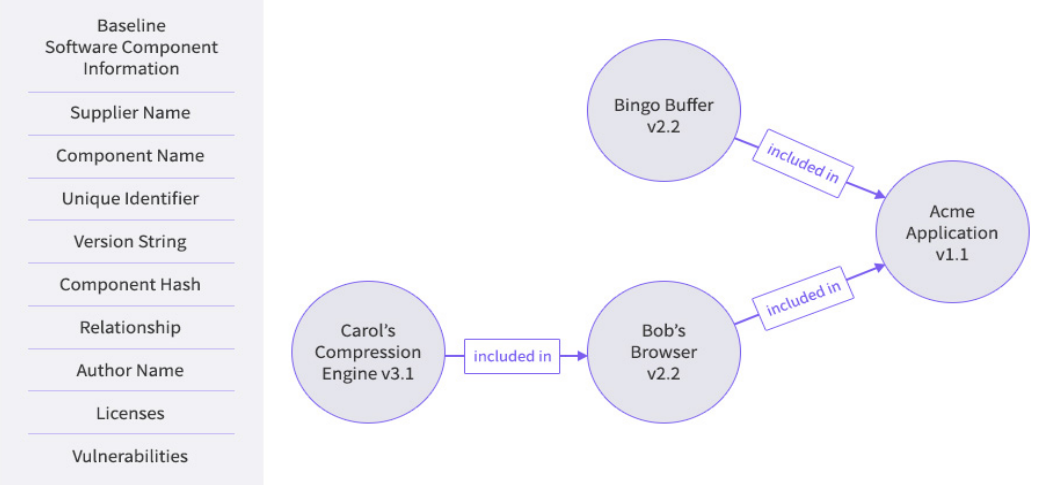
Chapter
02

주요국의 SBOM 동향: 공공부문 도입 및 연구개발

최민석_한국전자통신연구원 책임연구원

I. 서론

소프트웨어명세서(Software Bill of Materials: SBOM)는 소프트웨어를 구성하는 컴포넌트에 관한 메타데이터(metadata)이다. 예를 들면, [그림 1]의 Acme Application v1.1은 Bingo Buffer v2.2와 Bob's Browser v2.2 등의 소프트웨어 컴포넌트를 포함하고 있다. 따라서 Acme Application v1.1의 SBOM은 Bingo Buffer v2.2와 Bob's



〈자료〉 NIPA, "SBOM 가이드", https://www.globalict.kr/sbom/sbom.do?menuCode=040500

[그림 1] SBOM 설명을 위한 소프트웨어 구성 예시

* 본 내용은 최민석 책임연구원(☎ 042-860-1864, cooldeny@etri.re.kr)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.
***이 논문은 한국전자통신연구원 연구운영비지원사업(기본사업) 연구개발과제의 일환으로 수행되었음.
[국가지능화 기술정책 및 표준화 연구, 24ZF1100]

Browser v.2.2 등에 관한 컴포넌트 명칭, 공급자 명칭 등 필드와 필드별 값의 쌍으로 이루어진 데이터 집합이다.

소프트웨어가 사용된 제품이나 시설이 사회 전반에 사용되면서 SBOM이 중요해지고 있다. 만약, 소프트웨어의 결함이나 악의적 침입을 통해 소프트웨어가 잘못 작동하게 되면 개인정보를 포함한 중요한 정보가 유출되거나 사회기반시설이 멈출 수 있기 때문이다. 특히, 정부에 조달을 통해 납품된 소프트웨어가 문제를 일으키면 안보 위협까지 초래할 수 있다. 또한, 소프트웨어로 인해 문제가 발생했을 때 문제를 일으키는 소프트웨어 컴포넌트를 특정하지 않고 모든 소프트웨어 코드를 모두 검사한다면 원인 파악과 복구에 많은 시간이 소요된다. SBOM에 대한 정보를 가지고 있다면 문제가 되는 컴포넌트 또는 그로부터 영향을 받는 소프트웨어를 특정하여 대응할 수 있어 복구를 포함한 대응 시간을 단축하고 이차 피해를 최소화할 수 있을 것이다.

우리 정부도 SBOM에 대해 정책적으로 대응하고 있다. 가장 대표적인 것이 2023년 4월에 발표된 「소프트웨어 진흥 전략」이다. 동 전략은 약 10년 만에 발표된 정부의 소프트웨어 분야 종합전략으로 추진과제 중 하나로 2024년부터 오픈소스를 포함한 소프트웨어의 세부 구성요소를 체계적·전자적으로 관리할 수 있도록 SBOM 작성에 필요한 컨설팅을 지원하겠다는 내용을 포함하고 있다[1]. 한편, 식품의약품안전처에서도 2023년 11월에 '의료기기 사이버보안원칙 및 실무 안내서'의 관련 문서로 '의료기기 사이버보안을 위한 소프트웨어 자재명세서 원칙 및 실무 안내서'를 발표했다[2]. 국방 분야에서도 우리 군의 무기체계 소프트웨어를 관리하고 방산 수출을 증대하기 위해 SBOM의 도입을 검토하고 있다[3][4]. 그리고 2024년 5월 13일에 과학기술정보통신부와 국가정보원, 디지털플랫폼정부위원회는 공동으로 작성한 '소프트웨어 공급망 보안 지침(가이드라인) 1.0'을 발표했다[5].

