Journal of Digital Convergence
Vol. 20. No. 2, pp. 9-20, 2022

ISSN 2713-6434 / eISSN 2713-6442
https://doi.org/10.14400/JDC.2022.20.2.009

사이버안보 강화를 위한 소프트웨어 공급망 보안 정책 연구 : SBOM 정책 추진 사례를 중심으로

손효현, 김동희, 김소정*
국가보안기술연구소

A Study on the Software Supply Chain Security Policy for the Strengthening of Cybersecurity : Based on SBOM Policy Cases

Hyo-Hyun Son, Dong-Hee Kim, So-Jeong Kim*
National Security Research Institute

요 약 공급망 공격은 주요기반시설을 타겟하여 피해 규모가 크고 공공 안전 및 국가안보를 위협하는 요소로 진화하고 있다. 이에 사이버안보 전략 및 정책 수립 시 공급망 위험관리를 명시하여 보안성을 제고하고 있으며, 2021년 美 바이든 행정부가 발표한 국가 사이버안보 강화를 위한 행정명령에서는 소프트웨어 공급망 보안 강화를 위한 지침 중 일부로 SBOM을 언급하였다. 정부 차원에서 SBOM을 의무화하여 공급망 보안 검증 도구로 활용한다면, 향후 국내 조달체계에도 영향을 받을 수 있으며 정책 시행 경과에 따라 국내 공급망 보안 체계 수립 시에도 참고 가능할 것으로 보인다. 이에 따라 본 논문에서는 소프트웨어 공급망 보안 강화 방안으로써 SBOM 정책을 추진 중인 국가를 선정하여 관련 사례를 중점으로 분석하였다. 또한, 국외 SBOM 정책 동향의 비교·분석을 통하여 국내 SBOM 도입 시 기술, 정책, 법률 측면에서의 활용 방안을 고찰하였다. 향후 공급망 무결성·투명성 검증 도구로 SBOM의 활용 가치가 기대되는바 SBOM에 대한 국제적 표준화 정립 및 정책 개발에 관한 지속적인 동향 파악과 표준 형식 개발 연구가 요구된다.

주제어 : 사이버안보, 공급망 보안, 소프트웨어 공급망 보안, 소프트웨어 자재명세서, SBOM

Abstract Supply chain attacks target critical infrastructure, causing large amounts of damage and evolving into a threat to public safety and national security. Accordingly, when establishing cybersecurity strategies and policies, supply chain risk management is specified to enhance security, and the US Biden administration recently issued the Executive Order on Improving the Nation's Cybersecurity, SBOM was mentioned as part of the guidelines for strengthening software supply chain security. If the government mandates SBOM and uses it as a security verification tool for supply chains, it can be affected by the domestic procurement system in the future and can be referenced when establishing a security system for domestic supply chains according to the progress of policy implementation. Accordingly, in this paper, countries that are promoting the SBOM policy as a way to strengthen the security of the software supply chain were selected and analyzed with a focus on related cases. In addition, through comparison and analysis of foreign SBOM policy trends, methods for using domestic SBOM in terms of technology, policy, and law were considered. As the value of using SBOM as a supply chain integrity/transparency verification tool is expected in the future, it is necessary to continuously identify trends in the establishment of international standardization and policy development for SBOM and study the standard format.

Key Words : Cybersecurity, Supply Chain Security, Software Supply Chain Security, Software Bill of Material, SBOM

*Corresponding Author : So-Jeong Kim(sjkim@nsr.re.kr)
Received November 26, 2021
Revised February 8, 2022
Accepted February 20, 2022
Published February 28, 2022

1. 서론

4차 산업혁명을 맞이하며 디지털 경제 영역이 확대되고 다양한 산업 분야에 디지털 전환을 위한 소프트웨어 산업 활성화와 함께 사이버공격 또한 진화하면서 사이버 안보를 위협하고 있다. 정보통신기술의 발전으로 제품 및 서비스의 개발·제조·유통·배포 과정이 서로 연결되고 지능화되며 업무의 생산성을 높이고 있으나, 이를 악용한 공급망 공격이 최근 빈번하게 발생하고 있다. 특히 소프트웨어 공급망 공격의 경우 정상 소프트웨어의 배포·업데이트 과정에 침투하여 악성코드를 변조하거나 삽입하며 사이버공간을 통해 빠른 전파가 이루어지는 만큼 공격 성공 시 피해 규모가 매우 크다. 미국에서 발생한 솔라윈즈 공급망 사건 및 콜로니얼 파이프라인 해킹 사건은 주요기반시설을 타겟으로 공급망 공격을 수행하여 공급 중단 및 소프트웨어 활용 국가에 대한 동시다발적 대규모 피해를 초래하였다. 공급망 공격은 개인과 조직에서 나아가 공공 안전 및 국가안보를 위협하는 사례로 그 심각성이 주목되며 공급망 보안 강화를 위한 정책 필요성이 논의되었다.

각국은 공급망 공격 사례와 위협행위들이 지속적으로 발생함에 따라 국가 사이버안보를 위협하는 요소로 인지하고 사이버안보전략 수립 및 사이버보안 정책 내 공급망 위험관리를 명시하며 공급망 보안 정책을 추진해왔다. 2021년 美 바이든 행정부는 연이어 발생한 사이버공격 사례를 기점으로 국가 사이버 방어체계를 전면 개선하고자 '국가 사이버안보 강화' 행정명령을 발표하였다[1].

상기 행정명령은 전반적으로 사이버안보 현대화를 위한 기술 추진 및 공공-민간 정보공유 강화, 침해사고 발생 대응역량 강화를 주요 골자로 구체적 지침을 명시하는 가운데 소프트웨어 공급망 보안 강화 섹션을 통해 소프트웨어 보안성을 제고하고자 하였다. 이에 소프트웨어 공급망 무결성을 검증하고 투명성을 제공하기 위한 용도로 SBOM 활용을 언급하였다. SBOM(Software Bill of Material)은 소프트웨어 자재명세서로 소프트웨어 구성요소를 목록화하여 구성요소 정보 및 종속 관계를 제공해준다. 미국은 SBOM을 의무화하여 공급망 보안성 제고를 위한 도구로써 활용하고자 하며, 이외 유럽에서도 IoT 및 ICT 제품의 공급망 보안 필요요소로 SBOM을 언급하고 있다.

이렇듯 국외는 공급망 보안의 필요성을 인지하여 사이버안보 차원에서 공급망을 관리하고자 정책을 추진 중이며, 최근 SBOM이라는 도구를 활용하여 정부기관에 도입되는 정보시스템을 대상으로 민간 및 공급업체 관점에서 접근할 수 있는 공급망 보안 강화 체계를 구축하고자 한다. 이에 반해 국내의 경우 국가사이버안보 전략 외 공급망 보안을 위한 정책이 발효되어 시행 중인 사례가 없으며 SBOM 또한 산업 내 일부 활용하고 국가·공공기관을 대상으로 적용하는 사례가 없다. 이에 본 논문에서는 선행연구로 SBOM 도입 배경 및 형식에 대하여 간략히 소개하며, 현재까지 논의된 국외 SBOM 정책 동향을 분석하여 소프트웨어 공급망 보안 강화를 위한 SBOM 활용 필요성과 향후 SBOM 정책 수립 방향성을 도출하였다. 이를 기반으로 국내에 적용 가능한 SBOM 요소와 기준을 분석하여 국내 활용방안을 제안하고자 한다.

