AI보안] AI에이전트 보안 III 좌장: 진승헌 (한국전자통신연구원)	86	LLM 멀티 에이전트 시스템의 전염형 공격 방어를 위한 매개 중심성 기반 검증기 배치 분석 서영민, 유지현(광운대학교)
	138	LLM 에이전트 환경에서 분해 공격 탐지를 위한 실행 능력 감시 기법의 제안 최동환, 김윤성, 하재철(호서대학교)
	254	멀티모달 대형 언어 모델 탈옥 공격과 에이전트 기반 방어 기술 동향 분석 연구 추송현, 권태경(연세대학교)
	337	추론형 LLM 및 에이전트 환경에서의 서비스 거부 공격과 방어 기술 동향 분석 황서영, 서정규, 서정택(가천대학교)
09:20~10:20 (6-B) [AI보안] AI에이전트 취약점 분석 II 좌장: 이상만 (고려대)	371	Computer-Use Agent의 공격 표면과 메모리를 통한 공격 지속성 분석 이희수(고려대학교), 박규남(아주대학교), 김미소(전북대학교), 백지훈(아주대학교), 전민규(명지대학교), 정유진(덕성여자대학교)
	110	다단계 추론 에이전트에서 간접 프롬프트 주입 포맷 변화가 은닉 상태 궤적에 미치는 영향 조원빈, 송현민(단국대학교)
	332	비인가 도구 호출을 동반하지 않는 LLM 에이전트 공격의 다중 모델 분석 김유민, 박지민, 목정현, 이석준(가천대학교)
	347	EchoLeak 유출 경로 재구성을 통한 LLM Agent 데이터 유출의 단계별 분석 오정민, 김준현, 한태현, 이태진(가천대학교)
09:20~10:20 (6-C) 로봇/자율이동체 보안 II 좌장: 박승환 (국방방첩본부)	21	대규모 언어 모델 생성 텍스트 워터마킹 기법 비교 분석 백가현, 구형준(성균관대학교)
	179	PUF를 활용한 전방향 안전성 제공 MAVLink2 인증 키 교환 기법 박병하, 정인수, 김득훈, 곽진(아주대학교)
	60	제한형 공격그래프 기반 무인기 항법 페일세이프 시험 생성 및 SITL 검증 김수민, 김태규(가천대학교)
	107	피지컬 AI 기기의 취약점 동향 분석 이인강, 이예준, 조효진(연세대학교)
09:20~10:20 (6-D) 부채널분석/대응 III 좌장: 이주현 (777 사령부)	233	On-device LLM의 전자기파 부채널 분석을 이용한 입력 구분 연구 하세영, 박수진, 백지우, 이규원, 김희석(고려대학교)
	273	라즈베리파이 2B에 대한 딥러닝 기반 비프로파일링 부채널 공격 김용재, 김주환, 한동국(국민대학교)
	301	XMEGA 기반 RSA Square-and-Multiply-Always의 타이밍 누설 분석 및 대응 윤이한, 김용재, 한동국(국민대학교)
	353	I^2C 회로 전자기파 누설 탐지를 위한 SCL 동기시간게이팅증폭(STGA) 기법 심정하, 전희도, 최원석(고려대학교)

2026년 10월 29일(목)

세션	논문번호	논문제목(저자/소속)
09:20~10:20 (6-E) PQC 및 PQC전환 III 좌장: 이현정 (한국시스템보증)	378	Implementation of Post-Quantum Cryptography on a DID/VC Platform: Considerations and Measurements Abdillah Ahmad, 최종욱(마크애니)
	90	PQC 전환을 고려한 V2X 인증서 및 키 관리의 표준화 현황과 발전 방향 장재영(국립공주대학교), 강찬구(라온컨버전스), 홍도원, 서창호(국립공주대학교)
	159	5G Core SBI 환경에서 Hybrid PQC 적용에 따른 TLS 핸드셰이크 처리량 분석 강지현, 오지언, 원태호, 김보남, 유일선(국민대학교)
	362	양자내성암호 전환을 위한 암호 자산 식별 도구 cdxgen의 한계 분석 김예찬, 최아영, 김예진, 김동현, 김동찬(국민대학교)
09:20~10:20 (6-F) 네트워크/클라우드 보안 III 좌장: 박애선 (국방보안지원단)	207	Hiworks Messenger의 Socket.IO 기반 통신 프로토콜 역공학을 통한 메신저 데이터 획득 신민석, 김한결, 최종윤, 박명서(한성대학교)
	125	LLM 기반 네트워크 프로토콜 명세서의 보안 요구사항 추출: 동향 조사 Hassan Asghar, 이현우(한국에너지대학교)
	374	국내 다층 접속차단 체계 우회 기술의 계층별 분류 프레임워크 이준우(시큐어머신스랩), 홍승후, 우사이먼성일(성균관대학교)
	239	국내 AS 토폴로지에서의 ASPA 부분 도입 효과 시뮬레이션 및 발행 현황 분석 오태호(광운대학교)

2026년 10월 29일(목)

세션	논문번호	논문제목(저자/소속)
10:30~11:30 (7-A) [AI보안] AI에이전트 검증 및 평가 II 좌장: 주범수 (프라이빗에이아이)	357	AI Agent 영속 메모리 기반 Tool 실행 이력 복원과 오류 요인 분석 송민경, 진규정, 이세영(강원대학교)
	114	에이전트 시스템 적합성 평가: 국내외 AI 모델 안전성 수준 평가 연구 김원재, 전인선, 이선우, 이태진(가천대학교)
	287	공세적 사이버보안 분야의국내외 오픈소스 LLM 성능평가 및 한계점 분석 허신욱, 넨 비엣 환, 박지성(스마트엠투엠), 김호원(스마트엠투엠/부산대학교)
	258	인공지능 모델 및 시스템 보안성 검증 프레임워크 설계 한정훈(한국정보통신기술협회)
10:30~11:30 (7-B) 소프트웨어보안 III 좌장: 강동호 (한국전자통신연구원)	71	차량 소프트웨어 취약점 분석을 위한 LLM Agent Skill 김호연, 송도경(연세대학교)
	42	Juliet 기반 LLM 취약점 경고 판정 평가에서 표면 단서의 영향 분석 조용엽, 강창협, 김현우, 전규현, 손주환(스틸리언)
	124	난독화 수준에 따른 코드 LLM의 행동 추론과 은닉 상태 분석 박민재, 박화비, 신민석, 박명서(한성대학교)
	69	보안성과 기능성 균형을 위한 Repair Experience Memory 기반 안전한 코드 생성 오정호, 김형식(성균관대학교)
10:30~11:30 (7-C) 산업/우주/국방보안 III 좌장: 이윤경 (한국전자통신연구원)	143	분산전원(DER) 대상 IT-OT 융합 공격 시나리오와 MITRE ATT&CK 매핑 최진춘(한국전자통신연구원)
	63	해양 CPS 복합 킬체인 대응을 위한 동적 피드백 기반 사이버보안 프레임워크 상세 설계 김남정, 김정호(가천대학교), 김유래(연세대학교), 서정택(가천대학교)
	344	미국 원자로 물리적방호 규제체계 변화와 주요 규제특징 분석 전성현, 서정규, 최동준, 서정택(가천대학교)
	346	휴머노이드 로봇의 물리적 안전 위반 탐지를 위한 시뮬레이션 기반 퍼징 방법 진규정, 이세영(강원대학교)
10:30~11:30 (7-D) 정보보호 표준/정책/평가 II 좌장: 장상운 (국가보안기술연구소)	333	HITRUST r2와의 비교를 통한 ISMS-P 사후관리 개편방안 분석 김건우, 이효경, 주민재, 임민혁, 최예윤, 이세영(강원대학교)
	95	LLM 기반 제로 트러스트 보안 정책 운영 프레임워크 -규범 근거 기반 정책 생성 및 4-Layer 검증 체계- 오윤경, 차진희, 손윤서, 곽진(아주대학교)
	231	N2SF 업무정보 등급분류의 맥락 보완을 위한 보조속성 모델 제안 어명규(수원대학교), 서민주(고려대학교), 김효빈(성신여자대학교), 이유진(서울여자대학교), 이주오(명지대학교), 유재욱, 김현민(금융보안원)
	375	NIST CSF 2.0 Subcategory 매핑 기반 ISMS-P 통합관리 프레임워크 설계 제안 정세영(서울여자대학교), 이재윤(수원대학교), 두경은(성신여자대학교), 이영언(서울여자대학교), 박지원(중앙대학교), 우지민(고려대학교), 육은서(서울여자대학교), 홍석현(중앙대학교), 김채영, 공지훈(소속없음)

2026년 10월 29일(목)

세션	논문번호	논문제목(저자/소속)
10:30~11:30 (7-E) 암호이론 및 구현 II 좌장: 구본욱 (국가보안기술연구소)	9	메시지 기반 데이터센터 전송 암호화의 키 교환 개선 남재호, 강준혁, 권태경(서울대학교)
	238	동형암호 기반 이상 탐지의 점수·판정 출력에 따른 임계값 누출 분석 조수빈, 방지원, 김민서, 이승원, 서화정(한성대학교)
	165	ARM 아키텍처 특성을 고려한 Microsoft SEAL-Embedded CKKS NTT 최적화 및 성능 분석 김채린, 김영범, 서석충(국민대학교)
	310	저사양 장치를 위한 CKKS 메모리 최적화 신종식, 이진현, 신동현, 김채린, 서석충(국민대학교)
10:30~11:30 (7-F) 블록체인/암호화폐 II 좌장: 이석준 (가천대)	94	영지식증명(Zero-Knowledge Proof) 기반 하이퍼레저 패브릭 트랜잭션 정렬 무결성 검증 시스템 박효준, 박기석(인천대학교)
	104	프라이버시 보존형 지불 채널 허브를 위한 감사 가능성 분석 프레임워크 김현서, 신영아, 정익래(고려대학교)
	168	배치 순서 공정 시스템에서의 프론트러닝 억제 및 트랜잭션 정렬 이동욱, 조남수, 윤택영(단국대학교)
	169	이기종 Hyperledger Fabric 환경에서 온체인 MCDM의 수치 결정성 확보 김진수, 김희찬, 이경윤, 손준영(부산대학교)

2026년 10월 29일(목)

세션	논문번호	논문제목(저자/소속)
11:40~12:40 (8-A) [AI보안] LLM탈옥/프롬프트 인젝션 방어 II 좌장: 박해룡 (한국인터넷진흥원)	170	최신 상용 LLM의 세대 간 멀티턴 탈옥 저항성 비교 연구 박민서, 김민서, 김준상, 정승민, 고윤서, 신상욱(국립부경대학교)
	318	정상 근거 중복이 유사도 기반 RAG 오염 방어에 미치는 영향 김성엽, 유진호(상명대학교)
	366	한국어 말투 변이에 따른 LLM 프롬프트 인젝션 판정의 강건성 평가 최주혁, 권현수(인하대학교)
	101	프롬프트 주입 공격에 대한 의미 기반 및 구조 기반 방어 기법의 효과 분석 권나현, 신동원, 손수엘(한국과학기술원)
11:40~12:40 (8-B) 취약점분석 III 좌장: 한인성 (국방과학연구소)	139	Android-CDS: 단일 모바일 단말 내 보안 도메인 간 파일 전송 통제를 위한 설계 이용재, 이여민, 김수빈, 박정수(강남대학교)
	197	동형암호 기반의 프라이버시 보존차량 디지털 포렌식 기법 하상우, 김도현, 최현민, 조성제(단국대학교)
	380	디지털포렌식의 프라이버시 보호를 위한 검색 가능 대칭키 암호 기반 증거 수집 방안 안도연, 박채민, 이우진, 이상현, 주현아, 김도현(국립한국해양대학교)
	406	역방향 추적 기반 Android Intent 취약점 분석 기법 안효빈, 신정헌, 방예현, 배준영, 김민석, 권민준, 배진석, 나웅재, 김주원, 장정안(KISA 화이트햇 스쿨)
11:40~12:40 (8-C) 자동차보안 II 좌장: 한상윤 (국가보안기술연구소)	189	차량 침입대응 정책 비교를 위한 틱 동기 그림자 실행과 기록 일관성 검사 박영주, 손준영(부산대학교)
	387	도로 지도 정합성 검사를 이용한 V2X Constant Position Offset 공격의 탐지 조건 분석 강민정(충북대학교), 이혁재(명지대학교), 홍석진(광운대학교), 이세영(강원대학교)
	195	서명자별 설치 권한 세분화를 위한 이중 게이트 기반 OTA 검증 계층 고윤민(한동대학교), 장인수, 김진홍(한국전자통신연구원)
	217	CVE-ATM 증거 그래프를 활용한 TARA 공격경로 생성 및 분석 방안 박준호, 김찬민, 이상욱(한국자동차연구원)
11:40~12:40 (8-D) 시스템보안 II 좌장: 김익균 (한국전자통신연구원)	211	HID 위장 장치의 키 입력 복원 및 실행 의미 분석을 통한 BadUSB 탐지 기법 한우혁, 곽나영, 정지윤, 정유찬, 현상원(명지대학교)
	334	TPM 원격 증명을 위한 기준 상태 전이 승인 검증 기법 제안 이성은, 박미리(가천대학교), 박춘서(한국전자통신연구원), 서정택(가천대학교)
	26	WSL2를 통한 Windows 파일 변조 실시간 탐지 및 차단 시스템 한동균, 김한결, 박화비, 박명서(한성대학교)
	31	지식 증류 기반 경량 비전 트랜스포머를 이용한 악성코드 이미지 탐지 기법 이영재, 김병만(국립금오공과대학교)