위와 같은 정부의 대응은 정책과 문서로 발표되기 전부터 시작되었다. 2021년 하반기부터 전문가 그룹을 구성하여 논의를 이끌었다. 2021년 5월에 미국 백악관에서 SBOM의 공공부문 도입 내용이 담긴 대통령 행정명령이 발표된 것이 계기가 되었다. 이때는 주로 SBOM의 실체와 관련 해외 동향을 파악하는 것에 집중했다. 2022년 2월에 처음으

로 정보통신산업진흥원(NIPA)에서 주관하여 SBOM을 주제로 한 세미나가 개최되었다[6]. NIPA 글로벌 ICT 포털에 SBOM 웹페이지(https://www.globalict.kr/sbom/sbom.do)를 개설했다. 또한, 소프트웨어정책연구소(SPRi)에서 2022년 12월에 미국을 포함한 주요 국가에서의 SBOM 정책 동향을 분석하여 보고서로 발간하였다[7][8]. 동 보고서들에서는 각국의 정책 대응뿐만 아니라 법제화, 실증사업을 다루었다.

본 고에서는 2018년에 미국 정부에서 SBOM을 주제로 정책 연구를 진행하던 때부터 지금까지 미국과 일본, 유럽의 SBOM에 관한 공공부문 도입과 연구개발 진행 과정을 시기를 구분하여 체계적으로 정리하고자 한다. 세계 여러 국가 중 미국과 일본, 유럽을 대상으로 선정한 것은 SBOM에 대해 다른 국가보다 빨리 정책 논의를 진행하여 가시적인 결과를 만들었기 때문이다. 한편, 본 고에서는 SBOM에 관한 민간의 움직임이 아닌 정부의 추진 동향을 중심으로 살펴볼 것이다. 이를 통해 향후 우리 정부의 SBOM 추진 방향을 설정할 때 시사하는 바를 도출하고자 한다.

II. 미국 정부의 도입 및 연구개발

미국 연방정부의 SBOM 도입 과정을 크게 3단계로 구분할 수 있다. 첫 번째 시기는 상무부 정보통신청(National Telecommunications and Information Administration: NTIA)에서 SBOM에 관한 복수의 전문가 워킹그룹을 3년간 운영한 때이다. 개념 정의, 현황 분석, 표준 및 포맷, 시범 적용 등을 진행했다. 그리고 2021년 5월에 백악관에서 SBOM 도입을 포함한 대통령 행정명령 14028호를 발표했다. 두 번째는 연방정부 각 부처가 대통령 행정명령에 포함된 지시사항을 이행한 시기이다. 그런데 대통령 행정명령에서 명시한 실행기한인 2022년 5월 이후에도 연방정부 조달에 SBOM을 도입하기 위해 필요한 후속 조치가 이어졌다. 그리고 최근 미국 연방정부는 SBOM을 국가안보 차원에서 접근하고 있다. 각 부처에 SBOM 도입하는 것을 넘어 현행 SBOM의 한계를 극복하고 강화하고자 한다. 인공지능, 이동통신 등 다른 분야로의 확산이나 국제협력, 연구개발사업 지원 등이 대표적이다.

[표 1] 미국 상무부 정보통신청의 SBOM 워킹그룹

제1기(2018.10.1.~2019.11.17.)	제2기(2019.11.18.~2021.11.17)	주도기관
문제 이해	문제 정의	CMU-SEI, MedSEc
현황 및 사례 분석	도입 활성화	CMU-SEI
표준 및 포맷	포맷 및 툴	리눅스재단, NTIA
헬스케어 개념 검증(PoC)	헬스케어 개념 검증(PoC)	CMU-SEI, NTIA

〈자료〉 NTIA, “Software Component Transparency”, https://www.ntia.gov/other-publication/2021/ntia-software-component-transparency, 재구성

미 연방정부의 SBOM에 관한 준비는 2018년 7월 19일부터 상무부 정보통신청이 소프트웨어 컴포넌트 투명성 이니셔티브(Software Component Transparency Initiative)를 출범시키면서 시작되었다[9]. 동 이니셔티브는 소프트웨어 투명성에 관한 문제 이해와 SBOM을 활용한 해결 가능성을 응용 분야별로 검증하고자 했다. 그리고 이니셔티브의 목적 달성을 위해 2018년 10월 1일부터 2021년 4월 29일까지 두 차례에 걸쳐 SBOM 워킹그룹을 구성하여 10회 이상의 회의를 개최했다[10]. SBOM 워킹그룹의 분과는 [표 1]과 같이 문제 이해 및 정의, 현황·사례 분석 및 도입 활성화, 표준 및 포맷 등이고, 워킹그룹별 주도 기관은 NTIA뿐만 아니라 카네기멜론대학교(Carnegie Mellon University: CMU)의 소프트웨어공학연구소(Software Engineering Institute: SEI), 리눅스재단(Linux Foundation), 의료 보안 전문기업인 MedSec(Medical Device Cybersecurity Solutions) 등이다.

