SW공급망 관리 및 SBOM 동향

Software Supply Chain Management and SBOM Trends

류원옥 (W.O. Ryoo, woryoo@etri.re.kr) 오픈소스센터 책임연구원
박수명 (S.M. Park, smpahk@etri.re.kr) 오픈소스센터 책임연구원
이승윤 (S.Y. Lee, syl@etri.re.kr) 오픈소스센터 책임연구원/센터장

ABSTRACT

The increased adoption of open source security management in supply chains is gaining worldwide attention. In particular, as security and threatening situations, such as solar winds, Kaseya ransomware, and Log4j vulnerability, are becoming more common in supply chains using software (SW)-defined networks, SW bills of materials (SBOMs) for SW products should be prepared to protect major countries like the United States. An SBOM provides SW component information and is expected to become required for SW supply chain management. We focus on SW supply chain management policies and SBOM trends in major countries and private organizations worldwide for safe SW use and determine the current status of Korea and ETRI's open source SW supply chain management trends.

KEYWORDS open source management, SBOM, SW integrity/transparency, SW supply chain

Ⅰ. 서론

전 세계적으로 오픈소스 활용 비중이 지속해서 증가하고 있다. 시놉시스의 오픈소스 보안 및 위험 분석 보고서에 의하면 검증한 코드 베이스의 98%가 오픈소스를 활용하고, 84%에서 하나 이상의 보안취약점이 발견되었으며, 65%의 라이선스 충돌이 발견되었다고 한다[1]. 가트너 보고서에 따르면 '25년에는 전 세계 조직의 45%가 SW공급망에 대한 공격을 경험할 것이라고 한다[2].

미국 정부는 사용하는 SW에 대한 안전성 확보 및 SW공급망 관리를 위해 H.R.5793(사이버 공급망 관리 및 투명성에 관한 법률)을 도입하여 모든 상용제품 및 오픈소스SW 컴포넌트의 명세서 제공과 알려진 취약점이 없음을 입증하는 절차를 만들었다[3].

특히, SW공급망에서 솔라윈즈, Kaseya, Log4j 등 보안 위협 사례가 증가하면서 미국 연방정부는 '21년 5월에 조달한 SW제품에 대해 SW컴포넌트 정보를 기술한 SBOM(Software Bill of Materials)을 제출하도록 요구하는 행정명령(EO 14028)을 발표하였다.

* DOI: https://doi.org/10.22648/ETRI.2023.J.380408
* 본 연구는 한국전자통신연구원 내부연구과제의 일환으로 수행되었음[23YF1100, 개방형 ICT R&D 생태계 강화를 위한 ETRI 오픈소스 R&D 대응체계 구축].

SBOM 정보는 SW공급망의 보안과 무결성/투명성을 제공하여 SW를 개발, 구매, 운영하는 사람들에게 이해를 높이는 정보를 제공한다. 제공되는 정보는 알려진 보안취약점 및 새로운 취약점의 추적 및 대응을 빠르게 하고, 최신의 컴포넌트 상태를 확인하고, 라이선스 준수 여부 확인 및 SW의 가시성 정보를 확인할 수 있는 장점이 있다[4].

본고에서는 안전한 SW 사용을 위한 SW공급망 관리 정책 및 SBOM에 대하여 주요 국가 및 민간단체의 동향을 알아보고, 국내 현황과 한국전자통신연구원(ETRI) 사례를 중심으로 오픈소스 SW공급망 관리 현황과 이슈를 알아본다.

II. SW공급망과 SBOM 동향

1. 배경

디지털 전환 시대의 전 산업 분야의 혁신은 SW가 주도하고 있으며, 특히 오픈소스SW 기술을 기반으로 디지털 전환이 가속화되고 있다. 하지만 현재의 SW공급망은 상용SW의 보안 업데이트 서버를 통한 악의적인 침투 또는 오픈소스SW 보안취약점 등의 위협에 취약하다[5]. 특히, SW공급망 위협은 신뢰하는 공급망을 통해 SW컴포넌트 수준의 악성 SW가 침투하거나, 공급망의 투명성 부족으로 신속한 대응이 이루어지지 못해 피해가 커지고 있다.

따라서, SW공급망 투명성 제공을 위해 SW컴포넌트 정보를 자동화하여 제공하는 SBOM은 조직의 개발·법무·조달·위험 관리를 가능하게 하는 IT 인프라에 활용할 수 있다. SW공급망 투명성 확보를 위해 미국을 비롯한 글로벌 SW공급망 연결성을 가지는 주요 국가가 SBOM 도입 및 제도화 등의 동향에 관심을 두고 대응책을 마련하고 있다.

2. 국외 주요 동향

가. 미국

최근 몇 년 사이 전 세계적으로 SW공급망을 통한 보안 위협이 급증함에 따라, 미국 정부는 더욱 안전한 SW공급망 관리를 위해 SBOM 도입을 적극적으로 검토하고 '21년 5월 SW공급망 보안 강화를 위해 행정명령 "국가 사이버보안 개선"(EO 14028)을 발표함으로써 공공조달에서 SBOM 제출을 의무화하고 있다[3].

1) 정부

미국 정부는 SBOM 활용 정착을 위해 관련 이니셔티브를 발족한 바 있으며, 이를 통해 SBOM 활용에 대한 실증과 SBOM 관리 절차 및 양식 표준 등에 대한 법제화를 추진하고 있으며 점진적으로 민간의 자발적인 확산을 유도하고 있다(표 1).

2) 정책 추진

의료, IoT 등의 분야에서 SW컴포넌트 관리 필요성이 제기되어 '18년에 NTIA 주도로 관련 이니셔티브를 발족하였으며, SBOM의 개념 검증을 위한 실증과정을 거치고 이해관계자 의견 수렴을 통해 SBOM의 정의와 범주 등을 설정하는 작업을 추진하였다.

또한, SBOM에 대한 최소 구성요소를 정의함으로써(표 2 참고) 범정부적 SBOM 정책 준수의 기준점을 마련하기도 하였다.

3) 법·제도

미국 하원은 SW공급망 투명성 확보를 위해 이미 '14년도에 H.R.5793(사이버 공급망 관리 및 투명성에 관한 법률)을 발의한 바 있다.

