의료기기 소프트웨어의 사이버보안 평가를 위한 SBOM 적용 국내 표준모델 제안

연세대학교 대학원

융합의학과

손 예 인

의료기기 소프트웨어의 사이버보안 평가를 위한 SBOM 적용 국내 표준모델 제안

지도교수 구 성 욱 · 장 원 석

이 논문을 석사 학위논문으로 제출함

2024년 6월

연세대학교 대학원

융 합 의 학 과

손 예 인

손예인의 석사 학위논문으로 인준함

심사위원 구성욱

심사위원 장원석

심사위원 정희교

연세대학교 대학원

2024년 6월

감사의 글

융합의학과에 입학하여 대학원 생활을 한 지 어느덧 2년이라는 시간이 흘러 졸업을 앞두고 있습니다. 학업과 실무를 병행하겠다는 의지를 다잡던 날이 기억이 납니다. 대학원 생활을 하며 큰 도움을 주시고 격려를 아끼지 않았던 모든 분께 감사의 마음을 전하고자 합니다.

특히, 논문을 지도해주시고 심사해주신 구성욱 교수님과 장원석 교수님께 감사의 말씀을 드립니다. 바쁘신 와중에도 논문 작성에 많은 관심과 심사를 해주신 정희교 고문님께도 큰 감사를 표합니다. 말씀해주신 귀중한 피드백으로 연구의 질을 한층 더 높일 수 있었던 가장 큰 원동력이 되었습니다.

더불어, 연구에 필요한 정보와 조언을 아끼지 않으신 KTL 유우진 책임님, 김정훈 박사님, 권문영 박사님 외 센터 분들께 정말 감사하다는 말씀 전합니다.

마지막으로, 저의 선택을 지지해주고 응원해준 가족과 친구들에게도 사랑한다는 말과 감사하다는 말을 전합니다.

도움을 주신 모두에게 감사하다는 말 다시 한번 드리며, 본 논문이 학문적 발전에 조금이나마 이바지할 수 있기를 바라며 글을 마칩니다.

2024년 6월
손예인 올림

차 례

그림 차례

표 차례

국 문 요 약

의료기기 소프트웨어의 사이버보안 평가를 위한 SBOM 적용 국내 표준모델 제안

본 연구를 통해 국제 사회의 소프트웨어 자재명세서(Software Bill Of Materials, SBOM) 반영 동향에 맞추어 국내 의료기기 소프트웨어 품질관리 사이버보안 측면에서 소프트웨어 자재명세서 작성에 필요한 권고 사항을 제언하고자 한다.

디지털 헬스케어의 확장에 따른 보안위협이 증가하고 있어 의료기기 소프트웨어의 보안관리가 중요해지고 있다. 오픈소스를 활용한 의료기기 소프트웨어 개발이 확장되면서 제조자가 의도치 않은 사이버보안 위협에 노출될 수 있다. 이에 대응하기 위해 소프트웨어 공급망의 투명성을 확보하는 SBOM(Software Bill Of Materials)의 필요성이 제시되고 있다. SBOM은 소프트웨어 제품에 포함된 모든 구성요소의 목록을 포함하여 소프트웨어 공급망의 보안위협을 관리하고 대응하는데 필요한 정보를 제공한다.

국제적 동향에 따라 의료기기 제품수명 전주기의 사이버보안 위험관리 절차를 개선하는데 활용할 수 있는 기본 자원인 SBOM을 반영하여 효과적인 위험관리를 진행할 수 있다.

의료기기 분야 외에도 국내 적용 선례가 많지 않으며 정부 차원의 정의가 없기에 의료기기 소프트웨어 SBOM 차원에서의 정책 동향을 제시하고 의료기기 소프트웨어 특성을 고려하여 적용 범위를 조사한다.

