2024. 05

SW 공급망 보안 가이드라인 v 1.0

SW 공급망 보안 국제동향 및 SBOM 활용사례

국가정보원
과학기술정보통신부
대통령직속 디지털플랫폼정부위원회

SW 공급망 보안 가이드라인 v 1.0

SW 공급망 보안 국제동향 및
SBOM 활용사례

2024. 05

국가정보원 과학기술정보통신부 대통령직속 디지털플랫폼정부위원회

서 문

Introduction

날로 증가하는 사이버 위협에 대응하기 위해서는 디지털 인프라의 근간인 소프트웨어(SW)와 SW 공급망의 신뢰성을 강화해야 합니다. SW를 포함한 디지털 제품에 포함될 수 있는 악성코드와 보안취약점을 악용한 사이버 공격을 사전에 방지하고, 사고 발생 시 신속하게 대응할 수 있는 SW 공급망 보안체계 수립을 위해 범정부적 노력이 필요합니다.

본 가이드라인은 국내 정부·공공기관 및 기업 관계자가 SW 공급망 보안 관련 국제동향을 비롯하여 SW 공급망을 위협할 수 있는 악성코드 및 보안취약점 관리 등에 관한 제반 사항을 쉽게 이해하고 활용할 수 있도록 지원하기 위해 마련되었습니다.

SW 개발과정에서 공개 SW와 같이 외부에서 개발된 SW의 사용 비중이 높아짐에 따라 SW에 포함된 악성코드 및 보안취약점 관리의 중요성이 커지고 있습니다. 일례로 공개 SW로 널리 활용되고 있는 'Log4j(자바 로깅 라이브러리)'의 보안취약점을 악용한 사이버보안 사고는 2021년 국내외에서 큰 피해를 입히며 맹위를 떨쳤던 대표적인 SW 공급망 공격사례입니다.

이와 같은 SW 공급망 공격은 대상 범위가 넓고 연쇄적 사고로 이어지며, 즉각 조치하지 못할 경우 수년간 피해가 지속되는 등 파급력이 큰 특징을 나타내고 있습니다. 그러나 SW의 보안취약점을 효과적으로 찾아내고 관리할 수 있다면 사전에 이를 예방할 수 있고, 사고 발생 시에는 타 사용자들에게 사고 상황을 빠르게 전파할 수 있을 뿐만 아니라, 신속하고 효과적인 복구를 지원하는 등 효율적인 대응이 가능합니다.

미국, 유럽 등 주요국은 SBOM(SW Bill of Materials)을 활용하여 SW의 신뢰성 확보에서 보안취약점 관리에 이르기까지 SW 공급망 보안 강화가 가능하다고 판단하고, SBOM을 적극 활용하기 위한 제도화를 추진하고 있습니다.

미국은 지난 2021년 5월, 연방정부에 SW를 납품할 때 SBOM을 포함한 보안관리 자체증명서(Self Attestation Form)를 제출하도록 하고 이를 위한 세부 이행계획을 마련 중이며, 유럽연합(EU)도 역내에 공급(유통)되는 디지털 제품의 보안취약점 관리를 주요 내용으로 하는 '사이버복원력법(CRA, Cyber Resilience Act)' 제정안에 대해 EU 의회(Parliament)와 EU 이사회(Council)가 정치적으로 합의('23.12월)하였고, 2024년 3월에는 EU 의회에서 제정 법안을 승인하는 등 법제화가 진행 중입니다. 그러나 SW 공급망의 신뢰성 강화를 위해 SBOM 제출을 의무화하는 것은 SW 개발기업은 물론 공급(유통)·수요 기업 등에게도 비용·인력 측면에서 현실적인 부담이 될 수 있습니다.

이에 국가정보원·과기정통부·디지털플랫폼정부위원회는 국내에 효과적으로 적용할 수 있는 SW 공급망 보안 강화방안을 마련하기 위해 산·학·연 전문가들과 협력하여 글로벌 동향을 분석·토론하였고, 국내 중소기업들이 제품 및 서비스 개발단계에서부터 SW 보안취약점을 찾아내고 보완할 수 있도록 기업 지원 시설을 보강하는 한편, 국산 SW 제품을 대상으로 SBOM 생성, 보안취약점 분석 및 조치 등에 관한 실증도 진행하였습니다. 금번 가이드라인에는 이와 같은 전문가 논의 결과, 중소기업 지원 경험 및 SBOM 국내 실증결과가 반영되었습니다.

본 가이드라인을 통해 SW 공급망 보안에 대한 사회적 인식이 새롭게 정립될 수 있기를 바랍니다. 정부는 앞으로도 해외사례 및 제도들을 모니터링하고, 주요 국가들과 협력을 강화하면서 가이드라인을 지속적으로 보완하고 발전시켜 나갈 계획입니다.

국가정보원 과학기술정보통신부 대통령직속 디지털플랫폼정부위원회

문서이력

제정일	버전	내역	비고
2024. 5.	1.0	「SW 공급망 보안 가이드라인 v1.0」 제정	

Contents

Contents

그림 차례

표 차례

제1장

추진 배경

제1장에서는 범정부 차원에서 광범위하고, 지속적인 확산성을 갖고 있는 SW 공급망 공격에 대응하기 위해 디지털 기술의 발전에 따른 환경변화와 미국, 유럽 등 주요국의 정책동향을 분석하였다.

제1절 (환경변화) 디지털 제품 및 서비스 개발과정의 연결성으로 인해 생태계 범위가 더욱 확장되고 있다. 디지털 제품 및 서비스의 중요 구성품인 SW의 개발·공급이 분업화되면서 최종 디지털 제품 및 서비스의 무결성에 대한 신뢰가 하락하고, 악성코드 삽입 및 보안취약점의 전파가 쉬운 공개 SW는 공급망 공격의 주요 목표가 되었다. 또한 KISA에서 발행한 2024년도 사이버보안 위협 전망에서도 SW 공급망 공격에 대한 대응의 필요성을 강조하고 있다.

제2절 (SW 공급망 위기 대응의 필요성) 디지털 제품 및 서비스에 포함된 악성코드 또는 보안취약점은 사전에 탐지하기가 어렵고, 사고가 발생하면 광범위한 피해와 함께 사고가 연이어 발생하는 특징을 갖는다. 공개 SW로 널리 활용되는 Log4j에서 초고도 보안취약점이 발견된 사건(2021년)은 국내외에 큰 충격을 주었고, 공개 SW의 보안 강화를 추진하게 하는 계기가 되었다. 아울러 공격대상 및 침투 경로를 표시한 SW 공급망 공격 유형(7종)을 제시하여 SW 공급망 보안에 대한 이해를 높일 수 있도록 하였다.

제3절 (주요국 공급망 보안 정책 동향) 미국은 바이든 행정부의 행정명령(EO 14028, '21.5월) 이후 보안관리 자체증명서를 제출하도록 제도화하였으며, EU는 SW 공급망 보안을 의무화하는 사이버 복원력법 제정 발의('22.9월) 후 EU 의회 및 이사회의 의결('24.3월) 등 제도화를 추진 중이며, 일본의 SBOM 실증사례와 4개국 안보협의체(Quad)의 정책동향을 분석하였다.

이를 통해 SBOM 기반 SW 공급망 보안 관리체계 확산의 필요성과 미국, 유럽 등 주요국의 무역장벽 극복 지원 필요성에 대한 정책적 시사점을 도출하였다.

제1절 환경변화

1. [변화-1] 초연결 사회의 도래

초(超)연결[1] 시대에 전 세계는 분산된 생산 체계와 다양한 경로로 연결된 공급망 생태계(Ecosystem)를 통해 서로 협력하고 있다. 특히, 디지털 제품 및 서비스의 개발-공급(유통)-운영의 연결성(Connectivity)으로 인해 생태계 참여 계층의 범위가 점점 확장되고 있다. [그림 1]

> 기존 공급망은 다양한 비즈니스 주체(예 : 부품 공급사, 최종 생산자[2], 공급(유통)사, 고객사)가 ❶ 원자재를 부품으로 전환하고, ❷ 부품을 지정된 최종 제품으로 조립하고, ❸ 이러한 제품을 최종 소비자에 전달하기 위해 협력하는 통합 프로세스

- TV, 냉장고 등 가전제품에서부터 의료, 자동차, 선박, 항공우주 등 전통산업에 이르기까지 SW가 서비스 구현의 핵심을 담당하는 디지털 전환(Digital Transformation, DX)의 가속화
- 모바일, 사물인터넷(IoT), 클라우드 등 디지털 제품 및 서비스 개발, 공급(유통)에서 혁신성과 경제성을 이유로 외부 SW의 활용이 늘어나고 있으며, 다양한 정보통신기술(ICT)과의 상호 의존성(Dependency)도 증가

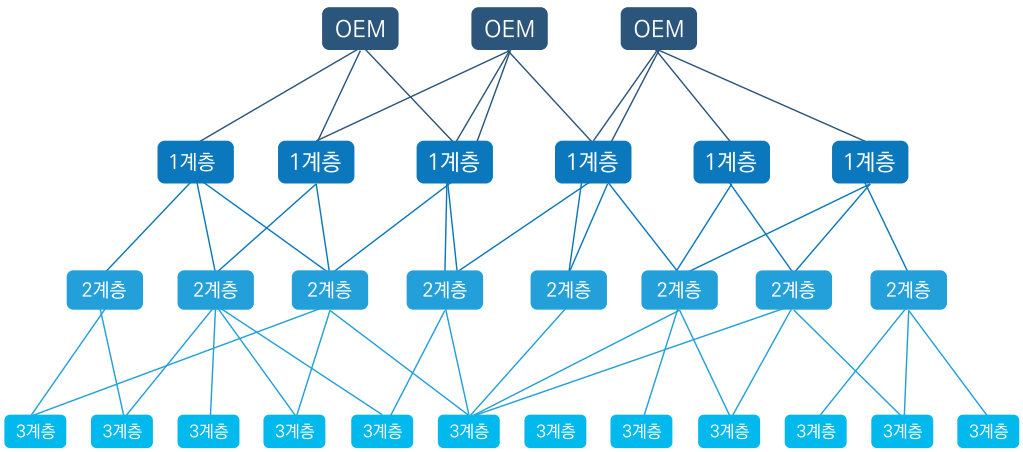


그림 1 공급망 생태계 기본 모형

.

1) 초연결(Hyper-Connectivity) 이란, 사람과 사물(공간·생물·정보·비즈니스 등)이 물리·가상공간의 경계 없이 서로 유기적으로 연결되어 소통하고 상호작용하는 만물 인터넷 (Internet of Everything) 인프라 [ETRI]

2) 최종 생산자(Original Equipment Manufacturer, OEM)

2. [변화-2] SW 부품 공급의 분업화

디지털 제품 및 서비스에 대한 SW 부품(코드) 공급 역할이 분업화되면서 최종 제품 및 서비스에 대한 관리 책임을 복잡하게 하고, 이는 SW 공급망을 통한 최종 디지털 제품 및 서비스의 무결성에 대한 '신뢰' 하락으로 이어지고 있다.

SW 공급망은 최종 SW 제품을 생산하는 사람, 장치, 시스템의 집합을 말함. 이는 개발자가 코드를 작성하는 때부터 해당 코드가 제품으로 생산된 후, 사용자 시스템에서 실행되는 때까지 일어나는 모든 일을 의미함 [그림 2]

- 외부 SW, CI/CD[3], 공용 리포지토리(Repository)[4]와 클라우드 호스팅 서비스 등 최신 SW 개발 파이프라인에 대한 공격 표면(Attack Surface)이 늘어나고 있어 SW 제품 개발환경에 대한 보안성 확보가 중요
- 특히 외부 SW의 활용과 보안취약점의 증가는 SW 품질에 대한 유지관리 비용뿐만 아니라 사이버보안 관리 비용도 높이고 있어서 SW 개발단계부터 운영단계까지 사이버보안 관리체계에 대한 지원도 중요
- 다만 SW 공급망 전반의 사이버 위협을 해결하기 위해서는 조직의 SW 개발 생명주기(SDLC)[5] 전체 과정에서 사이버보안 위험관리가 필요

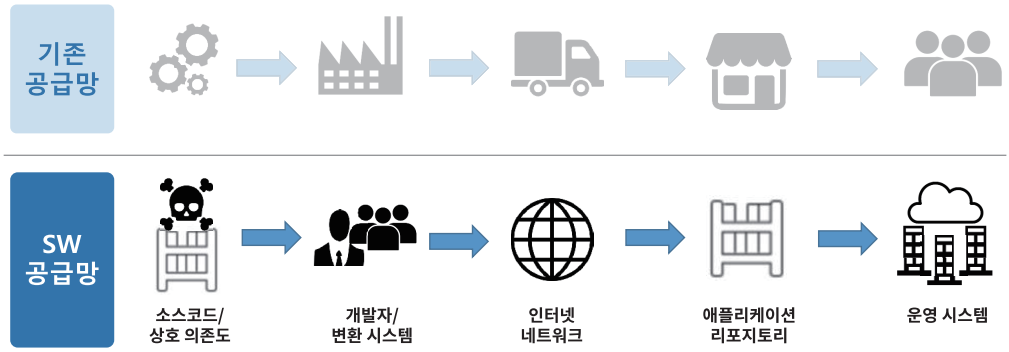


그림 2 전통적인 공급망과 SW 공급망 비교

3) 지속적 통합 및 지속적 배포(Continuous Integration & Continuous Delivery)를 실현하는 SW 개발 방식 [Wikipedia]
4) 개발자가 소스코드에 대한 변경을 수행 및 관리하는 데 사용하는 중앙화된 디지털 저장소 [AWS]
5) SDLC : Software Development Life Cycle

3. [변화-3] 공개 SW 사용의 확대

최근 디지털 제품 및 서비스는 대부분 자체(내부) 개발 SW 외에 다양한 외부 SW(공개 SW 또는 제3자 개발 SW)가 포함되어 있다. 특히, 공개 SW는 관리 주체가 명확하지 않고, 악성코드 및 보안취약점의 전파가 쉬워서 사이버 공격의 주요 목표가 되고 있다. [그림 3]

> 공개 SW(Open Source Software)는 SW의 내용을 프로그래밍 언어로 나타낸 '소스코드'를 공개하여, 정해진 라이선스에 따라 개량·재배포할 수 있는 SW
>
> '타사(3rd Party) SW 구성요소'는 SW의 원래 공급사가 아닌 다른 개발사에서 계약에 의해 배포하거나 판매할 수 있도록 개발된 재사용 가능한 SW 부품(Component)

- 상용 SDK 등 타사 SW 구성요소와 공개 SW를 활용하면 SW 개발기간 단축과 안정화된 서비스 구현으로 비용이 절감되고, 기업 간, 기업-기관 간 등 다양한 형태의 협력 개발이 가능해지는 등 개발 효율성 증대
- 다만, 전 세계적으로 널리 사용되는 공개 SW인 Log4j에서 심각한 보안취약점이 발견되어 우리나라 및 전 세계 기업과 정부·공공기관에 큰 피해 발생
- 이에, 미국, EU 등 주요국을 중심으로 SW 공급망 보안 강화를 위한 제도화를 추진 중이며, 우리나라도 SW 공급망의 사이버 위험을 관리하기 위한 국가적 대책 마련에 대한 필요성 증가
- [그림 3]은 국내 정보보호 전문기관인 한국인터넷진흥원(KISA)의 2024년도 사이버보안 위협 전망으로 SW 공급망 공격에 대한 대응 필요성을 제시

그림 3 2024년도 사이버보안 위협분석과 전망 리포트[KISA]

제2절 SW 공급망 위기 대응의 필요성

1. SW 공급망 공격 대응의 문제

디지털 제품 및 서비스의 공급망을 대상으로 하는 사이버 공격 방법이 다양해지고 고도화되고 있다. 악의적인 목적으로 특정 제품 및 서비스에 악성코드를 설치하여 공급한다면, 해당 제품 또는 서비스를 도입한 기관에서는 악성코드 존재와 이를 악용한 정보 유출 등의 피해 사실을 파악하기란 거의 불가능하다.

[사례-1] 2018년 9월, 유럽의 모 보안 SW 업체에서 UEFI[6]의 펌웨어 루트킷(Rootkit)[7]인 'LoJax'를 발견했다고 발표. 'LoJax'는 악의적인 UEFI 모듈을 시스템의 플래시 메모리에 기록하고, PC의 부팅 과정에서 악성코드를 저장소에 주입해 실행됨. 해당 루트킷은 운영체제를 재설치하여도 펌웨어 영역에 남아 삭제되지 않음 [ESET Research]

[사례-2] 2020년 3월, 軍은 국내 S사와 '해·강안 경계 과학화 사업' 납품 계약을 체결. 이후 자체 점검 결과 도입된 215대 모두 CCTV 內 DNS 서버 주소가 악성코드 유포 이력이 있는 중국 IP로 설정된 채 납품되었으며, 해당 제품은 국산 제품으로 위장된 외산 제품이었음. 다행히 설치된 CCTV는 모든 네트워크가 내부망으로만 구성되어 정보 유출은 없었지만, 인터넷과 연결된 환경이었다면 CCTV 영상 정보가 외부 공격자에게 넘어갈 수 있는 사고로 이어질 수 있었음 [보안뉴스]

[사례-3] 2023년 7월, 정부 기관에 납품된 외산 계측장비에서 악성코드가 발견되었음. 해당 장비는 지상에서 약 5㎞ 고도까지 바람의 속도와 방향을 측정하는 장비이며, 확인 결과 악성코드가 식별된 외산 장비는 A사 3대, B사 2대였음. 식별된 악성코드는 모두 컴퓨터 운영체계를 기반으로 하는 '신호처리부'에서 발견되었음[환경일보]

6) UEFI : Unified Extensible Firmware Interface
7) 공격자가 들키지 않고 시스템을 제어하도록 설계된 악성 SW 모음

2. SW 공급망 침해사고의 피해 규모

미국은 솔라윈즈(Solarwinds) 등 대규모 SW 공급망 공격을 경험하면서 2021년 5월 '국가 사이버보안의 개선에 관한 대통령의 행정명령(EO 14028)'을 발표하였다. 이는 연방정부의 SW 공급망 보안을 위한 정책 실행을 가속화하는 계기가 되었으며 이를 통해 연방정부의 사이버보안 개선 정책의 구체적인 제도화를 추진 중이다.

표 1 국내외 SW 공급망 침해사고의 피해 규모

공격명 (발생 시기)	사고 내용 및 피해 현황
SolarWinds (2020년)	러시아 기반 해킹 그룹의 공격으로 IT SW 공급사의 SW 개발환경 및 배포 시스템이 해킹되어 18,000개 이상의 기관이 피해를 입음
Codecov (2021년)	컨테이너 이미지 보안취약점을 악용해 소스코드 검증을 위한 배포 환경의 인증 정보가 유출, 전 세계 2만 9천여 개 고객사에 영향을 끼침
Colonial Pipeline (2021년)	송유관 관리사의 IT 시스템이 랜섬웨어에 감염되어 미국 남동부 8,900km 일대 공급이 중단, 지역 비상사태 선포와 약 50억 원의 랜섬머니(Ransom Money) 지급 발생
Log4Shell (2021년)	Log4j의 제로데이 보안취약점과 공개된 개념 증명 코드를 악용하여 악성코드를 심고, 전 세계 취약 서버를 대상으로 대량의 해킹 공격 발생
Kaseya (2022년)	클라우드 기반 IT 원격 관리 솔루션 서버를 해킹하고, 업데이트 파일로 위장한 랜섬웨어를 고객사에 배포. 17개국 1,500여 조직이 피해
3CX (2023년)	악성코드가 삽입된 X-트레이더 금융 SW를 다운받은 PC를 감염시켜 60만 명 이상의 고객과 1,200만 개 조직으로 전파
이니세이프 (2023년)	금융 보안인증 SW의 보안취약점을 악용해 PC 해킹 및 악성코드 유포로 국내 61개 기관, 총 207대의 기관, 기업, 개인 PC 해킹 피해

- 고객의 소스코드를 검증하는 회사인 Codecov사의 공급망 공격 사건은 도입사 리포지토리의 인증 정보가 유출되어 2차 공격의 파급을 가늠하기 어려움(2021년)
- 미국 사이버보안 검토 위원회의 보고(2022년)에 따르면 Log4j와 같이 수천 개의 프로젝트에 통합된 공개 SW는 관련 시스템의 인스턴스(Instance)를 삭제·업데이트하는 데만 10년이 소요
- SolarWinds(2020년), Log4j(2021년) 및 Kaseya(2022년)와 같이 대형 SW 공급망 공격이 매년 발생하고 있어서, 이에 대한 체계적인 대응이 필요
- 국내에서도 북한이 배후로 추정되는 3CX 화상회의 앱(App) 대상 연쇄 공급망 공격(2023년)이 있었고, 우리나라도 예외적인 상황이 아님

3. 공개 SW 사이버보안 관리의 중요성

공개 SW인 Log4j 보안취약점을 악용한 사이버 공격은 웹 방화벽 차단, 원격 코드베이스 비활성화, JNDI Lookup 비활성화 등 다양한 방법으로 방어할 수 있으나, 이보다 더 큰 위험은 Log4j가 어느 제품 및 서비스에 어떻게 사용되고 있는지 파악하기 어렵다는 점이다.

- 미국은 SW 공급망 보안 강화를 강조(EO 14028, '21.5월)한 이후, 공개 SW의 보안 측면을 살펴보고자 백악관에서 민관 전문가들이 참석하는 SW 보안 정상회의[8]를 개최
- 이후 리눅스(Linux) 재단에서 공개 SW 보안에 관한 구체적인 동원 계획[9]을 발표함으로써 SW 공급망의 보안 확보를 위한 공개 SW 보안 강화의 필요성 인식이 확산되기 시작
- 또한 와이어드(Wired) 뉴스의 보도에 따르면 Log4j 사태 발생 후 1년이 지났지만, 아직도 25%는 보안에 취약한 버전이 다운로드 되고 있음[10]. 따라서 공개 SW 구성요소에 대한 관리가 이루어지지 않는다면, 제2의 Log4j 사태는 언제든지 재발할 수 있는 상황

8) 백악관, "Readout of White House Meeting on Software Security"(2022년 1월)
9) 리눅스 재단, "Open Source Software Security Mobilization Plan"(2022년 5월)
10) Wired "A Year Later, That Brutal Log4j Vulnerability Is Still Lurking"(2022년 12월)

참고 국내외 SBOM 표준화 현황

[참고] 공개 SW의 활용 및 보안취약점 현황 분석

S社가 매년 발간하는 공개 SW 위험분석 보고서에 따르면, 2022년에 분석한 코드베이스[11]의 96%는 공개 SW를 포함하고 있는 것으로 파악 (총 1,703개 대상)

- 또한 코드베이스의 84%는 보안취약점을 한 개 이상 포함하고 있어 개발과정에서 공개 SW 활용 비중이 매우 높으나 보안 관리는 미흡하다는 것을 알 수 있음
- 고위험 보안취약점이 있는 구성요소의 비율도 매년 약 50%에 육박하여 공개 SW 재사용으로 인한 보안취약점 전파의 심각성이 드러남
- 특히, 리눅스 커널, PHP 개발 언어, 아파치 톰캣(Tomcat)과 같이 시스템 구축에 많이 사용하는 기반 SW에도 고위험 보안취약점이 발견되어, 공개 SW 공급망의 시작 단계부터 보안취약점 대응 조치가 필요함

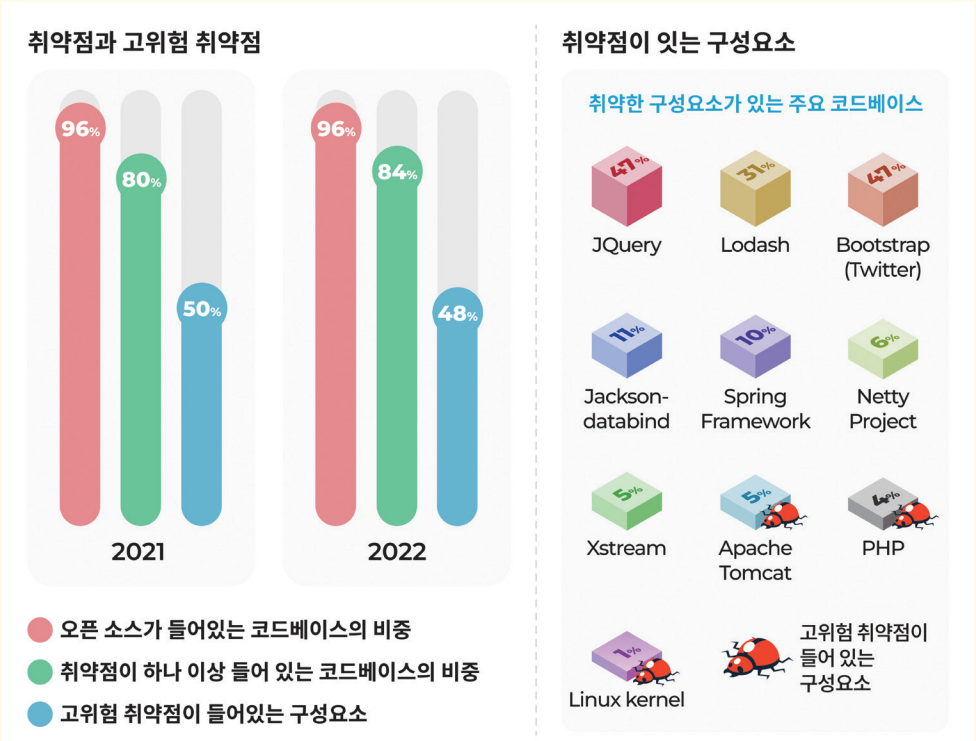


그림 4 공개 SW 사용률 분석(OSSRA Report 2023)

11) 코드베이스(Codebase) : SW를 빌드할 수 있는 소스 코드가 저장된 저장소

4. SW 공급망 공격의 주요 유형 및 대상

SW 공급망 공격은 공급망 구성요소 중 하나 이상의 약점(Weakness)이 손상되어(공격에 노출되어) 최종 제품이 변경되는 것을 의미한다. 즉, 공급망에서 어떤 방식으로든 구성요소의 일부가 변경되어 최종 제품이 취약해지거나 임의의 SW가 포함되는 공격을 뜻한다. 따라서, SW 개발, 변환(Build)[12], 배포, 운영 시스템 등 모든 SW 인프라가 공급망 공격의 대상이 된다. 대표적인 공급망 공격 유형은 [표 2]와 같다.

