업을 확장해가는 선순환적 생태계를 조성해야 한다. 셋째, 메타버스는 향후 서비스 목적과 종류에 따라 다양한 이용자 수요가 있을 것으로 예상되므로 비즈니스 모델 구축이 중요하다. 메타버스 시장에 대한 기대는 긍정적인 측면과 부정적인 측면이 공존하고 있다. 시대와 기술의 변화에 따른 성장 가능성에 대해서는 긍정적인 전망이 주를 이루나, 이용자 관점에서 보면 대중성 확보에 대한 면밀한 검토가 필요하다. 현재는 게임 및 엔터테인먼트 분야를 주축으로 메타버스가 발달하고 있으나 향후 목적에 따라 더욱 다양한 분야에서 활용될 가능성이 크다.

참고문헌

[1] 남현숙, 전이슬, “2023년 SW산업 10대 이슈 전망”, SPRI 이슈리포트, IS-155, 2022.12.22.

[2] 김달훈, “메타버스 시장 2027년까지 연간 47.2%로 성장… 엔터테인먼트 산업 주도”, https://www.ciokorea.com/news/250456

[3] 김재현. “메타버스 시대 플랫폼 서비스에 필요한 XR 기술”, DMC XR 기술 세미나, 2021.05.26.

[4] McKinsey(2022.8), McKinsey Technology Trends Outlook 2022

[5] https://learn.microsoft.com/ko-kr/mesh/overview

[6] https://news.lgdisplay.com/kr/2021/07/가상공간에서-교육-효과-재미-월등-lg디스플레이/

[7] https://virnect.com/products/twin/

새롭게 부각되는 소프트웨어 공급망 관리를 통한 사이버 보안 규제와 표준 동향

최윤성 고려대학교 소프트웨어보안연구소 교수
박춘식 고려대학교 소프트웨어보안연구소 교수
이희조 고려대학교 소프트웨어보안연구소 교수
송상효 숭실대학교 소프트웨어학부 교수

1. 머리말: 소프트웨어 공급망 보안 등장

소프트웨어 분야 오픈소스 이용 확대와 함께 보안 취약성도 크게 증가함에 따라 각종 보안 사고가 급증하고 있다. 이에 따라 미국이나 유럽 등에서 소프트웨어 공급망 보안 강화를 위한 보안 고려 개발 검증, SBOM(Software Bill of Materials) 제출 의무화 제도 등이 검토 또는 도입되고 있다. 우리나라 IT 산업이나 제조 산업 등의 경쟁력에도 많은 영향을 미칠 것으로 예상된다. 이에 따라 공급망 보안과 관련된, 그 중에서도 SBOM과 관련된 새로운 제도와 규제, 표준화 동향 등도 새롭게 등장하고 있다.

특히 미국에서는 소프트웨어 공급망 보안 강화를 위해 대통령령에 의한 행정 명령이 나오고, 의료계나 자동차업계 등 산업계에서도 소프트웨어 공급망 보안과 관련된 각종 제도나 규제가 등장하고 있다. 소프트웨어 공급망 보안 강화를 위한 SBOM의 유효성이 급격하게 대두되어 SPDX(Software Package Data Exchange), CycloneDX, SWID(Software Identification), OpenChain 등 SBOM 관련 국제 표준들도 속속 등장하고 있다.

2. 소프트웨어 공급망 보안 강화의 필요성

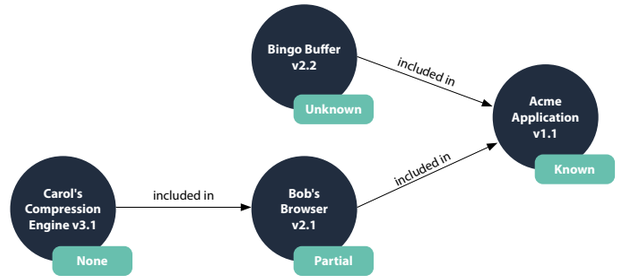
바이든 정부 출범과 함께 미국 사이버 보안 분야에 많은 변화가 나타나고 있다. 바이든 행정부는 정부 출범 시기부터 오바마 정부 사이버 안보 전문가로 활동했던 많은 전문가를 기용하거나 별도의 사이버 보안 조직을 신설하는 등 중국이나 러시아의 사이버 공격에 대응한 사이버 안보 정책에 강력한 의지와 대응을 보여 왔다.