이어서 미국 상원은 IoT 기기에 대한 SBOM 기반 보안체계를 위해 '17년도에 S.1691(IoT 사이버보

표 1 미국 SBOM 정책 추진 관련 기관 및 역할

기관명	조직 기능	SBOM 정책 역할
OMB (백악관)	대통령의 비전 구현을 위한 업무를 수행하고, 정책 · 예산 · 관리 · 규제 측면에서 대통령을 보좌하고 기관에 관련 사항 지시	연방 부처 · 기관의 준수 · 협조를 촉구 • 중요 SW(Critical SW) 보안 조치 준수를 기관에 전달 • SW공급망 보안 가이드 준수를 위해 조달 담당자 대상 온라인 워크숍 개최 • NIST 가이드 준수와 필요시 공급자에게 SBOM을 요구할 것을 연방기관에 지시
NTIA (상무부)	통신 · 정보 관련 국가 정책 수립 · 이행을 위해 대통령에게 조언	SBOM 정책 추진을 위한 기준을 마련 • SW 구성요소 투명성 이니셔티브를 발족해 SBOM 기반 투명성 확보 기준 정의 • 의료 · 에너지 등 SBOM 실증으로 산업 도입 효과성 검증 • SBOM 생성 · 공유 등에 대한 기준인 SBOM 최소 요소 공개
NIST (상무부)	측정 · 표준 · 기술 발전을 통해 혁신과 산업 경쟁력 제고를 촉진	SW공급망 보안 관련 가이드 배포 • 중요 SW 정의, 보안 조치 가이드 제작 • SW공급망 보안 가이드 공개
CISA (국토안보부)	사이버 · 물리 기반에 대한 위협 이해 · 관리 · 감소를 수행	SBOM 정책 초안 검토 및 인식 제고 • 중요 SW 정의, 보안 조치 가이드 검토, 중요 SW 목록 식별 • 인식, 제고, 의견 청취를 위한 토론 및 온라인 세션 운영

출처 Reprinted from [3], 공공누리4유형.

표 2 미국통신정보국(NTIA)의 SBOM 최소요소

최소요소	알고리즘
데이터필드 (Data Fields)	• 필수적으로 추적해야 할 각 컴포넌트와 기준 정보 문서화 – 컴포넌트의 공급자, 이름, 버전, 식별자, 의존관계 – SBOM 작성자, 작성 일시
자동화 지원 (Automation Support)	• SW 생태계상에서의 적용을 위한 자동 생성 및 기계 가독성 등을 포함한 자동화 지원 • SBOM 생성 · 소비를 위한 데이터 포맷으로 SPDX, SWID tag, CycloneDX 포함
사례 및 프로세스 (Practices and Processes)	• SBOM 유형 · 생성 · 사용에 대한 운영 정의 – 생성 빈도수, 컴포넌트 종속성 관계, 알려진 무지(Known unknown), 배포 및 전달, 접근 제어, 오류에 대한 양해

출처 Reprinted from [3], 공공누리4유형.

안 개선법)을 발의하였고, 미국 하원은 '21년 7월에 정보통신 기술·서비스 계약에 대하여 BOM(Bill of Material)을 제출하도록 하는 H.R.4611(국토안보부 SW공급망 위협 관리법)을 발의한 바 있다.

'22년 들어 미국 상원은 연방기관에서 직·간접적으로 사용하는 오픈소스SW에 대해 CISA(사이버보안 및 인프라 보안국)가 SBOM 기반 정기 보안 평가를 의무 시행하도록 S.4913(오픈소스SW 보안법)을 발의하였다.

4) 실증 사업

SBOM 활용 확산을 위한 다양한 분야에서의 실증을 추진하고 있으며, 대표적으로 의료, 에너지, 자동차 분야가 있다.

- 의료: 기기의 안전한 사용을 위해 의료 커뮤니티에서 제기된 수요 기반 실증 추진
- 에너지: 사회 기반 시설의 수준 높은 SW공급망 보안 확보를 위해 SW 컴포넌트 정보를 SBOM으로 제공하는 실증 추진
- 자동차: 차량 운행의 안전 확보 차원의 사이버 보안 지침 제공을 위하여 SW컴포넌트 관리·추적에 SBOM 실증 추진

5) 가이드 발간

SW컴포넌트 기반으로 잠재적인 사이버보안 취약점 관리 목적으로 표준화된 SBOM 생성 방법론 가이드 등을 제작·배포하고 있다.

- NTIA는 SBOM 국제표준 포맷과 관련하여 표 3과 같은 비교 분석 보고서를 공개[5-11]
- NIST는 SW공급망 보안 가이드 3가지(웹 가이드, SSDF, C-SCRM 가이드) 배포

표 3 SBOM 표준 포맷

표준 포맷	설명
SPDX (Software Package Data Exchange)	• '11년 리눅스 재단에서 개발해 '21년 국제표준(ISO/IEC 5962:2021)으로 등록되었다. • 오픈소스 라이선스 관리와 SBOM 포맷 활용에 용이하며, SW 패키지와 관련된 컴포넌트, 라이선스, 저작권 및 보안 정보를 전달할 수 있다. • xls, rdf, json, yml 언어로 작성되며, SPDX는 SBOM 자동 생성 도구를 제공하며, dotnet(.net), Maven(Java), PIP(Phython) 등의 패키지 매니저를 지원하여 SW가 어떤 하위 패키지를 포함하고 있는지 정보를 추출하고 이를 SBOM으로 만든다. • SPDX 문서는 문서 생성 정보, 패키지 정보, 파일 정보, 스니핏 정보, 라이선스 정보, 컴포넌트 간의 관계 정보(종속성 정보) 및 주석 등의 필드와 데이터들로 구성된다.
SWID (Software Identity)	• NIST가 '09년에 공개하여 '15년도에 국제표준(ISO/IEC19770-2:2015)으로 등록되었다. • SW제품의 특정 릴리즈에 대한 정보를 포함하고 있으며, SW 정보에 대한 태그를 생성하여 장치에 설치된 상용 및 오픈소스 SW 인벤토리를 지원한다. • SWID 태그는 소프트웨어 생명주기와 연계되어 SW 컴포넌트에 대한 식별 정보, SW 산출물에 대한 파일 및 암호화 해시 목록, SBOM 작성자 및 SW 컴포넌트에 대한 출처 정보를 제공한다.
CycloneDX	• OWASP 단체가 사이버 위험 감소를 위해 고급 공급망 기능을 지원하는 풀스택 BOM 산업 표준을 지향하며, '17년도에 초기 프로토타입 공개를 시작으로 현재 1.4버전까지 공개하였다. 처음부터 SBOM 포맷으로 설계된 점이 특징이며 SaaSBOM을 포함한 다양한 사양을 지원한다. • JSON, XML 언어로 작성되며 빌드 시스템에 구현하여 유연하고 쉽게 채택하여 활용할 수 있다는 장점이 있으며 메타데이터, 컴포넌트, 서비스, 종속성, 구성, 취약점, 확장으로 구성되어 있다.

