한국정보보호학회
Korea Institute of Information Security & Cryptology

2025년 한국정보보호학회 하계학술대회

CISC-S'25

Conference on Information Security and Cryptography Summer 2025

2025년 6월 24일(화) ~ 25일(수)

더케이호텔 경주

주최·주관 한국정보보호학회 Korea Institute of Information Security & Cryptology

후원 국가정보원 NATIONAL INTELLIGENCE SERVICE, 과학기술정보통신부, 행정안전부, KISA 한국인터넷진흥원, ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute, NSR 국가보안기술연구소 National Security Research Institute, KiSTi 한국과학기술정보연구원 Korea Institute of Science and Technology Information www.kisti.re.kr, 대신정보통신(주), 시너지온, 아이티센 피엔에스, SK broadband, LG유플러스, EUNICE

위원회

학술대회장

한국정보보호학회 회장 박영호 (세종사이버대학교)

운영위원회

- 운영위원장: 김창훈 (대구대학교)
- 운영위원: 김정녀 (한국전자통신연구원), 오진영 (한국인터넷진흥원), 윤종희 (영남대학교), 송중석 (한국과학기술정보연구원), 한대완 (국가보안기술연구소)

프로그램 위원회

- 프로그램위원장: 이문규 (인하대학교)
- 프로그램위원: 곽 진 (아주대학교), 구형준 (성균관대학교), 권태경 (연세대학교), 김도훈 (경기대학교), 김득훈 (아주대학교), 김성욱 (서울여자대학교), 김종성 (국민대학교), 김태성 (충북대학교), 김형식 (성균관대학교), 김호원 (부산대학교), 김휘강 (고려대학교), 노희준 (인하대학교), 류권상 (공주대학교), 박승현 (한성대학교), 박종환 (상명대학교), 변진욱 (평택대학교), 서민혜 (덕성여자대학교), 서승현 (한양대학교), 서지원 (단국대학교), 양대헌 (이화여자대학교), 유지현 (광운대학교), 윤주범 (세종대학교), 이경률 (목포대학교), 이덕규 (서원대학교), 이병영 (서울대학교), 이선우 (서울여자대학교), 이윤경 (한국전자통신연구원), 이종혁 (세종대학교), 이창훈 (서울과학기술대학교), 이현우 (한국에너지공과대학교), 장진수 (충남대학교), 정익래 (고려대학교), 최대선 (숭실대학교), 최원석 (고려대학교), 허준범 (고려대학교), 홍석희 (고려대학교), 김수현 (순천향대학교), 곽병일 (고려대학교), 권동현 (부산대학교), 권현수 (인하대학교), 김동우 (동국대학교), 김범현 (한양대학교), 김종길 (이화여자대학교), 김진우 (광운대학교), 김현일 (조선대학교), 김형종 (서울여자대학교), 김환국 (국민대학교), 김희석 (고려대학교), 도경화 (서강대학교), 박기웅 (세종대학교), 박정수 (강남대학교), 박철준 (경희대학교), 서대희 (상명대학교), 서석충 (국민대학교), 서정택 (가천대학교), 서화정 (한성대학교), 유일선 (국민대학교), 윤명근 (국민대학교), 윤택영 (단국대학교), 이광수 (세종대학교), 이만희 (한남대학교), 이석준 (가천대학교), 이세영 (강원대학교), 이일구 (성신여자대학교), 이 준 (한국과학기술정보연구원), 이태진 (가천대학교), 장대희 (경희대학교), 장항배 (중앙대학교), 주경호 (숭실대학교), 최선오 (전북대학교), 최윤호 (부산대학교), 홍득조 (전북대학교), 황성재 (성균관대학교)

(최)우수논문상

NO.	구분	상장	논문명	저자
1	최우수	과학기술정보통신부 최우수논문상	BPF 백도어 매직패킷 실시간 탐지 연구	손현기, 백승렬, 이윤호, 최영락, 장승현, 윤명근(국민대학교)
2	최우수	행정안전부 최우수논문상	SeekPass: DeepSeek 기반 패스워드 사전 생성 모델	최대호(서울과학기술대학교), 김역(전기정보기술연구소), 손기욱, 이창훈(서울과학기술대학교)
3	최우수	학회 최우수논문상	암호화 네트워크 트래픽의 탐지 가능성 확장을 위한 구조·행위 통합 분석 기법	이선우, 정혜란, 이태진(가천대학교)
4	우수	한국인터넷진흥원 원장상	악의적인 Registration Reject 메시지 기반 5G 단말 DoS 공격 연구	오범석, 김광민, 김덕우, 손민철, 오택경(KAIST), 박철준(경희대학교), 김용대(KAIST)
5	우수	한국인터넷진흥원 원장상	산업제어시스템 잠재적 사이버위협 탐지를 위한 하이브리드 모델 제안	이주현, 전승호, 서정택(가천대학교)
6	우수	한국전자통신연구원 원장상	RAN 데이터 기반 Autoencoder 이상 탐지 모델의 O-RAN 적용 및 성능 평가	이현지, 김환국(국민대학교)
7	우수	한국전자통신연구원 원장상	지식 그래프를 활용한 이해 가능한 적대적 이미지 탐지 방안 연구	김규영, 박소희, 최대선(숭실대학교)
8	우수	국가보안기술연구소 소장상	CKKS 기반 MultiMax 구현: 최신 동형 암호 Softmax 비교 연구	신호준, 김휘호, 최진아, 신재원, 한상훈, 코이 모티타, 이동환, 이윤호(서울과학기술대학교)
9	우수	국가보안기술연구소 소장상	제로 트러스트 기반 전기차 충전 인프라 보안 적용 방안	김태우, 송유래, 김득훈, 곽진(아주대학교)
10	우수	한국과학기술정보연구원 원장상	비프로파일링 환경의 분류 모델 기반오류 주입 공격 파라미터 생성 방안	김주환, 한동국(국민대학교)
11	우수	한국과학기술정보연구원 원장상	실제 오타 기반 타이포스쿼팅 패키지 생성과 탐지 회피	방수경, 김형식(성균관대학교)
12	우수	학회우수논문상	새로운 EP-PSU 방식에 관한 연구	김기환, 윤현지, 김수현, 이임영(순천향대학교)
13	우수	학회우수논문상	온디바이스 AI 시스템을 위한 Challenge-Response 기반 Remote Attestation 기술	강민정(숭실대학교), 나보림, 이승민, 조효진(연세대학교)
14	우수	학회우수논문상	KubeSmith: 클라우드 네이티브 환경의 보안 정책을 강화하기 위한 프레임워크	조치현, 박현준, 이승수(인천대학교)
15	우수	학회우수논문상	사이버 공격 유형 분석 기반 보안 로그 필드 경량화 방안 연구	김태현, 김태은, 오동환, 이새움, 최슬기, 김서연, 임준형(한국인터넷진흥원)
16	우수	학회우수논문상	Magecart 공격 시나리오 재현과 브라우저 아티팩트 기반 수사 증거 확보 가능성 연구	전예은, 김성민, 김학경(성신여자대학교)
17	우수	학회우수논문상	SupplyChainLang: 도메인 특화 언어를 이용한 MITRE 공급망 공격 패턴 모델링 언어 제안	정윤정, 이준희, 이만희(한남대학교)
18	우수	학회우수논문상	딥페이크 탐지 기술의 최신 연구 동향과 일반화 관점 분석	김예지, 황은비, 권태경(연세대학교)
19	우수	학회우수논문상	뱅크 충돌 최소화를 통한 GPU 기반 Camellia CTR 최적화 구현	엄시우, 송민호, 김상원, 서화정(한성대학교)
20	우수	학회우수논문상	디지털 포렌식을 위한 자동차 데이터 기반의 운전자 식별 알고리즘 제안	이서하, 사공상욱(계명대학교)

NO.	구분	상장	논문명	저자
21	우수	학회우수논문상	ARMv8 환경에서 Barrett Multiplication을 통한 Microsoft SEAL-Embedded 라이브러리 최적화	김채린, 김영범, 서석충(국민대학교)
22	우수	학회 우수논문상 (학부생)	SEIR 전염병 확산 모델을 활용한 AI Chatbot 기반 RPA 시스템 보안 위협 분석	손우영, 권순홍, 이종혁(세종대학교)
23	우수	학회 우수논문상 (학부생)	Android 환경에서 Naver Memo 아티팩트 분석 및 메모 재구성 연구	홍서현, 이용진, 박지수, 김종성(국민대학교)
24	우수	학회 우수논문상 (학부생)	Deepfake 피해자를 위한 실시간 Deepfake 불법 생성물탐지 및 제거요청 시스템 개발	박건우, 김원빈, 서대희(상명대학교)
25	우수	학회 우수논문상 (학부생)	CDS의 유연성 강화를 위한 Zero Trust Overlay 적용 제안	함상규, 김유진, 박정수(강남대학교)
26	우수	학회 우수논문상 (학부생)	클라우드 Shadow IT 위협 사례 분석을 통한 클라우드 리소스 스캐너 요구사항 도출	황혜경, 이지원, 백지은, 성아영, 최상훈, 박기웅(세종대학교)
27	우수	학회 우수논문상 (학부생)	StarPrint: 스타링크 취약점 분석 및 트랜스포머 기반 웹사이트 핑거프린팅 공격	강호성, 곽현정, 홍지우, 오세은(이화여자대학교)
28	우수	차세대 우수 여성과학자	Falcon Dynamic 버전에서의 ffSampling 고속화 기법	박현주, 이명훈, 장지훈(고려대학교), 김수리(성신여자대학교), 홍석희(고려대학교)
29	우수	차세대 우수 여성과학자	EMI 신호주입을 통한 PWM 기반 AC 충전 통신 조작 연구	김의진, 조현수, 최원석(고려대학교)
30	우수	차세대 우수 여성과학자	zk-LTARK 취약점을 개선한 UTXO 기반의 CBDC	남혜빈, 임준호, 정익래(고려대학교)

