정 보 보 호 학 회 지
제 32 권 제5호, 2022. 10

미국의 소프트웨어 공급망 보안 정책 동향: SBOM 사례를 중심으로

최 윤 성*

요 약

2021년에 발생한 일련의 소프트웨어 공급망 공격으로 미국 연방 정부의 사이버보안 개선 정책이 가속됐다. 이중 소프트웨어 구성 정보를 유통하는 SBOM 정책은 SW 구성요소의 투명성을 강화하여, 이를 활용하는 공급자와 수요자의 보안 인식 개선에도 도움을 줄 것이 기대된다. 다만 SBOM으로 공급망 보안 위협을 완화하려면 해결해야 할 기술적 이슈가 있고, SBOM 수집자를 위한 구체적인 가이드도 마련되지 않아 제도 정착에는 시간이 걸린다. SW 공급망 문제는 SW 개발 관행에 대한 지속적인 개선이 요구되며, 글로벌 연쇄 위험으로 결코 혼자서는 해결할 수 없다. 따라서 우리는 실태조사, 실증사업 등을 시작으로 현실에 맞는 정책을 먼저 적용하고, 제도적 조화를 위한 국제협력에도 힘써야 한다.

Ⅰ. 서 론

"우리의 세계는 서로 연결되어 있고, 적들은 이러한 연결의 가장 약한 고리를 수시로 노리고 있다"

정보통신기술(ICT)은 전 세계에 분산되어 여러 단계로 복잡하게 구성되고, 다양한 경로로 상호 연결된 공급망 생태계(Ecosystem)를 이룬다. 소프트웨어(SW) 공급망의 전반적인 사이버보안 위험은 공급자(개발업체 및 배포업체), 공급망(개발 환경 및 업데이트 전송로), 제품 및 서비스에서 발생할 수 있는 피해와 침해 가능성으로 정의되며, 사이버보안 위협원은 공급망 자체 또는 제품 및 서비스에 포함된 보안 취약점이나 의도치 않은 외부 노출을 악용하여 공격을 시도한다.[1]

2021년은 전 세계의 기업과 정부 기관을 대상으로 SW 공급망 공격이 유행한 해였다. 사이버보안 기업 Kaspersky의 조사에 의하면, 작년 한 해 동안 기업 대상 공급망 공격과 관련된 데이터 유출 사고의 평균 비용은 140만 달러(약 20억 원)로, 다른 유형의 사이버 공격보다 높게 나타났다.[2] 또한 Gartner는 2025년까지 전 세계 조직의 45%가 SW 공급망 공격을 경험할 것이며, 이는 2021년 조사 결과의 3배에 달한다고 예상했다.[3] 이렇게 SW 공급망을 이용한 공격은 경제적 피해가 크고 추가적인 위협도 예상되는 만큼 대비책 마련이 필요하다.

2021년 5월, 바이든 대통령은 '국가 사이버보안 개선에 관한 행정명령(EO 14028)'을 발표하며, 사이버보안 사고의 예방, 탐지, 평가 및 개선이 국가 및 경제 안보에 최우선 순위이며 필수적임을 강조했다. 특히 SW 공급망 강화에 관한 4절에서는 NIST(National Institute of Standards and Technology) 등 관련 부처와 기관에 1) SW 공급망 보안을 강화하기 위한 가이드 발행, 2) 주요 SW의 정의 및 보안 지침 발행, 3) 소프트웨어 라벨링(Labeling) 등의 조치를 지시했다.[4]

이중 소프트웨어 재료명세서(Software Bill of Materials, SBOM)는 우리가 사용하는 SW의 개발 및 취득, 운영에 대한 정보공유 방식을 개선하는 정책으로, SW 구매자가 정보에 입각한 선택을 할 수 있는 투명성을 보장한다.[5] 보다 구체적으로 SBOM은 SW를 만드는데 필요한 모든 구성요소에 대한 목록으로써, 미국 연방 기관의 SW 조달 시 함께 제출하도록 권고되고 있어, 본 제도가 활성화될 경우, 개발자뿐만 아니라 공급자와 수요자의 SW 안전에 대한 인식 변화가 함께 뒤따를 것으로 기대된다.[6]

본 행정명령은 미국 내 연방 기관을 대상으로 만들어진 정책을 담고 있지만, SW 보안을 개선하기 위한 공통 평가 기준이나 프로젝트, 지침서, 모범 사례 등은 우리 정부의 추진정책이나 기업의 보안 전략 수립에도 참고할 수 있다.

