주요국 SBOM(Software Bill of Materials) 정책 동향 분석

Analysis for Global SBOM(Software Bill of Materials) Policy Trends

김항규 선임연구원
소프트웨어정책연구소 SW기반정책·인재연구실
hkkim@spri.kr

Executive Summary

주요 국가 정부는 SW공급망 투명성 확보 수단 중 하나로 SW제품 내의 구성요소 정보를 기술한 문서, SBOM(Software Bill of Materials)에 주목하고 있다. 이는 공개SW를 비롯한 SW재사용 확산과 함께 신뢰 기반으로 형성된 SW공급망으로 국가 안보에 직·간접적으로 관련된 위협이 증가하고 있음에 기인한다. 디지털 가속화와 함께 신기술의 빠른 도입 수단으로 SW재사용이 전 산업에 걸쳐 필수적인 요소로 평가되는 만큼 관련된 위협 관리도 반드시 해결해야 하는 과제임을 뜻한다.

일본 정부는 경제산업성 내에 소프트웨어TF를 설치하고 의료·자동차·SW 분야에 걸친 SBOM 실증을 통해 개념 정립, 효과성 검증, 제도화 방안을 마련하고 있다. 이러한 움직임은 「ICT 사이버보안 종합대책 2022」을 통해 ICT 분야로 확대될 전망이다. EU는 공개SW 공급망 관리 측면에서 EU-FOSSA, FOSSEPS 등 프로젝트 추진을 통해 유럽 공공에서의 SW인벤토리를 구축·관리하고자 하고, D-SBOM과 같은 연구개발 프로젝트로 SBOM 원천기술 확보 및 실증에도 노력을 기울이고 있다. 뿐만 아니라 의료기기·IoT 보안 가이드 제시를 통해 SBOM 활용을 권고하고 있으며, 클라우드·의료기기 인증을 비롯해 디지털 요소를 포함한 제품에 SBOM을 적용하는 입법 추진을 통해 제도화 기반 마련 중에 있다. ICT 분야 보안에 관심이 높은 영국도 통신망 서비스 공급망 보안 강화를 위해, 보안 지침에 SBOM과 유사한 기준을 적용했다. 중국은 SW공급망 보안 강화 방안을 마련하기 위해 SBOM을 검토하는 협력체계 3S-LAB을 구성했고, CAICT를 중심으로 SBOM 관련 백서 및 가이드를 발간해 활용 확산을 위한 저변을 확대했다. 네덜란드는 주요 국가에서 추진하고 있는 SBOM 정책을 모니터링함으로써 효과적인 SBOM 도입 방안을 마련했다.

SW공급망 투명성 확보를 위해 SBOM 관련한 백서·가이드 배포, 실증 추진, 제도화 방안 마련 등의 글로벌 동향이 확인되고 있다. 국내 SW산업의 글로벌 경쟁력을 평가하는 기준으로 SBOM을 인식하고 기업에서는 생산·유통·활용 측면에서의 SBOM 도입을 적극적으로 검토해야 한다. 이를 뒷받침하는 정부의 지원 정책도 중장기적인 관점에서 준비될 필요가 있다.

Global governments are paying attention to SBOM (Software Bill of Materials), a document that describes the component information in software products, as one of the means to enhance the transparency of the software supply chain. This is due to the increase in threats such as security and license through the software supply chain formed on the basis of trust along with the spread of software reuse including open source software. As software reuse is evaluated as an essential element across all industries as a means of rapid application of new technologies along with digital transformation acceleration, it means that the management of the threats is also recognized as a task that must be solved.

The Japanese government has established a software task force within the Ministry of Economy, Trade and Industry, and is preparing a way to establish

a concept, verify effectiveness, and institutionalize it through SBOM proof-of-concept in the medical, automotive, and software fields. This movement is expected to expand to the ICT sector through the ICT Cyber Security Comprehensive Measures 2022. In terms of open source software supply chain management, the EU intends to build and manage a software inventory for European public services by promoting projects such as EU-FOSSA and FOSSEPS. In addition, the use of SBOM is recommended through the medical device and IoT security guide, and the institutionalization foundation is being laid by promoting legislation to apply SBOM to products including digital elements, including cloud service and medical device certification. The UK, which is highly interested in ICT security, also applied SBOM-like baselines to security guidelines to strengthen the security of the communication network service supply chain. China formed 3S-LAB, a cooperative system to review SBOM in order to prepare measures to strengthen software supply chain security, and published SBOM white papers and guides centering on CAICT, expanding the basis for widespread use. The Netherlands came up with an effective SBOM introduction plan by monitoring the SBOM policies promoted by other countries.

Global trends, such as distributing SBOM white papers and guides, promoting proof-of-concept, and preparing institutionalization measures to ensure transparency in the software supply chain, are being confirmed. Recognizing SBOM as a standard for evaluating the global competitiveness of the domestic software industry, companies should actively review the introduction of SBOM in terms of production, distribution, and application. The government's promotion policies that support this need should be prepared from a mid- to long-term perspective.

Ⅰ SW공급망 투명성 확보 수단, SBOM[1]

공개SW[2]를 비롯한 SW재사용 확산으로 SW공급망을 통한 위협 사례가 증가함에 따라 SW구성요소[3] 수준에서의 투명성 확보 필요성 제기

- 디지털전환 가속화로 전 산업에 SW재사용이 확산돼 SW제품의 구성요소에 대한 공급망 복잡성이 증가하면서 SW구성요소 가시성의 확보에 어려움 발생
  - SW신기술 도입, 빠른 시스템 구축, 비용 절감 등을 목적으로 공개SW를 포함한 SW재사용률이 높아지면서* SW개발 방식이 조립형으로 전환
    * 응답자 77%가 최근 1년 동안 조직의 공개SW 사용이 증가했다고 답변[4]
  - 글로벌 협업에 기반해 개발되는 공개SW, 상용SW 등 제3자 개발 SW구성요소의 재사용 확산으로 SW공급망의 경계가 국가를 넘어 복잡화 가중

- 신뢰 기반 채널로 동작하던 SW공급망(공개SW, SW업데이트 서버 등)에서 위협 사례가 공공·민간에 걸쳐 급증하면서 국가 안보 문제로 인식하기 시작
  - OpenSSL, Log4J 등 널리 사용되는 공개SW에 보안 취약점이 발견되면서 이를 악용해 데이터 탈취, 시스템 오작동 등의 시도 감지
    * Log4J 이슈 공개 후 72시간 이내에 80만 회 이상의 악용 시도가 나타남[5]
  - 주요 IT 인프라·시스템 업데이트 서버를 통해 악성코드가 침투하는 솔라윈즈, Kaseya 등 사례가 등장해 글로벌 공공·민간 영역에 피해 발생
    * 2025년까지 전 세계 조직 45%가 SW공급망 보안 위협을 경험하게 될 것[6]

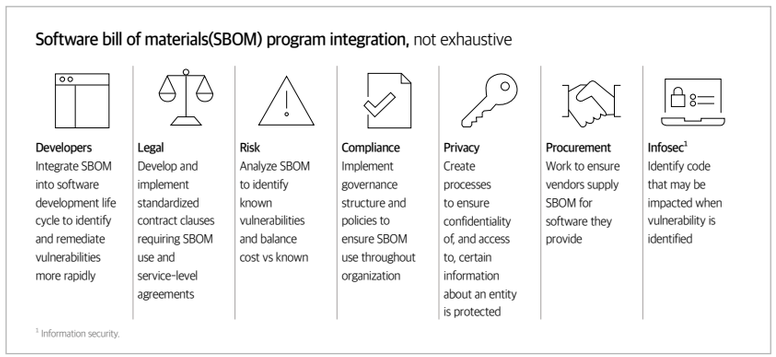
- 이에 따라, 국가 안보를 위한 SW구성요소 투명성 확보의 필요성 제기

1 Software Bill of Materials: SW구성요소에 대한 명세서로, SW를 이루는 구성요소의 세부 정보와 의존관계에 대한 정형화된 기술(Description)을 의미
2 소스코드가 공개돼 있어 사용수정배포를 자유롭게 허용하는 SW (자유SW와 오픈소스SW를 포괄)
3 빌드, 패키지, 배포 시점에 공급자로부터 정의된 SW 단위로 라이브러리, 파일 등을 뜻함 (美상무부)
4 OSI(2022.2.15.), "Ten takeaways from the 2022 State of Open Source survey"
5 CheckPoint(2021.12.29.), "The Numbers Behind Log4j Vulnerability CVE-2021-44228"
6 Gartner(2021.7.15.), "How Software Engineering Leaders Can Mitigate Software Supply Chain Security Risks"