표 2 주요 SW 공급망 공격 유형

유형	세부 내용
1. 공개 SW 보안취약점 (Vulnerabilities in OSS)	공개 SW에 취약한 코드 또는 유해한 구성요소가 포함되어 취약성이 공개 SW를 사용하는 모든 SW에 전파
2. 타사 의존성 (3rd Party Dependencies)	공격자가 타사 SW(상용 SDK, 라이브러리 또는 컴포넌트[13])에 악성코드를 삽입하여 이를 악용하는 운영 시스템을 침해
3. 공용 리포지토리 (Public Repositories)	공개 SW 코드를 찾는 개발자를 목표로 GitHub 등 알려진 리포지토리 호스팅 서비스에 합법적인 SW 패키지와 유사한 이름을 가진 악성코드를 업로드
4. 변환 시스템 (Build Systems)	개발 프로세스 자동화를 위한 CI/CD 상의 중요 코드, 리포지토리, 컨테이너 및 변환 서버를 침해하여 악성코드로 교체
5. 업데이트 가로채기 (Hijacking Updates)	공격자가 SW 업데이트 과정을 침해하거나 업데이트 서버의 관리 권한을 가로채어 악성코드를 삽입
6. 내부 리포지토리 (Private Repositories)	공격자가 기업 내부에서 사용 중인 코드 저장소에 침입하여 악성코드를 삽입
7. 공급사 및 협력사 (Suppliers and Business Partners)	SW 부품 또는 완제품 개발사, 공급사 등으로부터 외부 서비스를 제공받는 경우 관리되지 않는 타사 위험(Risk)이 내부 시스템으로 전이

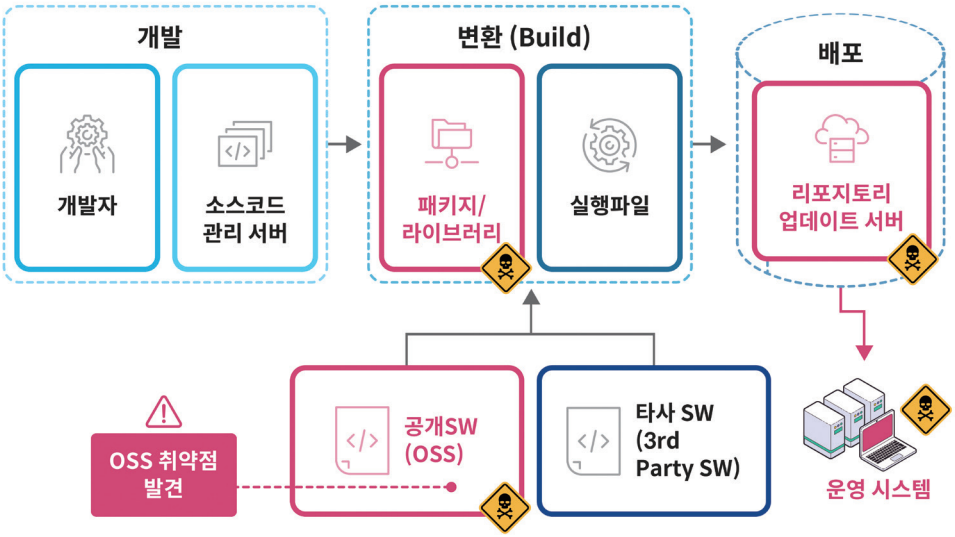
12) Build : 소스코드를 컴퓨터나 휴대전화에서 실행할 수 있는 독립 SW로 변환하는 과정 또는 결과물 [Wiki]

13) 컴포넌트(Component) : 독립된 단위 기능의 SW 부품 [Wikipedia]

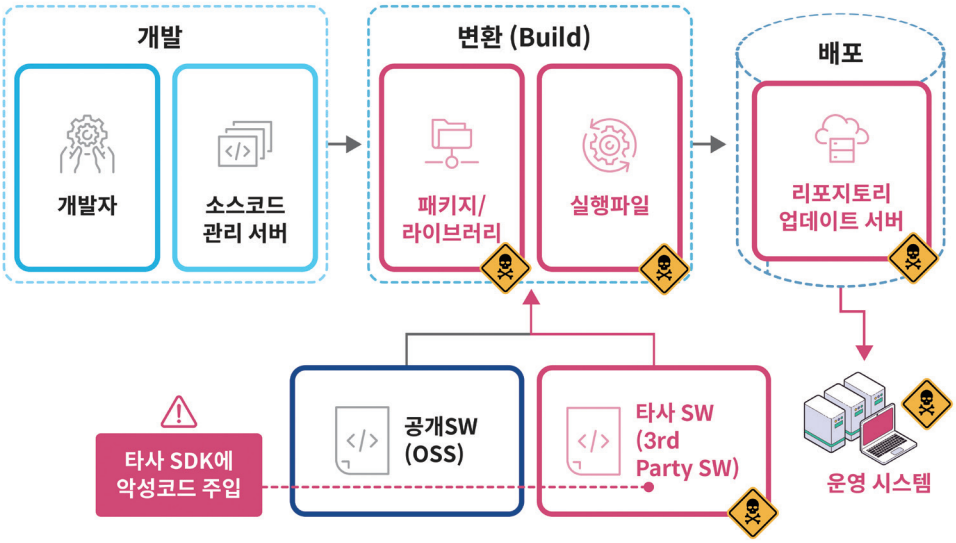
제시된 SW 공급망 공격 유형에 따른 시스템 침해 시나리오는 다음과 같다.

표 3 유형별 SW 공급망 공격 대상 및 침투 경로

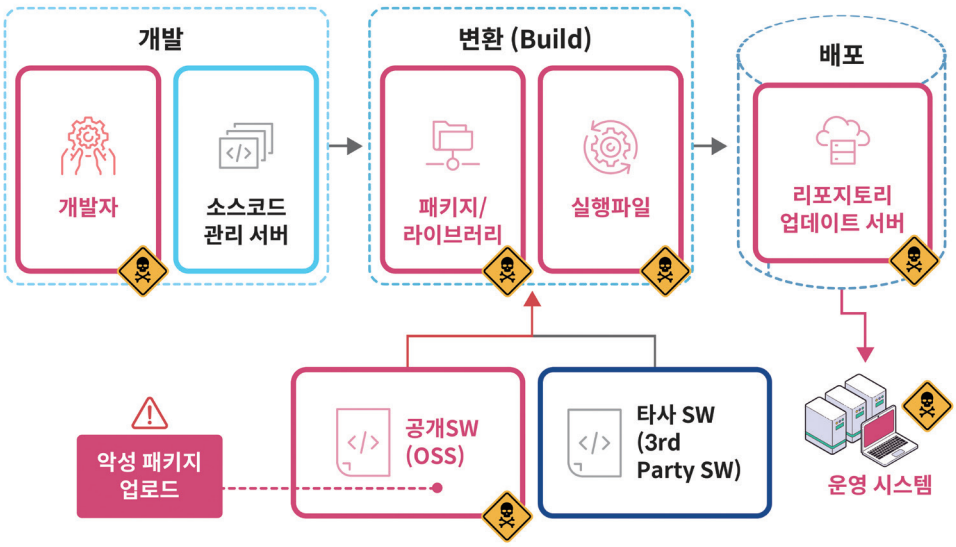
(유형1) 공개 SW 보안취약점(Vulnerabilities in OSS)



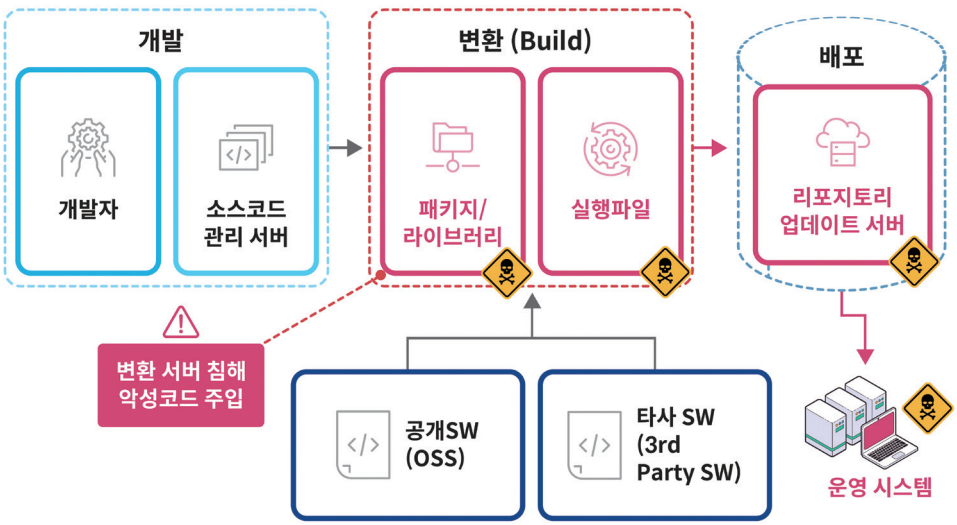
(유형2) 타사 의존성(Third-Party Dependencies)



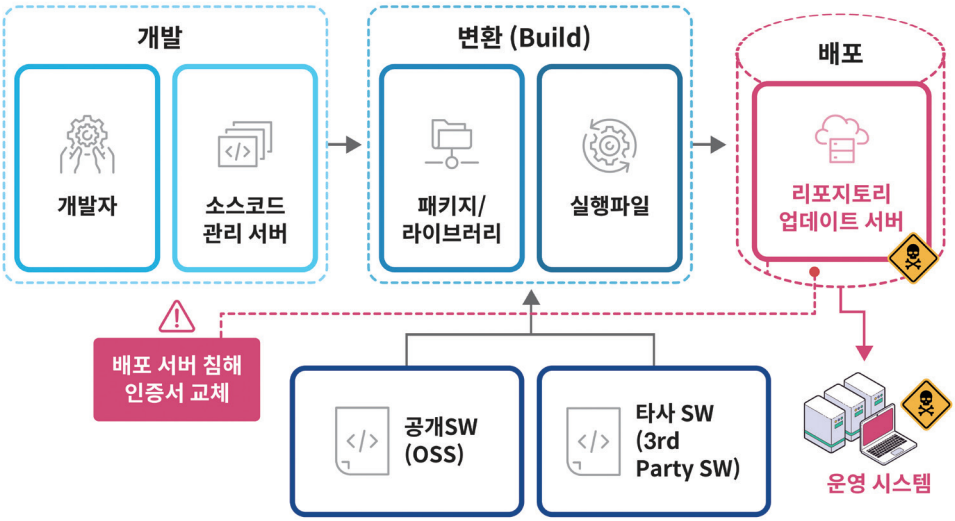
(유형3) 공용 리포지토리(Public Repositories)



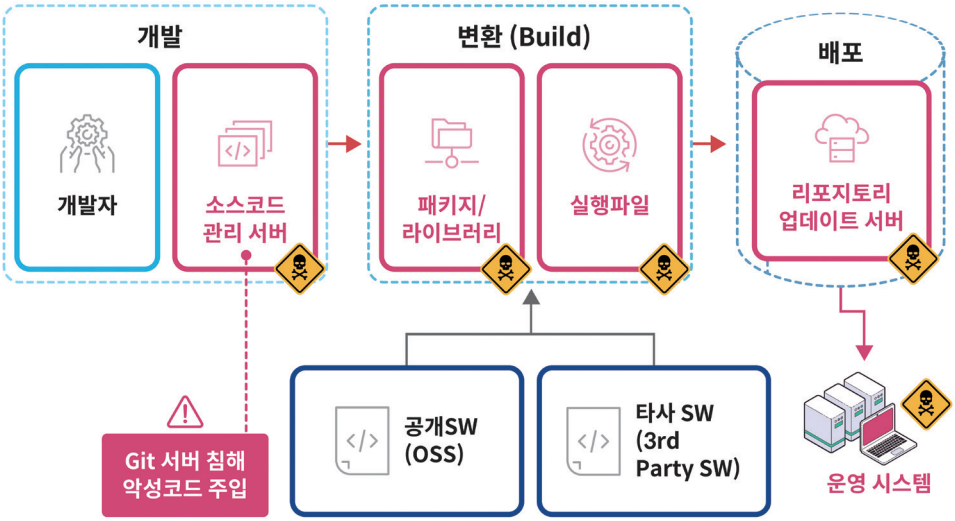
(유형4) 변환 시스템(Build Systems)



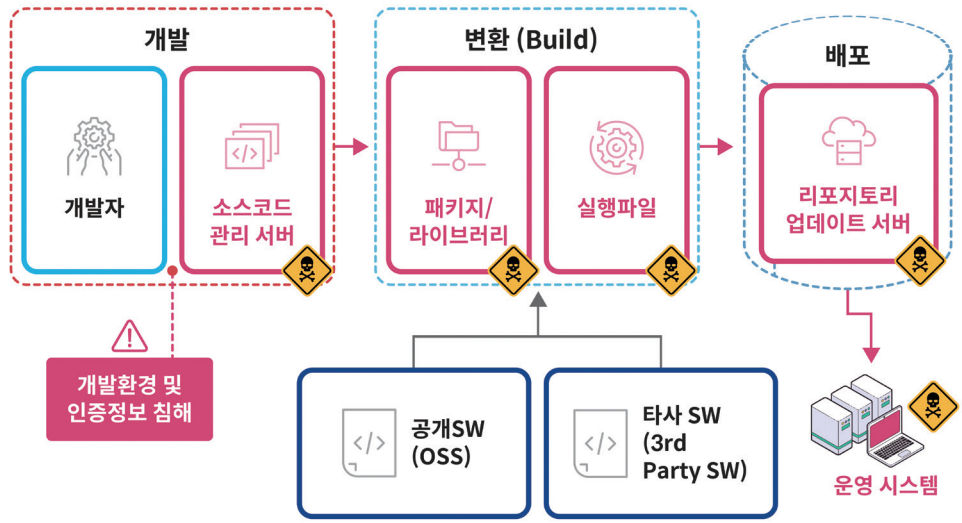
(유형5) 업데이트 가로채기(Hijacking Updates)



(유형6) 내부 리포지토리(Private Repositories)



(유형7) 공급사 및 협력사(Suppliers and Business partners)



제3절 국내외 주요국 SW 공급망 보안 정책 동향

1. 미국

가. 관리예산처(OMB) 'SW 보안 강화' 지침 발표

미국은 바이든 정부 행정명령(EO 14028, '21.5월)을 통해 연방정부에 납품되는 SW의 공급망 보안관리를 의무화하였고, '22년 9월, '안전한 정부를 위한 SW 공급망 보안 강화 지침'과 '행정 부서 및 기관장을 위한 각서(Memorandum)'를 발표했다.

OMB '행정 부서 및 기관장을 위한 각서(M-22-18)' 주요 내용

연방정부에 SW를 납품하는 공급자에게 미국 국가기술표준원(NIST)[14]의 '안전한 SW 개발 체계(SSDF)[15]'의 모범사례 준수를 요구하며, 이를 수행했음을 선언하는 '자체증명서(Self-attestation Form)[16]'를 함께 제출토록 함

- 자체 증명 항목 : 안전한 개발환경 구축, 자동화된 소스코드 출처 관리, 지속적 취약성 검사 등을 수행
- 이외에도 연방정부 기관은 안전한 SW 개발체계 적합성을 입증하는 증거를 별도로 요구할 수 있음
- 자체증명서 등의 제출은 온라인(softwaresecurity.cisa.gov) 또는 이메일로 접수

'M-23-16 update to M-22-18'을 통해 연기된 OMB 증명 양식[17]의 최종 버전이 2024년 3월에 확정되어 자체증명서 제출이 시행될 예정이다.

나. 식품의약국(FDA) 의료기기 사이버보안 강화 정책

2023년 1월, 미국 FDA는 의료기기의 사이버보안 강화 관련 자금 및 법적권한을 확대하기 위해 연방식품의약품화장품법(FD&C Act)을 개정했다.

FDA는 같은 해 3월, 의료기기의 시장 출시를 결정짓는 심사의 '승인 거부(Refuse to Accept, RTA)' 정책에 제조사가 보안이 내재된 안전한 의료장치 개발체계를 구축해야 한다는 요구사항을 추가하였다.

---

14) NIST : National Institute of Standards and Technology

15) SSDF : Secure Software Development Framework

16) 증명(Attestation) 이란 문서의 진위를 법적으로 인정하고, 적절한 프로세스를 따랐다는 것을 입증하는 절차로써, 문서의 내용에 구속된 사람들이 적절하게 행동했음을 확인하기 위해 서명하고, 제삼의 검증기관(3rd Party Organization)을 통해 공증하는 것 등을 의미함

17) 미국 관리예산처(OMB)이 공통 양식을 승인한 기점을 기준으로 중요(Critical) SW는 3개월 이내, 모든 SW는 6개월 이내 제출

FDA RTA(승인거부, REFUSE TO ACCEPT)의 주요 사이버보안 보증 요구사항

RTA의 요구사항은 SW를 포함하고 인터넷에 연결될 수 있어서 사이버보안 위협에 취약할 수 있는 모든 장치를 대상으로 하며, FDA에 승인을 요청하는 모든 제조사는 장치의 사이버보안 요구사항을 충족하는 계획을 제출

- 사이버보안 취약성 및 보안취약점 공격(Exploit)을 적시에 모니터링, 식별 및 해결하기 위한 계획
- 공개 SW 및 상용 SW의 구성요소 목록을 포함하는 SBOM 제공

참고로 RTA의 사이버보안 보증을 위한 두 가지 요구사항은 이미 승인되어 시장에 출시된 장치에도 요구할 수 있다.(2023년 10월부터 시행)

표 4 미국의 SW 공급망 보안 추진 경과

	공급망 보안 강화	SW 관리 및 보호	SBOM 적용 정책
'21	11월, NIST 공급망 보안 강화 예비 가이드 발표	7월, NIST SW 공급자/개발자 대상 소스 코드 검증 최소 기준 마련 (NIST IR 8397)	6월, NIST 중요(Critical) SW 정의 7월, NTIA SBOM 최소 구성요소 정의 7월, NIST 중요 SW 보안 조치 지침
'22	2월, NSA·CISA·ODNI 공급망 보안 강화 실행 지침 발표 5월, NIST 공급망 보안 강화 추가 가이드 발표 5월, NIST 공급망 사이버보안 위험 관리(C-SCRM) 기준 개정(SP 800-161)	2월, NIST 안전한 SW 개발보안 체계 발표 (SP 800-218 r1) 9월, ODNI·NSA·CISA 개발자의 SW 공급망 보안 지침 발표 (ESF) 9월, CISA S.4913-공개 SW 보호법 발의 10월, ODNI·NSA·CISA 고객사의 SW 공급망 보안 지침 발표(ESF)	12월, NIST 정부 납품 모든 SW에 SBOM 적용(연기)
'23	4월, CISA 1차 자체 증명서(초안) 공개 및 의견 수렴 11월, CISA 2차 자체 증명 공통 양식 공개 및 의견 수렴	5월, CISA H.R.3286-공개 SW 보호법 유사 법안의 하원 발의	10월, FDA FDA 의료기기 인허가 시 SBOM 제출 의무화

2. 유럽연합(EU)

EU는 역내에 공급(유통)되는 디지털기기의 SBOM 제출을 의무화[18]하는 사이버 복원력 법(Cyber Resilience Act, 이하 CRA) 제정안을 발의하였다.(2022년 9월, EU 집행위원회(Commission))

- 자체 또는 인증기관을 통해 사이버보안에 대한 적합성 평가를 시행하고 CE 마크[19]의 부착 여부를 결정하는데, 이때 기술 문서로서 SBOM을 요구할 계획(사이버보안 강화를 위해 제조사에 제품 보안 업데이트, 공급망 사이버보안 점검, 정부 당국과 보안 취약성 정보공유 등 일련의 요건을 부가함)
- 사이버보안 강화를 위해 제조사에 제품 보안 업데이트, 공급망 사이버보안 점검, 정부 당국과 보안 취약성 정보공유 등 일련의 요건을 부가함
- 개정안에 대한 입법 논의를 진행한 EU 의회(Parliament)와 EU 이사회(Council)는 관련 개정 법안의 역내 시행에 정치적으로 합의(2023년 12월)

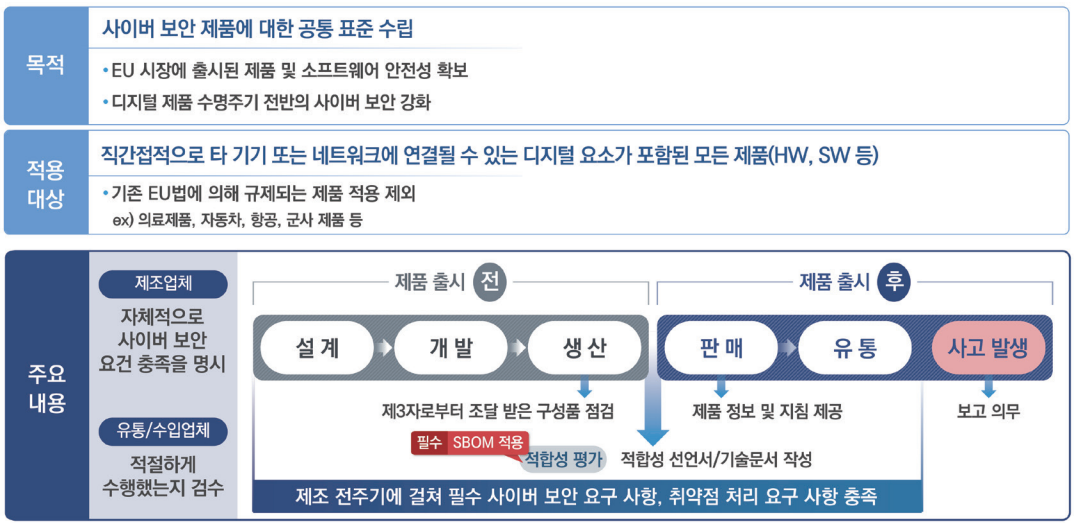


그림 5 EU 사이버 복원력 법안 개정 주요 내용

18) EU 시장에서 디지털 제품을 제조하거나 공급(유통)하려는 업체는 SBOM을 작성하는 등 제품에 포함된 구성요소를 식별하고 문서화해야 한다.(EU CRA 성명서 제37조)

19) CE 마크(CE Marking)는 EU 시장 공급(유통)을 위한 의무 사항으로 판매되는 제품이 안건, 건강, 환경 그리고 소비자 보호와 관련된 EU 규격의 조건을 준수한다는 의미임

3. 일본

일본 정부는 경제산업성에 SW TF를 설치하고 의료·자동차·SW 분야에 걸친 SBOM 실증(PoC)을 통해 개념 정립, 효과성 검증, 제도화 방안을 마련하고 있다.

- '경제산업성'은 공개 SW의 활용 및 보안성 강화를 위한 사례집[20]을 발간하고, SBOM 실증사업을 통해 SBOM 도입에 따른 비용·효과를 평가하여, 활용·거래 모델과 기술적 측면에서의 자동화·공유 방안 등을 검토. 또한, 자국 기업 내 보안 부서와 경영층을 위한 SBOM 도입 안내서[21]의 배포를 통해 민간 부문에 SBOM 활용을 확산하기 위해 노력
- '총무성'의 사이버보안 TF는 공개 SW의 급속한 확대로 통신 분야 공급망에 대한 SBOM 도입 가능성을 검토 중(SW 사이버보안 종합대책안 2023)

표 5 경제산업성이 공개한 SBOM 실증 로드맵(2022.05)

<table>
<tr><th></th><th>1단계(12개월)</th><th>2단계(12개월)</th><th>3단계(12개월)</th></tr>
<tr><td>① PoC를 통한 비용 및 이점 평가와 이슈 논의</td><td>대상 선정 및 PoC 구현</td><td colspan="2">PoC 구현
(필요성 및 대상 영역 고려)</td></tr>
<tr><td>② SBOM의 효과적인 활용 모델 논의</td><td>PoC 결과를 통한 활용 모델 논의</td><td>활용 모델 합의를 위한 방법 및 프로세스 논의</td><td>타 분야 적용 논의</td></tr>
<tr><td>③ SBOM 공유를 위한 거래 검토</td><td>이슈 정리</td><td>분야별 거래 합의 모델 논의</td><td>다른 영역에 대한 논의, PoC 결과 활용</td></tr>
<tr><td>④ SBOM 노하우 공유</td><td>가이드 문서 개발</td><td colspan="2">문서 홍보 및 업데이트</td></tr>
<tr><td>⑤ SBOM 자동화 및 공유를 위한 기술적 고려 사항</td><td>기술적 난제 파악</td><td>기술적 난제 해결을 지원하기 위한 이니셔티브(Initiative) 계획 및 논의</td><td>이니셔티브 실행</td></tr>
<tr><td rowspan="2">⑥ 타 국가와의 제도적 조화 검토</td><td>협력 항목 정리</td><td colspan="2">이니셔티브 계획 및 논의</td></tr>
<tr><td colspan="3">적절한 시기에 PoC 결과 등을 공유</td></tr>
</table>

20) 공개 SW 활용 및 보안성 확보를 위한 관리 방법 사례집(日 경제산업성, 2022년 8월)

21) SW 관리를 위한 SBOM 도입 안내서(日 경제산업성, 2023년 7월)

4. Quad 사이버보안 파트너십

4자 안보대화체(Quadrilateral Security Dialogue, Quad)로 불리는 4개국 사이버보안 파트너십에서는 SW 공급망 보안을 위한 SW 개발 활동(Practice)의 이행을 장려한다.

- 미국, 일본, 인도, 호주 등 4개국이 참여하는 회담에서 주요 기반 시설의 사이버보안, 공급망 위험관리, SW 보안, 대응 역량 강화 등을 중점 논의
- 높은 수준의 '안전한 SW 개발 활동'이 각국의 정부 정책에 반영되어 이를 충족하는 SW 확보 및 구현 환경을 구축할 수 있도록 장려하기로 협의
- 이를 위해 '안전한 SW를 위한 공동 원칙'을 발표하고, "정부가 SW의 개발·공급(유통)·운영을 위한 최소한의 사이버보안 지침을 수립하여, SW 보안을 공동으로 개선하겠다"는 약속을 재천명함[22]

표 6 Quad 사이버보안 파트너십 요약

〈Quad 사이버보안 파트너십 : 안전한 SW를 위한 공동의 원칙〉[23]

① 높은 수준의 안전한 SW 개발체계 활동을 추구
- 조직을 구성, 보안 테스트를 시행, 보안취약점의 식별 및 대응
- 무단 접근 방지, 릴리즈 보관, 릴리즈에 사용된 구성요소 세부 사항(SBOM 등), 공급망 관계에 대한 적절한 기록 유지 및 통제 보장

② SW 제품의 정부 조달에 대해 최소 가이드라인 추구
- 안전한 개발환경에 대한 Self-attestation 또는 타사 인증
- 각국의 보안취약점 공개 프로그램(Vulnerability Disclosure Program, VDP)에 개발자 보고를 권장

③ 정부 SW 사용에 대한 보안 조치를 추구
- SW 플랫폼에 대한 보안(데이터 기밀성, 무결성, 가용성 보장)
- 침해사고를 신속하게 탐지, 대응 및 복구, 사용자 교육 등

22) 각 회원국이 국제 및 국내 법률과 규정에 따라 자체적인 체계를 구축할 것, 다른 국가들도 안전한 SW에 대한 공동의 비전을 추구하기 위해 원칙을 채택하기를 권장함(2022년 5월)

23) https://www.pmc.gov.au/resources/quad-leaders-summit-2023/2023-quad-leaders-summit-documents

5. 시사점

디지털 전환 가속화의 핵심에는 SW가 있으며, SW 개발과정에서 공개 SW의 비중이 높아짐에 따라 SW 공급망 전반에 대한 사이버 위협이 높아지고 있다.