* 고려대학교 소프트웨어 보안 연구소 (산학협력중점교수, yunseong@korea.ac.kr)

이에 본문에는 피해 사례에 기반한 공급망 공격의 특징을 알아보고, 추가되는 보안 위협과 대응 방안을 분석한다. 그리고 미국 행정명령으로 촉발된 공급망 보안 정책과 SBOM의 도입 이슈를 소개한다. 결론에는 이러한 사례를 종합하여 국내 공급망 보안 정책에 반영하기 위한 시사점을 도출한다.

Ⅱ. 미국의 공급망 공격 사례

2021년 미국에서 발생한 일련의 공급망 공격 피해 사례를 살펴보면, 공급망 공격의 초기 단계에서 피싱(Phishing), 취약점, 악성코드 또는 랜섬웨어 전파 등 기존의 사이버 공격과 같은 기법을 사용하고 있다. 그리고 SW 공급자 시스템과 오픈소스(Open Source) SW 구성요소의 취약성을 활용한 공격 방법으로 큰 피해를 가져왔음을 알 수 있다. 특히 전 세계적으로 다수의 사용자를 보유한 IT 시스템이나 최근 외부 연결성의 증가로 사이버 공격의 주요 대상이 되는 사회기반시설이 공급망 공격으로 막대한 경제적 손실뿐만 아니라 연쇄적인 피해로 이어지는 사건이 지속해서 발생했다.

〔표 1〕 주요 공급망 공격 피해 사례

Case	Damage
Microsoft Exchange (2021-01)	이메일, 일정, 연락처 기능을 제공하는 MS 익스체인지 서버 SW의 취약점이 알려져, 전 세계 약 40만 개의 익스체인지 사용자가 공격에 노출됨〔7〕
SolarWinds (2021-04)	IT 소프트웨어 공급 업체의 SW 배포 시스템에 악성코드를 설치하는 공격 방식으로 1만 8천 명의 고객이 타격을 받음〔8〕
Codecov (2021-04)	컨테이너 이미지의 취약점을 악용해 SW 배포 환경의 인증 정보가 유출되는 사건이 발생함. Codecov는 소스코드 테스팅 기업으로, 전 세계의 2만 9천여 개 고객사가 영향을 받음〔9〕
Colonial Pipeline (2021-05)	송유관 회사의 IT시스템이 랜섬웨어에 감염되어 美 남동부 8,900km 일대 공급이 중단되고, 지역 휘발유 가격이 급상승함 (시스템 복구의 대가로도 약 50억 원의 가상화폐를 지불)〔10〕
Kaseya (2021-07)	중앙에서 원격으로 업데이트되는 컴퓨터에 악성코드를 배포하는 공격 방식으로 17개 국가의 800~15,000개 기업에 피해가 발생함〔8〕
Log4shell (2021-12)	수 천개의 패키지에 통합되어 있으나, 관리되지 않던 오픈소스 SW 구성요소에서 심각한 보안 취약점이 발견되어, 이를 악용한 공격이 계속 시도됨〔11〕

공급망 공격 사건이 사회적 이슈가 되는 이유는 1) 공급자와 소비자의 정상적인 계약 관계를 악용하여 방어 체계를 무력화시킴으로써, 공급 체계의 신뢰성을 약화하는 효과와 이에 따라 그동안 2) 내부 시스템에 설치된 HW와 SW만 책임 범위라는 인식이 생태계 가치사슬(Value Chain)을 공유하는 공급망까지 확대되었기 때문으로 분석된다.

내부가 아닌 외부 조직의 행위로 인해 손해 볼 가능성을 뜻하는 '제3자 위험(3rd Party Risk)'은 SW 공급망에서 경계선(Perimeter) 방어 전략의 한계를 노출했다. 이렇게 타사(3rd Party) 시스템 또는 취약한 구성요소의 종속성과 위험을 이용한 공격은 피해 당사자의 직접적인 제어가 불가능한 영역에서 발생하여, 경계선 방어만으로 피해를 예방하기가 불가능하다.

