KIISC

정보보호학회논문지
"AI보안" 논문모집

최근 AI 보안에 대한 관심이 증가하고 있습니다. 통합관제, 네트워크 침입탐지, 악성코드탐지같이 그간 AI 기술이 많이 활용되어온 분야 뿐 아니라, 생체인증, 위협 인텔리전스, 프라이버시 보호 분야에도 AI 활용이 증가하고 있습니다. 한편, AI 자체를 위협하는 적대적 예제, 학습데이터 오염, 백도어 공격 등 여러 공격 유형이 지속적으로 보고되고 있고, 자율주행차, AI스피커 등 엣지 AI의 보급과 OT 환경에의 AI 도입 등 AI에 대한 보안 공격의 파급효과가 커지고 있습니다. 프라이버시에 관련해서는 AI 학습에 사용되는 학습데이터 뿐만 아니라, 챗봇 등 학습된 AI를 통한 민감정보 유출 등 위협도 그 다양성과 심각성을 더해가고 있는 동시에, 비정형 개인정보 탐지 등 AI를 활용한 보호 기술도 존재하는 상황입니다. 또한, AI를 활용한 공격이라고 할 수 있는 딥페이크 또한 많은 관심을 모으는 이슈입니다.

한국정보보호학회 논문지에서는 이러한 AI 보안의 여러 측면의 다양한 최신 기술을 공유하기 위해 "AI보안" 특별섹션을 만들었으며, 이를 통해 우리나라의 최근 연구 현황과 성과를 소개하고자 합니다. 관련 연구자들의 많은 관심과 투고를 부탁드립니다.

본 특별섹션으로 투고하시면 일반투고 비용으로 긴급 심사를 통해 신속하게 출간됩니다. 단, 수정보완 등의 사유로 발간준비가 지연되면 일반논문으로 처리될 수 있습니다.

1. 일정

- 논문제출 : 2022년 ~~2월 4일(금)까지~~ **2월 11일(금)까지** / *제출기한 연장
- 논문발간 : 2022년 4월호 게재
- 담당편집위원 : 최대선 교수 (숭실대학교, sunchoi@ssu.ac.kr)

2. 논문 모집분야

- AI-based security tools, techniques and procedures
- AI-based authentication
- AI-driven data security and privacy
- Big data analytics for cybersecurity
- Applications of AI in digital forensics
- AI-based cryptography, side channel analysis
- AI-driven harmful content detection
- AI-based cyberwar
- Adversarial attack and defense
- Trustworthy AI
- Edge, IoT, OT AI Security
- Deepfake
- Privacy preserving machine learning
- AI model privacy
- Intelligent CCTV, Etc.

3. 논문제출 절차: 한국정보보호학회 홈페이지 (http://kiisc.or.kr) 논문제출 클릭

⇨ KISTI 한글 논문 시스템 로그인

⇨ 논문투고 분야: **특별섹션 (AI보안)** 선택

⇨ 심사진행

4. 논문제출문의: [e-mail] kiisc@kiisc.or.kr, [Tel] 02-564-9333 (내선:3)

한국정보보호학회 논문지편집위원회