SW공급망 투명성 확보 방안으로 SW구성요소 정보를 제공하는 SBOM에 주목

- 시스템 관리에서 SBOM을 활용할 경우, 제3자 SW구성요소 및 소스코드를 감시함으로써 보안 결함 발견 시 공급자·개발자 대응 전에 빠르게 조치 가능
  - SW재사용은 신기술 도입 및 시스템 구축 비용 절감을 위한 필수적 SW개발 방법론으로 자리매김했지만, 동시에 내포한 보안취약점도 동반하는 위험 발생
  - SBOM은 SW제품 내의 구성요소에 대한 세부 정보를 기술해 자동화에 기반한 SW공급망 관리를 가능하게 해 조직의 개발·법무·조달·위험관리 등을 지원

[그림 1] 조직 내 업무별 SBOM 도입 효과



출처: McKinsey(2022.9.19.), "Software bill of materials: Managing software cybersecurity risks"

- 미국 정부는 행정명령[7]을 통해 SW공급망 투명성 확보 방안으로 연방조달 납품 대상 SW제품에 대해 SBOM을 제출하도록 정책 추진

본고는 주요국에서 추진하고 있는 SBOM 관련 정책 동향을 살펴보고 시사점 도출

- 미국 정책 분석[8] 이후, 추가적으로 일본, EU, 영국, 중국 등 주요 국가에서 SBOM 도입을 위해 추진하고 있는 정책 동향 분석해 글로벌 정책 방향성 제시

7 백악관(2021.5.12.), "Executive Order on Improving the Nation's Cybersecurity"
8 SPRi(2022.12.16.), "미국 SBOM(Software Bill of Materials) 정책 분석 및 시사점"

Ⅱ 주요국 정책 동향

1 일본

경제산업성 내에 전담 조직 소프트웨어TF를 설치해 SBOM의 개념 및 효용성, 제도화 방안 등 검토 추진

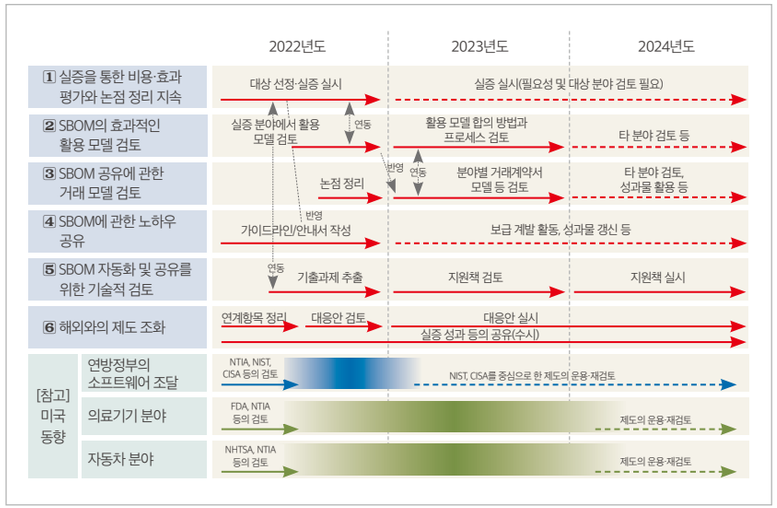
- 사이버물리 보안 확보 차원에서의 SW공급망 보안 강화를 위해 전문가로 구성된 조직체계를 마련해 SBOM을 포함한 SW관리 방법을 검토
  - 산업사이버보안연구회의 제도·기술·표준화 워킹그룹1에 3개 하위 횡단 분야 중 하나로 소프트웨어TF 설치·운영
    * 산업사이버보안연구회의 첫 회의를 '17년 12월에 개최하고, 소프트웨어TF를 포함한 제도·기술·표준화 워킹그룹1을 '18년 2월 발족
  - 소프트웨어TF는 ▲ 공개SW 관리 방법에 관한 우수사례집 발간, ▲ SBOM 정책 추진 방안 마련, ▲ SBOM 활용 촉진을 위한 실증사업(Proof-of-Concept: PoC) 실시를 주요 기능으로 설정

- SBOM 정책 방안 마련을 위해 산·학·연·관[9]이 참여하는 회의 운영
  - (1~3회) 절차적·개념적 기준 정립과 도입 효과 검토를 위해 SBOM 작성·운용 자동화, 필요 정보 및 수준, 공유·계약·은닉 등 논의 ('19)
  - (4회) SBOM 도입 비용 및 효과 검토와 활용 촉진을 위한 실증 제안 ('21.1)
  - (5회) SBOM 실증 수행·점검, SBOM 도입·활용의 장애·과제 논의 ('21.10)

- 6회 회의 이후 SBOM 활용 촉진을 위한 가이드라인 수립 및 제도화 방안 검토를 진행해 실질적인 SBOM 도입을 위한 기틀 마련 준비
  - (6회) 실증 성과를 정리하고 도구 정비 및 국제표준 포맷 논의 ('22.3)
  - (7회) SBOM 실증 대상 분야를 의료기기, 자동차, SW로 확대하고, 노하우집과 활용·거래 가이드의 구성안 제시·검토 ('22.7)

9 (산) 의료기기협회, SW협회, 도요타 등 (학) 오사카大, 나고야大 등 (연) 일본 전신 전화 주식회사 사회 정보 연구소 등 (관) 내각 사이버보안센터, 경찰청, 총무성, 방위장비청 등, 관은 옵저버로 참여

[그림 2] 일본 소프트웨어TF의 SBOM 검토 계획(안)



출처: 경제산업성(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"

소프트웨어TF를 중심으로 실증사업을 추진함으로써 SBOM 도입에 따른 비용·효과를 평가하고 활용·거래 모델과 기술적 측면에서의 자동화·공유 방안 검토

- 자율주행 시스템 검증 공개SW[10]를 실증 대상으로 선정하고, 공급자-제품 벤더-사용자 기업으로 SW공급망을 구성해 SBOM의 유통 과정을 실증[11]
  - (실증체제) 공급자가 개발한 SW구성요소에 대한 SBOM을 제품 벤더가 개발한 부분에 대한 SBOM과 통합해서 사용자 기업에게 제공
    * (일정) 실증 실시('21.9~11), 결과 분석 및 요약('21.12~'22.2)
  - (실증 항목) SBOM 도입의 효과와 비용을 정량적으로 산출*해 수작업을 통한 SW 공급망 관리 상황(SBOM 체계·도구 미도입)과 비교 평가
    * (효과) 취약점 수정까지 단축된 시간, 라이선스 위반 잔류 위협 저감도 등, (비용) 초기 체제 구축 및 환경 정비, 작성 공수와 도구·부품 관리 등으로 발생하는 비용

10 GARDEN ScenarioPlatform, NTT 데이터 ARC에서 공개SW로 개발해 자율주행SW의 안전성 평가를 위한 기능 동작 시뮬레이션 시나리오 생성 기능 제공, https://github.com/open-garden/garden, 2022.12.15. 방문
11 경제산업성(2021.10.29.), "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"

  - (결과) 취약점 발견 이후 대응 시간 단축, 공개SW 종속성 분석 정확도 향상 등 긍정적인 결과를 보였지만, 이는 SBOM 초기 도입 공수와 도구 기반 작성·활용 효과가 특정 조건*에 부합해야 함을 전제함[12]
    * SBOM 도구의 초기 공수·비용이 월등하게 낮고, SBOM 도구 정확도가 수작업과 동등하거나 그 이상이어야 하며, 공개SW가 아닌 상용SW 구성요소는 제외

- SBOM 도입 필요성이 제기되거나 효과가 높다고 평가되는 의료기기, 자동차, 소프트웨어 분야로 실증 범위를 확대 추진[13]
  - 하나의 실증으로 SBOM의 모든 활용사례(Use-Case)를 포괄하기 어렵기 때문에 분야에 맞는 전제 설정으로 실증을 수행하고 유효성 검증
  - 분야별 법제도의 요구, 비용·효과의 수용성 등에 근거해 SBOM 활동모델을 검토하고, 실증 등으로 얻은 지식을 공유해 SBOM 사용 촉진