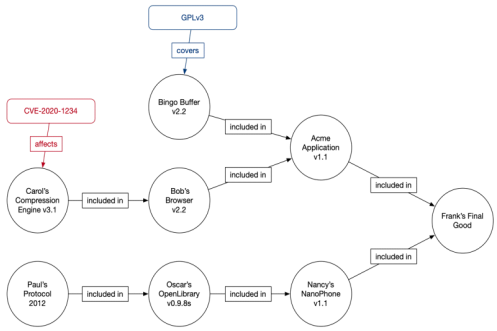
따라서 SW 공급망에서 안전하게 제품을 생산하기 위해서는 다단계의 타사 구성요소를 포괄하는 위험 관리(Risk Management) 체계가 필요하며, 이것은 기존 경계망 대응체계를 확장하여, SW 제품 공급에 관련된 모든 가치사슬 참여자와 최종 제품의 수요자도 사이버 공격의 대비에 참여해야 한다는 것을 뜻한다.

Ⅲ. 미국의 SW 공급망 보안 정책

3.1. SW 신뢰성 강화를 위한 SBOM

SBOM은 2018년 미국의 통신정보 관리청(National Telecommunications and Information Administration, NTIA)을 중심으로 민관의 정책 이해관계자가 모인 'SW 구성요소의 지속적인 투명성 강화를 위한 논의'를 통해 나온 정책이며, 일련의 대형 보안 사고와 행정명령으로 촉발된 'SW 구성요소를 표현하는 미국 중심의 표준화 정책'이라고 요약할 수 있다.

SBOM은 기본적으로 SW 구성요소에 대한 종속 관계를 표현하며, SW의 구성 정보를 교환하는 것이 전반적인 SW 구성요소의 투명성을 증가시키고, SBOM을 활발히 유통함으로써 공급망 체계의 신뢰도가 점차 높아진다는 아이디어이다. 다만 SBOM 정책은 하나의 표준만을 정하지 않고, 시장에서 활발히 유통되는 서



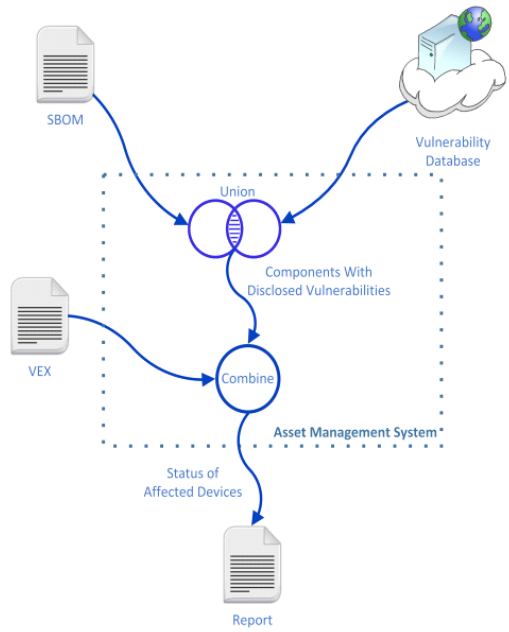
〔그림 1〕 SBOM Example (NTIA SBOM Framing Working Group, 2021)

로 다른 3개의 표준(SPDX, CycloneDX, SWID)을 모두 지원하고, 최소 요구 사항을 정의하는 방법으로 상호운용성을 확보했다.[12]

SBOM 정책은 우리의 현실 세계가 디지털 인프라에 대한 의존도는 갈수록 높아지고 있는데, SW 구성요소는 사회적인 중요도에 비해 신뢰성과 투명성이 부족하다는 인식에서 기인한다. 전 세계에 큰 파문을 가져온 Log4j 사건은 지금으로부터 9년 전인, 2013년에 오픈소스 커뮤니티의 한 구성원이 올린 수정 버전에서부터 시작되었다. 수천 개의 다른 SW 패키지에 통합되어 있을 정도로 많이 사용되는 구성요소였으나, 당시 네트워크 시스템과 하위 시스템의 SW 구성요소를 세부 목록화하여 관리하지 않던 조직들은 Log4j 취약점에 즉각적인 대응조치를 하지 못했다. Log4j의 위험성은 여전히 많은 시스템에 존재하고 있어 보안에 취약한 인스턴스(Instance)가 앞으로도 수년에서 10년 이상 남아 있을 것으로 평가되며, SBOM이 이러한 취약점 대응 시간을 줄일 것으로 판단된다.[13]

