미국 SBOM(Software Bill of Materials) 정책 분석 및 시사점

Analysis and Implications for SBOM(Software Bill of Materials) Policy of United States

김항규 선임연구원
소프트웨어정책연구소
SW정책·인재연구팀
hkkim@spri.kr

Executive Summary

미국 바이든 정부는 SW공급망 보안 강화를 위해 연방정부에서 조달한 SW제품에 대해 SW구성요소 정보를 기술한 문서, SBOM(Software Bill of Materials)을 제출하도록 요구하는 행정명령을 2021년 5월에 발표했다. 솔라윈즈, Kaseya, Log4J 등 SW공급망을 통한 보안 위협 사례가 증가함에 따라 연방정부 차원에서 이를 관리하기 시작한 것을 의미한다.

행정명령에 기반해 백악관과 OMB(Office of Management and Budget)를 중심으로 범부처적인 추진체계를 구축하고 민관협력을 추진하였다. 상무부 산하 NTIA(National Telecommuni- cations and Information Administration)와 NIST(National Institute of Standards and Technology)는 각각 SBOM의 개념 정립 및 실증과 표준화를 주도해 SBOM 정책 구현을 위한 이론적 검증과 기틀 마련을 담당했다. 국토안보부 산하 CISA(Cybersecurity & Infrastructure Security Agency)는 보안 측면에서의 내용 검토와 함께 SBOM 인식 제고 및 의견수렴을 위한 온라인 세션을 운영하였다. 미국 정부는 비영리 재단 주도로 정의된 SBOM 국제표준 포맷과 선도 기업들의 SBOM 유사 체계 모범사례를 바탕으로 정책을 수립하고 관련 분야의 민간전문가 의견을 청취하는 민관협력 체계도 병행하였다.

미국의 SBOM 정책은 개념 정립부터 제도화까지 단계적인 추진을 통해 민간 확산을 유도하고 있다. 우선 SBOM 범주·효과를 정의하고 준수 기준이 되는 최소요소(Minimum Elements)를 발표하였으며, 의료·에너지 등 실제 산업에서의 실증을 수행하였다. 표준화된 SBOM 활용과 정보 공유를 위해 SBOM 생성, SW공급망 관리, 산업별 보안 강화 등에 대한 가이드를 각각 배포하였다. SW공급망 보안 강화를 위해 행정명령으로 조달 규정 개정을 담당 부처에 지시하였고, 의료기기 등 개별적인 법안 발의를 통해 SBOM 확산을 위한 법적 기반을 마련하였다.

미국에서 추진한 SBOM 정책은 공공·민간에서의 안정적인 도입을 위해 단계적으로 추진되어 SW수출 대상국의 제재로서만이 아닌 SW기업의 경쟁력 제고를 위한 방향성으로 인식할 필요가 있다. 이니셔티브 발족과 실증 수행을 통해 SBOM 정착을 위한 기반을 마련하고, 가이드로 절차·포맷의 표준화를 진행하였다. 점진적인 민간 확산 유도를 위해 공공영역에서의 법제화를 추진함으로써 제도적 기반을 마련하고 있다. 국내에서도 정부와 기업이 대응책 마련과 함께 SBOM 도입을 신중하게 검토해야 할 시점이다.

In May 2021, the Biden government of the United States issued an executive order requiring the submission of SBOM (Software Bill of Materials), a document describing software component information, for software products procured from the federal government in order to enhance software supply chain security. As the number of security threats through software supply chain such as SolarWinds, Kaseya, and Log4J increases, it means that the federal government has started to manage them.

Based on the executive order, a government-wide implementation system was established led by the White House and the Office of Management and Budget (OMB) with public-private cooperation. National Telecommunications and Information Administration (NTIA) and National Institute of Standards and Technology (NIST) under Department of Commerce took the lead in framing SBOM with executing Proof-of-Concept (PoC), and providing the standard of SBOM, respectively, to establish theoretical verification and the foundation for the implementation of SBOM policies. Cybersecurity & Infrastructure Security Agency (CISA) under the Department of Homeland Security reviewed the content in terms of security, and operated virtual workshops to raise awareness of SBOM and collect opinions. A public-private cooperation system was also implemented to establish policies based on SBOM international standard formats defined by non-profit foundations and best practices for SBOM-like systems of global IT companies and to listen to the opinions of private experts in related fields.

The US SBOM policy is inducing the spread of SBOM to the private sector through a step-by-step process from concept establishment to institutionalization. First, SBOM scope and effects were defined, and the Minimum Elements, the baselines to comply with, were announced, with PoC conducted in actual industries such as medical and energy. Guides on SBOM generation, software supply chain management, and industry-specific security enhancement were distributed for standardized SBOM utilization and information sharing. In order to strengthen software supply chain security, departments in charge was instructed to revise the procurement regulations by the executive order, and the legal basis for the spread of SBOM was established through introduction of individual bills such as medical devices.

The SBOM policy promoted in the United States needs to be recognized as a direction for enhancing the competitiveness of software companies, not only as a sanction of the SW export destination country, as it is promoted in stages for stable introduction in the public and private sectors. The foundation for SBOM settlement was prepared through the initiation of an initiative and PoC, and the standardization of procedures and formats was carried out as a guide. In order to induce a gradual spread to the private sector, the institutional foundation is being laid by promoting legislation in the public domain. In Korea, it is time for the government and companies to carefully review the application of SBOM along with the preparation of countermeasures.

I 행정명령을 통한 SBOM[1] 도입 추진

▨ 미국 바이든 정부는 2021년 5월 보안 측면에서의 SW공급망 강화를 위해 행정명령 「국가 사이버 보안 개선」[2]을 발표하고 공공조달에서 SBOM을 제출하도록 함

○ 식품 자재명세서와 같이 SW구성요소를 목록화하는 SBOM은 SW공급망에 대한 이해를 향상시켜 보안·라이선스 위협에 기민한 대응을 가능하게 함

○ SBOM을 포함한 SW공급망 보안 강화 조치를 조달 체계에 반영하도록 관련 기관에 명함으로써 법 제·개정을 통한 SBOM 제도화 추진

- 구매자가 공급자에게 SBOM 제출을 요구하도록 하는 지침을 포함한 SW공급망 보안 강화 가이드라인을 작성·공개하도록 NIST[3]에 명령

- NTIA[4]는 정책적 기준점인 SBOM 최소요소를 정의·배포하도록 함

< 행정명령(EO14028) 중 SBOM 관련 항목 >

Sec. 4. Enhancing Software Supply Chain Security

(e) ... Such guidance shall include standards, procedures, or criteria regarding: ...

(vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website; ...

(f) ... and the Administrator of the National Telecommunications and Information Administration, shall publish minimum elements for an SBOM.

1) Software Bill of Materials: SW구성요소에 대한 명세서로, SW를 이루는 구성요소의 세부 정보와 의존관계에 대한 정형화된 기술(description)을 의미
2) 백악관(2021.5.12.), "Executive Order on Improving the Nation's Cybersecurity"
3) 국가표준기술연구소(National Institute of Standards and Technology), https://www.nist.gov/
4) 국가통신정보청(National Telecommunications and Information Administration), https://www.ntia.doc.gov/

▨ SW의 재사용률·복잡도가 높아져 SW공급망을 통한 위협 사례가 전세계적으로 증가함에 따라 미국 외의 국가에서도 SBOM 도입을 적극적으로 검토

○ 디지털전환 가속화로 빠른 SW신기술 도입을 위해 SW재사용률이 높아지는 가운데, 상용SW의 보안 업데이트 서버를 통한 침투, 공개SW[5] 프로젝트의 보안취약점 이용 등 SW공급망을 통한 위협 사례가 확산되는 추세

* 97%의 코드베이스가 공개SW를 포함하고 코드 중 78%를 공개SW로 구현[6]

- 솔라윈즈 사태[7]와 유사한 사례로, 2021년 7월 미국 SW기업 Kaseya의 원격 모니터링·관리 도구 업데이트 채널을 통해 랜섬웨어가 침투되어 약 1,500개에 이르는 최종 고객사에 피해 발생[8]

* 미국, 영국, 독일, 네덜란드, 뉴질랜드 등 전세계적으로 영향을 받았고, 스웨덴에서는 식료품 체인 Coop 약 800개 점포를 폐쇄하고 국영 철도 조직에도 타격[9]

- 2021년 12월에는 자바 시스템 주요 로깅 오픈소스 Log4j에서 취약점이 발견되어 이를 악용하는 사례가 기업 네트워크 48% 이상에서 감지[10]

* 공개SW 생태계를 통한 SW공급망 공격이 2021년에 전년 대비 650% 증가[11]

