

한국정보보호학회 2026년 하계학술대회

# CISC-S'26

Conference on Information Security and  
Cryptography Summer 2026

2026년 5월 7일(목)~8일(금)

부산 벅스코 제2전시장 1층/3층

등록데스크: 제2전시장 3층 5A홀 앞

**주최·주관** 한국정보보호학회

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

**기업후원** 그린텍아이엔씨, 대신정보통신, 수산아이엔티, 스마트엠투엠, 아이티센피엔에스,  
에스지에이솔루션즈, 에이치투테크, 앤앤에스피, LG유플러스, 오스코, 이글루코퍼레이션,  
KT, KTNF, 클럼엘, 트리즈엔, 한전KDN, 휴네시온

## 학술대회장

한국정보보호학회 회장 김호원 (부산대학교)

## 운영위원회

- 운영위원장
- 운영위원

신상욱 (부경대학교)	김창훈 (대구대학교)	
권동현 (부산대학교)	김기윤 (부경대학교)	김도현 (해양대학교)
김우년 (국가보안기술연구소)	김정녀 (한국전자통신연구원)	노시완 (동의대학교)
손준영 (부산대학교)	송중석 (한국과학기술정보연구원)	신인철 (부경대학교)
오진영 (한국인터넷진흥원)	최필주 (부경대학교)	한성화 (동명대학교)

## 프로그램 위원회

- 프로그램위원장
- 프로그램위원

서정택 (가천대학교)	이덕규 (서원대학교)	박승현 (한성대학교)
강동호 (한국전자통신연구원)	곽병일 (고려대학교)	곽 진 (아주대학교)
구본욱 (국가보안기술연구소)	구형준 (성균관대학교)	권동현 (부산대학교)
권태경 (연세대학교)	권태웅 (한국과학기술정보연구원)	김도훈 (경기대학교)
김동우 (동국대학교)	김득훈 (아주대학교)	김범현 (한양대학교)
김성욱 (서울여자대학교)	김수현 (순천향대학교)	김종길 (이화여자대학교)
김중성 (국민대학교)	김지윤 (경상국립대학교)	김진우 (충북대학교)
김태성 (충북대학교)	김현일 (조선대학교)	김형식 (성균관대학교)
김형중 (서울여자대학교)	김한국 (국민대학교)	김효승 (한림대학교)
김휘강 (국민대학교)	김희석 (고려대학교)	노희준 (인하대학교)
도경화 (서강대학교)	류권상 (공주대학교)	박기웅 (세종대학교)
박명서 (한성대학교)	박정수 (강남대학교)	박종근 (한국전자통신연구원)
박종환 (상명대학교)	박철준 (경희대학교)	변진욱 (평택대학교)
서대희 (상명대학교)	서민혜 (덕성여자대학교)	서석충 (국민대학교)
서승현 (한양대학교)	서지원 (단국대학교)	서화정 (한성대학교)
성하영 (한국과학기술정보연구원)	손경호 (강원대학교)	송도경 (연세대학교)
신 욱 (국가보안기술연구소)	신인철 (부경대학교)	신지호 (목원대학교)
양대현 (이화여자대학교)	오주형 (한국인터넷진흥원)	우사이먼 (성균관대학교)
유일선 (국민대학교)	유지현 (광운대학교)	윤경국 (한국해양대학교)
윤명근 (국민대학교)	윤인수 (한국과학기술원)	윤종희 (영남대학교)
윤주범 (세종대학교)	윤택영 (단국대학교)	이경률 (목포대학교)
이광수 (세종대학교)	이동재 (강원대학교)	이만희 (한남대학교)
이문규 (인하대학교)	이병영 (서울대학교)	이석준 (가천대학교)
이선우 (이화여자대학교)	이세영 (강원대학교)	이용준 (극동대학교)
이윤경 (한국전자통신연구원)	이유규 (중앙대학교)	이윤희 (서울과학기술대학교)
이일구 (성신여자대학교)	이정훈 (한국외국어대학교)	이종혁 (세종대학교)
이 준 (한국과학기술정보연구원)	이창훈 (서울과학기술대학교)	이태진 (가천대학교)
이현우 (한국에너지공과대학교)	임송빈 (한국인터넷진흥원)	임을규 (한양대학교)
임재덕 (한국전자통신연구원)	임준형 (한국인터넷진흥원)	장대희 (경희대학교)
장진수 (충남대학교)	장항배 (중앙대학교)	전상훈 (국민대학교)
전상훈 (수원대학교)	전유석 (고려대학교)	정성훈 (숙명여자대학교)
정익래 (고려대학교)	조남수 (단국대학교)	조해현 (송실대학교)
조효진 (연세대학교)	주경호 (송실대학교)	지승구 (한국인터넷진흥원)
최대선 (송실대학교)	최선오 (전북대학교)	최원석 (고려대학교)
최윤호 (부산대학교)	최현우 (성신여자대학교)	한승훈 (송실대학교)
홍득조 (전북대학교)	홍준호 (성신여자대학교)	황성재 (성균관대학교)

NO.	구분	상장	논문번호	논문명	저자
1	최우수	부총리 겸 과학기술 정보통신부 장관상	439	코드 다형성 기반 부채널 분석 대응기법의 이론적 분석과 실험적 검증	오성빈, 한동국(국민대학교)
2	최우수	행정안전부 장관상	33	A2A 프로토콜에서 보안 강화를 위한 JWT 서명 기반 바인딩 기법	유진, 김득훈, 곽진(아주대학교)
3	최우수	학회 최우수논문상	452	클라우드 보안사고 조사를 위한 통합 클라우드 포렌식 도구의 필요성	조한나, 최상훈, 박기웅(세종대학교)
4	우수	한국인터넷진흥원 원장상	201	블라인드 부채널 분석을 위한 분석 지점 탐색 기법 연구	이인훈(고려대학교), 김규상(고려대학교), 홍석희(스마트엠투엠), 김희석(고려대학교)
5	우수	한국인터넷진흥원 원장상	224	Why Overthink It? Reducing Pentest Agent Complexity via Modular Skill Injection	Anak Agung Ngurah Dharmawangsa, Thi-Thu-Huong Le, 장현진, 김민규, 김호원(부산대학교)
6	우수	한국전자통신연구원 원장상	82	Over-the-air 테스팅을 통한 5G 단말 메모리 취약점 탐지	오범석, 김광민, 손민철(한국과학기술원), 박철준(경희대학교), 김용대(한국과학기술원)
7	우수	한국전자통신연구원 원장상	274	암호화 트래픽 대상 이상 탐지를 위한 마스킹 기반 멀티모달 지식 증류 모델 제안	지일환, 이주현, 서정택(가천대학교)
8	우수	국가보안기술연구소 소장상	92	산업제어시스템 공급망 보안 강화를 위한 대규모 언어 모델 기반 VEX 생성 연구	김준석, 엄익채(전남대학교)
9	우수	국가보안기술연구소 소장상	168	공개 CVE 기반 AI/ML 프레임워크 취약점 공격 경로 분석 및 LLM 프롬프팅 기반 경량 버그헌팅 방법론	류석준, 박소희, 옥도민, 최대선 (숭실대학교)
10	우수	한국과학기술정보연구원 원장상	451	비밀번호 내 특수문자 사용 패턴을 고려한 확률 기반 비밀번호 생성 연구	정태진, 김억, 손기욱, 이창훈 (서울과학기술대학교)
11	우수	한국과학기술정보연구원 원장상	215	FT-Transformer 기반 준지도학습을 활용한 암호화 트래픽 공격 분류 성능 분석	김태훈, 김환국(국민대학교)
12	우수	학회우수논문상	391	가상 환경 선박 항해 시스템에서의 MITRE ATT&CK ICS 기반 사이버 공격 테크닉 분석 연구	이진성, 박성민, 김대운, 임준형, 나사랑 (한국인터넷진흥원)
13	우수	학회우수논문상	7	UnionSanitizer: Tagged Union Type Confusion 취약점 탐지를 위한 정적-동적 하이브리드 분석 도구	이동준, 윤인수(한국과학기술원)
14	우수	학회우수논문상	238	IoT 침입 탐지 시스템의 강건성 향상을 위한 GAN 기반 적대적 공격 생성-학습 프레임워크	최태준(한국에너지공과대학교), Segun Popoola(Anglia Ruskin University), 이현우(한국에너지공과대학교)
15	우수	학회우수논문상	276	원자력시설 사이버침해 사고 식별 및 탐지를 위한 시뮬레이션 기반 IOC지표 제안	최동준, 지일환, 서정택(가천대학교)
16	우수	학회우수논문상	341	MQTT 기반 IoT 환경에서 PQ-KEM 키 교환 알고리즘 성능 평가	윤성우, 목정현, 박지민, 박소영, 이석준 (가천대학교)
17	우수	학회우수논문상	279	자동화된 Agentic AI 보안 취약성 및 방어수준 진단	김현서, 정연수, 한태현, 이태진 (가천대학교)
18	우수	학회우수논문상	116	Agentic AI 보안 취약성 대응을 위한 Zero Trust 기반 아키텍처 설계	이여민, 이용재, 박정수(강남대학교)
19	우수	학회우수논문상	63	클라우드 스토리지 공유 URL의 비동기 접근에 관한 보안성 연구	문지윤, 장대희(경희대학교)
20	우수	학회우수논문상	222	LLVM IR 기반 디컴파일러 평가 프레임워크 제안	김태현, 최원석, 이동훈(고려대학교)
21	우수	학회우수논문상	412	자율주행 시스템을 위한 NDT 기반 실시간 LiDAR 공격 탐지 방법	최지훈, 최원석(고려대학교)
22	우수	학회우수논문상	32	학습 도메인 구성에 따른 AI 생성 이미지 탐지 일반화 성능 분석	강현성, 윤태준, 이재웅, 류권상 (공주대학교)
23	우수	학회우수논문상	134	Selective Symbolic Execution 기반 프레임워크를 이용한 RAT C2 통신 분석	유현준, 유지현(광운대학교)
24	우수	학회우수논문상	306	부분합 기법과 FFT를 이용한 7-라운드 Kiasu-BC에 대한 향상된 Square 공격	송원우, 김남일, 백승준, 김종성 (국민대학교)
25	우수	학회우수논문상	313	GPU 환경에서 비트 슬라이스 여부에 따른 워드 단위 이진 곱셈에 대한 성능 비교	김동천, 서석충(국민대학교)
26	우수	학회우수논문상	161	S-RMSNorm: Transformer의 보안 추론 가속화를 위한 정규화 연산의 상수화 기법	한상훈, 신호준, 이윤호 (서울과학기술대학교)

NO.	구분	상장	논문번호	논문명	저자
27	우수	학회우수논문상	80	인간과 AI의 시각적 인지 차이를 활용한 적대적 피싱 로고 생성 기법	조예나, 정희성, 방수경(성균관대학교), 김두원(테네시대학교), 김형식(성균관대학교)
28	우수	학회우수논문상	73	중앙 정책 기반 암호 민첩성 서버의 정책 집행 설계 옵션과 보안성 분석	양희재, 김다운, 손수경, 김성민 (성신여자대학교)
29	우수	학회우수논문상	242	ISMS-P 인증제도 실효성 강화 방안 - 현장조사 중심 전환과 인증취소 기준을 중심으로	강민서, 차유진, 홍준호(성신여자대학교)
30	우수	학회우수논문상	368	2라운드 양자내성 비대칭형 PAKE 프로토콜	황리교, 손예원, 배수하, 구자민, 백채원, 황정연(성신여자대학교)
31	우수	학회우수논문상	403	에이전틱 AI 환경에서의 데이터 과다 수집 위험 분석	김준식, 고남현, 김도영, 박준영, 윤주범 (세종대학교)
32	우수	학회우수논문상	142	저궤도 위성 텔레메트리 메타데이터 보호를 위한 형태보존암호 적용 및 오버헤드 임계값 분석	백승훈, 김수현(순천향대학교)
33	우수	학회우수논문상	98	안전한 스마트 그리드를 위한 함수 암호 기반 프라이버시 보장 데이터 집계에 관한 연구	김기환, 김수현, 이명영(순천향대학교)
34	우수	학회우수논문상	176	제로 트러스트 원칙을 적용한 OTT 서비스의 지속적 인증 및 세션 관리 메커니즘 제안	박서연, 이지은, 이종호, 장의진, 신용태 (숭실대학교)
35	우수	학회우수논문상	359	단어 치환 응답을 활용한 LLM 기반 탈옥평가 체계의 한계점 분석	선민준, 권태경(연세대학교)
36	우수	학회우수논문상	103	프로비던스 그래프의 시퀀스-그래프 교차 대조 학습 기반 APT 위험 탐지 프레임워크	윤성수, 엄익채(전남대학교)
37	우수	학회우수논문상	117	Activation Steering 기반 탈옥 공격을 통한 국내 개발 LLM의 안전 정렬 취약성 분석	최민영, 문찬빈, 김승한, 임창훈, 김현일 (조선대학교)
38	우수	학회우수논문상	314	심층 신경망에서 조건적 공분산 축소를 적용한 오류 주입 탐지 기법 제안	안경덕, 김윤성, 하재철(호서대학교)
39	우수	학회우수논문상 (학부생)	204	대규모 최적화 문제 해결을 위한 그래프 분할 기반 양자 어닐링 접근법	배준영, 이동재(강원대학교)
40	우수	학회우수논문상 (학부생)	169	Python 패키지 관리 도구 이질성이 TPL 설치 결과 일관성에 미치는 영향	이정호, 이세영(강원대학교)
41	우수	학회우수논문상 (학부생)	15	HWASan의 Short Granule 기법에 대한 성능 및 오류 검출 효과 분석	김경환, 강정환, 권동현(부산대학교)
42	우수	학회우수논문상 (학부생)	420	퍼징 기반 실행 경로 확장을 활용한 동적 SBOM 기반 취약점 탐지 기법	경서연, 정예림, 이일구(성신여자대학교)
43	우수	학회우수논문상 (학부생)	339	제로트러스트 성숙도 평가의 난점과 진단모델 설계 방향: 전문가 인터뷰를 중심으로	서진우, 서정우, 공나영, 송민희, 박기웅 (세종대학교)
44	우수	학회우수논문상 (학부생)	253	CycloneDX 1.7 업데이트 분석	정문경, 오재원, 김지민, 이만희 (한남대학교)
45	우수	학회우수논문상 (학부생)	129	macOS 환경에서의 취약한 바이너리를 통한 Dylib Hijacking 방법	박화비, 위다빈, 박명서(한성대학교)
46	우수	학회우수논문상 (학부생)	146	QED-Lite: 라이브러리 버전 핑거프린팅 기반 경량 양자 취약 ELF 바이너리 탐지	김하경, 이승원, 방지원, 김의재, 강희주, 김민서, 서화정(한성대학교)
47	우수	학회우수논문상 (학부생)	151	PromptLock의 내부 구조 분석: LLM 기반 랜섬웨어 오케스트레이터의 코드를 중심으로	서효리, 문규찬, 박주현, 이준우, 이윤수, 석병진(한성대학교)
48	우수	차세대 우수 여성과학자	242	ISMS-P 인증제도 실효성 강화 방안 - 현장조사 중심 전환과 인증취소 기준을 중심으로	강민서, 차유진, 홍준호(성신여자대학교)
49	우수	차세대 우수 여성과학자	368	2라운드 양자내성 비대칭형 PAKE 프로토콜	황리교, 손예원, 배수하, 구자민, 백채원, 황정연(성신여자대학교)
50	우수	차세대 우수 여성과학자	146	QED-Lite: 라이브러리 버전 핑거프린팅 기반 경량 양자 취약 ELF 바이너리 탐지	김하경, 이승원, 방지원, 김의재, 강희주, 김민서, 서화정(한성대학교)