3.2. SBOM 도입의 이슈 사항

SBOM은 데이터 표현의 중간 단계이며, 특정 시점의 스냅숏(Snapshot) 정보이기에, 동적으로 관리되는 SW의 특성상 SBOM이 발행된 이후 발생한 신규 SW의 취약성 식별을 지원할 수 없는 한계가 있다. 이에 VEX(Vulnerability and Exploitability eXchange)와 같이 별도로 제공되는 취약점 데이터와 상시 결합해야 공급망 보안 목표를 달성하는데 활용될 수 있다. 즉, SBOM 생성에서 작업이 종료되는 것이 아니라 단계별로 지속적인 정보 업데이트가 요구된다.[14]



〔그림 2〕 SBOM & VEX Ecosystem Example (Draft, Requirements for Sharing of Vulnerability Status Information, 2020)

SBOM은 SW의 중첩된 구조를 담고 있어 복잡하며, 사람이 이해하기 쉬운 형식이 아니기 때문에 기계 가독성(Machine-readability) 확보를 위한 추가적인 표준화도 필요하다.[15] 보안 및 사물인터넷에 관한 표준화를 담당하는 비영리 기관인 OASIS (Organization for the Advancement of Structured Information Standards)는 현재 HTML, PDF와 같은 정적 문서 형태의 보안 권고문을 VEX 정보를 포함하여, 구조화된 언어로써 자동화하는 CSAF(Common Security Advisory Framework 2.0)를 개발 중이며,[16] JSON 기반의 CASF 문서 생성 도구(Secvisogram)도 무료로 배포한다.[17]

또 다른 비영리 재단인 OWASP(The Open Web Application Security Project)는 SW 공급망의 구성요소 관리에 대한 검증을 표준화하고, 보증 수준을 정하는 SW 구성요소 검증 표준(Software Component Verification Standard, SCVS)을 개발했다. SCVS 1.0은 3가지 검증 수준과 인벤토리, SBOM, 개발 환경, 패키지 관리, 성분 분석, 가계 및 출처의 6개 컨트롤 집합으로 구성되며. 자사 및 협력사 평가에도 활용할 수 있다.[18]

SBOM 표준화를 위해 구성요소 명칭을 통일해야 하는 것도 선결 과제이다. 이는 글로벌 SW 네임스페이스(Namespace)를 체계화하는 장대한 작업에 비유할 수 있는데, 향후 유지 관리에도 많은 예산이 필요할 것으로 예상된다. DNS(Domain Name System) 및 IP 주소공간 할당 등을 관리하는 국제 인터넷주소 관리기구(Internet Corporation for Assigned Names and Numbers, ICANN)를 유사한 사례로 볼 수 있는데, ICANN은 중앙집권적인 관리기구로 전 세계에서 통용되는 단일 도메인 명칭을 유지하기 위해 등록 수수료를 부과하고 있다.[19]

Ⅳ. SBOM 활성화 정책

Log4j 사건으로 활성화된 SBOM 정책은 백악관의 1월 민관의 가속화 논의를 시작으로, 9월에 발표된 '행정 부처와 기관장을 위한 SW 공급망 보안 개선에 대한 각서(Memorandum)'를 통해 구체화 되었다.

〔표 2〕 미국 SW 공급망 보안 정책 타임라인 (2022)

US Policy	SBOM Remark
2022-01 White House Meeting on Software Security	Log4j에 대한 대응 방안을 주제로 정부와 민간 부문이 논의 (SBOM 가속화 등)
2022-05 Linux Foundation's Open Source SW Security Mobilization Plan	SW의 패치 배포 및 적용에 대한 응답 시간을 단축하는 방안으로써 민간 차원의 SBOM 활성화 방안 수립
2022-06 IMDRF's Drafting on "Principles and Practices for SBOM for Medical Device Cybersecurity"	SW 생산 비용의 큰 증가 없이 의료기기에 포함된 타사 SW의 취약성을 활용한 공격 가능성을 낮추는 방안으로 SBOM 활용 권고
2022-08 ESF's Securing the Software Supply Chain - Recommended Practices Guide for Developers	제조사는 SW의 보안 기준을 설정해야 하며, NTIA 표준과 SCA 도구를 활용해 SBOM을 생성하며, 타사 구성요소의 검증을 권고
2022-09 OMB's Enhancing the Security of the Software Supply Chain to Deliver a Secure Government Experience	연방 기관은 SW를 납품하는 생산자에 NIST 지침에 따른 자체 증명을 요구해야 하며, SW 개발 보안에 대한 적합성 입증 용도로써 SBOM을 요구할 수 있음