- SW 공급망 보안에서 공개 SW의 보안취약점 관리가 매우 중요하며, 특히 공개 SW의 비용 효과적인 보안취약점 관리 방안으로 SBOM이 대두되고 있음

지난 수년간 SW 공급망 공격은 국제적인 논의의 중심이 되고 있으며 미국, 유럽 등 주요국을 중심으로 제도화를 통한 SW 공급망 보안 강화 동향이 보고되고 있다.

- 국내에서도 SBOM 기반 SW 공급망 보안 체계 확산을 위해 SW 개발사 – 공급(유통)사 – 운영사 간에 SBOM을 원활하게 공급(유통)할 수 있는 관리 체계를 마련할 필요가 있음
- 미국, 유럽 등 변화하는 SW 공급망 보안 관련 정책을 빠르게 분석하고 선제적으로 대응하여, 공급망 분야 국내 기준과 글로벌 기준의 조화를 통해 국내 기업의 해외 진출을 위한 진입장벽의 해소 역할이 필요(세이프 하버 정책의 마련[24])

24) 안전한 항구(Safe Harbor) 정책이란 규제 당국이 제시한 요건이나 기준을 충족하면 해당 규범을 준수한 것으로 보아 더 이상 위법한 것으로 취급하지 않는다는 원칙

제2장

SW 공급망 위험관리 방안

제2장은 정부·공공기관 및 기업들의 SW 개발–공급(유통)–운영 등 공급망 전 과정에서 SW 공급망 보안관리를 위한 권고사항들을 체계적으로 정리하였고, 이와 함께 SBOM 기반 SW 공급망 보안 관리방안을 제시하였다.

제1절 (안전한 SW 개발환경의 필요성) 공급자, 공급망, 제품 및 서비스에서 발생할 수 있는 피해와 침해 가능성 등 SW 공급망 위험에 대응하여 사이버보안 공급망 위험관리(C-SCRM)를 전사적 위험관리 체계에 통합해야 하며, 공급망 참여자들이 개발, 공급(유통) 및 운영 등 각 단계에서 자신의 역할을 완수해야 SW 공급망 전체의 위험이 관리될 수 있다.

제2절 (SW 구성요소의 신뢰성 확보방안) SBOM은 SW의 구성요소를 목록화 한 것으로 'SW 구성요소 명세서'라 할 수 있으며, 이를 통해 SW 자산관리, 공개 SW 라이선스 및 보안취약점 관리가 가능하며, SBOM 도입 및 활성화를 위해 정부의 적극적인 지원과 기업들의 적극적인 참여가 필요하다. 보안취약점 관리 외에도 SBOM 활용·효과성을 강조하기 위해 '서체' 라이선스 위반사례 및 국내 공개 SW DB 통합 프로젝트(OSORI)를 소개하였다.

제3절 (SBOM 기반 SW 공급망 보안 강화방안) 개발, 공급(유통), 운영 등 SW 공급망 각 단계에서 SBOM을 생성, 보안취약점 분석 및 조치 등을 통해 SW 공급망의 투명성과 신뢰성을 확보할 수 있다. 이를 위해 SBOM 기반 SW 공급망 보안 관리체계를 정의하였고, 이를 확산하고 효과성을 높이기 위해 산업별 SW 공급망 거점 및 SW 공급망 관리센터 등을 제시하였다.

또한, SBOM 활용에 대한 국제적 사례로 국제의료기기규제당국자포럼(IMDRF)의 의료기기의 사이버보안을 위한 SBOM 원칙과 사례를 소개하였다.

제1절 안전한 SW 개발환경의 필요성

1. 공급망의 사이버보안 위험관리 개요

가. 공급망의 사이버보안 위험관리 정의

미국 NIST는 공급망 보안에 대한 기본 개념을 다음과 같이 정의하였다.[25)]

- **공급망 요소**(Supply Chain Element)는 시스템 및 구성요소의 연구 및 설계, 개발, 제조, 구입, 배포, 통합, 운영 및 유지보수 또는 폐기에 사용되는 조직과 개체, 도구를 포함
- 공급망의 전반적인 **사이버보안 위험**(Risk)은 공급자(개발사 및 공급(유통)사), 공급망(개발환경 및 업데이트 전송로), 제품 및 서비스에서 발생할 수 있는 **피해와 침해 가능성**으로 정의
- **공급망 전체의 사이버보안 위험**(Cybersecurity Risks throughout the Supply Chain)은 공급망에 걸쳐 있는 **제품 및 서비스의 보안취약점과 노출을 악용하는 위협에서 발생**
- **사이버보안 공급망 위험 평가**(Cybersecurity Supply Chain Risk Assessment)는 공급망 전체의 사이버보안 위험, 발생 가능성 및 잠재적 영향에 대한 체계적인 조사를 의미
- **공급망 사이버보안 위험관리**(Cybersecurity Supply Chain Risk Management, C-SCRM)는 공급망 전체에서 사이버보안 위험에 대한 노출을 관리하고 적절하게 대응하기 위한 전략, 정책 및 절차 등의 관리체계를 의미

나. 공급망 사이버보안 위험관리 체계 구축 방안

NIST는 '공급망 사이버보안 위험관리 활동'(이하 C-SCRM)을 통해 기업 또는 기관이 공급망에서 사이버보안 위험을 관리하는데 도움이 되는 활동을 제시하였으며, 주요 내용은 아래와 같다.

- C-SCRM은 연구 및 설계, 개발, 제조, 통합, 운영 및 유지보수, 폐기 등 전체 'SW 개발 생명주기(SDLC)'에 걸친 활동을 포괄하므로 공급망 전반의 사이버보안 위험을 해결하려면 C-SCRM이 SDLC 내에 통합되어야 함
- 또한, 정보보안 및 개인정보보호, 시스템 개발자 및 엔지니어, 인수, 조달, 법무, 인사(HR) 등 기업 내 다양한 이해관계자 그룹이 함께 참여해야 함
- 공급망 내에서는 적대적(Adversarial) 또는 비적대적 이유로 다양한 사이버 위협이 발생할 수 있으며, 사이버 위협을 해결하기 위해 C-SCRM을 전사적 위험관리 체계에 통합해야 함

25) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (C-SCRM), NIST SP 800-161r1 (2022년 5월)

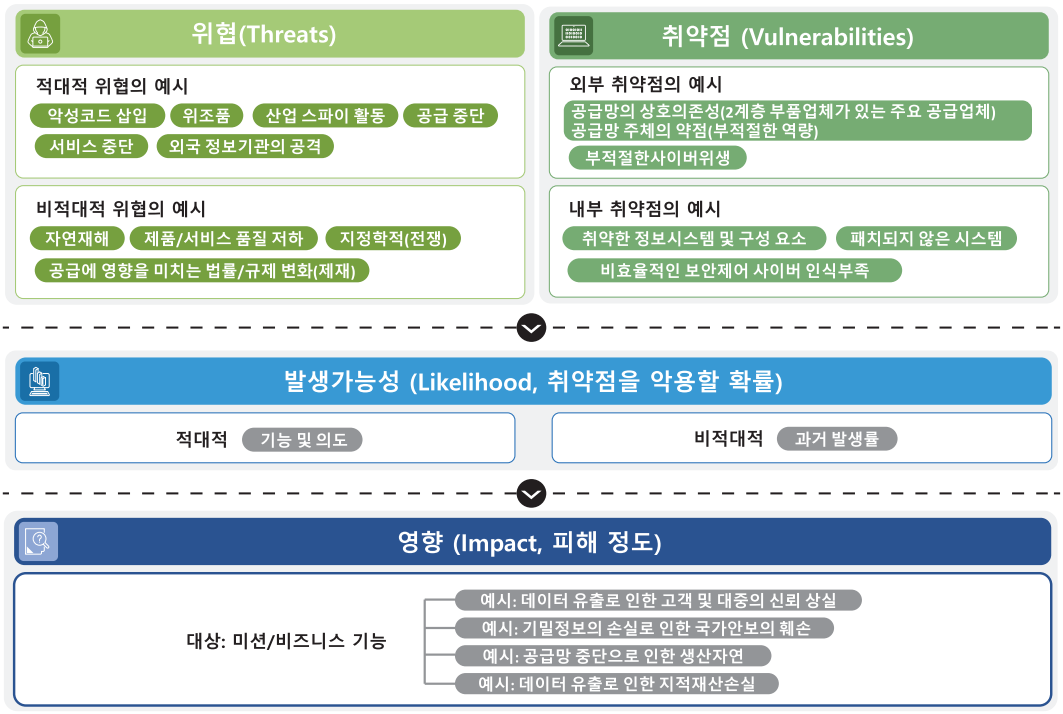


그림 6 공급망 전반의 사이버보안 위험 예시

또한, 기업 전반의 위험을 관리하기 위해서는 전사적 수준, 프로세스 수준, 운영 수준 모델을 포함하는 '다단계 전사적 위험관리'가 필요하다. '다단계 전사적 위험관리'에서 C-SCRM 활동은 아래와 같은 세 가지 레벨로 구분하여 수행한다.

- **레벨-1(전사)**
  전반적인 C-SCRM 전략, 정책, 이행 계획을 통해 전사적인 C-SCRM으로 관리되는데 필요한 기조, 거버넌스 구조, 경계를 설정

- **레벨-2(프로세스)**
  레벨-1에서 결정한 전사적인 상황과 방향을 가정하고, 그것을 특정한 미션(Mission) 및 비즈니스의 프로세스에 맞게 조정

- **레벨-3(운영)**
  C-SCRM 계획은 정보시스템이 비즈니스·기능·기술 요구사항을 충족하고, 적절하게 조정된 통제를 포함하는지를 결정하기 위한 기반을 제공함. 단, 운영 수준은 레벨-2에서 제공하는 환경과 방향 설정에 따라 결정됨

그림 7 다단계 전사적 위험관리(C-SCRM) 개요

표 7 이해관계자의 역할에 따른 주요 C-SCRM 활동 예시

수준	이해관계자	역할	활동
1. 전사	경영진[26]	C-SCRM 활동에 대한 경영진의 감독을 확립	• 전사적 C-SCRM 전략 정의 • 거버넌스 구조 및 운영 모델 수립 • 기업의 위험 구성, 위험관리 방식의 기조 설정 • 대체적인 구현 계획, 정책, 목적, 목표를 정의 • 전사적 수준의 C-SCRM 의사 결정 수행 • C-SCRM PMO(프로젝트 관리조직) 구성
2. 프로세스	비즈니스 관리자[27]	기업의 미션과 비즈니스 프로세스 측면에서 공급망의 사이버보안 위험을 평가, 대응, 모니터링	• 비즈니스 프로세스별 전략 개발 • 정책, 절차, 지침, 제약사항 개발 • 신규 IT 프로젝트에서 보안취약점 감축 • C-SCRM 구현 계획 개발 • 기업의 위험관리 체계를 비즈니스 프로세스에 맞게 조정 (예, 위험 허용 범위 설정) • 비즈니스 프로세스 내 위험관리 • C-SCRM에 관해 레벨1에 보고, 레벨3의 보고에 대한 조치
3. 운영	시스템 관리자[28]	개별 시스템 및 업무에 C-SCRM을 적용하고 운영 및 보고	• C-SCRM 계획 개발 • C-SCRM 정책과 요구사항 구현 • 레벨1과 2에서 제공한 제약사항 준수 • 개별 시스템의 상황에 맞게 C-SCRM을 조정하고 SDLC에 적용 • C-SCRM에 관해 레벨2에 보고

26) 기업의 C-Level 임원(예, CEO, CIO, COO, CTO, CISO, CPO, CAO 등)

27) 프로젝트 매니저, 통합 프로젝트 팀원, R&D, 엔지니어링(SDLC 감독자), 공급사 및 원가 관리, 기타 신뢰성, 안전성, 보안, 품질자, C-SCRM PMO(Project Management Office) 등

28) 아키텍트, 개발자, 시스템 책임자, QA/QC, 테스터, 계약 담당자, PMO 팀원, 제어시스템 운영자

2. SW 개발·운영 환경의 공급망 보안체계 구축 방안

SW 공급망의 참여자는 크게 개발사, 공급(유통)사, 운영(고객)사로 구분할 수 있으며, 각 참여자가 안전한 SW의 개발, 공급(유통), 운영을 위해 자신의 역할을 완수해야 SW 공급망 전체의 보안 위험이 관리될 수 있다.

가. 안전한 SW 개발·운영을 위한 개발사, 공급사, 운영사의 역할

2022년 8월, 미국의 지속적 보안 프레임워크(Enduring Security Framework, ESF)[29]는 'SW 공급망 보안 – 개발사, 공급(유통)사, 운영(고객)사를 위한 권장 활동'을 통해 SW 공급망 주요 참여자의 공급망 보안 활동을 제시하였으며, SW 개발, 공급(유통), 운영과 SW 보안 활동의 상호 관계는 아래 [그림 8]과 같다.

그림 8 SW 공급망 참여자에 따른 보안 활동

29) ESF는 CISA, NSA 등이 참여하는 주요 인프라 및 국가 안보 시스템에 대한 위험을 해결하기 위한 민관 파트너십

개발사	SW의 설계, 구현, 검증 등 개발단계에서 보안 활동을 통해 보안취약점을 최소화해야 할 뿐만 아니라, SW에 포함된 라이브러리와 빌드 및 배포 체계의 보안성을 확보하여야 함
공급사	보안 요구사항 충족 여부 확인, 타사 SW의 검증, 실행 파일 테스트를 통해 SW 제품의 보안을 검증하고, 보안취약점을 발견했을 때는 고객(운영)사에 이를 알리고, 보안취약점에 대응해야 함
운영사	보안 요구사항과 공급망 위험관리(SCRM) 요구사항을 정의하고, 그에 따라 SW 인수테스트를 진행하며, 제품 적용 및 생명주기 관리에 필요한 보안 및 공급망 위험관리 대책을 구현해야 함

1) [개발사]를 위한 공급망 보안 권장 활동 주요 내용[30)]

• [개발사]는 개발의 각 단계에서 개발자가 수행해야 할 보안 활동을 문서로 작성하고, 실제 준수되도록 해야 함

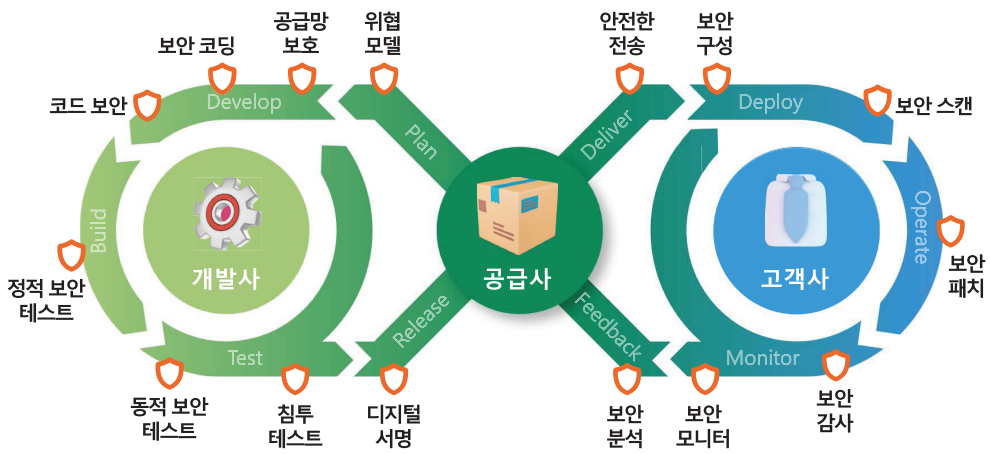


그림 9 SW 공급망 보안 개발 프로세스

30) Enduring Security Framework, 「Securing the Software Supply Chain – Recommended practices guide for developers」 (2022년 10월)

[개발사]가 해야 할 공급망 보안 권장 활동은 아래 표와 같다.

표 8 개발사를 위한 공급망 보안 권장 활동

구분	세부 내용
안전한 제품 기준 및 관리	• 개발팀이 SW 보안 개발 프로세스의 각 보안 활동에서 활용할 개발 보안 정책과 절차 등 프로세스를 문서로 정의 • 조직의 최고경영진은 보안 개발 정책과 관행이 예산과 일정 내에서 지원되고, 개발팀이 준수할 수 있도록 관리
안전한 코드의 개발	• 내부자에 의한 소스 코드 수정 또는 공격 차단 • 안전한 공개 SW 관리 관행 마련 • 안전한 SW 개발 관행 마련(안전한 개발자 환경 및 빌드 설정 사용) • 코드 통합시 보안성 검증 • 신고된 결함/보안취약점에 대한 체계적인 대응 • 외부 개발팀에 의한 제품 기능 확장 시 보안성 확보
타사 구성요소 검증	• 타사 바이너리의 보안취약점 점검 • 타사 구성요소 선택 및 통합시 보안 위험 평가 • 신뢰할 수 있는 공급사로부터 컴포넌트(부품) 확보 • 통합된 구성요소 유지 관리(공급사 활동 모니터링, 관련 계약 맺기) • SBOM을 이용한 검증
빌드 환경 보안 강화	• 빌드 체인 공격 대응(소스코드 저장소, 빌드 시스템에 대한 공격 대응) • 서명 서버 해킹 대응
코드 배포 시 보안 강화	• 최종 패키지 검증 • 배포 시스템의 SW 패키지·업데이트 보호 배포 • 시스템 보호

2) [공급사]를 위한 공급망 보안 권장 활동 주요 내용[31)]

[공급사]는 [개발사]와 [운영사] 사이의 중개자 역할을 하므로, 공급망 보안에 관한 다음 사항을 갖출 수 있도록 노력할 필요가 있다.

- 안전하게 제공되는 SW 무결성 유지
- SW 패키지·업데이트 유효성 검사(Validation)
- 알려진 보안취약점 관리
- 운영(고객)사의 보안취약점 신고를 접수하고 이를 해결하기 위해 개발사 통보

[공급사]가 해야 할 공급망 보안 권장 활동은 아래 표와 같다.[32)]

31) Securing the Software Supply Chain – Recommended practices guide for suppliers, Enduring Security Framework(2022년 9월)

32) 개발사가 공급사를 겸하는 경우, 개발사 권장 활동에 포함하여 수행함

표 9 공급사를 위한 공급망 보안 권장 활동

구분	세부 내용
조직 준비	• SW 보안 점검을 위한 기준 정의 및 수행 조직 준비
SW 보호	• 모든 형태의 코드를 비인가 접근으로부터 보호 • SW 출시(Release) 무결성 검증 메커니즘 제공 • SW 출시 버전의 보관 및 보호
보안성이 높은 SW 제작	• 보안 요구사항을 충족하는 SW 설계 • 타사 공급 SW가 보안 요구사항을 충족하는지 검증 • 컴파일 및 빌드 프로세스의 보안 구성 • 사람이 읽을 수 있는 코드(Human-readable code)에 대한 검토 및 분석 • 실행 파일 테스트를 통해 보안취약점 식별, 보안 요구사항 준수 여부 검증 • 기본 보안 설정이 안전하도록 SW 구성
보안취약점 대응	• 지속적인 보안취약점 식별, 분석, 보완

3) [운영사]를 위한 공급망 보안 권장 활동 주요 내용[33)]

- 운영사는 SW 제품의 구매 시 요구사항 정의, 제품 평가, 획득, 적용(배포), 유지 관리의 프로세스를 따름
- 운영사는 특정한 위험 완화 활동을 할 때 조직의 구조 및 임무, 위험의 허용 범위에 따라 각 프로세스를 보완하는 것이 필요

[운영사]가 해야 할 공급망 보안 권장 활동은 아래 표와 같다.

표 10 운영사를 위한 공급망 보안 권장 활동

구분	세부 내용
조달 및 인수	• 보안 요구사항 정의 • 제품 평가(평가 대상 제품에 대한 SBOM 요구) • 구매 계약에 공급망 보안 요구사항 추가
적용 (배포)	• 제품 인수 시 공급사가 사용하는 SW 배포 인프라의 보안 검증, 제품과 구성요소의 무결성 검증, 인수한 제품과 SBOM을 비교, 확인 등 보안 활동 수행 • 기능 테스트에는 제품 설치 및 설정, 테스트 수행 및 결과 보고 프로세스를 구비 (향후 참조를 위해 테스트 환경을 보관) • 보증, 충분한 시간 동안 테스트하여 숨겨진 악성 기능이 발생하지 않도록 유의하고 계약에 포함된 보안 관련 명세를 검증 • 구성 제어 위원회(Configuration Control Board)의 검토 • 기능 및 보증 결과 검토, SW 자체 및 기존 시스템/SW와의 연관성을 포함한 위험 검토, 이를 기반으로 한 제품의 진행/중단 결정

33) Securing the Software Supply Chain – Recommended practices guide for customers, Enduring Security Framework(2022년 10월)

구분	세부 내용
적용 (배포)	• 통합, 구매한 제품을 운영환경에 통합하면서 운영환경에 필요한 보안 통제를 배포하고, 지속적 모니터링 등 보안 활동 수행 • 초기 제품의 배포 시작 시 성공 여부를 검증하고 분석 수행 • 클라이언트 시스템, 기업 네트워크, 클라우드 등에 SW를 배포하는 단계로서 보안 운영 측면에서 암호화 세션 등을 지속해서 모니터링하는 등의 보안 활동 수행
제품 업그레이드	• 계획 수립, 통합-보안-상호운영 테스트, 회귀테스트 필요 • SW 업그레이드, SW를 다운받은 인프라에 관한 무결성 검증, 공급사의 SBOM 및 자체 증명서 확인 • 업그레이드 후 모니터링을 통해 이상 동작 확인 등 보안 활동 수행
제품 단종	• 단종된 제품의 제거 시 발생할 수 있는 보안 위협을 예방하기 위한 활동으로서 제품 관련 계정 및 권한의 비활성화 • 보안 인프라에서 제품 관련 모든 규칙/역할/그룹 제거 등 보안 활동 수행
교육/지원	• 교육·훈련 SW 및 관련 시스템, 환경을 보호함으로써 구매 SW에 관한 교육·훈련이 잘 진행될 수 있도록 지원
SW 운영	① 사용자 • 제품의 최종 사용자 또는 책임 있는 자는 운영사의 IT 시스템에서 발생하는 오류나 이상 현상을 보고함으로써 기업의 IT 보안에 기여해야 함 • 운영사는 이상 현상을 보고하는 방법을 사용자에게 교육하고, 문제가 발생한 특정한 제품을 격리할 수 있어야 하며, 접수된 문제를 공급사에 알리고 추적하는 절차를 마련하는 등 보안 활동 수행 ② 업데이트 • 운영사는 승인된 채널과 출처에서만 업데이트를 하고, 개발사와 공급사는 상세한 업데이트 노트, 전자서명 등을 이용해 제공 인프라와 메커니즘의 무결성 검증 방법을 도입사에 제공해야 함 • 운영사는 자동화된 방법으로 SBOM 활용 및 업데이트 내용의 무결성 확인, 업데이트 전과 후의 동작으로 비교하여 이상 동작을 모니터링하여 문제 발생 시 배포 중단 등 활동 수행
보안 및 공급망 위험 관리 운영	• 운영사는 제품의 기능 변경 및 보안 이벤트 모니터링, 정기적인 보안 테스트, 제품에 대한 감사 수행, 전체 SCRM에 관한 평가와 대응 등의 지속적인 보안 활동 필요 • 배포된 보안 에이전트의 무결성 보호, 지속적인 위협 헌팅(Hunting), SW 제품의 모니터링과 분석을 위한 보안 운영 교육, 제품에 대한 위협 모델링을 수행하고 정부 및 업계 간 협업을 통해 SW 공급망 위험 처리 등 활동

※ 다만, ESF 가이드를 국내에 적용할 때 [개발사]와 [공급사]의 역할이 미국의 환경과는 다소 차이가 있을 수 있어 이를 고려해야 한다.

나. 안전한 SW 개발 체계의 활용

개발사, 공급사, 운영사 등 SW 공급망 보안 참여자는 공급망 보안 활동을 수행할 때 NIST가 발표한 '안전한 SW 개발체계(SSDF)[34]를 활용할 수 있다.

- 인력, 프로세스, 기술이 안전한 SW 개발을 수행할 수 있도록 준비되어 있는지 확인
- SW의 모든 구성요소가 변조되거나 비인가 접근되지 않도록 보호
- 출시할 때 보안취약점을 최소화한 보안이 잘 갖춰진 SW를 제작
- 출시된 SW에 남아있는 보안취약점을 파악하고 해당 보안취약점을 해결하기 위해 적절히 대응하고 향후 유사한 보안취약점이 발생하지 않도록 예방

NIST의 SSDF는 다음과 같은 특징이 있다.

- 안전한 SW 개발에 관한 지식이 없어도 이해할 수 있는 공통 언어를 제공하여 조직 내·외부 이해관계자가 소통하는 데 도움을 줌

> 내·외부 이해관계자 : 조직 내부의 사업 책임자, SW 개발자, 프로젝트 관리자, 사이버보안 전문가, IT 운영자, 보안취약점이 적은 SW 확보가 필요한 조직 외부의 SW 구매자 등

- 사용하는 SDLC 모델과 관계없이 적용할 수 있음
- 기술, 플랫폼, 프로그래밍 언어, 운영환경과 관계없이 모든 유형의 SW 개발에 사용할 수 있음

SSDF는 위의 권고를 충족할 방법으로 아래 네 가지 권장 사항을 제시하였으며, 각 원칙에 관한 자세한 설명과 필요한 과업(Task), 이에 관한 개념적인 구현 예시와 관련 참고 문서도 함께 제시하고 있다.