국내·외 의료기기 사이버보안 규제 및 IMDRF지침과 국외 주요국 정책 분석 내용을 기반으로 국내 의료기기 분야에 적용 가능한 SBOM 요소 및 제안점을 식별하여 관련 제조자 및 수행자의 작성 편의성 및 유지보수 효용을 높이고자 한다.

핵심되는 말: 의료기기 소프트웨어, 사이버보안, 소프트웨어 자재명세서, SBOM

1. 서론

1.1. 연구배경 및 필요성

의료기기 분야에서의 소프트웨어 활용은 진단, 치료뿐만 아니라 예방에 이르기까지 다양한 영역으로 확장되고 있다. 기술의 발전과 의료서비스의 질 향상이라는 두 가지 주요배경을 바탕이 있으며, 하드웨어를 동반한 내장형 소프트웨어 외에도 의료인공지능(AI)과 빅데이터 기술을 기반으로 한 독립형 소프트웨어 의료기기의 개발이 증가하고 있다. 혁신적인 기술이 의료 분야에 통합되면서 소프트웨어의 역할이 점점 중요해지고 있으며 의료영상 분석 및 진단, 환자 모니터링 등 여러 분야에서 인공지능과 빅데이터를 활용하여 진단의 정확도를 높이고, 개인 맞춤형 치료 계획을 수립하는데 기여하고 있다.

디지털 헬스케어의 확장으로 의료 서비스의 디지털화와 원격 진료, 건강 관리 앱 등 소프트웨어 기반 서비스로 보건의료의 패러다임이 변화하고 있다.

그 중 세계 시장에서의 인공지능 기술 기반 소프트웨어는 2020년 약 1억 달러에서 2026년 예상액 약 450억 달러로, 연평균 45%의 성장할 것으로 전망한다.[1) 2)]

(단위: 백만 달러)

출처: MarketsandMarkets, Atificial Intelligence in Healthcare Market, 2020

그림 1. 주요 대륙별 인공지능 의료 시장의 규모 및 전망

의료기기 분야에서 소프트웨어의 중요성이 커짐에 따라 사이버보안 문제도 함께 대두되었다. M사의 인슐린 펌프 사이버보안 문제, 이식형 심장 장치 보안 취약성 발견 등의 의료기기 사이버보안 이슈 사례가 지속적으로 발생하고 있다. 2020년 독일 뒤셀도르프 대학병원에서 사이버공격을 받아 랜섬웨어 감염으로 병원 시스템이 마비되어 환자 진료 및 치료가 불가하였고 이로 인해 발생한 최초의 사망사고가 있었다.[3)]

이외에도 의료기기 소프트웨어는 종종 외부 네트워크에 연결되어 있어 외부에서 기기를 조작하거나 민감정보를 탈취할 수 있는 취약점이 있으며, 직접적인 환자 생명 위협 및 개인 의료 데이터 유출 등의 사이버 공격의 대상이 될 수 있다.

최근 의료기기 소프트웨어 개발을 위해 오픈소스를 활발하게 사용하고 있으며 인공지능의 경우 타 소프트웨어 기능 개발보다 더 적극적으로 활용 및 참고하는 경향이 있어 제조자가 의도치 않은 사이버보안 위협에 노출될 수 있다.

주요국에서는 이미 소프트웨어 공급망의 투명성을 확보하는 소프트웨어 자재명세서(Software Bill Of Materials)의 필요성이 주목받고 있다. 미국 바이든 행정부는 솔라윈즈 해킹 사고 및 콜로니얼 파이프라인 랜섬웨어 사건[4)] 등으로 2021년 7월 SBOM을 포함한 국가의 사이버안보 강화에 관한 행정명령(EO 14028)을 발표했다. 해당 행정명령은 사이버 보안의 현대화를 위한 기술 발전 및 공공과 민간 간의 정보 교류 강화를 목적으로 구체적인 지침을 명시하고 소프트웨어 공급망 보안 강화를 통해 소프트웨어 보안성을 제고하고자 하였다.[5)] 이에 소프트웨어 공급망의 무결성을 확인하고 투명성을 증진하는 목적으로 언급되었다.