5월 7일(목)

시간/장소	5A홀	구두트랙1 (321호)	구두트랙2 (322호)	구두트랙3 (323호)	구두트랙4 (324호)	구두트랙5 (325호)	구두트랙6 (326호)	구두트랙7 (121호)	구두트랙8 (122호)
09:00-10:00		참가자 등록 장소: 제2전시관 5A홀 앞 (3F) 등록대							
10:00-11:30		1A. 정보보호 정책/법/제도 I 좌장: 김동우 (동국대)	1B. 인공지능 보안 I 좌장: 손준영 (부산대)	1C. 융합보안 I 좌장: 이대성 (한국해양대)	1D. 금융보안 / 정보보호 일반 I 좌장: 최윤호 (부산대)	1E. 소프트웨어 보안 좌장: 권동현 (부산대)	1F. 디지털 포렌식 좌장: 김도현 (한국해양대)	1G. 해킹과 취약점 분석 I 좌장: 김기윤 (부경대)	1H. 여성과학자 I 좌장: 유지현 (광운대)
11:30-13:00		중식							
13:00-14:00	No Session	2A. 정보보호 정책/법/제도 II 좌장: 홍준호 (성신여대)	2B. 인공지능 보안 II 좌장: 이현우 (한국에너지공대)	2C. 융합보안 II 좌장: 박정수 (강남대)	2D. 암호이론 및 구현 I 좌장: 김수현 (순천향대)	2E. 양자내성암호 I 좌장: 서화정 (한성대)	2F. 네트워크/클라우드 보안 I 좌장: 주경호 (송실대)	2G. 해킹과 취약점 분석 II 좌장: 박명서 (한성대)	2H. 여성과학자 II 좌장: 조해현 (송실대)
14:00-14:10		휴식							
14:10-15:40		3A. IoT/CPS 보안 I 좌장: 윤주범 (세종대)	3B. 인공지능 보안 III 좌장: 류권상 (공주대)	3C. 융합보안 III 좌장: 이일구 (성신여대)	3D. 암호이론 및 구현 II 좌장: 구본욱 (국가보안기술 연구소)	3E. 양자 내성암호 II 좌장: 이석준 (가천대)	3F. 네트워크/클라우드 보안 II 좌장: 김지윤 (경상국립대)	3G. 해킹과 취약점 분석 III / KISA 동남정보보호 지원센터 좌장: 최현우 (성신여대)	3H. 여성과학자 III 좌장: 이윤경 (ETRI)
15:40-15:50		휴식							
15:50-16:20		초청강연 / 장소: 제2전시관 5A홀 (3F) 주제: 사이버 보안의 오늘과 내일 / 연사: 김창오 PM (정보통신기획평가원) / 좌장: 신상욱 (부경대)							
16:20-16:50		신진연구자 소개 / 장소: 제2 전시관 5A홀 (3F) 신지호 (목원대학교), 김기윤 (부경대학교), 박태준 (전남대학교), 김원빈 (상명대학교) / 좌장: 박정수 (강남대)							
16:50-17:30		개회식 및 (최)우수논문 시상식 / 장소: 제2 전시관 5A홀 (3F) 사회: 서정택 (가천대)							
16:50-17:30		<ul style="list-style-type: none"> <li>• 내빈 소개</li> <li>• 개회사: 김호원 회장 (한국정보보호학회)</li> <li>• 축 사: 이상중 원장 (한국인터넷진흥원) 이원태 위원장 (국가인공지능전략위원회)</li> <li>• 프로그램위원회 행사 보고: 이덕규 (서원대), 박승현 (한성대)</li> <li>• 운영위원회 보고 및 후원기관 소개: 김창훈 (대구대)</li> <li>• (최)우수논문 시상식</li> <li>• 경품 추첨</li> </ul>							
18:00~		참가자 만찬 / 일반: 제1전시관 (2F) 214-217호, 학생: 제2 전시관 5A홀 (3F)							

5월 8일(금)

시간/장소	포스터 트랙 (5A홀)	구두트랙1 (321호)	구두트랙2 (322호)	구두트랙3 (323호)	구두트랙4 (324호)	구두트랙5 (325호)	구두트랙6 (326호)	구두트랙7 (121호)	구두트랙8 (122호)	구두트랙9 (123호)	구두트랙10 (124호)	구두트랙11 (125호)	구두트랙12 (126호)
09:00-10:10	P1. 포스터 I 좌장: 이윤호(서울과기대) 강경민(고려대) 석병진(한성대)	4A. IoT/CPS 보안 II 좌장: 한성화 (동명대)	4B. 인공지능 보안 IV 좌장: 이태진 (가천대)	4C. 인공지능 보안 V 좌장: 김기윤 (부경대)	4D. 암호이론 및 구현 III 좌장: 서석중 (국민대)	4E. 산업보안/우주보안 I 좌장: 최대선 (송실대)	4F. 네트워크/클라우드 보안 III 좌장: 박기웅 (세종대)	4G. 하드웨어 보안 I 좌장: 최필주 (부경대)	4H. 모바일 보안 좌장: 김득훈 (아주대)	4I. 개인정보 보호/데이터 보안 좌장: 이세영 (강원대)	4J. 공공망 보안 I 좌장: 한동국 (국민대)	4K. 시스템 보안 I 좌장: 김희석 (고려대)	4L. 정보보호 일반 II 좌장: 박명서 (한성대)
10:10-10:40		휴식											
10:40-11:50	P2. 포스터 II 좌장: 이윤호(서울과기대) 이세영(강원대) 김영수(고려대)	5A. IoT/CPS 보안 III 좌장: 주경호 (송실대)	5B. 인공지능 보안 VI 좌장: 윤주범 (세종대)	5C. 인공지능 보안 VII 좌장: 윤종희 (영남대)	5D. 암호이론 및 구현 IV 좌장: 서승현 (한양대)	5E. 산업보안/우주보안 II 좌장: 이민우 (한국해양대)	5F. 네트워크/클라우드 보안 IV 좌장: 박기웅 (세종대)	5G. 하드웨어 보안 II 좌장: 서석중 (국민대)	5H. 정보보호 표준/평가/인증/교육 좌장: 김현일 (조선대)	5I. 인증/ID관리 및 콘텐츠/저작권 보안 좌장: 노시완 (동의대)	5J. 공공망 보안 II 좌장: 이만희 (한남대)	5K. 시스템 보안 II 좌장: 권동현 (부산대)	5L. 블록체인/암호화폐/메타버스 보안 좌장: 이동재 (강원대)
11:50-14:00		중식											

2026년 5월 7일(목)

세션명	순서	논문번호	제목 (저자/소속)
10:00~11:30 1A. 정보보호 정책/법/제도 I 좌장: 김동우 (동국대)	1A-1	441	CDS 기반 데이터 송수신 핵심 기능 도출 및 N2SF 보안통제 항목·보안 기술 통합 연구 전성현, 최동준, 서정택 (가천대학교)
	1A-2	39	보안 준수 심리의 동적 궤적: 피로 누적과 행동 관성의 상호작용 채은새, 김태성 (충북대학교)
	1A-3	59	N2SF 환경 정보유출 방지 기술 분석 신재현, 정우성, 김진하, 윤주범 (세종대학교)
	1A-4	126	사이버 침해사고 대응 강화를 위한 법제도 개선방안 연구 - 디지털 진정성(Digital Authenticity) 관점과 AHP 분석을 중심으로 - 김대원, 이상준 (전남대학교)
	1A-5	137	국가 망 보안 환경의 CDS를 위한 온톨로지 기반 콘텐츠 검사 아키텍처 신인준, 김창훈 (대구대학교)
	1A-6	355	해외사업자 국내대리인 제도의 실효성 검토와 개선방안 이기성, 양대현 (전남대학교), 정진우 (한국인터넷진흥원), 김수형 (전남대학교)
10:00~11:30 1B. 인공지능 보안 I 좌장: 손준영 (부산대)	1B-1	32	학습 도메인 구성에 따른 AI 생성 이미지 탐지 일반화 성능 분석 강현성, 윤태준, 이재웅, 류권상 (공주대학교)
	1B-2	279	자동화된 Agentic AI 보안 취약성 및 방어수준 진단 김현서, 정연수, 한태현, 이태진 (가천대학교)
	1B-3	115	ECDF 기반 공통 위험축을 활용한 데이터 오염 및 편향 신호 통합 평가 프레임 워크 이진우, 최대선 (숭실대학교)
	1B-4	81	코드가 현실이 될 때: LLM 기반 로봇 제어 코드의 안전성 위험 분석 및 대응 가능성 연구 채상준, 김형식 (성균관대학교)
	1B-5	360	설명 가능한 딥페이크 탐지를 위한 멀티모달 모델 동향 분석 이윤서, 황은비, 권태경 (연세대학교)
	1B-6	292	대규모 언어모델의 보안 위험 및 대응 기법 동향: Prompt Injection과 Jailbreak 공격 중심 박민재, 황시준, 이연준 (한양대학교)
10:00~11:30 1C. 융합보안 I 좌장: 이대성 (한국해양대)	1C-1	271	Zonal Architecture 기반 차량 네트워크를 위한 계층적 보안 구조 설계 강민재, 오현영 (가천대학교)
	1C-2	428	LiDAR 적대적 공격의 실제 위험도 평가 지표 김슬기, 백진현, 최원석 (고려대학교)
	1C-3	454	자율운행선박 충돌회피 시스템의 COLREGs 준수 과정에 대한 STRIDE-DREAD 기반 사이버 위협 평가 차은혁, 이민우 (한국해양대학교)
	1C-4	21	CAN 프로토콜에서 운동 기반 침입 탐지 시스템의 한계 분석 김이설, 사공상욱 (계명대학교)
	1C-5	55	Fuzzy Extractor 적용을 위한 딥러닝 기반 지문 벡터추출 박성준, 박종환 (상명대학교)
	1C-6	121	다중센서 불일치 공격에 대한 대응 기술 동향 정중환, 박영주, 이경민, 손준영 (부산대학교)

## 2026년 5월 7일(목)

세션명	순서	논문번호	제목 (저자/소속)
10:00~11:30 1D. 금융보안 / 정보보호 일반 좌장: 최윤호 (부산대)	1D-1	9	금융보안 관점에서의 양자내성암호 전환 로드맵과 이행 전략에 관한 고찰 이수왕, 김지윤 (경상국립대학교)
	1D-2	233	금융권 망분리 환경에서 AI 모델 개발 및 활용에 관한 연구 임시은, 강형우 (고려대학교)
	1D-3	350	PBM 래퍼 보안: 프로그래머블 머니의 보안 위협 및 대응 방안 이강호, 이승준 (IBK기업은행), 김경백 (전남대학교)
	1D-4	125	유출 경로별 선행지표 비교를 통한 내부자 정보 유출 징후 분석 : CERT r5.2 시나리오를 중심으로 이동우, 홍기완, 김혜원, 김지민, 조윤철, 장항배 (중앙대학교)
	1D-5	423	개인정보 보호 기록 연계를 위한 최소 통합 평가 프레임워크 이민호, 김호승 (한림대학교)
10:00~11:30 1E. 소프트웨어 보안 좌장: 권동현 (부산대)	1E-1	151	PromptLock의 내부 구조 분석: LLM 기반 랜섬웨어 오케스트레이터의 코드를 중심으로 서효리, 문규찬, 박주현, 이준우, 이윤수, 석병진 (한성대학교)
	1E-2	253	CycloneDX 1.7 업데이트 분석 정문경, 오재원, 김지민, 이만희 (한남대학교)
	1E-3	119	제어 흐름 그래프를 통한 난독화 기법 구분 김영대, 이동훈, 최원석 (고려대학교)
	1E-4	199	SSD Firmware 난독화 기술 동향 정가빈, 최원석 (고려대학교)
	1E-5	410	C-to-Rust 변환 시 발생하는 원시 포인터 문제와 해결 방안 연구 동향 김동현, 안승민, 김예진, 권다운, 김예찬, 김동찬 (국민대학교)
	1E-6	413	주요 C-to-Rust 자동 변환 도구 특성 분석 안승민, 김동현, 김예진, 권다운, 김예찬, 김동찬 (국민대학교)
10:00~11:30 1F. 디지털 포렌식 좌장: 김도현 (한국해양대)	1F-1	134	Selective Symbolic Execution 기반 프레임워크를 이용한 RAT C2 통신 분석 유현준, 유지현 (광운대학교)
	1F-2	334	클라우드 스토리지 내부 API 트래픽 분석을 통한파일 활동 로그 식별 연구 전나현, 윤우성, 최근영, 박정흠 (고려대학교)
	1F-3	122	macOS 환경에서의 카카오톡 데이터베이스 복호화 김대환, 안원석, 박명서 (한성대학교)
	1F-4	210	OTT 불법유통 대응을 위한 디지털 수집증거의 무결성 보존 및 검증 방법 장세영, 유인재, 박병찬, 김석윤, 김영모 (숭실대학교)
	1F-5	367	에이전트 보안성 평가 및 디지털 포렌식 아티팩트 수집을 위한 테스트베드 프레임워크 이라경, 조원빈, 송현민 (단국대학교)
	1F-6	72	침해사고 조사를 위한 House of Tangerine 힙 공격 아티팩트 정형화 연구 조은혜, 유동운, 최윤호 (부산대학교)

2026년 5월 7일(목)

세션명	순서	논문번호	제목 (저자/소속)
10:00~11:30 1G. 해킹과 취약점 분석 I 좌장: 김기윤 (부경대)	1G-1	7	UnionSanitizer: Tagged Union Type Confusion 취약점 탐지를 위한 정적-동적 하이브리드 분석 도구 이동준, 윤인수 (한국과학기술원)
	1G-2	366	Explainable AI를 활용한 사용자-커널 데이터 기반 악성코드 탐지 기술 연구 홍영우 (코어시큐리티)
	1G-3	465	AES 소비 전력 파형 구조 분해: 자기유사도기반 방법 제안과 LLM의 분해 분석 김현준 (난양이공대학교), 김현지, 심민주, 서화정 (한성대학교)
	1G-4	189	멀티모달 모델 적대적 공격에 대한 토큰 수준 영향도 분석 김용재, 이연준 (한양대학교)
	1G-5	28	딥페이크 탐지 기술의 주요 동향 및 한계 분석 장규영, 김동인, 박명서 (한성대학교)
	1G-6	456	피싱 웹사이트 인프라의 사용자 정보 제출 이후 동적 특성 분석 김예림, 김형식 (성균관대학교)
10:00~11:30 1H. 여성 과학자 I 좌장: 유지현 (광운대)	1H-1	242	ISMS-P 인증제도 실효성 강화 방안 - 현장조사 중심 전환과 인증취소 기준을 중심으로 강민서, 차유진, 홍준호 (성신여자대학교)
	1H-2	345	제로트러스트 기반 RAG 보안 위협 대응 방안 박지민, 목정현, 윤성우, 박소영, 이석준 (가천대학교)
	1H-3	145	AI 기반 KCMVP 사전 검증 시스템: 규칙 탐지와 LLM 의미론적 분석의 하이브리드 모델 조수빈, 박도윤, 임다은, 김재환, 정수민, 형유림, 서화정 (한성대학교)
	1H-4	65	Agentic AI에서의 보안 위협 및 대응 방안 신수진, 신상욱 (부경대학교)
	1H-5	71	CLIP 기반 감시 영상 이상 탐지에서의 다국어 성능 격차 분석 송다은, 김형식 (성균관대학교)
	1H-6	110	SMT: SBOM과 Merkle Tree를 이용한 서비스 환경의 무결성 검증 프레임워크 이지연, 경승기, 김원빈, 서대희 (상명대학교)
13:00~14:00 2A. 정보보호 정책/법/제도 II 좌장: 홍준호 (성신여대)	2A-1	356	국방 AX 추진에 따른 보안 거버넌스 공백과 제도적 대응 방안 안상현, 서정택 (가천대학교)
	2A-2	205	해양 및 선박 보안 위협에서의 사이버보안 대응 방안 제안 김남정 (가천대학교), 김유래 (연세대학교), 서정택 (가천대학교)
	2A-3	227	상당 음성 기반 프로파일 화자 분리 및 발화 재구성 연구 최종윤, 신민석, 김대환, 김한결, 박명서 (한성대학교)
	2A-4	209	플랫폼 기업의 제3자 광고 SDK를 통한 행태정보 수집 구조 분석 및 프라이버시 위협 연구 최진경, 이기성 (전남대학교), 차유훈 (한국인터넷진흥원), 이상준 (전남대학교)