- 조직 준비(Prepare the Organization, PO)
- SW 보호(Protect the Software, PS)
- 보안성 높은 SW 제작(Produce Well-Secured Software, PW)
- 보안취약점 대응(Respond to Vulnerabilities, RV)

34) Secure Software Development Framework(SSDF) Version 1.1 : Recommendations for Mitigating the Risk of Software Vulnerabilities, NIST SP 800-218(2022년 2월)

표 11 SW 개발 생명주기(SDLC) 단계별 개념 정의

단계	개념
설계	• 개발할 SW의 기능과 제약조건 등을 정의하고, 시스템이 무엇을 수행할지 기능을 정의하여 논리적으로 결정하는 단계
개발	• 설계 단계에서 논리적으로 결정한 해결 방법(알고리즘)을 프로그래밍 언어를 사용하여 실제 프로그램을 작성하는 단계
시험	• 개발한 시스템이 요구사항을 만족하는지, 실행 결과가 예상한 결과와 정확하게 맞는지를 검사하고 평가하는 단계
배포	• 상품이나 서비스가 생산자나 서비스 제공자로부터 최종 고객에게 이르는 과정에 개입되는 다양한 조직들 사이의 거래 관계를 설계하고 전달 및 운영하는 단계
운영	• 시스템을 구매 후 일어나는 프로그램 오류 수정, 시스템 디자인 수정, 새로운 요구사항, 시스템 환경변화에 대한 교정 등 일련의 과정을 수행하는 단계

표 12 SSDF 구현을 위한 공급망 보안 권장 활동

영역	관행
조직 준비 (PO)	PO.1 : SW 개발을 위한 보안 요구 사항 정의
	PO.2 : 역할 및 책임 구현
	PO.3 : 지원 도구(Tool chain) 구현
	PO.4 : SW 보안 점검 기준 정의 및 사용
	PO.5 : SW 개발을 위한 보안 환경 구현 및 유지 관리
SW 보호 (PS)	PS.1 : 모든 형태의 코드를 비인가 접근 및 변조로부터 보호
	PS.2 : 출시하는 SW의 무결성 검증을 위한 메커니즘 제공
	PS.3 : 출시된 SW의 보관 및 보호
보안성 높은 SW 제작 (PW)	PW.1 : 보안 요구사항을 충족하고 보안 위험을 완화하도록 SW를 설계
	PW.2 : SW 설계를 검토하여 보안 요구 사항 및 위험 정보를 준수하는지 검증
	PW.3 : 타사 SW가 보안 요구사항을 준수하는지 검증 (PW.4에 통합)
	PW.4 : 가능하면 기능을 복제하는 대신 보안이 잘된 기존 SW를 재사용
	PW.5 : 보안 코딩 관행을 준수하여 소스 코드 생성
	PW.6 : 실행파일의 보안을 개선하도록 컴파일, 인터프리터 및 빌드 프로세스를 구성
	PW.7 : 사람이 읽을 수 있는 코드(Human-readable code)를 검토·분석하여 보안취약점을 식별하고 보안 요구사항을 준수하는지 검증
	PW.8 : 실행 코드를 테스트하여 보안취약점 식별 및 보안 요구 사항 준수 여부 검증
	PW.9 : SW가 기본 설정으로 보안을 갖추도록 구성

영역	관행
보안취약점 대응 (RV)	RV.1 : 지속적인 보안취약점 식별 및 확인
	RV.2 : 보안취약점의 평가, 우선순위 지정, 해결
	RV.3 : 보안취약점을 분석하여 근본 원인 파악

참고 국내 자체 개발 공개 SW 'DevSecOps' 기술 공개

국내 기업이 자체 개발한 DevSecOps(개발·보안·운영) 시스템 'NShiftKey'를 공개 SW 앱으로 일반에 공개함[35)]

- **(추진배경)** 'Let's shift left' 전략으로 서비스의 기획부터 출시까지 각 단계에서 필요한 보안 요소들을 산출하고, 자체 기술을 적용하여 운영하고 있음. DevSecOps 전략 중 하나로, 소스코드를 사전에 점검하는 프로세스를 보다 쉽게 정착할 수 있도록 외부에서도 무료로 사용하도록 도구를 공개
- **(기대효과)** Github를 활용하여 개발이 이루어지고 있기 때문에, 개발자가 개발한 소스코드를 반영할 때마다 발생가능한 보안취약점을 확인하여 조치할 수 있음. 개발자라면 누구나 간단한 설치만으로 자신이 개발한 제품 및 서비스의 보안성을 높일 수 있으며, 깃허브(GitHub)를 통해 무료로 다운로드 가능함

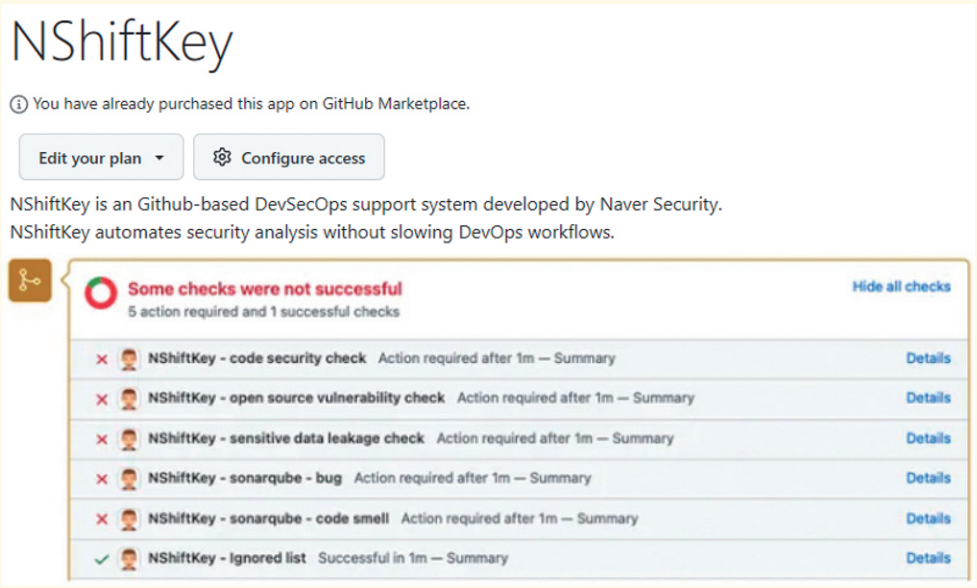


그림 10 NShiftKey 보안 체크 화면

35) Github marketplace를 통해 2023년 6월에 공개(https://github.com/marketplace/nshiftkey)

제2절 SW 구성요소의 신뢰성 확보 방안

미국 OMB의 'SW 공급망 보안 강화에 대한 각서(M-22-18)'는 연방정부의 SW 공급망 보안을 강화하기 위해 조달 정책을 개선하고자 한 것이다.

- 특히, SW 부품 명세서라고 할 수 있는 SBOM의 공유를 통한 SW 구성요소의 투명성 강화를 강조
- SBOM이 활성화되면 SW 구성요소의 전반적 가시성이 확보되어, 이에 기반한 보안 기술이 새롭게 등장하고, 향후 SW 공급망의 위험관리를 위한 인텔리전스(Intelligence) 업무의 자동화까지 가능할 것으로 기대
- 향후 미국, EU, 일본에 SW 제품 수출 시 보안성 강화 및 보증에 관한 다양한 컴플라이언스 준수 등 우리 기업에도 지속해서 도움이 될 것으로 예상되지만, ① 안전한 SW 개발환경을 구축하고, ② 공개 SW 및 기타 제3자 SW 구성요소의 위험을 관리할 수 있는 SBOM이 도입되고 일상화되어 정착하기까지는 범정부 차원의 지원과 기업들의 적극적인 참여가 중요

SBOM은 제조업의 자재명세서 또는 부품명세서(BoM, Bill of Materials), 식품 공급(유통)에 사용되는 식품의 원재료 명세서(food ingredients)의 개념을 SW에 적용함

표 13 SBOM과 기타 BOM 명세서와 비교

구분	적용 분야	사용 목적
Food ingredients	식품	공급(유통)되는 식품에 관한 소비자의 위험 성분 확인
BOM	제조업	지속적인 양산 체제 유지를 위한 부품 관리와 자동화
SBOM	SW	공급망 위험관리를 위한 투명한 SW 구성요소 정보 제공

1. SBOM이란?

SBOM은 SW 구성요소를 서술하는 일종의 메타 데이터로 SW 전체의 구성요소를 목록화한 것이다.

미국 NTIA는 SBOM을 'SW 재료의 목록'이며 "SW 구축에 사용되는 다양한 구성요소의 세부 사항과 공급망 관계를 포함하는 공식적인 기록"으로 정의[36]

- 대부분의 SW는 개발 시에 외부 라이브러리나 공개 SW를 포함하여 개발하고 있어 SW 공급망이 복잡해지고, 보안취약점이 늘어남에 따라 이를 추적하고 관리해야 할 필요성이 대두됨
- 국내에서는 SW 구성 명세서, SW 구성요소 명세서, SW 부품명세서 등으로 다양하게 부르고 있음

36) NTIA : National Telecommunications and Information Administration

- 본 가이드라인에서는 국내 정부·공공기관 및 기업 관계자 등의 편의를 위해 SBOM을 'SW 구성요소 명세서'로 통칭
- SW 구성요소를 식별·관리할 수 있는 정보를 제공하는 SBOM을 SW 구성요소의 투명성 강화 방안으로 사용하기 위해 NTIA는 SBOM의 최소 요건을 제시[37]
- 다만, 각 기업(기관)의 사용 목적에 부합하도록 SBOM에 포함되어야 하는 항목을 추가·수정하여 활용할 수 있음

SW 공급망을 통한 SolarWinds 및 Log4j 공격이 큰 피해를 초래하면서, SW 내 어떤 구성요소가 존재하는지 신속하게 파악하고, 위험에 대처하기 위한 도구로 SBOM이 주목받고 있다.

2. SBOM의 필요성 및 효과성

SBOM은 SW를 개발하거나, 구매할 때 또는 시스템 운영에도 활용할 수 있으며, SW 생명주기 및 역할에 따른 이점은 다음과 같다.

- **[개발자]**는 공개 SW 및 타사 SW의 구성요소[38]를 사용하여 제품을 만드는 경우가 많음. 이 경우 SW 개발기업은 SBOM을 통해 해당 구성요소가 최신 버전인지 식별하고, 새로운 보안취약점에 신속하게 대응할 수 있음
- **[구매자]**는 SBOM을 사용하여 투명하게 보안취약점 또는 라이선스 분석을 수행할 수 있으며, 이 두 가지 분석은 제품의 전반적인 위험 수준을 평가하는 데 활용할 수 있음
- **[운영자]**는 SBOM을 활용하여 새로 발견된 보안취약점이 잠재적 위험에 노출되어 있는지를 쉽고 빠르게 확인하고 관리할 수 있음

그림 11 SBOM 활용의 효과성

37) "The Minimum Elements For a Software Bill of Materials(SBOM)"(NTIA, 2021년 07월)

38) SBOM은 기본적으로 SW 구성요소가 가진 종속성(Dependency)을 연결하는 트리(Tree) 구조의 형식으로, 이를 통해 Log4j와 같이 여러 시스템과 패키지에서 사용하는 SW 구성요소를 빠르게 식별할 수 있음

참고 미국 전기통신정보청(NTIA)의 SBOM 효과성 분석 사례

미국은 의료기기, 자동차, 에너지 산업 등 분야의 SW를 대상으로 공급망 단계별로 SBOM 적용 전과 후에 대한 효과성을 분석

- 새로운 보안취약점이 발견되면 며칠 또는 몇 주 이내에 악용 사례가 보고되는 것과 대조적으로 방어자는 공급 단계의 복잡성으로 인해 최종 보안취약점 조치에 이르기까지 수개월 또는 수년까지 걸림
- SW 도입(운영)사의 보안취약점 관리는 개발 및 공급사에 의존할 수 밖에 없어 최종 운영단계에서 보안취약점 발견·조치에 필요한 기간이 길어질 수 있음
- SBOM이 제공하는 공급망 투명성은 SW 컴포넌트(부품) 개발사 및 공급사, 도입(운영)사 등을 포함하는 각 참여자가 동시에 보안취약점을 식별할 수 있도록 지원
- 아래 그림은 SBOM 적용 전과 후에 대한 보안취약점 발견 및 조치에 걸리는 시간을 비교한 것으로, SBOM 활용으로 보안취약점 발견과 동시에 공급망 전 단계에서 해결책 또는 완화(Mitigation) 조치를 즉시 시행

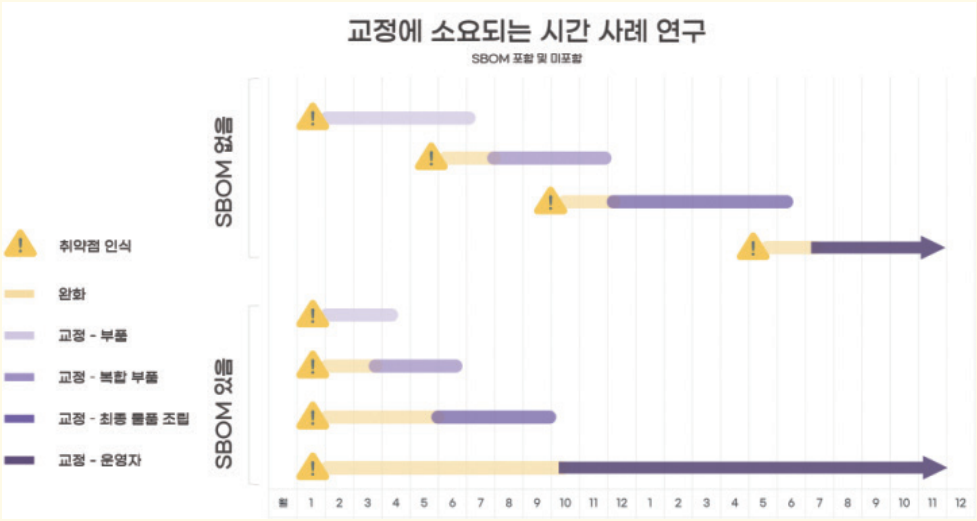


그림 12 SBOM 도입 효과성 분석

출처 : Roles and Benefits for SBOM Across the Supply Chain, NTIA(2019년 11월)

3. SBOM 최소 요건

가. NTIA의 SBOM 최소요건

SBOM이 기술해야 하는 데이터는 여러 가지가 있으나, 글로벌 공급(유통)을 위한 최소기준은 미국 NTIA에서 제시한 'SBOM을 위한 최소요건'이다.

- NTIA에서 정의한 SBOM의 최소요건은 ①데이터 필드(Data Fields), ②자동화 지원(Automation support), ③관행 및 프로세스(Practices and processes) 영역을 포함하도록 정의

1) 데이터 필드(Data Fields)

- NTIA는 SBOM 데이터 필드에 다음과 같은 7가지 기본항목이 포함되어야 한다고 명시[39)]

표 14 데이터 필드의 기본항목

항목	설명
공급자명 (Supplier Name)	• 구성요소를 생성하고, 정의 및 식별한 주체의 이름
타임스탬프 (Timestamp)	• SBOM 데이터로 변환(Assembly)한 날짜 및 시간 기록
저작권자 (Author Name)	• 구성요소에 대한 SBOM 데이터를 생성하는 주체의 이름
구성요소명 (Component Name)	• 최초 공급자에 의해 정의된 SW 단위에 할당된 명칭
버전 (Version String)	• 이전 버전으로부터 SW의 변경 사항을 지정하는 데 사용하는 식별자
고유 식별자 (Unique Identifier)	• 구성요소를 식별하는 데 사용되거나 관련 DB의 조회 키(Look-up Key) 역할을 하는 기타 식별자
종속성 관계 (Relationship)	• 상위(Upstream) 구성요소 X가 SW Y에 포함된다는 관계를 특정함

39) Framing Software Component Transparency : Establishing a Common Software Bill of Materials(2021년)

2) 자동화 지원(Automation support)

SBOM은 컴퓨터 시스템 간 교환이 용이하도록 정해진 형식에 맞춰 기술해야 한다. 이를 위해 NTIA는 다음 3가지 표준을 SBOM 최소 요소로 지정했다.

- NTIA는 SBOM 데이터 공유 및 교환을 위한 자동화 요구 사항으로 국제적으로 통용되는 세 가지 형식(SPDX, CycloneDX, SWID)을 활용하는 것으로 정의[40)]
- 다만, 각 형식마다 NTIA의 SBOM 기본 항목 데이터를 상이하게 표현 [표 15]

표 15 SBOM 표준간 데이터 속성 비교

Data Fields	SPDX	CycloneDX	SWID
공급자명 (Supplier Name)	PackageSupplier :	Supplier publisher	〈Entity〉@ role(soffwareCretor/ publisher),@name
컴포넌트명 (Component Name)	PackageName :	name	〈softwareIdentity〉 @ name
고유 식별자 (Unique Identifer)	SPDX Document Namespace SPDXID :	Bom/seriaNunber Component/bom-ref	〈softwareIdentity〉 @ tagID
버전 (Version String)	PackageVersion :	Version	〈softwareIdentity〉 @ version
컴포넌트 해시 (Component Hash)	PackageChecksum : PackageVerificationCode :	Hash “alg”	〈Payload〉/../〈File〉 @ [hash-algorithm]:hash
종속성 관계 (Relationship)	Relationship : DESCRIBES CONTAINS	(중첩된 어셈블리 또는 하위 어셈블리 및 종속성 그래프에 내장되어 있음)	〈Link〉 @rel, @href
저작권자 (Author Name)	Creator :	metadata/authors/ author	〈Entity〉 @role (tagCreator), @name

40) NTIA에서 직접적으로 SBOM 표준을 개발·제정한 것은 아니며, 빠른 시장 적용을 위해 기존에 활성화된 SBOM 표준을 인용한 것임

3) 활동 및 프로세스(Practices and processes)

SBOM을 업데이트하고 제공해야 하는 방법과 시기와 관련된 6가지 요구사항을 정의하고 있다.

- Frequency : 새롭게 빌드 또는 릴리즈(Release) 되는 경우 새로운 SBOM을 반드시 생성
- Depth : SBOM 작성자는 최상위 구성요소부터 하위 구성요소까지 포함하여 모든 종속성을 표시
- Known Unknowns : SBOM에 종속성이 표시되지 않은 경우에 표기
  1) 구성요소에 추가 종속성이 없어서 표시하지 않았는지 여부
  2) 종속성을 알 수 없는 불완전한 상태인지 기록
- Distribution and Delivery : SBOM을 적절한 접근권한과 방식을 통하여 제공
- Access Control : SBOM 공개 범위에 따라 적절한 접근제어 조건을 지정
- Accommodation of Mistake : SBOM 생성은 아직 초기 단계로 SBOM 수요자는 의도하지 않은 오류 또는 누락을 용인

CISA의 SBOM 최소요건 개정 예고

SBOM은 SW 공급망 보안을 강화하고, SW의 투명성을 높일 수 있는 수단이지만, 아직 SBOM에 어떤 정보를 담을 것인가에 대해서는 명확하게 정해지지 않았다. 이에 미국 CISA는 2021년에 SBOM 최소요건을 제정하였으나, 5개의 연구반(Working Group)을 중심으로 실현할 수 있는 기본 요소가 늘어났으며, 산업 피드백을 통해 요구사항이 확장되었음을 인정하고, 현재 최소요건의 개정 작업이 진행 중 임을 밝혔다.(2023년 9월)

SW 공급망 보안은 글로벌 표준과의 조화가 요구되는 만큼 본 가이드라인 개정 시, CISA의 SBOM 개정 사항을 적극 반영하여 우리 산업계가 국제적인 경쟁력을 갖출 수 있도록 지원할 것이다.

4. SW 보안취약점 및 라이선스 관리방안

가. 알려진 보안취약점 관리

SCA(SW Component Analysis)[41] 도구를 활용하여 SW 구성요소를 분석하고, SBOM을 생성할 수 있다.
또한 이를 기반으로 공개 SW의 알려진 보안취약점 정보와의 매칭이 가능하다.

1) SBOM에 연계된 보안취약점 정보 확인

- 공개 SW 등에 대한 구성요소를 식별하여 SBOM 생성 후 'Vulnerabilities' 항목 등에서 알려진 보안취약점 정보(CVE, KEV 등)[42]를 확인


```
"vulnerabilities": [
    {
        "bom-ref": "BomRef.6mrtsnb7hug.s9l1smbt9go",
        "id": "CVE-2019-11405",
        "ratings": [
            {
                "score": 7.4,
                "severity": "high",
                "method": "CVSSv3"
            }
        ],
        "properties": [
            {
                "name": "KEV",
                "value": "false"
            },
            {
                "name": "HEV",
                "value": "true"
            }
        ]
    },
```


그림 13 SBOM에 연계된 보안취약점 정보 예시(CycloneDX 포맷)

41) SCA : SW 구성요소 분석(Software Composition Analysis) 기술로 상용 및 공개 SW 도구가 있음

42) CVE(Common Vulnerabilities Exposures)란, 공개적으로 알려진 컴퓨터 보안 결함의 목록, CVE는 보통 CVE ID 번호가 할당된 보안 결함을 뜻함. KEV(Known Exploited Vulnerability)는 악용 사례가 알려진 보안취약점으로써, 공격 가능성이 매우 높아 보완 조치가 시급함

2) 발견된 보안취약점에 대한 관리 시스템의 영향범위를 분석

• 상용 및 공개 SW에서 발견된 보안취약점에 대하여 미국 NVD가 제공하는 보안취약점 정보 확인 (https://nvd.nist.gov/vuln/detail/{CVE_ID})

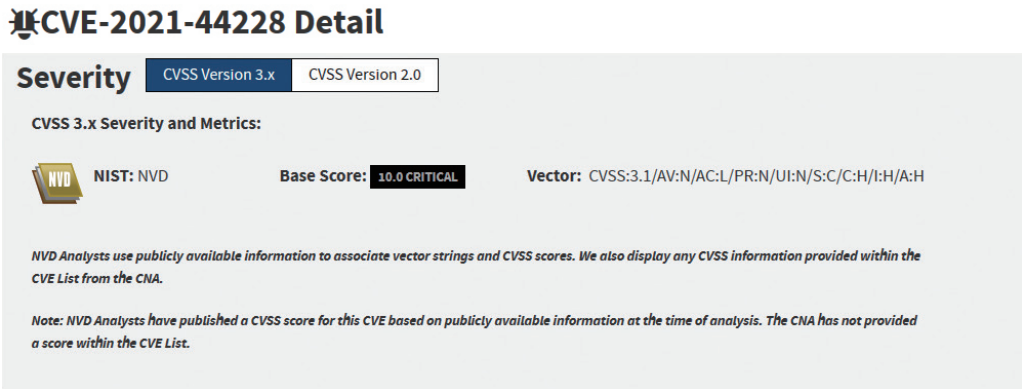


그림 14 NVD를 통한 알려진 보안취약점(CVE) 조회 화면

3) NIST에서 제공하는 보안취약점의 영향범위와 심각도 등을 활용하여 위험 수준을 평가하고 조치 우선순위를 결정[43]

• CVSS[44]는 NVD 보안취약점 데이터베이스에서 정한 심각도와 기본 점수(Base Score)의 등급으로 위험도를 나타냄(V2.0과 V3.0 두 가지 방식으로 제공)

CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	Base Score Range	Severity	Base Score Range
		None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

43) https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

44) CVSS(Common Vulnerabilities Scoring System)는 공격자가 보안취약점을 악용할 때 미치는 영향과 보안취약점의 위험도를 나타내며, 0.0 ~ 10.0 숫자가 높을수록 위험도가 더 높음

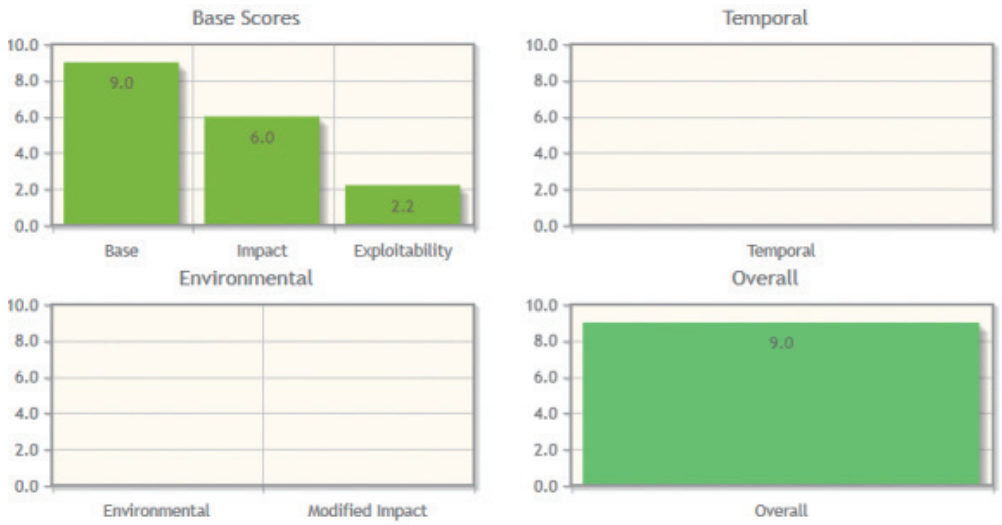


그림 15 기본 점수에 따른 악용 가능성 분석 예시(CVSS Calculator)

4) 보안취약점에 대한 조치계획 수립 및 관련자와 보안취약점 정보공유

- 타사 구성요소 등에서 발견된 보안취약점에 대하여 NVD 조치 방안을 확인
- 탐지된 보안취약점에 대한 조치계획을 산정된 우선순위에 따라 수립 후 개발기업, 운영기업(기관) 등에 해당 컴포넌트 정보를 공유
- 특히, CVSS 7.0 이상의 높은 위험도를 가진 보안취약점은 보안 담당자 등과 즉각적인 완화조치를 수행하거나, 조치 방안과 시기를 협의 해야함
- 위험도 판단에는 CVSS 외에 CISA의 KEV 등과 같이 추가적인 지표를 활용할 수 있음

Description

Apache Log4j2 2.0–beta9 through 2.15.0(excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0(along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j–core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

그림 16 NVD 보안취약점의 조치방안(Log4j 예시)

나. 공개 SW 라이선스 관리

특정 컴포넌트의 라이선스에 대해 준수가 불가능하거나 준수할 수 없는 조건을 발견할 수 있으며, 컴포넌트 자체를 변경하는 등의 조치를 수행

SBOM을 통해서 얻은 컴포넌트 정보에서 서비스 중단, 3rd 협력자 라이선스 만료 또는 폐기된 컴포넌트 정보를 확인하고 적절한 조치 필요

SBOM을 통해서 식별된 공개 SW, 상용 SW, 타사(3rd party) SW 등의 모든 라이선스 정보에 대해서 저작 권리와 사용 허가 등의 제공 여부를 추적·관리 필요

공개 SW 활용 확대와 함께 공개 SW 라이선스 관리의 중요성은 계속해서 강조되었으며, 이 과정에서 SBOM은 라이선스 관리에 유용하게 사용되고 있다.

- 생성된 SBOM은 SW에 포함된 컴포넌트의 라이선스 준수 상황을 확인하여야 하며, 라이선스 관리는 다음의 사항을 확인해야 함

공개 SW 라이선스는 저작권자의 저작 권리 주장 및 사용 허가를 제공하는 명문화된 형태, 코드 공개 여부와 범위에 따라 분류한다.[45)]

- Permissive 계열 : 사용자에게 광범위한 사용 권한을 부여하는 계열로 저작권 및 라이선스 사용 고지 정도만을 요구
- Copyleft 계열 : Free SW 계열의 라이선스
  1) Weak copyleft 계열 : 수정 부분을 포함한 소스코드 공개 요구
  2) (Strong) copyleft 계열 : 결합된 모든 코드의 소스코드 공개 요구

그림 17 공개 SW 라이선스 분류

45) 추가 정보는 2024년에 발간한 공개 SW 라이선스 가이드(NIPA)를 통해 확인

공개 SW를 활용하여 개발한 SW를 대상으로 필요한 라이선스 관리범위를 다음과 같이 정의할 수 있다.