2026년 10월 29일(목)

세션	논문번호	논문제목(저자/소속)
11:40~12:40 (8-E) [AI보안] 딥페이크 탐지/방어 II 좌장: 김희석 (고려대)	257	다양한 이미지 코덱 변환에 따른 AI 생성 이미지 탐지 성능 분석 연구 서상혁, 황은비, 권태경(연세대학교)
	19	BACE: Block-Adaptive Cross-attention Erasure를 이용한 확산 모델의 정합쌍 기반 유해 개념 제거 서채은, 류권상(국립공주대학교)
	36	생성형 AI 기반 이미지 합성·편집에 대한 선제적 보호 기술 동향 강현성, 류권상(국립공주대학교)
	372	AI 생성물 탐지를 위한 주파수 파워 스펙트럼 기반 실증적 연구 정민기, 이상용(성균관대학교), 윤성빈, 손동성(공소청), 우사이먼성일(성균관대학교/시큐어머신스랩)
11:40~12:40 (8-F) 사이버위협 인텔리전스 II 좌장: 문대성 (한국전자통신연구원)	119	네트워크 침입 탐지에서 데이터셋 및 탐지 모델에 따른 XAI 설명의 충실도 비교 백동명, 김선호, 이현우(한국에너지공과대학교)
	311	AI 에이전트 환경의 내부자 위협 탐지와 동작 로그 기반 통제 체계 구축 조윤철(중앙대학교), 홍기완(한라대학교), 김지민, 김혜원, 이동우, 이서진, 장항배(중앙대학교)
	186	데이터 불균형 환경에서 합성데이터를 활용한 침입 탐지 성능 분석 이재희, 박준혁, 조하늘, 안효범(국립공주대학교)
	187	Multi-Task 경량 언어 모델 기반 CVSS 지표 예측에 대한 Local XAI 기법 적용 및 보안 키워드 기여도 분석 박준혁, 이재희, 조하늘, 안효범(국립공주대학교)

2026년 10월 30일(금)

세션	논문번호	논문제목(저자/소속)
09:20~10:20 (9-A) [AI보안] AI에이전트 보안 IV 좌장: 권혁찬 (한국전자통신연구원)	56	머신 언러닝 모델의 탐지 가능성 완화를 위한 내부 표현 정렬 프레임워크 김현옥, 김상민, 이병천, 박형준(중앙대학교), 박성우(덕성여자대학교), 이미영, 노승민(중앙대학교)
	271	Massive SLM 협력 구조 기반 아키텍처 중심 머신 언러닝 박소현, 김서이, 한연주, 이일구(성신여자대학교)
	22	LoRA 기반 파인튜닝 모델의 오염 학습 샘플 사후 순위화 기법 강병수(명지대학교), 김민석, 구형준(성균관대학교)
	115	ATLAS 기반 에이전틱 AI 맞춤형 공격 시나리오 자동 생성 프레임워크 정연수, 이주영, 이태진(가천대학교)
09:20~10:20 (9-B) [AI보안] AI에이전트 취약점 분석 III 좌장: 김수현 (순천향대)	338	온라인 적응형 LLM 서빙에서 공유 추정기를 통한 사용자간 성능 저하 공격 분석 이도하(세종대학교), 김민기(서강대학교), 신가영(백석대학교), 허영조(아주대학교)
	43	언러닝된 언어 모델의 개인 식별 정보 복구 가능성 분석 권유정, 구형준(성균관대학교)
	117	Poison the Tiny Files, Break the Big Brains of Vision-Language-Action Policies Abhishek Chaudhary, 최선오(전북대학교)
	395	LLM 추론 엔진의 취약점 탐지 및 사고 대응을 위한 소스 레벨 로깅 방안 연구 조민혁, 정수은, 박정흠(고려대학교)
09:20~10:20 (9-C) 산업/우주/국방보안 IV 좌장: 공준진 (웨이브피아)	350	K-RMF 적용 무기체계 연구개발사업을 위한 리눅스 서버 자동화 점검도구 구현 노승일, 조한별(국방기술품질원)
	16	SCAP 기반 K-RMF 보안통제항목 자동 점검 및 형상변경 탐지 방안 하형전(아주대학교), 오재민(세종대학교), 김강석(아주대학교)
	164	이기종 협업 로봇 환경에서의 신뢰도 오염을 통한 선택적 배제 공격 임호현, 이세영(강원대학교)
	302	무기체계 보호대상 안티탬퍼링 기술 적용 수준 분류 방안에 관한 연구 이상헌, 허동회, 한인성(국방과학연구소)
09:20~10:20 (9-D) 부채널분석/대응 IV 좌장: 강유성 (한국전자통신연구원)	151	표준 ML-KEM-512에 대한 선택 암호문 부채널 공격 – PQClean의 Barrett Reduction 구현을 중심으로 오충연, 안현준, 한동국(국민대학교)
	219	t-SNI를 만족하는 효율적인 고차 Keccak 마스킹 구조의 설계와 안전성 증명 안현준, 한재승, 한동국(국민대학교)
	225	마스크 후보 확률을 이용한 코드워드 마스킹 HQC의 재실행 부채널 분석 이주원, 정상윤, 김희석(고려대학교)
	163	공개 마스킹 ML-DSA 하드웨어 구현에서의 잠재적 부채널 누설 분석 박현주, 박수진, 장지훈, 김수리(성신여자대학교), 홍석희(스마트엠투엠), 김희석(고려대학교)

2026년 10월 30일(금)

세션	논문번호	논문제목(저자/소속)
09:20~10:20 (9-E) PQC 및 PQC전환 IV 좌장: 김준섭 (한국인터넷진흥원)	270	추가 Ancilla Qubit 없는 동일한 두 S-box 양자 회로 생성기 이창민, 오진섭, 김영수, 최두호(고려대학교)
	292	큐비트 예산과 목표 성공 확률에 따른 CHAM 양자 키 탐색의 부분 중간값 보관 김민서, 이승원, 조수빈, 서화정(한성대학교)
	64	양자키분배(QKD)와 양자내성암호(PQC)의 지연 관련 서비스 품질(QoS) 특성 비교 진소정, 김형수(아이오티커뮤니케이션테크 양자통신연구소)
	261	PQC-QKD 하이브리드 키 관리와 장애 복구 기술 동향 김정도, 임우상, 김영식(대구경북과학기술원)
09:20~10:20 (9-F) 네트워크/클라우드 보안 IV 좌장: 이원혁 (한국과학기술정보연구원)	140	국방 전술 통신을 위한 O-RAN Near-RT RIC 내 DoS 공격의 PPS 및 연결 상태 분석 이현지, 유현수, 김환국(국민대학교)
	146	국방 통신환경에서의 Non-RT RIC rApp 배포 자동화를 위한 LLM 기반 설정 값 목록 생성 기법 조강익, 유현수, 김환국(국민대학교)
	245	전술통신 환경을 위한 Prototype 기반 가우시안 샘플링 데이터 증강 기법 제안 원채은, 김환국(국민대학교)
	317	5G 네트워크 슬라이싱 환경에서 시그널링 공격의 영향 분석 김진하, 김환국(국민대학교)

2026년 10월 30일(금)

세션	논문번호	논문제목(저자/소속)
10:30~11:30 (10-A) [AI보안] AI에이전트 검증 및 평가 III 좌장: 김수형 (한국전자통신연구원)	234	대규모 언어모델 언러닝의 방향적 비대칭 분석 장민, 권환우, 전용진, 김영화(유엠로직스)
	376	양자화된 LLM의 비트 수에 따른 안전성 분석 박주현, 송현태, 나건희, 유민준, 석병진(한성대학교)
	289	DART: 오픈월드 적대적 평가를 위한 Critical Cue Bank 기반 방어 인지형 레드티밍 신준석, 민동욱, 장진혁, 남승수, 최대선(숭실대학교)
	365	최적화된 FGSM 패치를 유해 시각 트리거로 활용한 비전-언어 모델의 화이트박스 백도어 학습 안드로 아프릴라 아디푸트라, 레티투흐엉, 신다윗, 김호원(부산대학교)
10:30~11:30 (10-B) 소프트웨어보안 IV 좌장: 이은경 (국가보안기술연구소)	194	대규모 코드베이스에서의 LLM 기반 소프트웨어 결함 위치 추정 기술 연구 박여웅, 심연호, 서지원(단국대학교)
	256	다중 분석과 독립 검증으로 구성된 LLM 기반 취약점 탐색 파이프라인 배연주, 강민주, 박정우, 한규상, 김정수, 전승호(가천대학교)
	275	LLM과 RAG를 활용한 트레이스 기반 Juliet Java 소스 코드 대상 취약점 탐지 및 평가 장현지, 최주언, 윤상권, 김승혁, 김경백, 최광훈(전남대학교)
	369	바이너리 유래 코드 표현이 LLM 기반 CWE 탐지 성능에 미치는 영향 분석 정서진, 김동엽, 장진수(충남대학교)
10:30~11:30 (10-C) [AI보안] 딥페이크 탐지/방어 III 좌장: 김종성 (국민대)	30	ISS-Guard: 신원, 의미론, 공간적 다중 손실 융합을 통한 딥페이크 사전 방어 기법 윤태준, 류권상(국립공주대학교)
	52	FoundDef: Frozen Pre-trained Encoder 기반 얼굴 교체 딥페이크 능동 방어 기법 유하늘, 류권상(국립공주대학교)
	68	음성 딥페이크 생성 억제를 위한 UAP의 취약 발화 특성 분석 김하진, 박서영, 정수환(숭실대학교)
	97	VAE 인코더 경로를 표적으로 하는 학습 불필요 딥페이크 선제 방어 기법 이재웅, 류권상(국립공주대학교)
10:30~11:30 (10-D) 콘텐츠/저작권 보안 좌장: 박상욱 (한국전자통신연구원)	37	한국어 방언 식별을 위한 Attention Pooling 및 Layer Freezing 적용 연구 양희준, 김인호, 이웅재, 정수환(숭실대학교)
	47	한국수어사전 표제어 피복 분석과 어휘 정비 후보 도출 -NCS 정보보호·개인정보보호 능력단위명을 대상으로- 한승재, 박민수, 김창훈(대구대학교)
	227	참조 음성 길이에 따른 음성 딥페이크 생성 억제 기법의 성능 분석 임지현, 박서영, 정수환(숭실대학교)

2026년 10월 30일(금)

세션	논문번호	논문제목(저자/소속)
10:30~11:30 (10-E) 취약점분석 IV 좌장: 전승호 (가천대)	250	정말 Apple 일까?: 숨겨진 자격증명 필드와 대규모 무료 호스팅 피싱의 탐지 사각지대 김도연, 박제만(경희대학교)
	325	RFC 9124 보안 요구사항 기반 SUIT 구현체의 보안 동작 자동 평가 방안 제안 가진섭, 박미리, 서정택(가천대학교)
	218	IoT eSIM RSP 보안 요구사항 변화와 시험 공백 분석 심범종, 원태호, 오지언, 김보남, 유일선(국민대학교)
	370	마스킹 정규화와 영역별 통계 특징을 이용한 QR 구조 기반 피싱 탐지 분석 양희지, 지전일, 조금환(고려대학교)
10:30~11:30 (10-F) 인증 및 ID관리 좌장: 이수미 (금융보안원)	259	Double Guessing Attack에 안전한 1라운드 saPAKE 프로토콜 황리교, 신채연, 황정연(성신여자대학교)
	7	Onion Encryption과 Counter를 활용한 문맥 기반 Message Franking 기법 강규현, 방지석, 김재윤, 배우리, 윤택영(단국대학교)
	242	공개 원장 환경에서 비밀번호 검증 기반 비밀키 복구 기법 김종현, 조남수, 윤택영(단국대학교)