그럼에도 불구하고 솔라윈즈 소프트웨어 제품이 악용돼, 복수의 연방 정부 기관과 민간 기업 100개 이상이 해킹 당했으며, 의료기관, 교육기관, 지방정부, 재판소 등도 랜섬웨어 공격을 당했다. 결국에는 미국 에너지 공급망에 대한 최악의 해킹 사고로 기억될 콜로니얼 파이프라인 사이버 공격 사태까지 발생해 미국의 사이버 안보 대응 역량의 문제점을 심각하게 드러냈다.

이에 따라 바이든 대통령은 정부 기관의 보안 향상, 연방 정부와 계약하고 있는 소프트웨어 제조사에 대한 새로운 기준 수립 등 연방 정부의 보안 대책을 향상시키는 내용을 담은 '국가의 사이버 보안 향상에 관한 행정 명령(Executive Order on Improving the Nation's Cybersecurity)'에 서명했다. 그러면서 미국 내에서 발생하는 일련의 사이버 공격에 대응하기 위해 정부와 민간 기업이 협력해 보다 안전한 사이버 공간을 육성하고, 정부가 규범을 정하여 주도해야 한다고 강조했다.

이 행정명령에 담긴 주요 내용은 사이버 위협 정보 공유의 장애 요소 제거, 다중 요소 인증, 암호화 채택, 제로 트러스트 아키텍처 도입, 안전한 클라우드 서비스로의 이행, 연방 정부 사이버 보안 체계 현대화, 소프트웨어 개발 위한 보안 기준 지침 수립, 구입자에 대한 각 제품의 소프트웨어 부품표(SBOM) 제공, 연방 정부와 조달 계약을 맺은 소프트웨어 회사에 대한 일정 수준의 사이버 안보 기준 충족 및 유지 의무 부과, 해킹 피해 보고 등이다.

이 중 SBOM은 소프트웨어의 개발, 배포, 이용, 업데이트 등과 같은 일련의 흐름을 말하는 소프트웨어 공급망에 대한 보안 강화를 위한 것이다. 연방정부와 사업 계약을 맺게 되는 기업들에 대한 SBOM 제출 의무화로 많은 민간 기업들의 소프트웨어 개발에 상당한 영향을 미칠 것으로 예상된다.



Conceptual SBOM graph with upstream relationship assertions

Component Name	Supplier Name	Version String	Author	Hash	UID	Relationship	Relationship Asserition
Application	Acme	1.1	Acme	0x123	234	Primary	Known
|--- Browser	Bob	2.1	Bob	0x223	334	Included in	Partial
|--- Compression Engine	Carol	3.1	Acme	0x323	434	Included in	None
|--- Buffer	Bingo	2.2	Acme	0x423	534	Included in	Unknown

Conceptual SBOM table with upstream relationship assertions

출처: 미 통신정보관리청(NTIA)

[그림 1] Software Bill of Material (SBOM)

소프트웨어의 구축에 사용되는 다양한 컴포넌트의 상세한 내용과 공급망의 관계에 관한 정식 기록을 보여주는 체계적인 기록인 SBOM은 식품 패키지에 기재된 성분 리스트와 유사하다. 복잡한 시스템이 어떻게 구성되어 있는 지를 가시화하여 추적 관리하기 쉽게 하기 위한 해결책으로 최근 수 년 주목받고 있다. SBOM은 복잡하게 구성된 소프트웨어를 이루는 요소들의 일람표이며, SBOM을 이용함으로써 시스템 구성을 쉽게 파악하고 관리할 수 있다.

오픈소스와 상용 소프트웨어 컴포넌트를 조합해 제품을 작성하는 소프트웨어 개발자와 제조사, 소프트웨어를 선택하고 구입하는 사람, 소프트웨어를 운용하는 사람 모두에게 유용할 것으로 생각된다.