- 의료, 자동차 등 주요 산업에서 사이버보안 강화 가이드를 공개하여 SBOM 활용 유도 중

6) 민관 협력

정부는 SBOM 개념 정립, 실증 과정은 민간 전문가의 협력을 받아 표준화, 가이드 생성에 대한 현장의 의견을 수렴하여 반영하고 있으며, SW공급망 보안 강화를 위해 오픈소스SW 중심으로 민관 협력체계를 구축하여 SBOM 확산 방안을 논의 중이다.

나. EU

1) 정부

EU는 '20년 10월, 공공 및 기술의 혁신을 위해 'Think Open'으로 "오픈소스SW 전략 2020-2023"을 발표하여 오픈소스SW 활성화를 촉진하고 있다[12]. EU 회원국 간의 상호운용성 향상을 위해 추진된 ISA(Interoperability solutions for public administrations, businesses and citizens) 프로그램은 Interoperable Europe으로 확대 개편하고, 디지털 서비스 전담 부처 DIGIT(Directorate-General for Informatics)에 오픈소스SW 전략 수립 및 정책 추진 조직인 OSPO(Open Source Program Office) 기능을 부여해 오픈소스SW 기반 조성을 위한 조직체계를 구축하였다[13,14].

2) 프로젝트(FOSSEPS)

EU는 '22년 2월에 FOSSEPS(Free and Open Source Software European Public Services) 파일럿 프로젝트를 발표하고, EU 회원국 공공서비스 대부분에 활용되고 있는 오픈소스SW에 대해 지속가능성, 보안성 강화, SW 자산 공유화를 유도하고 있다. 특히, FOSSEPS는 오픈소스SW 생태계 강화를 목적으로 하고 있으며, 공공서비스에서 개발·활용 중인 오픈소스SW 정보를 목록화하여 관리하고, 중요 오픈소스SW 프로젝트를 선정해 보안성 강화를 위한 협력체계 구축을 추진 중이다[15].

또한, SW공급망 보안 강화를 위해 중요 오픈소스SW에 대한 정의, 중요 오픈소스SW 목록화, EU 공공서비스 내 중요 오픈소스SW 조사, Top-30 중요 오픈소스SW 선정, 해당 오픈소스SW 프로젝트와의 위험성 대응 협력 등을 계획하고 있기도 하다.

FOSSEPS 프로젝트의 주요 임무로 EU 앱 목록 벤치마킹, EU 앱 목록 생성, 중요 오픈소스SW 저장소 생성, 오픈소스SW 협력, 프로젝트 확산 및 교훈, 사례 문서화를 포함한다.

3) 실증 사업(D-SBOM)

IoT 분야의 SW공급망 보안 강화를 위해 분산형 SBOM 관리 모델을 실증하기 위한 프로젝트로 D-SBOM(Distributed SBOM)을 추진하고 있다[16]. 특히, 해당 프로젝트에서는 개발된 결과물을 자동차 산업에 적용하는 실증 추진으로 그 효과성을 입증한다는 계획이다.

4) 가이드 발간

EU 공공서비스에서 사용하고 있는 중요 오픈소스SW를 조사하기 위해 EU 정보화 총국(DIGIT)은 의료기기, IoT 등에서 사이버보안 강화를 위해 SBOM 활용을 권고하는 가이드를 배포하였으며, 클라우드 서비스·의료기기 인증체계에서 SW공급망 투명성 제고를 위한 SBOM 도입을 검토하거나 이에 준하는 정보를 요구하고 있다.

선정된 최상위 중요 오픈소스SW는 EU에서 관리하고, 오픈소스SW 프로젝트 개발팀과의 긴밀한 협력체계를 유지함으로써 취약점 노출, 개발 중단 등 위험에 대응하고, 공공서비스의 안전한 오픈소스SW 활용 환경을 조성하고 있다.

5) 법·제도

'22년 9월 15일 EU 집행위원회는 인터넷 시장의 신뢰성을 확보하기 위해 지금까지 EU가 다루지 않았던 외장형 디바이스와 SW의 보안 수준과 능력을 법제화하려는 목적으로 유럽 내에서 디지털 요소를 가진 제품을 판매하기 위해 SBOM 제출을 요구하는 사이버복원력법안(Cyber Resilience Act)을 제안하였고, 이를 'CE 인증(CE Marking)'에 세부 규정으로 개정할 예정이며, 향후 1~2년 이내에 법안을 개정할 예정이다.

법안 내용에는 제조사가 제품의 개발 생명주기에서 취약점을 최소화하고 사용자가 제품 선정 및 활용에 보안성을 검토하는 체계를 조성하고 있으며, 사이버보안 위험 수준에 따라 제품을 1등급과 2등급으로 분류하며 위험 수준이 높은 2등급 제품은 의무적으로 외부 기관의 적합성 평가를 받도록 하고 있다.

다. 영국

영국은 ICT 분야의 보안 강화 정책으로 SW공급망 투명성 확보를 위한 국가사이버보안센터 NCSC(National Cyber Security Centre)에서 기기 보안 가이드를 배포해 SBOM 활용을 권고하고 있다[14].

또한, 통신망 서비스 공급망 보안 강화를 위해 관련 법제화를 추진하고 이를 근거로 디지털문화미디어스포츠부 DCMS(Department for Digital, Culture, Media & Sport)는 SBOM과 기능적으로 유사한 보안 지침을 마련하고 있다(표 4).

라. 일본

1) 정부

경제산업성 내에 소프트웨어TF를 설치하여 SBOM 개념, 효용성, 제도화 방안 등을 추진하고, 지속해서 미국의 SBOM 정책을 업데이트하면서 국내 도입(안) 수립에 반영하고 있다[14].

특히, 오프소스SW 라이선스 관리를 위해 선도적으로 SBOM을 적용하고 있는 기업 활용사례를 모아 모범사례집을 발간하고 있다.

총무성은 "ICT 사이버보안 종합대책 2022"에 SBOM 적용 범위를 ICT 전반으로 확대해 제도화할 방안을 검토하고 있다.