2026년 10월 28일(수)

세션	포스터번호	논문번호	논문제목(저자/소속)
13:00~14:00 포스터 I [AI보안] 좌장: 곽병일 (고려대)	P-001	384	증거 기반 독립 검증을 적용한 역할분리형 Agentic SOC 참조 아키텍처 설계 윤은한, 이광수(세종대학교)
	P-002	386	내부자 기반 원문 삽입 공격에 대한 LLM 에이전트메모리의 Top-k 강인성 분석 박민서, 장진수(충남대학교)
	P-003	398	위험행위 중심의 한국어 AI 에이전트 보안성 평가 벤치마크 설계 안훈성(동국대학교), 김진호(고려대학교), 박정은(명지대학교), 이환승(전주대학교), 김영옥(숭실대학교), 유명성(서울시립대학교)
	P-004	74	접근성 라벨·시각 정보 조작을 통한 안드로이드 AI 에이전트 오작동 유도 기법 윤성배, 박제만(경희대학교)
	P-005	83	AI 에이전트 데이터 처리 프레임워크의 비신뢰 외부 데이터 연결 문제 분석 임찬혁, 임수빈, 정수환(숭실대학교)
	P-006	92	Agentic Payment를 위한 보안 요구사항 분석 및 x402 프로토콜 평가 이소영, 유지현(광운대학교)
	P-007	112	SCH Guard: LLM 에이전트 스킬의 페이로드 없는 공격 탐지를 위한 의미론적 검증 코어의 설계 및 평가 함주혁, 조해현(숭실대학교)
	P-008	220	웹 보안 시나리오 기반 LLM기반 에이전트의 목표달성과 허용 규칙 준수 분리 평가 오도연(부산대학교), 이은진(숙명여자대학교), 이준혁(고려대학교), 차아미(수원대학교), 현석훈(미래에셋), 문재현(한국기술거래사회), 장상근(로그프레소)
	P-009	229	MCP Tool의 Description과 Annotation 간 불일치가 LLM Agent의 Tool 실행 판단에 미치는 영향 연구 임건형, 피여라, 원신영, 권태경(연세대학교)
	P-010	279	Skill Marketplace Poisoning: 메타데이터 조작을 통한 악성 스킬의 검색 노출 및 자동 선택 공격 김준현, 오정민, 한태현, 이태진(가천대학교)
	P-011	291	다중 출처 교차 검증 기반 AI 에이전트의 Injection 공격 방어 연구 최유나, 한태현, 이태진(가천대학교)
	P-012	327	AI 에이전트 가상화 격리 기술 동향 분석 유상원, 서정규, 서정택(가천대학교)
	P-013	351	Embodied Agent의 안전성과 실행 비용에 대한 SAS-MAS 비교 분석 오태경, 박가은, 김서이, 이일구(성신여자대학교)
	P-014	399	임바디드 에이전트 워크플로 경계별 안전 필터 설계: 이미지 기반 공격을 중심으로 이성민(서울시립대학교), 송영욱(한신대학교), 이재우(단국대학교), 오수진(이화여자대학교), 정시형(BoB), 유명성(서울시립대학교)
	P-015	81	LLM 에이전트를 위한 프롬프트 인젝션 방어 및 런타임 보안 제어: 비교 리뷰 레티투흐엉, 이창율, 조재한, 함단 아자니, 신다윗, 김호원(부산대학교)

2026년 10월 28일(수)

세션	포스터번호	논문번호	논문제목(저자/소속)
13:00~14:00 포스터 I [AI보안] 좌장: 곽병일 (고려대)	P-016	205	Agent 가드레일 신호 기반 백도어 가능성 분석 최나영, 나현식, 최대선(숭실대학교)
	P-017	232	엄격한 출력 스키마가 멀티에이전트 보안 분석의 실패 격리에 미치는 영향 김원겸(경찰청)
	P-018	82	공격적 보안을 위한 대규모 언어 모델 에이전트의 아키텍처 및 학습 요구사항 레티투흐엉, 한승민, 아낙 아궁 응우라 다르마왕사, 물야사리 울란 실바니, 안드로 아프릴라 아디푸트라, 김호원(부산대학교)
	P-019	246	Trust Boundary 기반 AI Agent 최소권한 식별 나건하, 김태희, 방은진, 박한빈, 오로라, 양유상, 박서연, 하승희(KISA 화이트햇 스쿨), 김수민, 박건호(소속없음)
	P-020	392	질의 기반 메모리 포이즈닝 공격의 운영상 한계 분석: 동적 메모리 구조와 정상 기록 축적의 영향 전수아, 김현서, 이태진(가천대학교)
	P-021	401	RAG 시스템의 텔레메트리 보호 설정 평가 박준석, 신정헌, 김창훈(대구대학교)
	P-022	59	RAG 기반 간접 프롬프트 인젝션 공격에서 난독화 기법별 공격 성능 분석 김예주, 송민주(성균관대학교), 우사이먼성일(성균관대학교/시큐어머신스랩)
	P-023	193	UAV 임무 모사 환경에서의 프롬포트 인젝션 반복 평가 백승아, 김진성, 유준수(전북대학교)
	P-024	322	청크 단위 RAG 오염 공격에 대한 방어 기법 제안 이서준, 서정택, 서정규(가천대학교)
	P-025	358	협력형 LLM 클라이언트의 누적 검사 기반 분할 전송 탐지 및 차단 평가 김서준, 이다솜, 박정수(강남대학교)
	P-026	364	간접 프롬프트 인젝션 방어 평가를 위한 업무 계약 보존 감사 김서진, 문형권(호서대학교)
	P-027	389	LLM 보조 코드 분석에서 사람 검증으로 걸러지지 않는 세가지 실패: 브라우저 확장 프로그램 사례 연구 이혁재, 문영민, 박제만(경희대학교)
	P-028	89	불순도 최소화 기반 특징 추출기 선택을 이용한 문제공간 모델 추출 공격 민동욱, 남승수, 최대선(숭실대학교)
	P-029	4	TriGate: LLM의 안전 뉴런 프루닝 공격 방어를 위한 동적 방어 기법 전재원, 유동운, 서준호, 최윤호(부산대학교)
	P-030	160	함정 사이버 위협 분석을 위한 멀티에이전트 기반 공격 체인 정제 및 분석 기법 옥지원, 이정식, 한인성(국방과학연구소)
	P-031	382	LLM 레드티밍 프레임워크 간 공격 성공률 격차의 원인: 판정기 설계 분석 이준우, 김규창, 박민재, 김덕연, 석병진(한성대학교)

2026년 10월 28일(수)

세션	포스터번호	논문번호	논문제목(저자/소속)
13:00~14:00 포스터 I [AI보안] 좌장: 곽병일 (고려대)	P-032	385	대학 생성형 AI 서비스의 개인정보 유출 방지를 위한 다단계 AI 가드레일 서다인, 강민송, 구여빈, 박후린(서울여자대학교)
	P-033	388	단일 턴 입력 가드레일 모델의 다중 턴 확장 및 대화 단위 평가 배예림, 유진호(상명대학교)
	P-034	105	VLA 백도어 방어의 적용 범위와 평가 기준 분석 차승언, 조효진(연세대학교)
	P-035	360	NeRF는 언제 학습 뷰를 기억한 것처럼 보이는가? 카메라 서포트와 뷰 수준 멤버십 신호 물야사리 울란 실바니, 레티투흐엉, 함단 아자니, 김호원(부산대학교)
	P-036	192	단일 순전파 기반 다중객체 추적기의 지속 상태 증폭 공격 김왕진, 유준수(전북대학교)
	P-037	405	동일 표면형의 문맥 의존적 PII 탐지를 위한 한국어 합성 데이터셋 생성 및 사전학습 언어모델 비교 정은혜, 이경현(국립부경대학교)
	P-038	3	Evilog: 공격 증거를 보존하는 LLM 기반 AIOps 로그 마스킹 기법 김보현, 김주영, 장은정(서울여자대학교), 오상학(한양대학교)
	P-039	66	LLM-as-a-Judge를 활용한 ERC-20 승인 오남용 탐지 성능 비교 연구 김건희, 김태훈, 최소현, 박제만(경희대학교)
	P-040	67	한국어 ASR 전사문의 PII 재라벨링을 위한 자모 가중 편집거리 및 LLM 기반 후보 선택 파이프라인 김문주, 박상준, 정수환(숭실대학교)
	P-041	120	AI 기반 사이버 자동대응의 법적 통제모델 연구: 위험등급별 인간감독과 실무자 책임보호를 중심으로 김영남(덕성여자대학교)
	P-042	122	LEAD: LLM 기반 Android 딥링크 세션 탈취 취약점 정적 분석 신현서(고려대학교)
	P-043	144	ChatGPT Windows 앱의 프로세스 상태 및 수집 시점에 따른 생성 응답의 메모리 잔존성 분석 임동현, 최성지, 이준희, 이재훈, 신상욱(국립부경대학교)
	P-044	185	국내외 AI 보안 가이드라인 비교 분석 및 통합 보안 통제 매트릭스 제안 조하늘, 박준혁, 이재희, 안효범(국립공주대학교)
	P-045	208	AI 시스템 수명주기 관점의 학습데이터 무결성 사후검증 방안 연구 노수리, 백남균(덕성여자대학교)
	P-046	241	FedAP: 저전력 IoT 환경의 자원 소모 공격 탐지 및 방어를 위한 유사도 전파 기반 클러스터링 연합 학습 정혜윤, 지승하, 이일구(성신여자대학교)

2026년 10월 28일(수)			
세션	포스터번호	논문번호	논문제목(저자/소속)
13:00~14:00 포스터 I [AI보안] 좌장: 곽병일 (고려대)	P-047	299	GPU 학습 모델의 NPU 추론에서 출력 신뢰성 향상을 위한 선택적 양자화 기법 박성재, 안경덕, 하재철(호서대학교)
	P-048	354	LLM 및 AI 에이전트 아티팩트의 디지털 포렌식 연구 동향 문선우, 이우진, 박채민 김도현(국립한국해양대학교)
	P-049	367	자율 대응을 위한 로컬 LLM 및 RAG 기반 투스테이지 하이브리드 침입탐지시스템 설계 및 구현 김윤섭, 박완(건국대학교)
	P-050	300	대규모 언어 모델을 활용한 악성코드 분석 기술 동향과 랜섬웨어 분석 적용 방안 김대환, 박화비, 최종윤, 박명서(한성대학교)
	P-051	363	신뢰도 기반 오프로딩과 평판 기반 집계를 활용한 연합 강화학습 태스크 오프로딩의 보안 강화 기법 제안 박건우, 이지언, 김원빈, 서대희(상명대학교)
	P-052	368	Physical AI의 행위 안전성을 위한 심각도 기반 차등 대응 프레임워크 이태경, 박소영, 윤성우, 이석준(가천대학교)
	P-053	41	Web GPT와 격리 실행 환경을 활용한 악성코드 분석 보조 시스템 소현우(우석대학교)

2026년 10월 28일(수)

