KIISC

정보보호학회논문지
“지능형사이버보안” 논문모집

디지털 시대로 전환되면서 기존 보안기술의 한계를 극복하고 인공지능(AI)과 빅데이터 등을 활용하여 보안기술을 고도화하거나 기존 보안기술을 자동화하는 등 지능형 사이버보안에 대한 기대가 커지고 있습니다. 그 대표적인 활용의 예로 AI를 활용해 사이버 공격에 대한 자동 감지 및 조기 차단을 하는 등 사이버 위협을 완화할 수 있습니다. 데이터 보안에서도 자동으로 보호 데이터를 처리 및 분류하고 데이터 처리과정의 투명성을 높이는데 AI를 활용할 수 있습니다. 그밖에 AI 기반 생체인증에서 보다 높은 차원으로 기술 활용이 이루어지고 있는가 하면 IT 보안업무의 자동화에 인공지능 기술을 적용하기도 합니다. 이와같이 끊임없이 진화하고 있는 사이버공격에 대응하고 예방하기 위해 기존 보안 기술의 자동화, 기술간 융합, 인공지능과 빅데이터 등을 활용한 보안 기술 고도화, 그리고 최신 보안 기술을 반영하는 보안 정책 등 지능형 사이버보안에 대한 연구는 시대적 흐름이라 할 수 있습니다.
한국정보보호학회 논문지에서는 이러한 지능형사이버보안의 다양한 최신 기술을 공유하기 위해 **“지능형사이버보안” 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 8월 12일(금)**~~ **8월 19일(금)까지** / *제출기한 연장
   - 논문발간 : 2022년 10월호 게재
   - 담당편집위원 : 김정녀 책임연구원 (한국전자통신연구원, jnkim@etri.re.kr)

2. 논문 모집분야
   - Intelligent System security
   - Intelligent Network security
   - Intelligent Security analysis
   - Intelligent Data-driven security and measurement studies
   - Privacy-enhancing technologies and anonymity
   - Intelligent Hardware security
   - Research on surveillance and censorship
   - Social issues and security intelligence
   - Intelligent Applications of cryptography
   - Related security education, management, law and policy, etc

3. 논문제출절차 : 한국정보보호학회 홈페이지 (http://kiisc.or.kr) “논문투고” 클릭
   ⇨ KISTI 한글 논문 시스템 로그인
   ⇨ 논문투고 분야: **특별섹션 (지능형사이버보안) 선택**
   ⇨ 심사 진행

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

한국정보보호학회 논문지편집위원회

《논문 모집분야 상세》

- Intelligent System security
  - Operating systems security
  - Web security
  - Mobile systems security
  - Distributed systems security
  - Cloud computing security

- Intelligent Network security
  - Intrusion and anomaly detection and prevention
  - Network infrastructure security
  - Denial-of-service attacks and countermeasures
  - Wireless security

- Intelligent Security analysis
  - Malware analysis
  - Analysis of network and security protocols
  - Attacks with novel insights, techniques, or results
  - Forensics and diagnostics for security
  - Automated security analysis of hardware designs and implementation
  - Automated security analysis of source code and binaries
  - Machine learning in a secure systems context
  - Program analysis

- Intelligent Data-driven security and measurement studies
  - Measurements of fraud, malware, spam
  - Measurements of human behavior and security

- Privacy-enhancing technologies and anonymity
  - Usable security and privacy
  - Intelligent Language-based security

- Intelligent Hardware security
  - Secure computer architectures
  - Embedded systems security
  - Methods for detection of malicious or counterfeit hardware
  - Side channels

- Research on surveillance and censorship

- Social issues and security intelligence
  - Research on computer security law and policy
  - Ethics of computer security research
  - Research on security education and training
  - Information manipulation
  - Online abuse

- Intelligent Applications of cryptography
  - Analysis of deployed cryptography and cryptographic protocols
  - Cryptographic implementation analysis
  - New cryptographic protocols with real-worldapplications

- Related security education management, law and policy, etc