- SW공급망 위협은 신뢰하는 채널을 통해 SW구성요소 수준의 악성SW가 침투하였으나 투명성 미확보로 빠른 대응이 이루어지지 못해 피해 확산

5) 소스코드가 공개되어 있어 사용수정배포를 자유롭게 허용하는 SW (자유SW와 오픈소스SW를 포괄)
6) Synopsys(2022.4.), "2022 OPEN SOURCE SECURITY AND RISK ANALYSIS REPORT"
7) MS 블로그(2020.12.17.), "A moment of reckoning: the need for a strong and global cybersecurity response"
8) Kaseya 보도자료(2021.7.5.), "Kaseya Responds Swiftly to Sophisticated Cyberattack, Mitigating Global Disruption to Customers"
9) Blocks & Files(2021.7.4.), "Kaseya VSA vulnerability opens a thousand-plus business doors to ransomware"
10) Check Point 블로그(2021.12.10.), "Protect Yourself Against The Apache Log4j Vulnerability"
11) sonatype(2021), "2021 State of the Software Supply Chain"

ㅇ 이와 같은 위협에 기민한 대응이 가능하도록 SW공급망 투명성을 높이고자 미국뿐만 아니라 일본, EU 등에서도 SBOM 도입을 검토하거나 권고

- 일본은 경제산업성 산하에 소프트웨어TF를 구성해 SBOM 정책 추진 방안을 마련하고 활용 촉진을 위한 실증사업 실시 및 제도 정비 방안 마련[12]
- EU 보안전문기관 ENISA[13]는 병원 사이버보안 조달 가이드라인[14]과 IoT 보안 가이드라인[15]을 통해 안전한 SW 사용을 위해 SBOM 포함을 권고

▨ 본고에서는 미국의 선도사례를 추진체계와 주요 정책 측면에서 살펴봄으로써 국내의 SW공급망 강화와 SW기업 역량 제고를 위한 SBOM 도입 방향 모색

ㅇ 공공·민간 전반에 걸친 SBOM 활용 활성화를 위해 범부처 및 민간 협력에 기반한 SBOM 정책 추진체계와 주요 담당 조직의 역할·기능 분석

ㅇ SBOM 활성화의 기반 마련을 목적으로 미국에서 추진한 세부적인 정책에 대해 목적, 내용 등을 분석해 정책 구현 수단을 영역별로 분류

ㅇ 미국 SBOM 정책 추진 현황에 대한 시사점 도출

12) 経済産業省(2022.3.3.), “サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースの検討の方向性”
13) EU 사이버보안청(European Union Agency for Cybersecurity), https://www.enisa.europa.eu/
14) ENISA(2020.2.), “PROCUREMENT GUIDELINES FOR CYBERSECURITY IN HOSPITALS”
15) ENISA(2020.11.), “GUIDELINES FOR SECURING THE INTERNET OF THINGS”

II SBOM 정의 및 필요성

▨ SBOM이란, SW를 이루는 구성요소의 세부 정보와 의존관계에 대한 정형화된 기술(description)을 의미함

ㅇ 세부적인 차이는 있으나 SW구성요소에 대한 정보에 대한 목록임에는 동일

* “SW 빌드에 사용된 다양한 구성요소의 상세 정보와 공급망 관계를 포함한 형식적인 기록” - 美행정명령 EO14028 Sec.10.(j)
* “완성된 제품 안에 있는 모든 SW구성요소의 목록” - MedCrypt 부사장[16]
* “SW를 구성하는 부분을 설명하는 전자문서 또는 기계가독적 파일” - 네덜란드 국가사이버보안 센터[17]

ㅇ SW공급망 위협에 대해 개선책 적용 및 대응 시간 단축을 목적으로 활용

▨ SBOM은 SW구성요소 수준의 정보를 명기·공유해 SW공급망 투명성을 제고함으로써 SW제품 수요자와 공급자에게 안전한 SW활용·개발을 가능하게 함

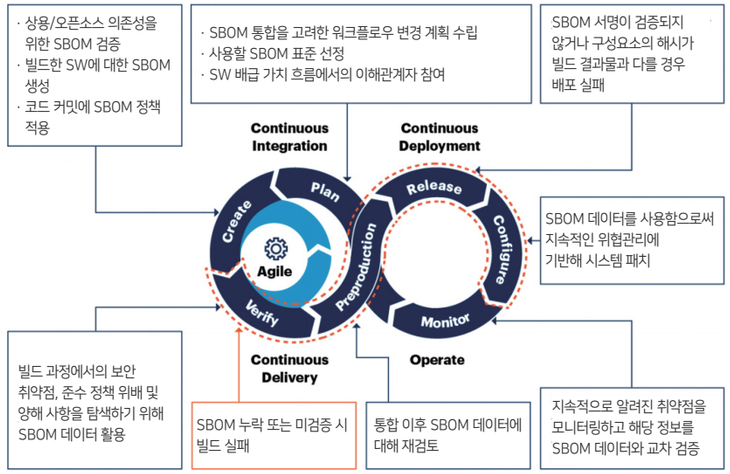
ㅇ (SW수요자) SW제품 구성요소의 속성, 의존성, 관련 외부 자료 등을 활용해 보안·라이선스·SW자산 관리 측면에서의 효율성 향상[18]

- (빠른 취약점 대응) 보안취약점 발견 시 관련 구성요소 탐색, 공급자를 통한 패치 확보, 시스템 개선까지의 시간 단축
- (라이선스 준수) 모든 구성요소의 라이선스를 검토·관리함으로써 SW제품의 라이선스를 명확히 하고 조직 시스템의 라이선스를 통합적으로 관리·준수
- (높은 신뢰성 확보) 구성요소의 원천 정보와 공급망에서의 관리 연속성(chain of custody)을 확보함으로써 SW제품에 대한 관리 효율화

16) Seth Carmody, et al.(2021.2.23.), “Building resilient medical technology supply chains with a software bill of materials”, npj Digital Medicine, Vol. 4, No. 34
17) Capgemini(2021.1.), “Using the Software Bill of Materials for Enhancing Cybersecurity”
18) NTIA(2021.10.21.), “Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM)”

○ (SW공급자) SW개발 생애주기 상에 SBOM을 도입함으로써 보안취약점 및 라이선스 검증을 자동화하고 안전한 SW개발·관리 수행

[그림 1] SW개발 생애주기 상에서의 SBOM 워크플로우 통합



* 출처 : Gartner(2022.2.14.), "Innovation Insight for SBOMs"; SPRi 수정

III 추진체계

2021년 행정명령을 기반으로 SBOM 제도화 및 안착을 위한 범부처 추진체계를 구성하고 민간 협력을 통한 의견수렴 및 민간 확산 기반 마련

○ 2010년 초부터 입법 및 개념 확립을 통한 SW공급망 투명성과 SBOM에 대한 인식 제고로 범부처 SBOM 정책 추진을 위한 동력 형성

- 정부 영역에서의 SW공급망 투명성을 향상시킴으로써 SW구성요소에서의 보안 위협을 방지하고자 하는 움직임이 입법 형태로 추진됨

  * 정부가 조달하는 SW제품을 대상으로 SW공급망 투명성 확보를 위한 법안과 IoT 보안에 관한 법안을 국회에서 발의 추진

- 실질적인 정책 구현에 앞서 SBOM에 대해 개념적인 부분을 명확화하고 도입 효과에 대한 검증을 위해 실증(PoC: Proof of Concept) 수행

  * SW구성요소 투명성 이니셔티브를 발족[19]하고, 의료·에너지 등 주요 분야에서 실증을 수행해 SBOM 정책의 개념적 기틀 정립 및 정책 방향성 검증

○ 행정명령 발표로 조달에서의 SBOM 정착을 위해 백악관을 중심으로 조직적 기능을 부처·기관에 할당하고 일관된 정책 추진을 위한 범부처 추진체계 구축

- (총괄) 백악관에서 행정명령을 바탕으로 범부처 SBOM 정책 추진의 리더십을 발휘하고, 기준·지침을 각 부처기관에서 수용하도록 조치

- (표준화) 상무부는 국제표준을 준용해 공공·민간에서의 효과적인 SBOM 활용을 위한 기준·지침을 정의하고 배포

- (보안검토) SBOM 관련 지침, 적용 범주, 연방 조달 규정 등을 국토안보부 및 국방부에서 검토해 보안 위협 대응 측면에서의 검증 진행

- (실증) 의료, 에너지 등 SBOM 주요 산업에서의 효과성 검증을 위해 보건복지부, 에너지부 등에서 상무부와 협력해 실증 수행

- (제도화) 연방 조달 규정의 수정을 위해 FAR 위원회[20]에서 개정을 진행하고, 국토안보부·보건복지부 등에서 관련 법안 마련

19) NTIA 블로그(2018.6.6.), "NTIA Launches Initiative to Improve Software Component Transparency"
20) Federal Acquisition Regulatory Council: 연방 조달 규정을 담당하는 위원회로, 조달처(GSA), 국방부, 항공우주국(NASA)로 구성

○ 민관협력을 바탕으로 SBOM 연구·산업계 의견수렴, 표준화 및 정책 방안 논의 등을 추진해 민간 영역에서의 SBOM 활용 활성화를 위한 기반 조성