표 16 공개 SW 라이선스 관리 범위(예시)

구분	주요 내용
형태	① 수정 없이 그대로 사용하는 복제, ② 수정 및 결합
이슈 사항	공개 SW를 사용함으로써 발생하는 사용자의 의무 사항과 관련 있으며, 사용자의 저작권에 해당하는 수정 및 결합 저작물의 경우 이슈가 많이 발생
의무 사항	라이선스 및 결합 형태별로 공개 범위는 다르지만, 소스코드 공개의 의무, 무상 특허 권리 허용의 의무, 사용 및 변경 사용에 대한 고지 필요
고지 방법	저작권과 라이선스 사본 고지
저작권	일반적으로 “copyright”라는 단어를 포함하여 연도와 저작권자 혹은 회사명을 포함하는 문자열로 표현
라이선스	사용한 공개 SW 라이선스를 명시하고 라이선스 사본을 첨부

국내 기업(기관)은 SW에서 SBOM을 생성하고 발견된 공개 SW 저작권에 대하여 빠르게 현황을 확인하여 관련 라이선스 조건에 따라 적절한 조치를 해야 할 필요가 있다.

- 국내 A기업 사례를 보면 공개 SW 라이선스 대응을 위한 전담 부서 외에도 법률 전문가들과 함께 라이선스 대응팀을 운영하고 있음
- 국내 B기관 사례에서는 공개 SW 라이선스 관리를 위한 전담 부서를 두고 자체 개발 SW 및 제3자 협력 개발 SW에 포함된 공개 SW 라이선스 관리를 수행하고 있음

국내 정부·공공기관 및 기업들은 공개 SW 활용 비중이 확대됨에 따라 해외 저작권자들로부터 저작권 소송을 경험하면서 이와 같은 상황에 대응하기 위해 저작권 관리에 활용되던 SBOM을 최근에는 보안취약점 관리에도 활용

참고 1 공개 SW 서체 라이선스 위반 탐지 사례

다음은 SBOM 생성 도구를 활용하여, 공개 SW 서체를 활용하는 컴포넌트의 라이선스 위반 여부를 확인한 사례

- 아래 그림의 SBOM 예시(SPDX 형식)에서 볼 수 있듯이 해당 SW는 “License” 항목에 ‘Non-Commercial-Use-Only-Font-License’의 서체를 사용하고 있음(빨간색 박스 부분)
- (이슈) 첨부된 라이선스의 정책에 따라 탐지된 서체는 개인의 작업 용도로는 사용할 수 있지만, 기업에서 영리 목적으로 판매용 제품에 적용하는 등 활용할 경우, 라이선스 정책 위반으로 향후 소유자가 라이선스 사용 위반에 대한 법적 조치를 요구할 가능성이 있음
- (조치) 영리 기업에서 사용이 가능한 다른 라이선스 종류의 공개 SW 서체로 대체하거나 해당 서체를 구매하여 라이선스 정책을 준수해야 함

```
  "SPDXID" : "SPDXRef-Package-161423",
  "copyrightText" : "NOASSERTION",
  "downloadLocation" : "https://www.kernel.org/pub/linux/kernel/v2.6",
  "filesAnalyzed" : false,
  "homepage" : "https://www.kernel.org",
  "licenseConcluded" : "GPL-2.0",
  "licenseDeclared" : "GPL-2.0",
  "licenseInfoFromFiles" : [ "GPL-2.0" ],
  "name" : "Linux Kernel",
  "originator" : "Organization: \"\"",
  "supplier" : "Person: \"\"",
  "versionInfo" : "2.6"
}, {
  "SPDXID" : "SPDXRef-Package-161422",
  "copyrightText" : "Bite Chalk is free for personal use only. Please, talk with the author for
  "downloadLocation" : "https://www.maisfontes.com/bite-chalk-normal.font",
  "filesAnalyzed" : false,
  "homepage" : "https://www.maisfontes.com/bite-chalk.font",
  "licenseConcluded" : "LicenseRef-Non-Commercial-Use-Only-Font-License",
  "licenseDeclared" : "LicenseRef-Non-Commercial-Use-Only-Font-License",
  "licenseInfoFromFiles" : [ "LicenseRef-Non-Commercial-Use-Only-Font-License" ],
  "name" : "BiteChalk Font",
  "originator" : "Organization: \"\"",
  "supplier" : "Person: \"\"",
  "versionInfo" : ""
} ],
```

그림 18 SBOM 라이선스 탐지 예시(SPDX 포맷)

참고 2 국내 공개 SW 데이터베이스 통합 프로젝트, 오소리(OSORI)[46]

공개 SW(소스코드, 폰트, 데이터베이스 등)는 누구나 자유롭게 복제, 배포, 수정이 가능해 유용하지만, 기업 · 개인 개발자가 공개 SW를 사용할 때 저작권 침해, 특허분쟁, 라이선스 위반 등의 법률적인 문제를 일으킬 위험도 있음

공개 SW는 '공개' 되어 있다는 의미 때문에 '무료' 또는 '마음대로' 쓸 수 있다고 생각하기 쉽지만 '공개 SW' 프로젝트마다 관련 라이선스 등 의무사항이 각각 다르게 설정되어 있음. 이를 인지하지 못했거나 인지하고도 따르지 않는 경우 법적 이슈 발생

- 특히 특허, 법률 등 전문 직원 확보가 어려운 개인, 중소기업 등은 공개 SW 사용 과정에서 공개 SW 라이선스와 관련된 저작권 문제를 겪음
- 공개 SW 컴플라이언스 : 공개 SW 사용 과정에서 발생 가능한 법률적 문제 등을 사전 검증해 리스크를 관리하는 활동을 말함

국내 3社에서도 자체적으로 구축한 공개 SW 라이선스 정보 6만여 건을 공유하고, 데이터에 접근할 수 있는 API를 무료로 제공(2023년)

- 3社는 자사가 보유한 DB 공개를 넘어 타사가 보유하고 있는 DB를 공유하고, 또한 교차 검증을 통해 추가적인 데이터의 신뢰성을 확보함
- 개발한 SW/디지털 서비스 등에 포함될 수 있는 공개 SW 라이선스 정보를 확인하여 관련 조치를 제품 출시 전에 취함으로써 신뢰도를 높이고, 분쟁을 사전에 예방할 수 있음

국내 개인, 중소기업 등도 자유롭게 오소리 프로젝트에 참여함으로써 공개 SW 사용과 관련된 저작권 문제를 사전에 예방할 수 있음

- 홈페이지(osori-db.github.io)에서 사용법을 포함한 가이드 제공
- 공개 SW 라이선스 종합정보시스템(olis.or.kr)에서도 공개 SW 데이터 활용을 지원하고 있음

46) 오소리는 '공개 SW 소리내다'라는 의미를 담고 있으며, 공개 SW 라이선스 정보를 표준화해 공개하고 개인, 기업 등이 무료로 활용할 수 있도록 함으로써 보다 투명하고 신뢰성 있는 공개 SW 생태계 구축에 기여하기 위해 출범

제3절 SBOM 기반 SW 공급망 보안 강화 방안

1. SW 위험관리를 위한 SBOM 기반 확산

SW 공급망은 최초 SW 개발사에서 시작되며, 공개 및 상용 SW 등 다양한 SW 구성요소가 개발·조립되어, SW 공급사 및 최종 고객사로 납품되는 과정을 포함한다.

- 외부 SW 또는 자체 개발 SW는 다양한 공개 SW를 포함할 수 있으며, SBOM 기반 SW 공급망 보안 관리체계를 통해 보안취약점 등 공개 SW 활용에 따른 위험에 대응할 수 있음

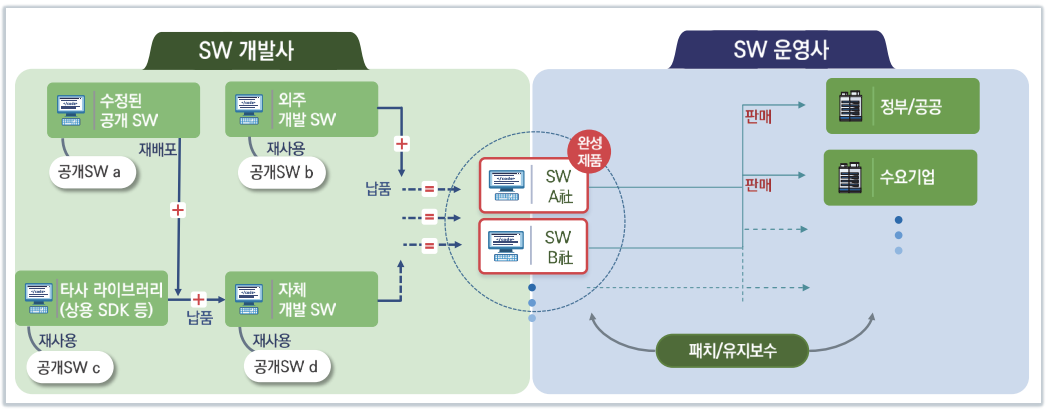


그림 19 SW 공급망과 내·외부 SW 유형 예시

이를 위해서는 [그림 19]의 a~d까지 공개 SW의 각 SW 개발 생명주기 단계마다 SBOM 생성 및 배포 체계를 구축하고, 보안 위험이 해소된 SW를 공급(유통)해야 한다.

- 각 공급망 참여자는 SBOM 공급(유통)을 통해 SW 공급망의 투명성과 신뢰성을 높일 필요성이 있음
- 그러나 모든 SW 구성요소에 대한 SBOM 생성이 어려운 경우, 타사 라이브러리 및 공개 SW 구성요소를 중심으로 작성자 등 출처 정보와 종속성 관계(Dependency Relationship)를 관리하는 체계를 우선 구축함
- SW 개발사 및 공급사는 SW 납품 전에 산업별 SW 공급망 거점의 지원을 받아 신뢰할 수 있는 SBOM을 생성 및 통합하고, 이를 기반으로 공개 SW 라이선스 및 보안취약점 등 SW 위험관리를 시행해야 함

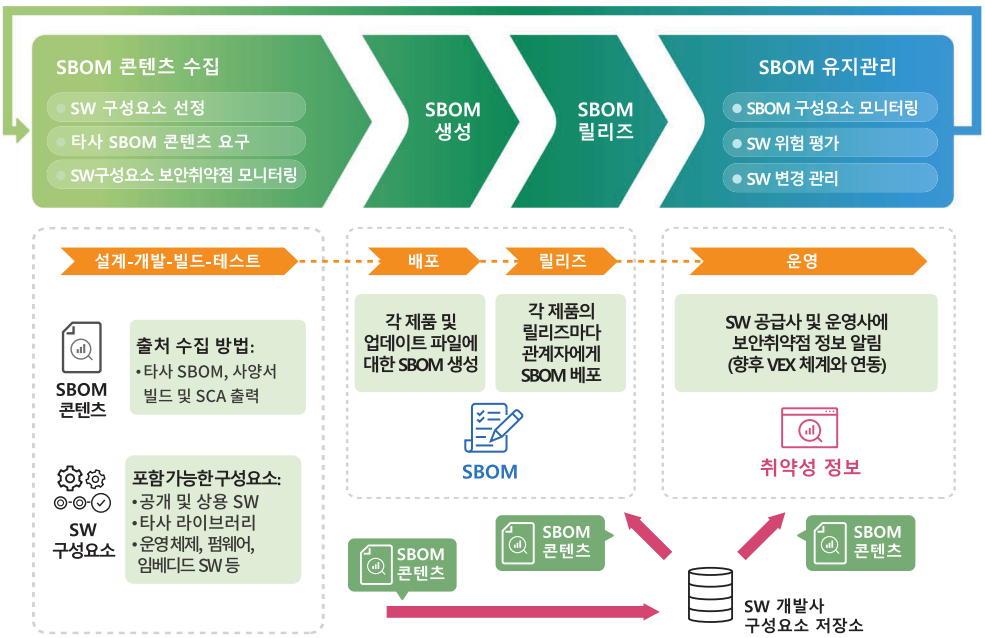


그림 20 SW 공급망과 내·외부 SW 유형 예시

[개발사] SW 개발 생명주기 전반에 걸친 SW 위험관리를 위해 기초 데이터가 되는 SBOM 생성을 위한 필수설비 구축이 필요하다.

- SBOM 도구(공개 SW 및 상용 도구 활용), SW 구성요소 저장소, SBOM 데이터베이스(DB), SW 위험 평가 및 관리를 위한 자체 보안취약점 DB 및 NVD 연계는 SBOM 기반의 SW 공급망 보안을 위한 기초 설비임
- 이와 같은 SBOM 기초 설비를 바탕으로 SW 공급사 및 운영사에 대한 SW 구성요소 자산 파악과 보안패치 등 선제 대응 및 신속한 사후 대응도 가능함

[공급사 및 운영사] 개발사 → 공급사 → 운영사로 이어지는 SW 공급망에 대한 SBOM 공급(유통) 체계를 구축한다.

- 정부·공공기관 및 협단체 등에 '산업별 SW 공급망 거점'을 구축하고 다수의 공급망 생태계에 검증된 정보를 제공하는 것이 이상적인 체계
- 제3자가 SW 개발사의 소스코드를 제공받기는 어려우므로 기업의 지적 재산이 보장되도록 정보를 선별, 최소화된 SBOM을 제공받아 SW 위험관리에 활용함

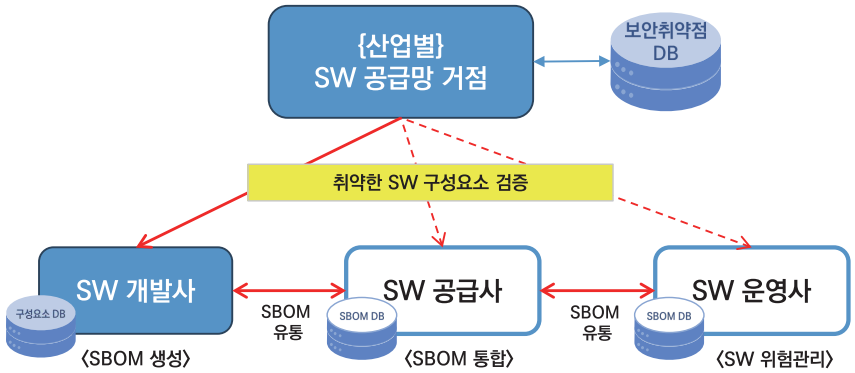


그림 21 산업별 거점을 활용한 SW 위험관리 구성도

[산업별 SW 공급망 거점] SW 개발자, 공급사, 운영사를 포괄하는 산업 생태계는 SBOM 정보를 스스로 공급(유통)하고, 정부는 산업별 SW 공급망에 대한 지원 기능을 수행하는 거점을 구축할 수 있다.

- 산업별 거점의 역할은 새로운 SW 위험 발생 시, 빠르게 조처할 수 있도록 SBOM 공급(유통)을 체계화하고 자동화하는 것이며, 다만 기업 지식재산권에 침해가 발생하지 않도록 산업 생태계에 최소한의 지원 필요
- 또한, SBOM으로 관리할 대상 SW는 우선순위를 두어 하나씩 시행하는 것이 부담을 줄이는 방법으로 자체적으로 개발하지 않은 상용 SDK와 같은 외부 SW부터 먼저 SBOM으로 관리 필요
- 공개 SW 역시 매우 중요한 관리 대상이지만 아직은 고려할 사항이 많아 시장의 자율성에 맡길 필요가 있으며, 정부는 공개 SW의 신뢰성을 높이는 방안을 추가 지원 필요

SW 공급망 거점은 기존의 보안성 점검 위주 시설(기업지원허브, 보안리빙랩, 기술공유실 등)에 정보공유 체계를 추가로 구성하는 발전적 활용이 가능하다.

- 다만, SBOM 정보공유 체계의 구성이 완료된 이후 보안취약점 패치 등 대응은 생태계 참여자의 책임으로 전환 필요

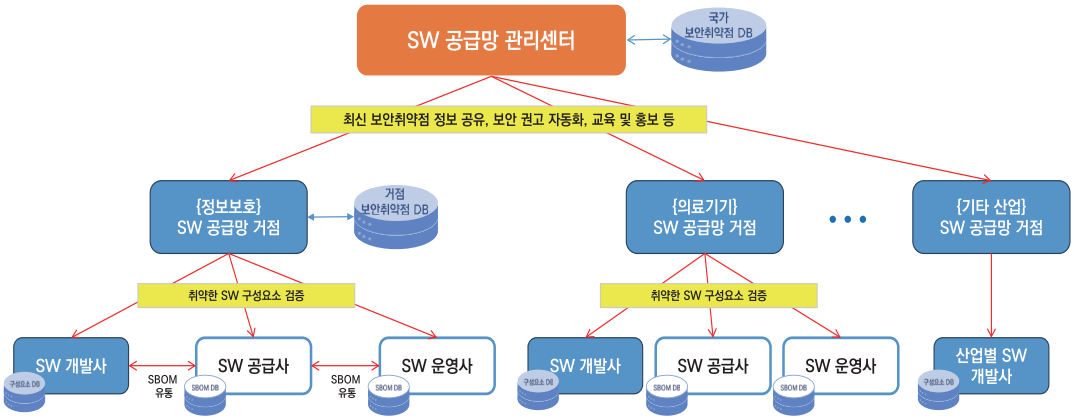


그림 22 SW 공급망 관리센터 체계도

[SW 공급망 관리센터] SW 공급망의 각 단계에서 발생할 수 있는 위험을 사전에 분석하고, 관리하는 상위 추진체계를 구축하여 산업별 공급망 거점에 필수 정보를 공유하는 기능을 부여한다. 거점을 통합하는 관리센터를 통해 체계적인 SW 공급망 위험관리가 가능하며, 이것이 SBOM 기반의 공급망 관리의 미래 비전이자 사이버 복원력 확보의 기초이다.

- SW 공급망 관리센터의 주요 역할은 ① SW 공급망 보안 활동 계획수립, ② 관련 이해관계자와 정보 교류, ③ 교육/홍보 등 정보격차 해소 노력 등이며, 상위 관리센터는 산업별로 여러 곳이 있어도 무방함
- 이러한 자동화된 체계를 지향하는 이유는 더 쉽고 안전하게 보안취약점 및 악성코드 정보를 공유하자는 취지이며, 궁극적으로는 현재 '비정형 문서 형태'인 '보안 권고(Security Advisory)'를 분야별로 체계화하고, 우선순위를 지정하여, 자동으로 대응(패치)하도록 함
- 또한, 공급망 생태계별 SBOM 정보 공급(유통) 체계를 기반으로 향후 '보안 취약성 및 악용 가능성 자동 교환(VEX)[47]' 인텔리전스 체계로 발전이 가능함
- 다만, SW 개발사를 포함하는 각 공급망 생태계와 SW 공급망 거점에 SBOM 기초 설비를 구축하는데 SW 제작 단가 상승 등 비용 증가가 예상되므로 기반 구축 초기 단계에 정부의 지원이 필요함

SBOM 기반 공급망 보안 체계의 활용 기대효과

[소비자 신뢰성 향상] 공급망 내 투명한 자산관리, 라이선스 관리, 보안취약점 관리를 통해 소비자들이 안심하고 활용할 수 있는 기반 제공

[글로벌 무역장벽 대비] 미국, 유럽 등 SBOM 제출을 제도화하는 움직임에 체계적으로 대비하여 국가 신뢰도를 높이며, 해외시장 진출을 위한 기업 경쟁력 강화에 도움

47) VEX : Vulnerability and Exploitability Exchange

참고 의료기기의 사이버보안을 위한 SBOM 원칙과 사례

국제의료기기규제당국자포럼(IMDRF[48])은 의료기기 시판 전 및 시판 후 사이버보안 관리 모범사례와 이해관계자를 위한 여러 권장 활동을 제공한다.

- 의료기기 SW 개발사와 병원 또는 의료 서비스와 같은 공급사 및 고객사 간의 SBOM 체계를 제시한 '의료기기 사이버보안을 위한 SBOM 원칙과 사례' 기술 문서를 발표하였음(2023년 4월)

- SBOM을 활용하면 의료 시스템이 타사 SW 구성요소를 포함하여 발생하는 위험을 관리할 수 있으며, SBOM이 의료기기와 관련된 SW 공급망의 취약점을 빠르게 식별하고 수정하여 악용 가능성을 줄이는 목표에 부합하는 투명한 메커니즘을 제공한다고 강조함

- 특히, 의료기기 SW 개발 생명주기(Lifecycle)에서 SBOM 개발 및 배포, 유지에 대한 고려사항을 포함하고 있으면, SBOM이 SW 생산 비용을 많이 증가시키지 않으면서도 의료 시스템의 공급망과 관련된 모든 이해관계자에 혜택을 줄 수 있는 잠재력이 있다고 평가함

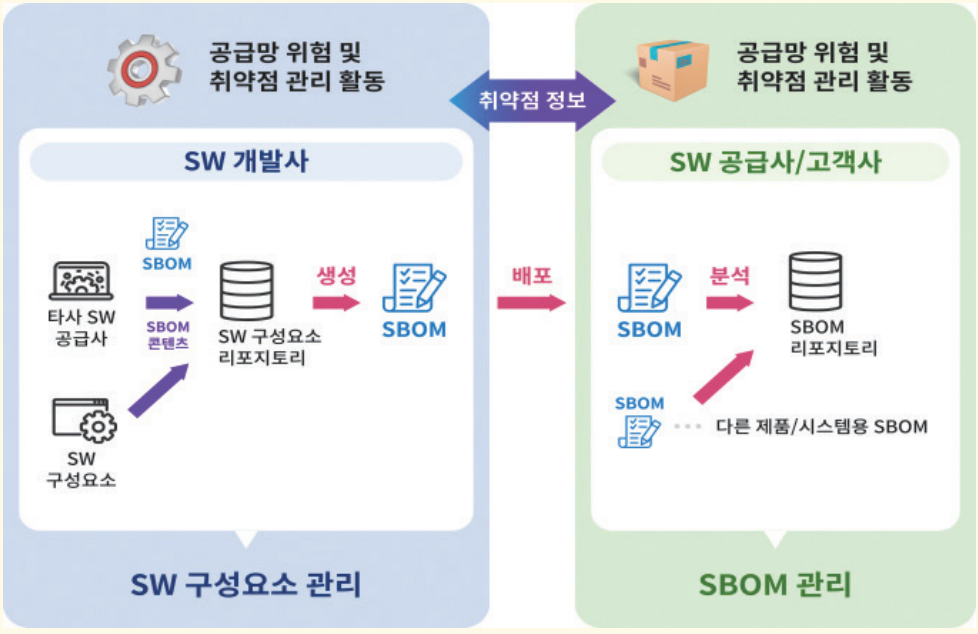


그림 23 SBOM 생성·공급(유통) 체계도

48) IMDRF : International Medical Device Regulators Forum

제3장

SBOM 기반 SW 공급망 보안 실증사례

제3장은 국내 정부·공공기관 및 기업이 SBOM 기반의 SW 공급망 보안 관리체계를 도입할 때 시행착오를 줄이고, 비용 효과적으로 도입할 수 있도록 지원하기 위해 마련되었다.

이를 위해 정부 주도의 전문가 그룹은 정보보호 및 의료 분야 국산 SW 3종에 대해 4종(유료 2종, 무료 2종)의 SBOM 도구를 활용하여 SCA 즉, SBOM을 생성하고 보안취약점 분석·조치 등에 관한 일련의 과정을 정리·제시하였다.

제1절 (SBOM 생성·활용 실증사례) 국산 SW를 대상으로 SBOM을 생성하고, 이를 분석하여 보안취약점을 발견하고, 조치할 수 있도록 하였다. 이 과정에서 SBOM 신뢰성 확보를 위한 유효성 검증 방법과 SW 컴포넌트 관리요령을 도출하였다.

제2절 (SW 공급망 보안 관리체계 점검 실증사례) 공개 SW 보안취약점 탐지·조치 외에도 SW 개발환경의 악성코드 반입 가능성을 확인하는 관리체계 점검은 매우 중요한 SW 공급망 보안 관리요소이다. 이를 통해 기업의 SW 공급망 공격에 대한 사고 발생 위험도를 점검하고, 취약한 항목을 발굴하여 이에 대한 보안대책을 포함한 분석 리포트를 공유하여 기업의 보안수준 제고를 지원하였다.

제3절 (자가 점검용 SW 공급망 단계별 보안 체크리스트) 미국 NIST 문서(NIST 800-161, NIST 800-218)를 참고하여 우리나라 정부·공공기관 및 기업의 실정에 맞도록 공급망 단계별 체크리스트를 마련하였다. SW 공급망 참여자들이 공급망 각 단계에서 보안수준을 스스로 점검할 수 있도록 제공하였다.

제1절 SBOM 생성·활용 실증사례

1. 실증 개요

국산 SW의 SBOM 생성·활용을 통한 SBOM 기반의 SW 공급망 보안 관리 실증을 위해 아래와 같은 계획을 수립하였다.

표 17 실증 추진계획 수립

구 분	주요 내용
실증대상	• 의료, 보안 분야 SW 3종
분석대상	• 소스코드 파일, 바이너리 파일
실증도구	• 개발, 공급(유통)단계 지원 솔루션(1종) • 운영, 유지보수 단계 지원 솔루션(1종) • 무료 SBOM 생성·점검 지원 도구(2종)
실증내용	• SBOM 생성 및 검증 • 보안취약점 탐지·조치 • SW 개발기업 대상 공급망 보안 관리체계 점검 지원

- 체계적인 실증을 위해 먼저 SW 개발기업 및 실증 대상 SW 제품의 환경분석을 실시한 후, 담당자 인터뷰를 통해 기업의 개발환경, 공급망 보안 관리 체계, 대상 SW 제품의 특성 등을 파악하였다.
- 분석대상 SW의 제반 상황을 확인한 후 SBOM 도구를 활용하여 SBOM을 생성하고 유효성을 검증한 후 검증된 SBOM에서 보안취약점 분석 및 대상 기업의 공급망 보안 관리체계를 점검하였다.
- 이를 기반으로 해당 기업의 SW 개발자 인식 및 개발 프로세스 개선 등 공급망 보안 관리체계 향상을 위해 보안 컨설팅도 제공하였다.

본 절에서는 국내 정부·공공기관 및 기업들의 SBOM 도입 활용과정에서 시행착오를 줄일 수 있도록 ① SBOM 생성 과정에서 수행하는 SBOM 유효성 분석, ② SBOM을 활용한 컴포넌트 관리사례, ③ SBOM을 활용한 보안취약점 탐지 및 조치 사례를 제시하였다.

그림 24 SBOM 기반 공급망 보안 관리 실증 절차

2. SBOM 생성 과정에서 SBOM 유효성 검증

유효성 검증의 필요성

① 개발자의 성향에 따라 의도 또는 비의도적 변경 등으로 일부 SW 구성요소의 누락, 오기 등과 같이 부정확한 SBOM 결과가 생성될 수 있다.
* 예시) OPENSSL –〉 OPENSL, SSL 등으로 컴포넌트명을 변경하여 사용

② SW의 소스코드 또는 바이너리 중 어떠한 대상을 분석하는가에 따라 결과가 다르며, 개발언어에 따라 추출한 SBOM 결과가 다를 수 있고, 이는 SBOM 도구 구입(도입) 시 필수 고려사항이다.

③ SW 개발과정에서 환경적 요인(개발/구축 시 등)에 따라 개발자도 모르는 새로운 SW 구성요소가 발견될 수 있다.

자동화된 도구를 이용해 SBOM을 생성하면 SBOM 항목 일부가 누락되거나 중복되는 현상이 발생한다. 이 단계에서 생성된 SBOM의 정보가 정확한지 검토하는 '유효성 검증' 절차가 필요하다.