6월 24일(화)

시간	거문고AB홀 (본관 2층)	구두트랙1 거문고C홀 (본관 2층)	구두트랙2 가야금A홀 (본관 2층)	구두트랙3 가야금B홀 (본관 2층)	구두트랙4 가야금C홀 (본관 2층)	구두트랙5 가야금D홀 (본관 2층)	구두트랙6 향비파A홀 (본관 2층)	구두트랙7 해금홀 (본관 1층)	구두트랙8 남산홀 (신관 1층)
12:00~13:00	등록 (6/24 거문고홀 6/25 향비파B홀)								
13:00~14:30	좌장 1 : 서화정 (한성대) 좌장 2 : 장진수 (충남대) 좌장 3 : 박명서 (한성대)	좌장 : 조효진 (연세대)	좌장 : 유지현 (광운대)	좌장 : 김윤정 (한기대)	좌장 : 김지연 (대구대)	좌장 : 김원빈 (상명대)	좌장 : 구형준 (성균관대)	좌장 : 이세영 (강원대)	
	포스터1	(1-1) 인공지능 보안 1	(1-2) 여성과학자1	(1-3) 여성과학자2	(1-4) 여성과학자3	(1-5) 융합보안	(1-6) 인공지능/ 기타 정보보안	(1-7) 개인정보보호/ 데이터보안 1	
14:30~14:40	Break Time								
14:40~16:10	좌장 1 : 김환국 (국민대) 좌장 2 : 이덕규 (서원대) 좌장 3 : 최윤호 (부산대)	좌장 : 서승현 (한양대)	좌장 : 이만희 (한남대)	좌장 : 박철준 (경희대)	좌장 : 서화정 (한성대)	좌장 : 김득훈 (아주대)	좌장 : 윤주범 (세종대)	좌장 : 김현일 (조선대)	좌장 : 주경호 (숭실대)
	포스터2	(2-1) 인공지능 보안 2	(2-2) 소프트웨어 보안	(2-3) IoT/ CPS 보안 1	(2-4) 암호이론 및 구현 1	(2-5) 정보보호 표준/평가/ 인증/교육	(2-6) 디지털 포렌식 1	(2-7) 개인정보보호/ 데이터보안 2	(2-8) 네트워크/ 클라우드 보안 1
16:10~16:20	Break Time								
16:20~16:50	초청강연 (본관 2층 거문고C홀) 좌장: 이문규 (인하대) 세계 최고 AX 1등 강국을 위한 한국적 AX 전략과 정보보호/KT 김광동 CR실장(전무)								
16:50~17:20	정보보호 R&D 신규과제 발굴을 위한 기술수요 조사 안내/정보통신기획평가원 (본관 2 층 거문고C홀)								
17:20~18:20	개회식 및 (최)우수논문시상 (본관 2층 거문고C홀) 사회: 김창훈 (대구대) 국민의례 내빈소개 개회사 : 한국정보보호학회 박영호 회장 행사보고 (최)우수논문 시상 경품 추첨								
18:30~	만찬 (본관 2층 거문고AB홀)								

6월 25일(수)

시간	구두트랙1 가야금A홀 (본관 2층)	구두트랙2 가야금B홀 (본관 2층)	구두트랙3 가야금C홀 (본관 2층)	구두트랙4 가야금D홀 (본관 2층)	구두트랙5 향비파A홀 (본관 2층)	구두트랙6 해금홀 (본관 1층)	구두트랙7 남산홀 (신관 1층)
09:00~10:30	좌장 : 이현우 (한국에너지공대)	좌장 : 이일구 (성신여대)	좌장 : 이동재 (강원대)	좌장 : 김득훈 (아주대)	좌장 : 김원빈 (상명대)	좌장 : 이윤호 (서울과기대)	좌장 : 박정수 (강남대)
	(3-1) 인공지능 보안 3	(3-2) IoT/ CPS 보안 2	(3-3) 암호이론 및 구현 2	(3-4) 블록체인	(3-5) 디지털 포렌식 2	(3-6) 양자내성암호 1	(3-7) 네트워크/ 클라우드 보안 2
10:30~10:50	Break Time						
10:50~12:20	좌장 : 신지선 (세종대)	좌장 : 윤주범 (세종대)	좌장 : 김동찬 (국민대)	좌장 : 노희준 (인하대)	좌장 : 이준 (KISTI)	좌장 : 강유성 (ETRI)	좌장 : 이일구 (성신여대)
	(4-1) 인공지능 보안 4	(4-2) IoT/ CPS 보안 3	(4-3) 암호이론 및 구현 3	(4-4) 해킹과 취약점 분석	(4-5) 학부생 우수논문	(4-6) 양자내성암호 2	(4-7) 네트워크/ 클라우드 보안 3
12:20~13:30	중식 (본관 2층 에델바이스)						

2025년 6월 24일(화)

세션	논문번호	논문제목 (저자/소속)
13:00~14:30 (1-1) 인공지능 보안 1 좌장 : 조효진 (연세대)	88	Security Analysis of Agentic Communication Protocols: Model Context Protocol (MCP) and Agent-to-Agent (A2A) Yiyue Zhang, 김민석, 구형준(성균관대학교)
	63	Causal tracing 기반 소형 언어 모델의 지식 저장 구조 및 백도어 취약 지점 분석 최민영, 임창훈(조선대학교), 박경철(케이포시큐리티), 김현일(조선대학교)
	61	연합학습에서 미세조정 기법 기반 소형 언어 모델 학습 효율성 분석 김승한, 임창훈(조선대학교), 박경철(케이포시큐리티), 김현일(조선대학교)
	48	대화형 인공지능 서비스의 탈옥 보안 위협 평가 태인규, 김영안, 장대희(경희대학교)
	26	연합학습 환경에서의 적대적 훈련 동향 조규찬, 정수용(공주대학교), 김현일(조선대학교), 서창호, 류권상(공주대학교)
	116	지식 그래프를 활용한 이해 가능한 적대적 이미지 탐지 방안 연구 김규영, 박소희, 최대선(숭실대학교)
13:00~14:30 (1-2) 여성과학자 1 좌장 : 유지현 (광운대)	258	GraphQL 웹 서버 대상 유형별 취약점 퍼징 기법 연구 박미리, 지일환, 이주현, 서정택(가천대학교)
	203	QIDS: AI 기반 쇼어 코드 신드롬 분석 양자 침입 탐지 위비, 윤혜진, 이옥연(국민대학교)
	153	Attention 기반 Multimodal 분석 기법을 통한 IoT 악성코드 탐지성능 향상방안 연구 김아름, 이태진(가천대학교)
	24	Apple M3 캐시 구조 분석 및 부채널 공격 가능성 평가 김세린, 장혜란, 신영주(고려대학교)
	3	BMC 펌웨어 취약점 탐지를 위한 정적 분석 기법의 적용에 대한 고찰 이지혜, 박찬희, 신영주(고려대학교)
	187	Falcon Dynamic 버전에서의 ffSampling 고속화 기법 박현주, 이명훈, 장지훈(고려대학교), 김수리(성신여자대학교), 홍석희(고려대학교)
13:00~14:30 (1-3) 여성과학자 2 좌장 : 김윤정 (한기대)	303	생체인증의 신뢰성 확보를 위한 기술 동향 이미라(고려대학교), 박종환(상명대학교), 이동훈(고려대학교)
	209	zk-LTARK 취약점을 개선한 UTXO 기반의 CBDC 남혜빈, 임준호, 정익래(고려대학교)
	144	PHP 기반 웹 취약점 탐지를 위한 Fuzzing 동향 및 향후 연구 김민경, 주경호(숭실대학교)
	131	지능형 로봇 구성요소 기반 공격벡터 및 보안위협 분석 박가을, 서승현(한양대학교)
	121	화이트박스 암호 기술에 대한 최신 연구 동향 분석 백지우, 김인성, 김규상, 김희석, 홍석희(고려대학교)
	68	차원 확장에 강건한 병렬 처리 기반 동형암호 선형 회귀 학습 구조 조예나, 김형식(성균관대학교)

2025년 6월 24일(화)