SBOM은 소프트웨어 제품에 포함된 모든 구성요소의 목록을 포함하여 공급망의 보안 위협을 관리하고 대응하는 데 필요한 정보를 제공한다. 미국은 SBOM의 의무화를 통해 공급망의 보안 강화를 추구하고 있으며, 유럽 역시 IoT 및 ICT 제품의 보안에 필수적인 요소로서 SBOM의 중요성을 강조하고 있다.

1.2. 연구목적

본 연구를 통해 국내·외 의료기기 사이버보안 규제 및 IMDRF 지침과 국외 주요국 SBOM 정책 분석을 통하여 국내 의료기기 분야에 적용 가능한 SBOM 요소 및 제안점을 식별하여 관련 제조소 및 수행자의 작성 편의성 및 유지보수 효용을 높이고자 한다.

SBOM은 의료기기에 사용된 소프트웨어 구성요소와 사이버보안 취약성 악용 가능성을 식별하고 해결하기 위한 도구로 사이버보안 강화를 위해 필요한 사항이다.

미국 식품의약국(Food and Drug Administration, FDA)은 소프트웨어 규제 동향에 맞추어 2023년 3월 의료기기 사이버 보안법(Ensuring Cybersecurity of Devices, Section 524B(a) of the FD&C Act)를 발표하였고, 이에 자국 내 유통되는 인터넷에 연결 가능한 모든 의료기기는 SBOM을 필수적으로 제출해야 한다.

국제의료기기규제당국자포럼(IMDRF, International Medical Device Regulators Forum) 또한 “의료기기 사이버보안을 위한 소프트웨어 자재명세 원칙 및 사례(Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity)”를 발간하였다.

이러한 국제적 동향을 비교 및 반영하여 국내 의료기기 소프트웨어 제조업체의 품질관리 사이버보안 측면에서 소프트웨어 자재명세서 작성에 필요한 권고 사항을 제언함으로써, 소프트웨어가 적용된 의료기기의 개발, 상품화 및 유지보수 과정에 도움을 제공하여 사이버보안 측면에서 환자의 안전 확보의 안정성이 유지될 수 있도록 하는 데 목적이 있다.

1.3. 연구범위 및 방법

1.3.1. 연구범위

국내 식품의약품안전처에서 제공하는 가이드라인과 동일하게 소프트웨어를 포함하는 의료기기(펌웨어 및 프로그램 가능 논리 제어기를 포함하는 의료기기) 또는 소프트웨어 의료기기 중 유·무선 통신(USB, Wi-Fi 등)을 사용하거나 통신 경로가 있는 의료기기에 적용한다.[6)]

의료기기 소프트웨어의 체계적인 사이버보안 관리를 위한 소프트웨어 자재명세서 작성 및 평가방법을 위한 작성모델을 제시한다.

1.3.2. 연구방법

문헌조사를 통해 국내·외 의료기기 사이버보안 규제 동향을 파악하고 IMDF 지침과 주요 국가 SBOM 정책 분석을 바탕으로 국내 의료기기에 적용 가능한 SBOM 요소 및 제안점을 식별한다.

의료기기 분야 외에도 국내 SBOM 적용 선례가 많지 않으며, 정부 차원의 정의가 없기에 소프트웨어 SBOM 차원에서의 정책 동향을 제시하고 의료기기 소프트웨어의 특성을 고려하여 적용 범위를 조사한다.

IMDRF, 미국 국립 표준 협회(ANSI, American National Standards Institute), 국제 표준화 기구(ISO, International Organization for Standardization) 등 국제 규격을 분석하고, 주요 국가의 SBOM 관련 규제와 요구사항을 비교하여, 사이버보안 위험 관리 도구 역할을 확립하고자 한다. 의료기기 제조소의 SBOM 작성 및 관리방법을 필두로 작성 시 고려사항, 작성예시를 포함한다.