SBOM을 구축해 이용하는 기업이나 사용자는 이들의 컴포넌트가 최신이라는 것을 확인하고, 새로운 취약성에 신속하게 대응할 수 있게 될 전망이다. 구입자는 취약성 분석이나 라이선스 분석을 행할 수 있어, 언제라도 부품의 리스크를 평가할 수 있다. 소프트웨어를 운용하는 사람은 새롭게 발견된 취약성의 잠재적인 리스크에 노출돼 있는지 신속하게 판단할 수 있다.

소프트웨어의 공급망을 이해하고, SBOM을 입수해 기존에 알고 있는 취약성을 분석할 수 있는 것은 시큐리티 리스크 관리에 큰 도움이 된다. 소프트웨어 공급망 보안, 더 나아가서는 국가의 사이버 보안 향상의 핵심이 될 것으로 판단된다.

소프트웨어 공급망 리스크 관리를 위한 노력

사이버 보안 공급망 위험 관리(C-SCRM, Cybersecurity Supply Chain Risk Management) 및 보안 소프트웨어 개발 프레임워크(SSDF, Secure Software Development Framework) 지침은 바이든 정부의 행정 명령 이전에도 존재했다. 그러나 2021년 벌어진 공급망 사이버 공격은 미국 연방 기관의 소프트웨어 보안 정책을 가속화하고 구체화했다.

소프트웨어 공급망의 전반적인 사이버 보안 위험은 공급업체(개발자 및 유통업체) 및 공급망(개발 환경 및 업데이트 제공 경로), 제품과 서비스에서 발생할 수 있는 잠재적 손상 및 침해 가능성으로 정의되며, 공격자는 제품 및 서비스에 포함된 보안 취약점 또는 의도하지 않은 외부 노출을 악용한다. 소프트웨어 공급망 공격 사건이 사회적 이슈가 되는 이유는 ① 공급자와 소비자 간의 정상적 계약 관계를 이용하여 방어 체계를 무력화함으로써 공급 시스템의 신뢰성을 약화시키고, 이에 따라 ② 내부 시스템에 설치된 HW나 SW의 범위를 넘어 생태계 가치사슬(Value Chain)을 공유하는 공급망까지 책임 범위가 확대되기 때문이다.

내부 조직이 아닌 외부 조직의 행동으로 인한 손실 가능성을 의미하는 '제3자 위험'은 SW 공급망에서 경계 방어 전략의 한계를 노출시켰다. 제3자 시스템이나 취약한 구성 요소의 종속성과 위험을 이용한 공격 방법은 피해자가 직접적으로 통제할 수 없는 영역에서 발생하므로 경계 방어만으로는 피해를 막을 수 없다. 따라서 SW 공급망에서 제품을 안전하게 생산하기 위해서는 기존의 경계망 대응 체계를 확장하여 다단계로 이루어진 제3자 구성요소까지 포괄하는 새로운 위험 관리 체계가 필요하다. 이는 SW 제품의 최종 소비자도 사이버 공격 위험에 대응하는 체계에 속함을 의미한다.

2021년 12월 발생한 Log4j 사건으로 기존 SW 정책에 오픈소스 SW 보안을 추가하게 되었다. 이듬해 1월 백악관은 Log4j 사건에 대한 대응 방안을 핵심 주제로 삼아 오픈소스 관련 정부기관과 민간기업, 비영리단체가 참여하는 회의를 열었다.

세계를 떠들썩하게 만든 Log4j 사건은 2013년 오픈소스 커뮤니티의 한 회원이 올린 수정본에서 시작됐다. Log4j는 수천 개의 SW 패키지에 통합돼 있을 정도로 널리 쓰이는 컴포넌트였지만, 당시 네트워크 시스템 및 하위 시스템의 SW 구성요소를 세부 목록화하여 관리하지 않은 조직은 Log4j 보안 취약점에 맞서 즉각적인 대응 조치를 할 수 없었다. 미국 사이버 안전 검토 위원회(Cyber Safety Review Board)의 보고서는 Log4j 위험이 여전히 많은 시스템에 존재하며, 보안에 취약한 인스턴스는 앞으로도 수년에서 10년 동안 남아 있을 것으로 예상했다.