세션	논문번호	논문제목 (저자/소속)
13:00~14:30 (1-4) 여성과학자 3 좌장 : 김지연 (대구대)	302	피싱 웹사이트의 생태계 분석 김예림, 김형식(성균관대학교)
	282	EMI 신호주입을 통한 PWM 기반 AC 충전 통신 조작 연구 김의진, 조현수, 최원석(고려대학교)
	261	합성 데이터 신뢰도 향상을 위한 최적 증강 기법 김유나, 김연진, 이일구(성신여자대학교)
	199	에어 갭 환경에서 고용량 정보 유출 공격을 위한 고차원 변조 기법 정예림, 김연진, 이일구(성신여자대학교)
	143	생성형 AI 프롬프트 보안을 위한 DistilBERT 기반 소스코드 내 민감 키워드 탐지 방안 연구 정주원(모아소프트, 광운대학교)
	94	보이스피싱 악용 COD 통화의 지터 기반 탐지 기법 노다영, 이상현, 임미래, 김지윤, 주경호(숭실대학교)
13:00~14:30 (1-5) 융합보안 좌장 : 김원빈 (상명대)	305	블루투스 취약점 악용을 통한 차량 인포테인먼트 시스템에서의 응용계층 Valet Attack 기법 연구 황혜정, 김다슬, 한미란(고려대학교)
	298	V2X 통신에서 양자 보안 달성을 위한 SQIsign 기반 경량 인증 체계 제안 한윤선, 서석충(국민대학교)
	287	자기지도학습을 활용한 가중치 기반 센서 융합 기법 전아영, 전유란, 이일구(성신여자대학교)
	220	제로 트러스트 기반 전기차 충전 인프라 보안 적용 방안 김태우, 송유래, 김득훈, 곽진(아주대학교)
	2	소프트웨어 정의 차량 환경을 위한 제로 트러스트 기반 보안 정책 프레임워크 변승민(경남대학교), 이학준(금오공과대학교)
13:00~14:30 (1-6) 인공지능/ 기타 정보보안 좌장 : 구형준 (성균관대)	277	효율적인 딥페이크 탐지를 위한 채널 어텐션 오토인코더 구현 안경덕, 김윤성, 김광태, 박원경, 하재철(호서대학교)
	270	BNN 추론 모델에 대한 화이트박스 공격 저항성 분석 염지훈, 신원근, 채민아, 김희석(고려대학교)
	267	AI 생성 코드 탐지 기술 동향 정희성, 김형식(성균관대학교)
	160	재번역 공격에 강인한 반복 인코딩 기반 텍스트 워터마킹 기법 이예인, 전유란, 이일구(성신여자대학교)
	152	XAI를 이용한 AI-agent 기반 자동화된 false alarm 처리 방안 연구 한태현, 이태진(가천대학교)
	85	비프로파일링 환경의 분류 모델 기반 오류 주입 공격 파라미터 생성 방안 김주환, 한동국(국민대학교)

2025년 6월 24일(화)		
세션	논문번호	논문제목 (저자/소속)
13:00~14:30 (1-7) 개인정보보호/ 데이터보안 1 좌장 : 이세영 (강원대)	136	오프라인 키오스크의 다크 패턴 적용 양상과 사용자 인지 한계에 대한 실증 연구 류나연, 이세영(강원대학교)
	117	브라우저 기반 비추출 키 증명을 이용한 MFA 우회 방지 기법 김지완, 최경식, 장대희(경희대학교)
	65	새로운 EP-PSU 방식에 관한 연구 김기환, 윤현지, 김수현, 이임영(순천향대학교)
	37	LLM 기반 템플릿 합성을 통한 비구조적 PII 탐지 학습 데이터셋 구축 김민규, 황성재(성균관대학교)
	227	본인확인서비스의 연계정보(CI) 처리 구조에서 발생하는 보안 취약점 분석 및 대응 방안 연구 권다운, 김경백(전남대학교), 송하영(한국인터넷진흥원)
	185	동형암호를 활용한 얼굴 식별 연구 동향 박윤수, 이문규(인하대학교)
14:40~16:10 (2-1) 인공지능 보안 2 좌장 : 서승현 (한양대)	92	대규모 언어 모델을 악용한 공격 기법 연구 동향 전미진, 권유정, 구형준(성균관대학교)
	161	양자 합성곱 층의 단층 성능 분석: 고전 및 양자 은닉층과의 비교 황윤재(고려대학교), 석병진(한성대학교), 홍석희(고려대학교)
	140	딥페이크 방어 방식의 분류와 기술적 한계 분석 이상윤, 이세영(강원대학교)
	119	LLM 기반 안전한 코드 생성을 위한 다단계 대응 기법 설계 채상준, 김형식(성균관대학교)
	107	온디바이스 AI 시스템을 위한 Challenge-Response 기반 Remote Attestation 기술 강민정(숭실대학교), 나보림, 이승민, 조효진(연세대학교)
	97	AgentBoard 기반의 세부적 분석 접근법을 활용한 머신러닝 보안 취약성 평가 프레임워크 제안 신준석, 장진혁, 최대선(숭실대학교)
14:40~16:10 (2-2) 소프트웨어 보안 좌장 : 이만희 (한남대)	279	COTS 바이너리의 1-day 취약점 탐지를 위한 Patch Presence Test 연구 양희동, 이정우, 우승훈(고려대학교)
	275	소프트웨어 공급망 보안 관행 준수 검증을 위한 블록체인 기술 적용 연구 이준희, 정윤정, 이만희(한남대학교)
	243	리눅스 커널 취약점 세대별 트렌드와 탐지기술 발전 조사 장수혁, 최상훈, 박기웅(세종대학교)
	240	사이버 공격 유형 분석 기반 보안 로그 필드 경량화 방안 연구 김태현, 김태은, 오동환, 이새움, 최슬기, 김서연, 임준형(한국인터넷진흥원)
	212	제로-오버헤드 프로파일링 도구 분석 및 벤치마크 적용 연구 박수진, 배대현, 김희석, 홍석희(고려대학교)
	19	Limitations of Automatically Generated API Specification for WordPress CMS Plugins: An Empirical Study Grace Ohiremen, 김범현(한양대학교)

2025년 6월 24일(화)

세션	논문번호	논문제목 (저자/소속)
14:40~16:10 (2-3) IoT/CPS 보안 1 좌장 : 박철준 (경희대)	171	TinyML을 활용한 침입 탐지 시스템(IDS) 연구 동향 분석 황지은, 김형식(성균관대학교)
	150	Transformer-MLP 앙상블을 활용한 AI 생성 MQTT 트래픽 탐지 기법 김병찬, 최선오(전북대학교)
	139	Zigbee 공격 시나리오 분석과 대응 방안 김정현, 이세영(강원대학교)
	49	상용 IoT 기기 대상의 전자기파 기반 시스템 모니터링 배대현, 박수진, 김희석, 홍석희(고려대학교)
	47	펌웨어 리호스팅 기술 한계점 분석 엄하은, 황성재(성균관대학교)
	7	ROS2 기반 로봇 시스템 퍼징 기술 연구 동향 분석 김진하, 유지현, 정우성, 윤주범(세종대학교)
14:40~16:10 (2-4) 암호이론 및 구현 1 좌장 : 서화정 (한성대)	309	RSA-OAEP 안전성 증명 이력에 관한 연구 김동현, 김동찬(국민대학교)
	308	테이블 참조 기반 화이트박스 구현 기법에 관한 연구 김예진, 김동찬(국민대학교)
	307	랜덤 오라클 모델과 양자 랜덤 오라클 모델에 관한 연구 박동현, 김동찬(국민대학교)
	306	이진 Goppa 부호의 Berlekamp-Massey 디코딩에 관한 연구 김민지, 김동찬(국민대학교)
	304	CKKS 기반 MultiMax 구현: 최신 동형 암호 Softmax 비교 연구 신호준, 김휘호, 최진아, 신재원, 한상훈, 코이 모티타, 이동환, 이윤호(서울과학기술대학교)
	254	ALTEQ의 HW/SW co-design 구현 최용렬, 이재석, 김영범, 서석충(국민대학교)
14:40~16:10 (2-5) 정보보호 표준/ 평가/인증/교육 좌장 : 김득훈 (아주대)	255	건강정보고속도로 사업의 정보보호 체계분석과 고도화 방안 연구 김동욱, 김수현(순천향대학교)
	224	제로트러스트 정책을 활용한 사이버 보안 프레임워크 설계 신인준(대구대학교), 권상오(포위즈시스템), 김창훈(대구대학교)
	164	MITRE ATT&CK – CAPEC을 적용한 사이버보안 훈련 행위 구조화 방법론 정상지, 주한익, 홍순좌(코어시큐리티), 박성일(워크포스에이아이)
	163	사이버보안 훈련 프로그램 자동 생성을 위한 시나리오 규격화 방법론 김창영, 주한익, 홍순좌(코어시큐리티), 박성일(워크포스에이아이)
	41	디지털 트윈 보안성 강화를 위한 표준 개선 방안 연구 김혜린, 권영우(경북대학교)
	31	중소기업 대상 ISMS-P 대응 쿠버네티스 통합 보안 진단 시스템 박도윤, 이형규, 임윤태, 이재환(네이버 클라우드 캠프, 이스트소프트)

2025년 6월 24일(화)