## 2026년 5월 7일(목)

세션명	순서	논문번호	제목 (저자/소속)
13:00~14:00 2B. 인공지능 보안 II 좌장: 이현우 (한국에너지공대)	2B-1	116	Agentic AI 보안 취약점 대응을 위한 Zero Trust 기반 아키텍처 설계 이여민, 이용재, 박정수 (강남대학교)
	2B-2	359	단어 치환 응답을 활용한 LLM 기반 탈옥평가 체계의 한계점 분석 선민준, 권태경 (연세대학교)
	2B-3	153	지식 그래프 기반 시각 표현 보정을 통한 LVLM 복원 연구 김규영, 나현식, 최대선 (숭실대학교)
	2B-4	237	Prefix Tuning 기반 출력 행동 LLM 핑거프린팅 기법을 이용한 무결성 검증 유경빈, 김형식 (성균관대학교)
13:00~14:00 2C. 융합 보안 II 좌장: 박정수 (강남대)	2C-1	412	자율주행 시스템을 위한 NDT 기반 실시간 LiDAR 공격 탐지 방법 최지훈, 최원석 (고려대학교)
	2C-2	262	차량 OTA 업데이트 결과의 검증 가능성 향상을 위한 선택적 원격 증명 구조 경보희, 오현영 (가천대학교)
	2C-3	443	색상 스트라이프 아티팩트 완화를 이용한 비전 센서 대상 레이저 기반 적대적 공격 방어 기법 조시은, 심상훈, 백진현, 최원석 (고려대학교)
	2C-4	466	RSSI-거리 및 다중 노드 교차검증 기반 AIS 이상 반응 분석 장윤서, 양건우, 김기현, 차은혁, 이민우 (한국해양대학교)
13:00~14:00 2D. 암호이론 및 구현 I 좌장: 김수현 (순천향대)	2D-1	161	S-RMSNorm: Transformer의 보안 추론 가속화를 위한 정규화 연산의 상수화 기법 한상훈, 신호준, 이윤호 (서울과학기술대학교)
	2D-2	293	Cortex-M3 환경에서 블록 암호 HIGHT 최적 구현 및 CTR_DRBG 적용 김채린, 김영법, 서석충 (국민대학교)
	2D-3	295	AVX2와 GFNI 명령어를 활용한 HQC의 리드-솔로몬 디코딩 최적화 구현 장지훈, 박현주, 김제빈 (고려대학교), 김수리 (성신여자대학교), 홍석희 (스마트 엠투엠)
	2D-4	383	Sparse Meta-BTS: 희소 패키징된 암호문에 대한 재부팅 문정훈, 김동우 (동국대학교)
13:00~14:00 2E. 양자내성 암호 I 좌장: 서화정 (한성대)	2E-1	341	MQTT 기반 IoT 환경에서 PQ-KEM 키 교환 알고리즘 성능 평가 윤성우, 목정현, 박지민, 박소영, 이석준 (가천대학교)
	2E-2	462	X.509 PQC 전환을 위한 하이브리드 서명 전략 비교 분석 이민우, 심민주, 조수빈, 형유림, 서화정 (한성대학교)
	2E-3	148	PQC 서명 크기가 B+tree 구조에 미치는 구조적 병목 분석 및 저장 전략 이승원, 김의재, 강희주, 김민서, 김하경, 방지원, 서화정 (한성대학교)
	2E-4	328	KpqC 전자서명 알고리즘 HAETA에 대한 NTT 정형 검증 연구 지용현, 서석충 (국민대학교)

2026년 5월 7일(목)

세션명	순서	논문번호	제목 (저자/소속)
13:00~14:00 2F. 네트워크/ 클라우드 보안 I  좌장: 주경호 (숭실대)	2F-1	63	클라우드 스토리지 공유 URL의 비동기 접근에 관한 보안성 연구 문지윤, 장대희 (경희대학교)
	2F-2	265	네트워크 행위 이력기반 사이버위협 위험도 분석 방안 연구 김세욱, 김태용 (가천대학교, 한국과학기술정보연구원), 송중석 (한국과학기술정보연구원), 서정택 (가천대학교)
	2F-3	1	한국 소재 C2 인프라의 프레임워크 전환 특성 및 호스팅 생태계 분석 남경현, 류재철 (충남대학교)
	2F-4	2	차세대 VPP 인프라를 위한 LLM 기반 제로트러스트 성숙도 평가 자동화 및 동적 사용자 신뢰 제어 모델에 대한 연구 송현석, 박택근 (한전KDN), 엄익채 (전남대학교)
13:00~14:00 2G. 해킹과 취약점 분석 II  좌장: 박명서 (한성대)	2G-1	129	macOS 환경에서의 취약한 바이너리를 통한 Dylib Hijacking 방법 박화비, 위다빈, 박명서 (한성대학교)
	2G-2	25	S-100 차세대 전자해도 참조구현체의 임의 코드 실행 및 서비스 거부 취약점 분석 조호연, 이창의, 이서정 (한국해양대학교)
	2G-3	373	CodeQL 기반 Python-C/C++ 확장 패키지 cross-language 취약점 탐지 프레임워크 지전일, 양희지, 조금환 (고려대학교)
	2G-4	74	오픈소스 방화벽 pfSense XSS 취약점 분석 및 위협 완화에 관한 연구 김형태, 장대희 (경희대학교)
13:00~14:00 2H. 여성 과학자 II  좌장: 조해현 (숭실대)	2H-1	368	2라운드 양자내성 비대칭형 PAKE 프로토콜 황리교, 손예원, 배수하, 구자민, 백채원, 황정연 (성신여자대학교)
	2H-2	340	Introspection 비활성화 상태의 GraphQL 대상 블랙박스 기반 스키마 복원을 통한 퍼징 기법 제안 박미리, 지일환, 서정택 (가천대학교)
	2H-3	259	Cortex-M4 상에서의 하이브리드 KEM/DSA 성능 비교 심민주, 이민우, 조수빈, 형유림, 서화정 (한성대학교)
	2H-4	141	L2Sec 프로토콜의 XMSS 기반 양자 내성 서명 체계 전환 및 성능 분석 윤현지, 김수현 (순천향대학교)

## 2026년 5월 7일(목)

세션명	순서	논문번호	제목 (저자/소속)
14:10~15:40 3A. IoT/CPS 보안 I  좌장: 윤주범 (세종대)	3A-1	238	IoT 침입 탐지 시스템의 강건성 향상을 위한 GAN 기반 적대적 공격 생성-학습 프레임워크 최태준 (한국에너지공과대학교), Segun Popoola (Anglia Ruskin University), 이현우 (한국에너지공과대학교)
	3A-2	112	교통안전시설 통합관리체계(ROADEE-IMS) 표준화를 위한 제로트러스트·N2SF·SW 공급망 보안 참조 프레임워크 고정호 (한국도로교통공단), 서정택 (가천대학교)
	3A-3	90	IoT 엣지 디바이스를 위한 TFLite 모델 파일정적 보안 분석 시스템 개발 김수윤 (동명대학교)
	3A-4	105	IIoT 환경을 위한 소프트웨어 정의 경계 기반 경량 텔레메트리 운용 방안 연구 임채민, 엄익채 (전남대학교)
	3A-5	223	ICS 사이버보안 공개 데이터셋의 시스템 특성 및 탐지 난이도 비교분석 오승렬, 손광섭 (한국원자력연구원)
	3A-6	232	차세대 전력망 적용 AI 기반 이상행위 탐지 기술의 신뢰도 향상을 위한 데이터 수집 및 분석 방법론 연구 김민용, 장승진, 박택근 (한전KDN)
14:10~15:40 3B. 인공지능 보안 III  좌장: 류권상 (공주대)	3B-1	80	인간과 AI의 시각적 인지 차이를 활용한 적대적 피싱 로고 생성 기법 조예나, 정희성, 방수경 (성균관대학교), 김두원 (테네시대학교), 김형식 (성균관대학교)
	3B-2	403	에이전틱 AI 환경에서의 데이터 과다 수집 위협 분석 김준식, 고남현, 김도영, 박준영, 윤주범 (세종대학교)
	3B-3	289	이미지 생성 모델의 개념 억제 연구 동향과 향후 연구 방향: 제어 장벽 함수를 중심으로 이상준, 나현식, 최대선 (숭실대학교)
	3B-4	319	핵심 특징을 기억하는 기만적 언러닝 기법 박선혜, 김형식 (성균관대학교)
	3B-5	361	화질 저하가 딥페이크 탐지 성능에 미치는 영향: Gaussian Blur를 중심으로 강지원, 황은비, 권태경 (연세대학교)
	3B-6	254	대규모 언어 모델 기반 단일 에이전트 및 다중 에이전트 시스템의 보안 양상 비교 연구 송진우, 이연준 (한양대학교)

2026년 5월 7일(목)

세션명	순서	논문번호	제목 (저자/소속)
14:10~15:40 3C. 융합 보안 III 좌장: 이일구 (성신여대)	3C-1	30	NIST CSF 2.0 기반 전기차 충전 인프라 보안 표준 정량적 갭 분석 김태우, 레리사 아데바 질차, 콕진 (아주대학교)
	3C-2	165	군집 드론 제어의 성능-부하-품질 트레이드오프 분석 노승덕, 박소희, 최대선 (숭실대학교)
	3C-3	273	자율주행 군집의 BLS 임계 서명에서 유출 share의 결정론적 추적 기법 조상우, 김영식 (대구경북과학기술원)
	3C-4	89	자율주행 객체 검출-추적 파이프라인의 지연 유발 공격에 대한 방어 기법 김진성, 유준수 (전북대학교)
	3C-5	398	Evaluation of eBPF-Based Kernel-Level Data Collection for Controller Area Network Intrusion Detection Systems 아마다 유스릴 카딧티야, 안드로 아프릴라 아디푸트라, 김호원 (부산대학교)
	3C-6	150	Quantifying AI-Driven Risk in V2G Authentication Protocols Using AI-Amplification Factor 가드가 나무라타, 레리사 아데바 질차, 콕진 (아주대학교)
14:10~15:40 3D. 암호이론 및 구현 II 좌장: 구본욱 (국가보안기술 연구소)	3D-1	306	부분합 기법과 FFT를 이용한 7-라운드 Kiasu-BC에 대한 향상된 Square 공격 송원우, 김남일, 백승준, 김종성 (국민대학교)
	3D-2	393	RSA 및 ECC를 위한 통합 하드웨어 가속기 설계 이상원, 정운혁, 최필주 (부경대학교)
	3D-3	5	누적 부채널 누설을 방지하기 위한 전체 디스크 암호화의 Epoch 기반 키 재설정 강동우, 김희석 (고려대학교), 홍석희 (스마트 엠투엠)
	3D-4	41	MAC 기반 Zero-Touch 공개키 분배시스템 유승환, 박종환 (상명대학교)
	3D-5	330	NTRU+를 위한 다항식 곱셈 하드웨어 아키텍처 연구 신동현, 이재석, 김영범, 서석충 (국민대학교)
	3D-6	75	HAETAE 부채널 분석 대응을 위한 보호 대상 식별 안현준, 한동국 (국민대학교)
14:10~15:40 3E. 양자내성 암호 II 좌장: 이석준 (가천대)	3E-1	146	QED-Lite: 라이브러리 버전 핑거프린팅 기반 경량 양자 취약 ELF 바이너리 탐지 김하경, 이승원, 방지원, 김의재, 강희주, 김민서, 서화정 (한성대학교)
	3E-2	329	16-bit MSP430 환경에서의 양자내성암호 HAETAE FFT/NTT 최적화 연구 김민기, 신동현, 서석충 (국민대학교)
	3E-3	348	대규모 언어 모델을 사용한 양자 암호 분석 연구 장경배 (난양이공대학교), 김현지, 이승원, 서화정 (한성대학교)
	3E-4	387	PQC 격자 기반 암호의 부채널 공격 동향을 통한 CKKS 복호화 단계의 공격 가능성 분석 김도용, 한동국 (국민대학교)
	3E-5	217	IoT 환경에서 비격자 기반 양자내성암호의 적용 제약과 최적화 동향 김동찬, 윤혜진, 장찬국, 이옥연 (국민대학교)
	3E-6	285	경량형 격자 기반 양자내성암호 가속기의 설계 및 검증 정운혁, 이상원, 최필주 (부경대학교)

## 2026년 5월 7일(목)

세션명	순서	논문번호	제목 (저자/소속)
14:10~15:40 3F. 네트워크/ 클라우드 보안 II  좌장: 김지윤 (경상국립대)	3F-1	73	중앙 정책 기반 암호 민첩성 서버의 정책 집행 설계 옵션과 보안성 분석 양희재, 김다운, 손수경, 김성민 (성신여자대학교)
	3F-2	13	차세대 이동통신 O-RAN 환경에서 F1AP Reset 메시지 삽입 공격 분석 및 탐지 기법 연구 박성민, 김대운 (한국인터넷진흥원, 김지윤 (경상국립대학교))
	3F-3	56	이미지 변환 기반 네트워크 침입탐지시스템 동향 차승연, 유진호, 조효진 (연세대학교)
	3F-4	66	대규모 환경에서의 Tor 트래픽 상관 분석을 위한 근사 최근접 이웃 탐색 기반 기법 홍세연, 김혜원 (이화여자대학교), Saidur Rahman Mohammad (University of Texas at El Paso), 오세은 (이화여자대학교)
	3F-5	124	ARES: 서버리스 환경에서의 에이전틱 AI 기반 실시간 권한 우회 방지 시스템 신창희, 이승수 (인천대학교)
	3F-6	378	클라우드 환경에서의 컨테이너 기반 KCMVP 암호모듈 라이브러리 자동 배포 프레임워크 설계 및 분석 김수현, 김민용, 박택근 (한전KDN)
14:10~15:40  3G. 해킹과 취약점 분석 III / KISA 동남정보보호 지원센터  좌장: 최현우 (성신여대)	3G-1	198	강화학습 기반 사이버 공방 환경 일반화 방법 분석 김범석, 구기종, 최양서, 유재학, 문대성 (한국전자통신연구원)
	3G-2	344	LLVM instrumentation을 활용한 WinAFL 오픈소스 커버리지 계속 기법 제안 고동의, 지일환, 서정택 (가천대학교)
	3G-3	298	Scoped Policy Enforcement for Autonomous Pentesting Agents: Balancing Offensive Capability with Operational Constraint 물야사리 울란 실바니, 레티투호영, 김호원 (부산대학교)
	3G-4	310	증거 기반 ReAct 에이전트를 활용한 윈도우 바이너리 취약점 자동 식별 및 재현 김재민, 박민제, 최준영 (스틸리언)
14:10~15:40  3H. 여성 과학자 III  좌장: 이윤경 (ETRI)	3H-1	452	클라우드 보안사고 조사를 위한 통합 클라우드 포렌식 도구의 필요성 조한나, 최상훈, 박기웅 (세종대학교)
	3H-2	36	SHAP 기반 Feature Importance을 이용한 IDS Feature Reduction과 탐지 성능 영향 분석 우나륜, 유지현 (광운대학교)
	3H-3	270	타원곡선 암호(ECDLP)에 대한 양자 해킹 동향 송경주, 서화정 (한성대학교)
	3H-4	179	VRBench: 순위 학습 알고리즘의 취약점 위험도 예측 성능 평가 프레임워크 한슬기, 박서현, 이현우 (한국에너지공과대학교)
	3H-5	305	Android 환경에서 VPN 애플리케이션 아티팩트 분석 연구 조윤영, 김강한, 박세준, 김종성 (국민대학교)
	3H-6	450	클라우드 포렌식 관점의 통합된 로그 분석 체계의 필요성 이지원, 최상훈, 박기웅 (세종대학교)