4.1. White House Meeting on Software Security (2022년 1월)

행정명령(EO 14028)을 통해 지속적이고 점점 더 정교해지는 악의적 사이버 캠페인(Campaign)에 대응하기 위해 정부 조치 이상의 노력이 필요하며, 사이버 보안 사고의 예방, 탐지, 평가 및 해결을 위한 연방 정부와 민간 부문이 협력이 필수적임을 강조했다. 이러한 인식 변화에 따라 백악관은 1월에 정부 기관과 민간 기업의 관계자 그리고 오픈소스 관련 비영리 단체가 참여하는 회의[1]를 개최했다. 회의의 핵심 주제는 2021년 12월 발생한 Log4j 사건에 대한 구체적인 대응 방안으로 이날 논의된 주제는 [표 3]과 같다.

〔표 3〕 SW 보안에 관한 백악관 미팅 주제

범주	세부 논의 주제
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
2. 결함 발견 및 수정 프로세스 개선	오픈소스 프로젝트의 우선순위 지정, 유지 관리를 위한 메커니즘 마련
3. 수정 배포 및 구현에 대한 응답 시간 단축	기업과 개발자의 SBOM 사용을 가속화하고 개선하는 방안

4.2. Linux Foundation's The Open Source Software Mobilization Plan (2022년 5월)

2022년 5월, 비영리 단체인 오픈소스 보안 재단(Open Source Security Foundation, OpenSSF)과 리눅스 재단은 오픈소스 SW 보안 동원 계획(Open Source Software Security Mobilization Plan, OSSSMP)을 발표했다. 본 계획의 3가지 핵심 목표는 지난 1월 백악관 회의의 논의의 목표를 그대로 이어왔으며, 목표별 수행 계획과 예산을 구체화했다.

1) 국가안보 및 사이버국, 과학기술정책실, 국방부, 상무부, 에너지부, 국토안보부, CISA(Cybersecurity & Infrastructure Security Agency), 국립표준기술원, 국립과학재단과 아마존, 애플, 페이스북, 구글, IBM, MS 등 IT 대기업, 아파치 SW 재단, 리눅스 재단, 오픈소스 보안 재단(OpenSSF), 레드햇 등 오픈소스 비영리단체가 참여함

〔표 4〕 백악관 미팅 범주와 OSSSMP 세부 목표

백악관 회의 범주	OSSSMP 세부 목표
1. 코드 및 오픈소스 패키지의 보안 결함 및 취약성 방지	(목표1) 오픈소스 SW 생산 확보
2. 결함 발견 및 수정 프로세스 개선	(목표2) 취약점 발견 및 수정 개선
3. 수정 배포 및 구현에 대한 응답 시간 단축	(목표3) 생태계의 패치 대응 시간 단축

OSSSMP에는 위의 3가지 목표를 기반으로 오픈소스 SW의 중장기 보안성 개선을 목표로 구체적인 10대 전략 스트림(10-stream strategy) 계획이 담겨 있다. 각 전략은 [표 5]와 같다.[20]

특히 SBOM Everywhere 스트림은 관련자의 SBOM 채택을 활성화하기 위해 SBOM 도구 및 교육 활동을 지원하는 프로젝트가 수행된다. SW 개발회사에 SBOM 도구를 개발하도록 자금을 지원하고, 가장 인기 있는 프로그래밍 언어의 SW 빌드(Build) 도구와 관련 시스템, 인프라에 SBOM을 적용한다. SBOM의 생성과 소비가 활성화되도록 교육 자료, 비디오, 기본 서식(Template), 예제 제작과 기타 커뮤니티 활동에 자금을 지원한다.[21]

〔표 5〕 오픈소스 SW 보안 동원(Mobilization) 계획

목표 1. 오픈소스 SW 생산 확보	
스트림 1	Security Education
스트림 2	Risk Assessment
스트림 3	Digital Signature
스트림 4	Memory Safety
목표 2. 취약점 발견 및 개선	
스트림 5	Incident Response
스트림 6	Better Scanning
스트림 7	Code Audit
스트림 8	Data Sharing
목표 3. 생태계 패치 대응 시간 단축	
스트림 9	SBOM Everywhere
스트림 10	Improved Supply Chain