* MS는 내부적으로 운영하던 SBOM 유사 체계를 미국 정부에서 권고한 SBOM 국제표준으로 전환해 약 2,000개 제품 및 서비스에 적용[21]

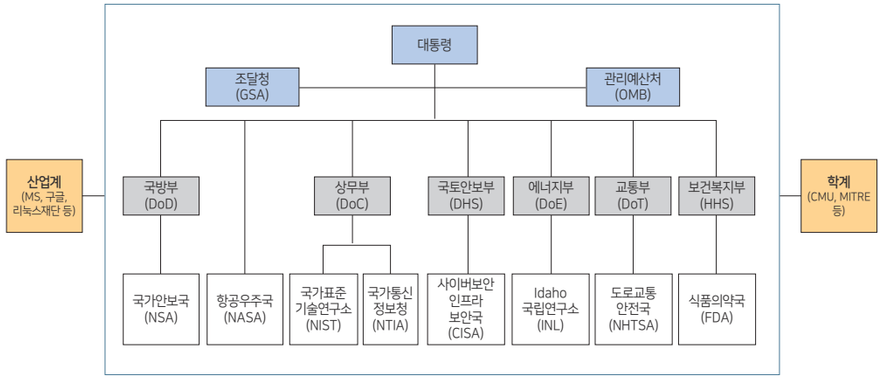
- 공개SW 및 보안 관련 비영리 재단은 SBOM 유통·공유를 위한 국제표준 포맷을 개발하고 관련 정보를 제공함으로써 체계 구축에 협력

* 리눅스재단, OWASP 등은 공개SW 라이선스 검증, SW구성요소 보안 강화를 위한 SBOM 포맷 국제표준 발표하고, 정부의 표준 포맷 선정 지원

- 주요 SW기업들은 선도적인 SBOM 유사 체계에 대한 정보를 공유하고, 정부 주도의 SBOM 제도화와 관련 기술적 이슈 사항에 대한 의견을 전달

* MS, 구글 등 기업 내부 및 협력업체에 기도입된 SW구성요소 식별 및 보안 관리 체계를 기반으로 SBOM 관련 지식·경험 공유

[그림 2] 미국 SBOM 정책 추진체계도



* 출처 : EO14028 Sec. 4 및 관련 정책 자료 기반 SPRi 분석

21) MS 블로그(2022.5.10.), "Continued investments in supply chain security in support of the cybersecurity Executive Order"

▨ 주요 기능별로 전담 기관을 설정해 SBOM 정책을 추진함으로써 정부 정책 구현에 있어서 전문성 및 일관성 확보

○ 범부처 추진체계에서 각 부처에 할당된 역할을 실질적으로 세부 조직·기관에서 담당·수행하고 SBOM 정책 구현을 위해 분업·협업 추진

[표 1] 미국 SBOM 정책 추진 관련 주요 기관 및 역할

기관명	조직 기능	SBOM 정책 역할
OMB[22] (백악관)	대통령의 비전 구현을 위한 업무를 수행하고, 정책·예산·관리·규제 측면에서 대통령을 보좌하고 기관에 관련 사항 지시	연방 부처·기관의 준수·협조를 촉구 - 중요SW(Critical SW[23]) 보안 조치[24] 준수를 기관에 전달 - SW공급망 보안 가이드 준수를 위해 조달 담당자 대상 온라인 워크샵 개최[25] - NIST 가이드 준수와, 필요 시 공급자에게 SBOM을 요구할 것을 연방기관에 지시[26]
NTIA (상무부)	통신·정보 관련 국가 정책 수립·이행을 위해 대통령에게 조언	SBOM 정책 추진을 위한 기준 마련 - SW구성요소 투명성 이니셔티브를 발족해 SBOM 기반 투명성 확보 기준 정의 - 의료·에너지 등 SBOM 실증으로 산업 도입 효과성 검증 - SBOM 생성·공유 등에 대한 기준인 SBOM 최소요소 공개
NIST (상무부)	측정·표준·기술 발전을 통해 혁신과 산업 경쟁력 제고를 촉진	SW공급망 보안 관련 가이드 배포 - 중요SW 정의, 보안 조치 가이드 제작 - SW공급망 보안 가이드 공개
CISA[27] (국토안보부)	사이버·물리 기반 시설에 대한 위협 이해·관리·감소를 수행	SBOM 정책 보안 검토 및 인식 제고 - 중요SW 정의, 보안 조치 가이드 검토, 중요SW 목록 식별 - 인식 제고, 의견 청취를 위한 토론[28] 및 온라인 세션[29] 운영

22) 관리예산처(Office of Management and Budget), https://www.whitehouse.gov/omb/
23) EO14028을 통해 정의된 개념으로 권한·네트워크·데이터 등 시스템 운영에 치명적인 자원과 관련된 SW를 의미, https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition-explanatory, 2022.12.14. 방문
24) Security Measures, 조치 항목 중 'SM-3.1'에서 SBOM과 같은 SW구성요소 정보 관리 요구, https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eo-critical-software-use, 2022.12.14. 방문
25) 백악관(2022.3.7.), "OMB Statement on 'Enhancing The Security Of Federally Procured Software'"
26) OMB(2022.9.14.), "M-22-18 MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES"
27) 사이버보안 인프라 보안국(Cybersecurity & Infrastructure Security Agency), https://www.cisa.gov/
28) CISA SBOM-A-RAMA, https://www.cisa.gov/cisa-sbom-rama, 2022.12.14. 방문
29) FEDERAL REGISTER(2022.6.1.), "Public Listening Sessions on Advancing SBOM Technology, Processes, and Practices"

Ⅳ 영역별 주요 정책 추진 현황

1. 개념 및 범주 확립

▨ 의료, IoT 등 분야에서 보안 확보를 위해 SW구성요소 관리의 필요성이 제기되면서 NTIA는 이론적 토대 마련을 위해 이니셔티브 발족 및 세부 워킹그룹 구성

○ SW공급망 상에서의 보안 위협 대응을 목적으로 2018년에 SBOM 활용 활성화를 위한 SW구성요소 투명성 이니셔티브[30]발표

- (배경) 사이버보안, IoT, 의료 등에 대한 민간의견 청취가 2015년 이래로 진행되면서 보안취약점 관리를 위한 SW공급망 투명성 확보 필요성 제기
- (미션) 조직의 SW취약점 대응을 위해 제조사와 유통사(vendor)가 제3자·임베디드 SW구성요소에 대한 유용한 정보를 교류하는 방법 개발·수행
- (범위) SBOM의 구조, SBOM 공유 방법, 보안 강화를 위한 SBOM 활용법 등을 정의해 모든 이해관계자에게 SBOM 유용성 제공

○ SBOM 정책 추진을 위한 개념적 기반 정립을 위해 SBOM의 구조·공유·활용 측면에서 기능별로 분류하고 각각에 대해 민간전문가 기반 워킹그룹 운영

- (프레이밍) 관련 용어, SBOM 항목·구조, 생성·공유 절차 등을 정의
- (표준) SBOM 공유를 위한 포맷 국제표준을 비교 분석
- (사례) 의료 영역의 SBOM 활용사례에 기반해 도입 효과·장애 도출

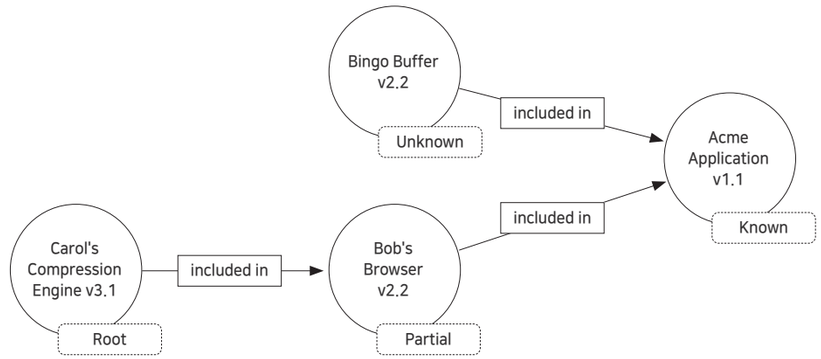
30) NTIA, "NTIA Software Component Transparency", https://ntia.gov/other-publication/ntia-software-component-transparency/, 2022.12.14. 방문

▨ 다중이해관계자 프로세스의 의견수렴과 개념 검증을 위한 실증 과정을 통해 정책 추진의 개념적 기반이 되는 SBOM 정의와 범주 설정

○ SBOM 개념 소개와 FAQ[31]를 통해 SBOM 이해관계자의 인식 제고

- (정의) SBOM이란, SW구성요소 정보와 계층적 의존관계를 형식적이고 기계가독적인 형태로 기술한 목록을 뜻함

[그림 3] SBOM의 개념적 구조 예시



* 출처: NTIA(2021.4.27.), "SBOM at a Glance"