2026년 5월 8일(금)

세션명	순서	논문번호	제목 (저자/소속)
09:00~10:30 4A. IoT/CPS 보안 II  좌장: 한성화 (동명대)	4A-1	201	블라인드 부채널 분석을 위한 분석 지점 탐색 기법 연구 이인훈, 김규상 (고려대학교), 홍석희 (스마트 엠투엠), 김희석 (고려대학교)
	4A-2	109	대규모 언어 모델 기반 전기차 충전 시스템 위협 분석 및 위험 평가 자동화 프레임워크 하재준, 엄익채 (전남대학교)
	4A-3	458	HRP UWB 거리 측정 시스템 보안 연구 동향 김지민, 김주언, 최원석 (고려대학교)
	4A-4	106	개방형 충전 프로토콜 기반 충전 관리 시스템의 디지털 포렌식 준비도 평가 신동혁, 엄익채 (전남대학교)
	4A-5	246	임베디드 기기 대상 커맨드 인젝션 퍼징 기법 동향 분석 김종인, 이우진, 김도현 (한국해양대학교)
	4A-6	258	드론 시스템의 다계층 통합 분석 방법 : XK Alien X250를 사례로 박찬진, 정수은, 박정흠 (고려대학교)
09:00~10:30 4B. 인공지능 보안 IV  좌장: 이태진 (가천대)	4B-1	117	Activation Steering 기반 탈옥 공격을 통한 국내 개발 LLM의 안전 정렬 취약성 분석 최민영, 문찬빈, 김승한, 임창훈, 김현일 (조선대학교)
	4B-2	188	LLM 에이전트에서의 간접 프롬프트 인젝션 공격 및 방어 기법에 대한 체계적 분류 김승근, 이연준 (한양대학교)
	4B-3	430	산업제어시스템 적용 적응형 이상탐지 모델 대상 재학습 데이터 포이즈닝 공격 기법 제안 서정규, 지일환, 서정택 (가천대학교)
	4B-4	425	CNN 기반 이미지 악성코드 분류에서 Grad-CAM 및 Fusion-CAM을 활용한 비교 분석 김혁진, 이동재 (강원대학교)
	4B-5	457	Blue Team Teacher : Relational Knowledge Distillation for White Box Adversarial Defense 안드로 아프릴라 아디푸트라, 무함마드 나빌 파들루르라흐만, 레티투흐영, 김호원 (부산대학교)
	4B-6	449	멀티모달 적대적 워터마킹 기반 OTT 콘텐츠 저작권 보호 기법 연구 김지훈, 장의진, 신용태 (숭실대학교)
09:00~10:30 4C. 인공지능 보안 V  좌장: 김기윤 (부경대)	4C-1	168	공개 CVE 기반 AI/ML 프레임워크 취약점 공격 경로 분석 및 LLM 프롬프팅 기반 경량 버그헌팅 방법론 류석준, 박소희, 옥도민, 최대선 (숭실대학교)
	4C-2	445	실사례 분석을 통한 AI agent 안전성 점검 기준 및 요구사항 도출 최유진, 정연수, 이태진 (가천대학교)
	4C-3	54	SOC/DFIR 환경에서 LLM 환각 완화 기법 비교 연구 권석재, 이상윤, 이세영 (강원대학교)
	4C-4	8	폐쇄망 로컬 LLM 보안을 위한 심층방어 구조 연구 장성훈, 이명락, 손태식 (아주대학교)
	4C-5	27	VLA 모델에 대한 적대적 공격 연구 동향 김주은, 김형훈, 조효진 (연세대학교)
	4C-6	95	물리 환경 기반 적대적 공격 기법 동향: 공격 대상 도메인 변화를 중심으로 권태현, 손준영 (부산대학교)

## 2026년 5월 8일(금)

세션명	순서	논문번호	제목 (저자/소속)
09:00~10:30 4D. 암호이론 및 구현 III  좌장: 서석총 (국민대)	4D-1	313	GPU 환경에서 비트 슬라이스 여부에 따른 워드 단위 이진 곱셈에 대한 성능 비교 김동천, 서석총 (국민대학교)
	4D-2	284	A Survey on Privacy Preserving Inference on Large Language Model using Homomorphic Encryption 모티타 코이, 시티 사레하, 이윤호 (서울과학기술대학교)
	4D-3	409	NIST SP 800-227에서 명시한 키 캡슐화 메커니즘의 구현 지침과 운용 요구사항 김예진, 김동현, 김동찬 (국민대학교)
	4D-4	228	NIST Threshold Call 기반 다자간 임계 암호 동향 분석 엄시우, 송민호, 이승원, 김하경, 서화정 (한성대학교)
	4D-5	343	ARMv8 환경에서 PQC-DSA HAETAE 최적화 연구 최준혁, 지용현, 서석총 (국민대학교)
	4D-6	239	MQ 기반 서명에서 UOV와 MAYO의 Rank 분포 특성 비교 분석 이호영, 윤지원 (고려대학교)
09:00~10:30 4E. 산업보안/ 우주보안 I  좌장: 최대선 (송실대)	4E-1	276	원자력시설 사이버침해 사고 식별 및 탐지를 위한 시뮬레이션 기반 IOC지표 제안 최동준, 지일환, 서정택 (가천대학교)
	4E-2	60	위성 RF 해킹 연구를 위한 가상 위성 안테나 시스템 설계 및 구현 황선혁, 장대희 (경희대학교)
	4E-3	93	그래프 분석 및 대조학습을 활용한 수동적 스캐닝 기반 산업제어시스템 네트워크 토폴로지 추론 연구 김가경, 엄익채 (전남대학교)
	4E-4	142	저궤도 위성 텔레메트리 메타데이터 보호를 위한 형태보존암호 적용 및 오버헤드 임계값 분석 백승훈, 김수현 (순천향대학교)
	4E-5	190	GNSS 스푸핑이 항공-해운 인프라에 미치는 보안 영향 분석 조소연, 전형민, 이용준 (극동대학교)
	4E-6	263	원전 시계열 이상 감시 연구의 데이터 제약 대응 기술 동향 성도범, 손준영 (부산대학교)

2026년 5월 8일(금)

세션명	순서	논문번호	제목 (저자/소속)
09:00~10:30 4F. 네트워크/ 클라우드 보안 III 좌장: 박기웅 (세종대)	4F-1	215	FT-Transformer 기반 준지도학습을 활용한 암호화 트래픽 공격 분류 성능 분석 김태훈, 김환국 (국민대학교)
	4F-2	200	단말 노드 신뢰도 검증을 위한 2단계 인증 기반의 Reverse Offloading 최적화 방안 연구 박건우, 명재민, 이지언, 김원빈, 유진호, 서대희 (상명대학교)
	4F-3	206	OpenRAN 환경에서 악성 O-CU를 이용한 UE 정보 유출 공격 실증 및 대응 방안 김대운, 김진강, 나사랑, 박성민 (한국인터넷진흥원)
	4F-4	304	이종 보안 로그의 상호운용성 향상을 위한 로그 포맷 변환 시스템 최형규, 이새움, 최승기, 김태현, 김서연, 이도현, 임준형, 김태은 (한국인터넷진흥원)
	4F-5	363	Transformer기반 침입탐지 시스템 구현 권혁호, 염동민, 이덕규, 홍기훈 (서원대학교)
	4F-6	364	O-RAN E2 인터페이스 공격 시나리오 설계 및 재현 실험 이현지, 이수현, 김환국 (국민대학교)
09:00~10:30 4G. 하드웨어 보안 I 좌장: 최필주 (부경대)	4G-1	314	심층 신경망에서 조건적 공분산 축소를 적용한 오류 주입 탐지 기법 제안 안경덕, 김윤성, 하재철 (호서대학교)
	4G-2	53	오류 주입 대응기법 FISSC의 실증적 취약성 분석 김주환, 한동국 (국민대학교)
	4G-3	86	마할라노비스 거리 기반 특징 벡터 분포 분석을 활용한 제로데이 하드웨어 트로잔 탐지 정상윤, 박예은, 박태운, 김희석 (고려대학교)
	4G-4	374	LLM 기반 화이트박스 프로파일링을 이용한 암호화된 Matter 기기 부채널 분석 이규원, 박수진, 김희석 (고려대학교)
	4G-5	311	IoT 펌웨어 분석 통합 자동화 파이프라인 연구 조건영, 이주협 (스틸리언)
	4G-6	386	EMR 부채널 기반 은닉 전자기기 탐지 연구 동향 노관우, 최원석 (고려대학교)
09:00~10:30 4H. 모바일 보안 좌장: 김득훈 (아주대)	4H-1	82	Over-the-air 테스트를 통한 5G 단말 메모리 취약점 탐지 오범석, 김광민, 손민철 (한국과학기술원), 박철준 (경희대학교), 김용대 (한국과학기술원)
	4H-2	375	LLM 기반 UI 탐색과 동적 계측을 활용한 안드로이드 네이티브 코드 퍼징 강민주, 이동하, 한규상, 박정우, 배연주, 전승호 (가천대학교)
	4H-3	346	양자내성 보안을 위한 Isogeny 기반 허위 기지국 대응 기법 설계 및 안전성 검증 한윤선, 서석중 (국민대학교)
	4H-4	402	TikTok 비디오 트래픽에서의 Fingerprinting 가능성 한소현, Cristina Alarcon, 김수진, 김효진, Mohammad Saidur Rahman, 오세은 (이화여자대학교)
	4H-5	24	QR 코드 보안 위협과 대응기법 유형 분류 이수왕, 이승빈, 김지윤 (경상국립대학교)
	4H-6	136	대형 언어 모델을 이용한 이동통신 네트워크의 취약점 자동 생성 김광민, 오범석, 손민철, 오택경, 김용대 (한국과학기술원)

## 2026년 5월 8일(금)

세션명	순서	논문번호	제목 (저자/소속)
09:00~10:30 4I. 개인정보 보호/데이터 보안 좌장: 이세영 (강원대)	4I-1	98	안전한 스마트 그리드를 위한 함수 암호 기반 프라이버시 보장 데이터 집계에 관한 연구 김기환, 김수현, 이임영 (순천향대학교)
	4I-2	447	HERALD: 선택적 LLM 호출과 사용자 정의 기반 민감정보 자동 비식별화 파이프라인 강주현, 최은경, 오홍석, 신현서, 황원석 (서울시립대학교)
	4I-3	260	한국어 대화형 텍스트 내 개인정보 탐지를 위한 하이브리드 파이프라인 고도화 김수정 (가천대학교), 장대일 (한국인터넷진흥원), 이태진 (가천대학교)
	4I-4	251	개인정보 유출사건에서의 중대한 과실 판단기준 명확화 방안 연구 강하은, 홍준호 (성신여자대학교)
	4I-5	17	CSS-based Exfiltration for Cross-Origin Login-State Fingerprinting WITHOUT JavaScript Roby Yusuf, Abhishek Chaudhary, 최선오 (전북대학교)
	4I-6	399	병원 키오스크의 개인정보 노출 문제 분석과 보호정책 제안 방지수, 천예슬 (서울여자대학교)
09:00~10:30 4J. 공급망 보안 I 좌장: 한동국 (국민대)	4J-1	103	프로비언스 그래프의 시퀀스-그래프 교차 대조 학습 기반 APT 위협 탐지 프레임워크 윤성수, 엄익채 (전남대학교)
	4J-2	169	Python 패키지 관리 도구 이질성이 TPL 설치 결과 일관성에 미치는 영향 이정호, 이세영 (강원대학교)
	4J-3	76	Deep SVDD 기반 현실적인 하드웨어 트로이목마 탐지 김용재, 한동국 (국민대학교)
	4J-4	143	지식 증류 기반 백도어 전이 평가를 위한 BLADE 프레임워크 최영호, 김호영, 김영수, 최두호 (고려대학교)
	4J-5	196	네트워크 동적 맥락을 활용한 Enhanced VEX 프레임워크 연구 김태현, 임준형, 김서연, 최슬기, 이새움, 김태은 (한국인터넷진흥원)
	4J-6	426	산업제어시스템 공급망 보안을 위한 SBOM-HBOM 통합 관리 체계에 관한 연구 신용희, 고웅, 엄익채 (전남대학교)
09:00~10:30 4K. 시스템 보안 I 좌장: 김희석 (고려대)	4K-1	15	HWASan의 Short Granule 기법에 대한 성능 및 오류 검출 효과 분석 김경환, 강정환, 권동현 (부산대학교)
	4K-2	34	I/Q 스펙트로그램 기반 STFT/U-Net 실시간 RF 재밍신호 탐지 기법 연구 임주영 (가천대학교)
	4K-3	46	다중 시간 윈도우 기반의 내부자 위협 유형 분류 방법 연구 이광훈, 유동운, 최윤호 (부산대학교)
	4K-4	49	MCP 기반 LLM 에이전트 오케스트레이션을 이용한 펌웨어 취약점 분석 파이프라인 설계 김서울, 한승훈 (숭실대학교)
	4K-5	64	Multimodal Graph Learning for Early APT Detection: Quantifying the Gain of OSINT Enrichment Prita Firdani, 한미란, 강정민 (고려대학교)
	4K-6	101	MUM-T 체계 적용을 위한 MOSA 기반 UGS 보안 아키텍처 연구 김진국, 이행호, 유찬곤, 이화성, 최민관, 윤호상 (국방과학연구소)

2026년 5월 8일(금)

세션명	순서	논문번호	제목 (저자/소속)
09:00~10:30 4L. 정보보호 일반 II  좌장: 박명서 (한성대)	4L-1	204	대규모 최적화 문제 해결을 위한 그래프 분할 기반 양자 어닐링 접근법 배준영, 이동재 (강원대학교)
	4L-2	256	RAG 기반 보이스피싱 대화 스크립트 식별 연구 배근우 (가천대학교), 장대일 (한국인터넷진흥원), 이태진 (가천대학교)
	4L-3	369	오류 주입 기반 HAETAE 서명 검증 우회 공격 최기훈, 한동국 (국민대학교)
	4L-4	18	사이버보안 교육용 LLM의 안전한 활용을 위한 다계층 가드레일 및 시각화 방안 정상지, 박주선, 주한익, 홍순좌 (코어시큐리티)
	4L-5	214	동형암호 알고리즘 구현 적합성 검증 도구 개발 김태훈, 김준섭 (한국인터넷진흥원)
	4L-6	22	재학습 공격을 통한 소형 언어 모델(SLM)의 지식 소거 복원력 및 잔류성 분석 장민 (유엠로직스)
10:40~11:55 5A. IoT/CPS 보안 III  좌장: 주경호 (송실대)	5A-1	274	암호화 트래픽 대상 이상탐지를 위한 마스킹 기반 멀티모달 지식 종류 모델 제안 지일환, 이주현, 서정택 (가천대학교)
	5A-2	286	임베디드 시스템 대상 퍼징 기법의 분류 및 동향 분석 이우진, 김종인, 김도현 (한국해양대학교)
	5A-3	395	스마트홈 제어형 LLM 에이전트의 비인가 명령 실행 위험 평가를 위한 Mock IoT 기반 실험 프레임워크 하업준, 김무영, 김민규, 김호원 (부산대학교)
	5A-4	195	전송 계층 독립적 PQC 기반 UAV 보안 프레임워크 설계 김찬혁, 김형엽, 위한샘, 이옥연 (국민대학교)
	5A-5	288	LoRaWAN에서 Flash 메모리 덤프 기반 루트 키 탈취 및 메시지 복호 이광용, 기한결, 유승민, 하재철 (호서대학교)
10:40~11:55 5B. 인공지능 보안 VI  좌장: 윤주범 (세종대)	5B-1	224	Why Overthink It? Reducing Pentest Agent Complexity via Modular Skill Injection Anak Agung Ngurah Dharmawangsa, Thi Thu Huong Le, 장현진, 김민규, 김호원 (부산대학교)
	5B-2	432	침해공격 사례에 기반한 상용 AI Agent 취약성분석방안 연구 서유민, 정연수, 이태진 (가천대학교)
	5B-3	108	취약점 대응 고도화를 위한 거대 언어 모델 기반 보안 약점 연계 연구_양희석 양희석, 윤성수, 엄익채 (전남대학교)
	5B-4	123	한국어 기반 모델의 파라미터 효율적 미세조정 이후 안전 정렬 변화 분석 임창훈, 문찬빈, 김승한, 최민영, 김현일 (조선대학교)
	5B-5	159	에이전틱 시의 안전한 실행을 위한 로그 기반 이상 탐지 엄석현, 손현기, 오준호, 김시우, 박진우, 임중혁, 윤명근 (국민대학교)