세션	논문번호	논문제목 (저자/소속)
14:40~16:10 (2-6) 디지털 포렌식 1 좌장 : 윤주범 (세종대)	76	Deepfake 악용 방지를 위한 GAN 방식의 스테가노그래피 기법 탐구 임한비, 이연준(한양대학교)
	35	안드로이드 환경에서의 애플리케이션 기반 안티 포렌식 아티팩트 김영석, 황성재(성균관대학교)
	13	macOS 환경에서의 Chrome 쿠키를 활용한 iCloud 데이터 수집 김대환, 김동인, 박명서(한성대학교)
	10	국방 사이버침해 사고 대응을 위한 디지털 포렌식 체계 구축 제안 : 정책과 기술의 융합적 접근 이창명, 한승호(국방기술진흥연구소)
	8	디지털 포렌식을 위한 자동차 데이터 기반의 운전자 식별 알고리즘 제안 이서하, 사공상욱(계명대학교)
	5	Windows 환경에서의 KakaoTalk, WhatsApp, LINE 앱의 암호화된 멀티미디어 파일 복호화 연구 안원석, 김한결, 위다빈, 김동인, 박명서(한성대학교)
14:40~16:10 (2-7) 개인정보보호/ 데이터보안 2 좌장 : 김현일 (조선대)	263	EAR알고리즘과 CNN을 활용한 졸음경고 디지털트윈 시스템 연구 이효민, 김현지, 김형종(서울여자대학교)
	223	A Hybrid Framework for Detecting Sensitive Information in Structured and Unstructured Enterprise Data. Khusnora Bakhtiyor Kizi Khusnora, Cho Nwe Zin Latt, 이경현(부경대학교)
	196	동형암호 기반의 트랜스포머 추론 연구 동향 송승준, 이문규(인하대학교)
	84	AI 기반 웹 콘텐츠 분석을 통한 암호화 압축파일 악성코드 탐지 및 차단 기술 개발 이성훈, 정대영, 김정환(네이버 클라우드 캠프, 이스트소프트)
	75	안전한 데이터 공유를 위한 교차 도메인 데이터 공유 기법에 관한 연구 윤성철, 조현아, 김수현, 이임영(순천향대학교)
	73	PDS 환경에서 집계형 프록시 재암호화 기법 연구 신재정, 김태훈, 김수현, 이임영(순천향대학교)
14:40~16:10 (2-8) 네트워크/ 클라우드 보안 1 좌장 : 주경호 (숭실대)	156	RAN 데이터 기반 Autoencoder 이상 탐지 모델의 O-RAN 적용 및 성능 평가 이현지, 김환국(국민대학교)
	138	CCS 기반 전기차 충전 통신 보안 연구 동향 박유희, 김주언, 최원석(고려대학교)
	132	Packet-Length is All You Need: 암호트래픽 앱 분류 손현기, 임중혁, 엄석현, 오주엽, 윤명근(국민대학교)
	81	암호화 네트워크 트래픽의 탐지 가능성 확장을 위한구조·행위 통합 분석 기법 연구 이선우, 정혜란, 이태진(가천대학교)
	44	거대 언어 모델을 활용한 코드형 인프라 생성에 대한 보안성 검토 연구 임예람, 유지원, 김성민(성신여자대학교)
	16	비지도 임베딩 기반 네트워크 트래픽 클러스터링을 활용한 Shadow IT 탐지 기법 서준호 김재석, 밀라티 프라티위, 윤건우, 김승혁, 정재영, 최두환, 최윤호(부산대학교)

2025년 6월 25일(수)

세션	논문번호	논문제목 (저자/소속)
09:00~10:30 (3-1) 인공지능 보안 3 좌장 : 이현우 (한국에너지공대)	208	LLM Safeguard 연구 동향 한지훈, 한미란(고려대학교)
	206	자동음성인식(ASR) 시스템에 대한 문장 타겟형 적대적 공격 구현 김윤성, 전서현, 안경덕, 하재철(호서대학교)
	198	FlowSpectrum을 활용한 암호화된 트래픽 분류 모델 성능 개선 연구 김찬형, 이브라히모바-나일라, 김태윤, 김가영, 배기태, 서주형, 윤종희(영남대학교)
	190	물리적 일관성을 이용한 자율 주행 차량 경로 예측 모델에 대한 적대적 공격 탐지 백진현, 최원석(고려대학교)
	179	점수 합 융합 기반 SASV에서 ASV와 CM 조합의 성능 검증 한성규, 정수환(숭실대학교)
	177	머신러닝 보안을 위한 허니팟 기반 방어 기법의 체계적 분류 유경빈, 김형식(성균관대학교)
09:00~10:30 (3-2) IoT/CPS 보안 2 좌장 : 이일구 (성신여대)	273	전장형 CPS 이상행동 탐지 기술 조사 하영빈, 최상훈, 박기웅(세종대학교)
	256	산업제어시스템 잠재적 사이버위협 탐지를 위한 하이브리드 모델 제안 이주현, 전승호, 서정택(가천대학교)
	237	RV에 대한 Stealthy attack 탐지 및 복구 연구 동향 김슬기, 이지원, 최원석(고려대학교)
	217	인공위성 통신 위협 및 보안 기술 연구 동향 박민서, 임우진, 장진수(충남대학교)
	207	Matter 커미셔닝 보안을 위한 사전 공유키 기반 컨트롤러 검증 체계 권순범, 한미란(고려대학교)
	11	우주기반 인프라의 사이버 위협 시나리오 분석 및 대응 모델링 제안 : 정책과 기술의 통합적 접근 이창명, 한승호(국방기술진흥연구소)
09:00~10:30 (3-3) 암호이론 및 구현 2 좌장 : 이동재 (강원대)	195	영 차분 기반 AES 분석을 위한 효율적 쌍 탐색 기법 이명규, 신한범, 김인성, 김선엽, 권동근(고려대학교), 홍득조(전북대학교), 성재철(서울시립대학교), 홍석희(고려대학교)
	180	ARM Cortex-M4 상에서의 SMAUG-T 다항식 곱셈 알고리즘 최적화 윤성우, 이석준(가천대학교)
	149	빠른 trial-division을 위한 개선된 GCD 알고리즘 우상원, 정윤혁, 최필주(부경대학교)
	133	블록암호 ARIA에 대한 비밀키 복구 블라인드 부채널 공격 이인훈, 김규상, 이정환, 김희석, 홍석희(고려대학교)
	34	뱅크 충돌 최소화를 통한 GPU 기반 Camellia CTR 최적화 구현 엄시우, 송민호, 김상원, 서화정(한성대학교)
	1	효율적인 암호화 연산을 위한 아키텍처별 병렬화 성능 분석 연구 : RISC-V vs x86 천혜수, 김성민(성신여자대학교)

2025년 6월 25일(수)

세션	논문번호	논문제목 (저자/소속)
09:00~10:30 (3-4) 블록체인 보안 좌장 : 김득훈 (아주대)	241	TPM 기반 ECC-DAA 익명 인증을 적용한 DAG-PBFT IoT 원장 설계 및 프로토타입 구현 김현준, 서화정(한성대학교)
	234	블록체인 상호운용성 확보를 위한 크로스 체인 프로토콜: 한계점 분석 및 대응 기법 김희찬, 이경윤, 손준영(부산대학교)
	202	블록체인을 활용한 xApp 인증 및 무결성 검증 보안 프레임워크 조남필, 박재형, 김지혜, 이종혁(세종대학교)
	151	생체 정보기반 비저장 개인 키 관리 체계 신수진, 신상욱(부경대학교)
	42	그래프 신경망 기반 암호화폐 자금 세탁 탐지 프레임워크 및 트리 앙상블 성능 향상 연구 권순홍, 손우영, 이종혁(세종대학교)
	25	선택적 코인 추적을 지원하는 이중 익명 오프라인 Mobile E-Cash Payment 조찬형, 최재현, 정익래(고려대학교)
09:00~10:30 (3-5) 디지털 포렌식 2 좌장 : 김원빈 (상명대)	231	부분 손실된 프린터 네트워크 트래픽을 활용한 출력물 복구 방법 조영효(서울과학기술대학교), 김역(전기정보기술연구소), 이창훈, 손기욱(서울과학기술대학교)
	155	폴라리스 오피스 대상의 클라우드 포렌식 기술 연구 위다빈, 김한결, 안원석, 신민석, 박명서(한성대학교)
	102	Magecart 공격 시나리오 재현과 브라우저 아티팩트 기반 수사 증거 확보 가능성 연구 전예은, 김성민, 김학경(성신여자대학교)
	93	온라인 메신저 디지털 증거 수집과 분석 방법 이수연, 율도쉬쿠자에브 샤크죠드, 구형준(성균관대학교)
	87	SeekPass: DeepSeek 기반 패스워드 사전 생성 모델 최대호(서울과학기술대학교), 김역(전기정보기술연구소), 손기욱, 이창훈(서울과학기술대학교)
	86	크리덴셜 마이그레이션을 활용한 MYBOX 탐색기 대상의 클라우드 포렌식 연구 김한결, 위다빈, 안원석, 최종윤, 박명서(한성대학교)
09:00~10:30 (3-6) 양자내성암호 1 좌장 : 이윤호 (서울과기대)	213	SQIsign의 상수 시간 구현 및 저사양 환경 구현을 위한 사원수 대수 원소의 정수 계수 상한 값 계산 김원, 이정환, 김현학, 강태훈, 허동회(고려대학교), 김수리(성신여자대학교), 홍석희(고려대학교)
	201	KPQC Lattice 기반 암호에 대한 HW/SW Codesign 구현 방법론 이재석, 김영범, 서석충(국민대학교)
	192	PQC 기반 하이브리드 인증서 표준 동향 분석 이여녕, 김제인, 서승현(한양대학교)
	188	양자내성암호에 대한 QAOA 기반 분석 연구 강태훈, 전찬호, 허동회(고려대학교), 석병진(한성대학교), 이동재(강원대학교), 홍석희(고려대학교)
	51	ARMv8상에서의 격자 기반 암호 최적 구현 연구 동향 이민우, 심민주, 엄시우, 송경주, 윤세영, 서화정(한성대학교)
	30	ML-KEM 대상 부채널 공격 동향 분석 정윤혁, 우상원, 최필주(부경대학교)

2025년 6월 25일(수)