* 주석: 원형은 SW구성요소 정보를, 화살표 직선은 계층적 의존관계를 나타냄, 우측 원 3개의 의미를 풀이하자면 'Acme에서 개발한 버전 1.1인 SW제품 Application에는 버전 2.2인 Bingo Buffer와 Bob이 개발한 버전 2.2 Browser가 포함되어 있음'을 의미함

○ SW공급망 투명성 강화의 정상적 수행을 위해 충족해야 할 최소한의 요건인 SBOM 최소요소[32]를 정의해 범정부적으로 SBOM 정책 준수의 기준점 제시

- 행정명령에 따라 NTIA는 다중이해관계자 프로세스와 실증을 통해 정립된 SBOM 개념과 범주에 기반해 SBOM 최소요소를 정의·공개

31) NTIA(2020.11.16.), "SBOM FAQ"
32) NTIA(2021.7.12.), "The Minimum Elements For a Software Bill of Materials (SBOM)"

[표 2] NTIA에서 정의한 SBOM 최소요소

최소요소 (Minimum Elements)	
데이터 필드 (Data Fields)	필수적으로 추적해야 할 각 구성요소의 기준 정보 문서화: 구성요소의 공급자·이름·버전·식별자·의존관계, SBOM 작성자·작성일시
자동화 지원 (Automation Support)	SW생태계 상에서의 적용을 위한 자동 생성·기계가독성 등을 포함한 자동화 지원, SBOM 생성·소비를 위한 데이터 포맷으로는 SPDX[33], CycloneDX[34], SWID tags[35] 포함
지침 및 절차 (Practices and Processes)	SBOM 요청·생성·사용에 대한 운영 정의: 생성 빈도수, SW구성요소 분석 깊이, 알려진 언노운(Known Unknowns), 배포 및 전달, 접근 제어, 오류에 대한 양해

* 출처: NTIA(2021.7.12.), "The Minimum Elements For a Software Bill of Materials (SBOM)"

○ SBOM이 제기된 문제 분석, 필수항목 도출, 관리절차 정의를 통해 SBOM에 대한 개념적 범주 설정해 정책 추진의 기반 마련[36]

- (문제정의) SW공급망의 복잡성·가변성은 잠재적 사이버보안 위협에 대한 시스템적 가시성에 손실을 발생시켜 개발·조달·유지보수 비용을 높이고 결과적으로 공공안전과 국가 안보에 위험을 초래
- (필수항목) SW구성요소와 의존관계를 모호함 없이 유일하게 식별할 수 있도록 주요 속성(최소요소)을 도출해 SBOM 필수항목으로 정의
- (관리절차) SBOM 생성 방법 및 시점, SBOM 교환에 대한 절차적 방법론과 SBOM 생산·선택·운영 과정에서의 역할을 정의해 필수 절차 구체화

▨ 이해관계자를 SW공급자와 SW수요자로 나누어 SBOM의 생산과 소비 단계에서의 절차·역할을 워크플로우 형태로 정의한 플레이북 공개

○ SW공급자*는 온전한 SBOM 생산을 위해 정확한 SW구성요소 식별을 수행하고 검증을 위해 출처(point of origin)에 대한 정보를 포함할 것을 강조[37]

* SW유통사(vendor), 계약SW 개발자, 공개SW 개발 프로젝트 등을 포함

33) Software Package Data Exchange, https://spdx.dev/
34) CycloneDX, https://cyclonedx.org/
35) ISO/IEC 19770-2:2015, https://www.iso.org/standard/65666.html, 2022.12.14. 방문
36) NTIA(2021.10.21.), "Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM)"
37) NTIA(2021.11.17.), "Software Suppliers Playbook: SBOM Production and Provision"

- SBOM 생산을 위한 공통 절차를 ① SW구성요소 식별, ② 관련 정보 추출, ③ SBOM 구조화, ④ 형식 검토 및 확인, 4단계로 나누어 정의
- 개발·배포 도구를 통한 SBOM 자동 생성을 개발 과정에 기본화하고, 필요시 바이너리 스캐닝, 코드 분석 등을 통한 수동 생성도 함께 수행

○ 보안취약점, SW자산 관리를 위해 SW수요자*에게 요구되는 SBOM 데이터 처리·관리 절차를 취득·저장·관리로 분류해 제시[38]

* 제3자 SW능력(capability)을 공급자로부터 취득한 개체를 통칭함

- SBOM 취득 과정은 상용 제품, IT 서비스, 공개SW 등 SW제품의 유형에 따라 제품·업데이트와 함께 수령, 계약 내용에 포함해 최종 산출물에 포함, 바이너리·소스코드 분석을 통해 직접 생성 등으로 분류될 수 있음
- 취득한 SBOM 데이터에 대해 개체명확화(entity resolution), 관리연속성 유지, 하위의존성(transitive dependency) 식별 등이 이루어져야 조직 내 다른 업무 프로세스와 연동해 정확한 취약점 및 SW자산 관리가 가능함을 강조

2. 실증사업 추진

▨ (의료) 기기의 안전한 사용을 위해 의료 커뮤니티에서 제기된 수요 기반으로 선도적인 실증을 추진함으로써 주요 산업에서의 SBOM 실증의 기반을 마련

○ 의료기기 생태계의 SW공급망 보안 위협에 대응하기 위해 NTIA는 SBOM 생성·소비에 대한 실증을 수행함으로써 SW공급망 투명성 확보 가능성 검토[39]

- (목적) 국제표준 포맷에 기반해 의료기기에 대한 SBOM 생성·소비를 수행함으로써 의료기기 생태계 보안 강화를 위한 SBOM 효용성 검증
- (범위) SPDX, SWID 등 국제표준 포맷으로 SW구성요소의 의존관계·공급자명·버전을 작성하고 SBOM을 인터넷으로 수요기관에 전달

* 실증 2단계는 사례·참여자 확대, 최소요소 증명, SBOM 생성 가이드 제작, 취약점 관리 등, 3단계는 의료 영역 적용 확대, 자동 SBOM 공유 등으로 계획 수립·수행[40]

38) NTIA(2021.11.17.), "Software Consumers Playbook: SBOM Acuisition, Management, and Use"
39) NTIA(2019.10.1.), "Software Component Transparency: Healthcare Proof of Concept Report"
40) NTIA(2021.10.14.), "Healthcare SBOM Proof of Concept – Phase II Summary"

- (내용) 의료기기 제조사와 의료기관[41]을 주체로 구성해 의료기기에 대한 SBOM 생성·소비 과정을 실증하고 정기 미팅으로 목적 정의 및 사례 개발

○ 실증을 통해 SBOM 생성·소비 및 제품 조달 과정에서의 현재 이슈를 점검하고 의료를 포함한 산업에서의 SBOM 정착을 위한 개선 방향 모색

- (생성) SBOM에 작성되어야 하는 SW구성요소 항목을 검토해, 공신력 있는(authoritative) 정보 획득 방법 및 필요성 확인 등이 제기됨

  * SW구성요소 명·버전·공급자에 대한 권위적 정보 취득, 취약점 관리 상에서의 의존정보 필요성 의문, 실증 시나리오에서 생략된 SBOM 버전관리 등 관련 이슈 발견

- (소비) 취약점 관리 시스템과 SBOM 연동을 위해 관련 정보를 식별·대응하기 위한 표준 범용 자원 식별자(URI) 필요성 확인

- (조달) 의료기기 구매 과정에서 의료기관이 물리적인 지연 없이 NVD와 연계해 취약점을 검토하기 위해서는 SBOM 이식·통합 자동화가 요구됨

[표 3] NTIA 의료 SBOM 실증 결과 분석

강점(Strengths)	약점(Weaknesses)
· SBOM을 내부 시스템에 이식해 질의, 외부정보 연계 등을 통한 양적·질적 분석을 성공적으로 수행 · SPDX, SWID로 SBOM 생성 · 조달 및 자산·위협·취약점 관리에서 SBOM 보안 이점 확인	· 표준 포맷 준수 · 의료기기에 대해 제조사마다 다르게 SBOM 생성 · SBOM 데이터 도구를 설정관리DB과 미연계 · 현재 SW구성요소 명·버전·공급자의 공신력 있는 정보 부재 · 의존관계 정보 추출의 어려움 존재 · SBOM 설정 취약점의 한계 · 패치 상태에 대한 관리 부재
기회(Opportunities)	**위협(Threats)**
· HW BOM 포함 · 하나의 표준 포맷 식별 · SBOM에 취약점 정보 포함 · 구성요소에 대한 범용 유일 식별자 및 문맥 · 프로그래밍된 방식으로 SBOM 데이터 접근 · 구성요소 생애주기 종료 시점 분석 · SBOM에 대한 XML 스키마 포함 · API, 웹 포탈, 기기 내 파일 등 SBOM 배포 채널	· SBOM 속성에 대한 범용 자원 식별자(URI)의 부재 · SBOM 정보 정확도·완성도를 확인하는 검증 방법 부재

* 출처: NTIA(2019.10.1.), "Software Component Transparency: Healthcare Proof of Concept Report"