## 2026년 5월 8일(금)

세션명	순서	논문번호	제목 (저자/소속)
10:40~11:55 5C. 인공지능 보안 VII 좌장: 윤종희 (영남대)	5C-1	277	Semantic 기반 로그 그룹핑 및 해석을 통한 TTP 탐지 및 실시간 공격양상 분석 연구 이주영, 오정민, 이태진 (가천대학교)
	5C-2	44	Neural Leakage-based Cryptanalysis of LowMC with Linear Complexity 김광조 (KAIST, IRCS)
	5C-3	163	가중치 기반 이중 벡터 스코어링을 활용한 HNSW 캐스케이드 프롬프트 인젝션 탐지 아키텍처 박종은, 정현욱, 김태성 (충북대학교)
	5C-4	182	시뮬레이션 기반 Physical AI 에이전트에서 로컬 프롬프트 인젝션에 의한 행동 환각의 보안성 평가 임호현, 이세영 (강원대학교)
	5C-5	278	Physical Agent의 잠재적 위험 조기 탐지를 위한 End-to-End 사전 검증 프레임워크 정혜란, 이태진 (가천대학교)
10:40~11:55 5D. 암호이론 및 구현 IV 좌장: 서승현 (한양대)	5D-1	439	코드 다형성 기반 부채널 분석 대응기법의 이론적 분석과 실험적 검증 오성빈, 한동국 (국민대학교)
	5D-2	379	설명 가능한 인공지능의 프라이버시 보존 연구 동향 신호준, 이동환, 김호영, 이윤호 (서울과학기술대학교)
	5D-3	351	효율적인 내적 마스킹 곱셈과 이를 적용한 2차 마스킹 AES 한재승, 한동국 (국민대학교)
	5D-4	421	노이즈 양자 네트워크 환경에서의 UBQC 핵심 구조에 대한 시뮬레이션 기반 성능 분석 김유민, 윤지원 (고려대학교)
	5D-5	323	2-radix, 3-radix, Trinomial 변환을 지원하는 격자 기반 암호 통합 butterfly 아키텍처 이재석, 신동현, 김영범, 서석중 (국민대학교)
10:40~11:55 5E. 산업보안/ 우주보안 II 좌장: 이민우 (한국해양대)	5E-1	391	가상 환경 선박 항해 시스템에서의 MITRE ATT&CK ICS 기반 사이버 공격 테크닉 분석 연구 이진성, 박성민, 김대운, 임준형, 나사랑 (한국인터넷진흥원)
	5E-2	70	인공위성 RF 신호 생성 통한 오픈소스 지상국 시스템 취약점 연구 오경제, 장대희 (경희대학교)
	5E-3	104	프롬프트 엔지니어링 기반 설명 가능한 산업제어시스템 이상 탐지 방안 연구 박주연, 엄익채 (전남대학교)
	5E-4	107	지식그래프 임베딩을 활용한 산업제어시스템 취약점-자산 잠재적 연관성 예측 연구 이성호, 엄익채 (전남대학교)
	5E-5	407	IACS UR E22 및 E26 기반 선박 CBS의 위협-실패 통합 시나리오 생성에 관한 연구 노창현, 김진강, 이진성, 임준형, 나사랑 (한국인터넷진흥원)

2026년 5월 8일(금)

세션명	순서	논문번호	제목 (저자/소속)
10:40~11:55 5F. 네트워크/ 클라우드 보안 IV  좌장: 박기웅 (세종대)	5F-1	301	그래프 신경망의 기능적 역할에 따른 생성형 AI 모델 분석 오영재, 박근우, 서창호 (공주대학교), 정수용 (한국과학기술정보연구원)
	5F-2	380	네트워크 침입탐지를 위한 딥러닝 기반 이상블 모델의 텔레메트리를 활용한 검증 프레임워크 백익준, 권태웅 (한국과학기술정보연구원)
	5F-3	282	무기체계용 5G 통신 인프라 보호를 위한 LLM 기반 폐쇄 루프 NGAP 프로토콜 퍼징 시스템 설계 및 실험적 검증 이나경, 김환국 (국민대학교)
	5F-4	401	TraMEL: 암호화된 맬웨어 트래픽 패밀리 분류를 위한 대표 샘플 기반 연속학습 박정민, 박지민, 지아현, 한소현 (이화여자대학교), Mohammad Saidur Rahman (University of Texas at El Paso), 오세은 (이화여자대학교)
	5F-5	436	제로트러스트 환경의 eBPF 활용 연구 동향 및 국가 망 분리(N2SF) 적용 방안 연구 지동혁, 최상훈, 박기웅 (세종대학교)
10:40~11:55 5G. 하드웨어 보안 II  좌장: 서석충 (국민대)	5G-1	139	베이지안 최적화 기반 오류 주입 파라미터 탐색 다양화 기법 제안 전승현, 신원근, 한이소, 김희석 (고려대학교)
	5G-2	316	임베디드 시스템 분석을 위한 시리얼 통신 기반 자동화 펌웨어 추출 전략 제안 이주협, 조건영 (스틸리언)
	5G-3	405	NAND 플래시 FTL의 내부 상태 변화 기반 취약점 탐지를 위한 Domain-aware 퍼징 기법 김진세, 전희도, 최원석 (고려대학교)
	5G-4	448	차량용 CAN 버스 물리 계층 EMI 공격 동향 조사 김가현, 최원석 (고려대학교)
	5G-5	427	전자기파 부채널 분석을 이용한 임베디드 기기 단일 실행 이상행위 탐지 연구 박수진, 배대현, 이인섭, 김희석 (고려대학교), 홍석희 (스마트 엠투엠)
10:40~11:55 5H. 정보보호 표준/평가/ 인증/교육  좌장: 김현일 (조선대)	5H-1	222	LLVM IR 기반 디컴파일러 평가 프레임워크 제안 김태현, 최원석, 이동훈 (고려대학교)
	5H-2	339	제로트러스트 성숙도 평가의 난점과 진단모델 설계 방향: 전문가 인터뷰를 중심으로 서진우, 서정우, 공나영, 송민희, 박기웅 (세종대학교)
	5H-3	332	산업제어시스템 공격 단계별 취약 지점 식별을 위한 Bow-tie 기반 보안 성숙도 해석 프레임워크 제안 최현서, 최동준, 서정택 (가천대학교)
	5H-4	261	NIST AI RMF 등 6개 주요 프레임워크 분석을 통한 Agentic AI 보안 아키텍처 설계 임준형, 박성민, 오진영, 나사랑 (한국인터넷진흥원)
	5H-5	455	직무 특성과 지식수준을 고려한 정량적 역량 평가 모형 개발 박진용, 김태성 (충북대학교)

## 2026년 5월 8일(금)

세션명	순서	논문번호	제목 (저자/소속)
5I. 인증/ID관리 및 콘텐츠/ 저작권 보안	5I-1	33	A2A 프로토콜에서 보안 강화를 위한 JWT 서명 기반 바인딩 기법 유진, 김득훈, 곽진 (아주대학교)
	5I-2	176	제로 트러스트 원칙을 적용한 OTT 서비스의 지속적 인증 및 세션 관리 메커니즘 제안 박서연, 이지은, 이종호, 장의진, 신용태 (숭실대학교)
	5I-3	451	비밀번호 내 특수문자 사용 패턴을 고려한 확률 기반 비밀번호 생성 연구 정태진, 김역, 손기욱, 이창훈 (서울과학기술대학교)
	5I-4	175	분산 신원 증명(DID)을 활용한 OTT 서비스의 보안 구독 공유 모델 설계 김지연, 이지은, 김하윤, 장의진, 신용태 (숭실대학교)
	5I-5	212	도메인 기반 다중 이미지 워터마킹의 요구사항 연구 전영준, 김효승 (한림대학교)
5J. 공급망 보안 II	5J-1	92	산업제어시스템 공급망 보안 강화를 위한 대규모 언어 모델 기반 VEX 생성 연구 김준석, 엄익채 (전남대학교)
	5J-2	420	퍼징 기반 실행 경로 확장을 활용한 동적 SBOM 기반 취약점 탐지 기법 경서연, 정예림, 이일구 (성신여자대학교)
	5J-3	326	LL2M: LLVM 및 대형 언어모델(LLM)을 활용한 의미론적 컴포넌트 식별 김지민, 이만희 (한남대학교)
	5J-4	406	On the Effect of LoRA Rank on Generalization and Adversarial Robustness in Smol Vision Language Models 무함마드 나빌 파들루르라흐만, 신다윗, 김호원 (부산대학교)
	5J-5	435	평균 기반 전처리 및 오토인코더를 활용한 하드웨어 트로이목마 탐지 문채윤, 한동국 (국민대학교)
5K. 시스템 보안 II	5K-1	342	암호화 환경에서의 SPLT-SHAP 매칭을 통한 신뢰성 있는 비인가 프로그램 탐지 연구 이현우 (가천대학교), 백익준, 권태웅 (한국과학기술정보연구원), 이태진 (가천대학교)
	5K-2	128	Kuberosy+: 컨테이너를 위한 상태 저장 기반 시스템 콜 보안 프레임워크 허진, 조치현, 이승수 (인천대학교)
	5K-3	144	CTI 보고서 기반 사이버 복원력 평가 방법론 이해음, 최슬기, 김태현, 김서연, 김태은 (한국인터넷진흥원)
	5K-4	236	RAG 시스템의 군집화 기반 방어 회피를 위한 분산형 지식 오염 공격 박준형, 김형식 (성균관대학교)
	5K-5	300	인증 삭제 기법 기반 에포크 강제형 비밀 분산 조승현, 김영식 (대구경북과학기술원)

2026년 5월 8일(금)

세션명	순서	논문번호	제목 (저자/소속)
10:40~11:55 5L. 블록체인/ 암호화폐/ 메타버스 보안  좌장: 이동재 (강원대)	5L-1	235	블록체인 기반 SBOM 무결성 검증 모델 이명선, 정승욱 (건양대학교)
	5L-2	220	프라이버시 코인 악용 방지를 위한 부분적 익명성과 추적 가능성을 보장하는 시스템 설계 연구 이동주, 임준호, 정익래 (고려대학교)
	5L-3	100	UAV 군집을 위한 스마트계약 기반 멤버 인증 및 그룹키 합의 기법 조현아, 김수현, 이임영 (순천향대학교)
	5L-4	26	DHT 기반 P2P 분산 파일 공유 시스템의 공격 시나리오 분석 및 자동화 방어 프레임워크 설계 이인진, 김재현, 김기천 (건국대학교)
	5L-5	111	분포 기반 동적 Contamination 조정을 통한 Isolation Forest 모델 미탐 최소화 연구 이하임, 홍승우, 김원빈, 서대희 (상명대학교)

## 2026년 5월 8일(금)

세션명	순서	논문번호	제목 (저자/소속)
09:00~10:10 P1. 포스터 I 좌장: 이윤호(서울과기대) 강정민(고려대) 석병진(한성대)	P1-001	173	psutil 기반 경량 프로세스 모니터링의 악성코드 행위 탐지 가능성과 한계 김유진, 함상규, 박정수 (강남대학교)
	P1-002	77	PQC 전환 환경에서 TLS 1.3 동적 리키잉(Rekeying)의 구조적 한계와 개선 방안 손수경, 양희재, 김다은, 김성민 (성신여자대학교)
	P1-003	177	AI 기반 계정 단위 이상 행위 탐지 모델 설계 박준석, 김창훈 (대구대학교)
	P1-004	178	LLM의 추론 불충실성에 대한 영공간 제약 기반 추론 무결성 보존 학습 이지수, 박성규, 박소희, 최대선 (송실대학교)
	P1-005	83	IoT 환경에서의 격자 기반 암호 구현 성능 분석 이다인, 이주희 (성신여자대학교)
	P1-006	180	BOSS: 차원 축소와 클래스간 거리를 활용한 체계적인 네트워크 침입 탐지용 특징 선택 프레임워크 김선호, 백동명, 이현우 (한국에너지공과대학교)
	P1-007	78	PUF + PQC 기반 Zero Trust 보안 이기동, 서정택 (가천대학교)
	P1-008	297	5G 기반 국방망 보호를 위한 신뢰할 수 없는 기지국에 의한 가입자 식별자 변조 시나리오 연구 조영건, 김한국 (국민대학교)
	P1-009	302	운용 환경을 고려한 Text-to-Image 생성 이미지 판별 프레임워크 최원혁, 김예은, 박종범, 송자운, 이재용, 이종현 (성공회대학교)
	P1-010	84	LoRa 통신에서 Chaskey 기반 데이터 무결성 성능 분석 및 재전송 공격 방지를 위한 방어 로직 구현 이재호, 최정열 (성결대학교)
	P1-011	167	PRESHIELD: 하이브리드 의미 기반 스코어링을 활용한 LLM Jailbreak 프롬프트 탐지 서희영, 이세영 (강원대학교)
	P1-012	307	언어 교환 애플리케이션 HelloTalk 데이터 복호화 및 아티팩트 분석 연구 함소영 (성신여자대학교), 김현준, 강수진, 김종성 (국민대학교)
	P1-013	431	실시간 통화 환경에서의 딥페이크 보이스피싱 대응 방안 연구: FFT 기반 음성 탐지 알고리즘 김주현, 손경호 (강원대학교)
	P1-014	20	LLM 에이전트 아키텍처의 자동 침투 테스트 비교 분석 김미향, 박재표 (송실대학교)
	P1-015	433	HWPX 문자 보호 기능의 복호화 메커니즘 분석 김성우 (서울과학기술대학교), 이나원 (중앙대학교), 김영진, 조민정, 김역, 손기욱, 이창훈 (서울과학기술대학교)
	P1-016	85	Google Drive 서비스의 API 재구성 기반 선택적 데이터 수집 및 숨김·삭제 파일 메타데이터 획득 연구 신민석, 최종윤, 김한결, 김대환, 박명서 (한성대학교)
	P1-017	308	생성형 AI 애플리케이션 'Manus AI'에 대한 디지털 포렌식 관점에서의 아티팩트 분석 박승현, 박유진, 박주연, 이용진, 박세준, 김종성 (국민대학교)

2026년 5월 8일(금)