세션	논문번호	논문제목 (저자/소속)
09:00~10:30 (3-7) 네트워크/ 클라우드 보안 2 좌장 : 박정수 (강남대)	214	Opentelemetry와 Elastic APM의 관측성(Observability) 기능 비교 연구 지동혁, 최상훈, 박기웅(세종대학교)
	204	다크웹 트래픽 탐지 연구 동향 전주혁, 한미란(고려대학교)
	189	임베디드·IoT 환경을 위한 TLS 1.3 경량화 기법 동향: 인증서 오버헤드 감소 및 핸드셰이크 경량화 고세화, 이범수, 손준영(부산대학교)
	183	5G NGAP 프로토콜 구조 및 취약점 분석 나승준, 김진하, 김환국(국민대학교)
	172	5G 특화망 NF 보안 점검을 위한 NGAP 퍼징 도구 설계 김진하, 나승준, 김환국(국민대학교)
	169	KubeSmith: 클라우드 네이티브 환경의 보안 정책을 강화하기 위한 프레임워크 조치현, 박현준, 이승수(인천대학교)
10:50~12:20 (4-1) 인공지능 보안 4 좌장 : 신지선 (세종대)	262	오류 주입 공격 위치에 따른 DNN 모델의 오분류 영향도 평가 김수형, 이상원, 하재철(호서대학교)
	260	AI기반 C&C서버 공격 탐지 및 유형 분류를 위한 탐지 모델 제안 서정규, 이주현, 서정택(가천대학교)
	259	암호화 트래픽 대상 통계 및 바이트 스트림 활용 멀티모달 기반 이상 탐지 기법 제안 지일환, 이주현, 서정택(가천대학교)
	226	딥페이크 탐지 기술의 최신 연구 동향과 일반화 관점 분석 김예지, 황은비, 권태경(연세대학교)
	222	LLM 기반 웹 API 침입 탐지 시스템 성능 실험 연구 김영재, 아디줄리아완, 김보남, 유일선(국민대학교), 이준용, 김명철(펜타시큐리티)
	210	LLM 오픈소스 데이터셋 신뢰성 확보를 위한 데이터 중심 평가 동향 분석 김규환, 권태경(연세대학교)
10:50~12:20 (4-2) IoT/CPS 보안 3 좌장 : 윤주범 (세종대)	271	블록체인을 활용한 합성 데이터 프레임워크의 장단점 분석 정은혜, 이경현(부경대학교)
	257	미국 차세대원자로 사이버보안 규제 지침 분석을 통한 국내 개선 방향 제시 고아름, 이주현, 이철권, 서정택(가천대학교)
	229	보안 솔루션 및 제로트러스트 솔루션 연동을 위한 통합연동 API에 관한 연구 최슬기, 김태은, 이새움, 김태현, 김서연, 오동환, 임준형(한국인터넷진흥원)
	194	다계층 상호연동 아키텍처(MLIA)를 통한 API 신뢰성, 보안성 제고에 관한 연구 오동환, 최슬기, 김태현, 김서연, 이새움, 김태은(안국인터넷진흥원), 곽진(아주대학교)
	174	SupplyChainLang: 도메인 특화 언어를 이용한 MITRE 공급망 공격 패턴 모델링 언어 제안 정윤정, 이준희, 이만희(한남대학교)
	32	사이버 공격 선제 대응을 위한 기업형 사이버 위협 인텔리전스 플랫폼 설계 제안 이동주(현대오토에버)

2025년 6월 25일(수)

세션	논문번호	논문제목 (저자/소속)
10:50~12:20 (4-3) 암호이론 및 구현 3 좌장 : 김동찬 (국민대)	197	Mordell 타원 곡선의 동형 곡선 활용 동적 S-box를 적용한 ARIA 암호 알고리즘에 대한 분석 이경민, 황연정, 손준영(부산대학교)
	290	GPU 환경에서의 MAYO 병렬 최적화 방안 분석 최준혁, 김동천, 서석충(국민대학교)
	288	ARMv8 환경에서 Barrett Multiplication을 통한 Microsoft SEAL-Embedded 라이브러리 최적화 김채린, 김영범, 서석충(국민대학교)
	278	Jasmin을 통한 고신뢰·고속 암호 알고리즘 어셈블리 코드 생성에 관한 연구 지용현, 서석충(국민대학교)
	239	동형암호를 활용한 비이진 데이터에 대한 안전한 패턴 매칭 문정훈, 김동우(동국대학교)
	289	CPU-GPU 혼합구조 기반 AFFT 최적 구현 연구 김동천, 서석충(국민대학교)
10:50~12:20 (4-4) 해킹과 취약점 분석 좌장 : 노희준 (인하대)	211	대규모 언어 모델을 활용한 바이너리 코드의 메모리 취약점 탐지 최영호, 최두호(고려대학교)
	191	BPF 백도어 매직패킷 실시간 탐지 연구 손현기, 백승렬, 이윤호, 최영락, 장승현, 윤명근(국민대학교)
	186	실제 오타 기반 타이포스쿼팅 패키지 생성과 탐지 회피 방수경, 김형식(성균관대학교)
	50	대규모 언어 모델을 활용한 Closed-Source 환경의 Patch Diffing 자동화 방안 제안 최현진, 김영안, 장대희(경희대학교)
	38	MCP를 활용한 Fuzz Driver 및 Seed 생성 자동화 김민수, 최경식, 장대희(경희대학교)
	20	대규모 언어 모델 기반 취약점 분석 기술 동향 분석 황시준, 이연준(한양대학교)
10:50~12:20 (4-5) 학부생 우수 논문 좌장 : 이준 (KISTI)	162	CDS의 유연성 강화를 위한 Zero Trust Overlay 적용 제안 함상규, 김유진, 박정수(강남대학교)
	130	클라우드 Shadow IT 위협 사례 분석을 통한 클라우드 리소스 스캐너 요구사항 도출 황혜경, 이지원, 백지은, 성아영, 최상훈, 박기웅(세종대학교)
	124	StarPrint: 스타링크 취약점 분석 및 트랜스포머 기반 웹사이트 핑거프린팅 공격 강호성, 곽현정, 홍지우, 오세은(이화여자대학교)
	43	SEIR 전염병 확산 모델을 활용한 AI Chatbot 기반 RPA 시스템 보안 위협 분석 손우영, 권순홍, 이종혁(세종대학교)
	36	Deepfake 피해자를 위한 실시간 Deepfake 불법 생성물탐지 및 제거요청 시스템 개발 박건우, 김원빈, 서대희(상명대학교)
	9	Android 환경에서 Naver Memo 아티팩트 분석 및 메모 재구성 연구 홍서현, 이용진, 박지수, 김종성(국민대학교)

2025년 6월 25일(수)

세션	논문번호	논문제목 (저자/소속)
10:50~12:20 (4-6) 양자내성암호 2 좌장 : 강유성 (ETRI)	272	Isogeny 기반 암호에서의 유한체 연산 최적화 연구 동향 김민기, 서석충(국민대학교)
	266	ML-DSA Dilithium에 대한 오류 주입 공격 분석 이상원, 김수형, 하재철(호서대학교)
	248	SROS 2에서의 PQC적용 시 고려사항 지찬웅, 김제인, 서승현(한양대학교)
	228	PIPO에 대한 저지연 하드웨어 1차 마스킹 한재승(국민대학교), 김연재(LIG넥스원), 한동국(국민대학교)
	218	KpqC AIMer에 대한 단일 파형 공격을 통한 비밀키 복구 김규상, 김희석, 홍석희(고려대학교)
	215	양자 이득을 위한 도메인별 연구 및 기술 동향 신다윗, 조재한, 김호원(부산대학교)
10:50~12:20 (4-7) 네트워크/ 클라우드 보안 3 좌장 : 이일구 (성신여대)	268	5G 로밍 환경에서의 제어 평면 서비스 거부 공격 취약성 실증 원태호, 아벨라빈센트, 김보남, 유일선(국민대학교)
	238	O-RAN 환경에서의 SCTP 취약점 활용 보안 위협 목정현, 이석준(가천대학교)
	219	CL-OTC: UAV 환경에서 LoRa 은닉 채널 기반의 OneTime-Command 프레임워크 구현 허남정, 최상훈, 박기웅(세종대학교)
	125	유한 상태 기계를 활용한 이동통신망 취약점 및 보안 패치 모델링 기법 김동혁, 백승진, 남호철, 강민석(KAIST)
	96	악의적인 Registration Reject 메시지 기반 5G 단말 DoS 공격 연구 오범석, 김광민, 김덕우, 손민철, 오택경(KAIST), 박철준(경희대학교), 김용대(KAIST)
	58	제로트러스트 아키텍처(ZTA)환경에서의 패스워드리스 인증 통합 방안 고찰 진승헌, 김수형(한국전자통신연구원)

2025년 6월 24일(화)