SBOM 워킹그룹은 SBOM의 개념 이해에 관한 문서를 포함하여 향후 미국 정부의 관련 정책에 기초가 될 주요 자료를 다수 생성했다. 그리고 원래 목표로 한 보건의료 분야뿐만 아니라 에너지 분야 그리고 자동차 분야에서 SBOM 실증 업무도 수행했다. 그러나 이때만 해도 우리나라를 포함하여 대부분 국가에서는 SBOM을 주목하지 않았다.

SBOM이 세계적으로 주목받게 된 것은 두 번째 시기이다. 2021년 5월 12일에 미국 백악관에서 대통령 국가 사이버안보에 관한 행정명령 14028호(Improving the Nation’s Cybersecurity)를 발표했기 때문이다[11]. 동 행정명령은 총 9개의 섹션으로 구성되어 있는데, SBOM은 4번째 섹션에 그 내용이 포함되어 있다. SBOM을 “소프트웨어의 다양

한 구성요소에 관한 세부사항과 공급망 관리에 관한 공식 기록(a formal record containing the details and supply chain relationships of various components used in building software)"으로 정의하고 있다. [표 2]는 상무부의 국립표준기술연구원(National Institute of Standards and Technology: NIST)과 NTIA, 국토안보부의 사이버보안인프라청(Cybersecurity and Infrastructure Security Agency: CISA), 백악관 관리예산실(Office of Management and Budget: OMB) 전자정부국 등이 SBOM 도입과 관련해서 할 일을 보여준다. NIST는 이해관계자 의견수렴을 시작으로 중요 소프트웨어(critical software)에 관한 정의 공개, 가이드라인 발표, 시범 프로젝트 실시 등 미국 공공부문 SBOM 도입에서 가장 많은 역할을 담당했다. 2018년부터 SBOM 워킹그룹을 운영했던 NTIA는 SBOM의 최소 구성요소를 정리하여 공개하는 역할을 맡았다. 그리고 2018년 11월에 확대되어 설립된 CISA는 중요 소프트웨어의 목록을 특정했다. 관리예산실 전자정부국은 앞에서 NIST와 CISA에서 정한 중요 소프트웨어에 대해 NTIA의 SBOM 최소 구성요소를 바탕으로 연방정부기관들이 준수해야 일을 안내했다. NIST는 1년 간의 대통령 행정명령 수행기간이 끝난 직후인 2022년 7월 11일에 대통령 행정명령 14028호의 섹션 4에 대한 이행 상황을 정리한 보고서를 발간했다[12].

[표 2] 미국 대통령 행정명령 14028 섹션 4의 정부 부처별 업무

마감	상무부 NIST	상무부 NTIA	국토안보부 CISA	백악관 OMB
30일	이해관계자 의견수렴			
45일	중요 SW 정의 공개			
60일	중요 SW 보안 측정지표	SBOM 최소 요소 공개		
75일			중요 SW 목록 특정	
90일				연방정부기관 준수 안내
180일	가이드라인 초안 공개			
270일	가이드라인 발표			
360일	가이드라인 업데이트			
365일	IoT 시범적용 결과보고			

〈자료〉 미국 대통령실, "Executive Order on Improving the Nation's Cybersecurity", EO14028, 재구성

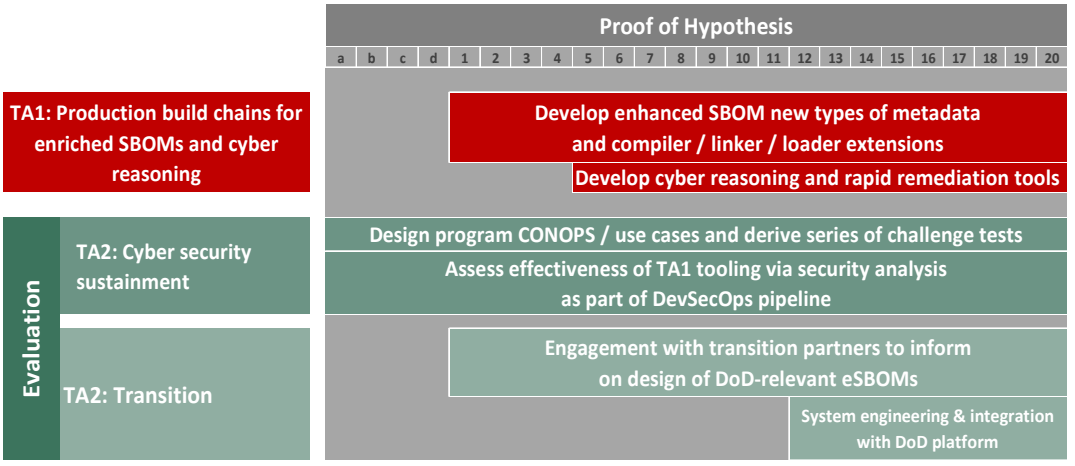
대통령 행정명령 14028호의 지시사항이 완료된 2022년 5월 이후에는 CISA가 SBOM 도입에서 주도적인 역할을 담당했다[12]. 2023년 4월에 CISA는 SBOM에 관한 문서 2건을 발표했는데, SBOM 문서 종류와 취약점 악용 가능성 교환(Vulnerability Exploitability eXchange: VEX) 문서 포맷의 최소 요구사항에 관한 것이다[14]. 같은 해 9월에는 SBOM 내용이 포함된 오픈소스 소프트웨어 보안 로드맵을 발표했다[15]. 그리고 11월에는 VEX 문서 발행 시점에 관한 문서를 발표했다[16]. 2024년 3월에는 SBOM에서의 역할을 SBOM 저자와 SBOM 사용자 그리고 SBOM 배포자로 구분한 문서를 공개했다[17].