[표 1] 일본 SBOM 실증의 분야별 중점 사항

실증 분야	중점 사항
의료기기	• 법제도의 요구에 맞춘 정밀도가 높은 SBOM 생성·관리가 요구됨 • 의료기관(사용자 기업)에 의한 SBOM 활동의 가능성 검토 • 관련 규제: IMDRF 가이드[14] 등
자동차	• 공급망이 넓고 깊은 계층 구조로 이루어지고 해외도 포함돼 있음 • SBOM 공통화를 이룸으로써 신뢰성 확보를 통한 비용 절감 기대 • 관련 규제: 미국 NHTSA 지침[15], UN R155[16] 등
소프트웨어	• SBOM 생성 주체가 되는 사례가 많고, 관련 도구에 대한 넓은 지식과 깊은 이해가 있어 SBOM 도입을 통한 이익이 클 것으로 기대 • SBOM의 효과적인 공유 방법, 상호운용 가능한 포맷으로의 작성 등 검토

출처: 경제산업성(2022.7.26.), "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"

12 경제산업성(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 경제산업성(2022.7.26.), "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"
14 International Medical Device Regulators Forum(2020.3.18.), "Principles and Practices for Medical Device Cybersecurity"
15 NHTSA(2020), "Cybersecurity Best Practices for the Safety of Modern Vehicles"
16 UN Regulation No. 155(2021.3.4.), "Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system"

경제산업성은 공개SW의 관리 방법 및 취약성 대응을 포함한 우수사례집[17]을 배포해 민간의 SBOM 활용 확산을 촉진

- 모범사례를 20개 이상의 국내외 주요 기업으로부터 선정해 보안취약점 대응과 적절한 관리 방안을 중심으로 공개SW 활용법 공유
  - 2021년 4월 첫 공개[18] 이후 소프트웨어TF 진행과 함께 지속 업데이트

- SBOM 또는 SW구성요소를 분석·관리하는 유사 체계를 구축한 기업 사례들을 분석해 SBOM 도입 필요성에 대한 인식을 제고하고 활용 활성화 유도
  - (도요타) OpenChain[19] 준수와 공급망 관리를 위해 SPDX Lite[20]를 채용하고, 활용 확산을 위해 국제 전시회에서 홍보·데모 진행
  - (올림푸스) 공급업체로부터 부품 및 SW제품 납품 시 공개SW 이용 유무 확인서를 요구하고 있고, SPDX Lite 도입을 검토
  - (히타치) 제품화 과정에서 SBOM을 통한 관리와 상용도구 활용을 통해 보안 취약성 대응과 엄격한 공개SW 라이선스 준수 구현

총무성은 「ICT 사이버보안 종합대책 2022」[21]에 SBOM 검토 필요성을 적시해 SBOM 적용 범위를 ICT 전반으로 확대할 것을 시사

- 일본 정부는 사회 전체의 디지털 전환과 공공의 사이버 활용 확산을 수반하는 사이버 보안 확보를 위해 ICT 분야에 대한 사이버보안 종합대책 발표
  * 「사이버보안 기본법」[22]에 의거해 2021년 7월에 「ICT 사이버보안 종합대책 2021」을 발표했고, 사회 전체의 디지털 전환과 시책 전개의 가속화를 위해 새롭게 정리된 종합대책을 2022년 8월에 공표
  - 중점 시책으로 ▲ 정보통신 네트워크의 안전성·신뢰성 확보, ▲ 사이버 공격에 대한 자율적 대처 능력 향상, ▲ 국제 연계 추진, ▲ 보급 개발 추진을 제시

17 경제산업성(2022.5.10.), "OSS の利活用及びそのセキュリティ確保に向けた管理手法に?する事例集"
18 경제산업성(2021.4.21.), "オープンソースソフトウェアの利活用及びそのセキュリティ確保に向けた管理手法に関する事例集を取りまとめました"
19 공개SW 거버넌스에 관한 국제표준으로 SBOM 생성·관리 내용 포함, https://www.iso.org/standard/81039.html, 2022.12.15. 방문
20 SBOM 작성 포맷 국제표준 SPDX(Software Package Data eXchange)를 경량화한 표준 포맷
21 총무성(2022.8.), "ICT サイバーセキュリティ総合対策 2022"
22 e-gov, "サイバーセキュリティ基本法", https://elaws.e-gov.go.jp/document?lawid=426AC1000000104, 2022.12.15. 방문

- 정보통신 분야에서의 공급망 위협 대응을 위한 향후의 대처 중 하나로 SBOM 도입 가능성 검토를 제시해 ICT 사이버보안 강화에 활용
  - 전국 5G의 특정 기지국 개설 설계 인정 및 지역 5G 면허 시, 공급망 위협 대응을 포함한 사이버보안 대책 강구를 조건으로 요구
  - SW구성요소 수준의 취약성 대응 방안으로 SBOM 도입 필요성 제기
  * "Apache Log4j와 같은 널리 사용되는 SW구성요소의 취약성에 대처하는 것이 중요해지고 있는 동안 SW제품의 구성요소를 관리하고 취약성에 신속하게 대응할 수 있는 메커니즘인 SBOM(Software Bill of Materials)의 경우, 정보통신 분야에서의 도입 가능성을 검토하는 것이 적절하다. 또한, 널리 보급되는 통신용 애플리케이션 등에 관한 이용 상 주의 방식을 검토해 나가는 것이 적당하다." -「ICT 사이버보안 종합대책 2022」中

2 EU

공개SW 공급망 강화 측면에서 SW인벤토리 관리를 통해 안전하고 신뢰할 수 있는 공개SW 활용 촉진을 목적으로 하는 프로젝트 추진

- EU는 공공서비스에서 활용되고 있는 주요 공개SW의 목록화 및 관리를 통해 SW자산·보안취약점 관리 및 재사용 활성화 유도
  - 공개SW 전략 발표, 전담 조직 개편 등을 통해 공공서비스에서 공개SW 활용을 촉진시켜왔고, 이 중 중요(Critical)[23] 공개SW를 SW인벤토리 형태로 관리함으로써 사실상 공개SW 중심으로 EU 단위의 SBOM 관리를 진행

- 유럽의회와 EC[24]는 SW공급망 보안 위협에 대응해 공개SW를 중심으로 SW코드의 보안성 및 투명성 강화를 위한 EU-FOSSA 프로젝트[25] 수행
  - Heartbleed[26]를 비롯한 SW공급망 보안 위협에 대한 우려가 증폭되면서 공개SW의 무결성·보안성 강화를 위한 체계적인 접근법 확립을 프로젝트 목표로 설정

23 유럽 공공서비스에서 활용·의존하고 있는 공개SW 구성요소 중 부수어지기 쉬운(Fragile) 프로젝트를 지속가능한 형태로 관리하고자 중요(Critical) SW로 식별
24 European Commission(유럽 집행위원회), https://ec.europa.eu/
25 EC DIGIT(2016.1.29.), "EP Pilot Project 'Free and Open Source Software Auditing'"
26 2014년 보안 연결에 사용되는 공개SW OpenSSL에서 서버와 연결 유지를 위해 전송하는 심장박동(heartbleed) 신호 통신 과정에 보안 취약점이 발견된 사례, 당시 보안 웹 서버 중 약 17%(약 50만 개)가 취약점에 노출

* 파일럿 프로젝트('15~'16) 시작해, EU-FOSSA 2('17~'20)[27]로 확대

- EU 연구기관 및 공공에서 공통으로 사용하는 공개SW를 취합해 SW인벤토리를 구축함으로써 보안취약점 대응 방안 마련

• EU-FOSSA의 연장선상에서 공공서비스에 활용 중인 공개SW에 대한 체계적 관리를 위해 FOSSEPS 파일럿 프로젝트[28] 발표

- SW자산 관리 측면에서 공공기관이 개발한 공개SW의 재사용 활성화와 중요 공개SW의 지속가능한 관리를 위해 프로젝트 추진

* ▲ 유럽 공공서비스를 위한 공개SW 응용프로그램 카탈로그, ▲ 중요 공개SW, ▲ 공개SW 기반 유럽 공공서비스 협력을 프로젝트 범주로 설정

- 공공행정의 안전한 공개SW 활용을 위해 중요 공개SW 목록을 도출하고 이를 체계적인 SW자산 관리에 이용

* 기존 EU 연구기관으로 한정된 중요SW 범위를 모든 공공 서비스로 확대

EU 기술혁신 프로그램 Horizon 2020을 통해 SBOM 관련 기술 연구와 실증을 수행하는 D-SBOM(Distributed SBOM) 프로젝트[29] 지원