작년 5월에는 리눅스 재단과 오픈소스 보안 재단(OpenSSF, Open Source Security Foundation)을 중심으로 '오픈소스 SW 보안 동원 계획(OSSSMP, Open Source Software Security Mobilization Plan)이 발표되었다. 백악관 논의의 목표를 이어받아 3대 핵심 목표를 설정하고, 각 목표별 실행계획과 예산을 구체화했다. OSSSMP에는 위의 3가지 목표를 기반으로 오픈소스 SW의 중장기 보안 향상을 목표로 구체적인 10가지 전략 계획 스트림이 포함되어 있다. (<표 1>)

SBOM은 2018년 미국 통신정보관리청(NTIA, National Telecommunications and Information Administration)을 중심으로 민관 정책 이해관계자들이 모인 'SW 구성요소의 지속적인 투명성 강화를 위한 논의'를 통해 등장한 정책으로, 일련의 대규모 보안 사고와 행정명령으로 촉발된 'SW 구성요소를 표현하는 미국 중심의 표준화 정책'으로 요약할 수 있다. 초기 SBOM은 공급망 보안이 아니라 최신 디지털 인프라의 낮은 신뢰성을 개선하기 위한 목적이었고, 특히 오픈소스 SW 구성요소의 의존성, 관리 주체의 불확실성, SW 공급망의 복잡성으로 인한 문제점 개선을 다뤘다.

이후 9월 백악관 관리예산처(OMB, Office of Management and Budget)는 '안전한 SW 개발 체계를 통한 SW 공급망 보안 강화'에 관한 각서(Memorandum)를 발표했다. 이에 따라 연방정부 기관에 SW 납품을 원하는 모든 공급업체는 NIST의 SSDF 및 SW 공급망 보안 지침을 준수하고 이에 대한 자체 증명을 제출해야 한다. 각서에 따르면 모든 연방 기관의 SW가 안전하게 생산되었음을 증명하기 위한 증거를 공급자에게 요청할 수 있으며, 공급자는 NTIA에서 설정한 최소 요구 사항을 충족하는 SBOM을 증거로 제출할 수 있다. 본 각서가 발효된 지 365일2023년 9월 21일까지) 이내에 각 연방 기관은 각서에 포함된 모든 SW의 증거를 수집해야 한다.

<표 1> OpenSSF의 '오픈소스 SW 보안 동원 계획' 개요

백악관 회의 주제		OSSSMP 목표
1. 코드 및 오픈소스 패키지의 보안 결함 및 취약성 방지	개발도구의 보안 기능 통합 코드 서명 및 디지털 ID를 통한 빌드(Build), 저장 및 배포 인프라 보호	오픈소스 SW 생산 확보 스트림 1. 보안 교육 스트림 2. 위험 평가 스트림 3. 디지털 서명 스트림 4. 메모리 안전성
2. 결함 발견 및 수정 프로세스 개선	오픈소스 프로젝트의 우선순위 지정, 유지 관리를 위한 메커니즘 마련	취약점 발견 및 개선 스트림 5. 사고 대응 스트림 6. 스캐닝 향상 스트림 7. 코드 감사 스트림 8. 데이터 공유
3. 수정 배포 및 구현에 대한 응답 시간 단축	기업과 개발자의 SBOM 사용을 가속화하고 개선하는 방안	생태계 패치 대응 시간 단축 스트림 9. SBOM 보급 스트림 10. 공급망 개선

3. 소프트웨어 공급망 관련 국내외 표준화 동향

NTIA는 SW 공급망 관리를 위한 SBOM의 최소 요소를 소프트웨어 구성 요소의 공급업체 식별, 구성 요소 버전에 대한 세부 정보 식별, 구성 요소 고유 식별자, 모든 구성 요소 종속성 관계, 시기와 기한의 타임스탬프, SBOM 보고서를 만든 사람으로 정의했다.