연방정부의 SBOM 도입을 마무리하기 시작했다. 2023년 10월에 미국 관보에 연방조달규칙(Federal Acquisition Regulation: FAR) 개정안에 관한 내용이 공개되어 의견을 수렴했다. 개정안은 사이버 위협 및 사고에 관한 정보 공유를 강화하기 위해 미국 연방정부에 ICT 제품 및 서비스를 납품하는 모든 계약자는 SBOM을 개발, 유지관리해야 하고 CISA가 필요할 때 SBOM 정보를 제공해야 한다는 내용이 담겨 있다[18]. 드디어 2021년 5월부터 시작된 SBOM에 관한 미국 정부의 노력이 일단락되었다고 볼 수 있다.

연방정부의 SBOM 추진의 세 번째 시기는 2021년 1월 1일에 백악관 국가사이버총괄국(Office of the National Cyber Director: ONCD)이 새롭게 설치되면서 시작되었다고 볼 수 있다. ONCD은 미국의 사이버안보 총괄 컨트롤타워 역할을 담당하고 있는데, 적극적으로 추진하고 있는 정책 중 하나가 SBOM이다. 2023년 3월에 발표된 국가사이버안보 전략(National Cybersecurity Strategy)과 같은 해 7월에 발표한 국가 사이버안보 전략 이행 계획(National Cybersecurity Strategy Implementation Plan)에도 SBOM 고도화에 관한 추진과제가 포함되어 있다[19]. 또, 11월 9일에 CISA와 국방부 국가안보국(National Security Agency) 등과 공동으로 SBOM 이용에 관한 가이드라인을 발표했다[21]. 한편, 2023년 5월에는 일본 총무성이 주관한 쿼드(Quad) 4개국의 중요·핵심기술 워킹그룹(Critical and Emerging Technology Working Group)에서 오픈랜 보안보고서(Open RAN Security Report)를 발표했는데, 동 보고서에서 SBOM의 활용을 중심으로 한 공동원칙이 포함되었다[31].

미 연방정부는 인공지능 분야에도 SBOM를 적극적으로 도입하고 있다. 예를 들면, 2023년 11월에 발표한 CISA의 2023~2024년 인공지능 로드맵에도 연방정부에서 사용하는 인공지능 시스템의 안전 확보를 위해 SBOM을 활용하기로 했다[32]. 2023년 3월에 재무부에서 발표한 금융서비스산업에서의 인공지능에 특화된 사이버보안 위험 관리(Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Service Sector)에서도 SBOM을 위해 관련 기관과 협력할 것을 밝히고 있다[33]. 2024년 4월에 NIST에서 발표한 '생성형 인공지능과 듀얼 사용 기반 모델을 위한 안전한 소프트웨어 개발 방법(Secure Software Development Practices for Generative AI and Dual-Use Foundation Models)'의 초안에서도 SBOM을 다루고 있다[34].

한편, 국방성 국방고등연구계획국(Defense Advanced Research Projects Agency: DARPA)은 2021년 12월 11일에 새로운 사업으로 Enhanced SBOM for Optimized Software Sustainment(E-BOSS)를 공고했다[35]. 동 사업은 2021년 12월에 세계를 강타한 Log4j 사태에서 확인된 문제를 해결하는 것을 목표로 한다. 당시 중국의 알리바바 클라우드 보안팀원 중 한 명이 소프트웨어 컴포넌트인 Log4j에 보안 취약점을 발견하여 공개적으로 알린 이후 72시간 동안 거의 100만 건 이상의 공격과 60종 이상의 변형된 공격이 있었고 시스템 복구에 평균 12~17일이 소요되었다고 한다. Log4J는 약 30억 개의 기기에 탑재될 정도로 널리 사용되었음에도 불구하고 8년 동안 그 문제를 인지하지 못했다는 사실에도 주목했다. 그래서 동 사업은 소프트웨어 개발 전주기를 대상으로 하는데, 성능 목표는 3일 이내의 문제 해결과 1주일 이내의 대응 복구로 하되 SBOM이 컴파일과 런타임에 주는 추가 부담을 각각 10% 이내로 유지하는 것이다. 총 20개월의 사업 기간에 2024년과 2025년에 각각 500만 달러와 1,100만 달러가 투자되는 이 사업은 [그림 2]와 같이 두 개의 과업으로 구분하여 사업이 진행된다. 첫 번째 과업은 소프트웨어 컴포넌트에 관한 새로운 메타데이터를 포함한 향상된 SBOM을 개발하고 개발한 SBOM을 활용하여 사이버 위험을 감지하고 빠르게 회복시킬 수 있는 도구를 개발하는 것이다. 다른 과업은 첫 번째 과업의 개발 결과를 평가하고 국방부의 소프트웨어 개발 플랫폼으로 개발 결과를 이전하는 것이다. 현재 미 공군은 소프트웨어 개발용