• 기술 기반의 사회적 신뢰성 확보를 위해 EU는 차세대 인터넷 이니셔티브[30]를 바탕으로 SW신기술 블록체인 프로젝트에 투자

- EU 투자 기반 프로젝트 TruBlo[31]를 통해 블록체인 기술 확보를 위한 투자*가 진행됐고, 이 중 하나로 D-SBOM 프로젝트가 선정됨

* Horizon 2020 Grant agreement No. 957228('20.9~'23.11)[32]에 근거하고 있으며, TruBlo는 D-SBOM을 포함해 총 45개 프로젝트 지원 중('22 기준)

27 EC DIGIT(2018.4.5.), "EU-FOSSA 2 Project Charter"
28 EC DIGIT(2022.2.2.), "Free and Open Source Solutions for European Public Services(FOSSEPS) - Project Charter"
29 D-SBOM, https://www.trublo.eu/d-sbom/, 2022.12.15. 방문
30 NGI(Next Generation Internet), https://www.ngi.eu/
31 TruBlo, https://www.trublo.eu/about-this-project/, 2022.12.15. 방문
32 CORDIS(The Community Research and Development Information Service), "Trusted and reliable content on future blockchains", https://cordis.europa.eu/project/id/957228, 2022.12.15. 방문

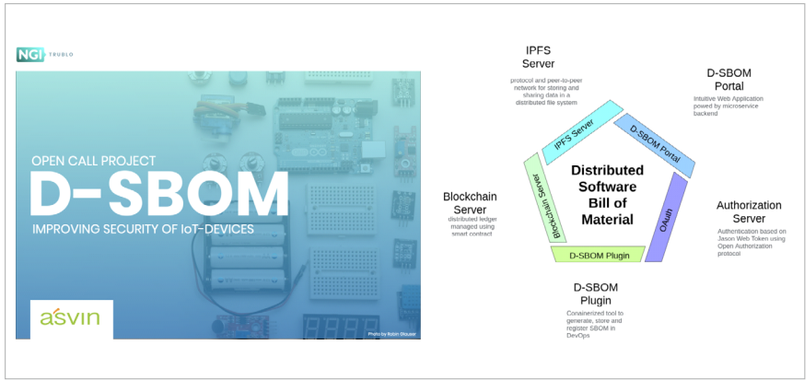
• IoT SW공급망 보안을 강화를 목적으로 하는 블록체인 기반 분산형 SBOM 기술 프로젝트에 투자해 SBOM 원천기술을 확보하고자 함

- 기존의 중앙집중적 SBOM 관리 시스템으로는 IoT의 복잡한 SW공급망을 관리하기 어려워 블록체인 기반 분산형 SBOM 생성·관리 기술 개발

* 독일 IoT SW공급망 보안 전문기업 Asvin[33]에서 프로젝트 추진 ('22~, 15개월)

- 개발된 D-SBOM을 자동차 산업에 적용한 데모를 구현하고 관련 1-티어 공급자, OEM 등의 승인·검토를 걸쳐 실효성을 검증하는 실증 수행

[그림 3] D-SBOM 프로젝트



출처: (좌)https://www.trublo.eu/d-sbom/, (우)https://asvin.io/d-sbom-technical-components/
주석: (좌) 프로젝트 대표 이미지, (우) D-SBOM 기술적 구성요소

유럽 보안 전문기관 ENISA는 의료기기, IoT 등에서의 사이버보안 강화를 위해 SBOM 활용을 권고하는 보안 가이드라인 배포

• 의료기관은 구매한 시스템 및 제품에 포함된 SW·HW에 대해 구성명세서(BOM)를 공급자에게 요구할 것을 권고

- 인터넷, 무선통신 등을 통한 의료기기의 상호연결성이 증가함에 따라 병원의 조달 과정에서 사이버보안을 강화하도록 하는 보안지침서[34] 공개

33 asvin, https://asvin.io/
34 ENISA(2020.2.), "PROCUREMENT GUIDELINES FOR CYBERSECURITY IN HOSPITALS"

- 취약점 식별·관리 절차 구현을 위해 제시된 보안 지침에 공개된 취약점 정보 기반 추적 시스템에서 BOM 활용을 검토하도록 함
  * "Healthcare organizations may consider including a requirement for the Bill of Materials (BOM) used in acquired systems or products. This will may help in the tracking of vulnerable systems in a healthcare organization's infrastructure based on publicly available vulnerability information." - ENISA 의료기기 보안가이드 中

• IoT 공급망 보안 강화를 위해 관련 이해관계자가 준수해야 하는 보안 지침 중 하나로 SBOM을 제공하도록 함
  - 이질적이고 복잡한 공급망으로 구성된 IoT 생태계 본질을 고려해 공급망을 통한 보안 위협 대응을 위한 가이드라인[35] 배포
  - SBOM은 SW구성요소 가시성을 확보해 보안 위협에 대한 빠른 식별·대응을 가능하게 하기 때문에 IoT 공급망 전체에 대해 제공돼야 한다고 강조
    * "(PRO-13) PROVIDE SOFTWARE BILL OF MATERIALS (SBOMS) FOR IOT DEVICES" - ENISA IoT 보안가이드 中

클라우드 서비스, 의료기기 관련한 인증체계에서 SW공급망 투명성 제고를 위해 SBOM 도입을 검토하거나 SBOM에 준하는 정보를 요구

• 유럽의 단일화된 클라우드 인증 제도 확립을 추진하는데 있어 SBOM 관리 및 제공에 관한 항목을 포함한 클라우드 서비스 인증체계 제안
  - 유럽의회와 유럽이사회에서 「사이버보안법(Cybersecurity Act)」[36]을 제정해 ENISA에 유럽 사이버보안 인증 프레임워크 구축 임무를 부여
  - ENISA는 클라우드 인증체계 초안[37]을 공유해 의견수렴을 진행
  - 클라우드 서비스 제공자(Cloud Service Provider: CSP)가 준수해야 하는 보안 개발 관련 항목에 제공하는 클라우드 서비스에 대한 SBOM 관리와 고객 요청 시 SBOM 제공을 명기
    * "(DEV-02.1) The CSP shall maintain a list of dependencies[38] to hardware and software products used in the development of its cloud service (DEV-02.3) The CSP makes its list of dependencies available to customers upon request" - ENISA 클라우드 인증체계 초안 中

• 의료기기의 안전 확보를 위해 판매 시 획득해야 하는 인증 과정에서 SBOM에 준하는 정보를 관리하도록 요구[39]
  - EU 내에서 의료기기*를 판매하기 위해서 제품 제조사 또는 수입자는 반드시 CE Marking 인증을 취득해야 하는 내용으로 의료기기 규정[40] 제정
    * 의료기기를 의료 목적으로 사용하는 장비, 자재, SW 등의 단독 또는 조합으로 정의
  - CE Marking 근거 법안[41]에서 심각한 위협을 가진 제품에 대한 빠른 대응을 위해 회원국 간에 교환하는 정보에 공급망 정보를 포함하도록 함
    * "Article 22.3 The information ... shall include all available details, in particular the data necessary for the identification of the product, the origin and the supply chain of the product, the related risk, ..." - Regulation No 765/2008 中
  - SW부분에 대한 완전 추적 가능한 목록을 CE Marking 인증에서 요구하는 것은 SW구성요소 투명성 확보를 위한 SBOM 내용과 유사하다고 평가[42]

EC는 유럽 내에서 디지털 요소를 가진 제품[43](이하 디지털 제품)을 판매하기 위해 SBOM 제출을 요구하는 「사이버복원력법(Cyber Resilience Act)」 제안[44]

• 공급망이 국가를 넘어 복잡하게 얽히는 디지털 제품에 대해 회원국의 공통 표준화된 사이버보안 프레임워크 구축을 위해 입법 추진
  - 위원장 폰데어라이엔(Von der Leyen)이 2021년 9월 국정연설에서 사이버보안의 공통 표준화를 위해 「사이버복원력법」 제안 계획 발표[45]