41) 의료기기 제조사: Medical Device Manufacturer, 의료기관: Healthcare Delivery Organization

(에너지) 의료기기 실증에 이어 사회 기반 시설에서의 수준 높은 SW공급망 보안 확보를 위해 SW 구성요소 정보를 SBOM으로 제공하는 실증 추진

○ 에너지부와 NTIA의 지원을 받아 INL[42]에서 담당해 실증 수행[43]

- (목적) 기술 공급자, 자산 소유자, 제3자 유통사 등 에너지 분야의 다양한 이해관계자를 모아 SBOM 관련 지식·경험 공유하고, 유통사와 자산 소유자 간에 SBOM 정보 생성·교환 촉진 및 모범사례 탐색

- (범위) SBOM 생성·배포·활용 관련 기술·절차·정책·법률 이슈를 논의하고, 기존 취약점 관리 도구 연동을 포함한 SBOM 활용사례 개발

- (산출물) 정기적인 공개 워크샵을 운영하고 SBOM 생성·활용함으로써 개념을 검증해 관련한 교훈·경험을 보고서로 공개

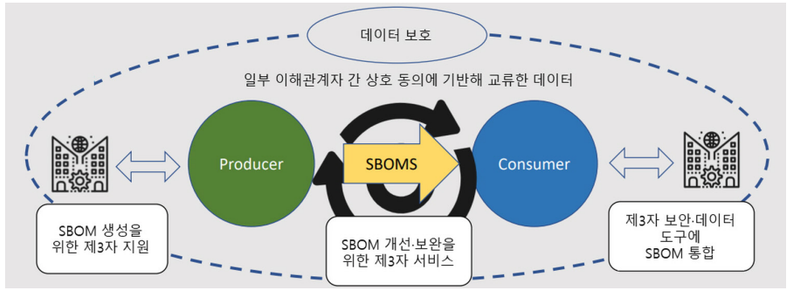
- (내용) SBOM 개념·생성·활용·전달을 주제로 토론하고 주요 활용사례를 공유함으로써 에너지 영역에서의 SBOM 기반 취약점 관리법 논의[44]

○ 에너지 산업 분야에서는 NVD, CVE[45]등을 이용한 취약점 관리가 대부분 SW구성요소가 아닌 SW제품 수준에 머무르는 한계를 가짐[46]

- 취약점 관리와 조달 과정 중 제품 평가에 SBOM을 활용해 SW구성요소 취약성을 추적·식별하기 위해 실증 추진

- SBOM이 높은 수준의 규제가 적용된 에너지 산업에 추가적인 규제가 아닌 민간 주도의 공급자·수요자 간 자발적인 동의로 작용해야 함을 강조

[그림 4] 에너지 SBOM 실증 개념도



* 출처: NTIA(2021.4.26.), "Software Bill of Material Exploring a Proof-of-Concept For the Energy Community""

42) 아이다호 국가 연구소(Idaho National Laboratory), https://inl.gov/
43) NTIA(2021.4.28.), "Energy Sector SBOM PoC Charter"
44) INL SBOM PoC, https://sbom.inl.gov/, 2022.12.14. 방문
45) 미국 정부가 관리·공개하는 보안취약점 정보 데이터베이스. NVD(National Vulnerability Database): https://nvd.nist.gov/, CVE(Common Vulnerabilities and Exposures): https://www.cve.org/
46) NTIA(2021), "SBOM use cases for the energy sector"

▨ (자동차) 차량 운행에서의 안전 확보 차원에서 사이버보안 지침을 통해 SW구성요소 관리·추적을 권고하고 산업에서의 SBOM 확산 가능성을 검토

○ 교통부 산하 NHTSA[47]는 2021년 「현대 차량 안전을 위한 사이버보안 모범사례」[48]를 공개해 구성요소 수준의 SW자산 목록 관리 필요성 강조

○ 이와 함께 산업에서의 SBOM 도입 효과성을 검토하는 SBOM 프로젝트 계획 수립[49]

- (내용) 기존의 실제 구현 경험을 기반해 자동차 산업의 SBOM 사례를 새로 개발하고 산업의 동의·추천 획득을 통해 공급업계의 자발적 채택 육성
- (운영) 의료 등 선행 실증 경험을 NTIA에서 공유하고, SBOM 구축 및 시험 실행 후 검토와 조정 과정을 거쳐 산업 표준에 대한 공급업체 권고사항 도출

3. 안내 지침서 제작·배포

▨ SW구성요소에 기반해 현재·미래의 잠재적 사이버보안 취약점 관리를 목적으로 표준화된 SBOM 생성 방법론을 안내하기 위한 가이드[50]를 제작·배포

○ NTIA에서 의료 분야 SBOM 실증의 산출물로 배포해 의료기기에 제한하지 않고 타 산업·분야에서의 확산을 전제로 범용 SBOM 생성 방법 공유

* NTIA 의료 SBOM 실증 2단계에서 실증을 통해 취합된 경험·지식에 기반해 작성

○ SBOM 생성 과정을 정보 수집, 내용 작성 2단계로 구분하고 각 단계에서의 실행 사항과 함께 주요 고려할 점을 명기함으로써 SBOM 생성 방법 안내

- (정보 수집) SW 개발·기획팀에서 SW구성요소 목록, SCA[51]로 감지된 정보, 조직에서 관리하는 라이선스 DB 등을 종합해 필수항목[52]의 정보 추출

* SW설계 문서를 참고하도록 하고, SCA 도구의 오류·누락을 감안해야 함을 강조

- (내용 작성) 고유한 SW구성요소 식별을 위해 SW 식별 정보, 고유 식별자, SBOM 식별 정보, 비식별 SW 구성요소 기입법을 설명하고, SBOM 국제표준 포맷인 SPDX, SWID로의 작성법을 예시로 가이드

* SBOM의 완결성(completeness)을 위해 외부정보 연계 등에 기반해 식별하도록 함

▨ NTIA에서 권고한 SBOM 포맷 국제표준들을 비교 분석한 보고서[53]를 공개해 현업에 적합한 표준을 선정·활용할 수 있도록 지원

○ SW구성요소 투명성 이니셔티브 내에 설치된 표준 및 포맷 워킹그룹에서 SW 식별을 위한 기계가독적 포맷 표준들을 대상으로 조사 및 정리

○ 선정된 3개의 SBOM 포맷 표준(SPDX, CycloneDX, SWID)에 대해 주요 정보, 특성, 활용사례, SBOM과의 관계 등을 소개해 표준 선택을 위한 정보 제시

- (SPDX) 리눅스재단에서 개발해 2021년 ISO/IEC 표준으로 등록[54]되었으며, 공개SW 라이선스 관리*와 함께 SBOM 활용에 용이

* 라이선스에 대한 모호함 해소를 위해 별도의 목록(SPDX License list)을 관리하고 지적재산권 및 라이선스 관련 정보 기술을 위한 항목을 풍부하게 제공

- (CycloneDX) OWASP에서 제안한 경량 SBOM 포맷 표준으로, 학습·적용이 용이하고 확장성*이 높아 조직·산업에 특화된 방식으로 적용하기 적합

* SaaSBOM, HBOM(HW BOM), VEX(취약점 정보) 등으로 확장·활용 가능

- (SWID) SW자산 관리를 위해 2012년에 ISO/IEC 표준으로 등록되었고, 패치·업데이트·설정 등을 포함한 SW생애주기* 상에서의 SBOM 교환 가능

* SW제품의 설치·패치·설정·삭제 등에서의 SW식별 정보 관리 기능 제공

47) 국가도로교통안전국(National Highway and Traffic Safety Administration), https://www.nhtsa.gov/
48) NHTSA(2020), "Cybersecurity Best Practices for the Safety of Modern Vehicles"
49) NTIA Automotive sector 발표자료, https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_energy_automotive.pdf, 2022.12.14. 방문
50) NTIA(2021), "How-To Guide for SBOM Generation"
51) SW구성요소 분석(Software Component Analysis): SW의 소스 코드 또는 바이너리를 분석해 하위 구성요소를 식별하고 관련 정보를 추출하는 과정
52) NTIA Framing 보고서(2021.10.21.)에 명시된 SBOM 작성자명, SW구성요소 명·공급자·버전·해시·식별자·의존정보
53) NTIA(2021), "Survey of Existing SBOM Formats and Standards"
54) ISO/IEC 5962:2021, https://www.iso.org/standard/81870.html, 2022.12.14. 방문