세션명	순서	논문번호	제목 (저자/소속)
09:00~10:10 P1. 포스터 I 좌장: 이윤호(서울과기대) 강정민(고려대) 석병진(한성대)	P1-018	424	차량 텔레매틱스 환경에서의 모바일 베이스밴드 취약점 재현 가능성 분석 정용래, 윤요섭, 황지웅, 정민찬, 임강빈 (순천향대학교)
	P1-019	183	군사작전 환경에서의 AI 활용 한계와 연합학습 적용 방안 김주빈, 이세영 (강원대학교)
	P1-020	184	NFT Discord 스캠 활동에 대한 측정 연구: 데이터 수집 도구 개발 및 스캠 특성 분석 유준혁, 황성재 (성균관대학교)
	P1-021	203	VPP 기반 차세대 전력망 운영을 위한 제로트러스트 아키텍처(ZTA) 구현 방안 연구 박택근, 김성철, 김민용 (한전KDN), 서정택 (가천대학교)
	P1-022	418	5G SBA 환경에서의 인증 신뢰성 확보를 위한 세션 및 전송 계층 보안 검증 연구 나성민, 오지연, 김보남, 유일선 (국민대학교)
	P1-023	87	보안 콘텐츠의 매칭 기술을 활용하는 CTFd 기반 보안 교육 시스템 설계 이재원, 김영재, 김태일, 심민규, 남수만 (청주대학교)
	P1-024	185	EIP-7702 스폰서 기반 위임 철회 메커니즘 설계 조은, 배준호, 강형우 (고려대학교)
	P1-025	3	AI 기반 ICS 이상탐지에서 Feature 스케일링 영향도 분석 전원준, 이예찬, 김윤성, 하재철 (호서대학교)
	P1-026	416	IEEE 802.11ax 업링크 OFDMA에서 악의적 BSR 보고에 대응하기 위한 안전한 RU 스케줄링 기법 손규하, 지승하, 이일구 (성신여자대학교)
	P1-027	434	이더리움 스마트 컨트랙트 환경에서의 PQC 전환 구조적 한계 김시성, 유제성 (강원대학교), 김상현 (고려대학교), 이서준 (호서대학교), 이동재 (강원대학교)
	P1-028	234	우주자산 암호모듈 무결성 보장을 위한 방사선 강화형 안티탐퍼링 방호체계 연구 민경령 (가천대학교), 조양찬 (스페이스엔비), 윤영삼 (서울과학기술대학교), 서정택 (가천대학교)
	P1-029	94	양자 컴퓨팅 성능 평가 방법론: Planted QUBO 벤치마크 분석 김이든, 이동재 (강원대학교)
	P1-030	102	CLI 환경에서 OS권한 수준에 따른 AI 에이전트의 유용성 및 보안 위험 분석 김진섭, 유지현 (광운대학교)
	P1-031	186	자율형 AI Agent 실행 흔적 기반 시스템 포렌식 가능성 분석 송민경, 진규정, 이세영 (강원대학교)
	P1-032	113	CloudTrail 로그 입력 형식에 따른 LLM 공격 탐지성과 비용 비교 장유나, 박소유, 남수민, 신예은, 김성민 (성신여자대학교)
P1-033	309	23라운드 LBC-IoT 블록암호에 대한 선형 공격 권혁태, 박준영, 송원우, 김남일, 백승준, 김종성 (국민대학교)	
P1-034	414	P2P 기반 서비스 개발 및 운영 시 고려해야 하는 국내 법령과 컴플라이언스 가이드라인에 대한 연구 김예찬, 김동현, 김예진, 권다은, 안승민, 김동찬 (국민대학교)	
P1-035	245	Beyond LLM-as-a-Judge: 신뢰성 있는 안전성 평가를 위한 도구 기반 에이전트 프레임워크 백종현, 이태진 (가천대학교)	

## 2026년 5월 8일(금)

세션명	순서	논문번호	제목 (저자/소속)
09:00~10:10 P1. 포스터 I 좌장: 이윤호(서울과기대) 강정민(고려대) 석병진(한성대)	P1-036	312	DPLL(T) 기반 ReLU 신경망 검증을 위한 교육용 오픈소스 소프트웨어 개발 김송현, 노정균, 이찬희, 최주연, 최광훈 (전남대학교), 김재권, 임효상 (연세대학교)
	P1-037	442	인공지능 보안을 위한 ETSI 기반 학습데이터 품질 검증 프레임워크 오예진, 표자연, 이은진, 이지은, 송재승 (세종대학교)
	P1-038	187	다국어 프롬프트 환경에서 LLM 성능 편차와 보안 신뢰성의 관계에 관한 분석 조수빈, 김형식 (성균관대학교)
	P1-039	4	임베디드 시스템 위협 분석을 위한 ESTM 3.0 프레임워크 활용 방안 한준수 (상명대학교), 임재덕 (한국전자통신연구원)
	P1-040	318	Cortex-M0/M0+ 환경에서 Kyber NTT 최적화를 위한 모듈러 곱셈 기법 비교 및 적용 연구 이진현, 신동현, 서석중 (국민대학교)
	P1-041	191	외부 가열 시간에 따른 USB 데이터 손상 양상 분석 오현민, 한승재, 박준석, 김창훈 (대구대학교)
	P1-042	264	SOME/IP 통신 환경을 위한 인증체인과 경량 런타임 보호의 분리 구조 김명선, 오현영 (가천대학교)
	P1-043	321	연합 학습 기반 SDV NLU 모델을 위한 계층별 하이브리드 그래디언트 방어 기법 박준혁, 이재희, 안효범 (공주대학교)
	P1-044	404	LLM 기반 C/C++ 코드 분석을 위한 가역적 식별자 치환 기반 토큰 효율화 기법 박성민, 임우진, 김동엽, 장진수 (충남대학교)
	P1-045	322	서비스 메시와 eBPF 연계 기반 크로스레이어 클라우드 네이티브 이상행위 탐지 기법 박가은, 김서이, 이일구 (성신여자대학교)
	P1-046	114	CloudTrail 기반 Prompt-based LLM 공격 탐지에서 프롬프트 구조에 따른 성능 및 오류 편향 분석 박소유, 장유나, 남수민, 신예은, 김성민 (성신여자대학교)
	P1-047	192	MCP의 SDK 간 프로토콜 적합성 분석 김아인, 이승수 (인천대학교)
	P1-048	324	프레임별 주파수 마스킹 최적화를 통한 음성 딥페이크 생성 억제 기법 임지현, 박서영, 정수환 (송실대학교)
	P1-049	280	도메인 특화 AI Agent에서의 목표 무결성 보호를 위한 Intent Capsule 기법 연구 최유나, 김려담, 정연수, 이태진 (가천대학교)
	P1-050	118	TransMUSIC 기반 DOA 추정 모델의 위협 시나리오 분석 전한아솔, 유지현 (광운대학교)
	P1-051	325	ML-DSA 주요 연산을 위한 Tensor core 적용 방안 분석 고주희, 최준혁, 김동천, 서석중 (국민대학교)
	P1-052	446	CPG 기반 SSRF 취약점 탐지의 한계 및 LLM 기반 보완 가능성 신준석, 한승균, 박민서, 양지연, 장진수 (충남대학교)
	P1-053	400	On-Premises 환경에서 사전 점검을 통한 네트워크 자동 설정 기법 개발 고성노, 임정민, 양혁주, 최민우, 남수만 (청주대학교)

2026년 5월 8일(금)

세션명	순서	논문번호	제목 (저자/소속)
09:00~10:10 P1. 포스터 I  좌장: 이윤호(서울과기대) 강정민(고려대) 석병진(한성대)	P1-054	327	5G NR 채널 상태 정보 피드백 보안 위협 연구 이준희, 서영재, 주경호 (송실대학교)
	P1-055	193	LLM 기반 스마트 컨트랙트 불변식 자동 생성 연구동향 분석 지영빈, 이세영 (강원대학교)
	P1-056	281	복합 공격 환경에서의 공격유형 및 전파 대상 예측을 위한 오프라인 강화학습 기반 모델 제안 이주현, 지일환, 전승호, 서정택 (가천대학교)
	P1-057	397	국내 STO 제도화의 쟁점과 설계 과제 김민규, 신다윗, 하업준, 김호원 (부산대학교)
	P1-058	120	도래각(DOA) 추정 성능 향상 기법 최신 연구 동향 분석 김경목, 유지현 (광운대학교)
	P1-059	459	SURE: LLM 기반 CVE 취약점 탐지를 위한 테스트 자동화 프레임워크 표자연, 정재형, 오예진, 이은진, 송재승 (세종대학교)
	P1-060	460	RAG 시스템 대상 간접 프롬프트 인젝션 공격의 체계적 분류와 방어 메커니즘 매핑 한초연 (성신여자대학교)
	P1-061	12	SUDA: 네트워크 침입 탐지에서의 선택적 언러닝 기반 드리프트 적응 임태인, 이미영, 노승민 (중앙대학교), 박성우 (덕성여자대학교)
	P1-062	331	AI 생성 이미지 탐지 모델의 강건성과 실패 양상에 대한 실증 연구 장현진, 하업준, 김무영, 김호원 (부산대학교)
	P1-063	283	다중 위협 모델 기반 보안관제 대응 연계 프레임워크 제안 진호준, 서정택 (가천대학교)
	P1-064	127	사족보행 로봇의 카메라 및 IMU 센서에 대한 물리적 취약점 분석 김택현, 우상민, 서지우, 김용대 (한국과학기술원)
	P1-065	6	UAE: Universal Adversarial Embedding을 이용한 확산 모델의 비파괴적 유해 개념 완화 서채은, 류권상 (공주대학교)
	P1-066	335	Cross-Attention 기반 다계층 융합을 통한 스마트 팩토리 APT 공격 탐지 모델 제안 이우곤, 고성노, 이재원, 정은수 (청주대학교)
	P1-067	194	Apple C1 펌웨어 분석 및 ARI 프로토콜 연구 김상현 (서울과학기술대학교), 오범석, 김광민, 김용대 (한국과학기술원)
	P1-068	197	스마트 팩토리 가상 공정 테스트베드 구축 및 Scapy 기반 사이버 공격 구현 이혜강, 현명준, 최현진, 하재철 (호서대학교)
	P1-069	202	IoT 환경의 양자내성암호(PQC) 전환을 위한 네트워크 통신 최적화 기법 동향 및 적용 분석 이승찬, 김수빈, 유동현 (전남대학교)
	P1-070	291	다자 승인 구조와 상태 기반 접근 제어를 활용한 디지털 유산 상속 시스템 제안 김지원, 김장호, 이채은, 지일환, 서정택 (가천대학교)
	P1-071	337	격자 기반 암호의 다항식 곱셈 최적화 기법 비교 분석 권보연 (대구가톨릭대학교), 박정식 (경희대학교)

## 2026년 5월 8일(금)

세션명	순서	논문번호	제목 (저자/소속)
09:00~10:10 P1. 포스터 I 좌장: 이윤호(서울과기대) 강정민(고려대) 석병진(한성대)	P1-072	461	ComfyUI 커스텀 노드의 공급망 공격 탐지를 위한 AST 기반 사전 검사 기법 박시우, 이지호, 송재승 (세종대학교)
	P1-073	396	다중 가상화 실행환경을 지원하는 seL4 기반 하이퍼바이저를 통한 네트워크 격리 방법 이동민, 박경빈, 푸레브바타르, 임강빈 (순천향대학교)
	P1-074	130	안드로이드 파일 보호 애플리케이션의 암호화 알고리즘 분석 한동균, 위다빈, 박명서 (한성대학교)
	P1-075	347	CLIP 기반 이미지-텍스트 검색 환경에서의 적대적 공격 및 방어 기법의 효과 분석 김형준, 이다영 (강원대학교)
	P1-076	211	MCP를 활용한 LLM 기반 SAST 취약점 분류 프레임워크 박동혁, 김영진, 이창훈, 손기욱 (서울과학기술대학교)
	P1-077	294	정적 분석과 실행 재현 기반 MCP 서버 구현 취약점 탐지 및 악용 가능성 검증 시스템 정수진, 황수빈, 김영훈, 최동준, 서정택 (가천대학교)
	P1-078	353	LangGraph 기반 AI 에이전트를 위한 다층 보안 방어 아키텍처의 설계 및 성능 분석 김아람, 이하늘, 전상훈 (수원대학교)
	P1-079	394	멀티 에이전트 AI 시스템에서 방어 개입 위치에 따른 권한 상승 억제 효과 분석 김무영, 신다윗, 김호원 (부산대학교)
	P1-080	463	의료 연합학습 활성화를 위한 파라미터 조건부 면책 제도 도입 방안 이종현 (한양대학교), 이진주 (경희대학교), 김고은 (중앙대학교), 김은우 (한양대학교), 신동일 (서울대학교)
	P1-081	389	임베디드 환경에서의 하이브리드 PQC 인증서 벤치마킹 장선우, 이여녕, 서승현 (한양대학교)
	P1-082	354	하드웨어 삼중진자 기반 TRNG의 설계 및 보안 검증 방법론 임승훈, 김한솔, 정재영, 이해령, 광진 (아주대학교)
	P1-083	218	초기 패킷 시퀀스 기반의 초경량 DDoS 선제적 탐지 모델 박윤서, 박상경, 권현수 (인하대학교)
	P1-084	296	불완전 로그에서의 침해사고 공격 흐름 추론 및 캠페인 식별 기법 연구 오정민, 이주영, 이태진 (가천대학교)
	P1-085	133	Flutter AOT 바이너리 분석 정제 도구 개발 및 보안 애플리케이션 분석 사례 연구 신준성, 김한결, 박명서 (한성대학교)
	P1-086	10	모의실험용 랜섬웨어 제작을 통한 랜섬웨어 대응 방안 연구 홍용민, 장대희 (경희대학교)
	P1-087	357	유럽 eIDAS 2.0과 한국 전자서명법의 효력 등급 및 신뢰서비스 비교 분석 이서준, 이성훈, 유동현 (전남대학교)
	P1-088	221	AI 모델 공급망 보안을 위한 Format-Aware Fuzzing 기반 검증 아키텍처 FuzzGate 신숙우, 이우곤, 윤종문 (청주대학교)
	P1-089	226	차량 CAN 버스 침입 탐지를 위한 XAI 기반 포렌식 분석 프레임워크 이윤주, 김규림, 김연희, 김종길 (이화여자대학교)

2026년 5월 8일(금)

세션명	순서	논문번호	제목 (저자/소속)
09:00~10:10 P1. 포스터 I  좌장: 이윤호(서울과기대) 강정민(고려대) 석병진(한성대)	P1-090	229	선박 Cyber Resilience를 위한 Forensic by Design 기반 보안 프레임워크 박채민, 김종인, 이우진, 이민우, 김도현 (한국해양대학교)
	P1-091	299	분석가 피로도 완화를 위한 피드백 기반 지식 축적 자동화 네트워크 침입 탐지 시스템 전수아, 이선우, 이태진 (가천대학교)
	P1-092	135	SPHINCS+ 대상 상관 전력 분석 공격 장진욱, 이민정, 한동국 (국민대학교)
	P1-093	138	바이오 데이터 클라우드 분석을 위한 특징 벡터 기반 동형암호 파이프라인 제안 이경윤, 김희찬, 손준영 (부산대학교)
	P1-094	147	TLS 연결의 양자 위협 기반 계층적 위험도 산출 모델 형유림, 정수민, 임다운, 박도윤, 조수빈, 김재환, 서화정 (한성대학교)
	P1-095	149	항공기 유지감항 활동에서의 사이버보안 고려사항 이서희, 송유래, 김득훈, 곽진 (아주대학교)
	P1-096	152	WavMark 딥페이크 음성 워터마킹 강건성 평가 (MP3 압축 및 AWGN 환경을 중심으로) 이인화, 김유민, 황태현, 김유정, 공다연, 손예린, 임서연, 석병진 (한성대학교)
	P1-097	11	하드웨어 기반 eBPF 격리 기술 동향: 성능 최적화와 보안 신뢰성 확보 방안 연구 박정원, 박성환, 권동현 (부산대학교)
	P1-098	303	정적·동적 분석을 이용한 Node.js 프로젝트 의존성 기반 공급망 공격 탐지 방법론 제안 정현영, 박소영, 손예진, 최동준, 서정택
	P1-099	230	iOS 얼굴 분석 서비스 아티팩트의 디지털포렌식 활용 방안 박주환, 박채민, 안도연, 김도현 (한국해양대학교)
	P1-100	231	피싱 공격 및 탐지 기술 동향과 향후 과제 박지영, 최원영, 김우주, 이다영 (강원대학교)
P1-101	240	IACS UR E26 검증 자동화를 위한 워크플로우 기반 점검 방법론 설계 차한술, 김영민, 김정호, 조해성, 박기웅 (세종대학교)	