2. 선행연구

2.1 SBOM 도입 배경

공급망 공격이 국가적 주요 사이버안보 문제로 대두되며 각국은 사이버보안 활동의 일환으로 ICT 공급망 위험관리 정책을 시행하며 안전한 공급망 환경을 구축하기 위한 제도를 마련하였다. ICT 제품 조달 시 취약점 진단 및 조치가 완료된 제품을 도입하고, 인증된 공급업체 활용을 권고하며 보안성을 제고하고자 하였다. 이외에도 보안요구사항 및 인증된 정보보호제품군을 지정하여 ICT 제품에 대한 안전성을 검증하였다.

그러자 공격자는 소프트웨어 공급망을 우회 경로로 악용하며 취약한 환경의 소프트웨어 개발·업데이트 과정 내 침투하여 악성코드를 배포하는 등의 공격을 수행하였다. 이에 인증된 제품에 대하여 추가적인 보안성 검증이 요구되었으며, 공급망 공격에 대한 탐지 및 선제적 대응, 피해 발생 후 발생 위치 파악, 피해 범위 산정, 신속한 후속 조치를 위한 방책으로 공급망 가시화 및 무결성 보증에 대한 필요성이 논의되었다.

이와 관련하여 CISQ에서 발행한 신뢰할 수 있는 시스템 선언문에서는 신뢰할 수 있는 시스템은 추적 가능해야 함이 요구되며 출처 및 신뢰에 대한 증거는 구성요소와 함께 공급망 전체에 공유되어야 한다고 명시하였다. 또한, MITRE의 국가안보 공급망을 위한 보고서에는 SBOM을 통하여 개별 요소의 위험을 기반으로 소프트웨어 구성요소의 전체 위험을 추정할 수 있다고 제언하였다. NIST는 소프트웨어 취약점 완화 백서를 통해 소프트웨어를 보호하기 위하여 소스코드 리포지토리에 저장된

소프트웨어에 대한 SBOM을 작성하고 유지 관리할 것을 권장하였다[2]. 이렇듯 소프트웨어 공급망 무결성 검증 및 정보공유, 가시화를 위한 방안으로 SBOM은 사이버 보안 관련 문건에 명시적 혹은 묵시적으로 꾸준히 언급되어왔다.

결론적으로 미국 행정명령 14028을 통하여 정부기관에 ICT 제품 조달 시 SBOM 제공 의무화가 언급되며 공급망 보안성 검증 도구로써 그 가치와 필요성이 강조되었고, 이에 각국에서도 SBOM을 활용한 공급망 보안 강화 정책 추진 사례가 나타나고 있다.

2.2 SBOM 구조 및 활용 사례

2.2.1 SBOM 정의

SBOM은 소프트웨어의 하나 이상 식별된 구성요소에 대한 정보를 제공하며 이를 통해 제품의 공급망 정보 취득이 가능하다. SBOM은 소프트웨어 시스템이 구성하는 공급망을 통해 다른 시스템의 구성요소와도 연결성·종속성을 이룰 수 있다. SBOM 작성 시 요구되는 기본 요소들은 최근 美 NTIA에서 발표한 SBOM 구조화 작업 보고서 두 번째 버전을 기준으로 작성자 이름, 타임스탬프, 공급업체 이름, 구성요소 이름, 구성요소 버전, 구성요소 해시정보, 고유 식별자, 관계성이 있다[3]. 그러나 현재 SBOM에 대한 표준화된 양식은 없으므로 개발 및 관행에 따라 추가 정보가 요구되기도 한다. NTIA에서 정의한 SBOM 구성요소에 대한 정의는 Table 1과 같다.

Table 1. SBOM Baseline Attributes[3]

Baseline	Description
Author Name	author of the SBOM
Timestamp	date and time when the SBOM was last updated
Supplier Name	name or other identifier of the supplier of a component in an SBOM entry
Component Name	name or other identifier of a component
Version String	version of a component
Component Hash	cryptographic hash of a component
Unique Identifier	additional information to help uniquely define a component
Relationship	association between SBOM components

2.2.2 SBOM 데이터 형식

앞서 서술한 바와 같이 SBOM의 경우 표준화된 형식이 존재하지 않는다. 이에 본 절에서는 일반적으로 많이 활용하고 있는 SBOM 데이터 형식 세가지를 소개하고 SBOM으로 활용 가능한 장점 및 보완점을 요약하였다. 또한, SBOM 구성요소를 각 데이터 형식에서 캡처한 정보와 매핑하여 표로 정리하였으며 예시를 통해 캡처된 정보 내 SBOM 구성요소를 식별하여 보았다.

가. SPDX

SPDX(Software Package Data Exchange)는 리눅스 재단의 SPDX 워킹그룹에서 개발한 오픈소스의 저작권 및 라이선스 정보교환 산업 표준이다[4]. 소프트웨어 패키지와 관련된 구성요소, 라이선스, 저작권 및 보안 정보를 전달할 수 있다. SPDX는 문서 생성 정보, 패키지 정보, 파일 정보, 코드 사용 정보, 기타 라이선스 정보, 관계성, 주석(SPDX 검토 및 추가 작성자)에 대한 요소들로 구성되어 SBOM 데이터로 활용 가능하다. SPDX 문서는 ISO 이미지, 컨테이너, 소프트웨어 패키지, 바이너리 파일, 소스파일 등에 포함된 코드를 나타내어 소프트웨어 요소와 문서를 매칭시켜 SBOM 메타데이터로 상호 참조할 수 있다.

그러나 SPDX 데이터를 SBOM으로 활용하여 공급망 투명성을 검증하고자 할 때 보안성 관점에서 추가로 고려해야 할 요소들이 있다. 우선 알려진 취약점 정보에 대한 업데이트 또는 패치 시기, 위치, 방법에 대한 정보가 명시되어야 한다. 또한, 관리 연속성에 따른 가계도 및 출처 정보 표기가 강화되어야 한다. 마지막으로 현재 SPDX 문서 중 SBOM으로 활용할 수 없는 사례를 식별하여 이를 지원하는 데 필요한 요소들을 판단하여 향후 반영해야 한다[5].

나. SWID

SWID(Software Identity)는 소프트웨어 정보에 대한 태그를 생성하여 장치에 설치된 상용 및 오픈소스 소프트웨어 인벤토리를 지원하는 장치이다. SWID는 ISO/IEC19770-2 표준에 의해 정의되었으며 소프트웨어 제품의 특정 릴리즈에 대한 정보를 포함하고 있다. 생성한 SWID 태그는 관리 장치에 설치된 소프트웨어를 추적할 수 있는 투명성을 제공한다[6,7].

SWID 태그는 소프트웨어 생명주기와 연계되어 소프트웨어 구성요소에 대한 식별 정보, 소프트웨어 산출물에 대한 파일 및 암호화 해시 목록, SBOM(태그) 작성자 및 소프트웨어 구성요소에 대한 출처 정보를 제공한다. 이에 따라 SWID 태그 정보는 SBOM 데이터로 활용 가능하며, 다른 SWID 태그에 링크하여 명시할 수 있어 소프트웨어의 종속 관계를 나타낼 수 있는 장점이 있다. 현

Table 2. Mapping baseline component information to existing formats[3]

Attribute	SPDX	CycloneDX	SWID
Author Name	(2.8) Creator:	metadata/authors/author	<Entity> @role (tagCreator), @name
Timestamp	(2.9) Created:	metadata/timestamp	<Meta>
Supplier Name	(3.5) PackageSupplier:	Supplier publisher	<Entity> @role (softwareCreator/publisher), @name
Component Name	(3.1) PackageName:	name	<softwareIdentity> @name
Version String	(3.3) PackageVersion:	version	<softwareIdentity> @version
Component Hash	(3.10) PackageChecksum: (3.9) PackageVerificationCode:	Hash "alg"	<Payload>/../<File> @[hash-algorithm]:hash
Unique Identifier	(2,5) SPDX Document Namespace (3.2) SPDXID:	bom/serialNumber component/bom-ref	<softwareIdentity> @tagID
Relationship	(7.1) Relationship: DESCRIBES CONTAINS	(Inherent in nested assembly/subassembly and/or dependency graphs)	<Link> @rel, @href

재 SWID 태그는 XML 형식으로 제공되어 용량이 크기 때문에, 향후 CBOR(Concise Binary Object Representation)을 기반으로 경량화된 SWID 태그 정보를 제공할 수 있는 CoSWID의 사용도 기대되는 바이다[4].