○ 표준별로 SBOM 필수항목 관련한 필드를 대응시켜 해당 포맷으로의 SBOM 생성과 표준 간의 포맷 변환을 위한 정보 제공

[표 4] SBOM 필수항목에 대한 SPDX, CycloneDX, SWID 필드 대응

SBOM 필수항목	SPDX	CycloneDX	SWID
작성자 이름 (Author Name)	Creator	metadata/authors/ author	<Entity> @role (tagCreator), @name
작성 일시 (Timestamp)	Created	metadata/timestamp	<Meta>
SW구성요소 공급자 (Supplier Name)	PackageSupplier	Supplier publisher	<Entity> @role (softwareCreator/ publisher), @name
SW구성요소 이름 (Component Name)	PackageName	name	<softwareIdentity> @name
SW구성요소 버전 (Version String)	PackageVersion	version	<softwareIdentity> @version
SW구성요소 해시 (Component Hash)	PackageChecksum 또는 VerificationCode	Hash “alg”	<Payload>/../<File> @[해시알고리즘]:hash
SW구성요소 식별자 (Unique Identifier)	DocumentNamespace (SPDXID와 함께)	bom/serialNumer component/bom-ref	<softwareIdentity> @tagID
SW구성요소 의존관계 (Realtionship)	DESCRIBES, CONTAINS	Dependency 그래프 또는 내부에 포함	<Link> @rel, @href

* 출처: NTIA(2021), “Survey of Existing SBOM Formats and Standards”

NIST는 행정명령에 따라 SW공급망 보안 가이드를 3가지 형태로 배포하였고, SW공급망 보안 향상을 위해 SBOM을 통한 구성요소 관리 절차 포함

○ (웹 가이드[55]) 연방 부처·공공기관의 조달 담당자에게 행정명령 준수를 위해 NTIA 최소요소에 부합하는 SBOM을 SW공급자가 제공할 수 있도록 확인하고, SBOM 안착을 위해 기관이 갖추어야 할 역량을 3단계로 분류해 제시

* SBOM은 기존의 보안취약점 관리 시스템의 대체가 아닌 보완 역할임을 언급하고, SBOM 정보 이식·분석이 불가한 기관은 보안 관리를 향상시키지 못할 것이라고 강조

55) NIST SBOM 가이드, https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1, 2022.12.14. 방문

- (기반) 모든 SW에 대해 NTIA 최소요소를 충족하는 SBOM을 관리하고, 디지털 서명 기반 저장소를 유지하면서 SBOM을 직접 또는 공용 웹사이트로 공유
- (지속) 상용 SW구성요소 세부 정보도 취합하고, SBOM 저장소와 외부정보를 연동해 SW공급망 상에서의 보안 위협을 자동적으로 탐지
- (발전) 조달 기관의 SBOM 취약점 감지 영향도를 동적으로 모니터링하고, SBOM 미제공 SW구성요소에 대한 바이너리 분석을 수행해 직접 생성

○ (SSDF[56]) SW개발 생애주기 상에서의 보안 강화를 위한 프레임워크를 제시하고, SW구성요소 관리를 위해 SBOM을 활용하도록 가이드

- 안전한 SW활용 환경 구축을 위해 SW 배포와 제3자 개발 구성요소 보안점검에서 SW구성요소에 대한 원천 정보를 SBOM으로 관리·검증하도록 함

  * (PS.3.2) SW 배포 시 모든 SW구성요소의 원천 데이터를 수집·유지·공유하고 SBOM으로 관리, (PW.4.1) SBOM으로 제3자 SW구성요소 보안성 검토

○ (C-SCRM 가이드[57]) 기업이 공급망 상에서의 사이버보안 위협 관리 절차를 식별·평가·선정·구현할 수 있도록 정책·전략·절차 등 체계를 개발해 제공

* EO14028의 Sec. 4(c)와 (d)에 대응해 NIST에서 가이드 제작·배포

- 보안 관리를 위해 SW구성요소 관리 및 모니터링이 필요하고, 이를 위해 기업은 SBOM을 연동할 것을 고려하도록 가이드에 명기

[표 5] C-SCRM 가이드 내 SBOM 관련 항목

SBOM 관련 항목	내용
CM-8. 설정 관리 – 시스템 구성요소 목록 (SYSTEM COMPONENT INVENTORY)	SW구성요소 목록화를 위해 SBOM 제시·관리
RA-5. 위협 평가 – 취약점 감시 및 탐색 (VULNERABILITY MONITORING AND SCANNING)	취약점 관리 및 모니터링을 위해 SBOM 연계
SR-4. 공급망 위협 관리 – 원천 정보 (PROVENANCE)	SW구성요소 원천 정보 취득을 위해 SBOM 확보

* 출처: NIST(2022.5.), “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations”

56) NIST(2022.2.), “Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities”
57) NIST(2022.5.), “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations”

▨ 의료, 자동차 등 주요 산업 영역에서 SBOM 제출을 권고하는 사이버보안 강화 가이드를 공개해 산업에서의 자발적인 SBOM 활용 유도

○ (의료기기) FDA[58]는 시판 전에 인증 취득을 원하는 의료기기 제조업체를 위해 사이버보안 규정안 초안[59]을 마련해 의료기기의 안전·품질·보안 강화

- 2018년에 발표된 사이버보안 지침을 대체하며, 의료 장비의 안전 설계와 제품의 수명 전반에 걸친 사이버보안 위협 완화가 목표

  * 2022년 4월에 초안을 공개해 7월까지 의견수렴 및 내용 수정·보완 진행

- 제3자 SW구성요소에 대한 사이버보안 위협 관리를 위해 기기 내의 SW를 식별·추적하는 도구로써 SBOM을 활용하도록 함

○ (자동차) NHTSA는 차량에 대한 사이버보안 강화를 위해 관련 모범사례를 일반과 기술로 분류해 제공하는 보안 모범사례 가이드[60] 배포

- 자동차 산업에서의 사이버보안 강화를 위해 2016년에 관련 지침을 발표하고, 관련 ISO/SAE 21434[61] 국제표준을 반영해 해당 지침을 갱신

- 차량의 복잡한 공급망에서의 사이버보안에 대해 고객과 공급망업체 간 상호작용·종속성·책임성 확장이 요구되어 SW구성요소 관리의 필요성을 명시

* (G.10) 제조업체는 SW구성요소에 대한 DB, 즉 SBOM을 유지해야 하고, (G.11) 새롭게 발견된 취약점이 ECU와 차량에 어떤 영향을 미치는지 식별하기 위해 제조업체는 SW구성요소 세부 정보를 추적해야 함

58) 식품의약국(Food and Drug Administration), https://www.fda.gov/
59) FDA(2022.4.8.), "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff"
60) NHTSA(2020), "Cybersecurity Best Practices for the Safety of Modern Vehicles"
61) ISO/SAE 21434:2021, https://www.iso.org/standard/70918.html, 2022.12.14. 방문

4. 민관협력 체계 구축

▨ SBOM 개념 정립, 실증 과정에서 민간전문가의 협력 지원을 받고, 정부에서 계획한 표준화 및 가이드 생성에 대해 현장 의견을 수렴해 반영

○ SW구성요소 투명성 이니셔티브에서 구성한 워킹그룹을 민간 중심으로 구성해 전문적 지식·경험을 바탕으로 SBOM의 개념적 기반 확립

- 산·학·연 다방면의 전문기관들이 세부 워킹그룹에 참여함으로써 SBOM 정의·범위·기능·효과 등을 정리하고 실증 지원

  * (기업) GitHub, 시놉시스, PTC, GE Healthcare 등, (재단) 리눅스재단, OWASP 등, (대학·연구기관) CMU, University of Nebraska at Omaha, MITRE 등

○ NIST에서 작성한 SW공급망 보안 강화 가이드에 대해 산·학계로부터의 의견을 취합[62]해 내용을 보완 및 개선

- 행정명령에서 가이드의 표준·절차·제안에 대해 기존 또는 새로운 표준·도구·모범사례 식별을 위한 민간 의견 청취 과정을 거치도록 함

  * EO14028 관련: Sec.4.(b)에 근거해 NIST에서 의견수렴 과정 진행

- 2021년 6월 표준·가이드 관련 온라인 워크샵 개최해 약 150개 의견서 취합

▨ 공개SW 중심으로 SW공급망 보안 강화 방안을 마련하기 위해 민관협력 체계를 구축하고 이를 통해 SBOM 민간 확산 방안 논의

○ 부처·기관의 수장들과 민간 영역의 리더들을 2022년 1월 백악관에 소집해 공개SW 관련한 SW공급망 보안 이슈를 논의하는 보안정상회의 개최[63]

* (정부) 안보보좌관, 국가사이버국장, 국방부, 상무부, 국토안보부 등, (민간) MS, 구글, 애플, 메타, 아파치재단, 리눅스재단, OpenSSF 등

62) NIST SW공급망 보안 가이드에 대한 산·학계 입장문, https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/enhancing-software-supply-chain-security, 2022.12.14. 방문
63) 백악관(2022.1.13.), "Readout of White House Meeting on Software Security"

- 3가지 주제로 논의 진행: ① 공개SW의 보안 결함 및 취약성 방지, ② 결함 발견·수정 절차 개선, ③ 수정 배포·구현을 위한 응답 시간 단축
- 수정 배포 시간 단축을 위한 방안으로 SBOM 활용 가속화·개선 의견 제시