표 4 통신 보안 행동강령 내 SBOM 관련 보안 평가항목

평가항목	보안 기대치
V.4.7 도구 · SW · 라이브러리 사용 (User of tools, software and libraries)	제3자 도구, SW 구성요소, SW 라이브러리에 대한 인벤토리 유지 Third party tools(e.g. code compilers), software components and software libraries that are used within and in the development of the product are inventoried.
V.B.3 내부 구성요소 관리 (Internal component management)	모든 내부 구성요소의 현행화 Any shared internal components of libraries are kept up to date and only the latest stable, supported version id used,
V.B.4 외부 구성요소 관리 (External component management)	지원하는 외부 구성요소만 제품 내에 사용 Only supported external components are used within a product.

출처 Reprinted from [14], 공공누리4유형.

2) 실증 사업

SBOM 도입의 실효성 검증을 위해 실증을 수행하였고, 이를 의료·자동차·SW로 분야로 확장하여 표 5와 같이 중점 사항을 정리하고, 개념 정립, 효과성 검증, 제도화 방안을 마련하고 있다.

'22년 7월에는 의료기기, 자동차, SW 실증 대상에 대한 노하우집과 활용·거래 가이드를 제시하고 있다.

3) 기업

기업들은 자체적으로 SBOM 활용체계를 구축해 SW공급망 보안 강화 측면에서의 경쟁력을 확보하고자 노력 중이다.

표 5 분야별 SBOM 실증의 중점 사항

실증 분야	중점 사항
의료 기기	• 법 제도의 요구에 맞춘 정밀도가 높은 SBOM 생성 관리가 요구됨 • 의료기관(사용자 기업)에 의한 SBOM 활동의 가능성 검토 • 관련 규제: IMDRF 가이드 등
자동차	• 공급망이 넓고 깊은 계층 구조로 이루어지고 해외도 포함되어 있음 • SBOM 공통화를 이룸으로써 신뢰성 확보를 통한 비용 절감 기대 • 관련 규제: 미국 NHTSA 지침, unR155 등
소프트웨어	• SBOM 생성 주체가 되는 사례가 많고, 관련 도구에 대한 넓은 지식과 깊은 이해가 있어 SBOM 도입을 통한 이익이 클 것으로 기대 • SBOM의 효과적인 공유 방법, 상호운용 가능한 포맷으로서의 작성 등 검토

출처 Reprinted from [14], 공공누리4유형.

마. 중국

1) 정부

중국은 '20년 공급망 보안 관리를 위해 국가인터넷정보판공실, 국가발전개혁위원회, 공업정보화부, 재정부에서 클라우드 서비스에 대한 보안 평가 의무화 규정을 마련한 바 있다[14]. 중국표준화관리위원회는 SW공급망의 보안 강화를 위해 SBOM을 사용하도록 하는 정보보안기술 SW공급망 보안 요구표준을 '22년에 발표하였다.

2) 가이드 발간

특히, SW공급망 보안 강화 방안을 마련하기 위해 공업정보화부 산하 CAICT(China Academy of Information and Communications Technology)에서 SBOM을 검토하는 협력체계로써 SW공급망보안연구소(3S-LAB)를 설치하고, CAICT를 중심으로 SBOM 관련 백서 및 가이드를 발간해 SBOM 활용 확산을 촉진하고 있다.

• SW공급망 투명성 확보를 통해 빠른 보안취약점 대응 방안 중 하나로 SBOM을 제시하는 SW

공급망 보안백서를 발간('21년)
- 작성법, 활용방안 등 SBOM 관련 세부 정보를 제공함으로써 필요성 인식을 향상하기 위해 SBOM 실무가이드를 발간('22년)
- SW보안 개발 생명주기 상에서의 SBOM 활용 촉진을 위해 SW제품의 개발·활용 단계를 대상으로 하는 SBOM 보안 응용 백서를 발표('22년)
- 경쟁국인 미국의 SBOM 도입 현황을 가이드 및 백서로 공유하여 SW공급망에서의 주도권 확보를 위한 SBOM 도입 필요성을 제시 중

바. 네덜란드

SW공급망 투명성 확보 측면에서 SBOM의 중요성을 인식하고 글로벌 동향 분석과 함께 SBOM 도입 방향을 연구 중이다[14].

법무부 산하 국가 사이버 보안국(National Cyber Security Centre)에서 SBOM 연구가 진행 중이며, NCSC는 사이버보안 강화를 위한 SBOM 활용법을 보고서로 발간하여 SBOM 필요성과 도입 방향을 제시하고 있다.

또한, 미국과 EU의 SBOM 정책 동향을 분석하고 감시하여 효과적인 SBOM 도입 방향을 모색하고 있다.

사. OpenSSF

오픈소스 관련 재단인 OpenSSF(Open Source Security Foundation)는 개발, 테스트, 투자 및 인프라 구축 과정에서의 안전한 오픈소스SW 활용을 목적으로 교육, 훈련, 정보 공유 등을 수행하고 있으며, 구글, MS, IBM, 아마존, 인텔, 메타 등 글로벌 IT 기업 다수가 참여하고 있다.

OpenSSF는 SW공급망 강화를 실현하기 위해 중요 SW를 식별하고, 이에 대한 대응체계를 구축하는 Alpha-Omega 프로젝트를 발표하였다[17].

Alpha-Omega 프로젝트는 최상위 중요 SW를 식별하고 이를 관리하는 Alpha 프로젝트와 롱테일(Long Tail)에 포함되는 다수의 중요 SW를 자동화된 방식으로 감시하는 Omega 프로젝트로 구성된다.
- Alpha 프로젝트: 최상위 중요 SW 프로젝트 관계자에게 위협 모델링, 자동화된 보안 테스트, 소스 코드 감시, 발견된 취약점 개선 등에 대한 지원을 제공하고, 대응 결과를 점수 카드나 배지 형태로 공개함으로써 해당 프로젝트의 보안대응 상태를 투명하고 표준화된 방식으로 가시화
- Omega 프로젝트: 롱테일에 해당하는 10,000개 이상의 널리 배포된 오픈소스SW 프로젝트에 대해 자동화된 방법과 도구를 통해 치명적인 보안취약점을 식별 추진. 특히 클라우드 규모의 분석, 보안 분석가의 감시 및 취약점 대응책 보고를 통해 이를 수행하고, 신규 취약점 식별의 정확도를 높이기 위한 분석 파이프라인을 최적화[18]

아. 리눅스 재단

리눅스 재단에서 수행하는 SPDX 프로젝트는 SW 패키지의 원활한 공유와 수집을 위해 필요한 관련 정보의 공통 데이터 포맷을 제공한다.