SBOM 유효성 검증은 정확하고 신뢰성이 높은 SBOM을 SW 공급망 내에서 원활하게 공급(유통)하고 관리하기 위한 절차이다. 검증 과정에서 SW 개발자의 참여는 필수적이며, 각 기관 및 기업들은 이를 참고·활용할 수 있다.

사례 데이터 누락·중복 수정 사례 – 기업 A

실증 기업 A의 SW를 대상으로 생성한 SBOM 신뢰성 향상을 위해 확인 작업을 실시하였다. SBOM 생성 시, 아래 [표 18]과 같이 SBOM 각 항목들 중 데이터가 누락되는 등 신뢰성이 낮은 것을 알 수 있다.

또한, 생성된 SBOM에서 공개 SW의 하나인[49]내 commons-io[50]공급자, 라이선스명 등에 대한 정보가 누락되었으며, 같은 컴포넌트 내용이 중복해서 포함된 것도 확인할 수 있었다.

49) apache-commons apache-commons: Apache SW 재단의 프로젝트로써, 재사용 가능한 자바 기반의 컴포넌트를 모아놓은 통합 프로젝트

50) commons-io: apache-commons 내 하위 프로젝트로써, 파일 복사, 삭제 또는 데이터 읽기/쓰기와 같은 파일 및 디렉토리 작업 관련 기능을 제공

표 18 SBOM 유효성 검증 단계에서 데이터 누락·중복 사례

컴포넌트 (Component Name)	버전 (Component Version)	공급자 (Supplier Name)	라이선스명·버전 (License Name·Version)
commons-io	1.3.2	정보누락	정보누락
commons-io	2.2		
commons-io: commons-io	2.2		Apache-2.0
commons-io: commons-io	2.1		Apache-2.0
commons-io: commons-io	1.3.2		Apache-2.0
commons-io: commons-io	1.3		Apache-2.0

발견된 오류를 수정하기 위해 commons-io에 대한 정보를 검색하여, 누락 정보인 공급자, 라이선스 정보를 확인하였고, 동일 버전의 중복 출력 내용을 삭제하여 아래와 같이 SBOM 정보를 수정하였다.

표 19 SBOM 데이터를 수정·보완한 사례

컴포넌트 (Component Name)	버전 (Component Version)	공급자 (Supplier Name)	라이선스명·버전 (License Name·Version)
commons-io	1.3.2	apache	Apache-2.0
commons-io	1.3	apache	Apache-2.0
commons-io	2.1	apache	Apache-2.0
commons-io	2.2	apache	Apache-2.0

SBOM 유효성 검증 요령

❶ (개발자 확인) 기업의 개발자와 함께 SW 제품 개발에 대한 상세 현황 정보와* 추출한 SBOM 데이터를 비교하여 오탐 또는 과탐 여부 등을 검토

* 제품정보 : 기업명, 서비스명, 개발언어, 패키지 형태, 개발 프레임워크, 공개 SW, 상용 SW, 빌드시스템, 형상관리시스템 등

❷ (완전성 확인) CycloneDX, SPDX 등 SBOM 표준에서 정한 기본항목 누락 여부 및 항목별 내용이 표준 요구 내용과 일치하는지 확인

3. SBOM 도구를 활용한 컴포넌트 관리사례

SW 공급망의 개발, 공급(유통), 운영단계별로 SBOM을 관리할 수 있으며, 본 실증에서는 ①개발단계에 해당되는 소스코드, ②공급(유통)단계에 해당하는 설치 파일 바이너리를 대상으로 SBOM을 생성 및 보안취약점 분석을 진행하였다.

SW 개발기업은 활용하는 공개 SW 또는 제3자 개발 SW의 컴포넌트를 정확히 관리하고 있어야 SW 자산관리, 라이선스 관리, 보안취약점 관리를 할 수 있다. 그러나 실증을 통해서 참여 기업들은 사용하는 컴포넌트들의 출처 및 사용이력 등을 체계적으로 관리하지 못하는 것으로 확인되었다.

특히, 대상 SW의 SBOM 분석 결과, 개발자가 인지하지 못한 공개 SW 컴포넌트가 식별되었으며, SW 설치 후 대상 SW와 연결되는 라이브러리에 포함된 공개 SW 컴포넌트도 추가로 발견할 수 있었다.

또한, 실증을 통해 SBOM 분석 방식(소스코드 또는 바이너리) 및 사용 도구 종류에 따라 SBOM 정보가 서로 일치하지 않을 수 있음을 확인하였다. 먼저, 소스코드 분석 방식과 바이너리 분석 방식은 SBOM 정보가 많이 상이함을 확인할 수 있었다. 따라서 SBOM의 신뢰도 향상을 위해 2개 이상의 도구를 이용한 교차 검증이 필요할 수 있다.

사례 소스코드, 바이너리 기반 SBOM 생성 비교 사례 – 기업 A

실증 기업 A의 SW 소스코드와 바이너리를 대상으로 SBOM 도구를 활용하여 SBOM을 생성하고 비교하였다. 소스코드 분석을 통한 SBOM 생성 결과, 약 1700~1800여 개의 컴포넌트가 식별되었으며 도구 간 차이가 적었다. 설치 전 바이너리 파일 분석을 통한 SBOM 생성 결과는 소스코드 기반 SBOM보다 숫자도 적었고, 도구 간 차이가 매우 큰 것을 확인하였다.

소스코드 분석 결과가 바이너리 분석 결과보다 더 많은 컴포넌트를 발견한 이유는 소스코드 분석 시 소스파일, 헤더파일, 그리고 소스코드에 연결이 명시된 라이브러리 및 공개 SW 등 소스코드 개발단계에서 많은 컴포넌트를 식별할 수 있기 때문인 것으로 판단된다.

컴포넌트 이름	컴포넌트 별칭	컴포넌트 버전	컴포넌트 개발자 이름	컴포넌트 해쉬
zstd		1.3.4-lp151.2.3		48490d67e486e092dbf2b68021ad7fea57
zstandard		1.5.5		065ed5dcc0716e5379e56f2e24017e18054
zookeeper		3.6.3	apache	ac44de96d37a80d463c1e01aaa2ea86b19
zookeeper		3.4.14	apache	6f463ade2b777f81e6c3e145b3fc03d4b39
zlib		1.2.13	gnu	606d1a61f2914869a827c0d6abafcf5feb40
zlib		1.2.11	gnu	9b5b171f5d54054782b6f166d96c248c012
zjsonpatch	zjsonpatch	0.2.3		ae4e5e931646a25cb09b55186de4f3346e3
xz-java	xz-java	1.9		211b306cfc44f8f96df3a0a3ddaf75ba8c52
websocket-common	websocket-common	9.4.11.v20180605		9377a68071137ae5f5c8cdc2ed20d6f904a
websocket-api	websocket-api	9.4.11.v20180605		9377a68071137ae5f5c8cdc2ed20d6f904a
univocity-parsers	univocity-parsers	2.9.1		31685122d5e392e98672ed6009a95a4c16
transaction-api	jta	1.1		b8ec163b4a47bad16f9a0b7d03c3210c6b
tink		1.7.0		8faf92d116a0ba138ee4e99a7418e985897
threeten-extra	threeten-extra	1.5.0		9bbcbe09a631320bdc3325bbb04c930684
super-csv	super-csv	2.2.0		bf743e0c1f1c42d19df236d82fa0b34128c0
stream	stream	2.9.6	xwp	d61aebbea8a08148c3aca6b03464495a4b
stax2-api	stax2-api	4.2.1		9377a68071137ae5f5c8cdc2ed20d6f904a
st4	ST4	4.0.4		17cc49dc535a0fbe58c3a8634e774572bec
spark		3.5.0	apache	b7687d4b2ae696b1d5f2c462af795c3ebae
spark		3.4.1	apache	061ec29d4eefc08ea0b8edac8ed6cec9978
snakeyaml	snakeyaml	2.0		880c9d896e4b74a06c549c15ca496450165
slf4j-api	slf4j-api	2.0.7		5d6298b93a1905c32cda6478808ac14c2d4
servlet-api	servlet-api	4.0.2		6d93010ca93301383c5ca960d55611a5c91
scopt-2.12	scopt_2.12	3.7.1		41c77bfc41a9492a9aa0760fa873cf992895
scala-xml	scala-xml	1.0.3-3		d9a6df43cfac692f05e7166d39aae4476a24
scala-reflect	scala-reflect	2.12.8		d6a24e175246541ffcbc965a231aa1d3bb0
scala-library	scala-library	2.13.12		fb68864a0248af0979d45921869eb1230b5
scala-library	scala-library	2.12.18		e51e6636c003359e106bea4ad99def70e61
scala-compiler	scala-compiler	2.13.12		b4c417591851cc8f98521d1c5f6e012e5d8
scala-compiler	scala-compiler	2.12.18		e64b8e321cb0d45471be40ce0069e223b2
scala		2.12.8	jetbrains	d8a8ed1e20a29d4d9a42c984a0b6d74f87

그림 25 SBOM 기반 공급망 보안 관리 실증 절차

바이너리 분석의 경우, 기업별로 바이너리에 사용된 공개 SW를 분석하는 기술과 데이터베이스가 크게 다르므로 도구 간 큰 격차를 보이는 것으로 판단된다. 이를 통해 한 종류의 도구에 의존하기보다 2종 이상의 도구를 사용하여 그 결과를 교차 비교하는 것이 보다 정확하게 SW 구성요소를 파악할 수 있을 것으로 보인다.

표 20 SW 제품 형태별 SBOM 생성 후 컴포넌트 수 비교 – 기업 A

도구 종류	소스코드 분석	도구 종류	바이너리 분석
A 도구	1,862	A 도구	141
B 도구	1,747	B 도구	924
C 도구	1,834	D 도구	453
		E 도구	186

※ 도구 A, B는 소스코드와 바이너리 모두 분석 가능, C, D, E는 소스코드 또는 바이너리 분석 전용 도구

컴포넌트 관리 요령

❶ SW를 개발·공급(유통)하는 과정에서 변경·수정되는 SW 제품에 대한 SBOM을 지속 공유해야만, 누락 없는 컴포넌트 관리가 가능하다.

❷ 개발자(기업)가 인지하지 못한 공개 SW 컴포넌트와 SW를 설치 후 생성되는 공개 SW 컴포넌트를 추가하여 관리하여야 한다.

❸ 소스코드, 바이너리, 의존성을 종합적으로 분석한 SBOM을 관리해야만, 신뢰성 높은 보안취약점, 라이선스, SW 자산관리를 할 수 있다.

4. SBOM을 활용한 보안취약점 탐지 및 조치

SW의 빠른 보안취약점 탐지 및 조치를 위해서는 SBOM 생성을 통한 컴포넌트 관리가 매우 필요하다. 다만, 대상 SW의 소스코드 또는 바이너리(SW 설치파일, SW 바이너리) 분석, 도구별 생성된 SBOM의 컴포넌트의 내용이 다를 수 있고, 그에 따라 보안취약점 탐지 결과도 상이할 수 있음을 주지해야 한다.

즉, SBOM에 포함된 컴포넌트의 버전 정보 또는 명칭 오류로 보안취약점 정보 매칭에 오류가 발생할 수 있으므로, SBOM 유효성 검증을 통해 SBOM의 신뢰성을 높이는 것이 효과적인 보안취약점 관리를 위해 필요한 사항이다.

사례 **SBOM 기반 SW 공급망 보안취약점 관리 실증사례 – 기업 A**

실증 기업 A의 SW 소스코드와 바이너리를 대상으로 SBOM을 생성하고, 이를 보안취약점 DB와 비교하여 보안취약점을 검출하였다. [그림 26]과 같이 CycloneDX 표준을 이용하는 SBOM에서는 'Vulnerabilities' 항목에서 보안취약점 정보 확인이 가능하다.


```
"vulnerablilities": [
    {
      "id": "CVE-2022-42003",
      "source" : {
        "name" : "NVD",
        "url" : "https://nvd.nist.gov/vuln/detail/CVE-2022-42003"
      }
    },
    {
      "id": "CVE-2021-20190",
      "source" : {
        "name" : "NVD",
        "url" : "https://nvd.nist.gov/vuln/detail/CVE-2021-20190"
      }
    },
    {
      "id": "CVE-2019-20330",
      "source" : {
        "name" : "NVD",
        "url" : "https://nvd.nist.gov/vuln/detail/CVE-2019-20330"
      }
    },
    {
      "id": "CVE-2019-17531",
      "source" : {
        "name" : "NVD",
        "url" : "https://nvd.nist.gov/vuln/detail/CVE-2019-17531"
      }
    },
    {
      "id": "CVE-2018-7489",
      "source" : {
        "name" : "NVD",
        "url" : "https://nvd.nist.gov/vuln/detail/CVE-2018-7489"
      }
    }
]
```


그림 26 SBOM을 활용한 보안취약점 탐지(예시)

발견된 보안취약점에 대한 더 자세한 정보 및 조치 수단은 미국 NIST의 보안취약점 데이터베이스(NVD)에서 확인할 수 있으며 검색 경로는 https://nvd. nist.gov/vuln/detail/(CVE 코드명)이다. [그림 27]

SBOM 도구에 따라 CVE-ID, 보안취약점 출처(보안취약점 소스명, URL), 조치방안 등 보안취약점의 상세 항목이 다르게 표현되므로 지속적인 활용을 통한 경험을 축적하는 것이 필요하다.

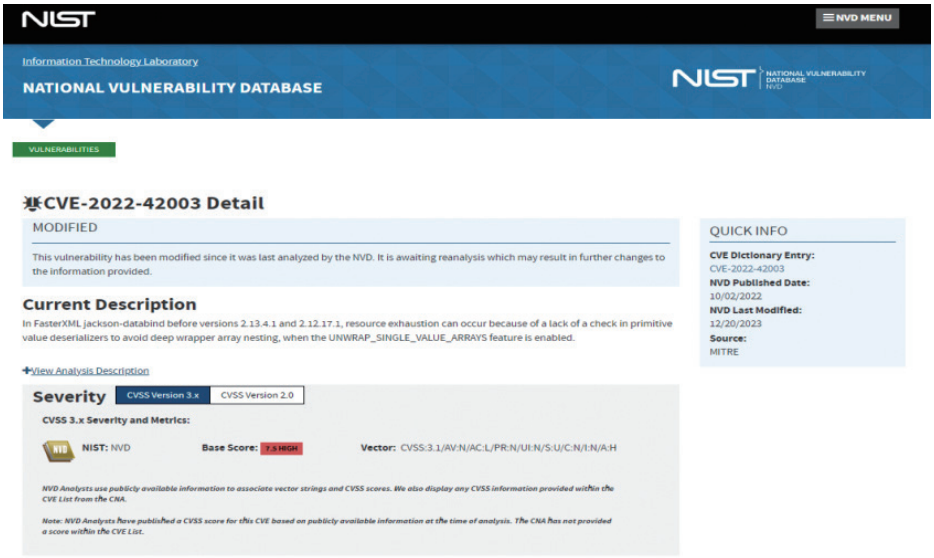


그림 27 보안취약점 데이터베이스 검색 결과(예시)

또한, 각 기관 및 기업들은 CVSS 점수 외에도 기업 내부 상황, 고객의 관련 SW 운영 현황 등 여러 상황을 종합 고려하여 조치 방안을 강구하는 것이 바람직하다.

SBOM 기반의 SW 공급망 보안 관리 요령

❶ 대상 SW 개발언어의 호환성, 도구의 분석 알고리즘, 기업의 공급망 특성 등을 꼼꼼하게 확인하여 SBOM의 신뢰성을 높일 수 있는 적합한 SBOM 도구 선정

❷ 소스코드 또는 바이너리 분석 방식 선택은 기업의 환경에 맞게 하되, 2개 이상의 도구를 상호 보완적으로 활용하는 것을 권장(상용 SBOM 도구 외에도 무료 도구 선택 可)

❸ 설계–개발–공급(유통)–도입 및 운영–유지보수 등 공급망 각 단계별로 SBOM을 생성·공급(유통)할 수 있는 관리체계를 구축할 것을 권고

❹ 보안취약점 탐지 성능을 높이기 위해 SBOM DB 구축, NVD(NIST의 보안취약점 데이터베이스) 등과 연동 체계구축 필요

❺ 보안취약점 탐지 시, 신속하게 개발자(부서, 기업 등)에 전파하여 조치계획을 수립하고, 고객(운영)사에도 적의 조치할 수 있는 체계 구축 필요

제2절 SW·공급망 보안 관리체계 점검 실증사례

공개 SW 보안취약점 탐지·조치 외에도 공급망 공격의 주요 목표가 되었던 개발환경, 악성코드 반입 가능성을 확인하는 관리체계 점검 등을 수행하였다. 이를 통해 대상 기업의 SW 공급망 공격에 대한 사고 발생 위험도를 점검하고, 취약한 항목을 발굴하여 이에 대한 보안대책을 포함한 분석 리포트를 공유하였다.

SW 공급망 보안 관리체계 점검을 위해 미국의 관련 가이드 참조 및 자체 항목 개발을 통해 5가지 분야, 54개 세부항목으로 구성된 SW 공급망 보안 점검 항목을 도출하여 기업의 실제 개발 현장에 적용하여 보았다.

표 21 SW 공급망 보안 점검 실증 항목 일부

보안 요구 분야	점검 항목(예)
안전한 제품 관리 (12개)	• 정기적인 SW 보안 교육 여부 • 모의해킹, 보안취약점 진단 등 보안을 위한 활동 여부
보안코드 개발 (13개)	• 빌드 관리 및 보안성 검토 수행 여부 • 빌드단계에서의 보안요구사항 확인 여부
타사 구성요소 확인 (7개)	• 공개 SW, 상용 SW의 보안요구사항 확인 여부 • 취약성, 라이선스 만료 확인 여부
개발환경 보안 (16개)	• 빌드 환경에 대한 공격 표면 조사 및 위협 모델링 수행 여부 • 개발환경에 대한 접근제어, 인터넷 차단 등 조치 수행 여부
보안코드 전달 (6개)	• 패키지 바이너리의 전자서명 생성 여부 • 계약 명기 시, SBOM 전달 여부

현장 점검을 통해서 대상 중소기업은 SW 공급망 보안관리에 대한 인식이 부족한 것을 확인하였다. 다만, 공급망보안 포럼 전문가 자문을 통해 국내 상당수의 대기업들은 SW의 투명성과 안전성을 확보하기 위해 SBOM 기반의 SW 공급망 보안관리 체계 구축·운영 중인 것을 확인할 수 있었다.

일부 기업들은 SW 개발 모든 단계에서 보안 테스트를 통합 지원하는[51] DevSecOps 도입도 검토 중이나, 보안취약점 관리보다 라이선스 관리에 중심을 두는 경우가 대부분이었다.

51) DevSecOps는 보안이 포함된 개발환경

사례 SW 공급망 보안 관리체계 점검 실증사례 – 기업 A

A기업의 SW 공급망 단계 중 개발기업에 요구되는 관리체계를 점검하고 담당자 인터뷰를 통해 공급망 보안 상태를 점검하였다. SW 공급망 보안 점검 요구사항 54개를 확인한 결과, 양호 24개, 부분 양호 16개, 취약 12개로 분석되었다. 특히, 보안 코드 개발과 개발환경 보안에서 취약 항목이 많았으며, 모든 분야에서 공급망 보안에 대한 보완이 시급함을 알 수 있다. [표 22].

표 22 SW 공급망 보안 점검 상세 결과

보안 요구사항	전체 항목	Y(양호)	P(부분양호)	N(취약)	N/A
안전한 제품 관리	12	5	6	1	0
보안 코드 개발	13	4	5	4	0
타사 구성요소 확인	7	5	1	1	0
개발환경 보안	16	7	3	4	2
보안 코드 전달	6	3	1	2	0
합계	54	24	16	12	2

표 23 SW 공급망 보안 점검 결과 미흡 사례

보안 요구사항	주요 내용
안전한 제품 관리	· 웹 보안취약점만 수행됨 · 모의침투, 소스코드 진단 등 추가적인 보안취약점 진단 필요
보안 코드 개발	· 보안성 검토 미수행으로 서비스 위주의 SW 개발을 수행
타사 구성요소 확인	· 관리자의 허가 없이 출처가 불분명한 공개 SW 무단 사용 · 서비스 계약이 종료된 SW 제품의 사용(보안 업데이트 미수행)
개발환경 보안	· 외부에서 개발한 단말기에 접속하여 개발(빌드)업무를 수행 · 악성코드 감염 USB를 백신검사 없이 개발 단말기에 무단 사용
보안 코드 전달	· 안전이 확인되지 않은 SW의 업데이트 파일 배포 · SW 제품에 대한 무결성 검증 미수행

SW 공급망 보안 관리체계 점검 실증 시사점

- 국내 중소기업들의 SBOM 기반 SW 공급망 보안 관리체계 구축이 아직 미흡한 상황임을 인식
- SW 개발(공급) 기업 중심의 개발·공급 생태계에 대한 SBOM 기반 SW 공급망 보안 관리체계 단계적 지원 필요
- 특히, 공급망 보안 수준 향상을 위해 SW 공급망 보안 점검 항목을 이용하여 개발 전 분야(안전한 제품 관리, 보안 코드 개발, 타사 구성요소 확인, 개발환경 보안, 보안 코드 전달)에 대해 지속 점검 지원 필요

제3절 자가 점검용 SW 공급망 단계별 체크리스트

실증 추진 과정에서 SW 공급망 보안 점검 실증 항목을 이용하여 기업의 공급망 보안 수준을 체계적으로 점검할 수 있었다. 하지만 항목의 수가 다소 많고 관련 기업들이 스스로 수행하기 어려운 항목들이 있어, 이 항목들을 정제하였다. 또한, 앞서 소개된 미국 공급망 보안 지침인 NIST SP 800-161(Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations) 및 NIST SP 800-218(Secure Software Development Framework) 등을 참조하여 국내 기업의 개발환경에서 효율적으로 적용할 수 있는 공급망 단계별 체크리스트를 마련하였다.

이 체크리스트는 SW 제품의 개발단계부터 운영단계까지 SW 제품 이해관계자(개발사, 공급(유통)사, 고객(운영)사 모두가 공급망 각 단계에서 공급망 보안 상태를 스스로 확인하는 점검 도구로 작성하였으므로, 이해관계자의 역할과 공급망 단계에 따라 선택적으로 활용할 수 있다.

- 개발사 : 개발자 공급망 보안 업무 지시, 개발환경 보안 자체 점검 등으로 활용
- 공급(유통)사 : 개발사 공급망 보안 준비도 점검, 고객(운영)사에 제품의 공급망 수준 입증 근거로 활용
- 고객(운영)사 : 도입 전 공급망 보안을 고려한 제품 개발 및 공급(유통) 여부에 대한 확인, SW 도입 후 공급망 관리에 활용

자가점검 항목은 공급망 보안 단계별로 설계, 개발, 공급(유통) 및 도입, 유지보수 단계로 이루어진다.

표 24 공급망 보안 단계별 체크리스트(안)

단계	연번	점검 항목	세부 설명
설계 단계	1	안전한 개발과 관련하여 조직 내 역할 및 책임을 명시하는가?	사내 공지 및 발령 내용에 역할 및 책임 명시
	2	SW 제품, 서비스 개발자 및 관련자에게 보안 교육을 하는가?	교육 자료에 보안교육 (공급망 보안, 시큐어 코딩 등) 확인
	3	개발단계에서 공급망 보안을 고려하였는가?	형상관리 시스템, SBOM 생성 및 관리
	4	개발환경의 보안상태를 관리하는가?	개발환경, 엔드포인트의 운영체제, 백신 업데이트 현황
	5	제품의 주요 보안항목을 식별하고 문서로 보관하는가?	주요 보안항목(데이터 보호 수준, 암호화, 인증, 인가, 접근 통제 등) 명세 확인
개발 단계	6	SW의 보안취약점 최소화를 위해서 시큐어코딩을 준수하는가?	소스코드 개발 또는 빌드 시 시큐어코딩 확인
	7	배포 전 기본 설정을 검토하였는가?	개발도구 내에 보안 설정 기능 제공 시 배포 전 기본 설정을 검토

단계	연번	점검 항목	세부 설명
개발 단계	8	외부 라이브러리를 도입할 때, 보안성을 확인하는가?	외부 라이브러리 검사(유해성, 무결성 등)
	9	내부 저장소에는 인가된 사용자만 접근하는가?	내부 저장소(소스코드 형상관리 시스템 등)에 접근통제 확인
개발 단계	10	내부 저장소에 저장된 공개 SW 및 내부 개발 소스코드의 보안취약점을 지속적으로 점검하는가?	SW의 보안취약점 확인(로그 등)
	11	빌드 과정에서 자동화된 보안 테스트를 수행하는가?	빌드 환경에 자동화 보안 테스트 포함 여부 확인
	12	컴파일러, 인터프리터의 사용 시 보안 옵션을 사용하는가?	빌드 옵션에 보안 기능 활성화 여부 확인
	13	빌드 후 결과물을 보관하는가?	빌드 관련 결과물(실행파일, 컴파일 로그, SBOM, 보안 테스트 결과물 등) 검토
	14	SBOM에 적시된 컴포넌트의 보안취약점을 확인하는가?	SBOM 결과 점검 시 컴포넌트의 보안취약점 식별
	15	SBOM을 통해 식별된 심각한 보안취약점에 대한 검증과정이 있는가?	CVSS 7.0 이상 높은 등급의 보안취약점을 가진 컴포넌트에 대한 경로 확인 등 유효성 검증
	16	SBOM 작성 이력은 일정 기간 보관하는가?	SBOM 생성 이력 검토
공급 (유통) 단계	17	SW의 무결성을 확인할 수 있는 데이터를 전달하는가?	코드서명, 해시값 등 전달 여부
	18	배포 SW 생성에 사용된 소스코드, 라이브러리, 공개 SW 정보를 안전하게 보관하는가?	소스코드, 라이브러리 등 안전하게 보관
	19	필요시, 공급(유통)사는 고객(운영)사에 SBOM, 보안취약점, 라이선스, 제재 정보 등을 제공하는가?	SBOM 활용
도입 및 운영 단계	20	SW 제품 도입에 대한 공급망 보안 요구사항 및 관리에 대한 매뉴얼이 있는가?	매뉴얼에 SBOM 제공, 보안취약점 제거 및 완화 및 업데이트 제공, 외주업체 보안 요구사항 등 검토
	21	도입 계약 체결 시, 보안 요구사항 이행을 확인하는가?	보안 요구사항 이행 여부 확인
	22	제품 도입 시, SW의 코드서명 또는 해시값으로 무결성을 확인하는가?	코드서명 및 해시값 검증
	23	CVE 등 주요 보안취약점 공개 시 해당 보안취약점 포함한 SW가 있는지 모니터링하는가?	알려진 보안취약점에 대한 확인

단계	연번	점검 항목	세부 설명
도입 및 운영 단계	24	심각한 보안취약점 발견 시, 공급(유통)사 또는 개발사에 보안취약점 처리 요구를 하는가?	보안취약점 조치를 위한 절차 점검 여부 확인
	25	외부 개발사를 통해 도입된 SW인 경우, SBOM을 제공 받는가?	SBOM 검토
	26	외부 개발사를 통해 도입된 SW인 경우, 소스코드에 대해 취약요인을 점검하는가?	외부 개발 소스코드에 대한 보안취약점 점검
유지 보수 단계	27	운영 SW에 대한 보안취약점 점검을 지속적으로 실시하는가?	보안취약점 점검결과 검토
	28	보안취약점 식별 시, 보안취약점 평가 및 대응 방안을 가지고 있는가?	보안취약점 평가 및 대응 방안 검토
	29	신속한 보안취약점 패치를 위한 효율적인 절차를 수행하였는가?	패치 적용 절차 확인
	30	배포/업데이트 서버 운영 시 서버에 대한 보안관리를 수행하는가?	배포/업데이트 서버에 적용된 보안정책 (인증, 인가, 접근통제 등) 검토

제4장

SBOM 기반 SW 공급망 보안 활성화 지원

제4장은 SBOM 기반 공급망 보안 활성화를 위한 정부 지원 및 전문가 활동을 중심으로 기술하였다. SW 공급망 보안 각 단계에서 활용할 수 있는 SBOM의 유용성에도 불구하고, 국내 중소기업들이 빠른 시일 내에 SBOM 기반의 SW 공급망 보안 관리체계를 도입(운영)하기에는 전문 인력 및 관리체계 구축을 위한 예산 부족 등으로 어려움을 겪을 수 있는 점을 감안하여 중소기업들이 효과적으로 이용할 수 있는 기업지원 시설과 국내에서 제정되었거나 제안된 SBOM 표준을 제시하였다.