세션	논문번호	논문제목 (저자/소속)
13:00~14:30 포스터 1 좌장 1 : 서화정 (한성대) 좌장 2 : 장진수 (충남대) 좌장 3 : 박명서 (한성대)	137	CVSS 지표 분류 자동화 모델의 알고리즘 적합성 박준혁, 강현성, 이재희, 류권상, 안효범(공주대학교)
	126	Rust 프로그래밍 언어의 비안전 영역 보안 기법 동향 전형준, 엄지용, 구형준(성균관대학교)
	123	검증 데이터 튜닝을 통한 모델 중독 공격 탐지 연구 류상범, 박소희, 최대선(숭실대학교)
	122	AI 기반 Anomaly Detection 시스템의 오탐 감소 연구 동향 유진호, 조효진(연세대학교)
	120	중소기업 환경에 적합한 비용 효율적 제로트러스트 보안 모델 개발 및 적용 방안 안효빈, 김범준, 이동재(강원대학교)
	118	텔레그램 사기 행위 분석을 위한 TF-IDF 기반 키워드 추출 연구 박규나, 유은선, 김성민(성신여자대학교)
	115	Tamarin을 사용한 암호 프로토콜 정형 분석 연구 동향 박현빈, 주경호(숭실대학교)
	114	다양한 노이즈를 활용한 SSL 기반 오디오 딥페이크 탐지 모델의 견고성 평가 서지원, 정수환(숭실대학교)
	113	AI 보안 관점에서의 인과성 활용 동향 분석 이지수, 이원호, 최대선(숭실대학교)
	112	소프트웨어 공급망 보안을 위한 오픈소스 VEX 도구 분석 이정호, 이세영(강원대학교)
	111	블록암호 DNA-PRESENT에 대한 전체 라운드 선형 공격 강동우, 신한범, 홍석희(고려대학교)
	110	LamGuard: 서버리스 환경을 위한 LLM 기반 동적 검증 프레임워크 신창희, 이승수(인천대학교)
	109	딥보이스 위협 대응 기술 동향 김다인, 김승민, 최대선(숭실대학교)
	108	Embedded Jailbreak Template : 유해 질의 삽입을 통한 LLM 탈옥 벤치마크 개선 기법 김하준, 강경문, 이채린, 최대선(숭실대학교)
	106	LLM Hallucination 평가 방법에 대한 분류 및 비교 권석재, 이세영(강원대학교)
	104	모바일 환경에서의 큐싱(Qshing) 공격 방지를 위한 실시간 머신러닝 기반 탐지 시스템 구현 이시언, 오나희, 이지원, 김기성(대구카톨릭대학교)
	103	한국어 LLM 공격 탐지 모델 성능 비교: 머신러닝, 파인튜닝, 후처리 기법 중심으로 장수원, 박제혁, 이광진, 이산하, 윤주범(세종대학교)
	101	단안 깊이 추정 모델에 대한 적대적 공격 연구 동향 김지윤, 주경호(숭실대학교)

2025년 6월 24일(화)

세션	논문번호	논문제목 (저자/소속)
13:00~14:30 포스터 1 좌장 1 : 서화정 (한성대) 좌장 2 : 장진수 (충남대) 좌장 3 : 박명서 (한성대)	100	MCP-A2A 기반 에이전트 협업형 보안 자동화 프레임워크 김경회, 김이든, 이세영(강원대학교)
	99	자율주행 시스템 경로 계획 기능 테스팅을 위한 커버리지 기반 테스트 스위트 생성 문지환(한양대학교), 김도현, 우상민, 김용대(KAIST)
	98	다크웹 탐지기법 기반 딥웹 이상 트래픽 탐지 시스템 개발 차한솔, 신문경, 김종현(세종대학교)
	95	연합학습 기반 인공지능 모델에 대한 공격 기법 분석 김송혜, 송일환, 유지현(광운대학교)
	90	스팸 메시지에서 불법 도박 링크 자동 추출을 위한 파이프라인 설계 김건우, 천정현, 민무홍(성균관대학교)
	89	웹 기반 도구를 활용한 딥페이크 이미지 탐지 프레임워크 김건우, 이정인, 민무홍(성균관대학교)
	83	AI 기반 정적 분석 및 시그니처 탐지를 결합한 크립토재킹 탐지 시스템 개발 연구 이찬영, 강요한, 조하선, 민준홍(네이버 클라우드 캠프, 이스트소프트)
	82	원격 의료 정보 시스템을 위한 사용자 인증 프로토콜에 대한 정형 검증 연구 강경아, 이주현, 김지윤(경상국립대학교)
	80	Active Directory 환경에서의 Pass-the-Hash 기반 측면 이동 기법 분석 김태영, 김연우, 김주환, 신준규, 서창진(상명대학교)
	79	OAuth 2.0 JWT 인증 시스템에서 NGINX Plus 도입 효과 분석 권선우, 남수민, 신예은, 김성민(성신여자대학교)
	78	안드로이드 사용자 앱 퍼징 연구 동향 및 기술적 챌린지 분석 강민주, 원신영, 전승호(가천대학교)
	77	LLM 기반 하네스 생성을 통한 퍼징 연구 동향 및 효과적 하네스 생성을 위한 요구사항 원신영, 강민주, 전승호(가천대학교)
	74	SDP 기반 분산된 환경에서 로그 및 패킷 기반 연합학습 이상탐지 방안 연구 우나륜, 임소미, 유지현(광운대학교)
	72	NSL— KDD 데이터셋 기반 머신러닝 모델의 성능 개선 방안 장홍서, 박성욱, 심춘보, 정세훈(순천대학교)
	71	LLM 기반 코드 난독화 해석 위협에 대한 암호화 기법의 대응 가능성 분석 조준환, 이동재(강원대학교)
	70	겸직·겸업 위반 대응을 위한 Hiworks 협업 도구 로그 분석 자동화 툴 개발 신민석, 위다빈, 박명서(한성대학교)
	69	ADS-B 시스템의 보안 위협 및 연구 동향 이상현, 주경호(숭실대학교)
	67	AsusWebStorage 사용자 데이터 수집 기법 김동인, 김대환, 박명서(한성대학교)

2025년 6월 24일(화)

세션	논문번호	논문제목 (저자/소속)
13:00~14:30 포스터 1 좌장 1 : 서화정 (한성대) 좌장 2 : 장진수 (충남대) 좌장 3 : 박명서 (한성대)	66	평생학습 기반 웹사이트 핑거프린팅 배주원, 신유진, 이서연, 오세은(이화여자대학교)
	64	연합학습에서의 백도어 공격 및 방어 기술 동향 황환민, 정수용, 류권상, 김현일, 서창호(공주대학교)
	62	연합학습 환경에서의 Triggerless Clean-label 백도어 공격 연구 임창훈, 김승한, 최민영, 김현일(조선대학교)
	60	불법 스포츠 스트리밍 사이트 탐지를 위한 텍스트 키워드 기반 랜덤 포레스트 모델 설계 최종윤, 김한결, 박명서(한성대학교)
	59	AI 실험 및 데이터 보호를 위한 AST 패턴매칭 활용 난독화 도구 안상준, 박혜연, 이석수, 노유정, 조은선(충남대학교)
	57	MITRE ATT&CK TTPs Capa-rule을 활용한 앙상블 기반 공급망 보안 강화형 악성코드 탐지 김나연(강원대학교), 김상훈(울산대학교), 이시언(대구가톨릭대학교), 임나현(울산대학교), 허라영(건국대학교)
	56	Gradient Inversion 공격 상황에서 강인한 Transformer 계열 구조에 대한 연구 김우철, 문채운, 백정은, 장진수(충남대학교)
	55	정밀도 향상을 위한 단어 조합 기반 LLM 프롬프트 필터링 기법 이산하, 이광진, 박제혁, 장수원, 윤주범(세종대학교)
	53	모바일 플랫폼 기반 카카오 T 아티팩트의 포렌식 분석 박수빈, 조서윤(전북대학교), 김도현(전주대학교), 이솔하, 홍득조(전북대학교)
	52	LLM을 활용한 보이스피싱 실시간 탐지 및 대응 연구 이정현, 최진우, 강평종, 이동호, 김진우(광운대학교)
	45	Bag-of-Bytes 모델을 활용한 딥웹 유사 구조 악성 URL 탐지 실험 신문경, 차한솔, 김종현(세종대학교)
	40	모델 컨텍스트 프로토콜(MCP) 기술 동향 및 보안 위협 분석 김이든, 이동재(강원대학교)
	39	보안 환경 내 DRL 적용 가능성 탐색을 위한 주요 연구 고찰 윤서웅(충남대학교)
	33	산업제어시스템(ICS)에 대한 제로트러스트 보안모델 적용 분석 및 연구 남보현, 강지민(한밭대학교), 노용훈(CYTUR)
	29	UML 기반의 Design SBOM 구현 유현아, 이만희(한남대학교)
	28	클라우드 오브젝트 스토리지 기반 개인정보 및 악성 파일 자동 탐지 시스템 개발 정지용, 이재윤, 신동엽, 정대영(네이버 클라우드 캠프, 이스트소프트)
	27	디지털 수사를 위한 ChatGPT 범죄 악용 가능성 평가 프레임워크 박승현, 유민정, 김성민(성신여자대학교)
	23	임베디드 시스템 대상 동적 분석 환경에서의 Unicorn 엔진을 활용한 코드 커버리지 개선 방법 연구 이재용, 조건영, 박경호, 이정주, 임강빈(순천향대학교)

2025년 6월 24일(화)		
세션	논문번호	논문제목 (저자/소속)
13:00~14:30 포스터 1 좌장 1 : 서화정 (한성대) 좌장 2 : 장진수 (충남대) 좌장 3 : 박명서 (한성대)	22	금융권에서의 LLM 및 AI 활용에 따른 위험 요소와 대응 방안 연구 김연우(상명대학교), 김민서(한밭대학교), 국봉호(대전대학교)
	21	키보드 음향 기반 패스워드 유추 공격 분석 연구 진규정, 이세영(강원대학교)
	18	딥페이크의 최신 탐지 기술 연구 동향 송민혁, 이연준(한양대학교)
	17	YOLO 기반 드론 탐지 모델의 적대적 공격 강건성 비교 양승원, 류다은(건국대학교)
	15	MAVLink 프로토콜을 사용하는 3DR Solo 드론 퍼징 황혜경, 이은진, 유지현, 윤주범(세종대학교)
	14	클라우드 기반 Google Workspace의 사용자 행위 추적을 위한 데이터 획득 연구 장규영, 위다빈, 박명서(한성대학교)
	12	Android 환경에서 인스턴트 메신저 KeeprChat의 암호화된 채팅 내역 복호화 연구 안현종, 이용진, 김현준, 김종성(국민대학교)
	6	난류 기반 진정 난수 생성기(TRNG)와 후양자 암호(PQC) 최지한(강릉원주대학교)
	4	제주 방언 기반 입력을 활용한 거대 언어 모델의 탈옥 공격 가능성 분석 서희영, 김경회, 이정호, 권석재, 이세영(강원대학교)