다. CycloneDX

CycloneDX는 애플리케이션 보안 컨텍스트 및 공급망 구성요소 분석에 사용하도록 설계된 경량 SBOM 표준이다[7]. 이는 오픈소스 웹 애플리케이션 보안 프로젝트(OWASP)에 의해 개발되었으며 소프트웨어 보안 요구사항 및 위험 분석을 위해 설계되었다.

CycloneDX는 JSON, XML 언어로 작성되며 빌드 시스템에 구현하여 유연하고 쉽게 채택하여 활용할 수 있다. BOM에 대한 메타데이터를 제공하여 제공업체 정보, 라이선스 및 저작권 정보, 구성요소 간의 종속성 등을 통해 SBOM 역할을 지원한다. 현재 CycloneDX 공식 홈페이지를 통하여 CycloneDX 소프트웨어를 배포하고 있으며 다양한 활용 예시를 제공한다[9].

2.2.3 SBOM 적용 예시

소프트웨어 개발 시 산출된 결과물을 기반으로 기준을 지정하여 SPDX, SWID 및 CycloneDX 데이터 형식을 SBOM에 적용하고자 할 때 매핑 가능한 요소를 선정하였다. 작성자 이름, 타임스탬프, 공급업체 이름, 구성요소 이름, 구성요소 버전, 구성요소 해시정보, 고유 식별자, 관계에 대한 정보를 기반으로 SPDX, SWID 및 CycloneDX에서 해당 정보를 담고 있는 속성 명을 예시로 Table 2를 작성하였다[3].

세 가지 데이터형식 모두 SBOM 활용에 있어 식별 가능한 정보를 제공하기에 상호 보완을 통하여 공통된 표준 형식을 도출하는 연구도 필요할 것으로 보인다. 이때 앞서 언급한 것과 같이 취약점에 대한 정보 및 사전 위협 식별 정보 등 공급망 보안을 위한 추가 고려사항을 포함하여 표준화된 SBOM 양식 개발이 요구된다.

추가로 SBOM 정보 제공 개념 증명 보고서에 제공된 SWID 예시 데이터를 기반으로 SBOM에 대한 정보를 식별하여 보았다(Fig. 1)[10]. Fig. 1에 형광으로 표시한 태그 정보를 Table 2의 SWID 형식과 매핑하여 보면 SWID 데이터를 통하여 SBOM 정보가 식별 가능함을 확인할 수 있다. 본 예시 SWID 데이터에는 태그 생성자 및 역할(name, role), 생성 정보(Meta), 소프트웨어 개발자(name), 구성요소 이름(name), 버전(version), 해시값(hash), 식별자(tagId), 관계 정보(rel, href)가 제공되었다.

```
<SoftwareIdentity
xmlns="http://standards.iso.org/iso/19770/-2/2015/schema.xsd" name="ACME
Roadrunner Detector 2013 Coyote Edition SP1"tagId="com.acme.rrd2013-ce-sp1-v4-1-
5-0" version="4.1.5">
        <Entity name="The ACME Corporation" regid="acme.com" role="tagCreator
        softwareCreator"/>
        <Link rel="license" href="www.gnu.org/licenses/gpl.txt"/>
        <Meta product="Roadrunner Detector" colloquialVersion="2013"
        edition="coyote" revision="sp1"/>
        <Payload>
                <File name="rrdetector.exe" size="532712"
                SHA256:hash="a314fc2dc663ae7a6b6bc6787594057396e6b3f569
                cd50fd5ddb4d1bbafd2b6a"/>
</Payload>
</SoftwareIdentity>
```

Fig. 1. Example SWID SBOM[10]

Table 3. Software Bill of Materials – Perspectives and Benefits[2]

	Perspective on Software		
Benefit	**Produce**	**Choose**	**Operate**
Cost	Less unplanned, unscheduled work	A more accurate total cost of ownership	More efficient administration
Security Risk	Avoid known vulnerabilities	Easier due diligence	Faster identification and resolution. Know if and where specific software is affected
License Risk	Quantify and manage licenses and associated risk	Easier due diligence	More efficient, accurate response to license claims
Compliance Risk	Easier risk evaluation. Identify compliance requirements earlier in lifecycle	More accurate due diligence, catch issues earlier in lifecycle	Streamlined process
High Assurance	Make assertions about artifacts, sources, and processes used.	Making informed, attack-resistant choices about components.	Validate claims under changing and adversarial conditions.

2.3 SBOM 활용방안

NTIA에서 발행한 '공급망 전반에 걸친 SBOM의 역할 및 이점'에 관한 보고서에서는 소프트웨어의 생성, 선택, 운영의 관점에서 SBOM 활용방안 및 가치에 대하여 서술하였다. 요약정리한 내용은 Table 3과 같이 나타낼 수 있으며, 일례로 보안 위험 측면에서 이점을 확인하여 보면 다음과 같다[2].

먼저 소프트웨어 생산 시 SBOM을 활용할 경우 소프트웨어 내 취약점에 대한 구성요소 모니터링이 용이하여 새로운 보안 위험이 발견될 경우 잠재적 취약성 판단이 가능하다. 또한, 소프트웨어 선택 시 SBOM을 통해 소프트웨어 전반에 대한 잠재적인 위험 요소를 식별하여 사전 위험분석을 수행할 수 있으며, 구성요소의 아웃소싱 정보 등을 확인해 검증을 통한 도입이 가능하다. 운영자는 소프트웨어 취득 이후 설치, 구성, 유지관리를 수행해야 하는데 이때 SBOM 활용이 가능하다. 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.

이렇듯 소프트웨어 공급망의 보안 관리 관점에서 다각도로 활용 가능한 SBOM의 효용성을 살펴보았다. 향후 공급망 보안 증진을 위한 추가 요구사항을 반영하여 표준화된 양식 개발 및 배포로 SBOM이 활성화된다면, 공급망 내 다양한 이해관계자 사이에 의사소통 및 운용절차에 있어 일관성 있는 정보 제공과 공유가 가능한 긍정적인 효과가 기대되는 바이다.

3. 국외 SBOM 정책 추진 동향

3.1 미국

미국은 2014년부터 SBOM 관련 법안 및 정책을 추진해왔으며, 2018년 NTIA는 소프트웨어 구성요소 투명성을 위한 다중 이해관계자를 소집하였다. 이후 현재까지 SBOM에 관한 연구를 지속하며 정책 수립을 위한 활동을 이어가고 있다. 본 절에서는 미국의 SBOM 추진 현황을 조사하였으며, NTIA 발행 문건 및 SBOM 관련 행정명령 현황과 FDD에서 발행한 위험관리를 위한 SBOM 중요성 보고서를 소개한다.