제1절 (SW 보안취약점 점검 지원 테스트베드) 기업지원허브(판교)에서는 가전, 금융, 스마트도시, 의료 등의 다양한 분야에서 활용되는 SW의 보안취약점 탐지 및 조치 등을 위해 SBOM 기반 SW 공급망 보안 관리체계를 포함한 다양한 보안취약점 점검 도구의 활용을 지원하고, 견학 및 교육 프로그램도 운영하고 있다. 디지털헬스케어 보안리빙랩(원주)에서는 SW 의료기기를 포함한 다양한 디지털헬스케어 의료기기에 대한 보안취약점 점검을 지원하고 있고, 국가사이버안보협력센터 기술공유실(판교)에서는 공급망보안 테스트베드 구축하고 시범 운영을 통해 SBOM 기반의 SW 공급망 보안취약점 점검 지원 및 관련 기술을 공유 중이다.

제2절 (SW 공급망 보안을 위한 SBOM 개발) 국내 민간 표준화 기관인 정보통신기술협회(TTA)를 통해서 정보통신 단체표준으로 SBOM 표준이 제정되어 있으며, 국가 표준 SBOM도 제정·등록되어 있다. 또한 국가정보원에서도 보안취약점 분석 및 관리 등에 특화된 NIS-SBOM을 마련하여 제시하였다.

제3절 (SBOM 기반 SW 공급망 보안 발전 제언) 공급망 각 단계가 연계되는 SBOM 기반 SW 공급망 보안 관리체계 확산을 통해 SW 공급망 보안을 강화하고, 기업도 자체적인 투자 노력을 통해 기업의 신뢰성을 확보할 수 있도록 노력할 필요가 있다. 또한 정부는 안전한 환경에서 SBOM을 유통할 수 있도록 연구개발 지원 등의 노력이 필요하다.

제1절 SW 보안취약점 점검 지원 테스트베드

1. 기업지원허브(판교)

모바일, 사물인터넷(IoT, Internet of Things) 기기, 클라우드 등 디지털 기술이 국민의 일상생활과 다양한 산업분야로 융·복합 확산되고 있다. 특히, 아파트 월패드, 도어락, 전기검침, 자동제어 등 IoT 기기들은 국민의 일상생활 깊숙이 자리 잡아가고 있다.

그러나 국민들과 산업계에서는 생활주변과 산업환경에서 사이버보안 위협을 정확하게 인식하고 있지 못하며, 막연한 불안감을 갖고 있는 것이 현실이다.

따라서 정부는 이와 같은 일반 국민들과 중소기업들의 애로사항을 해결하기 위하여 2015년 10월에 기업지원허브를 개소하고, 사이버보안 위협 시연 및 보안취약점 점검, 견학·교육 프로그램 등을 지원하고 있다.

가. 사이버보안 위협 시연

그림 28 기업지원허브 IoT 기기 사이버보안 위협 시연시설

정부는 기업지원허브 방문자들을 대상으로 국민들이 일상생활 및 산업 환경에서 일어날 수 있는 사이버위협을 체감할 수 있도록 시연함으로써 사이버위협을 제대로 인식할 수 있도록 지원하고 있다.

또한, 디지털기술의 융·복합 확산 동향에 맞춰서 시연환경도 연차별로 확대 및 개선 해나가고 있다. 홈·에너지('15년), 교통('16년), 의료('17년), 안전·재난·환경('18년), 건설('19년) 분야 시연환경, 홈 리빙랩('20년) 구축, 테스트베드 VR('21년), 메타버스('22년) 제작 및 드론·의료 시연환경 개선('23) 등 현재 6종의 사이버보안 위협 시연시설을 갖추고 있다.

나. 보안취약점 점검 지원

디지털 제품/서비스가 홈, 의료, 교통 등 다양한 융합 분야로 확산됨에 따라 다양한 디지털 제품·서비스의 보안 내재화를 위해 중소기업 등이 디지털 제품/서비스의 보안수준을 자체 검증하고 보완할 수 있는 환경을 제공하고 있다.

교통, 의료, 안전·재난·환경, 건설, 홈리빙랩, 드론 등 다양한 분야의 디지털제품 및 서비스의 소스코드, 펌웨어, 통신 프로토콜 등의 보안취약점 점검도구를 사용하여 보안취약점을 점검하고 조치할 수 있도록 지원하고 있다.

특히, SW 개발, 공급(유통), 운영, 폐기 등의 공급망 전 단계에 대한 사이버보안 위협이 강화되고 있어서 2024년부터 소스코드 분석 방식과 바이너리 분석 방식의 SBOM 생성·분석 도구를 도입하여 기업들이 디지털 제품 및 서비스 개발단계에서부터 보안성을 내재화할 수 있도록 지원하고 있다.

표 25 SBOM 생성 도구 현황 및 주요 특징(요약)

① 소스코드 분석 방식	② 바이너리 분석 방식
• SW 컴포넌트를 분석하여 공개 SW 라이선스 및 알려진 보안취약점 등 탐지 – (보안위협 탐지) 컴포넌트별 보안취약점 결과(보안취약점 정보 식별자, 위험점수, 개선상태, CWE, 보안취약점 완화 가능여부 등) 확인, 개선 및 수정 방법 안내 – (라이선스 탐지) 2,700개 이상의 공개 SW 라이선스 종류 검출 및 파일, 파일일부, 디렉토리 구조, 패키지 매니저 등 다양한 정보 분석, 라이선스 정책에 따른 위험도 분류 – (SBOM 생성) SPDX, CycloneDX 포맷 생성	• 정적·동적 분석엔진을 통해 바이너리 코드만으로 보안위험 탐지 – (보안위협 탐지) 메모리 손상, 메모리 참조, 네트워크 보안취약점, 기능 오용 등 알려지지 않은 중대한 보안취약점, 제로데이 보안취약점 탐지 및 포괄적 보안취약점 DB를 활용하여 알려진 보안취약점 탐지 – (라이선스 탐지) 공개 SW 라이선스 정보(라이선스 이름, 패키지 이름, 패키지 버전, 라이선스 구분, 라이선스 텍스트 정보 등) 제공 – (SBOM 생성) SPDX, CycloneDX 포맷 생성

다. 견학·교육 프로그램 운영

사이버보안 위협 시연 및 보안취약점 점검지원 외에도 학생, 일반인 등을 대상으로 디지털 제품 및 서비스 보안 점검도구 활용, 디지털 제품 및 서비스 보안 실습 교육 및 보안 테스트베드 견학 프로그램도 운영하고 있으며 연간 2,000여 명이 이용하고 있다.

표 26 연도별 기업지원허브(IoT 테스트베드) 이용 현황

	'16년	'17년	'18년	'19년	'20년	'21년	'22년	'23년	누적
횟수	164	370	402	404	457	568	512	447	2,877
이용자	224	1,455	1,789	2,135	1,432	2,132	2,284	2,246	11,451

이용절차 및 연락처

- **(신청서)** KISA 누리집(kisa.or.kr) – 공지사항 또는 정보보호산업진흥포털 – IoT 보안 – 공지사항에서 IoT 보안 테스트베드 이용 신청서를 다운로드
- **(소재지)** 경기도 성남시 수정구 대왕판교로 815 기업지원허브 4층 정보보호 클러스터 490호
- **(이용절차)** 이용 신청서 작성 → 신청서 제출 → 일정협의 → IoT보안 테스트베드 방문 → 테스트 점검 결과 검토 및 컨설팅

  ※ 이메일(iottestbed@kisa.or.kr) 신청

2. 디지털헬스케어 보안 리빙랩(원주)

의료분야에도 병원정보시스템부터 각종 진단·진료 및 치료기기에 SW가 내장되거나 SW 의료기기가 널리 확산되고 있다. 의료기기에 포함될 수 있는 SW 보안취약점은 기기 오작동, 민감정보 유출 등으로 이어질 수 있어서 더욱 중요하게 다루어져야 한다.

디지털헬스케어 보안리빙랩은 디지털헬스 기기 등에서 발생할 수 있는 사이버보안 위협 시연, 디지털헬스케어 기기·서비스에 대한 보안성을 테스트하고 다양한 사이버 위협에 대응하기 위해 구축한 시설로 2020년 12월에 개소하였다.

가. 사이버보안 위협 시연

일반인, 기업인, 의료인 등 다양한 분야의 종사자들이 디지털헬스케어 기기에 대한 사이버위협을 체감할 수 있도록 지원하는 시설로 구체적으로는 ① 환자 의료정보 모니터링 시스템 데이터 변조, ② 영상정보처리시스템(X-ray 등) 데이터 변조, ③ 개인의료장비(심박기, 약물주입기) 트래픽 변조를 통한 오작동 유도, ④ 네트워크(통신 구간 미암호화) 보안취약점을 통한 병원 모니터링 시스템 변조 등의 사이버 위협 시연 서비스를 제공하고 있다.

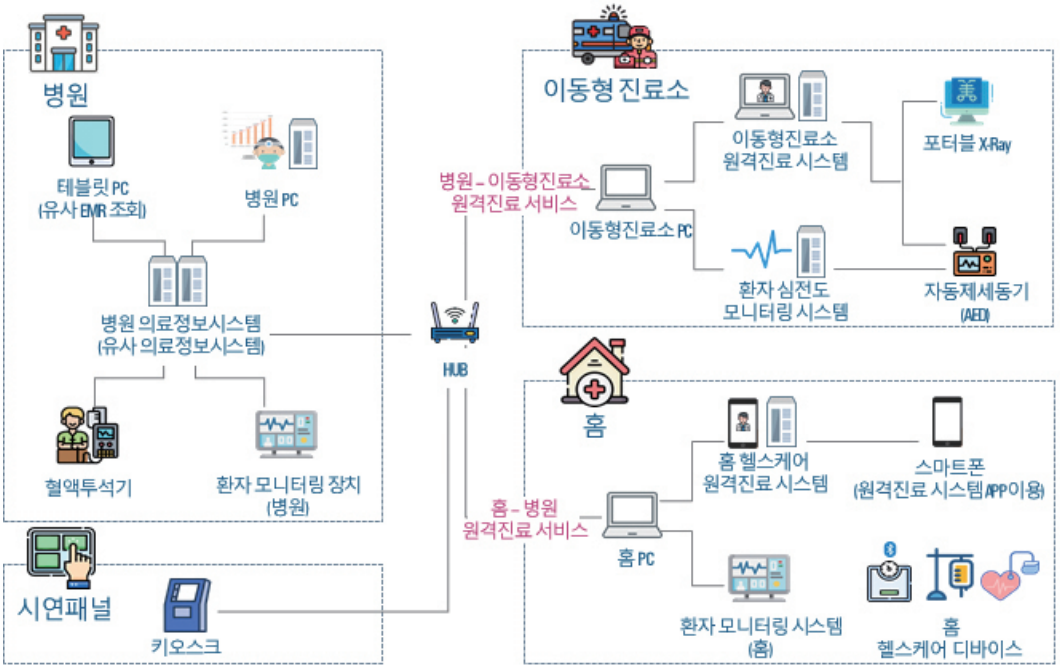


그림 29 디지털헬스케어 보안리빙랩 구성도

그림 30 디지털헬스케어 보안리빙랩 현장

나. 보안취약점 점검 지원

각종 디지털헬스케어기기에 대한 네트워크 보안취약점 점검, 소스코드 보안취약점 점검 등을 지원하고 있으며 2024년 상반기 부터 SBOM 생성 도구를 도입하여 디지털헬스케어기기의 SBOM 생성 및 보안취약점 조치를 지원해 나갈 계획이다.

표 27 보안취약점 점검도구 현황

도구명	주요특징
SBOM 도구	소스코드 분석 방식, SBOM 생성 및 보안취약점 분석
침투 테스트 도구	네트워크 프로토콜 보안취약점 점검
APP Security 도구	소스코드 보안취약점 점검 분석
보안취약점 분석 도구	네트워크 및 펌웨어 보안취약점 점검 분석

구체적인 사이버보안 시험항목은 디지털헬스케어 기기의 펌웨어 추출 및 수정 등 안정성, 메모리 보안취약점 점검, 네트워크 프로토콜, CVE 보안취약점, 무선통신 패킷 보안취약점 등의 네트워크 보안취약점 점검을 지원하고, 의료정보시스템의 경우 비인가 접근통제, 설정파일 및 기기 연동 보안취약점 점검을 지원하고 있다.

다. 의료기기 인허가 지원

우리나라 식약처 또한 SW가 포함된 의료기기 인·허가 시 사이버보안 적합성을 평가하고 있다. 디지털헬스케어 보안리빙랩에서 보안취약점 조치 확인서를 받아서 의료기기 인·허가시 첨부할 경우 사이버보안 시험항목은 기준을 만족한 것으로 갈음하고 있어서 디지털헬스케어 기업들에게 큰 도움이 되고 있다.

- 디지털헬스케어기기 인허가 지원은 관련 기관과 협의를 통해 연 8~9건을 선정하여 지원
- **(홍보)** 식약처, 원주의료기기테크노밸리, 강원테크노파크 등과 협력을 통해 보안취약점 점검 및 컨설팅 지원 사업 홍보 추진
  ※ 유관기관과의 협력을 통한 홍보와 보안취약점 점검 수행 사업자의 자체 설문조사[52]를 병행하여 보안취약점 점검 대상 수요조사 실시
- **(선정)** 보안모델 적용 · 실증 가능여부를 고려하여 점검 대상 업체를 목록화하고 유관기관 및 디지털헬스케어 보안협의체와 논의를 통해 선정
- **(검증)** 보안취약점 점검 및 컨설팅 결과를 토대로 디지털헬스케어 보안협의체에서 내용을 검토하고, 미흡 항목 보완

이용절차 및 연락처

- **(신청서)** KISA 누리집(kisa.or.kr)–사업소개 – 디지털산업본부(융합보안 산업 활성화 지원)–디지털헬스케어 보안강화 지원(신청서)
- **(이용절차)** 이용 신청서 작성 → 신청서 제출 → 일정협의 → 보안리빙랩 방문 후 테스트 → 테스트 점검 결과 검토 및 컨설팅
  ※ 이메일(cslivinglab@kisa.or.kr) 신청

52) 국내 디지털헬스케어 산업 실태조사(산업통상부) 기반 설문조사 대상 표본 추출

3. 국가사이버안보협력센터 기술공유실(판교)

국가정보원은 공급망 보안, 클라우드, 제로트러스트 등 급격하게 발전하는 ICT 기술의 안전성을 선제적으로 확인하고, IT 보안업체·시험기관에게 고가(高價)·신기술 융합제품에 대한 안전성 평가를 지원하기 위해 국가사이버안보협력센터내에 기술공유실을 2022년 11월 개소하였다.

기술공유실은 정부·공공기관에 도입되는 IT보안제품의 안전성을 검증하기 위하여 정부·공공기관의 네트워크 환경을 그대로 모사한 시험환경을 갖추고 있으며 실환경에서 발생될 수 있는 기능 오류, 보안취약점 등을 식별 · 분석을 할 수 있다.

가. 공급망 보안 테스트베드

Log4j·3CX 등 공급망 공격이 지속 발생함에 따라 SW 공급망 보안 강화를 위해 ❶ SBOM 생성 자동화 ❷ SBOM 관리 ❸ SW 보안취약점 추적·관리 등을 실증할 수 있는 테스트베드의 필요성이 대두되었다. 이에, 국가정보원은 정부·공공기관에 도입되는 SW 제품의 투명성 및 신뢰성을 확인하고 보안취약점을 식별·추적할 수 있는 SBOM 기반 공급망 보안 관리 체계를 실증할 수 있는 테스트베드를 기술공유실에 구축하였다.

표 28 분석 도구 지원 사양

	A	B	C
소스코드 지원언어	C, C++, C#, Go, Java, JavaScript, Kotlin, Python	Java, JavaScript, PHP, ASP.NET, Ruby, Swift, C/C++, Object-C, Python	C, C++, C#, Clojure, Erlang, Go, Groovy, Java, JavaScript, Kotlin, Node.js, Objective-C, Perl, Python, PHP, R, Ruby, Scala, Swift, .NET
바이너리 지원포맷	실행 파일 압축파일 설치파일 펌웨어 파일 디스크 이미지	실행파일 압축파일 패키지 매니저	실행파일 압축파일 설치파일 펌웨어 파일 디스크 이미지 패키지 매니저

기술공유실 공급망 보안 테스트베드에는 국내외 상용 SW 분석 도구(SCA) 3종이 선별 적용되었으며 각 분석 도구가 지원하는 소스코드 및 바이너리 포맷은 [표 28]과 같다. 분석 도구를 활용하여 SBOM을 생성하고 유효성을 검증하였다. 이를 통해 분석 도구의 주요 특징을 도출할 수 있었으며 신뢰성 높은 SBOM 생성 도구의 조건 네 가지를 식별할 수 있었다.

표 29 분석 도구 주요 특징

	주요 특징
A 도구	• 분석 대상 파일을 입력하면 대상 파일에서 문자열, 함수 또는 변수 이름과 같은 요소(Finger Print)를 추출
	• 공개 SW 데이터베이스를 구축하고 추출된 구성요소와 비교하여 공개 SW를 식별
B 도구	• 실행 파일 내 컴포넌트와 해당하는 해시값을 추출하고 공개 SW 데이터베이스를 구축하여 해시값을 비교하여 식별
	• 소스코드 내에 공개 SW의 소스코드 파일이 존재할 시 이를 구축된 데이터베이스와 비교하여 일치하는 공개 SW를 식별
	• 특정 언어에서 공개 SW에 필수로 사용되는 헤더파일이 있는 경우 이를 비교하여 공개 SW를 식별
C 도구	• 분석 대상 파일을 입력하면 폴더 및 파일 단위로 필요한 구성요소를 해시값으로 추출
	• 소스 일부분을 복사하여 사용할 경우, 소스 일부분 단위로 해시값을 추출하여 구축된 데이터베이스와 비교하여 공개 SW를 식별
	• 공개 SW 데이터베이스를 구축하여 추출된 구성요소 해시값과 비교하여 공개 SW를 식별

신뢰성 높은 SBOM 생성 도구의 조건

❶ 소스코드 및 바이너리 데이터 분석 가능

❷ 분석 결과에 대한 유효성 검증 가능(컴포넌트 해시, 경로 등 제공)

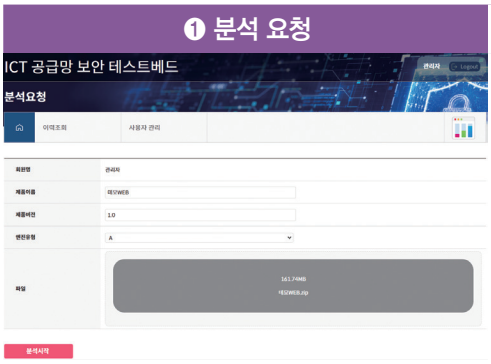
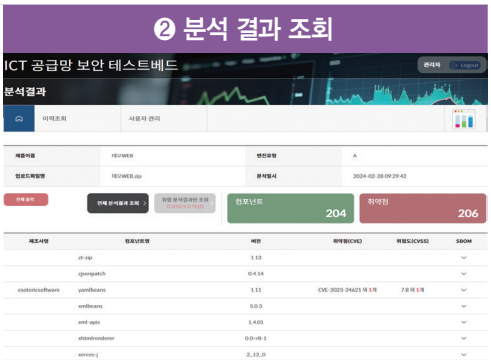
❸ 보안취약점 정보와 연동

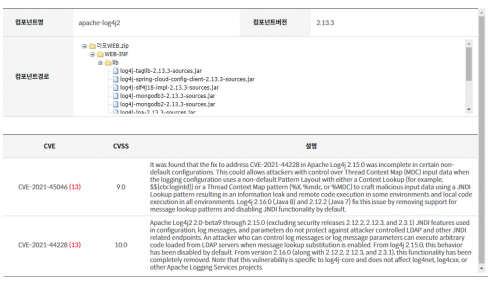
❹ 대용량 리포지토리 및 빠른 검색결과 제공

나. 테스트베드를 활용한 SBOM 출력

기술공유실에 구축된 공급망 보안 테스트베드는 사용자가 쉽게 활용할 수 있도록 개발하였으며 주요 동작 방식은 [표 30]과 같다.

표 30 SBOM 기반 공급망 보안 테스트베드 주요 동작 방식

❶ 분석 요청	❷ 분석 결과 조회
	
분석을 하고자 하는 SW를 선택하여 업로드	분석이 완료되면 완료된 결과를 컴포넌트 기준으로 보안취약점 정보 출력

❸ 보안취약점 정보 조회	❹ 문서출력
	
검출된 보안취약점을 클릭하면 파일명, CVE ID, CVSS, 보안취약점 설명 등 보안취약점 정보를 확인	PDF, 한글, 엑셀, JSON 형태로 다운로드 받아 출력. 엑셀에서 전체 컴포넌트 목록을 출력함

테스트베드에 검증대상 SW 제품의 소스코드 혹은 바이너리를 입력하면 자동으로 SBOM을 생성하고 보안취약점 등 주요 정보를 출력한다. 그리고 생성된 SBOM은 데이터베이스에 저장되어 해당 SW 제품의 보안취약점을 추적·관리하기 위해 활용할 수 있다.

다. 테스트베드를 활용한 보안취약점 탐지 및 패치 사례

기술공유실 테스트베드를 활용하여 국내외 펌웨어·운영 SW·웹소스·설치파일 등 4개 분야 10개 SW 제품을 대상으로 SBOM을 생성하고 SW 컴포넌트에 대한 분석을 수행하였다.

구 분	분석 대상
보안취약점 점검 제품군	• 펌웨어 : 네트워크장비 2대, CCTV 1대 • 운영 SW : 관측장비 1대 • 웹소스 : 웹애플리케이션 2개 • 설치파일 : 정보보호제품 4개

실증결과 10개의 제품 중 7개의 제품에서 CVSS 9.0 이상의 중대 보안취약점이 발견되었으며, 3개 제품에서는 중대 보안취약점이 발견되지 않았다. 중대 보안취약점이 발견되지 않은 3개의 제품 중 CCTV는 펌웨어 자체가 암호화되어 SBOM 출력 결과를 얻을 수 없었으며, 나머지 2개는 CVSS 9.0 미만의 보안취약점이 일부 확인되었다.

SBOM 분석 결과, 데이터베이스, 개발 프레임워크, 환경설정, 실행파일 배포 등 다양한 종류의 컴포넌트에서 보안취약점이 발견되었으며, 심각한 보안취약점은 원격코드실행(RCE), 명령어삽입(Command Injection), DB 명령어삽입(SQL Injection) 등이 확인되었다. 분석 결과 요약은 [표 31]과 같다.

공급망 보안 테스트베드를 활용하여 펌웨어, 운영 SW, 웹소스, 설치파일 등 대부분의 SW를 대상으로 SBOM을 출력할 수 있었고, 이를 통해 SW 제품의 보안취약점 점검이 가능한 것을 확인할 수 있었다. 이 과정에서 원격코드실행, 명령어삽입, DB 명령어삽입, 버퍼 오버플로우 등 즉시 공격 가능한 13개 중대 보안취약점을 확인하고 개발사에 통보하여 패치 완료하였다.

본 테스트베드를 통해 SBOM 기반 공급망 보안 관리체계가 사이버보안 위험 관리 및 대응역량 강화에 매우 중요한 역할을 할 수 있으며 이를 통해 사이버안보에 크게 기여할 수 있음을 확인하였다.

표 31 공급망 보안 테스트베드 활용 분석 결과

제품	컴포넌트	용도	보안취약점 (CVE)	위험도 (CVSS)
A	imagemagick v6.8.2	이미지 편집	CVE-2023-34152 (원격코드 실행)	9.8
	XStream v1.4.15	XML 변환	CVE-2021-21351 (원격코드 실행)	9.1
	libtiff v4.0.3	이미지 편집	CVE-2015-8668 (서비스거부 공격)	9.8
	Qt 5.3.2	개발 프레임워크	CVE-2017-10904 (원격공격)	9.8
B	OpenSSL v1.0.2k	암호화 통신	CVE-2022-2068 (명령어 삽입)	9.8
C	busybox v1.21.1	실행파일 배포	CVE-2018-1000517 (버퍼오버플로우)	9.8
D	Mybatis v3.2.1	데이터베이스	CVE-2023-25330 (DB명령어 삽입)	9.8
	OpenLDAP v2.4	디렉토리서비스	CVE-2022-29155 (SQL 삽입)	9.8
	spring-framework v3.2.8	웹개발 프레임워크	CVE-2022-22965 (원격코드 실행)	9.8
E	h2 v1.4.192	데이터베이스	CVE-2022-23221 (원격코드 실행)	9.8
	jackson-databind	XML 파서	CVE-2019-17531 (원격코드 삽입·실행)	9.8
F	Log4j v1.2	로그 관리	CVE-2022-23305 (SQL 삽입)	9.8
	thymeleaf v3.0.12	화면구성	CVE-2021-43466 (원격코드 실행)	9.8

라. 발전 계획

기술공유실 공급망 보안 테스트베드는 SBOM 생성 및 보안취약점 점검을 수행할 수 있도록 구축되었다. 신뢰할 수 있는 SW 공급망 보안 관리 체계를 구축하기 위해서 신규 보안취약점 공개시 개발사·공급사·운영사 간 SW의 보안취약점 정보를 실시간으로 전파·공유할 수 있는 공급망 보안 통합관리체계가 필요하다. 이에, 국가정보원은 산·학·연 전문가들과 SW 공급망 보안 통합관리 체계를 구축 방안을 지속적으로 논의하면서 각 방안들을 실증할 수 있는 테스트베드로 발전시켜 나갈 계획이다.