○ 후속 과정으로 동해 5월 워싱턴에서 2차 보안정상회의가 열렸고, 리눅스재단은 SBOM 확산을 포함한 SW 공급망 보안 강화 정책[64] 방안을 발표[65]

- 1차 회의에서 논의되었던 3가지 주제에 대해 10개 실행 계획을 도출하고, 이를 구현하기 위한 1.5억 달러 동원 계획 수립

  * 아마존, 구글, MS 등으로부터 3천만 달러 지원 약속 확인[66]

- SBOM 관련해서는 모든 곳에서의 활용을 촉진하기 위해 요구사항·포맷 도출, 도구 개발·지원, 교육·가이드 지원의 내용을 담은 세부 과제 제시

5. 법·제도적 기반 마련

▨ 행정명령 이전부터 SW공급망 투명성 확보에 대한 필요성이 제기되어 연방정부가 구매한 SW제품을 대상으로 하는 법안을 국회 중심으로 마련

○ 하원에서 2014년「사이버 공급망 관리 및 투명성 법안」[67]을 발의해 SBOM 유사 체계 도입을 통한 SW공급망 투명성 확보 필요성 제기

- 제3자 또는 공개SW 구성요소를 포함한 SW제품 조달 계약 시 BOM을 요구하도록 하는 가이드라인을 OMB에서 배포하도록 하는 내용 포함
- 산업계의 반발 등으로 최종 통과되지는 않았지만 정부 조달 상에서 SW제품에 대한 SBOM 제출 규정의 필요성을 인식시키는 계기로 작용

○ 사이버 공급망 관리 및 투명성 법안을 계기로, 상원은 2017년「IoT 사이버보안 개선법」[68] 입법을 추진해 IoT 기기에 대한 SBOM 기반 보안체계 기틀 마련

- 연방기관에서 구매한 IoT기기는 보안취약점을 가진 SW구성요소를 포함해서는 안 됨을 명시하였고, 이는 사실상 SBOM 기반 검증을 의미[69]

▨ 행정명령 발표 이후 사이버보안 관리가 요구되는 공공의 주요 영역을 중심으로 SBOM 제출을 의무화하는 법안을 입법해 법제화 추진

○ 정보통신 기술·서비스 계약에 대해 BOM을 제출하도록 하는「국토안보부 SW공급망 위협 관리법 2021」[70]이 2021년 7월에 발의되어 동해 10월 하원 통과

- 계약자에게 ① BOM 제출, ② BOM에 기술된 구성요소에 보안취약점이 없음을 인증, ③ 발견된 보안취약점 및 대응 계획 알림을 의무화하는 가이드를 국토안보부에서 배포하도록 함

  * "... each contractor ... shall submit to the covered officer - (1) the bill of materials used for such contract, upon the request of such officer ..."

- 해당 법안이 효력을 갖기 시작한지 180일 후부터 가이드 실제 적용

○ 시판 전 의료기기 승인을 위해 제조업체는 취약점 관리 계획과 함께 해당 기기에 대한 SBOM을 제출하도록 하는「PATCH 법」[71] 발의

- 사용자에게 전달될 SW구성요소에 대해 SBOM을 제출하도록 함

  * "... (4) The manufacturer shall furnish to the Secretary a software bill of materials, including commercial, open-sourced, and off-the-shelf software components that will be provided to users. ..."

- 2022년 3월 하원 발의와 함께 상원에서도 동법안[72] 발의 추진 중

64) 리눅스재단(2022.5.12.), "The Open Source Software Security Mobilization Plan"
65) OpenSSF(2022.5.12.), "The Linux Foundation and Open Source Software Security Foundation (OpenSSF) Gather Industry and Government Leaders for Open Source Software Security Summit II"
66) TechTimes(2022.5.16.), "Amazon, Microsoft, Google, and More Invest $30M to Reinforce Open Source Software Security"
67) CONGRESS.GOV, "H.R.5793 - Cyber Supply Chain Management and Transparency Act of 2014", https://www.congress.gov/bill/113th-congress/house-bill/5793/, 2022.12.14. 방문
68) CONGRESS.GOV, "S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017", https://www.congress.gov/bill/115th-congress/senate-bill/1691/, 2022.12.14. 방문
69) 관련 법이 2020년 12월 대통령 서명을 받아 NIST가 IoT 보안 강화 가이드를 배포하도록 하였고, 해당 가이드에서는 IoT기기 보안 관리를 위해 고객에게 공급자가 제공해야 하는 정보로 SBOM 권고
70) CONGRESS.GOV, "H.R.4611 - DHS Software Supply Chain Risk Management Act of 2021", https://www.congress.gov/bill/117th-congress/house-bill/4611/, 2022.12.14. 방문
71) CONGRESS.GOV, "H.R.7084 – PATCH Act of 2022", https://www.congress.gov/bill/117th-congress/house-bill/7084/, 2022.12.14. 방문
72) CONGRESS.GOV, "S.3983 – PATCH Act", https://www.congress.gov/bill/117th-congress/senate-bill/3983/, 2022.12.14. 방문

○ 연방기관에서 직·간접적으로 사용하는 공개SW 구성요소에 대해 CISA가 SBOM 기반 정기 보안 평가를 하도록 하는「공개SW보안법」[73] 발의 진행

- 법안에 CISA의 공개SW 보안관리 임무로 공개SW 보안 강화 지원, 보안 평가 프레임워크 개발, 보안 평가 시행, 핵심 기반 시설 시범 운영 적시
- 보안 평가 시행에 있어 SBOM과 같은 기계가독적 정보 활용토록 함

  * "...(i) perform an assessment of open source software components used directly or indirectly by Federal agencies based on readily available, and, to the greatest extent practicable, machine readable, information, such as— (I) software bills of material that are made available to the Agency or are otherwise accessible via the internet; ..."

▨ 조달 규정 개정을 통해 연방정부 전반에 걸친 SW공급망 보안 강화 적용

○ 관련 사항을 행정명령에 적시해 부처·기관에서 담당 역할 수행하도록 지시

  * EO14028 관련: Sec.4.(n) ~ (p)에 조달 규정 개정에 관한 사항 명기

- 국토안보부는 행정명령에 적시된 SW공급망 보안 강화 방안을 골자로 한 계약 언어(contract language)를 정의하고 권고안을 FAR 위원회에 제공
- FAR 위원회는 조달 규정에 반영될 수 있도록 국토안보부의 권고안을 검토하고, 최종안 반영 이후 각 기관은 이에 부합하지 않는 SW를 계약에서 제거

73) COMGRESS.GOV, "S.4913 – Securing Open Source Software Act of 2022", https://www.congress.gov/bill/117th-congress/senate-bill/4913, 2022.12.14. 방문

V 시사점

▨ 미국 정부는 SBOM의 안정적인 정착을 위해 이니셔티브 발족, 실증 수행 등으로 범주를 명확화하고 현장의 세부적인 이슈를 검토

○ 일찍이 SW공급망 투명성 확보 필요성이 제기되어 2014년 하원에서 입법을 시도했지만 SBOM 제출에 대한 산업적 저항으로 좌초된 경험이 있음

○ 실증으로 효과를 검증하고 SBOM에 대해 명확한 범주를 설정함으로써 산업에서의 혼란과 저항을 최소화하고 신중한 정책 방향성 수립

- 의료, 에너지 등 다양한 분야에서 3년 이상의 실증 과정을 거쳐 검증
- 지나치게 확장될 수 있는 SBOM 범위로 초래될 수 있는 산업적 부담을 줄이기 위해 SBOM 생성에 대한 필수 기준인 SBOM 최소요소 정의

▨ 불명확한 SBOM 생성·활용 프로세스로 인한 혼란과 포맷 불일치에 따른 재사용 저해 문제 해결을 위해 NIST에서 SBOM 관리 절차와 포맷 표준화 추진

○ SBOM 생성·활용 절차를 가이드로 표준화함으로써 연방 부처·기관뿐만 아니라 민간에서도 일관된 SBOM 도입을 유도하고 유통·공유 활성화

- 공공조달 담당자, SW개발자, 보안 시스템 관리·운영자 등 이해관계자별 가이드 제작해 SBOM 생애주기 상에서의 역할·기능 명확화
- 국제표준 포맷을 준용함으로써 기계가독성에 기반해 SBOM 이식·저장·관리 등의 자동화를 가능하게 하고 SBOM 재사용 활성화를 촉진

○ 절차·포맷의 표준화로 공공·민간에서의 SBOM 통용 기반을 마련함으로써 SW공급망 보안 위협에 대해 정확하고 민첩한 대응력을 가지게 함

- 솔라윈즈, Log4J 등 SW공급망을 통한 보안 위협에 주목해야 하는 이유는 SW구성요소에 대한 가시성이 부족할 경우 개선책 적용 시간이 지연될 뿐만 아니라 잠재적 위협 요소의 완전한 해소가 어렵기 때문임