NTIA 가이드라인은 SPDX, CycloneDX 및 SWID의 세 가지 표준을 승인된 형식으로 지정했고, NTIA는 SBOM의 최소 요소를 정의하고 배포하는 정책 기준도 마련하였다. 또한 SBOM이 자동으로 식별 가능하도록 SBOM 생성을 위한 개방형 표준인 SPDX(Software Package Data Exchange), 경량 SBOM 표준인 OWASP(The Open Web Application Security Project) CycloneDX, 국제표준화기구(ISO, International Organization for Standardization) 및 국제전기표준회의(IEC, International Electrotechnical Commission)가 개발한 XML 파일 형태의 SWID(Software Identification) 태그 등의 3가지 표준 형식 중 하나를 반드시 따르도록 요구하고 있다. 이 세 표준은 바이든 정부의 행정명령 이전부터 사용 사례를 해결하기 위해 다양한 오픈소스 프로젝트와 정부 기관에서 개발했다. 세 가지 모두 최소 SBOM 지침을 충족하지만 프로세스, 결과, 적용 범위가 다르고, 로드맵도 다르다.

SW 공급망 관련 국제 표준은 SBOM 도구들의 표준화 및 관리를 위해 만들어진 것들도 있고, 오픈소스 SW의 컴플라이언스와 프로세스 관리

를 위한 목적으로 하는 OpenChain의 국제표준(ISO/IEC 5230:2020)도 있다. 국내에서는 한국정보통신기술협회(TTA)의 공개 소프트웨어 프로젝트 그룹(PG602)을 통해서 정보통신단체표준(국문표준) 관련 논의를 진행하고 표준들을 만들고 있다.

[SPDX]

2021년 9월 9일 - Linux Foundation, JointDevelopment Foundation 및 SPDX 커뮤니티는 SPDX®(Software Package Data Exchange®) 사양이 ISO/IEC5962:2021로 게시되었으며 국제 공개 표준으로 인정받았다고 발표했다. SPDX는 보안, 라이센스 준수 및 기타 소프트웨어 공급망 증거에 대한 표준이다. Intel, Microsoft, Siemens, Sony, Synopsys, VMware 및 WindRiver는 SPDX를 사용하여 글로벌 소프트웨어 공급망 전반에서 규정을 준수하고 안전한 개발을 보장하기 위한 정책 또는 도구에서 SBOM 정보를 전달하는 대표적인 회사이다. SPDX는 공급망 전체에서 소프트웨어가 생성, 배포 및 소비되는 방식에 대한 신뢰와 투명성을 구축하는 데 중요한 역할을 하고 있고, 사실상의 산업 표준에서 공식 ISO/IEC JTC 1 표준으로의 전환으로 인해 SPDX는 글로벌 무대에서 채택율이 크게 증가하고 있다.

[CycloneDX]

CycloneDX는 애플리케이션 보안 컨텍스트 및 공급망 구성요소 분석에 사용하도록 설계된 경량 SBOM 표준으로 오픈소스 웹 애플리케이션 보안 프로젝트(OWASP)에 의해 개발되었으며 소프트웨어 보안 요구사항 및 위험 분석을 위해 설계되었다. CycloneDX는 JSON, XML 언어로 작성되며 빌드 시스템에 구현하여 유연하고 쉽게 채택하여 활용할 수 있다. BOM에 대한 메타데이터를 제공하여 제공업체 정보, 라이선스 및 저작권 정보, 구성요소 간 종속성 등을 통해 SBOM 역할을 지원한다. CycloneDX는 국제 표준에 등록이 되어 있지는 않다.