1.4. 약어 및 용어정리[7) 8) 9) 10) 11)]

(1) 가용성(Availability): 공인 기관의 요구 시 접근 가능하며 사용 가능한 성질 (KS X ISO/IEC 27000:2019)

(2) 기밀성(Confidentiality): 정보를 비인가 개인, 기관, 프로세스가 사용할 수 없게 하거나 이들에게 공개되지 않게 하는 성질 (KS ISO/IEC 27000:2019)

(3) 무결성(Intergrity): 생성, 전송 또는 저장된 이후로 비인기된 방식으로 데이터가 변경되지 않은 성질(KS X ISO/IEC 27000:2019)

(4) 소프트웨어 의료기기(SaMD, Software as a Medical Device): 하드웨어에 종속되지 않고 의료기기의 사용목적에 부합하는 기능을 가지며 독립적인 형태의 소프트웨어만으로 이루어진 의료기기

(5) 사이버보안(Cybersecurity): 전체 생명주기 동안 기밀성, 무결성, 가용성이 적절한 수준으로 유지되도록 접속, 사용, 공개, 변경 또는 파괴 등의 비인가된 활동으로부터 정보와 시스템이 보호된 상태(ISO 81001-1:2021)

(6) 취약성(Vulnerability): 하나 이상의 위협에 의해 유발될 수 있는 자산 또는 통제 부족의 보안 경영시스템(KS ISO/IEC 27000:2019)

(7) 어플리케이션 프로그래밍 인터페이스(API, Application Programming Interface): 애플리케이션 프로그램에서 네트워크 서비스, 장치 또는 운영 체제에 액세스하는데 사용할 수 있는 표준 소프트웨어 인터럽트, 호출, 함수 및 데이터 형식의 집합 (ISO 10303-1:2021)

(8) 자산(Asset): 개인, 정부 또는 정부기관에서 가치가 있다고 판단하는 물리적 또는 디지털 본질

(9) 구성요소(Component): 시스템의 물리적 또는 논리적 부분을 구성하는 시스템 리소스의 집합이며, 기능과 인터페이스가 명시되어 있으며 정책 또는 사양에 따라 시스템의 다른 부분과 독립적으로 존재하는 것

(10) 해시 해시값(hash): 데이터에서 고정된 길이의 임의 값을 생성하는데 사용되는 계산 방법인 해시 함수에 의해 계산된 값
(ISO 17090-4:2020)

(11) 수명주기(Life cycle): 제품 또는 시스템의 초기 구상부터 최종 폐기 및 폐기에 이르는 일련의 모든 수명 단계
(ISO 81001-1:2021)

(12) 릴리즈 및 업데이트(Release and Update): 의료기기 소프트웨어의 수정, 예방, 적응 또는 완벽한 수정하는 작업

(13) 저장소(Repository): 데이터 검색이 가능한 체계적이고 영구적인 데이터 저장소
(ISO/IEC/IEEE 26511:2018)

(14) 소프트웨어 자재명세서(SBOM, Software Bills of Materials): 하나 이상의 식별된 구성요소, 관계 및 기타 관련 정보의 목록

(15) 소프트웨어 구성요소(Software component): 소프트웨어 시스템 또는 모듈, 단위, 데이터 또는 문서와 같은 요소를 지칭하는데 사용되는 일반적인 용어임
(IEEE 1061)

(16) 소프트웨어 구성 분석(Software component analysis): 하나 이상의 도구를 사용하여 코드 베이스를 스캔하여 어떤 코드가 포함되어 있는지 식별하는 도구이며, 비공개 소스 소프트웨어, 무료 및 오픈소스 소프트웨어, 라이브러리 및 패키지 등이 있음

(17) 소프트웨어 투명성(Software transparency): 소프트웨어의 모든 프레임워크, 계층 구조 및 구성요소를 검토하는 소프트웨어의 개략적인 구조