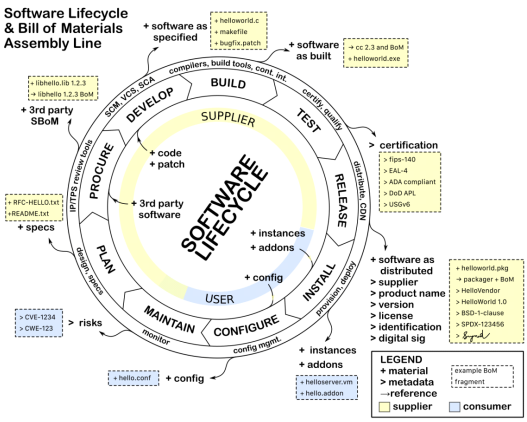
4.3. IMDRF's Principles & Practices for SBOM for Medical Device Cybersecurity (2022년 6월)

국제 의료기기 규제포럼(International Medical Device Regulators Forum, IMDRF)는 SBOM 활용에 관한 원칙 및 관행을 담은 문서 초안을 배포하고 7월부터 2개월간 의견을 수렴했다. 본 문서에 따르면 의료 기술에 타사 소프트웨어 구성요소를 포함하는 위험은 SBOM을 활용하여 부분적으로 관리할 수 있으며, SBOM은 취약성을 더욱 신속하게 식별하고 수정하여 공격 가능성을 줄이는 목표를 달성함으로써 의료기기 SW 제품 공급망의 보안을 보장하는 투명한 메커니즘을 제공한다고 강조했다.[22]

특히 SBOM이 소프트웨어 생산 비용을 많이 증가시키지 않으면서 의료 기술의 모든 공급망 이해관계자에 혜택을 줄 수 있는 잠재력이 있다고 평가하였으며, IMDRF는 우리나라 식약처도 회원으로 활동하고 있어, 향후 규제 완성 시 우리 의료기기 분야에 도입될 수 있다. 다만 SBOM 배포와 취득 이후의 관리에 대한 구체적인 모범 사례는 아직 나와 있지 않다.

4.4. ESF's Recommended Practices Guide For Developers – Securing the Software Supply Chain (2022년 8월)

NSA 등 기관과 민간의 파트너십으로 이루어진 ESF(Enduring Security Framework)는 안전한 SW 공급망을 위한 개발자 가이드를 발간했다. 본 가이드는 SW 개발자 및 배포업체 그리고 SW 구매 고객을 대상으로 개발되었으며, 타사 구성요소의 공급자 또는 소유자가 제공한 SBOM의 유효성을 검사하고 업데이트하도록 권고하고 있다. 제출된 SBOM 검증을 위해 SW 구성 분석(Software Composition Analysis, SCA) 도구를 활용하고, 제출된 SBOM이 없는 경우에도 SCA 도구를 활용해 SBOM 생성을 위한 정보를 도출한다. 타사에서 제공된 소스 코드가 내부 개발자에 의해 수정된 경우는 초기 SBOM과 업데이트된 소스 코드의 개선 및 결합을 SBOM 종속 관계에 추가하도록 기술되어 있다. 이외에도 보안 개발 모범 사례를 활용한 개발자 교육을 강조하고, 특히 기업 경영진에게 오픈소스 SW와 관련된 기준을 수립하고, 출시되는 모든 SW에 보안 지표를 적용하기를 권고한다.[23]



〔그림 3〕 SW Lifecycle & BoM Assembly Line 〔NTIA Survey of Existing SBOM Formats and Standards, 2021〕

4.5. OMB's Enhancing the Security of the SW Supply Chain through Secure Software Development Practices (2022년 9월)

미국 예산관리국(Office of Management and Budget, OMB)은 지난 9월 14일, '안전한 SW 개발 관행의 마련을 통한 SW 공급망 보안 강화에 관한 각서(Memorandum)'를 발표했다. 각서의 핵심은 연방정부에 SW를 납품하고자 하는 SW 공급자가 NIST의 보안 소프트웨어 개발 프레임워크(Secure Software Development Framework, SSDF v1.1) 및 SW 공급망 보안 지침(SW Supply Chain Security Guidance Under EO 14028 Section 4e)에서 제시하는 보안 SW 개발 관행을 준수하는 것과 이를 자체적으로 증명할 수 있는 증거(Self-attestation)를 제출하는 것이다.

