미상원 공개SW보안법 발의의 의미

김항규 선임연구원
소프트웨어 정책연구소 SW정책·인재연구팀
hkkim@spri.kr

미국 상원에서는 2022년 9월 공개SW보안법(Securing Open Source Software Act of 2022)이 발의되었다. 공개SW 보안 관리를 위해 CISA에 프레임워크 개발, 보안 평가 수행, 핵심 기반 시설에서의 시범 운영 등의 의무를 부여하였다. 연방 소스코드 정책에서 공개SW를 IT·SW 서비스 비용 절감 수단으로 바라보던 시각이 지속가능성과 보안취약성 측면에서 관리해야 하는 SW공급망으로 전환되었음을 보여준다. 신뢰할 수 있고 안전한 공개SW 활용 확산을 위해 국내에서도 SW공급망 관리 측면에서 공개SW를 바라볼 필요가 있다.

미상원, 공개SW보안법 발의

미국 상원은 공개SW[1] 활용에서의 보안 강화를 위해 공개SW보안법(Securing Open Source Software Act of 2022)을 발의[2]했다. 법안은 공개SW 보안 관리를 사이버보안 및 인프라 보안국(CISA) 국장의 의무로 설정하고, 법안 통과 시 공개SW를 활용한 SW제품은 반드시 보안성을 확보해야 한다는 법적 근거가 마련된다. 공개SW는 기술 개발을 촉진 시키고, 디지털 인프라의 한 부분으로서 그 보안성이 국가 안보에 직접적인 영향을 미친다고 인식되고 있다. 이에 따라 연방정부가 공개SW의 장기적 보안 확보를 위한 지원적 역할을 수행해야 한다는 의미에서 의회는 해당 법안의 발의를 추진하였다.

[그림 1] 공개SW보안법(Securing Open Source Software Act of 2022) 법안 서문

117TH CONGRESS
2D SESSION

S. 4913

To establish the duties of the Director of the Cybersecurity and Infrastructure Security Agency regarding open source software security, and for other purposes.

IN THE SENATE OF THE UNITED STATES
SEPTEMBER 21, 2022
Mr. PETERS (for himself and Mr. PORTMAN) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

A BILL

To establish the duties of the Director of the Cybersecurity and Infrastructure Security Agency regarding open source software security, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Securing Open Source Software Act of 2022".

※ 출처: CONGRESS.GOV(2022.9.21.), "S.4913 – Securing Open Source Software Act of 2022"

1) 소스코드가 공개되어 있어 사용·수정·배포를 자유롭게 허용하는 소프트웨어로, 자유SW와 오픈소스SW를 포괄하는 광의의 오픈소스SW를 뜻함
2) CONGRESS.GOV(2022.9.21.), "S.4913 – Securing Open Source Software Act of 2022"

법안 발의 의원(Gary Peters, Rob Portman)은 해당 법안이 Log4j와 같은 취약점 악용 방지에 도움이 될 것이라고 언급하였다. 시스템 로깅 및 모니터링을 위해 널리 사용된 공개SW Log4j에서 2021년 12월에 보안취약점이 발견되었고, 이를 악용한 시도가 기업 네트워크 48% 이상에서 감지[3]되었다. CISA 국장은 Log4j 취약점이 연방 네트워크 보안에 허용할 수 없는 위험을 발생시킨다고 하면서 연방기관에 긴급 명령을 발표[4]하였다. 주목할만한 직접적인 피해 사례가 발견되지 않았지만 CISA는 잠재적 위협에 대해 지속적으로 주시하고 있으며, 공개SW보안법 입법을 통해 관련 보안 관리가 체계화될 것이다.