35 ENISA(2020.11.), "GUIDELINES FOR SECURING THE INTERNET OF THINGS"
36 EUR-Lex(2019.4.17.), "Cybersecurity Act", https://eur-lex.europa.eu/eli/reg/2019/881/oj 2022.12.15. 방문
37 ENISA(2020.12.), "EUCS - CLOUD SERVICES SCHEME"
38 의존관계를 식별·문서화하도록 하는 사이버보안법 Article 51(d)에 근거함과 함께 의존관계 목록(list of dependencies)을 SBOM이라고도 지칭한다는 것을 인증체계 초안 문서에 적시
39 EMA, "Medical Devices", https://www.ema.europa.eu/en/human-regulatory/overview/medical-devices, 2022.12.15. 방문
40 EUR-Lex(2017.4.5.), "Regulation (EU) 2017/745", https://eur-lex.europa.eu/eli/reg/2017/745/oj 2022.12.15. 방문
41 EUR-Lex(2008.7.9.), "Regulation No 765/2008", https://eur-lex.europa.eu/eli/reg/2008/765/oj 2022.12.15. 방문
42 네덜란드 NCSC(2021.1.), "Using the Software Bill of Materials for Enhancing Cybersecurity"
43 "a product with digital elements": 모든 SW·HW제품과 원격 데이터 처리 솔루션(SW·HW구성요소를 포함해 시장에서 분리돼 위치하는 것)을 지칭
44 EC(2022.9.15.), "Cyber Resilience Act", https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act, 2022.12.15. 방문
45 EC(2021.9.15.), "State of the Union 2021", https://ec.europa.eu/info/strategy/strategic-planning/state-union-addresses/state-union-2021_en, 2022.12.15. 방문

- 제안서는 제조사가 제품의 개발 생애주기에서 취약성을 최소화하고 사용자가 제품 선정·활용에서 보안성을 검토하도록 하는 환경 조성을 목적으로 함
  * 사이버보안 위험 수준에 따라 제품을 1등급과 2등급으로 분류하며, 위험 수준이 높은 2등급 제품은 외부 기관의 적합성 평가를 의무적으로 받아야 함

• 디지털 제품의 시장 출시 전에 제출해야 하는 기술 문서에 보안 평가, 취약점 대응, 준수여부 확인 등을 위해 SBOM을 포함시키도록 함
- 취약점 분석을 위해 디지털 제품에 포함된 구성요소를 SBOM 등의 방법으로 식별·문서화해야 함을 강조
  * SBOM은 제조자·구매자·운영자의 공급망에 대한 이해를 향상시키는 정보를 제공함으로써 취약점 및 위협 대응을 포함해 다양한 도움을 주며, 특히 제3자가 개발한 구성요소에 대한 보안 취약성 존재 여부 검증에 중요한 역할을 함
- SBOM의 포맷·요소 정의 필요성과 함께 제조사가 법 준수를 위해 수행해야 하는 SBOM 생성·공유·제출 관련한 사항을 세부 조항으로 제시

[표 2] 「사이버복원력법」 제안서의 SBOM 관련 조항

구분	SBOM 관련 조항
포맷 및 요소	**EC는 법 구현 수단으로 SBOM의 포맷과 요소를 기술할 수 있다.** (Article 10 15.) The Commission may, by means of implementing acts, specify the format and elements of the software bill of materials set out in Section 2, point (1), of Annex I.
제조사의 필수 보안 요구사항	**디지털 제품 제조사는 SBOM을 포함한 방법으로 제품의 취약성·구성요소를 식별·문서화해야 한다.** (Annex I 2(1)) (Manufacturers of the products with digital elements shall) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;
제품 요건	**디지털 제품은 가능하면 SBOM 접근 위치를 가지고 있어야 한다.** (Annex II 6.) (As a minimum, the product with digital elements shall be accompanied by) if and, where applicable, where the software bill of materials can be accessed;
기술 문서	**기술 문서는 SBOM 등을 포함해 제조사에서의 취약점 대응 절차에 대한 완전한 정보·명세서를 포함해야 한다.** (Annex V 2(b)) (The technical documentation referred to in Article 23 shall contain at least the following information, as applicable to the relevant product with digital elements a description of the design, development and production of the product and vulnerability handling processes, including) complete information and specifications of the vulnerability handling processes put in place by the manufacturer, including the software bill of materials ...
	기술 문서는 시장 감시 당국의 필수 보안 요구사항 준수 여부 확인을 위해 SBOM을 포함해야 한다. (Annex V 7.) (The technical documentation referred to in Article 23 shall contain at least the following information, as applicable to the relevant product with digital elements) where applicable, the software bill of materials as defined in Article 3, point (36), further to a reasoned request from a market surveillance authority provided that it is necessary in order for this authority to be able to check compliance with the essential requirements set out in Annex I.

출처: EC(2022.9.15.), "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020"; EC(2022.9.15.), "ANNEXES to the PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020"

3 영국

영국 정부는 ICT 분야의 보안 강화 정책을 추진하는 가운데, SW공급망 투명성 확보 방안 중 하나로 SBOM을 인식하고 활용 권고

• 국가의 공급망 보안 및 5G 통신 보안정책을 담당하는 DCMS[46]에서 NCSC[47]와 협력해 보안정책 수립 및 이행
- NCSC는 정부통신본부(GCHQ) 산하의 사이버보안 전문 기관으로, 기술적 지침 개발 및 자문 등을 통해 DCMS를 지원

46 디지털문화미디어스포츠부(Department for Digital, Culture, Media & Sport), https://www.gov.uk/government/organisations/department-for-digital-culture-media-sport/.
47 국가사이버보안센터(National Cyber Security Centre), https://www.ncsc.gov.uk/

• DCMS는 공급망 보안관리 현황 파악을 위해 의견 수렴[48] 과정을 진행했고, 그 가운데 SBOM 필요성 제기 의견 포함
  - 의견 수렴은 2021년 5월부터 약 2개월간 온라인으로 진행됐으며, 214개의 개인·기관 의견을 종합해 공급망 보안에 대한 인식도를 조사
    * (주요 지표) 공급망 보안 위협 관리의 장애요인으로 98%가 공급망의 제한적 가시성을 꼽았으며, 정부의 역할로는 95%가 가이드 제시로 응답
  - 설문 응답 중 공급망 보안관리 방안 중 하나로 공급자로부터 SBOM을 취득해 보안 검토를 수행하는 의견 제안

• NCSC는 기기 보안 가이드를 배포해 SBOM 활용을 권고
  - 인터넷을 통한 조직의 위협에 대응하도록 모바일 기기, 태블릿, 랩탑 등 인터넷으로 연결된 기기에 대한 보안 가이드[49]를 배포
  - 기기의 업데이트 세부 정보에 알려진 취약점의 개선 여부를 공개하도록 하고, 관련 정보를 기계가독적인 형태로 기술하는 SBOM을 활용해 관리자가 직접 분석할 수 있도록 지원

통신망 서비스 공급망 보안 강화를 위해 관련 법제화를 추진하고, 이를 근거로 DCMS는 SBOM과 기능적으로 유사한 보안 지침을 마련

• 5G 및 유선망 보안 강화를 위해 통신(보안)법[50]을 근거로 통신망 서비스 제공자, 네트워크·장비 공급자 등이 준수해야 하는 보안 행동강령 초안[51] 공개
  - 차세대 통신망 보안·경제 위협의 확산에 대한 대응책 마련을 위해 정부는 영국 통신 공급망 리뷰 보고서[52]를 발간해 보안 프레임워크 필요성 제기
  - 기존의 통신법 2003을 통신(보안)법 2021로 개정하고, 세부 보안조치 항목을 기술한 전자통신(보안조치) 규정 2022 초안[53]을 국회에 전달

48 DCMS(2021.11.15.), "Government response to the call for views on supply chain cyber security"
49 NCSC(2021.6.), "Device Security Guidance", https://www.ncsc.gov.uk/collection/device-security-guidance. 2022.12.15. 방문
50 legislation.gov.uk, "Telecommunications (Security) Act 2021", https://www.legislation.gov.uk/ukpga/2021/31/. 2022.12.15. 방문
51 DCMS(2022.3.1.), "Draft Telecommunications Security Code of Practice"
52 DCMS(2019.7.), "UK TELECOMS SUPPLY CHAIN REVIEW REPORT"
53 legislation.gov.uk, "The Electronic Communications (Security Measures) Regulations 2022", https://www.legislation.gov.uk/uksi/2022/933/. 2022.12.15. 방문

- 이에 대한 기술적인 가이드를 제공함으로써 새로운 보안 프레임워크를 제시하는 통신보안 행동강령 초안을 발표

• 행동강령 초안에 공급망 보안 강화를 목적으로 SW구성요소 수준의 보안관리 기준을 적시해 ICT 공급망 보안에의 SBOM 유사 체계 도입 시사
  - 통신망 서비스의 공급망 상에서 발생할 수 있는 보안 위협 관리를 위해 NCSC에서 발간한 공급자 보안 평가 가이드[54]를 기준으로 제시
  - 공급자 보안 평가 가이드에 SBOM의 목적·기능 측면에서 유사한 SW구성요소 인벤토리 유지, 내외부 SW구성요소 관리 등을 평가항목으로 포함

[표 3] 통신보안 행동강령 내 SBOM 관련 보안 평가항목

평가항목	보안 기대치
V.A.7 도구·SW·라이브러리 사용 (Use of Tools, Software and Libraries)	**제3자 도구, SW구성요소, SW라이브러리에 대한 인벤토리 유지** Third party tools(e.g. code compilers), software components and software libraries that are used within and in the development of the product are inventoried.
V.B.3 내부 구성요소 관리 (Internal Component Management)	**모든 내부 구성요소의 현행화** Any shared internal components or libraries are kept up to date and only the latest stable, supported version is used.
V.B.4 외부 구성요소 관리 (External Component Management)	**지원하는 외부 구성요소만 제품 내에 사용** Only supported external components are used within a product.