(18) 시스템(System): 하나 이상의 기능을 수행하기 위해 구성된 상호 작용하는 요소 또는 자산의 조합(ISO/IEC/IEEE 12207:2017)

(19) 타사 소프트웨어(3rd-party software): 관련 당사자와 독립적인 것으로 인정되는 개인 또는 단체가 제공하는 소프트웨어이며 ISO/IEC 가이드 2에서 수정됨

(20) 관련 당사자: 1st party(공급자), 2nd party(구매자)의 이해관계자를 나타냄

(21) 취약점(vulnerability): 하나 이상의 위협에 의해 악용될 수 있는 자산 또는 제어의 약점(ISO/IEC 27000:2018)

2. 의료기기 사이버보안 현황

2.1. 의료기기 사이버보안 기본 원칙

의료기기 사이버보안에서 중요한 세 가지 원칙은 가용성(Availability), 기밀성(Confidentiality), 그리고 무결성(Integrity)이다.[12)]

가용성은 승인된 사용자가 필요할 때, 필요한 장소에서, 그리고 필요한 형태로 데이터에 접근할 수 있어야 한다.

기밀성은 데이터가 허가되지 않은 사람들에 의해 접근되거나 사용되지 않도록 보호되어야 하며 이를 위해 제조사는 데이터가 전송되는 과정에서 또는 비인가자에 의해 조회될 때도 정보를 해독하기 어렵도록 암호화를 적용해야 하고 접근은 인가된 사용자에게만 허용되어야 한다. 사용자는 자신의 목적과 권한에 맞게 접근범위를 제한해야 한다.

무결성은 데이터가 허가되지 않은 방식으로 변경되거나 손상되지 않아야 함을 의미한다. 정보는 정확하고 완전하게 유지되어야 하며 변경은 인가된 사용자에 의해서만 가능해야 하고, 이러한 변경 사항은 로그와 변경 이력으로 관리되어야 한다.

국제의료기기규제당국자포럼의 현재 사용되는 제품의 기술적 특성을 반영한 사이버보안 요구사항은 아래 <표 1>와 같다.[13)]

표 1. 의료기기 사이버보안 요구사항

항목	요구사항
보안통신	· 의료기기 제조자는 다른 기기나 네트워크와의 접속 방법을 고려해야 한다. 예시) USB, Wi-Fi 등 · 제조자는 내부 및 외부에서 들어오는 모든 입력의 유효성 확인을 위한 설계 특성을 고려해야 하고, 가정용 네트워크 등과 같은 보안이 약한

	통신을 지원하는 기기 및 환경에서의 통신도 고려해야 한다. · 비인가 접근, 변경, 반복을 방지하기 위해 의료기기의 데이터 송수신은 보안이 보장되어야 하며, 예로 시스템-기기 간 통신할 시에 상호 인증 방법, 암호화 필요성, 기존에 전송된 데이터 및 명령어의 비인가 반복 방지, 통신 종료 시점의 적절성이 있다.
데이터 보호	· 제조자는 기기와의 데이터 송수신이나 저장 시 안전성과 관련된 데이터에 대해 암호화 등의 보호 수준을 고려해야 하며, 예로 비밀번호는 암호화된 보안이 확보된 해시로의 저장이 있다. · 기밀성 위험을 통제할 때, 제조자는 통신 프로토콜의 컨트롤/시퀀싱 필드의 메시지를 보호해야 한다. 암호화 키 관련 자료가 손상되는 것을 방지해야 한다.
기기 무결성	· 데이터 부인 방지를 위한 설계 특성이 요구되는지 결정하기 위해 제조자는 시스템 레벨에서 아키텍처를 평가해야 하며, 예로 감사 로그 기록 기능을 제공이 있다. · 제조자는 기기 소프트웨어의 무결성에 대한 위험, 즉 비인가된 변경을 고려해야 한다. · 제조자는 기기에서 실행될 수 있는 바이러스, 스파이웨어, 랜섬웨어 등과 같은 악성 코드를 막기 위해 안티 멀웨어 프로그램 등의 통제 조치를 고려해야 한다.
사용자 인증	· 제조자는 기기의 사용이 입증된 사용자, 다른 역할의 사용자에게 사용 권한을 부여하거나, 응급상황에서 접근을 허용하는 것을 포함하여 사용자 접근 통제를 고려해야 한다.

