"공급망 보안" 특집호 발간에 즈음하여

2022년 10월에 발간된 공급망 보안 특별호 이후, 2년 반이라는 시간이 흘렀습니다. 그 사이 소프트웨어 공급망 보안 분야는 국내외적으로 중요한 변화를 맞이했습니다. 미국은 2021년 5월 발표된 행정명령 EO 14028을 기반으로 지속적인 보안 강화를 추진 해왔으며, 2024년 6월부터 연방정부 조달을 위한 Self-Attestation Form을 필수화하며 본격적으로 공급망 보안 체계를 적용하기 시작했습니다. 유럽연합(EU)도 강력한 공급망 보안 규정을 포함한 사이버 회복력법(CRA, Cyber Resilience Act)을 최종 통과시켜 2027년부터 시행을 앞두고 있습니다. 우리나라 역시 2024년 5월 소프트웨어 공급망 보안 가이드라인을 발표하며 공급망 보안 체계 구축을 본격화했으며, 같은 해 9월에는 다부처 태스크포스(TF)를 구성하여 공급망 보안 제도화 및 로드맵 수립을 진행 중입니다. 나아가 2025년 1월에는 디지털 의료기기 전자적 침해행위 보안 지침이 발표되며, 의료기기 분야에서도 공급망 보안의 필요성이 강조되고 있습니다.

초기 공급망 보안이 국내외에 소개될 때는 매우 생소한 내용이었고, 적용되는 분야도 한정적이었습니다. 초기에는 새로운 개념인 소프트웨어 자재명세서인 SBOM에 대한 관심이 높았고 적용되는 분야도 일반적인 소프트웨어에 대한 내용으로 한정되었습니다. 하지만 지금은 SBOM을 넘어서 이를 어떻게 생산하고 유통하고 활용할 것인가에 대해 관심이 확장되었고, 소프트웨어 범위도 일반 소프트웨어에서 의료SW, 자동차SW, 클라우드SW로 점차 확대되고 있습니다.

이에 본 특별호에서는 최근 공급망 보안의 최근 변화들에 대한 내용을 소개합니다. 먼저 SBOM과 관련하여 SBOM을 생산하는 연구 동향을 소개합니다. 고려대 우승훈 교수 연구팀은 소프트웨어의 구성요소를 분석하기 어려운 여러 난제들을 소개하고 이를 해결하려는 연구들을 소개합니다. ETRI의 강동호 실장 연구팀은 특히 바이너리 형태의 소프트웨어로부터 인공지능 기술을 이용하여 SBOM을 생성하는 연구에 대해 소개합니다. 한남대 이만희 교수 연구팀에서는 우리나라 SW 공급망 보안 가이드라인에서 제시되었던 NIS-SBOM을 CycloneDX와 SPDX를 이용해 구현하는 방안을 제시합니다.

전술한 것과 같이 소프트웨어 공급망 보안은 일반 소프트웨어에서 다양한 소프트웨어로 확대되고 있습니다. 본 특별호에서는 의료, 자동차, 클라우드 분야에 대한 기고문을 싣고 있습니다. 먼저 LG전자의 권중한 리더는 자동차 분야에서 공급망 보안의 중요성, 해외 정책 동향을 소개하고, 바람직한 자동차 소프트웨어 공급망 보안 관리체계를 제시합니다. KTC의 방지호 본부장은 국내외 의료분야 SW의 공급망 보안을 꼼꼼히 소개합니다. 특히 2025년 1월까지 피드백을 받은 우리나라 의료SW의 공급망 보안 분야 지침을 소개하는 등 최신 분야의 내용을 소개하고 있어 디지털 의료제품 제작자들과 일반 SW 제작자들에게 매우 도움 될 것으로 예상됩니다. 그리고 세종대의 박기웅 교수 연구팀에서는 클라우드에서의 공급망 보안 이슈에 대한 다양한 보안 사건과 그에 대한 대응책을 소개하고 있습니다. 클라우드의 중요도에 비해 클라우드 공급망 보안은 아직 덜 주목받고 있는 상황에서 매우 유용한 논문으로 판단됩니다.

본 소프트웨어 공급망 보안 특별호의 마지막 피날레는 LG전자의 김경애 연구위원의 오픈소스를 이용한 공급망 보안 관리에 대한 기고문입니다. LG전자는 오래전부터 라이선스와 공급망 보안을 전사적으로 관리하여 모범적인 기업 혁신을 이루었지만, 그 솔루션 인 FOSSLight를 오픈소스로 공개하여 학계 및 산업계에도 매우 긍정적인 영향을 주고 있습니다. LG전자는 이에 그치지 않고 오소리 프로젝트를 통해 삼성전자, 카카오, 한국저작권위원회오 함께 누구든지 활용할 수 있는 오픈소스 데이터베이스를 구축하고 서비스하고 있습니다. 본 고에서는 기존 FOSSLight와 오소리 프로젝트를 이용한 소프트웨어 공급망 보안 관리 방안을 제시합니다.

우리나라의 공급망 보안 수준은 어디까지 와 있는가 생각 해봅니다. 우리나라가 공급망 보안을 세계적으로 이끈다거나 세계적 모범이 되고 있다는 것을 뚜렷이 느끼지는 못하고 있습니다. 하지만 우리나라에는 세계적 수준의 연구 논문을 작성하는 연구 그룹이 있고, Gartner에서 매우 호평하는 공급망 보안 기업이 있습니다. 또한 세계에서 세 번째로 정부에서 작성한 SW공급망 보안 가이드라인을 작성했고 지금은 공급망 보안의 제도화를 위해서 국가 단위의 태스크포스를 운영하여 로드맵을 작성 중에 있습니다. 시작도 그리 늦지 않았고, 소프트웨어 공급망 보안에 대한 국가적, 기업적 관심도 그리 적지 않습니다. 그래서 본 특별호의 편집위원으로서, 정보보호학회 공급망 보안 연구회 위원장으로서 우리나라의

공급망 보안의 전망은 매우 밝다고 전망합니다. 아마 우리나라는 다른 나라들보다 매우 빠르게 공급망 보안을 제도적으로 도입할 것으로 예상되며, 이를 상시적으로 점검하고 일상화되는 첫 번째 나라가 될 것입니다. 이런 토대는 소프트웨어 공급망 보안 관련 기업들의 성장을 도울 것으로 확신합니다.

마지막으로 설 연휴에도 논문을 작성 해주신 저자 분들께 특별한 감사를 드리며, 편집에 수고 해주신 학회지 편집 위원회, 그리고 학회 사무국 관계자 여러분께도 깊은 감사의 마음을 전합니다.

2025년 2월

한남대학교 컴퓨터공학과 교수 이 만 희