출처: NCSC(2022.3.), "Vendor security assessment"

54 NCSC(2022.3.), "Vendor security assessment"

4 중국

공급망 보안관리를 위해 클라우드 서비스, SW 분야를 중심으로 평가 및 보안 표준을 제정하고, SW공급망에 대해서는 SBOM을 활용하도록 권고

- 공산당과 정부기관 및 핵심정보기반시설 운영자가 도입·이용하는 클라우드 서비스에 대해 보안 평가를 의무화하는 새로운 규정[55] 마련
  * 국가인터넷정보판공실, 국가발전개혁위원회, 공업정보화부, 재정부에서 제정
  - 보안 평가를 신청하는 클라우드 서비스 제공자에게 신고서, 보안 계획서 등과 함께 공급망 보안 보고서 제출 의무 부여

- 중국표준화관리위원회는 SW공급망의 보안 강화를 위해 SBOM을 사용하도록 하는 정보보안기술 SW공급망 보안 요구 표준[56]을 발표
  - 제3자 조직에 대한 SW공급망 보안 평가를 수행하기 위한 기준 마련을 목적으로 SW공급망 조직 및 공급 활동 관리에 대한 보안 요구사항 지정
  - 외부 SW구성요소의 출처 확인과 보안위험 제거를 위해 공급자와 구매자 모두에게 SBOM을 포함한 SW구성맵*을 형성하도록 적시[57]
  * SW구성맵에는 SBOM과 보안위험이 포함되며, SBOM 정보를 보안위험과 정확하게 연관시켜 SW공급망의 추적·감시 가능성 향상을 목적으로 사용

SW공급망 보안 강화를 위해 관련 연구·개발을 주도하는 전담조직을 구성

- 공업정보화부 산하 CAICT[58]에서 SW공급망보안연구소(3S-LAB)을 설치[59]해 SW공급망 보안 강화를 위한 협력체계 구축
  - 제1회 SW공급망 보안 포럼(3SCON)에서 연구소 설립 발표
  - 국내외 기업이 참여해 SW공급망 보안 산업의 건전하고 질서 있는 발전 촉진

55 중국 국무원(2019.8.28.), "云计算服务安全评估办法"
56 중국표준화관리위원회(2022.4.28.), "信息安全技术 软件供应链安全要求"
57 중국 국가표준화국, "信息安全技术 软件供应链安全要求（征求意见稿）"
58 중국 정보통신연구원 http://www.caict.ac.cn/
59 CAICT qq.com(2022.6.17.), "中国信通院首届软件供应链安全论坛（3SCON）召开 聚焦软件全生命周期安全"

[그림 4] 3S-LAB 참여기업

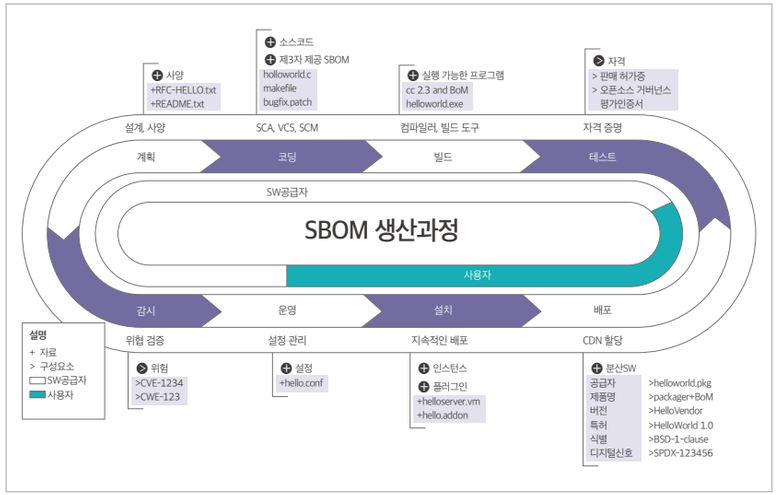
출처: CAICT qq.com(2022.6.17.), "中国信通院首届软件供应链安全论坛(3SCON) 召开 聚焦软件全生命周期安全"

CAICT를 중심으로 SBOM 관련 백서 및 가이드를 발간해 SW개발·운영 실무 수준에서 SBOM 활용 확산을 위한 발판 마련

- SW공급망 투명성 확보를 통해 빠른 보안취약점 대응 방안 중 하나로 SBOM을 제시하는 SW공급망 보안백서[60] 발간
  - 기존 공급망과 비교해 SW공급망 보안 공격은 경계가 제품 자체에서 SW생산 과정 전반으로 확장된다는 점에 주목하고, 공개SW 및 클라우드 네이티브 시대의 도래에 따라 복잡해진 SW공급망의 투명성 확보 필요성 제기
  - SW공급망 보안에 대해 주요 링크의 가시성 확보를 위해 SBOM을 활용하도록 하며 생성 공정, 도입 효과, 도구 이용 등 관련 정보 제공

60 CAICT(2021.8.), "软件供应链安全白皮书(2021)"

[그림 5] SW공급망 보안백서에서 정의한 SBOM 생성 과정



출처: CAICT(2021.8.), "软件供应链安全白皮书(2021)"

- 작성법, 활용방안 등 SBOM 관련 세부 정보를 제공함으로써 필요성 인식을 향상하기 위해 SBOM 실무가이드[61] 발간
  - 개념, 해외동향, 국제표준, 도구, 활용방안 등 전체적인 개괄을 설명해 SBOM에 대한 정보 제공
  - 의료를 비롯한 선도적으로 활용 중인 분야와 관련 개발 동향에 기반해 다방면에서 SBOM 활용 확산 가능성을 전망

- SW보안개발 생애주기 상에서의 SBOM 활용 촉진을 위해 SW제품의 개발·활용 단계를 대상으로 하는 SBOM 보안 응용 백서[62] 발표
  - 중국 건설 은행의 금융 기술 자회사 CCB Jinke와 CAICT가 공동으로 작성해 3SCON에서 공개
  - DevSecOps 및 보안 운영 플랫폼에서 SBOM의 구현 경로를 제공해 개발·운영 현장에서 SBOM의 활용 방향성 제시

