2022
공급망 보호를 위한
SBOM 조사 보고서

kisia 한국정보보호산업협회

CONTENTS

이 보고서는 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 보고서임
(No.2022-0-00277, SW공급망 보안을 위한 SBOM 자동생성 및 무결성 검증기술 개발 과제)

2022
공급망 보호를 위한
SBOM 조사 보고서

I.

SBOM 개요

Ⅰ. SBOM 개요

1. 등장 배경과 목적

각국은 사이버 보안을 위해 취약점 진단, 보안요구사항 준수, 인증된 정보보호제품군 및 공급업체 사용 등의 노력을 지속해왔다. 그러나 최근 주요 사이버안보 문제로 공급망 공격이 대두되면서, 공급망 환경을 안전하게 구축하기 위한 제도가 각국에서 마련되고 있다. 이에 공급망 공격에 관한 탐지 및 선제적 대응, 피해 발생 위치의 파악, 피해 범위 산정, 신속한 후속 조치 등을 목적으로 공급망 가시화와 무결성 보증에 관한 대응방안이 논의되고 있다. 이미 CISQ[1], MITRE[2], NIST[3] 등에서는 소프트웨어 공급망 무결성 검증 및 정보공유, 시각화를 위한 방안을 꾸준히 언급해왔다. 최근 공급망 보안을 위한 기초적인 방안으로, 소프트웨어 구성요소를 파악하기 위한 SBOM의 중요성이 대두되고 있다.

2. 기본 개념 및 구성

SBOM(Software Bill of Materials)[4]은 제조업에 사용되는 자재명세서(Bill Of Materials, BOM)의 개념을 소프트웨어 분야에 적용한 것으로 소프트웨어의 구성요소를 메타데이터로 나타낸 것이다.

[표: SBOM과 기존 명세서의 비교]

구분	목적	비고
SBOM	소프트웨어 공급망, 라이선스, 취약성 등 위험을 관리	소프트웨어
BOM	지속적인 양산체제 유지를 위한 공급망과 생산관리	제조업
Food ingredients	유통되는 식품에 관한 이용자의 인지 및 위험성 확인	식품

SBOM은 소프트웨어와 관련된 정보 및 도구의 표준 세트로 소프트웨어 공급망과 함께 발전한다. 다음 표는 NTIA Formats & Tooling 작업 그룹에서 SBOM의 기능별 유형을 분류한 것이다. SBOM의 기능은 생성, 소비 및 사용 범위이며, 이는 SBOM 도구가 필요한 사람들에게 사용 기능과 그 목적을 이해하는데 도움이 될 것이다.

1) https://www.it-cisq.org/
2) https://www.mitre.org/
3) https://www.nist.gov/
4) “The term “Software Bill of Materials” or “SBOM” means a formal record containing the details and supply chain relationships of various components used in building and loan association software. …” (2021.5, US EO14028)

[표: SBOM의 기능별 기본 유형]

구분	유형	설명
생성	빌드 (Build)	소프트웨어 인위적 작성의 일부로 자동 생성되며 빌드에 대한 정보도 포함한다.
	분석 (Analyze)	소스 및 바이너리 파일을 분석하여 인위적 내용물 및 관련 소스를 검사하고 SBOM을 생성한다.
	편집 (Edit)	사용자가 SBOM 데이터를 수동으로 입력하거나 편집할 수 있도록 지원한다.
소비	뷰 (View)	사람이 읽을 수 있는 형식(예: 그림, 표, 테스트 등)으로 내용을 이해할 수 있어야 하며, 의사 결정 및 비즈니스 프로세스를 지원하는데 사용한다.
	구별 (Diff)	여러 SBOM을 비교하여 차이점을 명확히 파악할 수 있어야 한다. (예: 두개의 다른 버전의 소프트웨어 결과 비교)
	불러오기 (Import)	추가 처리 및 분석을 위해 SBOM을 검색하여 시스템으로 가져올 수 있다.
활용	변경 (Translate)	동일한 정보를 유지하면서 파일 형식을 다른 파일 형식으로 변경할 수 있다.
	병합 (Merge)	SBOM 및 기타 데이터의 여러 소스를 분석 및 검사 목적으로 함께 결합할 수 있다.
	툴 지원 (Tool Support)	API, 객체 모델, 라이브러리, 전송 또는 기타 참조 소스에 의한 기타 도구의 사용을 지원한다.

3. 소프트웨어 공급망 보안

소프트웨어 공급망은 구성 요소, 작성자, 출처 등 소프트웨어에 관한 정보 네트워크를 포함한다. 구성 요소는 인프라, 하드웨어, 운영체제(OS), 클라우드 서비스 등과 같으며, 출처는 레지스트리, GitHub, 리포지터리(Repository) 등의 예로 표현할 수 있다. 이러한 공급망에는 소프트웨어 보안에 부정적인 영향을 줄 수 있는 취약점도 포함하기에 공급망 보안이 함께 요구된다.

소프트웨어 공급망의 구성 요소에 해당하는 위험은 해당 구성 요소를 사용하는 모든 소프트웨어에 잠재적 위험이 있을 수 있음을 나타낸다. 이는 해커가 멀웨어나 백도어 또는 악성코드를 삽입하여 구성 요소와 연결된 공급망을 손상시킬 가능성을 야기한다. 특히, 영리를 추구하는 공격자와 국가 행위자의 소프트웨어 공급망 공격이 증가하고 있으며, 디지털 환경과 함께 실제 세계에 모두 심각한 영향을 줄 수 있게 된다. 이러한 공격은 일반적으로 다음과 같이 4가지 위험 유형 중 하나에 해당한다.

[표: 소프트웨어 공급망 구성 요소에 대한 위험 유형 구분]

유형	내용
취약점	소프트웨어 코드의 결함으로, 악용되면 침해로 연결 가능
라이센싱	라이선스를 받은 소프트웨어 아티팩트를 오픈소스로 만들고 특허권을 무효화하도록 강제할 수 있는 법적 위험
제3자 종속성	소프트웨어 공급망에 포함된 모든 외부 조직에 대한 종속성
프로세스 및 정책	부재할 문제가 되며, 취약점에 대응하기 위한 정책이 필요

2022
공급망 보호를 위한
SBOM 조사 보고서

II.