SPDX는 SW 패키지, 파일 및 스니핏(Snippet)을 설명함으로써 동적 사양이 되는 것을 최종 목표로 하고 있으며, 현재 버전은 최상위 V2.3이고 SPDX 커뮤니티를 중심으로 3.0을 발표하였다[6].

SPDX 커뮤니티에는 유수 글로벌 IT 기업인 인텔, 마이크로소프트, 지멘스, 소니 등이 활동하고 있으며, '21년 9월 SPDX는 ISO(국제 표준화 기구) 국제표준으로 제정되기도 하였다[6].

자. OWASP

국제 웹 관련 보안 표준 프로젝트인 OWASP(Open

Web Application Security Project)에서는 보안 컨텍스트 및 공급망 컴포넌트 분석을 위해 별도의 SBOM 규격인 사이클론DX(CycloneDX)를 개발한 바 있다[9,10].

사이클론DX는 다음과 같은 기능적 특징을 가지고 있다.

- 하드웨어, 클라우드 및 SaaS 등과 관련하여 계층적 접근 방식으로 서로 다른 시스템 및 BOM의 컴포넌트, 서비스 및 취약점 참조 가능
- 사용되는 컴포넌트의 작성자와 공급자를 나타내는 출처(Provenance) 정보를 포함하고 있으며, 이를 통해 컴포넌트의 계층적 관리를 효율적으로 할 수 있음
- SW제품과 컴포넌트의 취약점 악용 가능성에 대한 인사이트를 제공하고 있으며, SW제작자에게 전달할 수 있는 VEX(Vulnerability Exploitability eXchange)를 지원

3. 국내 주요 동향

국내에서는 '19년에 오픈소스 SW공급망 관리 차원에서 TTA 오픈소스SW 표준분과(PG602)를 통해 개발된 "개방형 연구개발을 위한 공개SW 커뮤니티 거버넌스 지침, TTAK.KO-11.0257" 표준이 있다[19]. SW공급망의 라이선스 위반 및 보안취약점 위험 예방 등을 위한 SBOM은 "공개 소프트웨어 공급망 관리를 위한 소프트웨어 목록 구성(SBOM) 속성 규격, TTAK.KO-11.03097" 표준으로 '22년도에 표준화되었고[20], 오픈소스 SBOM 표준 속성 규격은 표 6과 같이 정의하고 있다.

표 6 SBOM 표준 속성 규격

구분(Baseline)	속성(Attribution)
① SBOM 검증 도구 (SBOM Validation Tool Name)	Ex) Folosology
② 공급자(Supplier Name)	ComponentSupplier:
③ 저작권자(Author Name)	ComponentAuthor:
④ 컴포넌트(Component Name)	ComponentName:
⑤ 버전(Version String)	ComponentVersion:
⑥ 고유식별자(Unique Identifier)	FormatID:
⑦ 컴포넌트 해시 (Component Hash)	FileChecksum:
⑧ 라이선스 명(License Name)	Component License:
⑨ 라이선스결합형태 (License Usage)	Dynamic/Static Linking:
⑩ 보안취약점 DB (Vulnerability DB)	VulnerabilityDB: NVD
⑪ 관계성(Relationship)	IncludeComponent, ImportComponent
⑫ 릴리즈 날짜(Release Date)	ReleaseDate:
⑬ CVE ID	CVE-Year-Serial Number
⑭ CVSS Base Score	Base: , Impact: , Exploitability:
⑮ CVSS Severity	CVSS Severity: High, Medium, Low, None

출처 Reprinted with permission from [20].

4. SBOM

이 절에서는 현재 SW공급망 안전성과 투명성 확보를 위해 가장 앞선 미국의 사례를 중심으로 알아본다.

미국 상무부는 NTIA와 협력하여 SW공급망에서 보안 위협 대응을 목적으로 '18년에 SBOM 활용 및 활성화를 위한 SW 컴포넌트 투명성 이니셔티브를 발족하고[3], SBOM의 "최소 구성요소"를 게시하도록 하였다. NTIA에서 정의한 SBOM의 최소 구성요소는 데이터 필드, 자동화 지원, 사례 및 프로세스 영역으로 SW 투명성을 제공한다[21].

가. 데이터 필드

SBOM 핵심은 SW를 구성하는 컴포넌트를 이해하는 데 사용되는 정보 식별 및 제공하는 일관된 통

표 7 데이터 필드 정보

데이터 필드	설명
공급업체 이름	컴포넌트를 생성, 정의 및 식별하는 엔터티 이름
컴포넌트 이름	원래 공급업체가 정의한 SW 단위에 할당된 지정 이름
컴포넌트 버전	공급업체가 이전에 식별된 버전에서 SW의 변경 사항을 지정하는 데 사용하는 식별자
다른 고유 식별자	컴포넌트를 식별하는 데 사용되거나 관련 데이터베이스의 검색 키 역할을 하는 기타 식별자
컴포넌트 종속성 관계	업스트림 컴포넌트 X가 SW Y에 포함되는 관계를 특성화한 정보
SBOM 데이터 작성자	컴포넌트에 대한 SBOM 데이터를 생성하는 엔터티의 이름
작성 일시	SBOM 데이터 만들어진 날짜 및 시간 기록

출처 Reproduced from [21].

일 표현으로, 표 7과 같은 데이터 필드에는 추적 및 유지 관리해야 하는 각 컴포넌트에 대한 기준 정보를 포함하고 있다.

나. 자동화 지원

자동화 지원은 자동 생성 및 기계 가독성을 포함한 자동화로, 기관 경계를 넘어 SW생태계 전반으로 확장할 수 있다. SBOM 데이터를 활용하려면 예측 가능한 구현과 데이터 포맷을 위한 도구가 필요하다.

SBOM을 생성하고 소비하는 데 사용되는 데이터 포맷은 다음과 같이 명시하고 있다.

- SW 패키지 데이터 교환(SPDX)
- SW 식별(SWID) 태그
- CycloneDX

SBOM을 구조화된 데이터 집합 이상으로 보안 또는 SW개발 생명주기에 통합하려면, 기관은 SBOM 사용 메커니즘에 초점을 맞춘 표 8과 같은 특정 사례와 프로세스를 따라야 한다. SBOM을 요청하거나 제공하기 위한 정책, 계약, 그리고 계약에는 여러 가지 요소(빈도, 깊이 등)가 명시적으로 언급되어야 한다.