61 CAICT(2022.5.26.), "软件物料清单实践指南"
62 CAICT(2022.6.17.), "软件物料清单(SBOM) 安全应用白皮书"

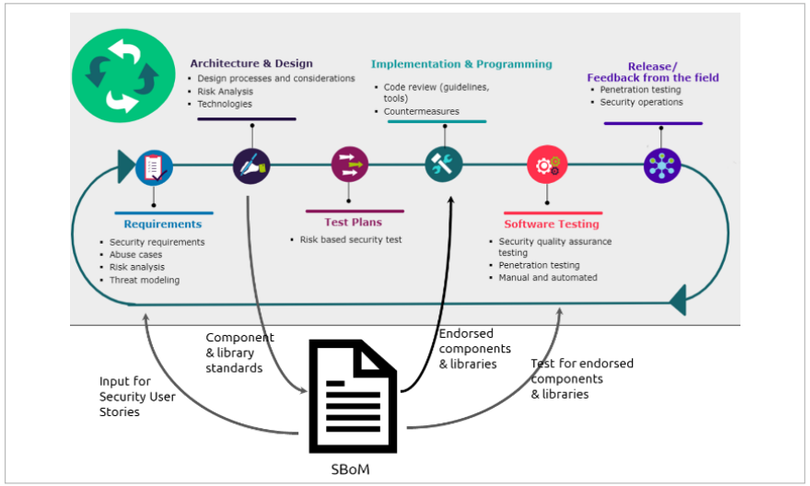
5 네덜란드

SW공급망 투명성 확보 측면에서 SBOM의 중요성을 인식하고 글로벌 동향 분석과 함께 SBOM 도입 방향을 제시하는 연구 추진

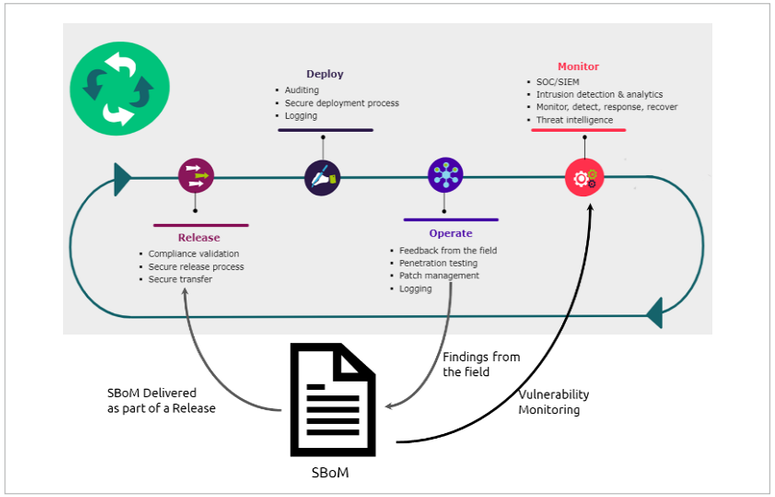
- 법무부 산하 NCSC[63]에서 SBOM 연구 진행
  - NCSC 연구 아젠다 2019-2022[64]에서 공급망 위협 항목을 도출하고, 관련해 SBOM을 통한 효과적인 의존성 식별 방안 검토

- 사이버보안 강화를 위한 SBOM 활용법을 담은 보고서[65]를 발간해 SW공급망 보안에서의 SBOM 필요성과 도입 방향 제시
  - 미국 SBOM 도입 및 연구 현황, EU 보안 가이드의 SBOM 권고 등 글로벌 동향을 살펴보고 SW투명성 제고 측면에서 SBOM 필요성 시사
  - SW 개발·운영 과정에서 SBOM 활용방안을 명기하고, 성공적인 SBOM 도입을 위한 온·오프라인 가용성, 기준, 자동화 도구 등 요건 제시

[그림 6] SW개발·운영 상에서의 SBOM 활용 방안



63 국가 사이버 보안국(National Cyber Security Centre), https://www.ncsc.nl/
64 네덜란드 NCSC(2020.1.), "NCSC Research Agenda 2019-2022"
65 네덜란드 NCSC(2021.1.), "Using the Software Bill of Materials for Enhancing Cybersecurity"



출처: NCSC(2021.1.), "Using the Software Bill of Materials for Enhancing Cybersecurity"
주석: (상) SBOM 표준 설정, 정보 기술 후 SW구성요소 검증으로 SW개발(DEVops)에 SBOM 활용, (하) SW제품과 함께 SBOM 배포 받아 SW 운영(devOPS)의 취약점 모니터링 및 패치에 SBOM 활용

Ⅲ 요약 및 시사점

주요 국가들은 SW공급망 투명성 강화를 위해 글로벌 SBOM 정책 동향을 모니터링하면서 활용사례집, 가이드 및 백서 등 발간을 통해 SBOM 활용을 권고

- 국제적 연결성을 가지는 SW공급망 특성 때문에 주변 국가의 SBOM 도입·제도화 동향을 주시하고 조화 방안 및 대응책 마련에 집중
  - 일본은 소프트웨어TF를 통해 지속적으로 미국의 SBOM 정책을 업데이트하면서 국내 도입 방안 수립에 이를 반영
  - 중국은 경쟁국인 미국의 SBOM 도입 현황을 가이드 및 백서로 공유해 SW공급망 상에서의 주도권 확보를 위한 SBOM 도입 필요성 제기
  - 네덜란드는 미국과 EU의 SBOM 정책 동향을 함께 분석한 보고서를 통해 종합적인 SBOM 활용방안과 도입 방향을 모색
- 산업에서의 SBOM 활용사례집과 보안 강화를 위한 가이드를 통해 현장에서 적용 가능한 실질적·구체적인 SBOM 활용방안을 제공
  - 일본의 소프트웨어TF는 공개SW 라이선스 관리를 위해 선도적으로 SBOM을 적용하고 있는 기업 활용사례를 취합해 모법사례집 발간
  - EU는 ENISA를 통해 SW공급망 보안이 중요시되는 의료기기, IoT 분야의 조달에 대해 SBOM 활용을 권고하는 보안 가이드 공개

직접 언급은 되지 않았지만 SBOM과 목적·기능 측면에서 동일하게 구현되는 유사 체계를 바탕으로 연구개발 및 제도화를 추진함으로써 SW공급망을 관리

- 공공 서비스에서 사용하는 공개SW를 SW자산으로 인식하고 SBOM과 유사한 SW인벤토리를 구축·관리해 SW공급망 관리체계 확립
  - EU에서 EU-FOSSA, FOSSEPS 등의 프로젝트 추진을 통해 공공 서비스에서의 안정적이고 신뢰할 수 있는 공개SW 활용 촉진
- 국가 기반 통신망 서비스에 대해 공급망 보안 강화를 목적으로 SW구성요소 수준으로 취약점을 점검하는 보안 지침을 통해 법제화 기반 마련
  - 영국 NCSC에서 통신(보안)법 2021, 전자통신(보안조치) 규정 2022에 근거해 공급자에게 SW구성요소 인벤토리 유지, 내외부 구성요소 관리 등 SBOM 유사 정보를 관리하도록 하는 보안 평가 지침 발행

SBOM의 본격적인 확산을 위해 전담 조직 구성, 실증사업 수행과 함께 제도화 방안을 검토하거나 보안 관련 인증·법안에 SBOM 적용 추진

- 주변 국가의 정책 동향, 국제표준, 도구·서비스 등 SBOM 관련 연구 및 정책 방안 수립을 담당하는 조직을 신설해 정책 추진력 확보 및 협력체계 구축
  - 일본 경제산업성은 소프트웨어TF를 구성해 관련 정책 및 SBOM 활용방안을 수립하고 제도화 가능성을 검토
  - 중국 공업정보화부는 CAICT를 중심으로 SW공급망 보안 강화 방안 중 하나로 SBOM

연구를 추진하고, 민간기업이 참여하는 3S-LAB을 신설해 SBOM 활용 확산을 위한 협력체계 마련

• SW공급망 보안 필요성이 특히 강조되는 주요 산업 영역 중심으로 SBOM 실증을 추진해 실효성을 점검하고 관련 가이드를 제공해 인식 개선
  - 일본 소프트웨어TF는 SBOM 도입의 실효성 검증을 위해 실증을 수행했고, 이를 의료·자동차·SW로 분야를 확장해 공통 가이드 배포 계획 수립
  - IoT SW공급망 보안 강화를 위해 EU는 D-SBOM 프로젝트를 추진하는 가운데 결과물을 자동차 산업에 적용하는 실증 추진으로 효과성 검토

• 일부 국가에서는 자체적인 SBOM 제도화 방안을 검토하거나 기존의 보안 점검 지침에 SBOM을 적용하는 적극적인 도입을 시도
  - 일본 총무성은 경제산업성 중심으로 점검하던 SBOM 체계 확립 방안을 ICT 전체로 확대해 제도화 방안을 검토하도록 하는 내용이 담긴 「ICT 사이버보안 종합대책 2022」 발표
  - 유럽 디지털시장의 SW공급망 보안 확보를 위해 EU는 클라우드 및 의료기기 관련 인증에 SBOM을 적용하고자 하고, 디지털제품 공급사의 SBOM 관리 의무를 명시한 「사이버복원력법」 법안을 마련