세션	포스터번호	논문번호	논문제목(저자/소속)
14:10~15:10 포스터 II [시스템보안] 좌장: 이재승 (국가보안기술연구소)	P-001	383	웹 애플리케이션 구성 및 배포 특성에 따른 SBOM 컴포넌트 식별 공백 분석 김지민, 이만희(한남대학교)
	P-002	391	취약점 대응을 위한 Third-Party Library 업그레이드의 코드 수정 영향 예측 이정호, 이세영(강원대학교)
	P-003	15	빌드 조건 변경과 보안 패치 적용에 따른 동적 실행 트레이스 변화량 비교 이경신, 이승광(단국대학교)
	P-004	251	OT-IT 융합 환경에서 공급망 침해에 따른 보안 책임의 법적 귀속에 관한 연구 강하은, 홍준호(성신여자대학교)
	P-005	264	그래프 기반 바이너리 역난독화 성능 평가 김영재, 이동훈, 최원석(고려대학교)
	P-006	339	컴파일러 최적화에 따른 C/C++ 메모리 취약 동작 변화 분석 김태헌, 최원석, 이동훈(고려대학교)
	P-007	407	Java 코드 기반 오픈소스 CBOM 생성 도구의 암호자산 식별 성능 평가 박가을, 서승현(한양대학교)
	P-008	314	블록체인과 DevOps CI/CD의융합: 소프트웨어 공급망 보안 관점의 서베이 아마다 유스릴 카딥티야, 조재한, 신다윗, 김호원(부산대학교)
	P-009	14	Client ID Metadata Document의 Fetch-Time SSRF: 재검증 미비와 자격증명 경로 도달 유원정, 신민석, 최종윤, 박명서(한성대학교)
	P-010	28	공개 웹상 개인정보 불법유통 의심 게시글의 게시 양상 분석 김현경(고려대학교), 이재우(인하대학교), 고나영(연세대학교)
	P-011	49	웹 로그인 시간 간격의 표준편차와 변동계수를 이용한 슬로우 무차별 대입 공격 탐지 기법 민준홍, 박지우, 노용균, 안유나, 장진희, 남수만(청주대학교)
	P-012	100	FlowScope: 다중 트래픽 소스와 계층 그래프를 이용한 API 인가 취약점 분석 프레임워크 김태훈, 김경훈, 김광원, 김태연, 서승린, 심지운, 전오규, 최원우, 김주원, 이상현(차세대 보안리더 양성 프로그램)
	P-013	154	내부 업무 환경의 분산된 크리덴셜 노출 탐지 및 대응 지원 프레임워크 제안 양승빈(한양대학교), 김건희(중부대학교), 안정빈(KISA 차세대 보안 리더 양성 프로그램), 우나륜(광운대학교), 장승수(중앙대학교), 전명환(인하대학교), 최우석, 김재성(KISA 차세대 보안 리더 양성 프로그램), 유지현(광운대학교)
	P-014	183	REST API 취약점 기반 SOAR 보안위협 도출 신찬혁, 정인수, 김득훈, 곽진(아주대학교)
	P-015	276	HTTP 인자값 취약점 탐지 관련 동향 연구 신지웅(고려대학교), 위성일(울산과학기술원), 전유석(고려대학교)

2026년 10월 28일(수)

세션	포스터번호	논문번호	논문제목(저자/소속)
14:10~15:10 포스터 II [시스템보안] 좌장: 이재승 (국가보안기술연구소)	P-016	308	로그인 메타데이터 노출 완화를 위한 미래 패스워드 파일 사전 전달 기반 UPAKE 이주현, 조남수, 윤택영(단국대학교)
	P-017	345	보안 분석 관점의 FIDO 연구 동향 홍서연, 김효승(한림대학교)
	P-018	38	URL과 QR 결합 특징을 활용한 스태킹 기반 Quishing 탐지 모델 강경아, 김재겸, 오다윤, 김지윤(경상국립대학교)
	P-019	209	Annotation-free 동적 taint 추적 방법을 이용한 Chrome 확장프로그램의 민감정보 유출 탐지 가능성 연구 문영민, 이혁재, 박제만(경희대학교)
	P-020	34	Infineon SLM9670 기반 TPM 보안 스택의 CVE 도달성 분석과 취약 동작 재현 이동규, 이승광(단국대학교)
	P-021	226	Device Tree 기반 HBOM 표현 구조의 효율화를 위한 하드웨어 구성요소 그룹화 기법 양기정, 신용희, 고웅(한국인터넷진흥원)
	P-022	285	최신 Windows 환경의 ASEP 탐지 한계에 대응하는 동적 프로파일링 기법 연구 엄유정, 이창민, 김영수(고려대학교)
	P-023	355	행위 로그 기반 랜섬웨어 및 정상 프로그램의 특징 공간 분석 정일준, 한승훈(숭실대학교)
	P-024	198	임베디드 리눅스 기반 산업제어시스템 장비의 HBOM 정보 추출 방안 연구 신용희, 양기정, 고웅(한국인터넷진흥원)
	P-025	328	클라우드 지뢰형 탐지 기술과 비가역적 Taint 기반 침해 영향 추적 구조 제안 유광민, 황주하(세종대학교), 김다혜(서울여자대학교), 서장훈(홍익대학교), 박기웅(세종대학교)
	P-026	331	MPU 기반 MCU의 메모리 격리 기법 조사 및 분석 김보규, 지일환, 서정택(가천대학교)
	P-027	316	신뢰 실행 환경을 활용한 원격 서비스의 가용성 향상을 위한 연구 임우진, 장진수(충남대학교)
	P-028	2	macOS Gatekeeper 우회 모델링: curl 다운로드 및 Git 배포 채널을 중심으로 박화비, 김대환, 박명서(한성대학교)
	P-029	17	네트워크 트래픽 기반 Jottacloud API 식별 및 포렌식 데이터 수집 연구 최지은, 신민석, 김대환, 최종윤, 박명서(한성대학교)
	P-030	33	비지상 네트워크 환경에서의 핸드오버 보안 연구 동향 이승빈, 정찬우, 김지윤(경상국립대학교)

2026년 10월 28일(수)

세션	포스터번호	논문번호	논문제목(저자/소속)
14:10~15:10 포스터 II [시스템보안] 좌장: 이재승 (국가보안기술연구소)	P-031	40	메모리 제약 환경을 위한 Rehearsal-Free 네트워크 침입탐지 연속학습 안시은, 김은서, 임연섭(성신여자대학교)
	P-032	121	국내 대규모 MQTT 노출 장비군의 식별 및 비인증 접근 특성 분석 이건형, 함형민(배재대학교)
	P-033	162	안드로이드 앱의 Certificate Pinning 효과 및 실태 연구 이영서, 박제만(경희대학교)
	P-034	200	멀티테넌트 클라우드를 위한 SmartNIC 기반 고성능 호스트 침입 방지 아키텍처 강영효, 김태하, 김이수(한국과학기술원), 유명성(서울시립대학교), 신승원(한국과학기술원)
	P-035	266	머신러닝 기반 경량 IoT 봇넷 탐지 모델 개발을 위한 N-BaloT 특징 축소 기법 연구 차영윤, 김한결, 김지연(대구대학교)
	P-036	361	스마트홈 카메라의 네트워크 제어 프로토콜 분석 및 완화 방안: 헤이홈 Hejhome을 중점으로 이상현, 이우진, 김도현(국립한국해양대학교)
	P-037	381	마이크로서비스 환경에서 제3자 개인정보 제공 정책의 런타임 검증 아키텍처 제안 김민수(중앙대학교), 민수림(국민대학교), 오준영(상명대학교), 오한결(차세대 보안 리더 양성 프로그램), 이가영(국민대학교)
	P-038	206	비밀키를 활용한 안전한 AI 기반 Wi-Fi 행동 인식 기술 박채연, 이일구(성신여자대학교)
	P-039	280	잠재 차원 확장에 따른 FlowSpectrum 기반 암호화 트래픽 분류 성능 분석 김찬형, 김태윤, 윤종희(영남대학교)
	P-040	396	정상 행동 모방 공격에 대한 음원 스트리밍 이상탐지의 보안성 평가 윤영준, 김하민, 조민정, 김역, 이창훈(서울과학기술대학교)
	P-041	111	시간 특징 기반 모바일 결제 이상거래 탐지 및 특징 중요도 분석 이채은, 김아람, 전상훈(수원대학교)
	P-042	167	머신러닝 기반 피싱 사이트 탐지 모델 정확도-지연시간 트레이드오프 비교 김민재, 박수지, 소나무, 전성한(아주대학교)
	P-043	221	침해사고 심각도 평가를 위한 C·I·A 손실 기반 포렌식 준비도 확장 연구 김현지, 백남균(덕성여자대학교)
	P-044	249	AutoSP : ROS 2 Fuzzing을 위한 증거 기반 Runner 자동 생성 박종현, 오현영(가천대학교)
	P-045	278	네트워크 포렌식 지원을 위한 효율적인 로그 저장 기법 이수경, 백남균(덕성여자대학교)
	P-046	161	보안 기능 기반 표준 보안 요구사항의 위협 모델 요소 매핑 및 검증 방법 채지선(삼성 SDS)

2026년 10월 28일(수)			
세션	포스터번호	논문번호	논문제목(저자/소속)
14:10~15:10 포스터 II [시스템보안] 좌장: 이재승 (국가보안기술연구소)	P-047	188	사용량 기반 스마트시티 서비스를 위한 State Channel 기반 스테이블코인 결제 및 환불 시스템 이준승, 이민섭, 정익래(고려대학교)
	P-048	290	Evaluating LLM-Enhanced OpenAPI Specifications for REST API Fuzzing 이수빈, 김범현(한양대학교)
	P-049	76	RGB 색상 데이터 기반 AI 패션 추천 시스템의 백엔드 설계 및 구현 김수환, 이덕규(서원대학교)
	P-050	78	K-Means 색상 정량화와 언어 모델(LLM) 연동을 통한 설명 가능한 개인화 AI 패션 추천 시스템 구현 김지환, 이덕규(서원대학교)
	P-051	400	의료기관 사이버사고 통지·보고 체계의 환자 피해 측정 공백 분석 이종현(한양대학교), 이진주(경희대학교), 김고은(중앙대학교), 김은우(한양대학교), 신동일(서울대학교)
	P-052	48	비금전형 사이버 협박의 위협 모델과 통합 대응 프로토콜 : 대응 지연과 청소년 표적 시나리오를 중심으로 박민수, 한승재, 황성민, 이하늘, 김창훈(대구대학교)
	P-053	75	K-Means 클러스터링 및 HSV 360° 매핑 기반 의류 대표 색상 정밀 추출 알고리즘 김성준, 이덕규(서원대학교)

2026년 10월 28일(수)

세션	포스터번호	논문번호	논문제목(저자/소속)
15:20~16:20 포스터 III [암호/융합보안] 좌장: 석우진 (한국과학기술정보연구원)	P-001	393	PQC 기반 OTAR을 위한 CCSDS TC/TM 전송 모델에서 처리 지연 생략의 영향 김하경, 서화정(한성대학교)
	P-002	394	QKD 키 공급 장애에 따른 ML-KEM 전환 지연 분석 이여녕, 서승현(한양대학교)
	P-003	397	PQC전환 우선순위 결정을 위한 지속적 암호 거버넌스 프레임워크: CycloneDX CBOM 1.6·1.7표현력분석을 중심으로 방지원, 조수빈, 김하경, 형유림, 서화정(한성대학교)
	P-004	62	QKD와 PQC의 결합 위치 및 목적에 따른 연구 동향 분석 박경빈(국립공주대학교), 강찬구(라온컨버전스), 홍도원, 서창호(국립공주대학교)
	P-005	65	HyBind: 연산 문맥에 기반한 PQ/T 하이브리드 암호의 구조적 판별 안종범, 김민서, 허문선, 조수빈, 서화정(한성대학교)
	P-006	99	무인체계를 위한 후양자 명령 인증: 실시간 및 대역폭 제약 하의 KpqC 실현가능성 연구 형유림, 박도윤, 방지원, 임다은, 김하경, 서화정(한성대학교)
	P-007	147	안전한 다자간 양자 계산 기법 비교 분석 신수진, 신상욱(국립부경대학교)
	P-008	214	분야별 양자내성암호(PQC) 전환에 따른 법적·제도적 대응 방안 연구 김준일(전남대학교/한국인터넷진흥원), 송강수(한국인터넷진흥원), 유동현(전남대학교)
	P-009	224	양자 인증 토큰의 경량화와 잡음 내성 연구 동향 김명준, 김영식(대구경북과학기술원)
	P-010	260	GPU 환경 NIST 표준 격자기반 PQC 최적화 구현 통합 라이브러리 설계 구준영, 고주희, 김동천, 최준혁, 서석충(국민대학교)
	P-011	306	GPU 환경에서의 HAETAE 최적화 연구 고주희, 최준혁, 김동천, 서석충(국민대학교)
	P-012	319	SDitH v3의 배치형 BFS VOLE에 대한 조기 종료 오류 분석 및 비밀키 복구 유채연, 김규상, 박수진, 김희석(고려대학교)
	P-013	113	PQC 전환을 위한 키 교환 구조 유승환, 박종환(상명대학교)
	P-014	307	ML-KEM, ML-DSA 및 HQC를 위한 통합 마스킹 ISE 설계 신동현, 서석충(국민대학교)
	P-015	297	하드웨어의 물리적 무결성 확보를 위한 양자 기술 적용 동향 연구 허동회, 이상헌, 한인성(국방과학연구소)
	P-016	281	PQC-Knocking을 이용한 WireGuard VPN 접속 전 인증 구조의 설계 및 구현 박민광, 강민서, 이유찬, 김영수(고려대학교)
	P-017	77	경량 블록 암호 PIPO에 대한 안전한 라운드 기반 저지연 하드웨어 1차 마스킹 김연재(LIG넥스원), 한재승(국민대학교), 허재원, 장우현(LIG넥스원), 한동국(국민대학교)

2026년 10월 28일(수)