## 2026년 5월 8일(금)

세션명	순서	논문번호	제목 (저자/소속)
10:40~11:50 P2. 포스터 II 좌장: 이윤호(서울과기대) 이세영(강원대) 김영수(고려대)	P2-001	388	LLM 기반 한국어 입력 패턴 분류를 통한 패스워드 룰셋 설계 연구 김나현, 조민정, 김역, 손기욱, 이창훈 (서울과학기술대학교)
	P2-002	315	Ground Truth 자동 기록 기반 포렌식 데이터셋 생성 및 AI 평가 Benchmark 프레임워크 윤지원, 오정민, 전수아, 최동준, 서정택 (가천대학교)
	P2-003	241	다중 참조 얼굴 부위 조합을 이용한 신원 비식별화 비디오 얼굴 합성 최원영, 이창진, 박지영, 이다영 (강원대학교)
	P2-004	244	비디오 컨퍼런싱 응용 트래픽 분류 기술 동향 이예찬, 노희준 (인하대학교)
	P2-005	247	OWASP Top 10 취약점 탐지를 위한 CI/CD 보안 파이프라인 개발 어윤규, 김태현, 김서연, 남수만 (청주대학교)
	P2-006	444	Skin Cancer Detection Using Spiking Neural Networks 칸 모하마드 아크바르 알리, 하산 Md 메헤디, 구롱 아스미, 타헤신 사미라 델와르 (경성대학교)
	P2-007	385	CRYSTALS-KYBER basemul 연산에 대한 부채널 대응기법 오버헤드 분석 이민정, 한동국 (국민대학교)
	P2-008	365	패키지 레지스트리의 다각적 위험도 측정 방법론 김형규, 이만희 (한남대학교)
	P2-009	317	Context Assembly 기반 분산 청크 오염을 통한 단일 문서 탐지 우회형 RAG 포이즈닝 공격 기법 제안 김지원, 원예람, 김가현, 지일환, 서정택 (가천대학교)
	P2-010	248	Sparse 제약을 적용한 LSTM-AE의 이상 탐지 성능 분석 최동환, 안경덕, 하재철 (호서대학교)
	P2-011	35	MCP Tool Poisoning Attack에 대한 Snyk Agent Scan 탐지 효용성 평가 남장우, 김득훈, 곽진 (아주대학교)
	P2-012	40	TLS 1.3 Hybrid KEM의 네트워크 지연에 따른 선택 가이드라인 제시 박희정, 김진욱 (한국방송통신대학교)
	P2-013	382	현행 침해사고 통지제도의 규범적 한계와 이용자 통지의무의 실효성 제고를 위한 법적 연구 손선민, 홍준호 (성신여자대학교)
	P2-014	52	Cortex-M4에서 VSEB 연산 최적화를 통한 TWFalcon 구현 박현주, 장지훈, 김규상 (고려대학교), 김수리 (성신여자대학교), 홍석희 (스마트 엠투엠)
	P2-015	333	O-RAN 환경에서의 xApp 신뢰도 평가 방안 연구 박소영, 목정현, 윤성우, 박지민, 이석준 (가천대학교)
	P2-016	14	RTOS의 성능 및 보안 특성 비교 분석 김지민, 박재열, 권동현 (부산대학교)
	P2-017	47	AnyONE: A Comprehensive 4-Layer Architecture for an All-in-One Autonomous Security Operations Center (SOC) Ghazi Akmal Fauzan, Ghaylan M. Fatih, Dhiwa Kusumah, Addin M. Yusuf, Mark Lee, Jong (John) Uk Choi (마크애니)

2026년 5월 8일(금)

세션명	순서	논문번호	제목 (저자/소속)
10:40~11:50 P2. 포스터 II 좌장: 이윤호(서울과기대) 이세영(강원대) 김영수(고려대)	P2-018	249	유무선 네트워크 환경에 따른 Google reCAPTCHA v2의 취약점 분석 연구 신속우, 어윤규, 남수만 (청주대학교)
	P2-019	250	LLM 챗봇 환경에서 프롬프트 주입을 이용한 개인정보 유출 체인 연구 양홍장, 나현식, 최대선 (송실대학교)
	P2-020	349	Brain Tumor Detection using Deep Learning: A Transfer Learning Approach 아크람 무함마드 삼라즈, 주나이드 이슬람 빈, 테베 트리자, 타헤신 사미라 델와 (경성대학교)
	P2-021	58	LLM 기반 동적 추론을 활용한 사이버 복원력 강화 전략 자동 생성 시스템 최슬기, 이새움, 김태현, 김서연, 임준형, 김태은 (한국인터넷진흥원)
	P2-022	336	Android 취약점을 이용한 스마트폰 데이터 탈취 시나리오 설계 가진섭, 지일환, 서정택 (가천대학교)
	P2-023	252	멀티에이전트 시스템에서의 구조별 오염 전파와 검증 방어 효과 분석 차한빈, 이다영 (강원대학교)
	P2-024	255	블록체인을 활용한 의료 장비 사용 이력 관리 시스템 설계 최현우, 김수현, 이임영 (순천향대학교)
	P2-025	61	품질 변화 유사도 기반 딥페이크 탐지 송일환, 유지현 (광운대학교)
	P2-026	69	Benchmarking Native HPKE in Java 26: SunJCE vs. Bouncy Castle Across Payloads and Platforms Vincent Abella, Jhury Kevin Lastre, 김보남, 유일선 (국민대학교)
	P2-027	79	양자화 수준에 따른 로컬 코드 생성 모델의 보안성 비교 분석 유승우, 김형식 (성균관대학교)
	P2-028	91	상태 전이 증폭 비율을 이용한 LLM의 추론 과정 공격 방어 방법 박성규, 박소희, 이지수, 나현식, 최대선 (송실대학교)
	P2-029	358	Python MCP 서버의 PyPI 의존성 취약점 현황 및 위험 패턴 분석 김보규, 지일환, 서정택 (가천대학교)
	P2-030	16	WebAssembly Multi-memory 기반 AddressSanitizer 메타데이터 보호 기법 및 보안 분석 전동훈, 송수현, 권동현 (부산대학교)
	P2-031	266	DDoS 공격 특성 비교를 통한 계층별 탐지 관점 분석 차주영, 강서연, 남하늘, 김성민 (성신여자대학교)
	P2-032	97	Data Poisoning 공격에 대한 MLOps 파이프라인의 통계 기반 탐지 및 대응 분석 차시현, 박성일 (워크포스에이아이), 홍순좌 (코어시큐리티)
P2-033	154	모델 추출 공격 연구 동향: 암호 분석적 기법을 중심으로 송현태, 이제형, 석병진 (한성대학교)	
P2-034	99	CDS를 위한 편집 가능 서명에 대한 연구 윤성철, 김수현, 이임영 (순천향대학교)	
P2-035	140	블록체인 기반 연합학습의 최근 기술 동향 분석 김진수, 김희찬, 손준영 (부산대학교)	

## 2026년 5월 8일(금)

세션명	순서	논문번호	제목 (저자/소속)	
10:40~11:50	P2-036	376	SAIL: 문법 인식 프로그램에 대한 LLM 에이전트 기반 퍼징 한규상, 강민주, 이동하, 박정우, 배연주, 전승호 (가천대학교)	
	P2-037	131	AI Agent Security: Attack Surfaces and Defense-in-Depth 레티투흐영, 신다윗, 조재한, 김호원 (부산대학교)	
	P2-038	181	HAWK SamplerSign의 누수 완화를 위한 마스킹 대응기법 설계 김동현, 이인훈, 김규상, 김희석 (고려대학교), 홍석희 (스마트 엠투엠)	
	P2-039	267	C-Guard: 사이버보안 경진대회를 위한 서버 중심 무결성 모니터링 아키텍처 임은강, 이해영 (청주대학교)	
	P2-040	23	eBPF 기반 파일 시스템 이벤트 모니터링을 활용한 리눅스 악성코드 탐지 최서연, 유지현 (광운대학교)	
	P2-041	268	클라우드 네이티브 환경에서의 외부 DDoS와 내부 DoS의 특성 구분 및 호스트 레벨 통합 탐지 관점 남하늘, 강서연, 차주영, 김성민 (성신여자대학교)	
	P2-042	19	WebAssembly와 JavaScript 상호작용에서의 공격 표면 분석 홍지연, 신채원, 권동현 (부산대학교)	
	P2-043	377	PwnSolver: LLM 기반 다중 에이전트를 통한 바이너리 익스플로잇 자동화 박정우, 강민주, 이동하, 한규상, 배연주, 전승호 (가천대학교)	
	P2. 포스터 II	P2-044	155	LightGBM 및 에스스로 컨트랙트 기반 이더리움 이상 거래 탐지 시스템 정윤녕, 김은성, 김덕연, 석병진 (한성대학교)
		P2-045	156	AI 기반 CTI 자동 수집 시스템 백승혜, 강민채, 윤주범 (세종대학교)
P2-046		57	TARA에서 공격 경로에 대한 공격 가능성 등급을 도출하기 위한 two-staging 방법론 한풍규 (현대케피코)	
P2-047		207	FPGA 시뮬레이션 기반 부채널 취약점 검증 기술 연구 김한빛, 박태환, 박정형 (ETRI 부설연구소)	
P2-048		208	제휴마케팅 플랫폼 API 기반 행태정보 수집 구조 및 개인정보 침해 위험성 연구 권유진, 최진경 (전남대학교), 차윤호 (한국인터넷진흥원), 이상준 (전남대학교)	
P2-049		390	N2SF 보안 체계 적용을 위한 망간 자료 전송 방안 제안 가진섭, 김주현, 이성은, 지일환, 서정택 (가천대학교)	
P2-050		213	비전언어행동(VLA) 모델의 보안 취약점 분류 및 분석 정희광, 신다윗, 김호원 (부산대학교)	
P2-051		174	복합 영상 변형 대응을 위한 프레임 분산 삽입 기반 비디오 워터마킹 방법 이지은, 장의진, 신용태 (송실대학교)	
P2-052		269	AWDL 프로토콜 기반 은닉 채널 구현 심아린, 최현우 (성신여자대학교)	
P2-053	216	검증 가능한 동형암호 연산 구현 및 분석 최주혁, 김동우 (동국대학교)		

좌장:  
이윤호(서울과기대)  
이세영(강원대)  
김영수(고려대)

2026년 5월 8일(금)

세션명	순서	논문번호	제목 (저자/소속)
10:40~11:50 P2. 포스터 II  좌장: 이윤호(서울과기대) 이세영(강원대) 김영수(고려대)	P2-054	219	Planning-Based LLM Agent Architecture for Autonomous Penetration Testing: A Comparative Study on CTF Challenges 무함마드 나빌 파들루르라흐만, 신다윗, 레티투흐영, 김호원 (부산대학교)
	P2-055	417	심볼릭 실행 기반 LLM 에이전트를 통한 허니팟 스마트 컨트랙트 탐지 방법론 제안 이동하, 한보윤, 김수민, 서정택 (가천대학교)
	P2-056	225	Where's the Key? Nowhere: Randomized Derivation and Scattering Against MITM Attacks 아낙 아궁 느구라 다마왕사, 몰아사리 울란 실바니, 레티투흐영, 장현진, 김호원 (부산대학교)
	P2-057	243	Istio 서비스 메시 환경에서의 내부 L7 DDoS 공격 탐지 및 대응을 위한 그래프 기반 프레임워크 강서연, 차주영, 남하늘, 김성민 (성신여자대학교)
	P2-058	257	DRPE의 취약점 분석 및 디퍼닝 기반 복원 기법 개선 연구 박경빈, 장재영, 박근우, 서창호 (공주대학교)
	P2-059	320	VMProtect에 적용된 보안 피처 분석 및 역난독화 가능성 연구 이재우, 최원석, 이동훈 (고려대학교)
	P2-060	29	멀티클래스 침입 탐지를 위한 유전 알고리즘 기반 Feature 선택 기법의 성능 분석 박성재, 안경덕, 하재철 (호서대학교)
	P2-061	429	국가망보안체계(N2SF) 기반 문서 라이프사이클 보안통제 참조모델 제안 김수민, 서정택 (가천대학교)
	P2-062	157	AI 기반 탐지 정책 생성 시스템 양혜연, 정은영, 윤주범 (세종대학교)
	P2-063	338	어텐션 강화 DesnowNet: 이미지 제설을 위한 CNN-트랜스포머 하이브리드 접근법 악타르 엠에스티 파르자나 아리프, 사키바 빈테 타헤신, 사미라 델와르, 이호상 (경남대학교)
	P2-064	371	CMALU: 양자내성암호용 소형 내결함성 모듈러산술유닛 김영범, 신동현, 이재석, 서석중 (국민대학교)
	P2-065	31	Format-Invariance Training: Master-Replica 전략을 활용한 생성형 이미지 탐지 모델의 압축 강건성 강화 윤태준, 강현성, 이재웅, 류권상 (공주대학교)
	P2-066	37	BOLA 탐지를 위한 행위 문맥 정보의 효과 분석 김송혜, 유지현 (광운대학교)
	P2-067	440	투명 프록시 환경에서의 위험 등급 기반 사용자 자율 정책 예외 시스템 제안 김다희, 서정택 (가천대학교)
	P2-068	384	AI 전술 통신망 보호를 위한 LLM 기반AI/ML Training Job 자동 생성 에이전트 구현 및 검증 김시환, 이수현, 김환국 (국민대학교)
P2-069	158	Widevine L3 환경에서의 콘텐츠 암호화 키 재사용 차단을 위한 세션 키 파생 사용 방안 김종건, 김수현 (순천향대학교)	
P2-070	160	브라우저 자원 경합 사이드채널을 통한 LLM 프롬프트 의도 추론 공격 진규정, 이세영 (강원대학교)	