공개SW보안법에 적시된 CISA의 주요 역할은 ▲공개SW 보안 강화 지원, ▲보안 평가 프레임워크 개발, ▲보안 평가 시행, ▲핵심 기반 시설 시범 운영으로 요약된다. 공개SW 보안 강화 지원 관련해서는, 연방기관을 지원하고 비연방기관과 협력하며 공급망 보안 확보를 위해 공개SW 취약점 정보를 공개하고 연방 조달 보안 위원회를 지원하도록 하였다. 보안 프레임워크는 SW구성요소의 보안 속성과 취약성 및 개발·빌드·배포 절차의 보안 관행 등을 포함해야 하고 법률 제정일로부터 1년 이내에 배포되어야 한다. 보안 프레임워크 발행 후 1년 이내에 2년마다 연방기관에서 직간접적으로 사용하는 공개SW 구성요소에 대한 보안 평가를 시행해야 하고, 평가는 공개SW로 개발된 도구로 최대한 자동화해야 한다. 보안 프레임워크 발행 후 2년 이내에 1개 이상의 핵심 기반 시설에서 시범 수행을 진행하고, 시범 수행 후 1년 이내 의회 위원회에 보고서를 제출해야 한다.

본 법안 발의는 미국 정부가 공개SW를 바라보는 시점의 변화 측면에서 살펴볼 필요가 있다. 기존의 연방 소스코드 정책[5]은 공개SW 활용을 최대한 권고하는 재사용률 확대에 초점을 두었다면, 이번 법안은 보안 측면에서 안전한 공개SW 활용 촉진에 중점을 두고 있다. 법안의 내용과 관련 정책·산업 동향을 연결해 공개SW보안법 발의가 가지는 의미를 세부적으로 살펴보도록 하겠다.

3) Check Point Blog(2021.12.10.), "Protect Yourself Against The Apache Log4j Vulnerability"
4) CISA(2021.12.17.), "CISA ISSUES EMERGENCY DIRECTIVE REQUIRING FEDERAL AGENCIES TO MITIGATE APACHE LOG4J VULNERABILITIES"
5) Office of Management and Budget(2016.8.8.), "Federal Source Code Policy: Achieving Efficiency, Transparency, andInnovation through Reusable and Open Source Software (M-16-21)"

연방정부 차원에서 본격적으로 공개SW 공급망 관리

EU는 공개SW 전략을 정기적으로 발표하면서 공공서비스에서의 공개SW 활용을 확산시켜 왔다. 이러한 가운데 공개SW가 공공영역에서 중요한 SW공급망으로 인식되어 안정적인 유지·관리 필요성이 제기되었으며, 대표적으로 EU-FOSSA[6], FOSSEPS[7] 등 프로젝트 추진을 통해 주요 공개SW 목록을 관리하고자 하였다. 관련 프로젝트들은 공통적으로 공공영역에서 널리 사용되고 있는 공개SW 프로젝트를 목록화(SW인벤토리 구축)함으로써, 프로젝트가 관리되지 않거나 버려짐으로 인해 공공서비스에 가해질 수 있는 위협을 관리하고자 하였다. 미국 정부가 공개SW를 바라보는 시각이 이와 같은 SW 공급망 강화 필요성 측면으로도 확장됨에 따라 본 법안 발의가 이루어진 것으로 볼 수 있다. 법안의 2절 의회 발견 사항을 보면 시각의 변화를 알 수 있다. (1)공개SW는 기술 개발을 촉진하고 전체 사이버 보안의 필수적인 부분입니다. (2)안전하고 건강하며 활기차고 탄력적인 공개SW 생태계는 미국의 국가 안보와 경제적 활력을 보장하는 데 중요합니다. (3)공개SW는 자유롭고 개방된 인터넷을 촉진하는 디지털 인프라 기반의 일부입니다. 이는 공개SW를 IT·SW 솔루션 비용 절감의 수단으로 인식하고 활용 확산을 촉진시켰던 연방 소스코드 정책의 시각과 크게 달라졌음을 보여준다. 공개SW는 기술 개발 촉진, 경제적 활력 보장, 디지털 인프라 기반의 일부 측면에서 사회적으로 중요한 의미를 가지고 있고, 따라서 국가 SW공급망으로 인식하고 유지·관리에 노력을 기울일 필요가 있음을 뜻한다. 이를 위해 연방정부는 공개SW의 장기적 보안을 보장하는 지원 역할이 요구됨을 법안에 명기하였다.