〈자료〉 DARPA "Enhanced SBOM for Optimized Software Sustainment(E-BOSS)", HR0011124S0005, 2023. 12. 11.

[그림 2] DARPA E-SBOM 사업의 과업 구성

플랫폼인 플랫폼원(Platform One)을 운영하고 있다.

III. 일본 정부의 SBOM 도입 및 연구개발

일본 정부는 2019년 상반기부터 준비하여 2019년 9월 5일부터 SBOM에 대해 본격적으로 정책 대응에 나섰다. 미 상무성에서 SBOM 워킹그룹을 운영한 지 1년이 조금 뒤의 일이고, 대통령 행정명령이 발표되기 1년 반 전의 일이다. 일본의 대응이 다른 국가에 비해 비교적 빨랐던 것은 일본 대기업의 현지법인 관계자가 미국 정보통신청의 SBOM 워킹그룹에 참여하는 등 미국의 SBOM 추진을 빠르게 인지할 수 있는 인적 네트워크 덕분이다. 미국 정부 또한 일본과의 협력에 긍정적이었다. 예를 들면, 미국 정보통신청이 2021년 4월 27일에 발표한 3페이지 분량의 'SBOM at a Glance'를 영어 버전[37]과 함께 일본어 버전[38]도 제작하여 공개했다.

일본 정부의 SBOM 대응은 미국과 마찬가지로 전문가 워킹그룹을 구성한 것부터 시작되었다. 담당 부서인 경제산업성 상무정보정책국 사이버보안과는 2017년 12월부터 존재하던 '산업사이버보안연구회' 산하의 '제도 · 기술 · 표준화 워킹그룹'에 '사이버-물

리적 보안 확보를 위한 소프트웨어 관리방법 등 검토를 위한 태스크포스팀'을 설치했다. 동 태스크포스팀은 총 17명의 위원으로 구성되었는데, 참여 위원들은 독립행정법인 정보처리추진기구의 보안센터 담당자를 제외하면 모두 대학과 기업 소속이었다. 다만, 내각관방의 사이버보안센터, 총무성, 경찰청, 후생노동성, 방위장비청 등의 관계자가 외부 참여자 자격으로 회의에 참여할 수 있게 했다.

2024년 4월 16일까지 동 태스크포스팀은 12번의 회의를 개최했다[39]. 일본 정부의 첫 번째 대응 시기는 2019년 9월 5일의 첫 회의부터 3차 회의가 개최된 2019년 12월 4일까지다. 태스크포스티의 목표인 '사이버-물리적 보안 대책 프레임워크'(Cyber-Physical Security Framework: CPSF)의 개발 방향 논의를 위해 소프트웨어에 관한 미국과 일본의 대응 사례 수집에 집중했다.

2020년에는 회의가 개최되지 않았고, 약 1년 뒤인 2021년 1월 13일에 개최된 4차 회의에서 SBOM에 관한 논의를 오픈소스 소프트웨어(Open Source Software: OSS)에 초점을 맞추었다. 먼저, OSS 관리 방법에 관한 사례집을 작성하고 일본 내에서 SBOM 활용을 촉진하기 위한 실증사업 추진 필요성에 대한 검토가 이루어졌다. 사례집은 2022년 5월 10일에 'OSS 활용 및 보안 확보를 위한 관리 방법 사례집'의 제목으로 공개되었는데, 토요타 자동차, 소니, 올림푸스 등의 일본 기업의 사례가 소개되어 있다. 실증사업은 미국 정보통신청의 SBOM 워킹그룹의 업무를 참고했다. 그러나 일본의 산업 구조가 미국과 다른 점에 착안하여 SBOM이 일본의 각 산업에서 도입될 때 발생할 비용의 사전 검증을 실증사업의 목적으로 삼았다는 점에 큰 차이가 있다.