세션	포스터번호	논문번호	논문제목(저자/소속)
15:20~16:20 포스터 III [암호/융합보안] 좌장: 석우진 (한국과학기술정보연구원)	P-018	103	KpqC 전자서명 HAETAE에 대한 비프로파일링 부채널 분석 이인훈, 유채연, 박수진(고려대학교), 홍석희(스마트엠투엠), 김희석(고려대학교)
	P-019	116	형태보존암호 FF1 타이밍 부채널의 상수시간 대응 백승훈, 김종건, 김수현(순천향대학교)
	P-020	132	KpqC AIMer v3의 S-box 출력 셰어 누적 연산에 대한 상관전력분석 김동현, 이인훈, 김희석(고려대학교), 홍석희(스마트엠투엠)
	P-021	153	정확한 동형암호 기반 나눗셈(역수) 연산을 위한 효과적인 근사식 설계 방식에 대한 연구 김우현(경희대학교), 박준서(단국대학교), 남기빈(경희대학교), 최현민(단국대학교)
	P-022	171	손실 압축 환경에서 키보드 음향 부채널 공격 기법의 정량적 평가 주현석, 배진석, 김진수, 김찬우, 유준혁(대구대학교)
	P-023	181	HEaaN-FP의 영(Zero) 처리 및 정규화 개선 방법 시티 사례하, 모티타 코이, 신호준, 이동환, 김호영, 정민희, 이윤호(서울과학기술대학교)
	P-024	262	Falcon 가우시안 샘플러의 부채널 분석 및 보호 기법 연구 동향 김영창, 김영식(대구경북과학기술원)
	P-025	288	ATxmega128D4 대상 1차 마스킹 AES-128의 재결합 누설 완화 기법 박예나, 한재승, 한동국(국민대학교)
	P-026	298	MCU와 멀티코어 임베디드 프로세서에서 셔플링 및 더미 연산 기반 소프트웨어 하이딩의 부채널 누설 비교 문채윤, 안현준, 한동국(국민대학교)
	P-027	309	GPU 환경에서 최신 블록암호 운영모드 병렬 최적화 연구 최준혁, 김동천, 서석충(국민대학교)
	P-028	80	CDR 시 활용 가능한 ECDSA 기반 편집 가능 서명에 대한 연구 윤성철, 김수현, 이임영(순천향대학교)
	P-029	128	폴링 주기 변경을 통한 타이밍 관측의 실제·허위 경계 구분: MCUboot 이미지 크기 검증 사례 박정은, 박종환(상명대학교)
	P-030	390	암호화 C-ITS 트래픽에서 공격 탐지를 위한 윈도우 크기 분석 안도현(한국과학기술정보연구원/가천대학교), 신창의(한국과학기술정보연구원), 차충일(한국과학기술정보연구원/가천대학교), 권태웅(한국과학기술정보연구원), 서정택(가천대학교)
	P-031	402	GCS-리더-멤버의 계층 구조에서 동적 UAV 그룹키 합의 기법에 관한 연구 조현아, 전유빈, 김수현, 이임영(순천향대학교)
	P-032	184	DDS-XRCE 환경에서의 런타임 원격검증 기반 세션 권한 관리 기법 이서희, 송유래, 레리사 아데바 질차, 곽진(아주대학교)
	P-033	109	트래픽 메타데이터 기반 암호화 UAV 통신 식별 기법 양채린, 김민철(국립목포대학교)

2026년 10월 28일(수)

세션	포스터번호	논문번호	논문제목(저자/소속)
15:20~16:20 포스터 III [암호/융합보안] 좌장: 석우진 (한국과학기술정보연구원)	P-034	274	차량용 사이버보안 규제 대응을 위한 CVE-UN R155-테스트케이스 자동화 매핑 프레임워크 연구 안혜정, 장수정, 송종혁, 이종국, 심상규(아우토크립트)
	P-035	403	ZT-Odometer: ISO/SAE 21434 Lifecycle 기반 Zero Trust 이행 지표 도출 프레임워크 이세한(페스카로)
	P-036	296	불확실성 보존을 통한 CVE 기반 차량별 Partial 공격 그래프 생성 노관우, 이미라, 최원석(고려대학교)
	P-037	102	UAV GPS 재밍·스푸핑 탐지에서 공격 데이터 증강 기법에 따른 침입탐지 모델 성능 비교 김태훈, 김환국(국민대학교)
	P-038	50	VDE-TER 인증 단말의 자원 보유 이상 탐지 및 가용성 회복 연구 정인서(국민대학교), 조성현(고려대학교), 김대원(국립한국해양대학교), 박무열(한국외국어대학교), 이민우(국립한국해양대학교)
	P-039	216	위성통신 세그먼트 기반 보안 위협 재분류 차재현, 이창민, 김영수(고려대학교)
	P-040	352	CCI 기반 K-RMF 적용 무기체계의 Oracle Database 기술적 점검방안 연구 조한별(충남대학교/국방기술품질원), 노승일(국방기술품질원), 김현수(충남대학교)
	P-041	126	저궤도 위성 네트워크에서 임계위도 구간의 안전한 클러스터 재구성을 위한 인증 기법에 관한 연구 명재민, 이하임, 김원빈, 서대희(상명대학교)
	P-042	27	경로 변조 시 산업용 이동로봇의 보호구역 침범 방지를 위한 지오펜싱 안전여유 설계 및 모의검증 양찬식, 김슬아(한국원자력통제기술원)
	P-043	51	IALA G1192 기반 VDES 인증에서 서명 누락 처리 분석 및 상태 기반 개선 방안 김명서(덕성여자대학교), 이상화(고려대학교), 장원지(국립창원대학교), 황동현(고려대학교), 이민우(국립한국해양대학교)
	P-044	118	스마트항만 구축 단계별 사이버보안 위험요인 분석과 관리체계 방안 김선영, 던소트홀, 김기원(국립목포해양대학교)
	P-045	349	스마트 선박 환경의 랜섬웨어 위협 동향 및 대응 과제 채수민, 최상훈, 박기웅(세종대학교)
	P-046	230	정보보호 예비인력 교육효과성 제고를 위한 역량평가에 관한 연구: 자가인식-훈련수행 격차 분석을 중심으로 박혜민, 김준희, 김아윤, 강주영(한국정보보호산업협회)
	P-047	329	철도 사이버보안 표준 및 보안 기술 동향 분석 정헌영, 최현서, 서정택(가천대학교)
	P-048	54	국외 사이버보안 통제체계 정합성 분석 기반 N²SF 통제항목 보완 방안 제안 전규현, 김현우, 강창협, 조용엽, 손주환(스틸리언)

2026년 10월 28일(수)			
세션	포스터번호	논문번호	논문제목(저자/소속)
15:20~16:20 포스터 III [암호/융합보안] 좌장: 석우진 (한국과학기술정보연구원)	P-049	108	학습 화자 규모별 지식 증류 기반 경량 화자 검증 성능 분석 남은우, 이요원, 항성규, 정수환(숭실대학교)
	P-050	199	해상도 및 측면 각도 변화에 따른 얼굴 유사도 변화 및 3D 정면화 사진의 인식 모델 비교 김석훈, 백승연, 우사이먼성일(성균관대학교/시큐어머신스랩)
	P-051	323	N²SF 환경의 신규 위협 시나리오 분석과 공격 대응을 위한 보안 아키텍처 설계 김효빈(성신여자대학교), 이찬형(한국전자통신연구원), 황주하, 유광민, 박기웅(세종대학교)
	P-052	201	개인정보 보호법과 GDPR상 개인정보 처리관계에서의 역할 분류 기준 비교 분석 연구 유수지(성신여자대학교), 조원재(경기대학교), 임창범(조선대학교)

학술대회 등록방법

◈ 등록비

구분	회원	비회원	현장등록
일반	400,000원	500,000원	500,000원
군 / 공무원	300,000원	350,000원	350,000원
학생(전일제 대학원생)	300,000원	350,000원	350,000원
학부생	250,000원	300,000원	300,000원
시니어(63세이상) 종신회원	무료		

* 등록비 포함 사항: 행사 기간 중 제공되는 식사, 리플릿, 온라인 프로시딩 등

〈제공 식사〉

10월 28일(수) 중식, 석식

10월 29일(목) 중식, 석식(만찬)

10월 30일(금) 중식

- 군/공무원 등록은 주무관청에 소속 중인 공무원증 소지자에 한합니다. (국공립 교직원 제외)
- 시니어 무료등록은 학회 종신회원으로 1964년 12월 31일 이전 출생자에 한합니다.
- 학회 특별회원사 임직원은 학회 회원으로 준합니다.
  특별회원사 여부는 학회 홈페이지 (www.kiisc.or.kr) 회원광장 → 특별회원사에서 확인하실 수 있습니다.
- 회원가 혜택 기준은 행사 당일인 2026/10/28(수)까지 '활동 회원(연회비 납부 회원)'이어야 합니다.
- 학생은 학부생/대학원생 전일제에 한합니다. (타소속 없음)
- 논문 한편당 저자 한 분은 반드시 사전 등록을 하셔야 합니다.

[사전등록]

- 학회 홈페이지(www.kiisc.or.kr)에서 접속할 경우, 학회행사 → 사전등록바로가기 → 학술행사 선택(2026 동계학술대회) 등록하기 선택
- 사전등록 마감일

– 발표자 사전등록: ~2026년 10월 5일(월)까지

– 참가자 사전등록: ~2026년 10월 19일(월)까지

- 계좌번호: 국민은행 754-01-0008-146 (예금주 한국정보보호학회)
- 무통장 입금 결제 시 등록비는 위 계좌로 송금하시고, 입금자가 대리일 경우 통보 바랍니다.
- 신용카드 결제 시 계산서 발급이 불가합니다. (부가가치세법 시행령 제57조)
- 사전등록 시 (2-3일 이내) 기재해주신 이메일로 청구용 계산서가 발행되오니 영수용 계산서가 필요하신 경우 미리 학회로 연락바랍니다.
- 참가확인서는 등록비를 완납하신 분에 한하여 발급 가능합니다.
  한국정보보호학회 홈페이지 상단의 「행사등록 및 참가확인서」 바로가기를 클릭하신 후, 등록 시 입력한 성함과 이메일 주소를 동일하게 입력하시면 출력하실 수 있습니다. (단, 참가확인서는 행사종료 후 다음날부터 발급 가능)

[계산서 문의처]

- 한국정보보호학회 사무국 02-564-9333(내선5), kiisc@kiisc.or.kr

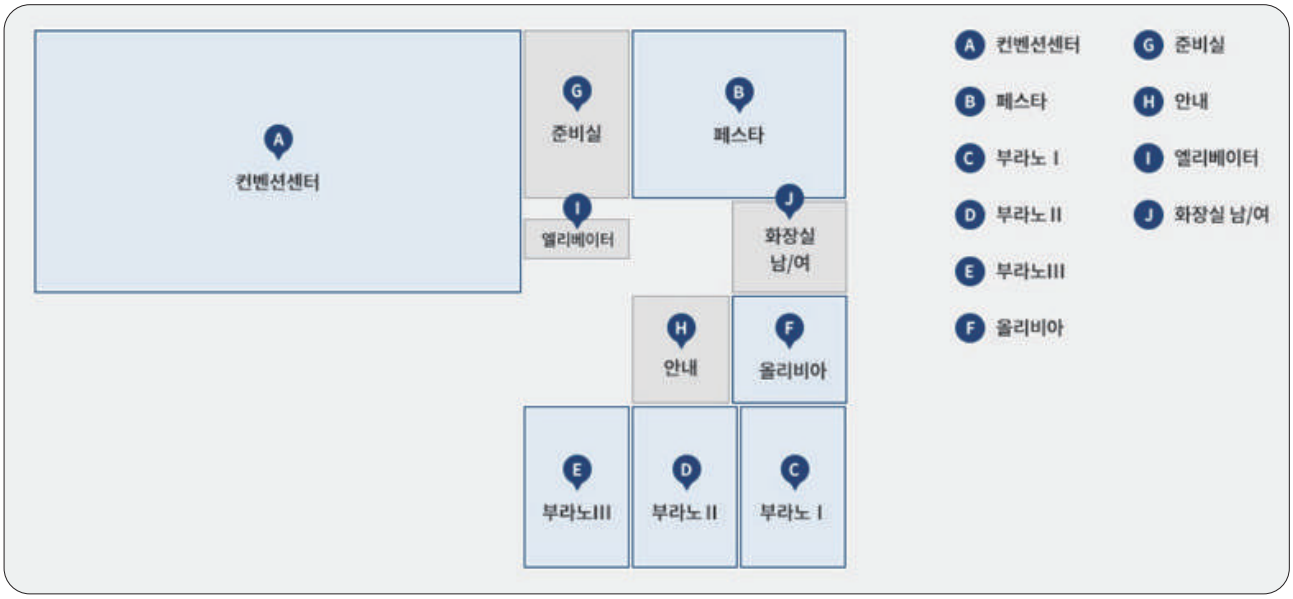
[행사 문의처]