2025년 6월 24일(화)		
세션	논문번호	논문제목 (저자/소속)
14:40~16:10 포스터 2 좌장 1 : 김환국 (국민대) 좌장 2 : 이덕규 (서원대) 좌장 3 : 최윤호 (부산대)	181	소형 로봇 시스템에서의 영상 암호화 성능 분석 이상진, 김주언, 최원석(고려대학교)
	301	정적 코드 다형성과 루프 셔플링 하이딩 대응기법 결합 방안 및 분석 오성빈, 한재승, 한동국(국민대학교)
	300	다중 공개 키 인증서를 이용한 PQ-TLS 구현 방안 전원준, 이혜강, 기한결, 하재철(호서대학교)
	299	효율적인 3라운드 양자내성 비대칭 PAKE 프로토콜 김현서, 이예솔, 황리교, 손예원, 황정연(성신여자대학교)
	297	EVTX 로그의 손상된 데이터 복원을 위한 N-gram 기반 복구 프레임워크 지전일, 조금환(고려대학교)
	296	경량화된 룰 기반 랜섬웨어 조기 탐지 프레임워크 문정민, 김가영, 박나은, 이일구(성신여자대학교)
	295	위성 통신 보안 분석을 위한 자동화 도구 개발 박정식, 황선혁, 박철준(경희대학교)
	294	경량 블록 암호의 최적화를 위한 GPU 구현 연구 동향 송민호, 김상원, 서화정(한성대학교)
	293	에어갭 환경에서 전원선 변조 기반 암묵적 채널 공격에 대한 적응형 방어 시스템 김가영, 박나은, 이일구(성신여자대학교)
	291	AI 환경 내 암호 기반 보안 기술 적용 사례 분석 남영서, 김동천, 서석충(국민대학교)
	292	GPU 기반 다항식 곱셈 병렬 최적화 연구 고주희, 최준혁, 서석충(국민대학교)
	286	차량 외부 부착 재질에 따른 LiDAR 반사 강도 및 탐지 성능 분석 안채원, 최원석(고려대학교)
	285	TraceChain : 블록체인 기반 믹싱 탐지 시스템 이시온, 최경중, 양해정, 한희수, 윤주범(세종대학교)
	283	웹 CMS WordPress 취약점 동향 분석 및 대응 방안 이현우, 이동재(강원대학교)
	281	5G RACH 과정의 리소스 고갈 공격 시나리오 분석 및 LTE와의 비교 연구 이동원, 박철준(경희대학교)
	276	1라운드 강한 비대칭 PAKE 프로토콜의 구성 황리교, 손예원, 김현서, 이예솔, 황정연(성신여자대학교)
	269	트랜스포머 기반 비밀번호 추측 모델 연구 동향 전승현, 신원근, 김희석(고려대학교)
	264	공유기 펌웨어 보안 기술의 한계 식별 및 개선 방안에 대한 연구 최현서, 최희원, 서정택(가천대학교)

2025년 6월 24일(화)

세션	논문번호	논문제목 (저자/소속)
14:40~16:10 포스터 2 좌장 1 : 김환국 (국민대) 좌장 2 : 이덕규 (서원대) 좌장 3 : 최윤호 (부산대)	253	ARM 기밀 컴퓨팅 아키텍쳐에 대한 성능 분석 서영욱(한국에너지공과대학교), 황명하, 주정현, 강희운, 권유진(한국전력공사 전력연구원), 이현우(한국에너지공과대학교)
	252	LLM 기반 실시간 명령어 분석을 통한 사이버 디셉션 시스템의 구현과 실험 김도영, 김종현(세종대학교)
	251	부채널 분석을 이용한 하드웨어 트로이 목마 탐지 기술 동향 박예은, 신원근, 김희석(고려대학교)
	250	5G 시스템 내 키에 대한 NIST SP 800-57 기반 키 관리 정책 분석 우창현, 고용호, 김보남, 유일선(국민대학교)
	249	AutoEncoder 기반 트래픽 분석 기법의 동향 분석 김가영, 서주형, 김태윤, 배기태, 김찬형, 이브라히모바-나일라, 윤종희(영남대학교)
	247	역할극 기반 탈옥 공격에 대한 프롬프트 기반 방어 기법의 실효성 분석 이광진, 박제혁, 장수원, 이산하, 윤주범(세종대학교)
	246	NIST SP 800-53과 N2SF의 보안통제 체계 비교 박지민, 목정현, 이석준(가천대학교)
	245	워드프레스 취약점 동향 분석 박채우, 홍득조(전북대학교)
	244	PQNetSim: PQC 네트워킹 부하 측정 시뮬레이터 성하경, 강윤의, 김현주, 이현우(한국에너지공과대학교)
	242	차량 OTA에서 5G 기반 Network Slicing 기술의 도입 효과 분석 김주은, 박하민, 민준기, 원유빈, 허우원, 전상훈, 유일선(국민대학교)
	236	OT/ICS 환경에서 제로트러스트 구현을 위한 정책 중심 접근 분석 박소영, 목정현, 이석준(가천대학교)
	235	S-100 표준 적용에 따른 ECDIS GPS 신호 조작 위협 시나리오 분석: STRIDE 모델 기반 접근 이태용, 유인서(순천향대학교), 김주찬(동국대학교), 이규민(인하공업전문대학), 진형권(세종대학교), 양승권(중부대학교), 윤현빈(고려대학교), 노용훈(CYTUR), 이민우(국립한국해양대학교)
	233	S-100 표준 적용에 따른 ECDIS의 IP 인터페이스 사이버 위협 평가 방법론 연구 이태용, 유인서(순천향대학교), 김주찬(동국대학교), 이규민(인하공업전문대학), 진형권(세종대학교), 양승권(중부대학교), 윤현빈(고려대학교), 노용훈(CYTUR), 이민우(국립한국해양대학교)
	232	ObfusTree: 구조적 변형을 통한 구문 수준 코드 난독화 도구 조인우, 손지웅, 노형우, 조은선(충남대학교)
	230	BiSwert: 바이너리 프로그램에서 난독화 제어 구조를 식별하는 LLM 모델 박혜연, 손예진, 안상준, 조은선(충남대학교)
	225	V8 자바스크립트 엔진 취약점 동향에 대한 정량적 분석 공하랑, 서지원(단국대학교)
	221	웜 확산 사례 분석을 통한 확률론적 SEIR 모델 적용 및 시뮬레이션 강민채, 손우영, 권순홍, 이종혁(세종대학교)

2025년 6월 24일(화)

세션	논문번호	논문제목 (저자/소속)
14:40~16:10 포스터 2 좌장 1 : 김환국 (국민대) 좌장 2 : 이덕규 (서원대) 좌장 3 : 최윤호 (부산대)	216	A Blockchain-Based ESG Certification Framework for Cosmetic Product Refurbishment Cho Nwe Zin Latt, Sobirova Khusnora Bakhtiyor Kizi, 이경현(부경대학교)
	205	블록체인을 이용한 정보 보안 프레임워크에 대한 연구 강현성, 박준혁, 안효범(공주대학교)
	200	자기지도 학습 기반 암호화 트래픽 분류 모델의 어텐션 메커니즘 경량화 방안 분석 김태윤, 배기태, 김가영, 서주형, 김찬형, 이브라히보마-나일라, 윤종희(영남대학교)
	193	상호 위장 기반 MTD 모델의 시뮬레이션 및 게임이론적 평가 김준식, 김종현(세종대학교)
	184	위치 정보를 이용한 경량 원타임패스워드 기반 멀티 팩터 인증 기법 안예현, 이선진, 이일구(성신여자대학교)
	182	ROS2-fuzz++: ROS2 로봇 운영체제 퍼징 성능 향상 연구 서진우, 이성원, 오현규, 정우성, 유지현, 윤주범(세종대학교)
	178	피싱 기반 사이버 금융사기 동향 및 증거 수집 방안 : 중고거래 플랫폼을 중심으로 최승민, 엄예지, 김정우, 박정수(강남대학교)
	176	앙상블 모델을 고려한 ML-BOM 기술 방법론 제안 이준혁, 김지민, 이만희(한남대학교)
	175	프롬프트 분리·합산 및 오토인코더 보정 기반 적대적 프롬프트 방어 프레임워크 손재현, 류권상(공주대학교)
	173	MCP 아키텍쳐 보안 위협 분류 및 분석 황예인, 이민지, 최현우(성신여자대학교)
	170	유해 이미지 생성 방지를 위한 개념 제거 연구 동향 이재석, 안효범, 류권상(공주대학교)
	168	효율적이고 안전한 소그룹 통신을 위한 개선된 메시지 계층 보안 프로토콜 이가은, 이서진, 이일구(성신여자대학교)
	167	NFT 기반 전자책 소유권 증명과 샤미르의 비밀 분산을 통한 키 관리 허진혁, 이덕규(서원대학교)
	166	LWE 기반 암호 분석 기법 연구 동향 조사 김제빈, 강태훈, 전찬호(고려대학교), 김수리(성신여자대학교), 홍석희(고려대학교)
	165	ROS2-DDS 환경에서의 퍼징 아키텍처 제안 김재민, 이민재, 이보겸, 황덕연, 윤주범(세종대학교)
	159	스프링 시큐리티 기반 제로트러스트 초기 보안 모델 연구 이주현, 박정수(강남대학교)
	158	PyPI 패키지 건전성 검증 자동화를 위한 GitHub Actions 기반의 Custom Action 개발 조은정, 이만희(한남대학교)
	157	암호화 공격 트래픽 분석을 위한 딥러닝 모델의 성능 비교 연구 김태훈, 김환국(국민대학교)