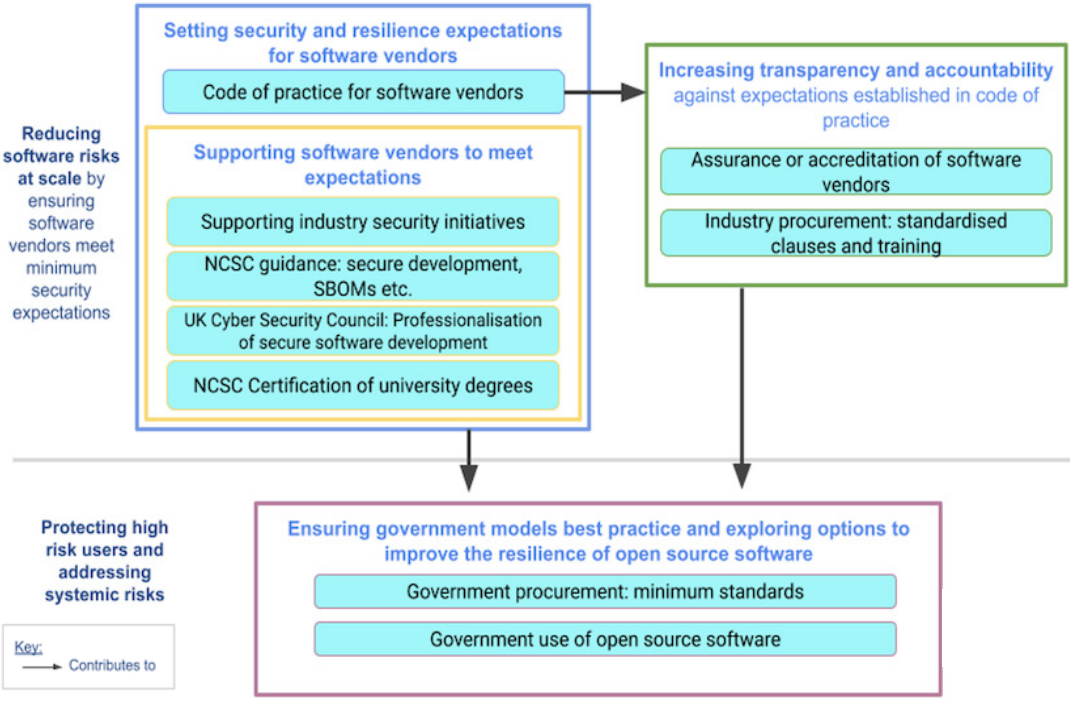
2022년 7월 26일 개최된 7차 회의에서 향후 추진할 4개의 과제를 선정하면서 체계적인 전략의 구성을 갖추기 시작했다. 선정된 추진 과제는 각 산업에 적합한 SBOM 활용 모델 최적화와 SBOM 공유를 위한 환경 정비, SBOM 도구의 활성화를 위한 효율성 제고, 국내와 글로벌 기준에 적합한 무결성 확보이다. 또, 2022년 내에 진행할 실증사업의 일정을 발표했는데, 분야는 의료기기와 자동차, 인터넷 협업용 소프트웨어였다. 그리고 당시까지 수집하고 논의한 내용을 정리해서 발간할, SBOM의 도입과 교환, 활용에 관한 보고서의 목차를 검토했다. 2023년 2월 28일에 경제산업성은 SBOM 도입 안내서

초안을 검토하고, 2023년 4월 25일부터 5월 25일까지 공개 의견을 청취한 후 반영하여 2023년 7월 18일에 최종안을 공개했다. 2023년 10월 31일의 11차 회의에서는 SBOM에 관한 정보 교환(VEX)을 위한 안내서를 작성하기 위해 안내서의 목차 검토가 이루어졌다. 이때 디지털청에서의 SBOM 활용 사례도 함께 보고되었다. 2024년 2월 28일에 개최된 최근 회의에서는 지금까지의 실증사업의 결과에 대한 보고와 함께 SBOM의 교환과 활용까지 담은 안내서 2.0버전을 공개했다. 동 회의에서 총무성의 사이버보안총괄관실에서는 통신 분야에서의 SBOM 도입 필요성을 인식하여 실증사업을 추진할 것임을 밝혔다.

한편, 일본 정부도 SBOM에 관한 연구개발과제를 지원하고 있다. 그러나 과제 규모는 크지 않다. 예를 들면, 난잔대학에서 2023년 4월 1일부터 2027년 3월 30일까지 4년간 수행하는 'SPDX 포맷을 이용한 소프트웨어 생태계 분석을 위한 인프라 구축' 과제가 있다. 총 연구개발비는 4년 간 1,800만 엔이다.

IV. 영국 정부와 유럽연합 집행위원회의 SBOM 도입

유럽 국가 정부 중 SBOM에 대해 가장 빠르게 논의를 시작하고 적극적으로 대응하고 있는 곳 중 하나는 영국이다. 영국의 디지털문화미디어스포츠부(Department of Digital, Culture, Media and Sport: DCMS)는 2021년 5월 17일부터 7월 27일까지 2달 간 공급망 사이버보안에 관한 의견을 공개적으로 수집했는데, 이때 SBOM 유효성을 주장한 의견들이 있었다[40]. 2023년 2월 6월부터 5월 1일까지 12주 동안 DCMS의 후신인 과학혁신기술부(Department for Science, Innovation and Technology: DSIT)가 공개적으로 의견을 구했을 때는 SBOM에 관한 인지도와 유용성에 대한 기대가 한층 높아졌다[41]. [그림 3]은 영국 정부가 소프트웨어 보안 및 회복력을 높이기 위한 해결 방향을 나타내는데, 소프트웨어 공급자를 지원하기 위한 도구 중 하나로 SBOM을 포함하고 있다. 2023년 11월 27일에 발표된 안전한 인공지능 시스템 개발의 위한 가이드라인(Guidelines for secure AI system development)에도 SBOM이 포함되었다[42].