6) EC DIGIT(2018.4.5.), "EU-FOSSA 2 Project Charter"
7) EC DIGIT(2022.2.2.), "Free and Open Source Solutions for European Public Services(FOSSEPS) - Project Charter"

보안 측면에서의 안전한 공개SW 활용체계 확립

2022년 1월 공개SW 보안 강화 방안 논의를 위해 백악관에서 민관이 함께 참석하는 미팅[8]이 이루어졌다. 공개SW가 대부분의 SW 패키지에 포함됨에 따라 독특한 가치(unique value)를 가져오는 동시에 독특한 보안 과제(unique security challenges)도 가지고 있음을 공유하였다. 보안 과제를 해결하기 위해 공개SW 패키지 내의 보안 결함·취약점 방지, 결함 발견·수정을 위한 절차 개선, 개선책 배포·구현 반응시간 단축이라는 3가지 주제를 중심으로 논의가 이루어졌다. 후속 대응으로 2차 회의가 동해 5월에 개최되어 리눅스 재단에서 1차 회의의 3개 주제를 10개 세부 과제로 구체화하는 동원 계획[9]을 발표하였다. 이러한 공개SW 보안에 대한 관심은 민간에서의 자발적인 요구로 나타났다. 구글, MS, IBM 등이 참여해 개발·테스트·투자 및 인프라 구축 과정에서의 안전한 공개SW 활용을 목적으로 교육·훈련, 정보공유 등을 수행하는 OpenSSF를 리눅스 재단 프로젝트 일환으로 2020년에 설립하였다. OpenSSF는 Alpha-Omega 프로젝트를 추진해 신속한 취약점 발견·개선으로 공개SW 프로젝트를 보안 측면에서 지원하였다. 민관 모두가 공개SW 보안 강화 필요성에 대한 인식을 공유하고 있음을 알 수 있다.

이러한 인식 하에 의회는 CISA에게 공개SW 보안 관리의 의무를 부여한 것이다. 공개SW 보안 강화를 위한 전반적인 지원을 담당하고, 보안 평가 프레임워크 개발 및 시범 운영 및 시행할 것을 CISA의 역할 범위 내에 설정하였다. 개발된 프레임워크는 공개SW 구성요소에 대해 보안 속성, 개발·빌드·배포 절차에 대한 보안 관행, 알려진 취약점의 개수와 심각성, 배포 범위, 관련 위협 수준, 커뮤니티의 활성화 정도를 최소한 포함하도록 하고 있다. 보안 관리 비용적 측면에서의 부담을 최소화하기 위해 가능한 자동화를 지원하도록 하였다. 자동화 지원 도구를 공개SW로 개발하고 연방기관 또는 비연방기관에서 이를 다운로드 받아 활용할 수 있도록 공유하게 하였다. 프레임워크 배포 후 2년 이내에 핵심 기반 시설에서의 보안 평가 실효성을 검토하고, 실효성이 인정될 경우 부문별 위협 관리 기관[10]과 협력해서 시범 운영할 것을 명시했다. 이를 통해 본 법안은 보안 측면에서의 안전한 공개SW 활용체계를 구축하기 위한 법적 기반을 마련한 것이다.

8) 백악관 보도자료(2022.1.13.), "Readout of White House Meeting on Software Security"

9) 리눅스재단(2022.5.12.), "The Open Source Software Security Mobilization Plan"

10) 대통령 정책 지시 PPD-21(https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil)에 적시된 16개 부문 관련 부처 및 기관