해외 동향

Ⅱ. 해외 동향

1. SBOM 관련 정책의 발단 배경

최근 발생한 심각한 사이버안보 위협 상황과 코로나19로 디지털 전환이 가속화되면서 해킹 악성코드 등 사이버공격은 국가안보와 외교정책에 심각한 영향을 미치는 핵심 이슈로 등장했다.

미국 SolarWinds 해킹 : SolarWinds는 18,000여 개의 미국 연방 부처와 민간 기업 등의 시스템과 네트워크에 사용되었으며, 해당 제품에 악성 백도어가 내재되어 있어 공격자에 의한 정보수집과 기밀탈취가 발생했다.

우크라이나 MeDoc 업데이터 서버 해킹 : MeDoc은 회계 관리 소프트웨어를 개발하는 기업으로 공격자가 MeDoc의 업데이터 서버를 해킹하여, 업데이터 요청 시 정상 업데이트가 아닌 Petya 랜섬웨어를 배포하도록 변조했다. 그 결과 전 세계 총 10조원의 손실을 입었다.

중국 해킹 : 2021년 1월부터 마이크로소프트의 이메일 서버 제로데이 취약성을 이용하여 침입 후 백도어를 심어 공격하여 미국 정부부처와 기업 등 30,000곳 이상 피해를 입었다.

북한 해킹 : 각국 정부부처와 기업 등에 대한 랜섬웨어 공격 및 전 시계 은행과 기업, 가상화폐 거래소 등에 대한 사이버공격을 통해 총 1억 1200만 달러의 피해가 발생했다.

2. 미국

미국은 국가 주요 기반시설의 사이버 보안 강화를 위해 사이버 보안 프레임워크를 신설해 산업별로 적용을 추진하고 있다. 이에 더해 연방 정부 기관들의 보안 위협 점검을 위한 목적으로, 기존 특정 기능의 방어(중요 인프라 중심)중심으로부터 공급망 위험관리로 점검 영역을 확대하고 있다.

2.1. NISTNTIA 공급망 보안기준

공급망 보안기준	내용
NIST IR 7622	연방 기관이 ICT 공급망 위험 관리를 위하여, ICT 제품 및 서비스를 도입할 경우 고려해야 할 사항 명시 및 공급망 위험 관리에 대한 전체적인 배경 지식을 제공하는 것을 목표로 한다.
NIST Cybersecurity Framework (CSF)	에너지, 은행, 통신, 국방 산업 기지를 포함한 국가 주요 기반시설의 운영 주체가 사이버 위협 상황에 대한 인식 및 적절한 대응을 할 수 있도록 안내하는 일종의 보안관리 가이드라인이다. 공급망에 있어 불충분한 제조나 개발, 잠재적으로 악의가 있는 기능, 가짜 혹은 취약성이 있는 제품이나 서비스를 특정하고, 평가·경감하는 것을 목표로 한다.
NIST SP800-161	공급의 품질 저하 문제나 악의적 개입으로 ICT 시스템 피해 발생 시, 종합적인 해결 방안을 수립하기 위한 보안 관리대책이다. 공급망에서의 위협과 조직의 취약점에서 보안 문제가 발생할 확률과 영향을 평가해 위험기반의 공급망 대책을 실행하고, 통합적인 위험 관리 수행을 위해 위험 관리를 계층화하여 조직 계층 간 위험을 전략적으로 통합 관리를 목표로 한다.
NIST SP800-171	연방정보시스템 및 기구 내에서의 비기밀통제정보 (미국의 국가안보 관련 중요한 기밀정보로 분류되지 않은 정보 중 기밀 관리되는 정보) 의 보호를 목적으로 하며, 연방을 대상으로 조달계약을 체결하는 모든 계약자(또는 공급자)가 준수해야하는 것을 목표로 한다. 연방 정부와 거래 시 비기밀정보에 대한 보안 요구사항의 이행 혹은 이행을 위한 계획을 기술하고, 필요한 경우 시스템 보안계획과 조치 일정을 연방 정부나 연방 측의 계약 상대방에게 제출한다는 내용을 담고 있다.

공급망 보안기준	내용
NTIA Software Component Transparency	소프트웨어 구성요소 투명성 연구를 위해 다중 이해관계자 프로세스를 구조화(Framing), 형식 및 도구(Formats and Tooling), 인식 및 채택(Awareness and Adoption), 의료 개념 증명(Healthcare Proof of Concept) 그룹으로 구성했다. '공통 소프트웨어 재료명세서(SBOM) 구축'에 관한 보고서 및 SBOM 생성 및 활용에 대한 자동화 방안 연구에 중점을 두어 진행하며, SBOM 기존 도구를 카탈로그화 하고 데이터 형식의 변환이 가능한 도구를 개발하고자 한다.

2.2. 행정명령 14028

행정명령 14028(국가의 사이버 안보 개선을 위한 행정 명령)은 연방정부 네트워크의 현대화, 연방정부의 소프트웨어 공급망 보안 강화, 연방 정부의 향상된 사이버 안보 관행 및 절차 구현, 정부 차원의 사고 대응 계획에 대한 수립 등 사이버 안보 위협에 대응하고 예방할 수 있도록 연방정부의 역량을 강화하는 것을 목표로 한다.

[표: 행정명령 14028의 각 섹션 별 주요 지시사항]

섹션 번호	주요 지시사항
섹션2	정부와 민간 부문 간 위협 정보 공유에 대한 장벽을 제거
섹션3	연방정부의 사이버 보안 표준 현대화
섹션4	소프트웨어 공급망 보안 개선, 소프트웨어를 구성하는 개별 요소를 추적하는 SBOM에 대한 최소 요소 게시 의무
섹션5	사이버 안전심의위원회 구성
섹션6	사고 대응을 위한 표준 플레이북(Playbook)[5]
섹션7	엔드포인트 탐지 및 대응 시스템 활성화 및 사이버 보안 사고 탐지 개선
섹션8	연방정부의 조사 및 수정 기능 개선

2.3. 포괄적인 리스크 관리 권장사항

FDD TCIL(Foundation for Defense of Democracies Transformative Cyber Innovation Lab)은 SBOM의 유용성을 검증하여 NTIA와 NIST에 몇 가지 권장사항을 제안했다.