Ⅲ. ETRI SW공급망 관리

1. 추진 체계

오픈소스의 사용 및 위험이 증가하고 있어, ’16년부터 SW공급망 관리의 목적으로 외부 배포 SW결과물에 대한 오픈소스 라이선스 검증을 추진하고,

표 8 사례 및 프로세스 정보

사례 및 프로세스	설명
1) SBOM 생성 빈도	SW 컴포넌트가 새로운 빌드 또는 릴리즈로 업데이트되는 경우, 새 버전의 SW를 반영하기 위한 새로운 SBOM을 생성해야 한다.
2) 컴포넌트 종속성 깊이	SBOM에는 모든 기본(최상위) 컴포넌트가 포함되어야 하며, 모든 전이 종속성이 나열되어야 하며, 전이 종속성 수준에 따라 투명성이 강화되어야 한다.
3) Known unknown	전체 종속성 그래프가 SBOM에 열거되어 있지 않은 경우, SBOM 작성자는 “Known Unknown”을 명시적으로 식별하며, 자동화된 데이터 처리에 통합되어야 한다.
4) 배포 및 전달	SBOM은 필요한 사람이 적시에 사용할 수 있어야 하며, 적절한 접근 권한과 역할이 필요하다.
5) 접근 제어	오픈소스 유지 관리자 또는 널리 사용되는 SW를 보유한 대부분의 공급업체는 SBOM 데이터를 공개하는 것이 자신의 이익에 가장 부합한다고 생각할 수 있다. 특히, 처음에는 이 데이터를 기밀로 유지하고 특정 고객이나 사용자에 대한 접근을 제한하고자 하는 기관이 있을 수 있다. 접근 제어를 원하는 경우, SBOM 데이터를 사용자의 보안 도구에 통합하기 위한 구체적인 허용 및 조정 사항을 포함하여 약관을 지정해야 한다.
6) 오류에 대한 양해	투명하고 가시적인 SBOM 적용을 위해 초기 사용은 누락과 오류 사용이 고려되어 구축되고 운영되어야 한다.

출처 Reproduced from [21].

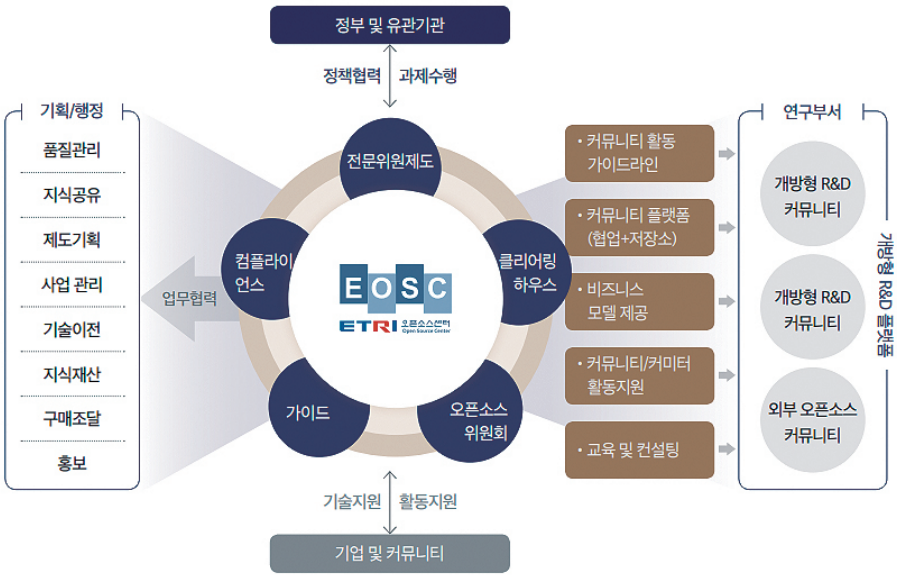

그림 1 ETRI 오픈소스 거버넌스 대응체계

'17년도 6월에 오픈소스전담조직(OSPO)으로 오픈소스센터를 설립하였다.

OSPO는 그림 1과 같이 오픈소스 거버넌스 체계 확립, 기획/행정 부서와 협업, 연구부서에 개방형 R&D 플랫폼 지원, 정부 및 관계기관과 정책을 협력, 기업 및 커뮤니티 활동 등을 지원하고 있다.

가. 정책 추진

SW결과물에 오픈소스SW 사용에 따른 위험 및 문제점을 최소화하여 SW공급망의 투명성을 제공하기 위해 별도의 SW공급망 관리 정책을 수립하여 시행하고 있다(표 9).

표 9 ETRI SW공급망 관리 정책

대상	SW공급망 관리 활동
내부 SW결과물	오픈소스 라이선스 검증을 통해 라이선스 준법성 여부를 확인한다.
외부에서 유입되는 용역/위탁 SW결과물	SW개발 시 오픈소스관리 계획을 수립하고, SW결과물에 대한 오픈소스관리 계획에 따른 라이선스 검증결과서를 확인한다.
외부로 배포하는 공개, 기술이전 SW결과물	SW결과물에 대한 외부 배포에 따른 오픈소스 사용 적정성 및 위험 여부를 심의한다.

나. 조직

오픈소스SW 사용에 따른 위험을 최소화하기 위해 OSPO는 오픈소스 거버넌스 체계를 구축하여 다음과 같은 업무를 수행하고 있다.

① 제도 및 정책
② 오픈소스 R&D 표준프로세스 정의
③ 외주 SW결과물 관리
④ 배포 SW결과물 관리
⑤ 라이선스/의존성/보안취약점 검증
⑥ 교육
⑦ 개방형 오픈소스 R&D 플랫폼 구축
⑧ 오픈소스 커뮤니티 구축 및 지원
⑨ 오픈소스 비즈니스 모델 개발
⑩ 법률 자문 등

다. 프로세스

SW개발 생명주기를 프로세스로 관리하여 SW공급망에서 SBOM 정보의 무결성 및 투명성을 제공한다.

1) 과제관리 프로세스 범주

SW공급망 관리를 위한 주요 프로세스의 활동은 표 10과 같다.

2) 시스템/소프트웨어 연구개발 생명주기 프로세스 범주

SW공급망에서 SBOM 관리를 위한 주요 프로세스의 활동은 표 11과 같다.