- 한국정보보호학회 사무국(등록 및 행사 진행) 02-564-9333(내선3), kiisc@kiisc.or.kr
- 한국정보보호학회 사무국(논문) 02-564-9333(내선1), kiisc@kiisc.or.kr

주요 행사 장소 안내

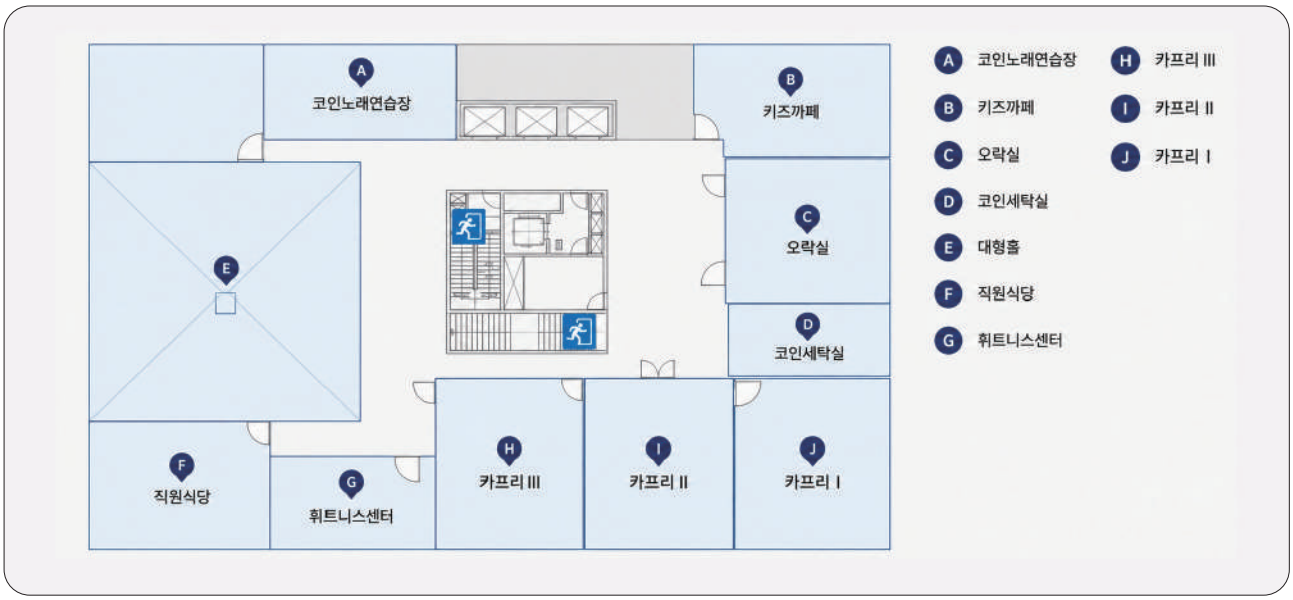
◈ [3층]

- (10/28(수)~29(목)) 등록대: 컨벤션 센터 앞 / (10/30(금)) 등록대: 부라노 I, II, III 앞
- 포스터 세션(10/28, 수), 개회식(10/29, 목): 컨벤션 센터
- 논문 발표: 부라노 I, II, III
- 운영 대기실: 올리비아



◈ [2층]

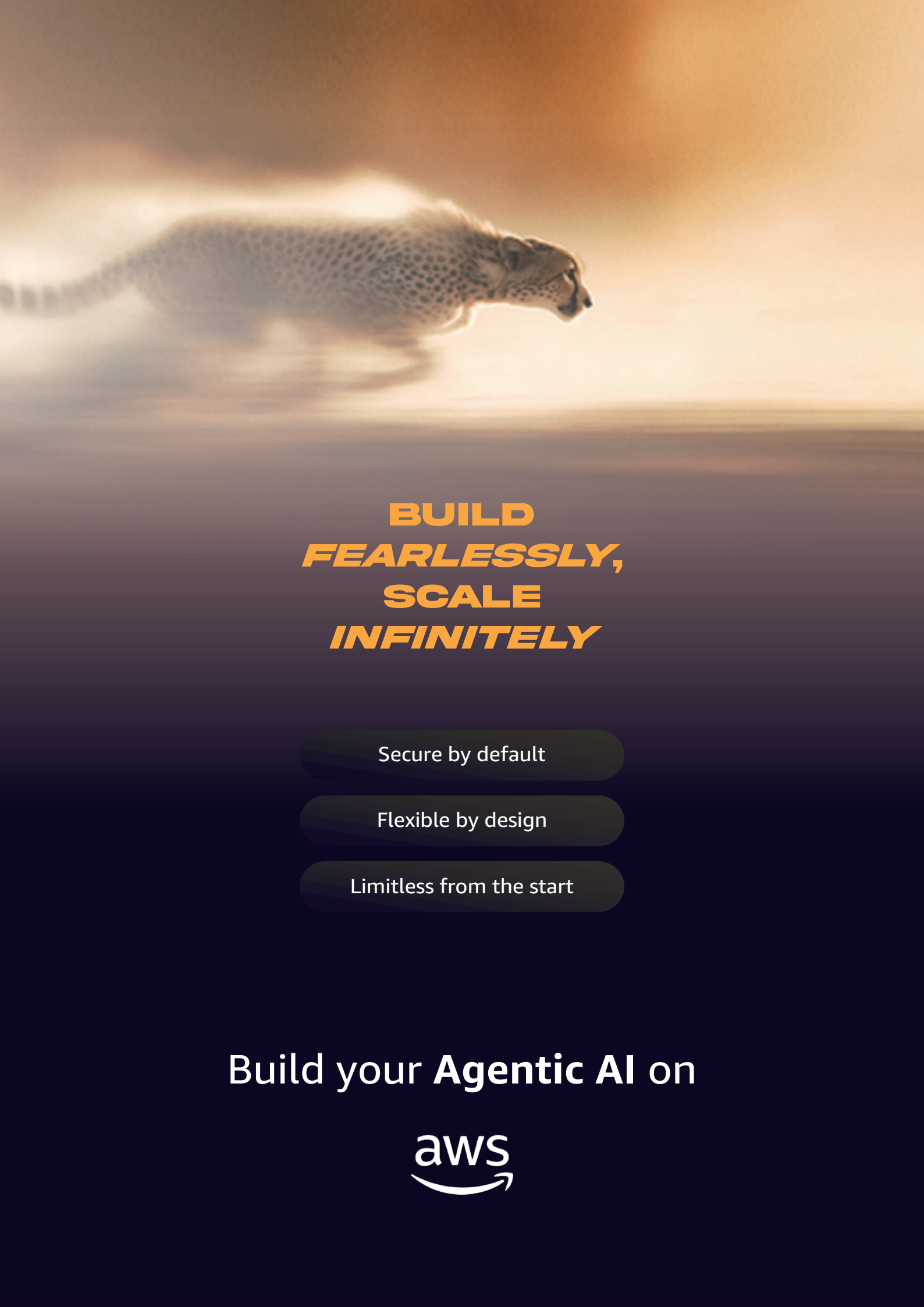
- 논문 발표: 카프리 I, II, III



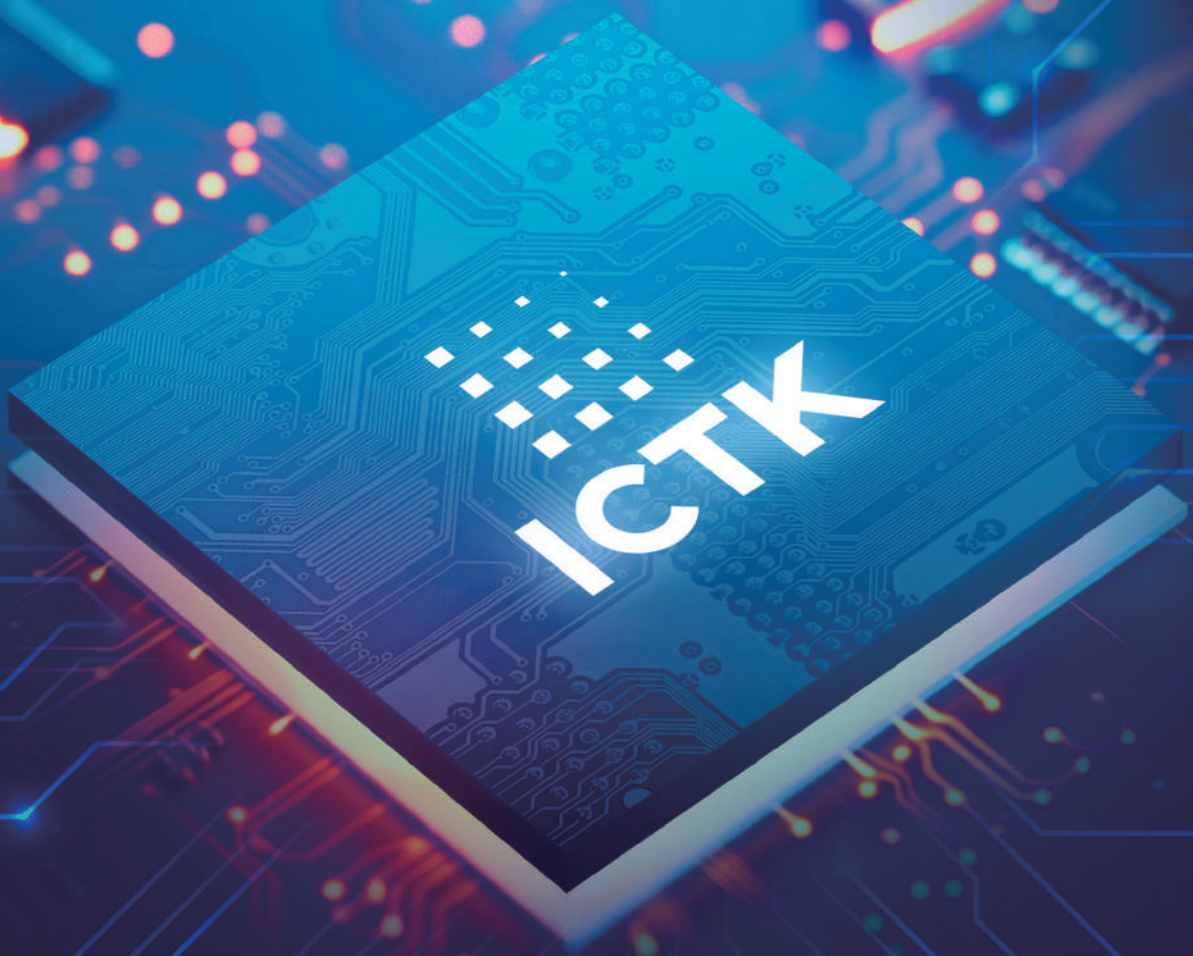
◈ 식사 장소 안내

- 등록데스크에 비치된 안내문 및 사전등록자에게 발송된 안내 이메일을 참고하시어 식사 장소를 확인해 주시기 바랍니다.
- 식사 시 반드시 식사권을 지참하시고, 해당 식사 장소에 제출해 주시기 바랍니다.

※ 명찰 분실 시 재발급이 불가하오니, 행사 기간 중 분실하지 않도록 각별히 유의해 주시기 바랍니다.


BUILD
FEARLESSLY,
SCALE
INFINITELY
Secure by default
Flexible by design
Limitless from the start
Build your Agentic AI on
aws

www.ictk.com



기기의 신원을 증명하고,
암호키를 보호하고,
신뢰를 연결합니다.

Beyond PQC

복제할 수 없는 고유 신원으로 시작하는 하드웨어 보안과
양자 시대까지 신뢰를 이어가는 차세대 보안 기술을 제공합니다.