권장사항	내용
SBOM 지침의 지속적인 업데이트	- 새로운 데이터 형식에 통합 가능한 유연성 - 감사의 불변함과 확장성 - 기계 가독성 보장 및 지속적인 모니터링 - SBOM 지원 시스템 구조에 대한 아키텍처 및 설계에 있어 제로 트러스트 개념 적용방안을 연구 필요
민간부문의 SBOM 이해 장려 및 활용 권고	- 민간 및 공공 작업 그룹 형성과 정부의 지원 필요 - 민관 파트너십을 구축
모든 관련 정부 계약 내 SBOM 요구사항 포함	- SBOM 계약 언어로 FAR 및 DFARS 업데이트 - 연방 정부부처 및 기관을 대상으로 적용 가능한 부분에 SBOM 요구사항 제출 시범 운영 권장

5) 플레이북이란, 사이버 위협 대응을 위해 센터의 전문인력이 수동으로 수행하는 보안관제 프로세스를 자동으로 수행하기 위한 업무 절차서다.

2.4. 소프트웨어 보안 관련 백악관 회의

백악관은 정부, 민간 기업의 관계자, 오픈소스 관련 비영리 단체가 참여하는 회의를 개최하여 Log4j 사건에 대한 구체적인 대응 방안을 논의했다.

대응방안	내용
코드 및 오픈소스 패키지의 보안 결함 및 취약성 방지	- 개발도구의 보안 기능 통합 코드 서명 - 디지털 ID를 통한 빌드, 저장 및 배포 인프라 보호
결함 발견 및 수정 프로세스 개선	- 오픈소스 프로젝트의 우선순위 지정 - 유지 관리를 위한 매카니즘 마련
수정 배포 및 구현에 대한 응답 시간 단축	- 기업과 개발자의 SBOM 사용 및 개선 가속화

2.5. 오픈소스 SW보안법

오픈소스 SW 보안법은 CISA가 현존하는 최고의 오픈소스 보안 기술을 사용함과 동시에 오픈소스 소프트웨어의 리스크를 완화하는 방법을 식별하도록 요구한다. 또한 일부 연방기관에서 '오피스(오픈소스 프로그램)'를 시작할 것을 제안하며, 미국 예산관리국(OMB)이 CISA 소프트웨어 보안 소위원회에 자금 지원 및 사용자의 오픈소스 소프트웨어 보호 방법에 대한 연방지침을 발행해야 한다고 명시한다.

3. 일본

현재 일본 정부의 공식적인 SBOM 움직임은 PoC(Proof of Concept)의 실증 사업을 추진하고 있으며, 일본 경제산업성 상무정보정책국 사이버보안과는 소프트웨어 관리방법 검토 TF를 구성하여 분야별 SWG에서 사이버 물리적 보안 대책 프레임워크(CPSF)를 구체화할 예정이다. 또한 OSS(Open Source Software) 추진 포럼에서는 기업 간 정보교환을 하며, 리스크 및 모니터링 관련 논의를 지속하고 있다.

3.1. SBOM의 PoC (Proof of Concept)

SBOM의 실증은 반복적으로 계속해서 실시할 수 있는 것이 중요하다. 또한 고유하기 때문에 맞출 수 없는 부분, 맞출 필요가 없는 것을 나누는 것을 목적으로 하여, 사업자의 단체나 ISAC 등과도 상담을 하면서 PoC를 해 나가야 한다. 또한 특정 업종을 대상으로 여러 조직에 걸쳐 PoC를 이루고, 횡단적인 대응의 경우에는 제품 식별이 필요하지만 그 점을 검증하는 노력이 필요하다.

3.2. SBOM도구정보

IPA의 JVN을 개조하고, SWID 태그, SPDX, CycloneDX 등 소프트웨어의 식별자를 등록하는 데이터베이스의 정비와 취약성 정보 및 위협정보를 함께 보낼 수 있도록 형식 변환에 대해 검토가 이루어지고 있다.

4. 중국

4.1. 국가 및 산업 감독 수준에서의 권고사항

- 소프트웨어 공급망 및 오픈 소스 소프트웨어 구성 요소 보안 위험 분석 플랫폼 구축
- 중요 인프라 및 중요 정보 시스템 사용자를 위한 일일 자체 검사 서비스를 제공하여 적시에 발견하는 기능 개발 및 소프트웨어 공급망 보안 위험 처리
- 제품 평가, 시스템 평가 등에 소프트웨어 공급망 보안 내용을 포함
- 소프트웨어 소스 코드, 완제품 및 실행 중인 소프트웨어 시스템에 대한 소프트웨어 공급망 보안 테스트

4.2. 소프트웨어 최종 사용자 수준에서의 권고사항

- 소프트웨어 공급망 보안 관리를 명확히 하고 책임 부서에 충분한 권한 부여
- 상용 선반 소프트웨어를 구입 시, 공급자의 보안 기능 평가하고, 공급자와 소프트웨어에 사용되는 오픈 소스 구성 요소 목록을 제공한다는 보안 책임 계약서 작성
- 타사 오픈 소스 구성 요소에 보안 취약성이 있는 경우, 공급 업체도 필요한 기술 지원 제공
- 소프트웨어 시스템을 자체 개발 및 제3자에게 소프트웨어 시스템 맞춤화를 위탁하는 경우, 소프트웨어 소스 코드에 대한 보안 결함 감지 및 복구 수행
- 소프트웨어 자산 원장은 사용되는 오픈소스 소프트웨어의 보안위험 지속적인 모니터링

5. 유럽

유럽에서는 공급망 보안정책과 관련 EU 차원에서 단일시장 구현과 중요 인프라에 최신의 사이버 보안 대응(NIS Directive)을 구현하고, 네트워크에 접속하는 기기의 보안성을 인증 및 확인하기 위한 사이버 보안 인증 프레임워크를 수립하고 있다.

향후 단일 사이버 보안 시장을 목표로 하고, 네트워크에 연결되는 기기의 인증, 프레임 도입을 검토하고 있으며 규제가 아닌 자발적이고 산업계는 국제표준에 근거하는 자기 적합 선언을 하도록 할 방침이다. 또한 ENISA와 유럽 사이버 보안 인증그룹이 협력해 EU 전체 인증체계를 개발하고 EU 회원국은 인증 감독기관과 적합성 평가기관을 운영할 예정이다.

5.1. SBOM 활용 사례

• 의료기기 소프트웨어 제조에서 SBOM

의료 기관용 의료 기기의 보안 (및 개인정보 보호) 측면을 용이하게 하기 위해 의료 기기 제조업체 커뮤니티에서 MIDS2 (의료 기기 보안에 대한 제조업체 공개 성명)를 도입했다.