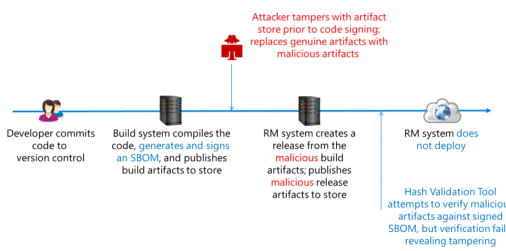
또한 기관은 SW가 안전하게 생산되었는지를 입증하는 아티팩트(Artifact)를 공급자에게 요구할 수 있으며, 아티팩트는 NTIA에서 정한 최소 요구 사항을 만족하는 SBOM을 활용할 수 있다. OMB는 NIST의 지침이 연방 정부에 도입된 SW의 새로운 취약점이 발견될 때 보안 위협을 신속하게 식별할 수 있을 것이라 설명했지만, 각서의 SBOM 제출이 강제력이 있는 규제가 아닌 권고 사항으로 되어 있고, SBOM 등 아티팩트(Artifact) 수집 이후의 관리에 대한 추가적인 가이드가 부족하여, SBOM을 활용한 보안 위협 완화가 실질적인 효과를 발휘하기까지는 다소 시간이 걸릴 것으로 예상된다.[24]

V. 결 론

이와 같은 이슈에도 왜 SBOM 정책을 도입해야 하는가? 앞서 살펴본 미국의 정부 정책은 '향후 SW 제품 도입 시 어떤 구성요소가 포함되었는지 모르는 공급 업체를 믿을 수 없다'라는 SW 투명성에 대한 인식 변화를 보여준다. 이제 연방 기관에 납품을 희망하는 제조사는 보안 개발 생명주기(Secure Software Development Life Cycle, S-SDLC) 관리를 도입해야 하고, 타사 구성요소에 대한 형상 관리 체계도 구축해야 한다. 수요기관에도 SBOM 취득자를 위한 관리 도구와 SBOM 검증 시스템의 도입 비용이 추가될 것으로 예상되지만, 미국은 과감한 변화 정책을 택했다.

SBOM 도입의 장점이 발휘하기 위해서는 먼저 모든 공급망 참여자에 의해 널리 채택되어야 하며, 각 이해관계자가 생성, 관리, 배포, 수집 및 활용과 같은 각자의 SBOM 활용 역할을 이해해야 한다.[5] 즉, SBOM을 생성하고 배포하는 측이 있다면, SBOM을 취득하고 관리하는 역할도 있으며, 이 과정에서 VEX와 같은 보안성 검증 요구가 발생한다. 또한 SBOM 데이터 자체의 신뢰성 보장 문제, 위조 등 투명성을 악용한 새로운 위협이 추가될 수 있어, 보안 전문업체의 솔루션 개발도 필요할 것으로 예상된다.

오픈소스 SW를 많이 사용하는 우리에게도 SBOM은 SW 공급망의 신뢰성과 투명성을 높이는 인프라이다. 다만 정책 시행 초기 단계에서 SW 보안 수준을 높이는 것이 제품 가격 상승의 주요 원인으로 작용함으로, 정부 조달 납품 시 인센티브를 제공하는 등 유인책을 통해 국내 SW 산업의 적극적인 참여를 유도하는 것이 중요하다. 앞선 사례에서처럼 공급망 공격이 경제적 효과가 낮은 자산을 대상으로 시도되지 않고, SBOM은 초기 도입에 투자가 필요한 만큼 보안 위험



〔그림 4〕 Validating our SBOMs at release 〔Engineering@Microsoft, 2021〕

이 큰 주요 산업 분야와 공공기관, 국가·민간의 주요 정보통신 기반 시설 등을 대상으로 우선 적용하는 것이 타당하다.

미국은 CISA와 OpenSSF를 통한 제도 홍보 및 관련 기술 콘퍼런스 개최 등 글로벌 SBOM 협력에 다양한 노력을 기울이고 있으며, 중국 정보통신연구원(中國信息通信研究院)과 싱가포르 난양기술대학교도 OpenSSF 활동에 참여하고 있다. 일본 경제산업성은 SBOM을 자동차 및 의료, SW 산업에 적용하고자 오픈소스 SW 보안 이니셔티브(Initiative)를 구성해 SBOM 시연 결과를 공유하고, 2025년까지 SBOM 실증(Proof of Concept) 사업에 대한 일정 계획도 발표했다.[25]

SW 공급망 문제는 SW 개발 관행에 대한 지속적인 개선이 요구되고, 글로벌 연쇄 위험으로 혼자서는 해결할 수 없다. 따라서 실태조사, 실증사업 등을 통해 우리의 SW 현실에 맞는 정책을 먼저 적용하고, 제도적 조화를 위한 국제협력에도 힘써야 한다. 끝으로 본고가 SBOM 보안 연구자에 길잡이가 되길 희망한다.