ICTK

K intelligence

kt, 당신과 미래 사이에



AI시대도 KT

시대가 바뀌어도
연결의 이름은 바뀌지 않습니다

사람과 사람을 잇고,
일상과 기술을 잇고,
AI와 세상을 잇는 이름

AI의 시대 역시 KT,
K intelligence입니다

SmartM2M

AI기반 사이버보안 검증 플랫폼

SmartX

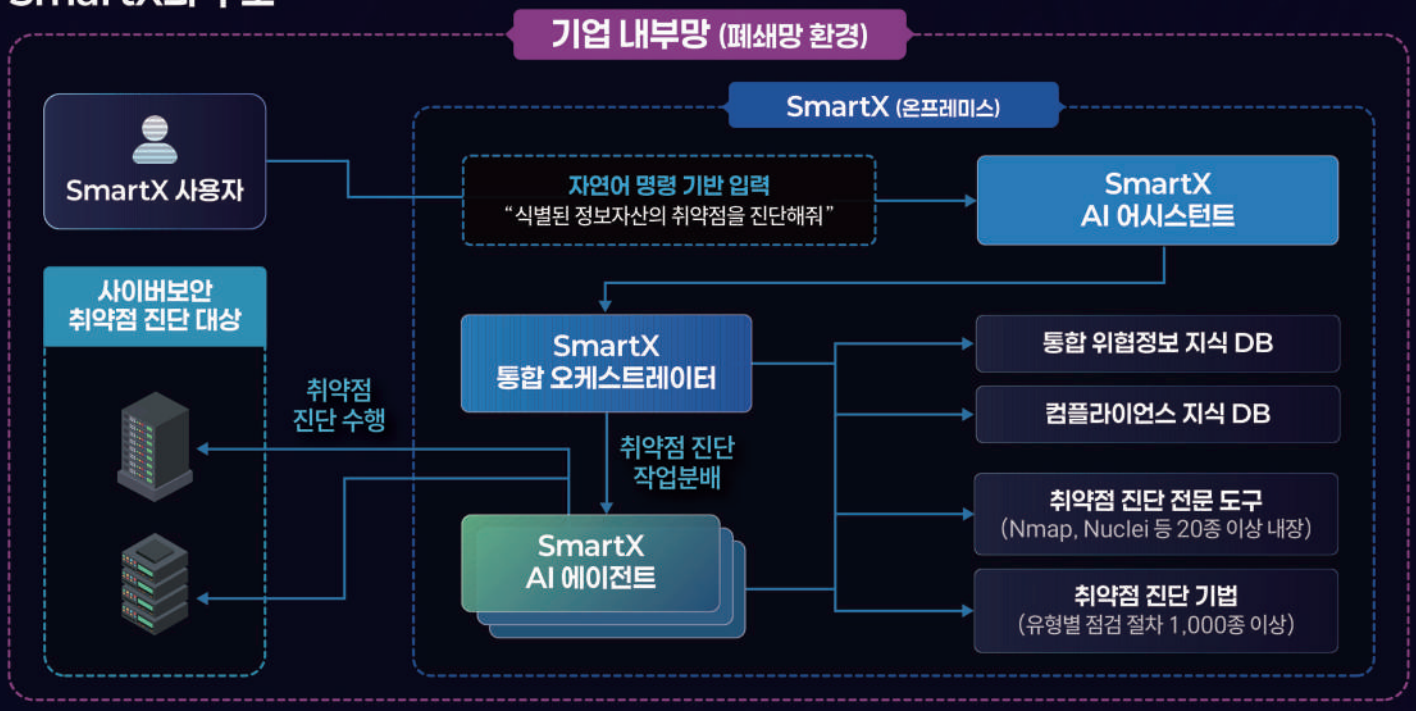
SmartX의 특징

- **폐쇄망 운용**
- **AI기반 취약점 진단**
- **컴플라이언스 검증**
- **결과보고서 자동생성**

폐쇄망 독립 운영 지원 | 온프레미스 구축으로내부망 단독 운영 지원

AI기반 취약점 진단 전 과정 자동화 | 정보자산 식별부터 결과보고서 생성까지 자동 수행

SmartX의 구조



SmartX 사이버보안 취약점 진단 절차

프로젝트 설정 및 생성

보안 검증 범위 단위로 프로젝트를 생성하고 진단 대상 정보를 설정합니다

정보자산 정찰 및 분석

AI 에이전트가 지정한 취약점 진단 범위를 스캔하여 정보자산을 식별하고 분석합니다

사이버보안 취약성 탐지 및 검증

AI 에이전트가 정보자산의 취약점을 단계별로 탐지하고 근거를 확인해 유효한 취약점만 선별합니다

증적 관리 및 결과보고서 생성

AI 에이전트가 취약점 진단 과정에서 증적을 자동으로 수집하고 결과 보고서를 생성합니다

사이버보안 전문가 SmartX를 활용하여 최신 사이버 위협에 대비하세요.

김현곤 이사 | 사이버보안 사업부 | hyeongonkim@smartm2m.co.kr

PriviCam

이미지가 생성되기 전부터 개인정보를 보호합니다

- 개인정보 보호 중심 설계
- 엣지 AI
- 긴급 전환
- 양자내성 암호





이미지 생성 전 개인정보 보호





- 개인정보 보호 중심 설계
- 엣지 AI
- 긴급 전환
- 양자내성 암호



병원



고령자 돌봄 시설



공항

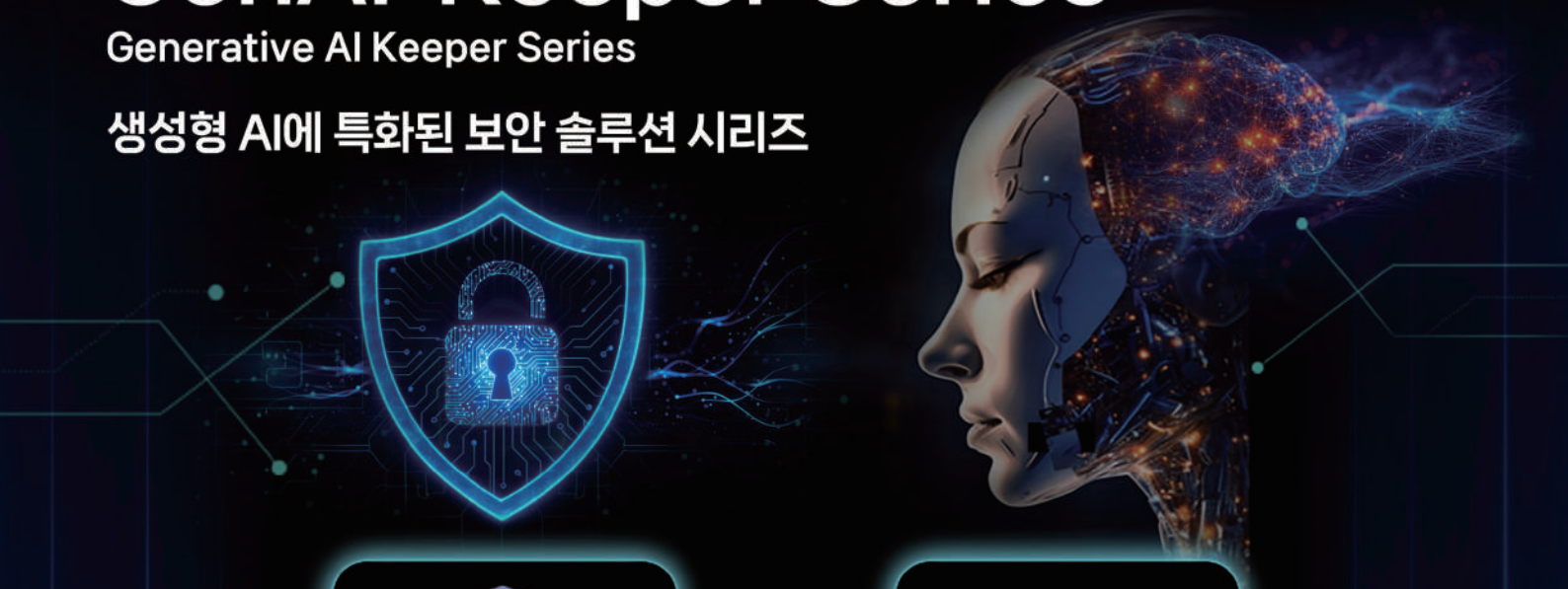
PriviCam by SEQRYPTON
개인정보 보호형 IoT 기술

EUNICESOFT

GenAI-Keeper Series

Generative AI Keeper Series

생성형 AI에 특화된 보안 솔루션 시리즈



생성형 AI 모델을 대상으로 한
적대적 공격 탐지 및 방어

생성형 AI 관련
데이터 무결성 보장

GenAI-Keeper

개인정보/기밀정보 유출방지

가짜뉴스/악성코드
/딥페이크/금칙어 노출 방지

GenAI-Keeper Series

GenAI-Keeper Series는 생성형 AI 모델이 오염되거나 이용자에게 잘못된 정보 및 악성코드 등이 제공되는 것으로부터 생성형 AI 모델과 이용자를 보호합니다.

GenAI-Keeper Series는 클라이언트형, 게이트웨이형, API형 등으로 구성되어, 고객의 니즈에 따라 설치·운영 할 수 있으며, 다양한 생성형 AI 모델을 지원합니다.

유니스소프트 EUNICE

㈜유니스소프트

대전광역시 대덕구 대화로 106번길 66, 711호
(대화동, 펜타플렉스)

제품문의 : ㈜유니스소프트 기획관리본부
T. 042-482-8367 E. eunice@eunicesoft.co.kr

COONTEC

공급망 보안

- AEZIZ
- AEZIZ RMS
- mend.io
- sonatype

인프라 보안

- TeraGRID
- CLAROTY

AI 보안

- ASH
- AEZIZ AICA
- zscaler

조선/해양

- TGM
- KR-CyberOne
- KR-Tester

공격표면 보안

- Cyber Hawk Eye
- penzzer

임베디드 보안

- SecureALPS
- SECURE-IC

임베디드 가상화

- FastVLabs
- RAPITA Systems
- PikeOS RTOS & Hypervisor

5G 특화망

- NXTCore

데이터 보안

- NEXA

COONTEC
marketing@coontec

COONTEC

ⓒ 2026. COONTEC Co., Ltd. All rights reserved.

Global Platform Based
Service Company

TOTAL
Network SERVICES

트리즌엔은
기술과 사람, 세상을 연결하는
지능형 네트워크의 미래를 열어갑니다.



Global Platform
경계를 넘어
세상을 연결하는
세계 최대 서비스 플랫폼

Smart & Intelligent
지능형 AI 기술로
토탈 네트워크의
새로운 가치 창출

Future Innovation
데이터와 기술로
미래를 연결하는
지속가능한 디지털 혁신

㈜트리즌엔 경기도 수원시 영통구 대학3로 4번길 15 테라스힐 2F / 전화 (031) 247-5966 / Fax (031) 212-5903
www.trizn.kr

기업의 성장을,
지역의 혁신을,
무역의 강국을,
국민의 안전을 보증합니다

KTC
한국기계전기전자시험연구원
Korea Testing Certification Institute

글로벌 K-산업의 기준

한국기계전기전자시험연구원

Korea Testing Certification institute



KSA (주)한국보안인증

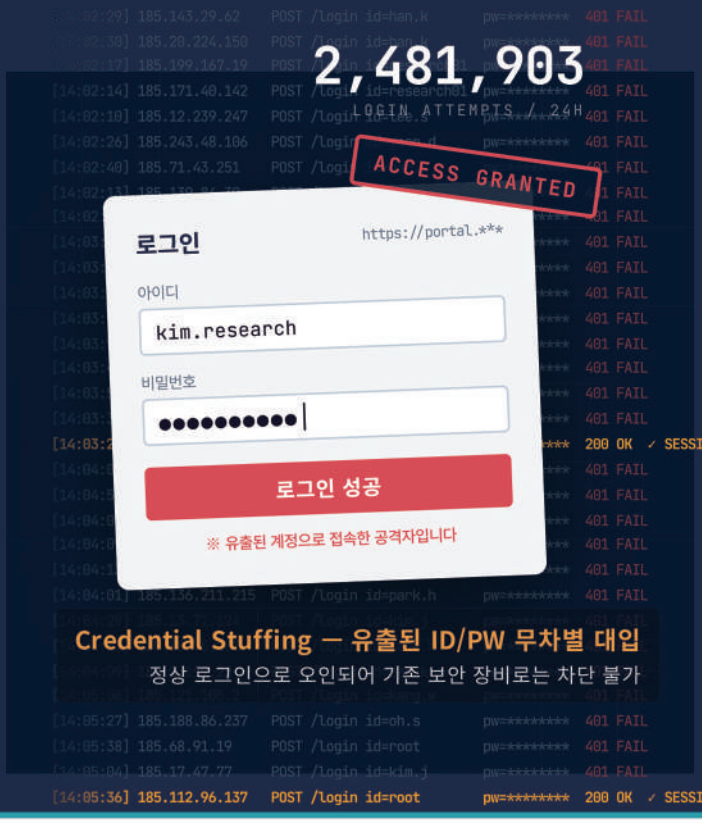
ID·비밀번호만으로는 이미 뚫렸습니다

개인정보 없이.
서버 없이.
네트워크 없이.
2차인증을 완성하다

AI가 공격을 자동화하는 시대 —
사람부터 IoT 기기, AI까지 **전 규모 · 전 환경**을 하나의 플랫폼으로.