• ENISA(The European Union Agency for Cybersecurity)
'사물 인터넷 보안을 위한 가이드라인' 보고서는 IT 기기용 SBOM의 존재를 사용할 것을 권장하고 Dependency Track 도구를 사용하여 기본 소프트웨어를 식별하고 SBOM을 생성할 것을 제안한다.

또한 '사이버 보안 병원을 위한 조달 가이드라인' 보고서는 의료 기기를 선택할 때 하드웨어 및 소프트웨어에 대한 BOM(Bill of Material) 요구사항을 포함하는 것을 고려할 것을 권장한다.

• 유럽 의회(European Parliament)와 집행위원회(European Commission) FOSSEPS 파일럿 프로젝트는 주요 업무 패키지를

(1) 유럽 앱 카탈로그 벤치마킹,
(2) EU 앱 카탈로그 생성,
(3) 중요 공개SW 저장소 생성,
(4) 공개SW 협력,
(5) 프로젝트 확산,
(6) 교훈

문서화 이렇게 총 6가지를 정의한다.

5.2. 영국 ICT공급망 보안정책

[표: 영국 NCSC(National Cyber Security Centre) 공급망 보안 원칙]

보안원칙 4단계	보안 원칙
위험 이해	- 보호대상 및 보호 이유 정당화 - 공급업체 파악 및 보안상태 확인 - 공급망 보안위협 식별
통제권 확립	- 공급업체에 보안 필요성 전달 - 공급업체에 최소보안 요구사항 설정 - 계약 프로세스의 보안 요구사항 구축 - 보안책임 완수 - 공급망 내 보안인식 제고 - 보안사고 대응 지원
준비사항 확인	- 공급망 관리에 보증 활동 구축
지속적인 개선	- 공급망 내 지속적인 보안개선활동 - 공급업체와 신뢰 구축

[표: SAF(Supplier Assurance Framework)]

주요 항목	내용
공급업체와 계약 식별	계약현황 파악과 목록작성
위험평가가 필요한 계약 식별	개인정보, 기밀정보 취급 계약 등 분석
cc위험평가 주체 식별	정보자산과 시스템소유자, 계약주관부서, 보안부서 등 참여
위험관리 전략 확보	기밀성, 무결성, 가용성 관점에서 비즈니스 영향평가와 위험완화 전략은 조직의 위험성향과 일치
cc위험평가 대응 조정	공급자의 CCAR에서 검토하여 위험 허용 수준과 위험성향을 매핑
결과 정리	계약과 관련된 위험평가의 우선순위 지정하여 우선적인 대책 수립
보증 구현 프로그램	SoA(Statement of Assurance)를 기반으로 상, 중, 하 계약을 분류하여 공급업체 보증 프로세스의 비례적인 접근방식 채택

2022
공급망 보호를 위한
SBOM 조사 보고서

III.

SBOM의 기술적 내용

Ⅲ. SBOM 의 기술적 내용

1. SBOM 표준 배경

소프트웨어 구성 요소의 품질, 보안 또는 작성자에 대한 기본적인 가시성과 투명성이 부족하면 소프트웨어 공급망이 공격에 쉽게 취약해진다. 이를 방지하기 위해 바이든 대통령의 국가 공급망 개선에 관한 행정 명령은 소프트웨어 구성 요소를 식별하고 설명하는 방법으로 SBOM(Software Bill of Materials)을 채택할 것을 권장하였다.

SBOM은 소프트웨어를 구성하는 컴포넌트 자체와 의존관계(Dependency)에 관한 정보를 관리한다는 점에서 소프트웨어 복잡성을 가시화하려는 시도이다.

2. 데이터 형식 및 표준

SBOM 포맷은 SBOM을 생성하기 위한 통합 구조를 정의하고 최종 사용자 또는 고객과 공유하기 위한 표준이며, 소프트웨어의 구성을 다른 툴이 이해할 수 있도록 공통의 형식으로 설명한다.

2.1. SPDX (Software Package Data eXchange)

리눅스 재단에서 운영하는 프로젝트인 SPDX는 공유 및 수집을 위한 소프트웨어 패키지와 관련된 정보에 대해 공통 데이터 교환 포맷을 만드는 것이 목적이었다. 주요 SBOM 포맷 중에서 가장 많은 파일 형식을 지원하며 일련의 소프트웨어 패키지, 파일 또는 스니펫(Snippet)을 설명함으로써 동적 사양이 되는 것을 목표로 하고 있다.

2.2. CycloneDX

CycloneDX는 자체적으로 “애플리케이션 보안 컨텍스트 및 공급망 구성 요소 분석에 사용하도록 설계된 경량의 SBOM 표준” 이라고 정의한다. 주요 지원 기능에는 BOM 링크(BOM-Link), 프로비넌스(provenance), VEX (Vulnerability Exploitability eXchange)[6], 해시값과 암호화를 통한 BOM 관련 구성요소의 무결성 검증 등이 있다.

2.3. SWID - 소프트웨어 식별 태그

NIST에 따르면 "SWID 표준은 SWID 태그가 소프트웨어 제품 설치 프로세스의 일부로 끝점에 추가되고 제품 제거 프로세스에 의해 삭제되는 라이프사이클“로 정의한다. SWID 태그는 소프트웨어 수명 주기 전반에 걸쳐 소프트웨어를 보다 쉽게 검색, 식별 및 컨텍스트화 하여 기업이 정확한 소프트웨어 재고를 생성하도록 지원하는 것을 목표로 한다.

2.4. SPDX Light

SPDX Lite는 전체 SPDX가 필요하지 않은 상황을 위한 SPDX의 경량 하위 집합이다. 오픈 소스 라이선스에

6) https://cyclonedx.org/capabilities/vex/

대한 지식이나 경험이 없는 사람들도 쉽게 사용할 수 있도록 하고 "일부 산업에서 SPDX 표준과 실제 워크플로우 간의 균형"을 유지하기 위한 것이다.