표 32 SW 공급망 보안 관리 체계 시나리오

주체	주체별 주요기능
개발사	❶ 개발사는 개발하는 SW 대상 SBOM을 생성하고 통합관리 시스템에 등록 ❷ 신규 보안취약점이 공개되면 개발사 SBOM 통합관리 시스템에 등록된 SW 대상 보안취약점을 자동으로 진단 ❸ 보안취약 SW 식별 시 공급사·운영사에 위기 상황을 전파, 보안조치를 지원
공급사	❶ 개발사로부터 도입, 운영사에 공급하는 SW 대상 SBOM을 생성 통합관리 시스템에 등록 ❷ 신규 보안취약점이 공개되면 공급사 SBOM 통합관리 시스템에 등록된 SW 대상 보안취약점을 자동으로 진단 ❸ 보안취약 SW 식별 시 개발사·운영사에 위기 상황을 전파, 보안조치를 지원
운영사	❶ 공급사로부터 도입한 SW 대상 SBOM을 생성 통합관리 시스템에 등록 ❷ 신규 보안취약점이 공개되면 운영사 SBOM 통합관리 시스템에 등록된 SW 대상 보안취약점을 자동으로 진단 ❸ 보안취약 SW 식별 시 공급사에 보안조치를 요청
보안 취약점 관리기관	❶ 전 세계에서 공개되는 보안취약점을 실시간으로 수집하고 통합관리 ❷ 신규 보안취약점이 식별되면 관할 내 개발사·공급사·운영사에게 보안권고 등 위협정보를 자동으로 전파 · 공유하고 보안조치 현황을 취합

국가정보원은 기술공유실 공급망 보안 테스트베드를 공급망 보안 통합관리 체계로 확장 발전시키고 실증을 통해 SW 공급망의 발생 가능한 위험요소를 분석하고, SW 공급망 위기대응 체계를 마련해 나갈 것이다.

제2절 SW 공급망 보안을 위한 SBOM 개발

1. 국내 SBOM 표준 사례

국제적으로 잘 알려진 SBOM 형식으로는 SPDX, CycloneDX, SWID가 있다. 리눅스재단에서 개발한 SPDX는 공개 SW 라이선스 관리 및 SW 패키지 정보 공유에 중점을 두고 있고, OWASP(The Open Worldwide Application Security Project)에서 개발한 CycloneDX는 사이버 위험 감소를 위한 공급망 관리를 위해 만들어졌으며 보안취약점 정보 공유 등 확장성을 제공한다. ISO/IEC 표준화 그룹에 의해 개발된 SWID는 IT 자산 관리를 위해 SW 식별 및 관리에 사용될 수 있다.

국내 산업계에서도 SBOM 도입·활용을 위해 산·학·연 전문가들이 협력하여 표준화를 진행하였고, 정보통신기술협회(TTA)와 국립전파연구원에 각각 단체표준과 국가표준이 제정되어 있다. SBOM 단체표준(TTAK.KO-11.0182)은 SPDX v2.0 일부를 참조하여 국내 실정에 맞게 적용할 수 있도록 개선한 것으로 공개 SW 정보 교환 명세(Open Source Software Package Data Exchange Specification)에 중점을 두었고, 국가 표준(KS X ISO/IEC 19770-2)은 SWID(ISO/IEC 19770-2)를 한글 표준으로 도입한 것으로 분석된다. 다만, SW 보안취약점 관리에 SWID가 널리 활용되지 않고 있다는 점은 주지할 필요가 있다.

표 33 SBOM 관련 국내외 표준 현황

구 분	개발기구	국제표준	국내표준	
			국가표준	단체표준
SPDX	리눅스재단	ISO/IEC5962 ('21)	-	TTAK.KO-11.0182('15) ※ SPDX v2.0 일부 참조
CycloneDX	OWASP	-	-	-
SWID	ISO/IEC 19770-2 ('09제정,'15개정)		KS X ISO/IEC 19770-2('21)	-

현재는 2022년 12월에 제정된 "공개 SW 공급망 관리를 위한 SW 목록 구성(SBOM) 속성 규격"(TTAK.KO-11.0309)에 이르고 있으며, 이 표준에서는 15개의 SBOM 구성요소를 정의하고 있다.

SBOM 구성요소는 SBOM 표준 제정 당시 SBOM 활용 목적, 분야 등을 유추할 수 있는 좋은 정보를 포함하고 있다. [표 34]는 정보통신 단체표준의 SBOM 구성요소를 설명한다. 구성요소 중 CVE 항목은 SW 보안취약점 관리에 직접 활용할 수 있는 정보로 우리나라 SBOM 정보통신 단체표준도 SW 보안취약점 관리에 활용할 수 있음을 알 수 있다.

표 34 정보통신 단체표준 SBOM 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 라이선스 결합 형태(License Usage)	Dynamic/Satic 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

또한 상기 표준 제정을 추진한 기술위원회는 2023년 12월 추가적으로 “공개 SW SBOM 거버넌스 관리 지침”(TTAK.KO-11.0322)을 정보통신단체표준으로 제정하였다. 이 표준은 SW 공급망 관리를 목적으로 SBOM 환경분석, SBOM 관리포맷 정의, 자동화 지원 SBOM 생성을 위한 관리정책, R&R, 관리 프로세스 구축 및 주요 수행 내용을 정의하고 있다.

이와 같이 국내에서도 SBOM 활용을 위한 다양한 표준화 노력이 있었다는 것을 확인할 수 있었고, 향후 자동차, 방위산업 등 다양한 산업 분야에 특화된 SBOM 표준화 활동이 기대된다.

2. 국가정보원 제안 SBOM 기본항목

가. SBOM 기본항목 제안

미국, 유럽 등 주요국은 SW에 포함된 보안취약점을 추적·관리하기 위해 정부·공공기관에 도입되는 SW 대상 SBOM 제출을 의무화하는 제도를 추진하는 등 공급망 보안을 강화 중이다. 미국의 경우, NTIA(전기통신정보청)에서 선정한 7개 항목을 SBOM의 기본항목으로 권고하였으며 사이버보안 체계를 강화를 위해서 항목 추가도 가능하다.

국내에서도 공개 SW 관리 및 보안취약점 식별을 위한 SBOM 생성·활용에 대한 관심이 증가하고 있으나, 현재 국제적으로 통용되고 있는 SBOM 데이터 교환 표맷(CyclonceDX, SPDX)은 항목이 지나치게 많거나 보안취약점 정보 등을 제공하지 않고, NTIA 데이터 필드의 기본항목은 너무 적어 구성요소에 대한 충분한 정보를 제공하지 못하는 단점이 존재한다. 정보통신단체표준 SBOM 속성 규격 또한 실증 과정에서 다소 부족한 부분이 있어, 정부·공공기관에 도입되는 SW의 관리를 위해 공통으로 활용할 수 SBOM 기본항목 선정을 추진하게 되었다.

본 절에서는 정부·공공기관에 도입되는 SW의 공급망 보안 관리 체계를 구축하기 위해 국가정보원이 제안하는 SBOM(NIS-SBOM) 기본항목을 소개한다. NIS-SBOM 기본항목은 ❶기본항목 간소화 ❷보안취약점 정보연동 ❸사이버 위험관리 효율성 향상을 주요 목표하였다.

NIS-SBOM 기본항목은 NTIA의 권고안, 국내외 표준 등을 분석하여 선정하였고, 추가적으로 7개 항목을 자체 선정하여 총 20개 항목으로 구성하였다. 보안취약점 정보는 CVE, KEV, CVSS를 연동하여 사용하며, 보안취약점 관리는 SW 제품별로 하고, 보안취약점은 제품내 구성요소 단위로 식별된다. 또한, 테이블 형태의 표준 출력 양식을 지원하여 PDF, 한글, 엑셀 등 보고서 형태에서 작업하는 사용자의 편의성을 향상시켰다.

국내 SBOM 개발업체 및 유관 부처를 대상으로 NIS-SBOM 설명회를 개최하고 의견을 수렴하였으며 앞 절에서 소개한 협력센터 기술공유실 테스트베드에 NIS-SBOM 기본항목을 적용하여 정부·공공기관 도입 SW의 공급망 보안 관리 체계 구축 시 활용 가능한지 실증을 수행하였다.

나. NIS-SBOM 기본항목

표 35 NIS-SBOM 기본항목 (* : 자체 선정)

구분	속성
① SBOM Standard*	NIS / SPDX / CycloneDX / TTA 등 SBOM 표준
② SBOM Type*	개발 / 유통 등 SBOM 생성단계
③ CycloneDXNo.	CycloneDX번호
④ SPDX Doc. ID	SPDX 문서번호
⑤ SBOM ID*	SBOM 문서번호
⑥ Product Name*	제품 이름
⑦ Product Version*	제품 버전
⑧ Component Name	컴포넌트 이름
⑨ Component Alias*	컴포넌트 별칭
⑩ Component Version	컴포넌트 버전
⑪ Component Supplier Name	컴포넌트 공급자 이름
⑫ Component Hash	컴포넌트 해시(SHA-256 이상 사용)
⑬ Component Path*	컴포넌트 경로(컴포넌트 실제 위치 식별)
⑭ SBOM Author Name	SBOM 작성자
⑮ Unique Identifier	컴포넌트 버전 외에 조회가 가능한 고유 식별자 (CPE, PURL 등)
⑯ Dependency Relationship	상위 컴포넌트와의 종속 관계
⑰ Timestamp	SBOM 생성일시
⑱ License Name·Version	라이선스 이름·버전
⑲ Vul. DB	NVD(CVE), CISA(KEV) 등 보안취약점 DB
⑳ Vul. Info	CVE 식별자 및 CVSS 보안취약점 등급

① SBOM Standard(SBOM 표준)

– SBOM 표준의 종류로 NIS 1.0, CycloneDX 1.6 등과 같이 표기

② SBOM Type(SBOM 생성단계)

– Design, Source, Build, Analyzed, Deployed, Runtime 등 SBOM이 생성된 단계 표기

③ CycloneDXNo.(CycloneDX번호)

– CycloneDX SBOM을 사용하는 경우 해당 CycloneDX번호를 표기

④ SPDX Doc. ID(SPDX 문서번호)

– SPDX SBOM을 사용하는 경우 해당 SPDX 문서번호를 표기

⑤ SBOM ID(SBOM 문서번호)

– SBOM 문서의 고유 식별자로, 기업명–생성년월일–일련번호(6자리)로 표기

⑥ Product Name(제품 이름)

– SBOM 생성 대상 제품의 이름 표기

⑦ Product Version(제품 버전)

– SBOM 생성 대상 제품의 버전 표기

⑧ Component Name(컴포넌트 이름)

– SW 구성요소인 컴포넌트의 이름 표기

* CycloneDX는 Component, SPDX는 Package로 SW 구성요소 표기

⑨ Component Alias(컴포넌트 별칭)

– 보안취약점을 식별하기 위한 최소 구성요소인 컴포넌트의 별칭 표기, 컴포넌트 이름이 중복되는 경우 Alias로 구분하기 위함

⑩ Component Version(컴포넌트 버전)

– 보안취약점을 식별하기 위한 최소 구성요소인 컴포넌트의 버전 표기

⑪ Component Supplier Name(컴포넌트 공급자 이름)

– 컴포넌트를 개발한 개발자 이름을 표기

⑫ Component Hash(컴포넌트 해시)

– 식별된 컴포넌트가 정확한지 검증을 위하여 사용, SHA–256 이상 안정성이 확보된 해시를 이용하여 표기

⑬ Component Path(컴포넌트 경로)

– 식별된 컴포넌트가 정확한지 검증을 위하여 사용, 컴포넌트의 정확한 위치를 확인하여 검증

⑭ SBOM Author Name(SBOM 작성자)

– SBOM을 작성한 작성자의 이름을 표기

⑮ Unique Identifier(고유 식별자)

– SBOM의 고유 식별자로 조회가 가능한 Key(CPE, PURL 등), 컴포넌트의 정보를 알 수 있는 유일한 정보를 표기

⑯ Dependency Relationship(종속성 관계)

– 상위 컴포넌트와 종속관계가 있는 경우 상위 컴포넌트를 표기

⑰ Timestamp(SBOM 생성일시)

– SBOM을 생성한 날짜 및 시간을 표기

⑱ License Name · Version(라이선스 이름 · 버전)

– 대상 컴포넌트의 라이선스 이름과 버전을 표기

⑲ Vul. DB(보안취약점 DB)

– NVD(CVE), CISA(KEV) 등 보안취약점 DB에 대한 정보를 표기

⑳ Vul. Info(CVE ID(CVSS))

– SW 보안취약점에 번호를 부여한 CVE 번호와 보안취약점의 심각성을 등급(0.0 없음 → 0.1~3.9 낮음 → 4.0~6.9 중간 → 7.0~8.9 확인 → 9.0~10.0 심각)화한 CVSS를 연동하여 사용

국가사이버안보협력센터 기술공유실에 구축된 공급망보안 테스트베드를 통해 출력한 NIS-SBOM 예시는 [그림 31]과 같다.

컴포넌트별 SBOM 출력결과

번호	항목	설명	내용(Data)
1	SBOM Standard	SBOM 표준	NIS 1.0
2	SBOM Type	SBOM 생성단계	Deployed
3	CycloneDX No.	CycloneDX 번호	
4	SPDX Doc. ID	SPDX 문서번호	
5	SBOM ID	NIS 식별자	NIS-20240228-000006
6	Product Name	제품 이름	데모WEB
7	Product Version	제품 버전	1.0
8	Component Name	컴포넌트 이름	apache-log4j2
9	Component Alias	컴포넌트 별칭	log4j-core
10	Component Version	컴포넌트 버전	2.13.3
11	Component Supplier Name	컴포넌트 개발자 이름	apache
12	Component Hash	컴포넌트 해쉬	**alg :** SHA-256 **content :**627066dd32135572c986122f67c23fe0add4f2e9dd90ae73330849e1ceceeb1b
13	Component Path	컴포넌트 경로	/(데모WEB.zip)/WEB-INF/lib/log4j-core-2.13.3-sources.jar /(데모WEB.zip)/WEB-INF/lib/log4j-appserver-2.13.3-sources.jar
14	SBOM Author Name	SBOM 작성자	관리자
15	Unique Identifier	고유 식별자	
16	Dependency Relationship	종속성 관계	org.apache.logging.log4j
17	Timestamp	SBOM 생성일시	2024-02-28 09:32:52
18	License Name·Version	라이선스 이름·버전	Apache-2.0
19	Vul. DB	취약점 DB	
20	Vul. Info	CVE ID(CVSS)	CVE-2021-45046 (9.0) CVE-2021-44228 (10.0)

그림 31 NIS-SBOM 기본항목 적용 SW 컴포넌트별 출력 예시

다. NIS-SBOM 기본항목 의의와 향후 계획

NIS-SBOM 기본항목은 정부·공공기관에 도입되는 SW의 SBOM 기본항목을 제안함으로써 SW 공급자와 도입기관들 간에 일관성을 제공하고 국가적으로 SW 공급망의 투명성과 신뢰성을 확보하고 관리 효율성을 제고할 수 있다. 향후, NIS-SBOM을 통해 정부·공공기관에 도입되는 SW를 추적·관리할 수 있는 체계가 마련된다면 알려진 보안취약점에 대한 더 빠르고 확실한 보안조치를 촉진하여 국가 사이버안보 강화에 이바지할 것으로 기대된다.

본 절에서 명시된 NIS-SBOM 기본항목은 공급망 보안 관리 체계 구축을 위해 국내 산·학·연 관계자들과 의견을 나누고 실증을 통해 확인된 SBOM 기본항목을 제안한 것이다. SBOM의 기본항목을 검증하는 절차는 끝나지 않았다. 본 문서에서 제안한 NIS-SBOM 기본항목은 버전 1.00이며 국내 산·학·연 관계자들과 지속적인 논의를 통해 발전시켜 나갈 것이다. 또한 현재 SBOM 개정을 추진중인 美 CISA의 개정 사항들을 적극 검토하고, SW 공급망 보안 관련 국제 협력도 강화하여 우리 산업계가 국제적인 경쟁력을 갖출 수 있도록 지원할 것이다. 그에 따라 기본항목은 변경되고 버전도 업데이트 될 것이다.

제3절 SBOM 기반 SW 공급망 보안 발전 제언

정부·공공기관 및 기업들은 SBOM 도입을 통해 SW 투명성을 확보할 수 있고, 이를 통해 SW 제품 전반의 품질 제고와 함께 기업의 신뢰도를 개선할 수 있을 것이다. 본 가이드는 SW 투명성 확보를 통해 SW에 포함된 보안취약점 및 라이선스 관리를 가능하게 하고, 이는 SW 제품 및 서비스의 보안성 향상 및 지적 재산권 침해 위험을 제거하는데 실질적인 도움이 될 수 있음을 보여주었다. 그러나 SW 투명성을 확보하는 과정에서 SW 공급망 참여자들은 전문 인력의 확보, 시설 등 SW 공급망 보안 관리체계 구축 부담 및 민감 정보 유출 우려 등의 어려움을 겪을 수밖에 없다.

따라서 본 절에서는 SW 공급망 참여자들의 애로사항 개선을 적극 지원하고, SBOM 기반의 SW 공급망 보안 관리체계 도입 과정에서 겪을 수 있는 시행착오를 줄이는 한편, 향후 SBOM 도입·확산을 위해 해결해야 할 과제들을 순차적으로 제시하였다.

가. 개발기업의 SW 투명성 확보 지원

SW 공급망 전단계에서 SW 투명성을 확보하기 위해서는 먼저 관련 기술이 도입되어야 하고, 이를 운영할 수 있는 인력이 필요하다. 또한 SW 개발·제작 공정에 공급망 보안 관리가 추가되어야 하므로 SW 개발·제작 기간이 늘어날 수 밖에 없으며, 이는 SW 생산 비용 증가의 원인이 될 수 있으며, 이 비용을 SW 개발기업에 전가하는 것은 국내 SW 기업에 경제적 부담이 될 수밖에 없다.

이 문제를 해결하기 위해 공적 자원 투입을 고려할 수 있다. 먼저 SW 공급망 보안을 지원하기 위한 지원센터를 통해서 SW의 투명성을 확보하려는 기업들에게 보안취약점 관리 및 컨설팅 지원 등을 제공할 필요가 있다.

또한 SW 개발기업이 SBOM 기반의 SW 공급망 보안 관리체계를 구축·운영하거나 필요시 이용할 수 있도록 지원할 수 있어야 하며, 이를 위해 SBOM 기반의 SW 공급망 보안 관리체계 공통모델에 대한 선제적인 연구도 필요하다.

나. SBOM 및 SW 공급망 보안에 대한 적극적 투자

미국 FDA의 의료기기 인·허가 시 SBOM 제출, 연방정부의 '안전한 SW 개발 증명'제도 도입 및 유럽의 CRA 사이버복원력법 개정 등은 모두 자국 시장보호 기능을 활용한 사이버보안 정책으로 향후 우리 기업들에게 무역장벽으로 작용할 수 있다. 이 위기를 새로운 기회로 전환시키는 방안으로 SBOM 및 공급망 보안 기술 확보를 위한 적극적인 투자가 필요하다.

다수의 기업들이 소극적으로 SW 공급망 보안 관리체계의 도입을 망설일 때, 오히려 적극적으로 투자를 한다면 무역장벽을 극복할 수도 있고, 유럽과 미국에서 규정하는 보안취약점 관리 수준에 이른다면 기업 신뢰성 향상으로 이어져서 기업에게 장기적으로 더 큰 이익이 될 것이다. 보안 수준이 높은 기업은 신뢰도가 향상되고, 신뢰도가 높은 기업의 제품 및 서비스는 소비자가 믿고 구매할 수 있음을 잊지 말아야 할 것이다.

다. 공급자와 수요자가 연계되는 SBOM 기반 공급망 보안 관리

현재 EU, 미국 등 주요국의 공급망 보안은 SW 공급자, 즉 개발기업을 대상으로 한 정책이 주를 이룬다. 하지만, 보안취약점과 악성코드를 통해 발생하는 피해자는 결국 SW 수요자, 즉 SW를 도입해서 사용하는 기관 및 기업이다. 특히, 대부분의 기관과 기업은 내부 IT 시스템에 설치된 SW의 세부 구성요소 정보를 전혀 모르고, 해당 SW의 구성요소 관리에 대한 필요성조차 인식하지 못하고 있다. 이런 상태에서는 세계적으로 심각한 보안취약점이 발표되어도 대응이 매우 어렵다.

이를 해결하기 위해서는 기관 내 IT 자산과 SW, 그리고 SW의 구성요소를 같이 관리하고 관련 보안취약점을 지속적으로 모니터링 할 수 있는 입체적인 관리체계를 구축할 필요가 있다. 이렇게 함으로써 SW 개발기업과 수요기업의 공급망 관리 체계가 연동될 수 있다면 상호 시너지 효과를 발휘할 수 있고, 산업 전반에서 선순환 효과를 창출할 수 있게 될 것이다.

라. 안전한 SW 개발환경 조성 등 사이버 복원력 강화

디지털 및 사이버보안 정책의 핵심 개념으로 SW 위험관리 및 사이버 복원력을 강조하고, 향후 이를 제도적으로 구체화하고 실행하기 위한 법적, 기술적 프레임워크를 도입할 필요가 있다. 시장에 공급되는 SW 제품 및 서비스 등의 생애주기 전반에서 보안 관리를 강화하고, 소비자가 SW 제품 및 서비스 등을 선택할 때 보안성 내재화 여부를 고려할 수 있도록 제도화(보안적합성, IoT 보안 라벨링 등) 하는 방안도 필요하다.

또한 기업 차원에서는 안전한 SW 개발환경을 조성할 수 있도록 개발자 커뮤니티를 통한 SW 공급망 보안 문화의 확산, SDL 또는 DevSecOps 등 SW 개발보안 체계에 대한 교육 및 기술지원 방안에 대한 본격적인 논의와 함께 SW 공급사 및 운영사의 임원급(C-Level)에 대한 보안인식 제고 활동도 필요하다.

마. SBOM의 안전한 활용 및 기밀성 보장 기반 공유 방안

SBOM은 공개 SW의 라이선스 및 보안취약점 관리 등을 위한 다양한 정보를 포함할 수 있다. 따라서 무제한적 SBOM 공유·활용은 자칫 보안취약점 공격에 역으로 활용될 수 있고, 기업의 지적재산권을 탈취하는데 악용될 수도 있다. 또한 공급기업이 기업비밀 보장을 이유로 SBOM 공유를 거부한다면, 사용자 측면에서 SW내에 어떠한 위험 요소가 내재 되어 있는지 알 수 없는 어려움에 처하게 된다.

따라서 SBOM 활용에 따른 SW 개발기업의 리스크를 최소화하면서도 보안취약점 관리를 통해 수요자의 보안 리스크도 동시에 최소화 할 수 있는 방안이 필요하다. 이를 해결하기 위해 SBOM의 기밀성을 보장하면서 동시에 SBOM을 안전하게 공유하는 기술에 대한 다양한 연구가 진행되기를 바란다.

예를 들면, 기밀성이 보장되는 컴퓨팅 환경에서 SBOM을 안전하게 관리할 수 있으며, 이를 통해 기업 비밀정보의 보호와 함께 보안취약점 데이터베이스 서비스도 안전하게 보호될 수 있다. 더 나아가 이러한 안전한 환경에서 SW 안전 문자나 익명 통보와 같은 공공 시스템을 구축할 수 있으며, 정부는 이를 통해 SBOM의 안전한 활용 및 공유 거점을 구축하고 SW 구성요소 별로 신규 보안취약점에 대한 신속하고 효과적인 대응을 위한 자동화된 시스템을 구축할 수 있을 것으로 기대된다.

제5장

맺음말

우리나라는 세계 어느 나라보다 빠르게 디지털화를 이루어냈으며, 이런 디지털화의 핵심 요소로 SW가 자리하고 있습니다. 정부·공공기관 및 기업의 대다수 업무가 SW 기반으로 운영되고 있으며, 스마트폰 앱을 통해서 가전제품을 편리하게 제어할 수 있고, 다양한 레저활동도 즐길 수 있게 되었습니다. 생산 현장에서도 네트워크 기반의 스마트 공장이 확산되고 있으며, 이를 통해 산업 생산성을 크게 향상시킬 수 있는 기반이 구축되었습니다.

본 가이드라인은 이와 같이 중요성이 커지고 있는 SW의 개발, 공급(유통), 운영, 폐기 등 SW 공급망 각 단계에서 SW에 포함될 수 있는 보안취약점 등을 효과적으로 관리할 수 있는 방안을 제시하고, 정부의 기업지원 대책을 소개하였습니다.

특히, SW 공급망 보안의 핵심 요소로 부상한 SBOM에 대해 소개하고, 정부 주도로 수행한 SBOM 실증결과와 기업지원을 위한 테스트베드도 소개하였습니다. SBOM은 구성요소의 버전 및 저작권을 관리할 뿐만 아니라, 제3자 SW에 대한 보안취약점을 찾아냄으로써 보안 사고를 사전에 예방하는 데에도 유용하기 때문에 그 쓰임새가 나날이 확대되고 있습니다.

국가정보원, 과학기술정보통신부 및 디지털플랫폼정부위원회와 SW 공급망 보안 포럼 전문가들은 지난 수 개월 간 독자의 범위, 수록 내용 등 집필 방향에 대해 치열하게 고민하고 많은 논의를 거쳤고, 정부·공공기관 및 기업의 SBOM 도입을 위한 첫 걸음에 도움을 줄 수 있도록 합동으로 본 가이드라인을 만들게 되었습니다.

SW 공급망 보안 수준을 높이는 것은 국가 안보는 물론 수출과 산업 발전에도 큰 도움이 될 것이며, 궁극적으로 대한민국의 글로벌 경쟁력 강화에 기여할 것으로 기대합니다.

국가정보원, 과학기술정보통신부, 디지털플랫폼정부위원회는 앞으로도 국민의 안전과 국가 경쟁력 강화를 위해 더욱 긴밀하게 협력하면서 SW 공급망 보안 가이드라인을 지속적으로 발전시켜 나가겠습니다.

국가정보원 · 과학기술정보통신부 · 디지털플랫폼정부위원회

집필진

고려대학교 **최윤성 교수**

한남대학교 **이만희 교수**

한국과학기술원(KAIST) **강병훈 교수**

한국인터넷진흥원(KISA) **이향진 디지털안전정책팀장**

한국정보보호산업협회(KISIA) **박윤현 정책연구소장**

SW 공급망 보안 민관 전문가 협의체(국가정보원)

SW 공급망 보안 포럼(과학기술정보통신부)

제로트러스트·공급망 보안 TF(디지털플랫폼정부위원회)

SW 공급망 보안 가이드라인 v 1.0

2024년 5월 13일 1판 1쇄

발행처 한국인터넷진흥원
나주시 진흥길 9 한국인터넷진흥원

제 작 국가정보원, 과학기술정보통신부, 디지털플랫폼정부위원회,
한국인터넷진흥원

SW 공급망 보안 가이드라인 v 1.0

SW 공급망 보안 국제동향 및
SBOM 활용사례