2025년 6월 24일(화)		
세션	논문번호	논문제목 (저자/소속)
14:40~16:10 포스터 2 좌장 1 : 김환국 (국민대) 좌장 2 : 이덕규 (서원대) 좌장 3 : 최윤호 (부산대)	154	온라인 여론조사의 조작 방지를 위한 블록체인 기반 시스템 설계 및 구현 백승훈(순천향대학교), 이동주(개런터블), 김수현(순천향대학교)
	148	허니팟 자동화 방안: 디지털 트윈과 MITRE ATT&CK TTP 매핑을 통하여 박준영, 김종현(세종대학교)
	146	만료된 Access Token의 허니토큰화: 디셉션 기반 비인가 탐지 기법 연구 고남현, 김종현(세종대학교)
	145	얼굴 인식 분야의 딥러닝 모델 압축 기술 동향 분석 남윤창, 이문규(인하대학교)
	142	컨테이너 이미지에 대한 SBOM 생성의 일관성 분석 구시은, 현혜연, 박다연, 김성민(성신여자대학교)
	141	코퍼스 전이를 통한 상용 소프트웨어에 대한 바이너리 전용 퍼징 성능 향상 이동하, 전승호(가천대학교)
	135	로봇 청소기 네트워크 트래픽 분석을 통한 비의도적 영상 데이터 전송 탐지 모델 연구 박민제, 전희도, 최원석(고려대학교)
	134	δ-Tracer: 도커 이미지 델타 추적을 통한 위협벡터 탐색 프레임워크 우상민, 이재욱, 황대성, 장도원, 최상훈, 박기웅(세종대학교)
	129	정적 분석 기반 Call Offset 특징과 Dynamic Class weighting 손실 함수 조정 기법을 활용한 악성코드 패밀리 분류 유현준, 임소미, 유지현(광운대학교)
	127	제로데이 공격 대응 방안 연구 동향 최서연, 김진섭, 유지현(광운대학교)

학술대회 등록방법

[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		

- 등록비 포함사항 : 6/24(화) 만찬 , 6/25(수) 중식, 리플릿, 온라인 프로시딩, 기념품
- 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 1963년 12월 31일 이전 출생자로 학회 종신회원 분들에 한합니다.
- 회원혜택 기준은 행사 당일인 2025/6/25(수)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. (예시 : 한국인터넷진흥원, 한국전자통신연구원, 국가보안기술연구소 등)
- 대학원생은 전일제에 한합니다. (타소속 없음)
- 논문 한편 당 저자 한 분은 반드시 사전등록을 하셔야 합니다.

[사전등록]

- 학회 홈페이지(www.kiisc.or.kr)에서 접속할 경우, 학회행사 → 사전등록바로가기 → 학술행사 선택(2025 하계학술대회) 등록하기 선택
- 사전등록 마감일 :

– 논문 발표자 사전등록 : ~ 2025년 6월 2일(월) 까지

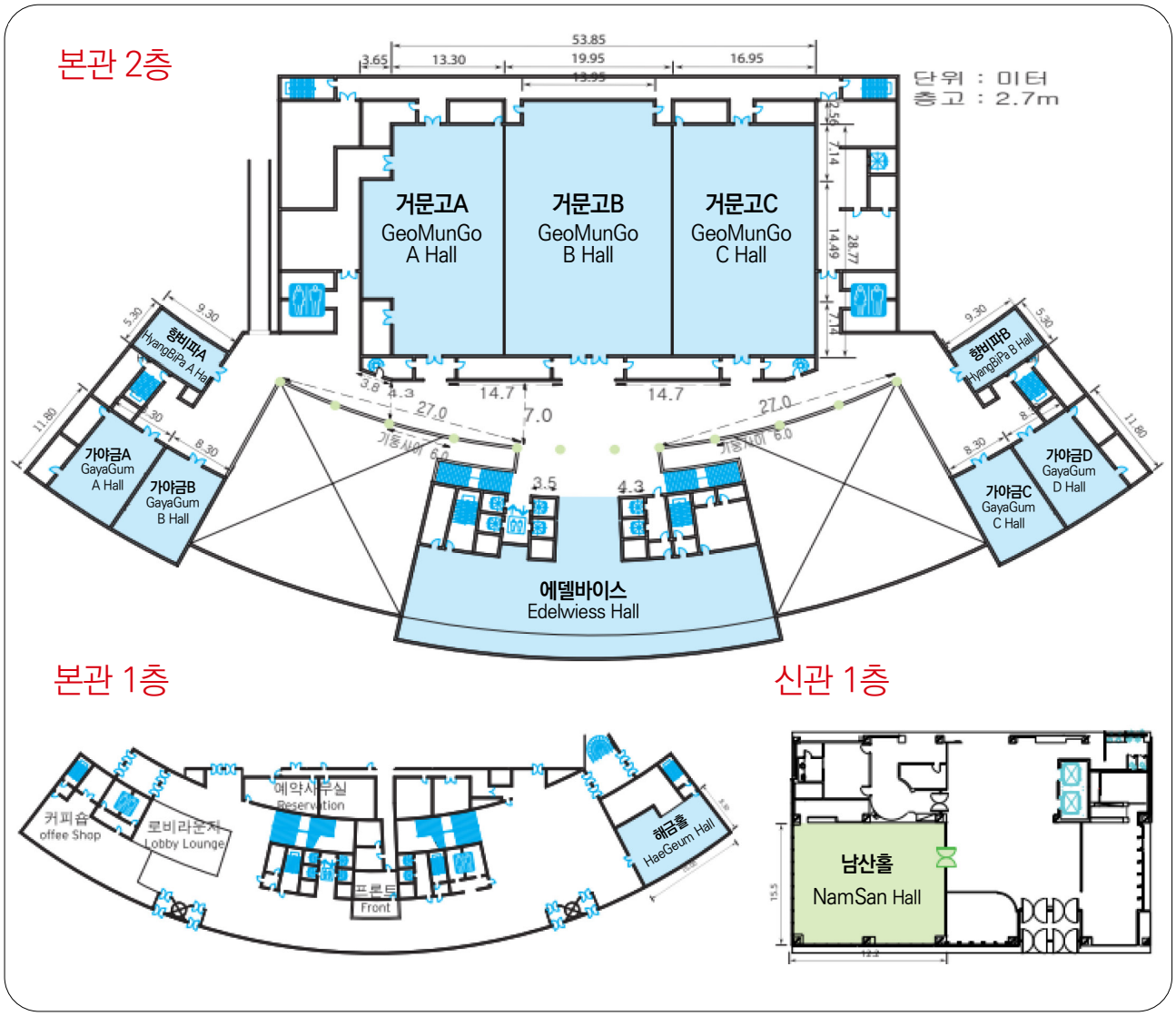
– 일반 참가자 사전등록 : ~ 2025년 6월 13일(금) 까지

- 계좌번호 : 국민은행 754-01-0008-146 (예금주 한국정보보호학회)
- 무통장 입금 결제 시 등록비는 위의 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 영수증 계산서가 필요하신 경우 미리 학회로 연락바랍니다.
- 입금명은 소속명으로만 기재하여 입금 시 확인이 되지 않습니다. 이에 등록 누락을 방지하고자 입금명은 필히 입금자 성함으로 기재해주시기 바랍니다.
- 등록확인서 및 참가확인서는 등록비 납부완료자에 한하여 한국정보보호학회 홈페이지 상단 "행사등록 및 참가확인서" 바로 가기를 클릭하신 후 등록 시 기재하신 성함과 이메일을 기재하시면 출력 가능합니다. (단, 참가확인서는 행사종료 후 다음날부터 발급 가능)

[문의처]

- 행사 문의처 : 한국정보보호학회 사무국 02-564-9333(내선2), kiisc@kiisc.or.kr
- 계산서 문의처 : 한국정보보호학회 사무국 02-564-9333(내선5), kiisc@kiisc.or.kr

[주요 행사 및 프로그램 장소 안내]



행사 내용	장소	위치
참가자 등록	6/24 거문고홀, 6/25 향비파B홀	본관 2층
구두세션	해금홀	본관 1층
	가야금홀, 향비파A홀	본관 2층
	남산홀	신관 1층
초청강연 IITP 사업소개 개회식 우수논문 시상식 경품추첨 (아이패드에어2개, 에어팟 8개)	거문고 C홀	본관 2층
포스터세션	거문고 AB홀	본관 2층

※ 개회식 종료 후 경품추첨이 진행될 예정입니다.

행사장소 안내

◈ 식사 제공 및 장소 안내

일자	내용	시간	장소	
6/24(화)	만찬	18:30~	거문고AB홀	본관 2층
6/25(수)	중식	12:20~	에델바이스	본관 2층

※ 명찰 뒷면의 식권 지참 후 해당 장소에서 식사

※ 주차안내: 학술대회 참가자 주차 무료

Memo

2025년 한국정보보호학회 하계학술대회

CISC-S'25

Conference on Information Security and Cryptography Summer 2025

2025년 6월 24일(화) ~ 25일(수) | 더케이호텔 경주