3. 도구 리스트

도구명	내용
Dynamic SBOM Platform	Rezilion社가 개발한 SBOM 관리 솔루션으로 애플리케이션, 라이브러리, 도커(Docker) 컨테이너 등에 포함된 SBOM을 활용하여 동적으로 소프트웨어의 오픈소스 구성요소 및 취약한 구성요소를 관리한다.
Phylum	Phylum社가 개발한 소프트웨어 공급망 보안 솔루션으로, 개발 및 CI/CD 환경에서 휴리스틱, 머신러닝을 이용하여 소프트웨어 패키지를 자동으로 식별하고 공급망 위험을 분석한다.
Cyber Security Asset Management	Qualys社가 개발한 IT 자산 관리 솔루션으로 사이버 보안 태세를 지속해서 측정, 분류, 검색할 수 있도록 고객의 내부 및 외부 IT 자산을 관리할 수 있는 클라우드형 서비스이다.
NextGen SCA	Cycode社가 개발한 소프트웨어 구성요소의 종속성 관리 도구로, 소프트웨어 개발 생명주기(SDLC, Software Development Life Cycle)의 파이프라인 구성 분석(PCA, Pipeline Composition Analysis)을 통해 포함된 구성요소와 종속성을 식별한다.
Software Composition Analysis	Veracode社가 개발한 소프트웨어 구성 분석 솔루션으로, 소프트웨어 공급망을 보호하기 위해 구성요소를 분석한 후 라이브러리 내의 취약점을 자동으로 식별한다.
Black Duck Software Composition Analysis	Synopsys社가 개발한 소프트웨어 구성 분석 솔루션으로 애플리케이션 및 컨테이너에서 오픈소스 또는 타사 코드 사용으로 인해 발생하는 보안, 품질 및 라이센스 규정 준수 위험을 관리하는 기능을 제공한다.
Anchore	Anchore社가 개발한 SBOM 관리 솔루션으로 소프트웨어의 종속성을 포함한 모든 구성요소를 식별 및 관리한다.
CodeSentry	GrammaTech社가 개발한 바이너리 소프트웨어 구성 분석 도구로 바이너리 분석을 통하여 SBOM을 생성하고 종속성을 포함하여 탐지된 구성요소에서 알려진 취약점(NVD, National Vulnerabilities Database)을 식별한다.
Nexus Lifecycle	Sonatype社가 개발한 오픈소스 보안 및 종속성 관리 제품으로, 소프트웨어 수명 주기 전반에서 오픈소스 취약점을 자동으로 식별 및 수정하는 기능을 제공한다.
RKVST	RKVST社가 개발한 SBOM 관리 플랫폼으로 자산 정보를 지속적으로 증명하기 위해 블록체인 기반의 데이터 교환 및 보증기술을 사용한다.
NowSecure Platform SBOM	NowSecure社가 개발한 모바일 SBOM 보안 솔루션으로 iOS(.ipa) 및 Android(.apk) 장치에서 실행되는 모바일 앱 바이너리를 정적/동적 분석하여 라이브러리, 프레임워크, API 정보, 네트워크 통신지 및 취약성 정보 등에 대한 정보를 생성한다.
Application Security Posture Management (ASPM)	Bionic社가 개발한 프로덕션 애플리케이션의 보안성 향상을 위한 통합 보안 관리 솔루션이다.
CycloneDX-CLI	기계가 읽을 수 있는 형식과 SBOM을 취약점, 종속성 그래프 및 BOM 설명자를 염두에 둔 추가 기능과 공유하는 방법을 제공한다.
FOSSology	FOSSology는 오픈소스 라이선스 컴플라이언스 소프트웨어 시스템 및 도구로, 소프트웨어를 검색하는 여러 가지 방법을 제공한다.
Tern	Tern은 컨테이너 이미지에 설치된 패키지의 메타 데이터를 찾기 위한 검사 도구이다. 패키지 라이선스를 위해 컨테이너와 이미지 계층을 스캔하는 것을 전문으로 한다.
ScanCode toolkit	Scancode toolkit은 쉽게 찾을 수 없는 라이선스 및 원본 패키지 데이터들을 검색하고 정규화 한다.

도구명	내용
SBOM Operator	Codenotary 社가 개발한 SBOM 오퍼레이터는 쿠버네티스로 실행되는 모든 소프트웨어와 소프트웨어 종속성을 트래킹하여 소프트웨어 공급 체인 공격의 리스크를 줄인다.
SBOM Generator	마이크로소프트 社가 사용하는 SBOM 도구는 오픈소스이며, 최신 버전의 마이크로소프트 SBOM 도구는 커맨드라인 기반 애플리케이션이다. 핵심 구성요소 중 하나는 CD(Component Detection)로 일반적인 소프트웨어 기술을 거의 다 지원한다.
Clarity	Insignary 社의 Clarity는 소프트웨어 공급망에서 타사 코드의 보안 및 라이선스 준수 문제를 관리할 수 있는 상용 소프트웨어 구성 분석 도구이다.
Snyk	SW개발 tool chain에 연동하여, commit이나 build, CI/CD 시 프로젝트의 의존성을 검사해서 보안 취약점이 있는 외부 open source 사용여부를 알려주는 보안 도구
Mend	오픈소스 취약점 분석 솔루션으로, 오픈 소스 품질 이슈와 라이선스 관련 모든 정보를 하나의 솔루션에서 확인할 수 있으며, 간편한 보고서 형태로 결과까지 제공하는 제품
Labrador	국내 보안업체인 아이오티큐브社에서 개발한 제품으로, 오픈소스 컴포넌트를 분석하여 취약점 및 라이선스 리스크를 자동으로 도출하며, 소스코드에 대한 오류, 무선통신 프로토콜의 취약점 분석, 바이너리 취약점 분석 등 다양한 보안 취약점 분석 기능을 제공하는 국산 플랫폼 분석 서비스
Sparrow SCA	국내 보안업체인 스패로우社에서 개발한 제품으로, 효율적인 소프트웨어 공급망 관리를 위해, 오픈소스 소프트웨어 라이선스 식별 및 보안 취약점을 진단 서비스 제공

4. SBOM에 필요한 최소 요건

SBOM의 최소 구성 요소들은 소프트웨어 투명성에 대한 진화하는 접근 방식을 가능하게 하여 기술과 기능적 운영을 모두 포착할 수 있도록 지원한다. 요소들의 세 가지 범주는 다음과 같다.

4.1. 데이터 필드

데이터 필드에는 추적하고 유지 관리해야 하는 각 구성 요소에 대한 기본 정보가 있다. 이 정보는 Supplier Name, Component Name, Version of the Component, Other Unique Identifiers, Dependency Relationship, Author of SBOM data, Timestamp를 포함한다.