3.1.1 NTIA Software Component Transparency

NTIA는 소프트웨어 구성요소 투명성 연구를 위하여 2018년 다중 이해관계자 프로세스를 구성하였다. 이때 구조화(Framing), 관행 및 사용 사례(Practices and Use Cases), 표준 및 형식(Standards and Formats), 의료 개념 증명(Healthcare Proof of Concept) 그룹으로 나누어 연구를 수행하였다.

표준 및 형식 그룹은 '기존 SBOM 형식 및 표준 조사' 보고서를 발행하였으며, 이는 SBOM용 소프트웨어 제품 구성에 사용되는 외부 구성요소 및 공유 라이브러리 식별에 적용되는 기존 표준, 형식 및 이니셔티브에 대한 요약을 제공하였다[5]. 또한, SBOM 데이터를 기계가 읽을

수 있는 방식으로 정보를 전달하는 것과 관련하여 다른 그룹에서 진행 중인 노력에 대하여 분석하였다. SBOM에 요구되는 향후 방향성에 대하여 다음과 같이 서술하였다.

- 소프트웨어 식별자 문제: 소프트웨어 구성요소를 명확하고 고유하게 식별하는 '기본키'가 요구된다.
- 도구 문제: SBOM을 더 광범위하게 채택하기 위하여 자동화가 필요하며 이에 활용 가능한 도구가 요구된다.
- SBOM 제공 및 배포 문제: 소비자가 지정된 연락처(예: sbom-request@example.com 또는 http://example.org/sbom)를 통하여 공급업체로부터 SBOM을 제공 받을 방법의 표준화가 필요하다. 이때 SBOM 자체의 데이터 라이선스를 고려해야한다.
- 소프트웨어 구성요소 수정: 공급업체는 특정 소프트웨어 구성요소를 사용하여 특정 부분에 대한 수정을 진행할 수 있으며, SBOM 데이터 소비자는 기본 코드베이스 정보를 요청할 수 있기에 변경 및 수정사항에 대한 문서화가 요구된다.
- 높은 신뢰와 출처를 위한 SBOM 형식: SBOM 구성요소를 확인하기 위하여 관리 공급망 또는 이전 기록에서 구성요소를 추적할 수 있어야 한다, 이러한 평가를 수행하기 위한 요구 정보의 표준화는 연구가 필요하다.

관행 및 사용 사례 그룹은 '공급망 전반에 걸친 SBOM의 역할 및 이점'에 관한 보고서를 발행하여 소프트웨어 개발자, 구매자, 운영자의 관점에서의 SBOM 역할 및 이점에 대하여 요약 제공한다[2]. 이는 보안, 품질, 효율성 및 기타 조직의 이점뿐 아닌 공급망 전반에 걸친 광범위한 SBOM의 잠재력을 보여준다.

구조화 그룹은 '소프트웨어 구성요소 투명성 구조화: 공통 소프트웨어 재료명세서(SBOM) 구축'에 관한 보고서를 발행하였다[3]. 산업부문 전반에 보편적이고 투명하게 공유할 수 있는 소프트웨어 구성요소 정보에 대한 모델 생성을 목표로, SBOM 개념 및 관련 용어를 정의하고, 소프트웨어 구성요소 표현의 기본 요소를 제공하여 SBOM 생성 프로세스에 관해 설명하였다. 최근에는 기존 요소에 대하여 타임스탬프를 추가하고, 데이터형식으로 CycloneDX를 추가하였으며, 요구사항을 구체화한 한 업데이트 버전을 공개하였다. 이를 통해 첫 번째 보고서 발간 이후 피드백 및 다른 그룹들의 활동 결과물을 반영하여 SBOM 프로세스를 제공한다.

이후 NTIA는 2020년 표준 및 형식 그룹과 관행 및 사용 사례 그룹에 대한 활동을 종료하고 형식 및 도구(Formats and Tooling)와 인식 및 채택(Awareness and Adoption) 그룹을 신설하였다. 이들은 이전 그룹 활동에서 나아가 SBOM 생성 및 활용에 대한 자동화 방안 연구에 중점을 두어 진행하며, SBOM 기존 도구를 카탈로그화 하고 데이터 형식의 변환이 가능한 도구를 개발하고자 한다. 또한, SBOM의 채택과 활성화를 위하여 부문, 조직 등에 대한 명시적인 비즈니스 사례를 제시하며 적극적인 지원 활동을 수행한다.

3.1.2 행정명령 14028: Improving the Nation's Cybersecurity

미 정부는 2021년 5월 '국가 사이버안보 강화' 행정명령 14028을 발표하며, 소프트웨어 공급망 보안 강화를 공표하였다[1]. 본 지침에는 NTIA가 행정명령 발표 60일 이내에 SBOM의 최소 구성요소를 제공하여야 하며, NIST는 90일 이내에 구매자에게 각 제품에 대한 SBOM을 직접 제공 또는 공공 웹사이트에 게시해야하는 강화된 지침을 포함하여야 한다. 행정명령 발표 이후, SBOM 관련 지침에 대한 진행 현황을 확인하였다.

먼저 60일 이내에 발표되어야 했던 SBOM 최소 구성요소 문건은 NTIA에서 2021년 7월 12일 'SBOM의 최소 구성요소(The Minimum Elements For a Software Bill of Materials(SBOM))' 보고서로 제공하였다[11]. 본문에서는 SBOM의 최소 구성요소로 데이터 필드, 자동화지원, 관행 및 절차를 명시하였으며 정의는 다음과 같다.

- 데이터필드: 추적 대상 구성요소에 대한 기본 정보(공급자, 구성요소 이름, 구성요소 버전, 기타 고유 식별자, 종속 관계, SBOM 데이터 작성자, 타임스탬프)를 문서화해야 한다.
- 자동화 지원: 자동 생성 및 기계 가독성을 이용하여 자동화를 구현하고 소프트웨어 생태계 전반에 걸쳐 확장할 수 있다. SBOM 생성 및 활용 데이터 형식은 SPDX, CycloneDX, SWID 태그가 있다.
- 관행 및 절차: 빈도, 깊이, 배포 및 제공, 접근 제어, 인지된 불확실성 정보, 오류 조정을 포함한 SBOM 요청, 생성 및 운영 활동을 정의한다.

NIST는 라벨링 프로그램에 사용할 수 있는 소비자 소프트웨어 기준 초안을 2021년 11월 1일에 발표하였다. 이는 현재 기존 소비자 소프트웨어 및 IoT에 대한 라벨링 프로그램 기준을 개발하였으며, 향후 지침에는 구매

자에게 SBOM 제공 등 소프트웨어 보안 강화를 위한 방안을 추가할 예정이다. 또한 NIST는 기존의 공급망 위험관리 가이드라인인 SP 800-161 문서의 개정 작업을 진행 중이며, 본 문건 내에도 공급망 보안 강화를 위한 지침으로 SBOM 정보가 포함될 예정이다.

3.1.3 FDD 'A Software Bill of Materials Is Critical for Comprehensive Risk Management'

FDD(Foundation for Defense of Democracies)는 미국 민주주의수호재단으로 비영리 싱크탱크 기관이다. FDD TCIL(Transformative Cyber Innovation Lab)은 SBOM의 유용성에 대하여 공공 및 민간부문의 이해를 돕고자 직접 SBOM을 개발하고 분석한 결과 보고서 '포괄적인 위험관리를 위한 SBOM의 중요성'을 공개하였다[12].

