"사이버 위협 인텔리전스" 특집호 발간에 즈음하여

사이버 위협 인텔리전스(Cyber Threat Intelligence)는 다양한 정보소스로부터 사이버위협 정보를 수집해 사이버보안 위협 상황을 분석하고 효과적으로 대응하는 방법론이다. 글로벌 IT 조사업체 가트너는 현존하거나 발생 가능한 위협에 대한 신속한 대응 결정을 위해 사이버위협정보, 메커니즘, 지표, 대응전략수립 등을 포괄하는 증거기반의 지식베이스로 정의하고 있으며, 이머징 기술 중에 하나이다.

그러나 새로운 ICT 기술을 기반한 디지털 대전환이 가속화 되는 과정에서 사이버공간의 영역이 경계가 없어지고 확장되고 있는 변화 과정 속에서 사이버공격에 활용되는 공격 도구, 공격 전술(TTP), 보안 취약점 정보 등 분석 대상의 확대와 복잡성 증대는 CTI 분석 역량을 현재보다 고도화하고 지능화하기 위한 기술 연구가 매우 중요하고 새로운 도전과제가 되고 있다. 본 특집호에서는 사이버위협인텔리전스 정보 수집, 분석, 생성, 활용, 공유 과정의 최신 연구와 국내 사이버침해사고대응 현장의 주요 이슈와 적용 사례를 집중적으로 다루었다.

첫 번째 원고는 코로나 19 팬데믹 환경에서 재택근무 등 비대면 환경에서 국가 과학기술분야의 핵심정보자산을 보호하기 위한 과학기술사이버안전센터에서 수행하고 있는 침해사고 데이터 분석과 사이버위협인텔리전스 분석 현황을 살펴보았다. 두 번째 원고는 사이버위협인텔리전스 정보를 수집하기 위한 다양한 정보 소스 중에서 급증하고 있는 네트워크 암호화 트래픽의 핑거프린팅 분석 사례에 대해서 소개하였다. 세 번째 원고는 사이버보안분야에 인공지능 기술을 활용하는 사례가 증가하면서, 인공지능 기반 보안기술에서 생성될 수 있는 사이버위협인텔리전스 정보를 효과적으로 해석하고 분석하기 위한 XAI 기술과 방법론에 관한 동향을 다루었다. 네 번째 원고는 한국인터넷진흥원 종합분석팀에서 수행하는 사이버위협인텔리전스 환경에서 보안위협 분석과 관련하여, MITRE TTP 기반 분석 및 활용 사례에 대해서 소개하였다. 다섯 번째 원고는 안보 관점에서 공개인텔리전스정보(OSINT)와 소셜인텔리전스(SOCMINT) 조사 분석의 한계와 극복방안을 제시하였다. 마지막 원고는 국내 사이버위협정보 공유 기술과 체계 현황을 분석하고 기술의 발전 방향에 대해서 고찰하였다.

끝으로 바쁘신 중에도 소중한 시간을 내시어 원고를 집필해 주신 집필자분들과 편집에 수고해 주신 학회지 편집 위원회, 그리고 학회 사무국 관계자 여러분께 감사를 드립니다.

2021년 10월

상명대학교 정보보안공학과 김환국