4.2. 자동화 지원

자동 생성 및 기계 가독성을 포함한 자동화 지원을 통해 소프트웨어 에코시스템 전반, 특히 조직 경계 전반에 걸쳐 확장할 수 있다. 자동화는 이 기능을 그들의 기존 취약성 관리 관행에 통합하고자 하는 기업과 보안 정책에 대한 보안 정책에 대한 준수 여부를 감사하기를 원하는 사람들 모두에게 핵심이 될 것이다.

4.3. 실제 사용과 프로세스 (Practice and Process)

SBOM은 구조화된 데이터 집합 그 이상으로, 이를 안전한 개발 수명 주기의 운영에 통합하려면 SBOM 사용 역학에 초점을 맞춘 특정 관행과 프로세스를 따라야 한다. SBOM을 요청하거나 제공하기 위한 정책, 계약 또는 약정에서 많은 요소를 명시적으로 다루어야 한다. 해당 요소에는 Frequency, Depth, Known Unknown, Distribution and Delivery, Access Control, Accommodation of Mistakes가 있다.

4.4. 권장 데이터 필드

위의 최소 요소에 설명된 데이터 필드 외에도, 특히 몇 년에 걸쳐 계획되었거나 더 높은 수준의 보안이 필요한 작업에 대해 다음 데이터 필드를 고려하는 것이 좋다. 권장하는 데이터 필드는 구성 요소의 해시, Lifecycle Phase, 기타 구성요소와 관계, 라이선스 정보이다.

5. SBOM 도입 활용 방안

먼저 소프트웨어 생산 시, 소프트웨어 내 취약점에 대한 구성요소 모니터링이 용이하여 새로운 보안 위험이 발견될 경우 잠재적 취약성 판단이 가능하다. 소프트웨어 선택 시에는 소프트웨어 전반에 대한 잠재적인 위험 요소를 식별하여 사전 위험분석을 수행할 수 있으며, 구성요소의 아웃소싱 정보 등을 확인해 검증을 통한 도입이 가능하다.

소프트웨어 취득 이후 설치, 구성, 유지관리를 수행할 때에는 구성요소 목록을 통하여 현재 소프트웨어에 적용되는 새로운 취약점을 빠르게 식별하여 해결할 수 있으며, 특정 소프트웨어가 영향을 받는지에 대한 여부를 평가하고 해당 위치 파악에 용이하다. 이외에도 비용, 라이선스 위험, 규정준수 위험, 높은 보증 차원 요소에서 소프트웨어의 효율적 운영 및 관리, 정량화된 라이선스 및 위험관리 등을 위해 SBOM을 활용할 수 있다.

6. 개발자가 알아야 할 SW 공급망 보호 가이드

프로세스와 활동에는 위협 모델링, SAST[7], DAST[8], 침투 테스트와 같은 모범 사례뿐만 아니라 디지털 서명과 같은 보안 릴리스 활동 등이 있다.

위협 모델링은 제품 개발 과정에서 배포와 관여된 팀은 위협 시나리오와 이를 완화하기 위한 통제 수단을 검토해야 한다고 설명한다. 또한, 허용할 수 없는 취약점이 프로덕션 환경으로 유입되거나 고객에게 전달되지 않도록 보안 테스트 계획 및 관련된 릴리스 준비 기준도 마련해야 한다고 제시한다.

기업은 적절한 인증을 수행, 코드를 대상으로 정적/동적 테스트를 실행하고 노출된 기밀 사항을 점검하는 명문화된 소스 제어 프로세스를 구축해 관련 위협을 완화할 수 있다. 또한, 일일 빌드 및 보안 회귀 테스트도 구현해서 결함과 취약점을 인지하고 처리해야 한다. 개발 작업은 구체적인 시스템 요구사항에 따라 진행돼야 하며 관련 보안 테스트를 통해 위험을 유발할 수 있는 기능의 과도한 확장(feature creep)을 피해야 한다.

소프트웨어는 최종 구성에 대한 SBOM을 포함해 안전하게 고객에 제공되어야 한다. 소프트웨어 패키지와 업데이트의 침해에 대처하기 위해 제품과 구성요소 모두 제품 배포, 구성요소 및 업그레이드에 해시와 디지털 서명을 사용할 수 있다. 또한, 기업은 리포지토리 및 패키지 관리자에 보안 수단을 적용하거나 안전한 전송 계층 매카니즘을 사용하는 등 배포 시스템 자체의 침해를 완화하기 위한 조치도 취해야 한다.

---

7) SAST(Static Application Security Testing): 정적 분석 툴
8) DAST(Dynamic Application Security Testing): 동적 분석 툴

2022
공급망 보호를 위한
SBOM 조사 보고서

IV.

국내 현황

Ⅳ. 국내 현황

1. 국내 관련 법률

공급망 공격에 대해 적용 가능한 국내 법률은 조달청 지침과 정보통신망법에 의거하여 규정되고 있다. 먼저 조달청지침 제527호 「네트워크 장비 구축 운영 사업 추가 특수 조건」의 제4조 (계약상대자 정보보안 준수의무)는 보안요구사항 관리와 네트워크의 비정상적인 접근에 대해 규제하고 있으며, 정상적인 인증과정을 거치지 않는 공급망 공격 중 하나인 백도어에 관해서도 언급한다. 이러한 조달청 지침에 따라 네트워크 장비 구축 또는 네트워크 장비 운영사업의 계약상대자는 국가정보원의 국가 정보보호 기본지침 및 수요기관 보안업무 규정 및 세부지침을 준수해야 한다. 만약 본 지침을 위반할 경우에는 제5조에 의거하여, 입찰참가 자격 제한 및 계약 해제 또는 해지될 수 있는 처분을 받게 된다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서는 정보통신망 침입에 대해 규정하고 있으며, 제48조 (정보통신망 침해행위 등의 금지)에서는 접근권한이 없는 자가 통신망에 침입하는 것은 안 된다고 명시한다. 또한, 정당한 사유 없이 악성프로그램을 전달 또는 유포하고, 데이터나 프로그램을 훼손, 변경, 위조 등을 하여서는 아니 된다. 이를 위반하면 제72조(벌칙)에 의해 3년 이하의 징역 또는 3천만원 이하의 벌금을 받게 되며, 비수범의 경우는 처벌만 진행된다.