OKey-Platform

강한 인증, 더 큰 신뢰



WHY OKey-Platform · 3대 차별화

ID·비밀번호가 탈취되어도 계정은 지켜집니다 — 3가지 '無'로 설계된 2차인증

01

개인정보 없이 CID 기반

원본 개인정보를 저장하지 않고 고유 식별자(CID)만 처리합니다. DB가 탈취되어도 복원 가능한 정보가 없어 2차 피해를 원천 차단합니다.

02

서버 없이 Jar 라이브러리

인증 서버·DB 구축 없이 Jar 라이브러리 임베드만으로 2차인증을 구현합니다. 수 주~수개월 걸리던 구축 기간을 수일 이내로 단축합니다.

03

네트워크 없이 스탠드얼론

OS 로그인 단계에서 직접 2차인증을 수행해 폐쇄망·오프라인 환경에서도 완벽히 동작합니다. 서버 설치만으로 즉시 적용됩니다.

PRODUCT LINE-UP · 하나의 플랫폼, 여섯 가지 인증

OKey-OTP Enterprise
CID 중앙 서버형 · HR/ERP/VPN 연계

OKey-OTP Standard
서버·DB 없는 Jar 임베드형

OKey-Credential
OS 로그인 · su/sudo 권한 통제

OKey-Trust
단방향 제로 트러스트 · 1·2차 동시 검증

OKey-FIDO
FIDO2 / 패스키 생체인증

OKey-PKI
공동·사설 인증서 · 자체 RA/CA

COMPLIANCE · 규제 대응

2027.07 의무화
ISMS-P 2.5.3
인증 수단의 안전한 운영 · MFA 적용

2025.05 시행
N2SF
국가망 보안체계 · 2개 이상 인증요소

시행 중
전자금융감독규정 §14-9
OS 계정 로그인 시 추가인증

시행 중
개인정보보호법 §28의2
안전한 인증수단 + 개인정보 無저장

KSA R&D · NEXT EVOLUTION

사람, PC, 서버를 넘어 Non-Human까지 인증

챗봇·AI Agent·자동화 봇 등 비인간 신원(NHI)을 위한 인증 방식을 연구하고 있습니다.

사람 → PC → 서버 → Non-Human

KSA (주)한국보안인증

무료 상담 · 제품 데모 · PoC 문의 환영

CONTACT 김동규 이사 · 영업 대표
TEL 010-3049-5241
E-MAIL dkkim@kcert.co.kr · www.kcert.co.kr

KOSYAS 한국시스템보증(주)
Korea System Assurance, Inc.

COMPANY PROFILE
회사소개서

THE BEST GLOBAL POWER WITH KOSYAS

정보보호제품 시험·평가·인증 전문기관

한국시스템보증(KOSYAS)은 정보보호제품의 보안성과 성능을 객관적으로 시험·평가하는 전문기관입니다. CC평가, KCMVP 암호모듈 검증, 보안기능확인서, 성능평가부터 취약성 분석·모의해킹과 인증 컨설팅까지 제품이 시장과 공공기관에 도입되는 전 과정을 지원합니다.

IT보안인증사무국 지정	국가정보원 지정	국가정보원 지정	과학기술정보통신부 지정
CC 평가기관	**암호모듈 시험기관**	**보안기능 시험기관**	**성능평가기관**

주요 서비스

01 CC 평가

정보보호제품에 구현된 보안기능의 안전성과 신뢰성을 공통평가기준에 따라 평가합니다.

- KOLAS 인정 평가기관으로서 보안기능 평가 수행
- 인증효력 유지 · 인증서 효력연장 평가 지원
- 근거 : 지능정보화 기본법 제58조

02 암호모듈 검증 (KCMVP)

국가·공공기관이 도입하는 암호모듈의 안전성과 구현적합성을 시험합니다.

- 국내 최초 민간 암호모듈 시험기관
- 기준 : KS X ISO/IEC 19790 · 24759
- 근거 : 사이버안보 업무 규정 등

03 보안기능확인서

보안기능 시험을 통해 확인서 발급 제품은 공공기관 도입 시 보안적합성 검증을 생략됩니다.

- 대상 : 정보보호시스템, L3 이상 스위치·라우터·SDN, 영상정보처리기기 등
- 시험 수행 후 보안기능 확인서 발급
- 근거 : 전자정부법 제56조

04 정보보호제품 성능평가

운영환경에서 제품의 처리능력을 객관적으로 평가해 성능 중심의 제품 선택을 돕습니다.

- 주요기능 구현 · 보안 성능
- 네트워크 성능 (CPS · TPS · Throughput · Latency)
- 근거: 정보보호산업의 진흥에 관한 법률 제17조

05 취약성 분석 · 모의해킹

외부 경계부터 펌웨어 · IoT까지 공격자 관점에서 보안 취약점을 진단합니다.

- 침투테스트 (웹/앱 · 인프라 · API · Wi-Fi)
- 레드팀 · APT 시뮬레이션 (MITRE ATT&CK 기반)
- 시큐어코드 · 바이너리 분석 (SAST/DAST)

06 ICT 서비스 · 컨설팅

CC · KCMVP 인증 준비에 필요한 제출물 작성과 ISMS 보안 컨설팅을 제공합니다.

- CC 보증 제출물 작성 컨설팅
- KCMVP 암호모듈 제출물 작성 지원
- 보안기능시험제도 준비 컨설팅
- 영상정보처리기기 개발지원 시험/컨설팅

한국시스템보증(주)
Tel 02-2097-9700 Fax 02-2097-9777 kosyas.com

한국정보통신기술협회
Telecommunications Technology Association

정보보호안전연구소

디지털 대전환에 따른 복합적인 리스크에 선제적으로 대응하기 위해 개인정보보호, AI 보안, 공공·재난안전을 핵심 축으로 과학적이고 객관적인 검증 체계를 구축하고 있는 기관입니다. 개인정보의 안전한 활용 기반 강화, 신뢰할 수 있는 AI 보안성 검증, 국가 핵심 인프라의 안정성 확보를 통해 급변하는 디지털 환경 속에서 국가 보안을 고고히 하고 국민의 안전과 일상을 지키는 디지털 신뢰 기반을 선도해 나가고 있습니다.

디지털 리스크 선제 대응을 위한

보안·안전 신뢰 기반의 적합성평가 전문기관

개인정보보호 및 안전 활용 지원

- 가명·익명정보 처리 및 데이터 보호 기술 검증
- AI 프라이버시 보호 기술 및 신기술 보안성 평가
- 모바일 신분증, 생체인식 등 차세대 신원인증 보안성 평가
- 개인정보 처리 전 과정에 대한 단계적 시험·인증 체계 구축

AI·디지털 분야 보안성 검증 및 연구

- 공공 분야 AI 시스템 도입을 위한 보안성 및 신뢰성 검증
- 생성형 AI·딥페이크 악용에 따른 신원 위·변조 위협 대응 평가기술 고도화
- 디지털자산(토큰증권, 스테이블코인 등) 보안성·신뢰성 검증
- 디지털의료제품 규제지원센터(전자적 침해행위 예방 등)

안전성·신뢰성 검증 & 공공안전기기

- 철도통합무선망(LTE-R), 재난망 등 통합공공망 연동, 상호운용성 검증
- 공공안전 ICT제품(영상정보처리기기, 드론 등)에 대한 보안 시험·인증
- 실제 운영 환경을 고려한 현장 중심의 기술 적합성 시험
- 재난 예방 및 신속 대응을 위한 공공 인프라 기술 지원

공공·민간 정보보호 및 신뢰성 확보

- CC 평가, 보안기능 시험, 암호모듈 시험, IoT 보안인증
- 개인정보 및 정보보호 관리체계(ISMS-P), 전자서명, 블록체인 신뢰성 검증
- 신용카드 단말기 보안 시험 등 지불결제 시험
- TTA Verified 인증(IPTV용 가입자 단말기능, LTE-R, V-PASS)

주요 추진 성과 및 신규 서비스

- 디지털의료제품 규제지원센터 지정
- 국내 최초, AI 보안 시험서비스 개시
- 영상정보처리기기 보안 시험서비스 제공
- LTE-R 통합공공망 연동 시험서비스 제공
- 모바일 신분증 적합성 평가서비스 제공
- 암호모듈 시험 서비스 제공

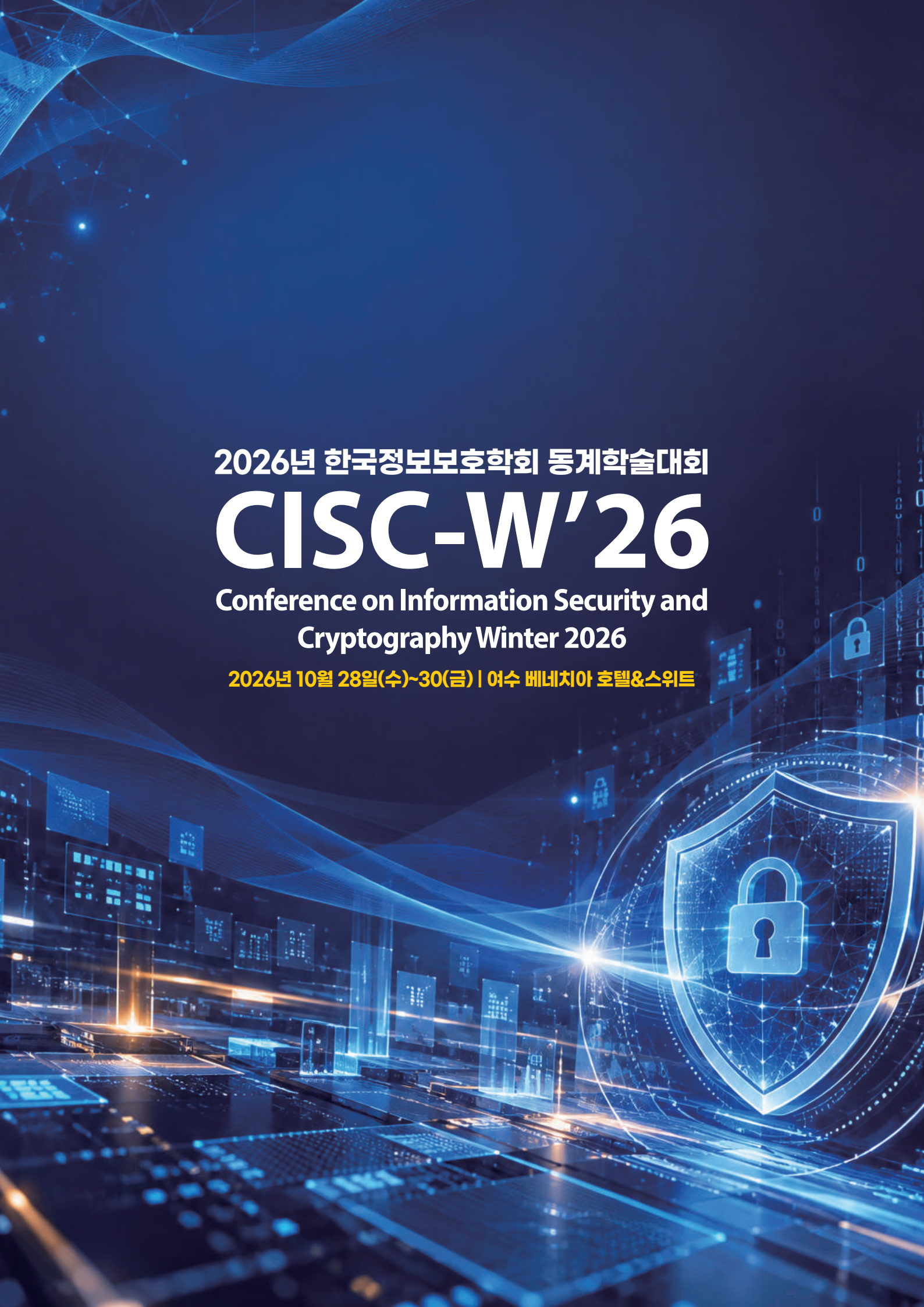
www.tta.or.kr | (13591) 경기도 성남시 분당구 분당로 47 대표전화 1551-1774

MEMO

MEMO

MEMO

MEMO



2026년 한국정보보호학회 동계학술대회

CISC-W'26

Conference on Information Security and Cryptography Winter 2026

2026년 10월 28일(수)~30(금) | 여수 베네치아 호텔&스위트