TCIL은 솔루션 파일럿을 통하여 SBOM을 개발하여 분석을 수행하였다. 1단계로 소프트웨어를 식별하였으며, 국방부에서 사용하는 타사 소프트웨어 프로그램을 선택하여 진행하였다. 2단계는 데이터 다운로드 및 SBOM 생성으로 공개적으로 사용 가능한 파일을 다운로드하여 소프트웨어 공급망을 전문으로 하는 ION Channel의 자동화 프로세스를 사용하여 SBOM을 생성하였다. TCIL은 행정명령 14028에 따른 SBOM 최소 구성요소가 발표되기 이전에 파일럿을 수행하였으나 NTIA가 공개한 최소 구성요소 중 데이터필드 기본사항들과 자동화 및 프로세스에 대한 권장사항을 충족하였다. 3단계로 SBOM 분석이 진행되는데 NTIA 권장 최소 요건으로 SBOM을 구성한 이후 데이터를 스캔하여 전체 소프트웨어 패키지와 중첩되는 구성요소 소프트웨어에 대한 분석을 수행하였다. 그 결과로 의사결정자는 소프트웨어에 대한 분석 정보를 취득 가능하며 이를 기반으로 위험관리 계획 수립이 가능하다. 마지막 4단계는 이러한 SBOM의 무결성을 보증하고 제공하기 위하여 블록체인을 활용하여 SBOM 내용 및 변경 이력, 출처에 대한 기록을 생성하여 전달하였다. 이를 통해 변경 사항에 대한 새로운 블록 및 해시값 생성 여부를 기존 사항과 비교하여 무결성 검증이 가능하였다.

이렇듯 직접 실험을 통해 SBOM의 유용성을 검증한 FDD TCIL은 실험 결과를 기반으로 NTIA와 NIST에 몇 가지 권장사항을 제안하였다.

- SBOM 지침의 지속적인 업데이트: SBOM이 새로운 데이터 형식에 통합 가능한 유연성이 요구되며, 감사의 불변함과 확장성을 갖도록 하는 지침을 발행해야한다. 기계 가독성이 보장되어야 하며 지속적으로 모니터링 할 것을 권장한다. 또한, SBOM 지원 시스템구조에 대한 아키텍처 및 설계에 있어 제로트러스트 개념 적용방안을 연구해야한다.
- 민간부문의 SBOM 이해장려 및 활용 권고: 파일럿을 통하여 SBOM 활용의 상대적 용이성과 중요성을 확인하였지만 현재 민간부문에서 SBOM은 다소 알려지지 않은 생소한 개념이다. 이에 따라 SBOM 관련 정책 형성을 위한 민간 및 공공 작업 그룹 형성을 위해 미 정부의 지원이 요구된다. 또한, SBOM에 대한 지속적인 모니터링을 수행할 수 있도록 민관 파트너십을 구축해야한다.
- 모든 관련 정부 계약 내 SBOM 요구사항 포함: SBOM 활용의 가장 즉각적인 방안은 SBOM 계약 언어로 FAR 및 DFARS를 업데이트 하는 것이다. 그러나 즉각적인 규제 업데이트 보다는 단계적접근 방법으로 진행하여야 업계에서도 인정 받을 수 있을 것으로 보여진다. 연방 정부부처 및 기관을 대상으로 적용 가능한 부분에 SBOM 요구사항 제출 시범 운영을 권장한다.

3.2 EU

유럽은 ENISA에서 발행한 IoT 보안을 위한 가이드라인 문서 내에 공급망 보호를 위한 모범 사례로 SBOM 제공을 제안하며 공급망 보안을 위한 활동에 SBOM 활용 가능성을 언급하였다. 또한, 네덜란드 NCSC는 사이버보안 강화를 위한 SBOM 사용보고서를 통해 미국 및 유럽의 SBOM 활용 현황과 향후 방향성에 대한 연구를 수행하였다.

3.2.1 ENISA 'Guidelines for Securing the IoT'

ENISA는 2020년 11월 'IoT 보안을 위한 지침'을 발행하였다[13]. 본 보고서는 IoT 공급망 단계를 분석하여 단계별 주요 사이버보안 과제를 제안하고, IoT 공급망을 타겟으로 하는 주요 사이버보안 위협을 식별하였다. IoT 공급망 전반에 걸쳐 보안을 적용하기 위한 조치를 판단하고 위협 및 공급망 단계에 매핑하였다. 이를 통해 IoT 공급망을 보호하는 IoT 이해관계자가 활용 가능한 지침 개발을 목적하였다.

ENISA는 다양한 IoT 공급망 보안 위협에 대하여 보안 개선을 위한 모범사례를 선정하였고, 프로세스 부문

에서 13번째 제안내용으로 'IoT 장치용 SBOM 제공'을 명시하였다. 본문 내에서 SBOM은 제품에 대한 가시성을 높이고 제조업체와 외부 사용자 모두가 알려진 취약점을 확인하고 보안 관점에서 장치를 검증할 수 있도록 하여 공격자가 취약점을 악의적으로 활용하지 못하도록 통제하는 역할을 한다. 또한, 제품에 대한 가시성을 제공하여 공급망 관계자 내 신뢰도를 향상시킨다. 이렇듯 SBOM을 통해 구성관리 및 버전 관리 시스템을 구현하고, 추적성을 개선하여 사용자 및 조직이 소프트웨어 버전을 자유롭게 활용할 수 있도록 지원해야 함을 제안했다.

3.2.2 네덜란드 NCSC 'Using the Software Bill of Materials for Enhancing Cybersecurity'

네덜란드 NCSC는 사이버보안의 현황에서 잠재적 목적 및 SBOM 사용 현황을 조사하였고 이를 바탕으로 '사이버보안 강화를 위한 SBOM 활용' 백서를 발행하였다. 본문은 소프트웨어 생산, 선택 및 조달, 운영, SecDevOps의 관점에서 SBOM의 보안 가치를 제공하며, 취약점 탐지를 위한 방안을 소개한다[14].

소프트웨어 생산에서 SBOM은 생성 및 유지관리 관점에서의 필요성을 언급한다. 소프트웨어의 일관성있는 투명성을 보장하고자 SBOM은 제품 문서의 일부로 릴리즈된 모든 소프트웨어 제품 버전에 대하여 제공되어야 함을 강조하였다. 또한, 개발 시 보안 강화를 위해 동일한 라이브러리의 여러 다른 버전의 생성을 감소시켜 다양성을 줄이고 종속성에 따른 상속된 코드의 취약점을 사전 평가할 수 있도록 해야 한다.

소프트웨어 구성요소 선택 프로세스 내에서는 일반적으로 정보수집 및 선택 과정에서 여러 단계를 활용한다. 이때 주요 고려사항은 소프트웨어 구성요소의 보안 취약성에 따른 조직에 미치는 영향 파악이다. SBOM을 활용하여 취약성에 대한 사전 검증을 진행함으로써 보안 설정 및 위협 분류가 가능하다.

소프트웨어 운영 시 잠재적으로 취약한 소프트웨어 구성요소에 대하여 IT 환경에 따른 지속적인 평가가 요구된다. 이를 통해 조직 내 위험을 자체적으로 관리가능하며 SBOM과 CVE의 정보를 자동화로 대조하여 매핑되는 취약점을 식별하고 관리 가능하다. 이때 소프트웨어 구성요소에 대해 검증 가능한 데이터 형식 및 호환 가능한 데이터 값을 통해 진행할 수 있어야한다.

마지막으로 소프트웨어의 SecDevOps 관점은 기본적으로 생산 및 운영에 대한 부분을 결합하여 일컫는다. 소프트웨어 개발 과정에서 SBOM을 생성하고 특정 라이브러리에 대한 설명을 포함하고 있으며, 작업 시에는 SBOM의 모니터링을 통해 파악된 내용에 대한 업데이트가 필요하다.