2. 국내 기업 대응 현황

국내 대기업은 미국의 행정명령에 관한 주요 내용과 관련 기사 등을 통해 정보를 파악하고 있다. 미국 연방정부 차원에서 계약 시 효력을 발휘하는 사항이기에 아직까지 구체적인 대응은 하지 않고 있지만 향후 민간기업에도 영향을 줄 것으로 예상됨에 따라 지속적인 관심을 갖고 주시하고 있는 상황이다. 공공 및 표준화 측면에서는 정부에서 적극적으로 도입할 상황은 아니나 표준화를 위한 참여를 통해 상황 공유가 필요해 보이며, R&D 측면보다는 SW 취약점 등의 관리를 위한 거버넌스 정책 및 관리 시스템 구축에 대한 측면이 클 것으로 보인다. 반면에 솔루션 제공 기업의 입장에서는 SW 보안의 관점에서 개별적으로 접근하고 있는 상황이다.

공기업에서는 오픈소스 관점에서 대기업이 관리 및 절차를 구축하고 있다고 다음 표와 같이 보고 있다.

[표: 국내 기업들의 대응 사례]

구분	대응
A사의 경우	오픈소스 관점에서 2000년대 후반부터 오픈소스 컴플라이언스 활동을 시작하고 소스코드 내 저작권 및 라이선스 표기를 위해 SPDX 등을 선택하고 있으며, 사내 오픈소스 시스템(FoSSLight Hub)에 오픈소스 확약서와 오픈소스 BOM을 등록하고 관리하고 있다.
B사의 경우	배포용 소프트웨어에 회사의 오픈소스 컴플라이언스 프로세스에 따라 점검 도구를 활용하여 오픈소스, 3rd party proprietary software 등에 대한 Software BOM을 생성하고 있으며, 이를 3년 이상 보관하고 있다.
C사의 경우	a라는 완성 제품 안에는 SW 정보내용이 기재되어 관리되며, 협력 업체에는 자체 내부체계로 관리하고 외부제공 시에는 SPDX 체계로 변환하고 있다.
D사의 경우	2020년 전사적으로 SBOM 관련해서 오픈소스 SW 관리 정책 및 절차를 구축하고 있다.
표준화에 관한 경우	SBOM의 필요성은 궁극적으로 소프트웨어에 포함된 컴포넌트들에 대한 보안 및 라이선스 관리에 있으며 현재까지 SBOM 관련 관리도구들 역시 보안취약점 관리에서 출발하고 있다. 또한, 현재 TTA PG602(공개SW 프로젝트 그룹)에서 진행한 SBOM관련 단체 표준은 오픈체인 기반 공개 소프트웨어 공급망 관리지침, 공개소프트웨어 보안취약점 관리지침, 공개 소프트웨어 정보 교환명세가 있다.
공급기업의 경우	현재 국내 기관 및 기업에서는 소프트웨어 구성 요소에 관심을 갖고 체계적으로 관리하는 조직이 매우 드문 것으로 파악되며, 오픈소스 소프트웨어가 수정, 재구성, 재정의 과정을 거치면서 그 안에 숨겨져 있는 취약점들이 발견되지 않은 상태로 소프트웨어 공급망을 통해 확산되는 문제가 최근 큰 이슈가 되고 있다. 따라서, 관련 문제점을 인식하고 있으며 자체 솔루션 등을 기반으로 보안취약점 진단/관리 서비스를 제공중에 있다.

3. 국내 정책 현황

국내 기업의 경우, SAM(Software Asset Management) 측면의 내부 Software 자산 관리를 위해 노력하고 있지만 배포용 소프트웨어에 대한 SBOM 관리에 대해서는 아직 체계적인 정부의 관리 지침이나 표준 적용이 미흡하다. 따라서 오픈소스 SW 기반의 정책 및 절차(ex. SPDX, CycloneDX)를 활용하여 관리체계를 따르는 것이 방향으로 좋을 것으로 보인다. 이에 대응 마련은 필요할 것이며, 향후 미국과 교역하는 글로벌 소프트웨어 공급업체만이 아니라 임베디드 SW부품 등을 제공하는 제조 기업들도 원활한 비즈니스 성사를 위해 SBOM을 적극 도입할 것으로 판단됨에 따라 판매자/구매자 입장에서 균형 있는 제도 마련이 필요하다고 판단이 된다.

4. SBOM의 국내 활용 방안

SBOM에 관한 정부차원의 정의는 아직 없으며, 국내 사용 선례도 많지 않기에 보급화에 관한 혼동이 발생할 수 있다. 따라서 기술적으로 SBOM의 데이터 형식과 기본 구성요소에 관한 정립이 요구되기에 국가통신정보청(National Telecommunications and Information Administration, NTIA)에서 제시한 최소 요구사항을 통해 SBOM의 구조와 데이터 형식에 대한 구체화가 논의될 필요가 있다. 또한, SBOM을 생성하고 이를 내재화하기 위한 자동화 도구의 개발도 함께 진행되어야 할 것이다.

정부 및 민간기관에서 SBOM이 도입되기 위해서는 시간 및 비용 절감과 편리성이 요구된다. 이런 측면에서 신규 제품 개발과 업데이트 및 배포를 위한 자동화 시스템은 필수적이며, 보안 측면에서도 사람의 개입을 최소화하기에 공급망의 무결성과 투명성에 기여할 것으로 보인다.

Ⅳ. 국내 현황

다음으로 법률 및 정책을 기반으로 한 기술 분야의 요구사항 문서화가 필요하다. 이를 통해 위반 시 책임을 명시하며, 모든 기관 내 절차를 이행하기 위한 검증으로 활용될 수 있다. 따라서 국내 국가·공공기관을 대상으로 한 정보시스템에서 개발, 도입, 운영, 절차 등의 과정 내 시행중인 가이드라인과 법률에 SBOM을 명시할 방안이 요구된다.

예를 들어, 행정안전부와 한국인터넷진흥원에서 발간한 “전자정부 SW 개발·운영자를 위한 소프트웨어 개발 가이드라인(2019.11.)”은 SW 개발보안의 방법론을 제공한다. 이는 요구사항분석, 설계, 구현, 테스트, 유지보수 등의 SW 개발 생명주기에 요구되는 보안 활동을 정의하는 문서이다. 그러나 해당 문서는 공급망 보안에 관한 필수적 요구사항은 명시하고 있지 않았다. 따라서 SW 개발주기 단계별 결과물은 새롭게 생성되고 전달되는 과정이기에 산출물에 관한 무결성과 투명성에 대한 검증이 요구된다. 즉 생명주기 개발 프로세스에 SBOM을 적용한다면 구현 과정 내 소스코드 취약점 진단 및 개선 절차에서 보안 취약점을 파악하고 통제할 수 있게 될 것이다.