  * 솔라윈즈는 첫 진입부터 공식 발표까지 15개월이 걸렸고, Log4J의 보안패치가 빠르게 이루어졌음에도 CISA는 잠재적 위협 관리를 위해 지속적인 모니터링 강조

- Log4J에 대해 美상원에서 CISCO 부사장은 SW구성요소 정보에 기반한 보안대응 체계 구축으로 빠른 대응이 가능했음을 증언[74]해 SBOM 필요성 피력

  * 2014년 Heartbleed 사건에서 취약점 식별에만 50일이 소요된 반면, 이후 SW구성요소에 기반한 보안대응 체계를 구축해 Log4j는 10일 만에 패치까지 완료

○ 국내에서도 SBOM 포맷에 대한 형식적 기준이 되는 국제표준들에 대한 정보를 공유함으로써 자발적인 SBOM 활용 활성화 유도 필요

- 국제적으로 통용·인정되고 있는 SPDX, CycloneDX, SWID 등에 대해 관련 정보를 제공하고 관련 국내의 표준을 홍보해 SBOM 활용 촉진

- 국제표준에 대한 부합화를 검토함으로써 글로벌 진출을 준비하는 SW산업에서의 SBOM 생성·관리를 위한 기반 정보 접근성 제고

▨ 미국 정부는 공공영역에서의 SBOM 제도화를 추진함으로써 발전 방향성을 제시하고, 이를 바탕으로 단계적이고 자발적인 민간 확산을 위한 기반 구축

○ 고수준의 안전이 요구되는 분야를 중심으로 법제화를 추진함으로써 SBOM의 점층적 확산을 위한 토대 마련

- 의료·자동차 등 산업별 보안 가이드 배포, 국토안보부 SW공급망 위협 관리법, PATCH법, 공개SW보안법의 입법 추진 등 주요 분야를 중심으로 SBOM을 권고·의무화함으로써 공공·민간에서의 단계적 확산 저변 확보

○ 사회 안전 영역뿐만 아니라 모든 SW융합산업에서 SW공급망 투명성 확보는 보안·라이선스 관리 측면에서 제품 품질에 대한 신뢰성과 연결되기 때문에 결국 기업의 경쟁력을 의미하게 될 것이라는 인식 확산 중

- SW공급망을 통한 보안 위협 사례가 증가하고 공개SW 라이선스 관리 필요성에 대한 인식이 높아짐에 따라 SBOM에 대한 요구도 함께 높아짐

  * 리눅스재단 설문조사[75]에 따르면 응답 기관 47%가 현재 SBOM을 사용하고 있으며, 2023년에는 88%가 사용할 것이라고 답변하였고, 공개SW 라이선스 준수 국제표준 OpenChain[76]에서도 BOM 생성·관리 절차를 확보하도록 함

- 미국 정부는 공공영역을 중심으로 SBOM을 제도화하고 있으며, MS, 구글 등 글로벌 IT기업도 기존의 체계를 변경해 정부의 정책 방향에 동조

○ 국내 SW공급·수요 기업에서도 글로벌 경쟁력과 SW공급망 투명성 확보를 위해 SBOM 효용성을 인식하고 적극적으로 활용 방안을 검토해야 하는 시점임

74) 美상원 증언 자료(2022.2.8.), "Testimony of Brad Arkin, Senior Vice President, Chief Security and Trust Officer, Cisco Systems Before Senate Homeland Security and Governmental Affairs Committee Responding to and Learning from the Log4Shell Vulnerability"
75) 리눅스재단(2022.1.), "Software Bill of Materials (SBOM) and Cybersecurity Readiness"
76) ISO/IEC 5230:2020, https://www.iso.org/standard/81039.html, 2022.12.14. 방문

참고 문헌

1. 국내문헌

· 민성현, 손경호(2020), "ICT 공급망 보안기준 및 프레임워크 비교 분석", 정보보호학회 논문지, Vol. 30, No. 6, pp.1189-1206.

· 손효현, 김동희, 김소정(2022), "사이버안보 강화를 위한 소프트웨어 공급망 보안 정책 연구 : SBOM 정책 추진 사례를 중심으로", Journal of Digital Convergence, Vol. 20, No. 2, pp.9-20.

· 최윤성(2022), "미국의 소프트웨어 공급망 보안 정책 동향: SBOM 사례를 중심으로", 정보보호학회지, Vol. 32, No. 5, pp.7-14.

2. 국외문헌

· Blocks & Files(2021.7.4.), "Kaseya VSA vulnerability opens a thousand-plus business doors to ransomware".

· Check Point(2021.12.10.), "Protect Yourself Against The Apache Log4j Vulnerability".

· ENISA(2020.11.), "GUIDELINES FOR SECURING THE INTERNET OF THINGS".

· ENISA(2020.2.), "PROCUREMENT GUIDELINES FOR CYBERSECURITY IN HOSPITALS".

· FDA(2022.4.8.), "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff".

· FEDERAL REGISTER(2022.6.1.), "Public Listening Sessions on Advancing SBOM Technology, Processes, and Practices".

· Fortress(2021.8.2.), "Enhancing Cybersecurity Best Practices with Software Bill of Materials (SBOM)".

· Gartner(2022.2.14.), "Innovation Insight for SBOMs".

· Kaseya(2021.7.5.), "Kaseya Responds Swiftly to Sophisticated Cyberattack, Mitigating Global Disruption to Customers".

· MS 블로그(2020.12.17.), "A moment of reckoning: the need for a strong and global cybersecurity response".

· MS 블로그(2022.5.10.), "Continued investments in supply chain security in support of the cybersecurity Executive Order".

참고 문헌

- NHTSA(2020), “Cybersecurity Best Practices for the Safety of Modern Vehicles”.
- NIST(2022.2.), “Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities”.
- NIST(2022.5.), “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations”.
- NTIA 블로그(2018.6.6.), “NTIA Launches Initiative to Improve Software Component Transparency”.
- NTIA(2019.10.1.), “Software Component Transparency: Healthcare Proof of Concept Report”.
- NTIA(2020.11.16.), “SBOM FAQ”.
- NTIA(2021), “How-To Guide for SBOM Generation”.
- NTIA(2021), “Survey of Existing SBOM Formats and Standards”.
- NTIA(2021.10.21.), “Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM)”.
- NTIA(2021.4.28.), “Energy Sector SBOM PoC Charter”.
- NTIA(2021.7.12.), “The Minimum Elements For a Software Bill of Materials (SBOM)”.
- OpenSSF(2022.5.12.), “The Linux Foundation and Open Source Software Security Foundation (OpenSSF) Gather Industry and Government Leaders for Open Source Software Security Summit II”.
- sonatype(2021), “2021 State of the Software Supply Chain”.
- Synopsys(2022.4.), “2022 OPEN SOURCE SECURITY AND RISK ANALYSIS REPORT”.
- TechTimes(2022.5.16.), “Amazon, Microsoft, Google, and More Invest $30M to Reinforce Open Source Software Security”.
- 리눅스재단(2022.1.), “Software Bill of Materials (SBOM) and Cybersecurity Readiness”.
- 리눅스재단(2022.5.12.), “The Open Source Software Security Mobilization Plan”.
- 美상원 증언 자료(2022.2.8.), “Testimony of Brad Arkin, Senior Vice President, Chief Security and Trust Officer, Cisco Systems Before Senate Homeland Security and Governmental Affairs Committee Responding to and Learning from the Log4Shell Vulnerability”.
- 백악관(2021.5.12.), “Executive Order on Improving the Nation’s Cybersecurity”.
- 백악관(2022.1.13.), “Readout of White House Meeting on Software Security”.
- 백악관(2022.3.7.), “OMB Statement on ‘Enhancing The Security Of Federally Procured Software’”

3. 기타

- CISA SBOM-A-RAMA, https://www.cisa.gov/cisa-sbom-rama, 2022.12.14. 방문.
- CONGRESS,GOV, https://www.congress.gov/.
- CycloneDX, https://cyclonedx.org/.
- INL SBOM PoC, https://sbom.inl.gov/, 2022.12.14. 방문.
- ISO/IEC 19770-2:2015, https://www.iso.org/standard/65666.html, 2022.12.14. 방문.
- ISO/IEC 5230:2020, https://www.iso.org/standard/81039.html, 2022.12.14. 방문.
- ISO/IEC 5962:2021, https://www.iso.org/standard/81870.html, 2022.12.14. 방문.
- ISO/SAE 21434:2021, https://www.iso.org/standard/70918.html, 2022.12.14. 방문.
- NIST SBOM 가이드, https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1, 2022.12.14. 방문.
- NIST SW공급망 보안 가이드에 대한 산·학계 입장문, https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/enhancing-software-supply-chain-security, 2022.12.14. 방문.
- NTIA Automotive sector 발표자료, https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_energy_automotive.pdf, 2022.12.14. 방문.
- NTIA, “NTIA Software Component Transparency”, https://www.ntia.doc.gov/SoftwareTransparency, 2022.12.14. 방문.
- Software Package Data Exchange, https://spdx.dev/.