이외에도 본 보고서는 SBOM을 이용하여 취약점을 탐지하고 공급망 공격을 식별하기 위한 핵심 요소들로 다음을 선정하였다.

- SBOM의 온라인 및 오프라인 가용성
- 활용 목적에 따른 SBOM 정보 제공
- 보안 평가시 요구되는 SBOM 정보 요소
- 기본 SBOM 데이터형식의 CycloneDX 활용
- 보안 식별 강화를 위한 자동화 및 도구

이렇듯 네덜란드 또한 SBOM의 필요성을 인지하고 자국 내 공급망 및 소프트웨어 보안 관점에서 SBOM 활용방안을 고안하고자 해외 정책 현황 파악 및 SBOM 활성화를 위한 연구를 진행 중이다.

3.3 국외 정책 동향 비교·분석

앞서 미국과 유럽의 정책 동향 연구 내용을 바탕으로 공급망 보안 강화를 위한 SBOM의 필요성을 분석해보았다. 또한, 국외 정책을 비교하여 SBOM의 향후 추진 방향성 및 추가 보안 요구사항을 요약하였다.

먼저 국외 정책 분석 결과 SBOM은 공급망 보안 관리 방안으로 무결성과 투명성을 입증할 수 있는 도구로써 가치 있는 제도임을 확인하였다. 문건들이 기술한 사항을 조합해 보았을 때 SBOM의 핵심 기능은 소프트웨어 구성요소 식별을 통한 인지와 가시성 제공이다. 이는 SBOM 데이터를 통해 공급망 내 취약점 데이터베이스와 매핑을 진행하는 것부터 여러 데이터 소스와의 상관관계 분석을 통해 정의된 위협에 대한 지속적인 모니터링까지 공급망 보안 관리 전반에 활용 가능하다. 또한, 조직 내 위험관리 활동에서 SBOM 분석 결과를 바탕으로 위험을 식별하고 우선순위를 지정하여 관리할 수 있는 이점을 가진다.

공통적으로 SBOM을 소프트웨어 생명주기 전반에 사용하여 제품에 대한 투명성을 높이고 취약점 식별 및 보안 계획 수립에 활용을 강조하였다. 이를 크게 세가지 관점에서 분석하면, 우선 소프트웨어 개발(개발자) 단계에서 SBOM의 자동 생성과 내재화를 통해 배포 및 전달이 용이할 수 있도록 추진해야 한다. 다음으로 소프트웨어 선택(구매자) 시 SBOM 정보를 활용하여 사전 위협 분석 및 구성요소 내 취약점을 식별하여 관리 방안을 수립할 수 있다. 마지막으로 소프트웨어 운영(운영자) 시 유지관리 활동 전반에 SBOM을 이용하여 취약점에 대한 지속

적인 모니터링과 변경사항에 대한 업데이트가 가능하도록 해야 한다.

SBOM 필요성이 구체화되고 각국 내 활용방안이 논의되고 있는 시점에서 이를 비교하여 향후 SBOM 활성화를 위한 고려사항을 단계별로 서술하였다. 첫째, SBOM의 국제적 표준 정립이 필요하다. 현재 SBOM에 대한 표준 형식이 존재하지 않아 개발과정 및 보안 요구사항에 따라 추가로 요구되거나 불필요한 SBOM 구성요소가 혼재되어 있을 수 있다. 따라서 제품 보안등급 및 취급 구성요소 등의 기준을 지정하고, 기준에 따른 최소한의 SBOM 구성요소를 개발하여 SBOM 생성과정에서 혼란 없이 일관성있는 정보 생성이 가능하도록 해야 한다. 둘째, 정부 및 국가적 차원에서 SBOM 표준화에 따른 정책 수립이 요구된다. 이를 위한 세부적 단계 뒷받침이 요구되는데 순차적으로 다음과 같이 정리할 수 있다.

- 기존 SBOM 생성 도구에 대한 카탈로그화 추진
- SBOM 데이터형식의 통합 및 변환 가능한 도구 개발(자동화 지원)
- 통합 및 도구 개발 상황에 따른 SBOM 지침 업데이트
- SBOM 배포 및 활성화를 위한 정부차원의 민간부문 SBOM 활용 권고 및 장려 정책 시행
- 정부 조달 계약 내 SBOM 요구사항 명시

셋째, SBOM 무결성·신뢰성 검증 및 강화를 위한 계획 수립이 필요하다. SBOM 제공 및 배포 과정에서 디지털 서명과 공개키 기술을 활용하여 SBOM 정보에 대한 변조를 감지할 수 있으며 블록체인을 활용하여 내용 변경 이력 및 출처에 대한 해시값을 기록하여 원본과의 대조가 가능할 것이다. 이를 기반으로 보안성은 더욱 강화하고 무결성을 입증하여 향후 공급망 관리 도구로의 SBOM 활성화를 기대한다.

4. 국내 SBOM 활용방안

본 장에서는 국외 SBOM 정책 분석 내용을 바탕으로 국내의 소프트웨어 공급망 보안에 채용 가능한 요소 및 제안점을 식별하였다. 이를 기술분야에 도입 가능한 부분과 법률 및 정책분야에서 확립해야 할 부분을 구분하여 국내 SBOM 활용방안을 제안하고자 한다.

먼저 기술분야 경우 SBOM 데이터형식 선별 및 기본 구성요소 정립이 요구된다. 국내에 SBOM에 대한 사용 선례가 많지 않으며, 정부차원에서 정의한 내용이 없기에 국내에 SBOM을 보급화하고자 할 때 혼동이 발생할 수 있다. 이에 NTIA의 SBOM 최소 요구사항을 적극 활용하여 SBOM 구조 및 데이터형식에 대한 구체화가 필요하다. 또한, SBOM 생성 및 소프트웨어 내재화를 위한 자동화 도구 개발이 필요하다. 정부 및 민간기관이 SBOM을 도입하여 운용하기 위해서는 시간 및 비용의 절감과 편리성이 보장되어야 한다. 이런 측면에서 자동화 시스템은 새로운 제품 개발과 업데이트 및 배포 절차에 필수 요소 중 하나이며, 보안 측면에서도 사람의 개입을 최소화하여 공급망 무결성과 투명성 입증에 용이하다.

다음으로 기술분야의 요구사항을 문서화하고 검증을 통해 위반 시 책임을 명시하며, 모든 기관 내 절차를 이행하기 위해서는 법률 및 정책이 기반되어야 한다. 이에 국내에서 국가·공공기관을 대상으로 정보시스템 개발·도입·운영 절차 내 시행 중인 가이드라인과 법률들을 대상으로 SBOM 활용을 명시할 수 있는 방안을 모색하였다.

먼저 행정안전부와 한국인터넷진흥원에서 발간한 “전자정부 SW 개발·운영자를 위한 소프트웨어 개발 가이드라인(2019.11.)”은 소프트웨어 개발보안에 방법론을 제공하는 문서이다[15]. 이는 소프트웨어 개발 생명주기(요구사항분석–설계–구현–테스트–유지보수)에 거쳐 요구되는 보안활동을 정의하고 있으며 각 단계별 수행 절차는 다음과 같다.