	· 동일한 자격 증명은 기기와 고객들 사이에 공유되지 않아야 한다. 접근 통제의 예로는 비밀번호, 하드웨어 키, 생체 인증 등이 있다.
소프트웨어 유지보수	· 제조자는 정기적인 업데이트의 실현과 배포를 위한 절차를 수립하고 통보해야 한다. · 제조자는 운영 체제 소프트웨어/ 오픈소스 소프트웨어/ 제3자 소프트웨어가 업데이트나 통제될 경우를 고려해야 하며 외부 통제로 인한 소프트웨어 갱신이나 운영 시스템 종료에 대한 대처 전략을 마련해야 한다. 예시) 보안이 보장되지 않은 운영 체제 버전에서 운영되는 경우 · 제조자는 최신 사이버보안 약점에 대처하기 위한 의료기기 업데이트 전략을 검토해야 한다. 업데이트 과정에서 사용자 개입 또는 자동 갱신 여부, 장치의 성능 및 안정성에 미치는 영향을 확신할 수 있는 업데이트 유효성 검증을 고려해야 한다. · 제조자는 업데이트를 위해 필요한 연결과 코드 서명 등을 통한 연결이나 업데이트의 진본성을 고려해야 한다.
물리적 접근	· 제조자는 허용되지 않은 개인이 의료기기에 무단 접근하는 것을 막기 위한 통제 수단을 고려해야 한다. 예시) 물리적 잠금 장치나 연결 포트의 접근 조절, 인증 불필요한 물리적 연결선의 접근 통제 등
신뢰성 및 가용성	· 제조자는 의료기기가 필수 성능을 보존하기 위해 사이버보안 공격을 인지, 방어, 대체, 및 복구 가능한 설계 특성을 고려해야 한다.

기밀성과 무결성 원칙의 가혹한 적용은 가용성을 손실하는 결과를 초래할 수 있으므로 제조자는 의료기기의 사이버보안과 환자의 안전을 보장하기 위해 가용성, 기밀성, 무결성이 조화로운 수준에서 준수되어야 하며, 의료기기 위험관리와 같이 「의료기기 제조 및 품질관리 기준」에 따라 의료기기 제조업체가 품질시스템 내에서 확립한 위험 관리 절차를 적용해야 한다.

2.2. 의료기기 사이버보안 취약점

Cynerio사가 발행한 “The State of Healthcare IoT Device Security(2022)”에 따르면, 2021년에는 미국의 의료기관이 500건 이상의 사이버 공격을 받아 210억 달러의 손실을 입었다. 랜섬웨어 공격은 전년도에 비해 123% 증가하였으며, 각 랜섬웨어 공격으로 인한 복구 비용은 평균적으로 800만 달러가 소요되었고 피해 복구 기간은 대략 287일이 소요되었다.

매달 한 번 이상 사용되는 IoT 기기는 전체의 79%를 차지하며, 한 달에 한 번도 사용되지 않는 기기는 21%였다.[14] 병원에서 일반적으로 사용되는 의료 IoT 기기 중 38%는 정맥 주입 펌프로, 이들 중 73%는 환자의 안전, 데이터 기밀성, 서비스 가용성을 위협할 수 있는 적어도 하나 이상의 취약점을 가지고 있었다. 정맥 펌프 외에도 아래 <표 2>와 같이 보안 취약점 및 사고 사례가 발생했다.