〈자료〉 DSIT, "Government response to the call for views on software resilience and security for businesses and organisations", 2024. 1. 23.

[그림 3] 영국 정부의 소프트웨어 보안 및 회복력 향상을 위한 정책 방향

유럽연합(European Union: EU)의 정부 문서 중 SBOM이 처음 등장한 것은 사이버보안청(European Union Agency for Cybersecurity: ENISA)이 2020년 11월 20일에 발표한 사물인터넷 안전을 위한 가이드라인(Guidelines for Securing the Internet of Things)이다[43]. 이후 클라우드 등 개별 가이드라인에서 SBOM이 등장했다. 그리고 2022년 9월에 사이버복원력법(Cyber Resilience Act) 초안을 공개했는데, SBOM 도입이 포함되어 있다[44]. 한편, EU 회원국인 네덜란드와 독일은 각각 2023년 7월과 8월에 SBOM 가이드라인을 공개했다[45]. 네덜란드 국가사이버보안센터는 초보자를 위한 가이드라인을 작성했고, 독일 연방정보보안청은 EU의 사이버복원법에 의해 향후 제조업체에게 부과되는 요건을 사전에 알릴 목적으로 SBOM의 포맷과 기술 요건을 정리한 가이드라인을 공개했다. 또, EU는 2024년 1월 30일에 미국의 워싱턴 DC에서 미국

국토안보부와 SBOM에 관한 협력 내용이 포함된 사이버복원력에 관한 공동선언문을 채택했다[46].

V. 결론

본 고에서는 미국과 일본, 유럽 국가 정부가 SBOM을 공공부문에 도입하는 과정과 연구개발 동향을 살펴보았다. 2018년에 미국 상무부 NTIA의 소프트웨어 컴포넌트 투명성 이니셔티브의 시작과 함께 SBOM의 공공부문 도입이 논의되기 시작한 이후 미국과 일본, 유럽의 정부는 SBOM과 VEX에 관한 가이드라인을 포함해서 다양한 정책을 만들어냈다. 우리나라 정부 또한 최근 SBOM 가이드라인을 발표했다. 미국은 연방 조달 규정의 개정을 목전에 두고 있다.

그럼 앞으로 SBOM에 관한 각국 정부의 정책은 어떻게 전개될 것인가? 주요 국가의 최근 움직임을 통해 다음과 같은 세 가지 특징을 도출할 수 있다. 첫째, 각국은 SBOM을 소프트웨어 고유의 분야를 넘어 그 적용 범위를 확대하고 있다. 인공지능과 오픈랜이 대표적이다. 최근 인공지능의 안전이 중요해지고 있어 인공지능 안전 확보를 위해 SBOM을 적극적으로 활용하고 있다. 인공지능 모델이 소프트웨어로 구성되어 있고, 학습과 추론 과정에서 다양한 소프트웨어 컴포넌트와 연계되기 때문에 SBOM 도입은 인공지능 시스템의 투명성을 높일 수 있을 것이다.

둘째, SBOM에 관한 국제협력이 활발해지고 있다. 2024년 1월의 미국과 유럽연합이 공동으로 채택한 사이버복원력 선언문과 2023년 5월의 쿼드의 오픈랜 보고서가 대표적 예다. 최근 코로나 바이러스 펜데믹과 국제정세 불안 등으로 국가 안보의 중요성이 더 커지고 각국 정상을 보좌하는 국가 사이버안보 담당 부서가 설치된 것과 연관된다. SBOM에서의 국제협력은 인공지능, 오픈랜 등에서의 국제 규범 마련에 일조할 것으로 기대된다.

셋째, SBOM에 관한 도전적 연구개발과제가 추진되고 있다. 미국 국방성 DARPA의 E-BOSS사업은 지금까지의 SBOM을 새롭게 탈바꿈시키려는 노력이다. 따라서 향후

E-BOSS사업의 연구 결과에 주목해야 할 것이다. 그리고 DARPA의 선도적 연구가 후속 연구로 이어지거나 다른 국가의 도전적인 SBOM 연구 개발로 확산할 수 있다.

SBOM의 공공부문 도입과 연구 개발은 여전히 진행 중이다. 따라서 본 고에서 살펴본 미국과 일본, 유럽의 공공부문 도입 동향은 계속해서 모니터링해야 한다. 특히, 국제 협력의 움직임에 집중해서 그 동향을 파악할 필요가 있다. 각국의 SBOM 가이드라인이 국제 정합성을 갖게 될 수도 있고 인공지능 등 여러 분야의 논의와 연관되어 등장할 수 있다. 또, 새롭게 SBOM을 도입하는 국가로 모니터링 대상을 확대하는 것도 필요하다. 예를 들면, 유럽연합에 속한 각국의 독립적인 움직임이나 아시아권 국가들의 SBOM 도입 동향에 주목할 필요가 있다. 특히, 중국 정부의 SBOM 대응이 어떻게 이루어지는지 주목해야 한다. 마지막으로 비영리 단체와 기업의 움직임도 함께 정리하면 SBOM에 관한 국제사회의 논의를 입체적으로 조망할 수 있게 할 것이고, 이는 우리나라의 관련 정책 입안에 도움이 될 것이다.