마지막으로 국내 정보시스템에 관한 행정규칙 중 “행정기관 및 공공기관 정보시스템 구축·운영 지침”은 전자정부법 제45조제3항에 따라 행정기관 등의 장이 정보시스템을 구축·운영함에 있어 준수해야 할 기준, 표준 및 절차와 법제49조제1항(상호운용성 확보 등을 위한 기술평가)에 따른 기술평가 관련 사항을 지정해야 한다.

법률에서 정의하는 제안요청서는 행정기관 등의 장이 입찰에 참여하고자 하는 이에게 제안서의 제출을 요청하도록 교부하는 서류이다. 이에 제안요청서에 SBOM을 적용한다면, 소프트웨어 개발보안 원칙 적용 및 요구사항 명세에 SBOM 검증 항목을 추가하는 것이다. 또한 소프트웨어 진흥법 시행령에 따른 “소프트웨어 품질인증 운영에 관한 지침”은 소프트웨어 품질인증에 관한 규제를 나열하는 제품설명서를 통해 SW 제품이 사용 목적에 적합한지 판단하는 SW 제품, 속성, 설명 등의 인증절차에서도 SBOM의 적용이 가능할 것이다.

현재 국내 민간부문에서는 오픈소스 취약점을 점검하기 위한 솔루션 개발에 SBOM을 활용하고 있지만, 이를 국가·공공기관에 도입 및 검증하는 도구로 활용한 사례는 찾기 어렵다. 따라서 해외 SBOM 추진 및 진행 현황을 통해 국내에 적용할 수 있는 활용방안이 요구되며, 국내 SBOM 도입에 관한 검토와 적극적인 활용을 위해서는 정부의 역할이 중요할 것으로 보인다. 물론 민간부문과의 협의는 필수적이며, 정부와 민간의 논의를 통한 SBOM의 보편화는 조속히 실현되어야 할 것이다.

2022
공급망 보호를 위한
SBOM 조사 보고서

V.
참 고

V. 참 고

1. SBOM 가이드, 글로벌 비즈니스 지원, NIPA 글로벌ICT 포털

2. Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM) NTIA Multistakeholder Process on Software Component Transparency Framing Working Group 2019-11-12

3. ICT 공급망 보안기준 및 프레임워크 비교 분석 (민성현, 손경호 강원대학교 대학원생, 교수) 논문

4. 소프트웨어 공급망 보안이란?, IT 보안의 이해, 토픽 RedHat (https://www.redhat.com/ko/topics/security/what-is-software-supply-chain-security)

5. 사이버안보 강화를 위한 소프트웨어 공급망 보안 정책 연구: SBOM 정책 추진 사례를 중심으로 (손효현, 김동희, 김소정 국가보안기술연구소) 논문

6. 국방 소프트웨어의 현대화 및 공급망 보안을 위한 DevSecOps 도입 방안 연구 (이승운, 류한얼, 홍수연, 김태규) 정보보호학회지 제32권 제5호, 2022. 10 논문

7. 바이든 정부의 사이버안보 정책 전망, INSS 전략보고, April 2021. No. 119

8. 미국 공급망 보안 관리 체계 분석 (손효현, 김광준, 이만희, 한남대학교) 논문

9. 美 상원, '오픈소스 SW 보안법' 상정, 보안뉴스

10. Securing Open Source Software Act of 2022 (https://www.govinfo.gov/content/pkg/BILLS-117s4913is/pdf/BILLS-117s4913is.pdf)

11. 공개 SW 가이드/보고서, 정보마당, OSS (https://www.oss.kr/oss_guide/show/bfaf10b4-ab87-4f0a-be06-c1ec2cbfb98e?page=1)

12. 'SBOM 포맷 따라잡기' SPDX와 사이클론DX의 비교, CIO Korea, 뉴스 (https://www.ciokorea.com/news/250432#csidx7ca99f1053697d695284a17d601a4b6)

13. 통합개발 프레임워크 기반 SBOM 조사 분석 연구

14. 소프트웨어 공급망 관리를 위한 글로벌 솔루션 동향 (김광준, 이만희 정보보호학회지 제32권 제5호, 2022. 10) 논문

15. 코드노토리, 오픈소스 커뮤니티 통해 SBOM 배포, 코딩월드 뉴스 (https://www.codingworldnews.com/news/articleView.html?idxno=10785)

16. 미 정부의 '개발자가 알아야 할 SW 공급망 보호 가이드' 핵심 살펴보기, CIO Korea 뉴스 (https://www.ciokorea.com/news/255616)

17. 바이든 정부의 사이버안보 정책 전망 [전자자료], 오일석

18. Analysis of U.S. Supply Chain Security Manag ement System, Son, Hyo-hyun;Kim, Kwang-jun;Lee, Man-hee; (www.koreascience.or.kr)

19. ICT 공급망 보안기준 및 프레임워크 비교 분석, Min, Seong -hyun;Son, Kyung -ho; (koreascience.or.kr)

20. 사이버안보 강화를 위한 소프트웨어 공급망 보안 정책 연구:SBOM 정책 추진 사례를 중심으로, 손효현, 김동희, 김소정

21. 미 바이든 행정부의 야심 찬 사이버보안 집행 명령, 효과가 있을까(www.itworld.co.kr)

22. 사이버보안 - ITWorld Korea (www.itworld.co.kr)

23. 미상원, '오픈소스 SW 보안법' 상정 - ZDNet korea (zdnet.co.kr)

24. SW공급망 강화를 위한 글로벌 동향 - 소프트웨어정책연구소 (spri.kr)

25. 2014 제 16 회 한국 소프트웨어공학 학술대회 논문집 - 건국대학교 [dslab.konkuk.ac.kr]

26. The Minimum Elements For a Software Bill of Materials (SBOM): Pursuant to Executive Order 14028 on Improving the Nation's Cybersecurity, The United States Department of Commerce, July 12, 2021

27. 최윤성(2022), 미국의 소프트웨어 공급망 보안 정책 동향: SBOM 사례를 중심으로, 정보보호학회지, 제32권 제5호

이 보고서는 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 보고서임 (No.2022-0-00277, SW공급망 보안을 위한 SBOM 자동생성 및 무결성 검증기술 개발 과제)

2022

공급망 보호를 위한 SBOM 조사 보고서

kisia 한국정보보호산업협회