## 2026년 5월 8일(금)

세션명	순서	논문번호	제목 (저자/소속)
10:40~11:50 P2. 포스터 II 좌장: 이윤호(서울과기대) 이세영(강원대) 김영수(고려대)	P2-071	42	DINOV2 기반 딥페이크 검출에서 중간 레이어 표현 차이와 배경 의존성 이재웅, 강현성, 윤태준, 류권상 (공주대학교)
	P2-072	43	Arm TrustZone을 이용한 스택 카나리 격리 :TF-M 환경에서의 오버헤드 평가 안동기, 남유찬, 정기현 (건국대학교), 이예준, 조효진 (연세대학교)
	P2-073	38	Sequence 기반 악성코드 탐지 및 회피 공격 분석 소예나, 방지수, 유새나, 오나현, 김성욱 (서울여자대학교)
	P2-074	453	SVD 기반 부분공간 제거를 통한 선형 검증형 CNN 워터마킹 제거 기법 제안 이성은, 지일환, 서정택 (가천대학교)
	P2-075	162	AMD SEV-SNP의 VMPL 구조와 SVSM 중심 특권 처리 경로에 대한 가용성 분석 용현서, 김다운, 양희재, 김지은, 김성민 (성신여자대학교)
	P2-076	392	예측 확률 기반 동적 제약 손실을 이용한 CVE-CWE 자동 매핑 기법 김영진, 권태웅, 이준 (한국과학기술정보연구원)
	P2-077	408	LLM 기반 Agent 보안 취약점 탐지 요구사항 분석 및 향후 방향 제안 원신영, 최지혁, 권태경 (연세대학교)
	P2-078	272	체이닝과 디코일을 활용한 AI 저항성 CTF 문제 설계 접근 방식 임용현, 이재원, 유지민, 신숙우, 임은강, 이해영, (청주대학교), 신선우 (클라우드에어)
	P2-079	287	고도화된 음성 합성 공격에 대한 SASV 강건성 분석 및 강건한 구조 설계 방향 임찬혁, 이요원, 정수환 (숭실대학교)
	P2-080	290	FOSSLight Binary scanner JAR 분석 과정에서의 confidence 기반 OSS 식별 신뢰성 개선 방안 이은섭, 이만희 (한남대학교)
	P2-081	464	결과 중심 위협 분류에 기반한 MCP 서버 동적 보안 분석 방법론 제안 전우진, 민건호, 김민규, 최동준, 서정택 (가천대학교)
	P2-082	164	GPU-DPU 오프로드 환경에서 GPUNetIO 실행 구조의 보안 분석 김지은, 김다운, 양희재, 용현서, 김성민 (성신여자대학교)
	P2-083	45	VR 리듬 게임 리플레이 데이터를 활용한 다중 사용자 행위 생체 인증 연구 김동휘, 안효범, 이완복, 윤성현, 정현지, 오승원, 류권상 (공주대학교)
	P2-084	48	암호화된 네트워크 트래픽 메타데이터 분석을 통한 생성형 AI 서비스 식별 가능성 연구 이산, 김준희, 박병욱 (연세대학교)
	P2-085	411	K-STIG 구축을 위한 LLM 기반 비정형 보안 문서의 SCAP 계열 XML 변환 파이프라인 설계 및 구현 안효빈, 김이든, 이동재 (강원대학교)
	P2-086	50	PCA 재구성오차 기반 프로세스 단위 랜섬웨어 탐지 정일준, 한승훈 (숭실대학교)
	P2-087	415	LLM 기반 리버스 엔지니어링을 위한 MCP 도구의 구현 방식 및 동향 분석 최준영, 김재민, 박민제 (스틸리언)
	P2-088	370	클라우드 관측 가능성 환경 내 공격 분석의 한계와 시공간 식별자를 활용한 그래프 분석 박주원, 권수빈, 이은진, 표자연, 박기웅 (세종대학교)

2026년 5월 8일(금)

세션명	순서	논문번호	제목 (저자/소속)
10:40~11:50 P2. 포스터 II 좌장: 이윤호(서울과기대) 이세영(강원대) 김영수(고려대)	P2-089	372	Post-Quantum TLS의 애플리케이션 환경별 적용 특성 및 연구 동향 분석 노희원, 김제인, 서승현 (한양대학교)
	P2-090	419	PQC 마이그레이션 환경에서의 Sandwich 플랫폼 분석 및 개선 방향 송민호, 이승원, 엄시우, 김하경, 서화정 (한성대학교)
	P2-091	437	IACS Rec.194 기반 운항선 SMS 연계 표준 교육안 제안 윤민홍, 이민우 (한국해양대학교)
	P2-092	166	상관 전력 분석을 이용한 FAEST 대상 비밀키 복구 유채연 (성신여자대학교), 김규상, 박수진, 김희석 (고려대학교)
	P2-093	51	RISC-V SoC 환경에서 FPGA 기반 독립적 메모리 무결성 감시 구조 천현우, 김재현, 한승훈 (송실대학교)
	P2-094	438	지능형 차량 네트워크의 구조화된 데이터를 위한 합성데이터 생성 기법 비교 연구 정은혜, 이경현 (부경대학교)
	P2-095	381	oneM2M 기반 연합학습을 활용한 베어링 고장 조기 탐지 시스템 설계 및 구현 이은진, 표자연, 오예진, 송재승 (세종대학교)
	P2-096	67	디지털 포렌식 트리아지 환경에서 암호화 파일 식별 기술 활용 분석: 엔트로피 기반 한계 및 AI/ML 기반 기술 동향 이유정 (강남대학교), 김득훈, 곽진 (아주대학교)
	P2-097	68	LLM 코드 생성 평가에서 기능성과 보안성을 동시에 고려한 벤치마크 비교 분석 오정호, 김형식 (성균관대학교)
	P2-098	170	차량 TCU의 LTE Attach 과정에서의 IMSI 노출 사례 분석 우다현, 서영재, 주경호 (송실대학교)
	P2-099	171	금융 API 환경에서의 Snort 3 탐지 규칙 설계 및 유효성 분석 윤서현, 김덕연, 서효리, 송현태, 이인화, 석병진 (한성대학교)
P2-100	172	IEEE 802.1X 기반 K-RMF 모니터링 단계 보안통제항목 분석 박병하, 송유래, 곽진 (아주대학교)	
P2-101	362	클라우드 침해사고 초동대응에서의 실무적 난해도 서베이 및 분석 이지호, 김병우, 이근형, 최진규, 박기웅 (세종대학교)	

**[등록비]**

구분	회원	비회원	현장등록
일반	300,000	400,000	400,000
군·공무원	200,000	250,000	250,000
학생(전일제)	200,000	250,000	250,000
학부생	100,000	100,000	100,000
시니어(63세이상) 종신회원	무료		

**[사전등록안내]**

## ▶ 사전등록 마감일

- 논문 발표자 사전등록 : ~ 2026년 4월 21일(화) 까지
- 일반 참가자 사전등록 : ~ 2026년 4월 24일(금) 까지

▶ 등록 방법 : ① 학회 홈페이지 접속 → 학회행사 → 사전등록 바로가기 → 학술행사(NetSec-KR 2026) 선택 → 등록  
② 신용카드 결제 혹은 무통장 입금

\*계좌번호: 국민은행 754-01-0008-146 (예금주 한국정보보호학회)

\*무통장 입금 결제 시 등록비는 위의 계좌로 송금하시고, 입금자가 대리일 경우 통보 바랍니다.

**[등록관련 안내사항]**

- 신용카드 결제 시 계산서 발급 불가합니다. (부가가치세법 시행령 제57조)
- 사전등록 시 청구용 계산서가 등록 이메일로 2~3일 이내 발행됩니다.
- 영수용 계산서가 필요한 경우 사전 문의해 주시기 바랍니다.
- 입금명은 소속명만으로 기재하여 입금 시 확인이 되지 않습니다. 이에 등록 누락을 방지하고자 입금명은 필히 [행사명 첫글자+등록자 성함]으로 기재해 주시기 바랍니다.

**[등록대상 및 유의사항]**

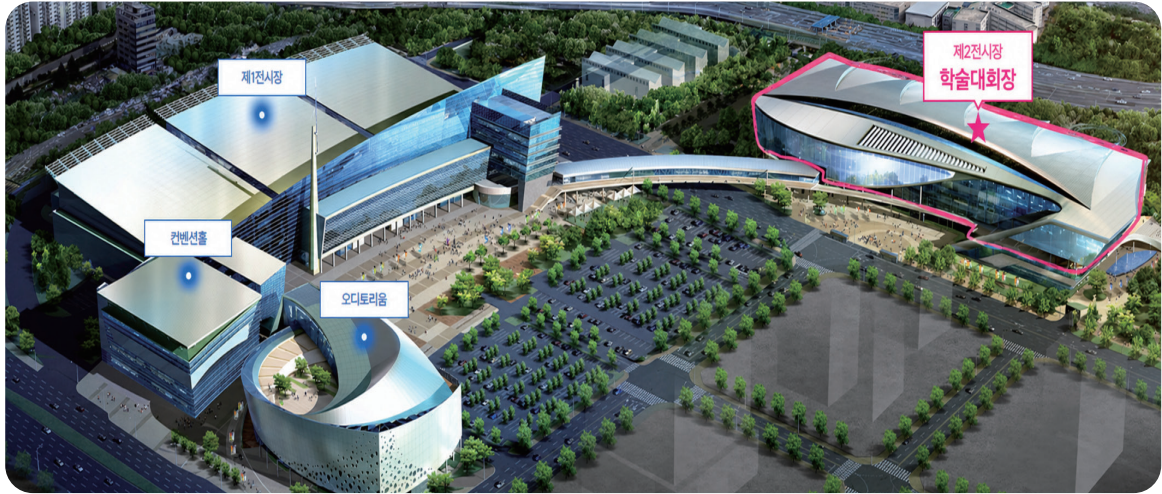
- 군·공무원 등록은 주무관청에 소속 중인 공무원증 소지자에 한하며 군·공무원 등록증 사본을 kiisc@kiisc.or.kr로 송부해 주시기 바랍니다. (국공립 교직원 제외)
- 시니어 무료등록은 학회 종신회원으로 1964년 12월 31일 이전 출생자로 학회 종신회원 분들에 한합니다.
- 회원혜택 기준은 행사 당일인 2026/5/8(금)까지 활동 회원(연회비 납부 회원)이어야 합니다.
- 학부생의 경우 kiisc@kiisc.or.kr 로 학생증 사본 송부해 주시기 바랍니다.
- 학회 특별회원사 임직원은 학회 회원으로 준합니다. 특별회원사 여부는 학회 홈페이지 (www.kiisc.or.kr) 회원광장 → 특별회원사에서 확인하실 수 있습니다.
- 대학원생은 전일제에 한합니다. (타소속 없음)
- 논문 한편 당 저자 한 분은 반드시 사전등록을 하셔야 합니다.
- 등록확인서 및 참가확인서는 등록비 납부완료자에 한하여 한국정보보호학회 홈페이지 상단 "행사등록 및 참가확인서" 바로 가기를 클릭 하신 후 등록 시 기재하신 성함과 이메일을 기재하시면 출력 가능합니다. (단, 참가확인서는 행사종료 후 다음날부터 발급 가능)

**[참가자 제공사항]**

- ▶ 5/7 (목) 중식 및 만찬
- ▶ 5/8 (금) 중식
- ▶ 행사 리플릿, 온라인 프로시딩 논문집 제공, 기념품은 행사 종료 후 등록자에게 모바일 쿠키쿠폰으로 발송

계산서 문의처      한국정보보호학회 사무국 02-564-9333 (내선5), kiisc@kiisc.or.kr  
 행사 문의처      한국정보보호학회 사무국 02-564-9333 (내선2), kiisc@kiisc.or.kr  
 회비 납부 및 회원 확인      한국정보보호학회 사무국 02-564-9333 (내선3), kiisc@kiisc.or.kr

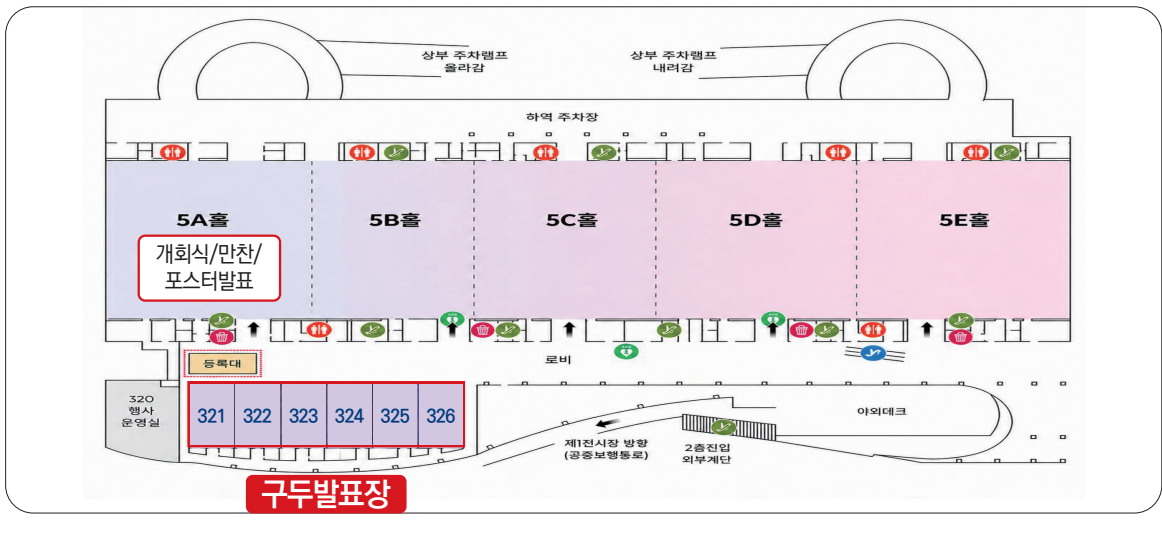
학술대회장 제2전시장



제2전시관 1F



제2전시관 3F



	5A (3F)	321호~326호	121~122호	123호~126호
DAY 1 / 5월 7일(목)	개회식/초청강연/신진연구자 소개	구두발표	구두발표	-
DAY 2 / 5월 8일(금)	포스터 발표	구두발표	구두발표	구두발표

#### ◆ 참가자등록대

제2전시관3층5A홀앞(5A홀과321호사이)

#### ◆ 주차안내

행사장내주차지원이불가하오니가급적대중교통을이용하여주시기바랍니다.

#### [백스코 부설주차장 기본 주차요금]

구분	10분마다	일일주차
소형	450원	15,000원
대형	900원	30,000원

#### ◆ 식사 제공 및 장소 안내

일자	구분	시간	장소
5/7(목)	중식	11:30~13:00	백스코개미집, 착한집밥, 한식당
	만찬	18:00~	일반: 제1전시관 (2F) 214~217호, 학생: 제2 전시관 5A홀 (3F)
5/8(금)	중식	11:55~14:00	백스코개미집, 착한집밥, 한식당

#### [중식장소]

- 백스코 제1전시장 지하 1층 식당 안내
- 아래 3곳 중 1곳 선택 이용

- (1) 개미집 백스코점 주요 메뉴: 낙지볶음, 낙지새우볶음, 낙지곰창볶음, 낙지곰창새우볶음밥
- (2) 착한 집밥 주요 메뉴: 착한정식, 제육정식, 불고기정식, 생선구이정식, 돈까스정식
- (3) 한식당 주요 메뉴: 순두부찌개, 된장찌개, 비빔밥, 등심돈까스, 차돌된장찌개, 육개장, 생선구이, 떡갈비

#### [이용안내]

- 명찰 내 중식 쿠폰을 제시하시면 식사 가능합니다.
- 식권 금액: 13,000원 기준으로 이용 가능합니다.





행운의 주인공은 바로 당신!

# 경품 안내

참석해 주신 여러분께 감사드리며,  
경품 추첨을 통해 푸짐한 선물을 드립니다!



일시

2026년 5월 7일(목)  
개회식 종료 후  
(개회식 16:50~17:30)



장소

3층 5A홀

## 경품 내역

경 품	수 량
아이패드 에어	1
갤럭시워치8 (44mm)	1
갤럭시버즈4 프로	2
에어팟4	3
갤럭시버즈4	3
스타벅스 상품권	10
<b>총 수량</b>	<b>20</b>



경품 추첨은 현장 참석자에 한해 진행됩니다.  
추첨 시 본인 확인 후 경품을 수령하실 수 있습니다.

한국정보보호학회 2026년 하계학술대회

# CISC-S'26

Conference on Information Security and Cryptography Summer 2026

2026년 5월 7일(목)~8일(금) | 부산 벡스코 제2전시장 1층/3층