참 고 문 헌

[1] NIST, “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations”, *NIST SP 800-161r1*, pp. 1-3, May 2022.

[2] Kasperkey, “Managing the trend of growing IT complexity”, *IT security economics report*, p.9, 2021.

[3] Gartner, 7 Top Trends in Cybersecurity for 2022 from https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022, April 2022.

[4] 이태준, 이희조, 박춘식, “소프트웨어 보안 관점에서 본 미국 사이버보안 행정명령과 우리의 대응 방안”, *KISA Report*, Vol. 12, p.3, 2021.

[5] NTIA, “Roles and Benefits for SBOM Across the Supply Chain”, 2019.

[6] The White House, Enhancing the Security of the Software Supply Chain to Deliver a Secure Government Experience from https://www.whitehouse.gov/omb/briefing-room/2022/09/14/enhancing-the-security-of-the-software-supply-chain-to-deliver-a-secure-government-experience/, Sept. 2022.

[7] A. M. Pitney et al., “A Systematic Review of 2021 Microsoft Exchange Data Breach Exploiting Multiple Vulnerabilities”, *2022 7th Int’l Conference on Smart and Sustainable Technologies*, pp. 1-3, 2022.

[8] N. Kshetri, “Economics of Supply Chain Cyberattacks”, *IEEE Computer Society*, pp. 1-2, June 2022.

[9] BleepingComputer, Hundreds of networks reportedly hacked in Codecov supply-chain attack from https://www.bleepingcomputer.com/news/security/hundreds-of-networks-reportedly-hacked-in-codecov-supply-chain-attack/, April 2022.

[10] BBC, US fuel pipeline hackers did not mean to create problems from https://www.bbc.com/news/business-57050690, May 2021.

[11] Infosecurity Group, North Korean Lazarus Group Hacked Energy Providers Worldwide from https://www.infosecurity-magazine.com/news/lazarus-group-hacked-energy/, Sept. 2022.

[12] NTIA, Software Component Transparency from https://www.ntia.gov/SoftwareTransparency

[13] US Cyber Safety Review Board, “Review of the December 2021 Log4j Event”, pp. 3-6, July 2022.

[14] US Chamber of Commerce, “Software Bill of Materials Elements and Considerations”, June 2021.

[15] NTIA, “SBOM Options and Decision Points”, April 2021.

[16] OASIS, Common Security Advisory Framework (CSAF) from https://oasis-open.github.io/csaf-documentation/

[17] https://secvisogram.github.io/

[18] OWASP Foundation, “Software Component Verification Standard(SCVS) v1.0”, June 2020.

[19] https://en.wikipedia.org/wiki/ICANN

[20] Linux Foundation, “The Open Source Software Security Mobilization Plan”, May 2022.

[21] B. Behlendorf, “Deep Dive into the OpenSSF Mobilization Plan”, *Open Source Summit Europe - OpenSSF Day*, Sept. 2022.

[22] IMDRF, “Draft, Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity“ from https://www.imdrf.org/consultations/principles-and-practices-software-bill-materials-medical-device-cybersecurity, International Medical Device Regulation Forum, 2022.

[23] ESF, “Securing the Software Supply Chain – Recommended Practices Guide for Developers”, US Enduring Security Framework, pp. 26-27, Aug. 2022.

[24] OMB, “Enhancing the Security of the Software Supply Chain through Secure Software Development Practices - MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES“, M-22-18, US Office of Management and Budget, Sept. 2022.

[25] OpenSSF, Outcomes from Open Source Software Security Summit in Japan from https://openssf.org/blog/2022/08/24/outcomes-from-open-source-software-security-summit-in-japan/

〈저자소개〉

최 윤 성 (Yunseong Choi)

종신회원

2004년 2월 : 상명대학교 정보통신학부 졸업

2014년 2월 : 서강대학교 정보통신대학원 석사

2018년 2월~현재 : 고려대학교 컴퓨터학과 박사과정

2011년 3월~2014년 10월 : 한국정보기술연구원 (KITRI) BoB 교육센터장

2017년 3월~현재 : 고려대 소프트웨어보안연구소, 융합보안대학원 산학협력중점교수

<관심분야> 화이트해커 인재양성, OT/ICS 융합보안, SBOM 공급망보안 정책