[SWID]

SWID(Software Identity)는 소프트웨어 정보에 대한 태그를 생성하여 장치에 설치된 상용 및 오픈소스 소프트웨어 인벤토리를 지원하는 장치이다. SWID는 ISO/IEC19770-2 표준에 의해 정의되었으며 소프트웨어 제품의 특정 릴리즈에 대한 정보를 포함하고 있다. SWID 태그는 소프트웨어 생명주기와 연계되어 소프트웨어 구성요소에 대한 식별 정보, 소프트웨어 산출물에 대한 파일 및 암호화 해시 목록, SBOM(태그) 작성자 및 소프트웨어 구성요소에 대한 출처 정보를 제공한다. SWID 태그 정보는 SBOM 데이터로 활용 가능하며, 다른 SWID 태그에 링크하여 명시할 수 있어 소프트웨어의 종속 관계를 나타낼 수 있는 장점이 있다. 현재 SWID 태그는 XML 형식으로 제공되어 용량이 크기 때문에, 향후 CBOR(Concise Binary Object Representation)을 기반으로 경량화된 SWID 태그 정보를 제공할 수 있는 CoSWID(Concise SWID)의 사용도 기대된다.

[OpenChain]

ISO/IEC 5230은 오픈소스가 포함된 소프트웨어의 공급망 관리를 위해 Linux Foundation의 OpenChain Project에서 만든 규격으로 2020년 국제표준으로 인증되었다. 소프트웨어 공급망 내 신뢰할 수 있는 오픈소스 컴플라이언스를 보장하기 위한 최소한의 핵심 요구 사항을 정의하였다. OpenChain 규격은 기업 규모나 업종과 관계없이 모든 기업에 적합하도록 설계되었다. 2016년 OpenChain 규격 버전 1.0이 발표되었고, 2020년 버전 2.1의 규격이 배포됐다. 기업이 오픈소스 컴플라이언스 달성을 위해 꼭 수행해야 할 여섯 가지 핵심 요구사항(프로그램 설립, 관련 업무 정의 및 지원, 오픈소스 콘텐츠 검토 및 승인, 컴플라이언스 산출물 생성 및 전달, 오픈소스 커뮤니티 참여에 대한 이해, 규격 요구사항 준수)과 이를 입증하기 위해 필요한 자료 목록을 정의하고 있다. OpenChain은 SPDX를 기반으로 구성되고 관리되고 있다.

국내는 SW 공급망 관련 표준보다는 공개소프트웨어 공급망 관리를 위한 SBOM 속성 규격을 TTA 공개 소프트웨어 프로젝트 그룹(PG602)에서 논의하여 정보통신단체 표준을 2020년과 2022년 12월 제정했다. 2020년 10월에는 “오픈체인 기반 공개 소프트웨어 공급망 관리 지침”을 만들었다. 이 표준은 공개 소프트웨어 개발 및 사용이 산업 전반에 걸쳐 급증하고 있는 반면 공개 소프트웨어 공급망 관리 부재로 인한 피해 및 이슈에 대응하기는 어렵다는 어려움을 해소하기 위한 표준이다. 산업에서 공개 소프트웨어를 보다 안전하고 유연하게 개발 및 사용할 수 있도록 리눅스 재단에서 운영하고 있는 공개 소프트웨어 공급망 관리를 위한 오픈체인 프로젝트에서 제시하고, OpenChain 2.0 Specification의 준수사항 및 2020년 1월 20일 정보통신산업진흥원에서 제정한 기업 공개SW 거버넌스 가이드(OpenChain 2.0 해설서)를 기반으로 한 실무 가이드를 제시했다. 2022년 12월에 제정한 “공개 소프트웨어 공급망 관리를 위한 소프트웨어 목록 구성(SBOM) 속성 구성” 표준에서는 다양한 소프트웨어 공급망과 사용목적에 따른 가변적인 소프트웨어 구성요소목록 관리에 있어 소프트웨어 공급자들이 기본적인 기준을 가지고 소프트웨어 구성요소목록을 생성 및 관리할 수 있도록 소프트웨어 개발 및 공급에 공통적으로 필요시 되는 15가지의 소프트웨어 구성요소 관리 항목을 제시하고 있다.