요구사항분석 단계는 고객의 보안요구사항에 대한 명세서를 작성하고 필요에 따른 보안 활동은 추가한다. 이후 요구사양서와 설계단계에서 산출한 설계사양서를 기반으로 사용자 지침서 및 시험 계획서를 작성하며 한다. 설계 및 계획이 완료되면 이를 바탕으로 프로그래밍을 통해 프로그램을 구현한다. 표준코딩정의 또는 소프트웨어 개발보안가이드를 준수하며 개발완료 후 완성된 결과물에 대한 테스트를 수행한다. 개발된 모듈에 대한 요구사항 및 오류사항을 테스트함으로써 최종적으로 소프트웨어의 안전성이 보장되는지 확인한다. 개발한 소프트웨어가 배포된 이후에도 발생가능한 보안사고에 대하여 관리 및 대응을 위한 유지보수 단계 또한 중요한 보안활동 중 하나이다.

이와 같이 기존의 가이드라인 내에는 소프트웨어 개발 과정에서 기본적으로 준수해야하는 보안활동 및 절차를 나열하고 있다. 그러나 공급망 보안성 검증에 대한 필수적 요구사항이 명시되어 있지 않음을 확인할 수 있다. 소프트웨어 개발주기 단계별로 새롭게 생성된 결과물이 전달되는 과정이므로 산출물에 대한 무결성 및 투명성에 대한 추가적 검증이 요구된다. 이에 따라 SBOM을 소프트웨어 공급망 보안성 검증에 활용하고자 국외 사례를

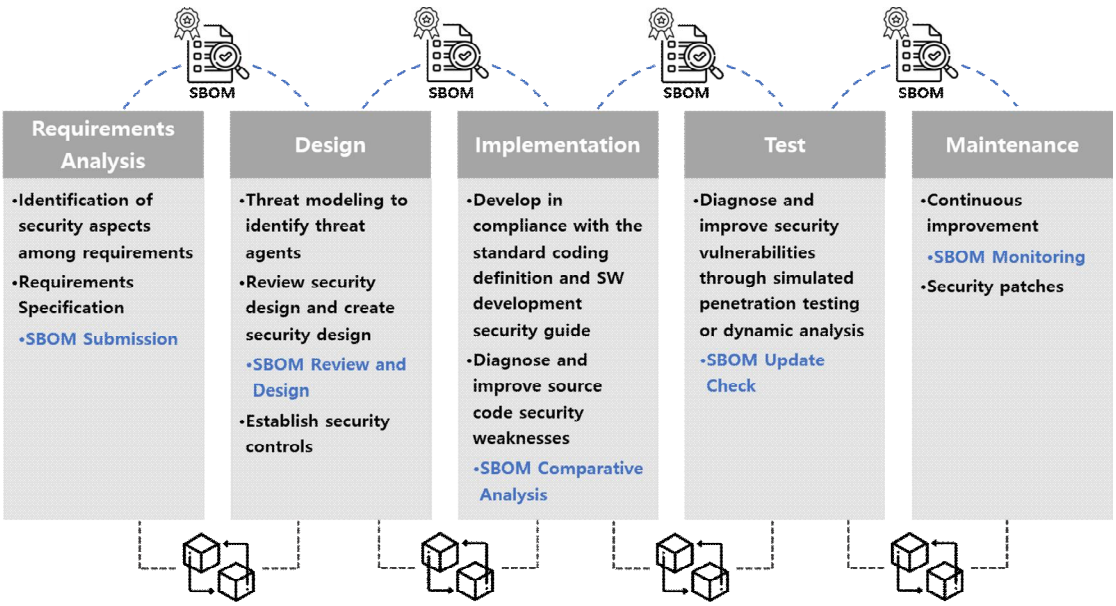

Fig. 2. SW development security methodology using SBOM

기반으로 소프트웨어 개발 가이드라인에 적용해보았으며 Fig. 2와 같이 제안하는 바이다.

우선 요구사항분석 과정에 있어, SBOM 문서 제출을 명시하여 요구사항 명세서와 함께 제공할 수 있도록 권장한다. 설계 단계에서는 보안 설계 검토 및 보안 설계서 작성 진행 시에 SBOM을 검토하고 추가 요구사항을 반영하여 진행한다. 이후 구현 과정 내 소스코드 취약점 진단 및 개선 절차에서 사용하는 소스코드의 SBOM 검증을 통해 보안 취약점을 파악하여 통제할 수 있도록 한다. 이후 테스트 과정 내 업데이트된 취약점은 없는지 SBOM과 연계하여 추가로 확인한다. 마지막 유지보수 절차는 SBOM을 함께 활용하며 지속적인 모니터링을 유지하고 발견된 취약점 및 유지보수 된 정보에 대한 업데이트가 요구된다. Fig. 2와 같이 개발 생명주기 전 과정 내에서 SBOM은 지속적으로 제공 및 전달을 통해 활용이 되어야 하며, 해당 과정에서 무결성을 보장하기 위하여 앞서 제안한 디지털 서명 및 공개키 기반으로 작성할 것을 권고하며, 블록체인을 이용한 방법도 고려하여야 한다.

다음으로 국내 정보시스템에 관한 행정규칙 중 “행정기관 및 공공기관 정보시스템 구축·운영 지침”은 전자정부법 제45조제3항에 따라 행정기관등의 장이 정보시스템을 구축·운영함에 있어 준수해야 할 기준, 표준 및 절차와 법제49조제1항(상호운용성 확보 등을 위한 기술평가)에 따른 기술평가 관련 사항을 지정해야 한다[16]. 본 지침에서는 “제안요청서” 부분을 중점으로 SBOM을 적용해보고자 한다. 법률에서 정의하는 제안요청서란 행정기관등의 장이 입찰에 참여하고자 하는 자에게 제안서의 제출을 요청하기 위하여 교부하는 서류를 말한다. 제안요청서의 작성요소 중 소프트웨어 개발보안 원칙 적용 및 요구사항 명세에 SBOM 검증 항목을 추가한다. 추가로 소프트웨어 진흥법 시행령에 따른 시행규칙인 “소프트웨어 품질인증 운영에 관한 지침”은 소프트웨어 품질인증에 대한 규제를 나열하는데 제품설명서를 통하여 소프트웨어 제품이 사용 목적에 적합한지 판단하기 위한 소프트웨어 제품 속성 설명 문서 등을 인증하는 절차에서 또한 SBOM의 적용이 가능할 것으로 보인다.

현재 국내에는 민간부문에서 오픈소스 취약점을 점검하기 위한 솔루션 개발방안으로 SBOM을 활용한 사례는 있으나, SBOM을 국가·공공기관에 도입 및 검증 도구로 활용하는 사례는 없는 것으로 보인다. 이에 따라 국외 SBOM 추진현황을 바탕으로 국내에 적용 가능한 요소들을 식별하고 활용방안을 제안하였다. 연구결과를 기반으로 국내 SBOM 도입에 대한 긍정적인 검토 및 적극적인 활용을 위해서는 정부의 역할이 중요할 것으로 보인다. 그러나 SBOM의 실현을 위해서는 무엇보다 개발 및 배포를 진행하는 민간부문과의 협의가 이루어져야할 것이며, 추가 고려사항 및 보안사항에 대해 정부와 민간부문

의 논의를 통해 보편적 사용을 위한 SBOM 산출물이 도출되어야 할 것이다.

5. 결론

정보통신기술의 발전은 사이버공격의 지능화 또한 이루었으며, 특히 소프트웨어 공급망 공격의 경우 대규모 피해를 초래하며 국가안보를 위협하는 사례로 증가하고 있다. 이에 각국은 사이버안보 강화를 위한 목적으로 소프트웨어 공급망 보안 정책 수립하였다. 미국은 연이은 공급망 공격에 따라 국가 사이버안보 강화를 위한 행정명령을 발표하였으며, 소프트웨어 공급망 보안 강화를 위한 도구로 SBOM을 언급하였다. SBOM은 소프트웨어 공급망의 가시성을 제공해주며 무결성을 검증할 수 있는 도구이다. 미국 외에도 공급망 보안성 제고를 위한 도구로 SBOM 활용성을 언급하는 문건이 발행됨에 따라, 그 필요성을 인지하고 국외 SBOM 정책 수립 동향에 따른 국내 조달체계에 미치는 영향과 추후 국내 공급망 보안 수립 체계 시 참고 자료로 활용 가능하기에 본 연구를 수행하였다.