3) 조직기반 프로세스 범주

SW공급망 관리를 위해 연구개발 결과물을 외부 배포하기 위한 주요 프로세스의 활동 중 하나로 오픈소스심의 제도를 도입하여 운영하고 있으며, SW 결과물에 대한 외부공개 또는 기술이전 시 발생하는 기술적·법적인 위험이 없는지를 심의한다.

표 10 과제관리의 SW공급망 관리 활동

프로세스	SW공급망 관리 활동
사업수주 프로세스	수행계획서 작성 및 위탁/용역/공동연구 계획 수립 활동에서 오픈소스관리 계획을 작성한다.
외주관리 프로세스	과제추진 계획 수립 활동에서 오픈소스관리 계획을 수립하고, 외주 결과물 검증 활동에서 SW의 라이선스/의존성/보안취약점 검증을 수행한다.
인도 프로세스	과제 결과물로 SW의 라이선스/의존성/보안취약점 검증결과서를 확인한다.
커뮤니티 관리 프로세스	공개한 과제 결과물의 커뮤니티 운영 전략 및 결과 분석활동을 수행한다.

표 11 연구개발 생명주기의 SW공급망 관리 활동

프로세스	SW공급망 관리 활동
요구사항 정의 프로세스	프로세스에서 사용할 오픈소스를 조사하고 검증한다.
설계/구현 프로세스	오픈소스를 활용하고 검증한다.
시험 프로세스	SW결과물에 대한 라이선스/의존성/보안취약점 검증을 수행하여 시험결과를 작성한다.
소프트웨어 공개 프로세스	공개를 위한 전략을 수립하고, 오픈소스 정보(이름, 버전, 라이선스, 사이트) 및 외부 배포에 따른 적정성을 심의한다.

라. 교육

오픈소스에 대한 교육은 모든 구성원을 위해 부서별 특성에 따라 수시 온·오프라인 교육, 정기 온·오프라인 교육, 외부 전문가 교육 등을 시행하고 있다.

마. 도구

오픈소스 기반 SW 개발 및 관리를 위해 전사적인 차원에서 소스 분석 도구, 저장소 관리 도구 등을 지원하고 있다. 라이선스·의존성 관리를 위해 오픈소스SW 라이선스 검증 도구, 보안취약점 관리를 위한 오픈소스 보안취약점 검증 도구, SW결과물 저장 및 관리를 위한 저장소(GitHub, GitLab 등) 및 개발지원 도구(CI/CD 등)를 지원하고 있다.

2. SW공급망 관리 현황

ETRI는 '21년부터 외주 SW개발 결과물에 대한 오픈소스관리와 외부로 배포하는 SW결과물에 대한 관리를 그림 2와 같이 시행해오고 있으며, '22년부터 SW공급망 관점에서 그 범위를 확대함으로써 효율적이고 체계적인 관리를 위한 대응체계 개선을 추진하고 있다. 특히, SW공급망의 투명성 확보를 위해 외부개발(아웃소싱) SW결과물에 대한 오픈소스를 관리 체계를 마련함과 동시에 내부 공유 SW결과물에 대한 라이선스 검증 및 지식재산권에 대한 심의 등을 수행함으로써 외부 배포(기술이전, 공개)에 따른 투명성과 안전성을 확보하고 있다. 이러한 관리 체계는 향후 SBOM 기반으로 확대함으로써 오픈소스 관리/심의/검증의 효율성을 제고할 계획이다.

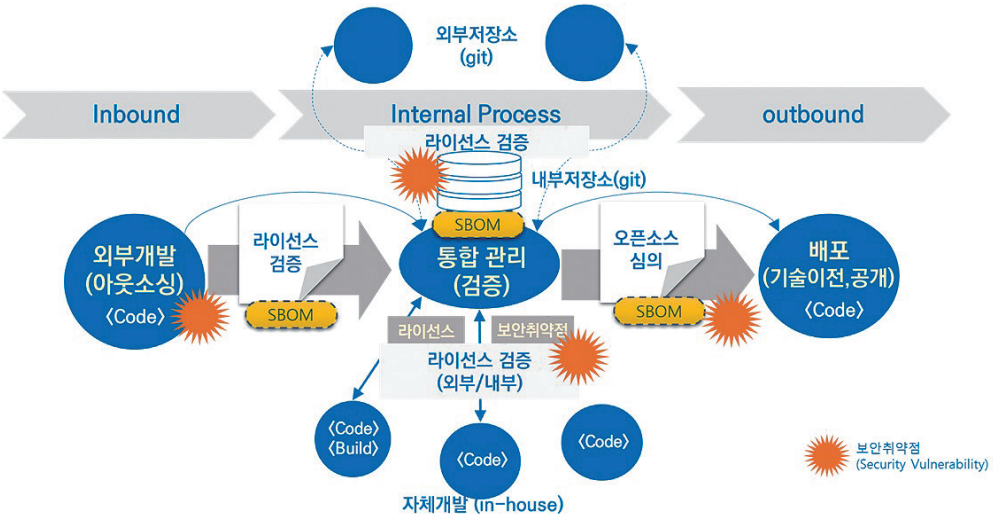

그림 2 ETRI SW공급망 관리 체계

Ⅳ. 결론 및 향후 과제

ICT 분야에서의 오픈소스 활용이 확대되고 동시에 보안취약점 문제가 증가함에 따라 국가적인 차원에서 SW공급망 관리의 중요성이 새롭게 인식되고 있다.

주요 국가의 SW공급망 관리 및 SBOM 정책을 살펴보면 SW공급망 투명성 제공을 위한 제도 마련과 함께 ICT 정책으로 확대를 추진하고 있다. 이에 따라 향후 SW제품의 글로벌 진출을 위해서는 SBOM 관리가 필수적인 요소가 될 것으로 전망되며, SBOM 관련 정책사례, 적용 가이드 및 백서 등의 발간으로 SBOM 활용을 권고할 것으로 보인다.

우리나라의 경우 과학기술정보통신부는 '23년 4월에 「소프트웨어 진흥 전략」을 발표하고[22], 세부 추진과제로 안전한 오픈소스SW 활용을 위해 라이선스 검증과 SBOM을 통해 투명한 SW공급망 관리를 지원하겠다는 계획을 소개한 바 있다.