참고문헌

[1] 관계부처 합동, “디지털 기초체력 강화와 해외진출 촉진을 위한 소프트웨어 진흥 전략”, 비상경제장관회의 23-12-4, 2023. 4.

[2] 식품의약품안전처 의료기기안전국, “의료기기 사이버보안을 위한 소프트웨어 자재명세서 원칙 및 실무”, 2023. 11.

[3] 서영희, “국방 SW 공급망 보안 강화를 위한 SBOM 적용방향”, 국방논단, 제1949호, 2023. 6. 14.

[4] 이상은, “美 국방획득시스템 분석 및 협력 소요 발굴을 통한 우리나라 방산기반 강화 및 방산수출 증대 방안 연구”, 방위사업청, 2023. 10.

[5] 과학기술정보통신부, “정부, 소프트웨어 공급망 보안 지침(가이드라인) 1.0 발표”, 보도자료, 2024. 5. 13.

[6] 정보통신산업진흥원, “SBOM 전문가 회의 개최”, https://www.nipa.kr/home/4-4-1/8525

[7] 김항규, “미국 SBOM 정책 분석 및 시사점”, SPRi Issue Report IS-144, 2022. 12. 16.

[8] 김항규, “주요국 SBOm 정책 동향 분석”, SPRi Issue Report IS-150, 2022. 12. 22.

[9] NTIA, “Software Component Transparency”, https://www.ntia.gov/other-publication/2021/ntia-software-component-transparency

[10] NTIA, “Software Bill of Materials”, https://www.ntia.gov/page/software-bill-materials

[11] 미국 대통령실, “Executive Order on Improving the Nation’s Cybersecurity”, EO14028, 2021. 5. 12.

[12] 미국 상무부, “A Report to the President on Progress in Implementing Section 4 of Executive Order 14028 on Improving the Nation’s Cybersecurity”, 2022. 5. 12.
[13] CISA, “Software Bill of Materials(SBOM),” https://www.cisa.gov/sbom
[14] CISA, “CISA Releases Two SBOM Documents”, 2023. 4. 21.
[15] CISA, “CISA Open Source Software Security Roadmap”, 2023. 9. 12.
[16] CISA, “When to Issue VEX Information”, 2023. 11. 6.
[17] CISA, “SBOM Sharing Roles and Consideration”, 2024. 3. 28.
[18] 미국 Federal Register, “Federal Acquisition Regulation: Cyber Threat and Incident Reporting and Information Sharing”, Vol.88, No.190, 2023. 10. 3., pp.68055-68067.
[19] 미국 대통령실, “National Cybersecurity Strategy”, 2023. 3.
[20] 미국 대통령실, “National Cybersecurity Strategy Implementation Plan)”, 2023. 7.
[21] NSA, ODNI, CISA, “Securing the Software Supply Chain: Recommended Practices for Software Bill of Materials Consumption”, 2023. 11.
[31] Quad Critical and Emerging Technology Working Group, “Open RAN Security Report”, 2023. 5.
[32] CISA, “CISA Roadmap for Artificial Intelligence 2023-2024”, 2023. 11.
[33] 미국 재무부, “Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector”, 2023.3.
[34] NIST, “Secure Software Development Practices for Generative AI and Dual-Use Foundation Models”, Initial Pulic Draft, NIST SP 800-218A ipd, 2024.4.
[35] DARPA, “Enhanced SBOM for Optimized Software Sustainment(E-BOSS)”, HR0011124S0005, 2023. 12. 11.
[36] 미국 공군, “Platform One”, https://p1.dso.mil/who-we-are
[37] NTIA, “SBOM at a Glance”, 2021.
[38] NTIA, “一般社団法人JPCERTコーディネーションセンター”, 2021. 4. 27.
[39] 일본 경제산업성, “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”, https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/index.html
[40] DCMS, “Call for views on cyber security in supply chains and managed service providers”, 2021. 11. 15.
[41] DSIT, “Government response to the call for views on software resilience and security for businesses and organisations”, 2024. 1. 23.
[42] 영국 국가사이버보안센터, “Guidelines for secure AI system development”, 2023. 11. 27.
[43] ENISA, “Guidelines for Securing the Internet of Things”, 2020. 11. 20.
[44] EU, “Cyber Resilience Act”, 2022. 9. 15.

[45] 일본 경제산업성, “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”, 2023. 10. 31.
[46] 미국 국토안보부, “Joint Statement by United States Secretary of Homeland Security Mayorkas and European Union Commissioner for Internal Market Breton”, 2024. 1. 30.