안전한 사이버 환경 및 글로벌 ICT 공급망 복원을 강화하기 위하여 정부·민간·학계의 협력을 통하여 국제적 표준화 정책 수립 활동 및 국내 환경에 적합한 공급망 보안 정책 수립, 민간기업 내 적용가능한 실질적 보안검증 체계, 학술적 연구 수행 결과를 기반으로 한 새로운 공급망 보안 기술 제언 등 각 분야별 꾸준한 활동이 요구되는 바이다. 이러한 관점에서 본 논문은 소프트웨어 공급망 보안 정책으로 SBOM을 제안하며 정의 및 활용 사례를 소개하였고, 국외 SBOM 정책 동향을 파악하였다. 그 중 정부적 차원에서 SBOM을 소프트웨어 보안 강화 요소로 적극 추진 중인 미국의 사례와 SBOM의 필요성을 언급한 유럽의 사례를 연구하여 분석하였다. 그 결과 SBOM의 표준화 필요성을 도출하였고, 공급망 보안 관점에서 소프트웨어 가시성을 제공하는 SBOM에 대한 효용성을 입증하였다.

또한, 현재 국내 국가·공공기관의 공급망 보안 관리를 위하여 SBOM을 활용하고 있는 사례가 없는 것으로 보이는바, 국외 사례를 바탕으로 국내 적용방안을 고찰하였다. 기술과 정책·법률 측면에서 접근하여 SBOM 적용 방안을 도출하였고, SBOM 기본 구성요소 수립, 자동화 도구 개발, SBOM 제공 요구사항 명시 등의 필요성을 확인하였다. 향후 국내 공급망 보안 관리를 위한 가이드라인 및 정책이 수립 시 본 연구결과가 기초자료로써 활용할 수 있기를 기대한다.

현재 미국은 소프트웨어 신뢰성 향상을 위한 소프트웨어 보증 연구를 지속함에 따라, 행정명령 14028에서 요구하는 SBOM에 대한 개선방안을 개정 진행 중인 美 공급망 위험관리의 기본 가이드라인 문건 SP 800-161에 업데이트 할 예정이다. 네덜란드는 향상된 도구 개발을 위해 SBOM과 취약점의 상관관계를 심층 분석하기 위하여 더 많은 데이터를 기반으로 AI를 통한 연구를 진행하고자 한다. 이렇듯 SBOM은 향후 공급망 보안 관리체계에 더 많이 활용 될 것으로 보여지며 SBOM이 제공하는 소프트웨어 구성요소의 가시성을 바탕으로 제품에 대한 품질 평가 지표로 활용되길 전망한다. 현재 세계적으로 SBOM에 대한 데이터 및 도구가 제한적이고 표준화가 미비하지만, 향후 공급망 검증 도구로써 SBOM의 범용적 활용을 위하여 지속적인 동향 파악 및 표준 형식 개발을 위한 연구가 요구된다.

REFERENCES

[1] Executive Office of the President of U.S. (2021). *Improving of Nation's Cybersecurity* (Executive Order 14028 of May 12, 2021).

[2] NTIA. (2019). *Roles and Benefits for SBOM Across the Supply Chain.* Washington D.C. : NTIA.

[3] National Telecommunications and Information Administration(NTIA). (2021). *Framing Software .Common Software Bill of Materials(SBOM) - Second Edition.* Washington D.C. : NTIA.

[4] The Linux Foundation Projects, (2010). *The Software Package Data Exchange.* SPDX. https://spdx/dev

[5] NTIA. (2019). *Survey of Existing SBOM Formats and Standards.* Washington D.C. : NTIA.

[6] National Institute of Standards and Technology(NIST). (2018). *Software Identification(SWID) Tagging.* NIST. https://csrc.nist.gov/projects/Software-Identification-SWID

[7] ISO/IEC. (2015). *ISO/IEC 19770-2 Information technology-IT asset management-Part2:Software identification tag.* ISO. https://iso.org/standard/65666.html/

[8] Open Web Application Security Project(OWASP). (2001). *OWASP CycloneDX.* OWASP Foundation. https://owasp.org/www-project-cyclonedx

[9] CycloneDX. (2017). *CycloneDX Overview.* CycloneDX. https://cyclonedx.org

[10] NTIA. (2021). *Healthcare Delivery Organization (HDO)*

Software Bill of Materials (SBOM) Proof of Concept (PoC) 2.0 Quick Start Guide V1.2. Washington D.C. : NTIA.

[11] NTIA. (2021). *The Minimum Elements For a Software Bill of Materials(SBOM).* Washington D.C. : NTIA.

[12] G. Shea. (2021). *A Software Bill of Material Is Critical for Comprehensive Risk Management.* Foundation for Defense of Democracies(FDD). https://fdd.org/analysis/2021/09/29/a-software-bill-of-materials-is-critical-for-comprehensive-risk-management

[13] C. Skouloudi, A. Malatras, R. Naydenov & G. Dede. (2020). *Guidelines for Securing the Internet of Things.* ENISA. https://enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

[14] B. Riel, S. Kuijpers & R. Koning. (2021). *Using the Software Bill of Materials for Enhancing Cybersecurity.* National Cyber Security Centre(NCSC). https://english.ncsc.nl/publications/publications/2021/february/4/using-the-software-bill-of-materials-for-enhancing-cybersecurity

[15] MOIS & KISA. (2019). *Development Security Guide for E-Government SW Development and Operators.* Sejong & Naju : MOIS & KISA.

[16] MOIS. (2021). *Guidelines for establishment and operation of information systems for administrative and public institutions.* Sejong : MOIS.

손 효 현(Hyo-Hyun Son) [정회원]

비공개

· 2020년 2월 : 한남대학교 일반대학원 컴퓨터공학과(공학석사)
· 2020년 12월 ~ 2021년 11월 : 국가보안기술연구소 연구원
· 관심분야 : 사이버안보정책, 공급망보안정책
· E-Mail : sonhyohyun.kr@gmail.com

김 동 희(Dong-Hee Kim) [정회원]

비공개

· 2009년 2월 : 고려대학교 정보보호대학원(공학석사)
· 2017년 2월 : 고려대학교 정보보호대학원(공학박사)
· 2008년 1월 ~ 2015년 4월 : 한국인터넷진흥원 선임연구원
· 2015년 5월 ~ 2016년 3월 : 한국정보통신기술협회 선임연구원
· 2016년 3월 ~ 현재 : 국가보안기술연구소 선임연구원
· 관심분야 : 사이버안보전략/정책, 융합보안 정책
· E-Mail : dh_kim@nsr.re.kr

김 소 정(So-Jeong Kim) [정회원]

비공개

· 2001년 2월 : 경희대학교 평화복지대학원 동북아학과(정치학석사)
· 2005년 2월 : 고려대학교 정보보호대학원 정보보호정책학과(공학박사)
· 2001년 ~ 2002년 : 한국전파진흥협회 ITU-WRC 담당 연구원
· 2004년 5월 ~ 현재 : 국가보안기술연구소 정책연구실장
· 관심분야 : 사이버안보전략/정책, 국제안보정책
· E-Mail : sjkim@nsr.re.kr