[표 4] 주요국[66] SBOM 관련 정책 동향 요약

구분	일본	EU	영국	중국	네덜란드
주요 특성	전담조직 소프트웨어TF에서 SBOM 체계 구축과 실증을 추진해 ICT 보안으로 제도화 방안 검토	공개SW 중심으로 SW공급망 관리해 클라우드·의료기기 인증부터 「사이버복원력법」 입법까지 제도화 추진	ICT 분야의 통신 보안 강화를 위해 SBOM 또는 유사체계 적용을 촉진하는 보안가이드 배포	경쟁국의 SBOM 정책 추진 현황을 모니터링하고, SW공급망 안전 확보를 위해 보안지침 및 SBOM 가이드 발간	미국, EU 등 선도적으로 SBOM을 도입·검토하는 국가 동향을 주시하고 국내 도입 방안 제시
전담 조직	소프트웨어TF			3S-LAB	

66 본고에서는 선행 연구 대상인 미국을 제외해 분석

구분	일본	EU	영국	중국	네덜란드
SBOM 백서·지침	배포 예정 ('22~)			SBOM 실무가이드, SBOM 응용 백서	NCSC 보고서
보안 지침	우수사례집	ENISA 의료·IoT 보안가이드	NCSC 기기 보안 가이드, 통신보안 행동강령	SW공급망 보안백서	
연구·개발		D-SBOM			
실증	의료·자동차·SW 분야 SBOM 실증	D-SBOM			
법·제도	「ICT 사이버보안 종합대책 2022」 제도화 검토	클라우드·의료기기 인증, 「사이버복원력법」	전자통신 (보안조치) 규정 2022	SW공급망 보안 요구 표준	

주석: SBOM이 직접 언급되지 않은 유사체계 사례는 기울임체로 표기

SW공급망 투명성 확보를 목적으로 주요 국가들에서 SBOM에 주목하고 있는 만큼 국내 SW생태계 경쟁력 확보 차원에서 대응책 마련 필요

• 기업은 글로벌 추세에 맞추어 경쟁력 격차를 발생시키지 않기 위해, 개발에서 운영까지 SW제품의 생애주기 상에서 SBOM 도입을 검토해야 하는 시점
  - 일본 기업들은 자체적으로 SBOM 활용체계를 구축해 SW공급망 보안 강화 측면에서의 경쟁력을 확보하고자 노력 중
  - 주요국에서 SBOM 또는 유사체계의 제도화와 ICT 정책으로의 확대 등이 추진되는 만큼 해외 진출 측면에서도 SBOM 필요성 인식 필요

• 정부는 기업의 SBOM 활용 여건을 조성하기 위한 제반 마련에 집중
  - 글로벌 제도화 동향을 지속적으로 모니터링하고 주요 정보를 공유함으로써 수출기업에서 관련 제도에 대한 대응 지연이 발생하지 않도록 지원
  - 국내 산업 실정을 반영한 정보 획득을 위해 주요 산업에서의 SBOM 실증을 추진하고 포맷·도구·절차 등 관련해 유효한 정보의 공개를 촉진

▧ 참고문헌

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.
- SPRi(2022.12.16.), “미국 SBOM(Software Bill of Materials) 정책 분석 및 시사점”.

2. 국외문헌
- CAICT qq.com(2022.6.17.), “中国信通院首届软件供应链安全论坛(3SCON) 召开 聚焦软件全生命周期安全”.
- CAICT(2021.8.), “软件供应链安全白皮书(2021)”.
- CAICT(2022.5.26.), “软件物料清单实践指南”.
- CAICT(2022.6.17.), “软件物料清单(SBOM) 安全应用白皮书”.
- Capgemini Invent(2021.1.), “Using the Software Bill of Materials for Enhancing Cybersecurity”.
- CheckPoint(2021.12.29.), “The Numbers Behind Log4j Vulnerability CVE-2021-44228”.
- DCMS(2019.7.), “UK TELECOMS SUPPLY CHAIN REVIEW REPORT”.
- DCMS(2021.11.15.), “Government response to the call for views on supply chain cyber security”.
- DCMS(2022.3.1.), “Draft Telecommunications Security Code of Practice“.
- EC DIGIT(2016.1.29.), “EP Pilot Project ‘Free and Open Source Software Auditing’”.
- EC DIGIT(2018.4.5.), “EU-FOSSA 2 Project Charter”.
- EC DIGIT(2022.2.2.), “Free and Open Source Solutions for European Public Services(FOSSEPS) - Project Charter”.
- ENISA(2020.11.), “GUIDELINES FOR SECURING THE INTERNET OF THINGS”.
- ENISA(2020.12.), “EUCS - CLOUD SERVICES SCHEME”.
- ENISA(2020.2.), “PROCUREMENT GUIDELINES FOR CYBERSECURITY IN HOSPITALS”.
- Gartner(2021.7.15.), “How Software Engineering Leaders Can Mitigate Software Supply Chain Security Risks”.
- International Medical Device Regulators Forum(2020.3.18.), “Principles and Practices for Medical Device Cybersecurity”.
- NCSC(2022.3.), “Vendor security assessment”.
- NHTSA(2020), “Cybersecurity Best Practices for the Safety of Modern Vehicles”.
- OSI(2022.2.15.), “Ten takeaways from the 2022 State of Open Source survey”.
- UN Regulation No. 155(2021.3.4.), “Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system”.
- 경제산업성(2021.4.21.), “オープンソースソフトウェアの利活用及びそのセキュリティ確保に向けた管理手法に関する事例集を取りまとめました”.
- 경제산업성(2021.7.26.), “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”.
- 경제산업성(2022.5.10.), “OSS の利活用及びそのセキュリティ確保に向けた管理手法に?する事例集”.
- 네덜란드 NCSC(2020.1.), “NCSC Research Agenda 2019-2022”.
- 네덜란드 NCSC(2021.1.), “Using the Software Bill of Materials for Enhancing Cybersecurity”.
- 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’”.
- 중국 국무원(2019.8.28.), “云计算服务安全评估办法”.
- 중국표준화관리위원회(2022.4.28.), “信息安全技术 软件供应链安全要求”.
- 총무성(2022.8.), “ICT サイバーセキュリティ総合対策 2022”.

3. 기 타
- asvin, https://asvin.io/, 2022.12.15. 방문.
- CORDIS, “Trusted and reliable content on future blockchains”, https://cordis.europa.eu/project/id/957228, 2022.12.15. 방문.
- D-SBOM, https://www.trublo.eu/d-sbom/, 2022.12.15. 방문.
- EC(2021.9.15.), “State of the Union 2021”, https://ec.europa.eu/info/strategy/strategic-planning/state-union-addresses/state-union-2021_en, 2022.12.15. 방문.
- EC(2022.9.15.), “Cyber Resilience Act”, https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act, 2022.12.15. 방문.
- e-gov, “サイバーセキュリティ基本法”, https://elaws.e-gov.go.jp/document?lawid=426AC1000000104, 2022.12.15. 방문.
- EMA, “Medical Devices”, https://www.ema.europa.eu/en/human-regulatory/overview/medical-devices, 2022.12.15. 방문.
- EUR-Lex(2008.7.9.), “Regulation No 765/2008”, https://eur-lex.europa.eu/eli/reg/2008/765/oj, 2022.12.15. 방문.
- EUR-Lex(2017.4.5.), “Regulation (EU) 2017/745”, https://eur-lex.europa.eu/eli/reg/2017/745/oj, 2022.12.15. 방문.
- EUR-Lex(2019.4.17.), “Cybersecurity Act”, https://eur-lex.europa.eu/eli/reg/2019/881/oj, 2022.12.15. 방문.
- legislation.gov.uk, “Telecommunications (Security) Act 2021”, https://www.legislation.gov.uk/ukpga/2021/31/, 2022.12.15. 방문.
- legislation.gov.uk, “The Electronic Communications (Security Measures) Regulations 2022”, https://www.legislation.gov.uk/uksi/2022/933/, 2022.12.15. 방문.
- NCSC(2021.6.), “Device Security Guidance”, https://www.ncsc.gov.uk/collection/device-security-guidance, 2022.12.15. 방문.
- NGI(Next Generation Internet), https://www.ngi.eu/, 2022.12.15. 방문.
- TruBlo, https://www.trublo.eu/about-this-project/, 2022.12.15. 방문.
- 영국 국가사이버보안센터(National Cyber Security Centre), https://www.ncsc.gov.uk/, 2022.12.15. 방문.
- 네덜란드 국가 사이버 보안국(National Cyber Security Centre), https://www.ncsc.nl/, 2022.12.15. 방문
- 중국 정보통신연구원, http://www.caict.ac.cn/, 2022.12.15. 방문.