최근 과학기술정보통신부와 한국소프트웨어산업협회(KOSA)는 소프트웨어(SW) 공급망 보안을 위해 'SW자재명세서(SBOM)' 확산을 위한 민간 협의체를 구성하여 국내 산업 맞춤형 SBOM 규격을 마련하고, 국내 SBOM 인지 확산과 기업 간 교류 확대를 통한 공급망 보안 강화를 추진하며, 국내 정보보호 전문기업을 선정해 실증 사업을 추진하여 실증 결과를 바탕으로 SW공급망 보안 가이드라인을 마련할 방침이다[23]. 국내 SW공급망의 SBOM 도입은 초기 상태로, SBOM 생성, 유통, 활용 측면에서 정부와 기업의 적극적인 SBOM 도입 검토가 필요하며, 이를 위해 산업 도메인에 필요한 SBOM 활용 백서(포맷, 도구, 모범사례 등) 발간이 시급히 필요하다.

원내 SW결과물의 활용 증가에 따라 SW공급망 관리가 매우 중요해지고 있으며, 위탁·용역 등 외주 SW결과물에 대한 오픈소스관리 제도 및 SW결과물의 외부 배포 시 오픈소스심의 제도 운영 등은 필수적인 요건으로 인식되고 있다. 특히, SBOM을 활용한 SW공급망 관리는 투명하고 안전한 SW유통 환경을 제공하며, SW개발의 무결성과 투명성 제공을 통하여 SW결과물의 품질을 제고하고 나아가 조직의 SW기술 경쟁력을 향상할 수 있을 것으로 기대한다.

따라서 향후에는 SBOM 활용 기반의 효율적인 SW공급망 관리 체계와 다양한 분야에서의 실증 기반의 SBOM 관리 체계 마련이 필요하며, 시장의 요구사항을 반영한 표준규격과 적용 가이드라인 제공이 동반되어야 할 것이다.

용어해설

SW공급망 소프트웨어의 생성, 배포, 그리고 유지보수 등과 이 과정을 관리하고 자동화하기 위한 시스템과 도구

SBOM 소프트웨어 자재명세서, 소프트웨어에 포함된 컴포넌트명, 버전, 라이선스, 체크섬 정보와 같은 소프트웨어를 구성하고 있는 다양한 메타데이터의 목록

오픈소스관리 SW개발 시 오픈소스 사용 및 개발에 따른 오픈소스 라이선스/의존성/보안취약점 관리, 특허 정보 관리, 라이선스 검증결과서 작성 등의 계획 수립과 SW결과물의 계획 대비 결과 확인 업무

오픈소스심의 제도 자체 개발 SW결과물을 외부에 배포하기 전에 오픈소스 정보(이름, 버전, 라이선스, 사이트), 특허 등을 검토하고 배포에 따른 문제점 및 위험성 없는지 심의하는 제도

약어 정리

CAICT	China Academy of Information and Communications Technology
DCMS	Department for Digital, Culture, Media & Sport
DIGIT	Directorate-General for Informatics
D-SBOM	Distributed SBOM
EU-FOSSA	Free and Open Source Software Auditing
FOSSEPS	Free and Open Source Software European Public Services
CISA	Cybersecurity & Infrastructure Security Agency
CPE	Common Platform Enumeration
C-SCRM	Cybersecurity Supply Chain Risk Management
ISA	Interoperability solutions for public administrations, businesses and citizens
NCSC	National Cyber Security Centre
NTIA	National Telecommunications and Information Administration
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OpenSSF	Open Source Security Foundation
OSPO	Open Source Program Office
OWASP	Open Web Application Security Project
SBOM	Software Bill of Materials
SSDF	Secure Software Development Framework
SPDX	Software Package Data Exchange
SWID	Software Identity
TTA	Telecommunications Technology Association
VEX	Vulnerability Exploitability eXchange

참고문헌

[1] 시놉시스, "시놉시스 2023 오픈소스 보안 및 위험 분석 보고서," 2023, https://www.synopsys.com/ko-kr/software-integrity/em/ossra.html

[2] Gartner, Gartner Identifies Top Security and Risk Management Trends for 2022, 2022. 3., https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022

[3] 김항규, "미국 SBOM(Software Bill of Materials) 정책 분석 및 시사점," SPRi, 2022. 12.

[4] 2023 OSSRA Webinar, "SBOM 소개 및 SBOM 대응을 위한 Black Duck 활용," 2023. 5.

[5] Synopsys, 2022 Open Source Security and Risk Analysis Report, 2022. 4.

[6] SPDX, https://spdx.dev/

[7] ISO/IEC 5962:2021, Information technology —SPDX® Specification V2.2.1, https://www.iso.org/standard/81870.html

[8] https://www.csoonline.com/article/3668530/sbom-formats-spdx-and-cyclonedx-compared. html

[9] https://cyclonedx.org/

[10] https://docs.sigstore.dev/cosign/overview/

[11] https://owasp.org/blog/2023/02/07/vdr-vex-comparison

[12] https://open-ae.eu/tag/open-source-software-

strategy-2020-2023/

[13] DIGIT, Directorate-General for Informatics, https://ec.europa.eu/info/departments/informatics_en

[14] 김항규, "주요국 SBOM(Software Bill of Materials) 정책 분석 및 시사점," SPRi, 2022. 12.

[15] https://joinup.ec.europa.eu/collection/fosseps

[16] D-SBOM(Distributed Software Bill of Materials), https://www.trublo.eu/d-sbom/

[17] https://openssf.org/community/alpha-omega/

[18] 김항규, "소프트웨어공급망 강화를 위한 글로벌 동향," SPRi, 2022. 4.

[19] TTA, "개방형 연구개발을 위한 공개소프트웨어 커뮤니티 거버넌스 지침," TTAK.KO-11.0256, 2019. 12.

[20] TTA, "공개 소프트웨어 공급망 관리를 위한 소프트웨어 목록 구성(SBOM) 속성 규격," TTAK.KO-11.0309, 2022. 12.

[21] The Minimum Elements For a Software Bill of Materials(SBOM), NTIA, 2021. 7., https://ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom

[22] 과학기술정보통신부, 소프트웨어 진흥 전략, 2023. 4.

[23] 전자신문, "공급망 보안 위한 S-BOM 협의체 뜬다," 2023. 7. 4., p. 18, http://mail2.scrapmaster.co.kr/mail/include/iitp_display.php?news_id=59628&scrapBookNo=1758&scrapinfo=202307040&article_serial=20230704