공개SW 중심의 SBOM (Software Bill of Materials) 체계 도입

SW공급망 투명성 확보를 위해 SW구성요소에 대한 세부 정보, 의존관계 등을 기술한 명세서를 가리켜 SBOM(Software Bill of Materials)라고 한다. 미국 정부는 SW구성요소 수준에서의 SW공급망 보안 확보를 위한 수단 중 하나로 SBOM을 인식하고 연방기관 보안 강화를 위한 행정명령[11]에 관련 내용을 포함시켰다. 이후 중요(critical) SW에 대해 연방기관이 준수해야 하는 보안조치와 SW공급망 보안 관리 가이드를 배포해 SBOM 관리·활용을 촉구하였다. 국토안보부 IT서비스, 의료기기 등 높은 수준의 보안이 요구되는 영역에 대해서는 조달 과정에서 SBOM을 제출하도록 하는 법안도 발의되었다. 이와 같은 SBOM 제도화 맥락에 맞추어 공개SW 중심의 SBOM 체계 기반을 마련하는 것이 공개SW보안법 발의 목적 중 하나인 것으로 볼 수 있다. 안정적인 SBOM 제도화를 위해 상용SW에 대한 SW구성요소 정보까지 포괄하기에 앞서 개방성에 기반한 공개SW에 우선 적용하는 방식으로 접근한 것이다.

본 법안은 프레임워크에 기반해 2년마다 CISA에서 보안 평가를 수행하도록 하고 있다. 평가는 연방기관에서 직간접적으로 사용하고 있는 공개SW 구성요소에 대해서 수행되며, 이미 구비되어 있는 가능한 기계가독적인 정보를 사용하도록 강조하면서 관련 정보로 다음 3가지를 제시하였다: (1) CISA가 확보하고 있거나 인터넷을 통해 접근할 수 있는 SBOM, (2) CISA의 CDM(Continuous Diagnostics and Mitigation) 프로그램[12]에서 수집된 SW인벤토리, (3) 공개SW 구성요소 관련해 공개적으로 접근 가능한 정보. SBOM 포맷 관련한 국제표준(SPDX, CycloneDX 등)은 SBOM 생성·관리·활용의 자동화를 위해 기계가독적인 형식을 지원하고 있다. SW구성요소 정보의 기계가독성을 강조한 것은 SBOM 활용 권고를 의미하며, 이는 보안 평가를 위해 연방기관에서 공개SW 구성요소에 대한 정보를 SBOM으로 CISA에 제출해야 함을 말한다. 제출된 SBOM은 기계가독성에 기반해 자동화된 보안 평가 수행을 지원할 것이다. 공개SW보안법은 SBOM을 활용해 SW구성요소 보안 평가의 자동화를 구현하고, 나아가 상용SW를 포함한 SBOM 활용 확산의 시작점을 마련하고 있다.

11) 백악관(2021.5.12.), "Executive Order on Improving the Nation's Cybersecurity"
12) CISA CDM, https://www.cisa.gov/cdm

공개SW, 이제는 SW공급망 관리 측면에서 바라보아야 할 시점

공개SW는 제품에 들어가는 대부분의 SW 기반을 이루고 있고, AI·블록체인·클라우드 등 SW신기술의 개발과 확산의 토대를 형성하고 있다. 공개SW 프로젝트의 지속가능성이나 보안취약성은 전 산업과 사회 기반에 영향을 주고 있다. 미상원 공개SW보안법 발의는 미국이 공개SW의 사회적 영향을 인식하고 SW공급망 관리 차원에서 바라보아야 한다는 시각의 전환을 보여준다. 법안이 통과되고 효력을 가지기까지는 많은 시간이 요구되지만, 미국 현정부의 공개SW 공급망 보안 강화 정책 기조에 부합하기에 입법 과정에서 추진력을 가질 것으로 기대된다. 단기적으로는 수출기업에서의 대응책 마련과 컨설팅·교육 등을 통한 정부 지원이 요구된다. 중장기적인 관점에서는 기업 경쟁력 제고와 사회 안전망 구축을 위해 국내에서 활용되는 공개SW에 대한 관리·보완·강화를 위한 정책 검토도 필요하다. 국내에서도 공개SW를 사회 기반의 SW공급망으로 인식하고, 안전하고 안정적인 공개SW 활용을 위한 시각의 전환이 필요한 시점이다.