4. 맺음말

현재 제품 기반 공급망에서 사용되는 BOM은 대부분 하드웨어(부품)의 유통과 품질을 관리하는 용도로 활용되어 왔다. 그러나 예전과 달리 대부분의 하드웨어(부품)들이 소프트웨어를 포함하는 형태로 변화함에 따라 소프트웨어를 관리하는 공급망의 필요성이 요구되어 왔다. 최근에 오픈소스 소프트웨어의 유통을 관리하고 사용된 코드에 포함된 취약점을 관리하는 목적도 추가되어 오픈소스 거버넌스의 중요한 항목으로 인지되었다. 오픈소스 취약점으로 발생하는 다양한 보안 문제에 대응이 큰 이슈가 되었기 때문이다.

소프트웨어 공급망 보안의 강화는 미국의 경우 바이든 정부가 사이버 보안 이슈에 대응하는 형태로 진행되고 있고, 유럽연합은 기업을 중심으로 소프트웨어 공급망 기반 보안을 강화하려는 형태로 대응을 하고 있다. 한국의 경우 수출기업을 중심으로 오픈소스 소프트웨어 공급망 관리와 취약점 대응을 시작하였으며, 정부 및 공공기관은 관심은 가지고 있으나 대응은 시작하지 못하고 있는 것으로 보인다. 다만, 미국 정부의 추진 방향을 지켜보면서 정부와 공공기관에서 어떻게 대응해야 되는지에 대해서는 과학기술정보통신부를 통해서 준비하고 있지만, 실제로 정부의 적용은 진행되고 있지 못한 상황이다.

정부/공공기관, 중소기업은 아직 오픈소스의 취약점에 대한 준비조차도 제대로 대응하고 있지 못한 상황이라 소프트웨어 공급망과 SBOM의 적용도 고려되지 못하고 있다. 그러나 향후 디지털 시대의 보안은 외부 침입에 대한 보안도 중요하지만, 개발 단계부터 오픈소스 소프트웨어와 외부에서 개발된 모듈 관리를 위한 SBOM을 도입하고,이를 기반으로 소프트웨어 공급망 기반의 리스크가 관리되어야 할 것이다.

※ 본 연구의 일부는 2022년 과학기술정보통신부의 재원으로 정보통신기획평가원의 지원을 받아 수행된 SW 공급망 보안을 위한 SBOM 자동 생성 및 무결성 검증 기술 개발 과제의 일환으로 수행됨

참고문헌

[1] 최윤성(2022), 미국의 소프트웨어 공급망 보안 정책 동향: SBOM 사례를 중심으로, 정보보호학회지, 제32권 제5호, pp. 7-14;
[2] 이태준, 이희조, 박춘식(2022), 소프트웨어 보안 관점에서 본 미국 사이버보안 행정명령과 우리의 대응 방안, KISA Report, Vol 12
[3] 박춘식(2021), 미국 사이버 보안 행정 명령에 대한 단상, 데이터넷
[4] NIST, “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (C-SCRM)”, May 2022.
[5] US Cyber Safety Review Board, “Review of the December 2021 Log4j Event”, July 2022.
[6] Linux Foundation, “The Open Source Software Security Mobilization Plan”, May 2022.
[7] US Office of Management and Budget (OMB), “Enhancing the Security of the Software Supply Chain through Secure Software Development Practices - MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES“, Sept. 2022.
[8] [시장동향] 오픈소스 취약점 노린 SW공급망보안 위협, ‘SBOM’이 해결사 될까 - 컴퓨터월드 정종길 기사 2023.01.31
[9] [SETTLETOP] SBOM 표준 이해: CycloneDX,SPDX, SWID 소프트웨어 SBOM(Bill of Materials) - 소프트웨어 공급망 위험 8월 27일
[10] SPDX, 소프트웨어 BOM에 대한 국제적으로 인정받는 표준이 됨 -리눅스 재단 | 2021년 9월 9일
[11] 사이버안보 강화를 위한 소프트웨어 공급망 보안 정책 연구: SBOM 정책 추진 사례를 중심으로 - 손효현, 김동희, 김소정 (국가보안기술연구소)
[12] OSBC - 오픈소스 ISO 5230 인증 컨설팅
[13] 공개 소프트웨어 공급망 관리를 위한 소프트웨어 목록 구성(SBOM) 속성 규격 - 정보통신단체표준(국문표준) TTAK.KO-11.0309