표 2. 사이버보안 취약점 및 사고 사례

위험도 구분	사례	내용
취약점	심장박동기, ICD 취약점	- ‘08년, Medical Device Security Center는

	심장박동기(Implantable Cardioverter Defibrillator)에 전기를 공급하여 기기의 작동을 멈출 수 있다는 연구 결과를 발표함. - '17년, St.Jude Medical사 심장박동기 보안 취약성 발견.
인슐린 펌프 해킹	- '11년, Black Hat는 당뇨 환자의 인슐린 주입기에 있는 무선 기능의 약점을 통해 인슐린 투여량을 외부에서 변경할 수 있는 '치명적 공격' 가능성을 공표함. - '11년, McAfee FOCUS 이벤트에서 인슐린 주입기 관련 해킹 시연. - '16년, J&J사 인슐린 펌프 사이버보안 경고. - '19년, Medtronic사 인슐린 펌프 사이버보안 문제 확인.
맥박 조정기 해킹	- '12년, BreakPoint security conference 2012에서 맥박 조정기에 해킹에 대해 발표.
의료기기의 하드 코드 된 암호	- '13년, ICS-CERT에서 의료기기 내부에 하드 코드 된 암호에 대한 경고 발표. - 수술 장비, 마취용 인공호흡기, 약물 주입기 등이 있으며, 장비에 따라 원격 제어가 가능함.
생화학 자동 분석 장치에 쓰이는 Oracle 소프트웨어의 취약점 발견	- '13년, FDA Enforcement Report에서 장치의 데이터베이스에 대한 원격 접근의 취약점 발표.

사고사례	Beth Israel Deaconess Medical Center에서 태아 모니터링용 시스템	- 고위험군 임산부용 태아 모니터링 시스템이 악성코드에 감염되어 장치의 성능이 저하됨.
	원격 모니터링 취약점	- '12년, ICS-CERT에서 의료기기 원격 감시에 대한 경고 발표

CT, MRI, 심전도기, 초음파 기기 등 고가의 의료기기를 운영하기 위해 여러 대의 PC 서버가 필요하며, 연동 PC에는 오래된 OS 운영체제가 사용되고 있었다. 도입된 지 10년에서 20년 이상이 지난 OS의 사용 및 기기의 운영, 교체, 개선 등의 작업은 제조사나 공급업체가 원격으로 접수하여 진행했다. 또한, Linux OS는 전 세계 웹 서버의 70%와 IoT 기기의 48%에서 사용되고 있어, 의료기관을 대상으로 랜섬웨어 조직이 리눅스 기반 의료기기를 공격하는 경우가 급증하였다.

의료기관의 경우, 병원 내부망 네트워크에 와이파이 등 외부와 연결될 수 있으며, 의사 및 간호사, 의공기사, 유지보수 IT 관련자 등 의료기기 접근 및 사용을 통해 의료데이터 유출과 악성코드 감염 위험에 노출되어있다.

그림 2. 의료기기 보안 위협 요소[15]

2.3. 의료기기 사이버보안 규제 동향

2.3.1. 국내 규제 동향

국내 식품의약품안전처에서는 2019년 11월에 “의료기기 사이버보안 허가·심사 가이드라인(민원인 안내서)”를 최초 제정하여 사이버보안 자료 제출을 필수화하였으며, 2022년에 IMDRF의 “의료기기 사이버보안 원칙 및 기준”의 적용범위, 정의, 시판 전 고려사항을 적용하여 개정하였다. 해당 개정에서 가장 큰 변화는 ‘필수원칙 체크리스트’ 제출에서 ‘요구사항 체크리스트’ 제출로 변경되었으며, 필수원칙의 항목 또한 요구사항의 항목으로 시판 전 사이버보안 고려 항목을 좀 더 일반화하였다. 이는 의료기기 사이버보안에 대한 요구사항 준수 이행을 확인 가능하게 하며, 제조자는 요구사항을 실제로 검증한 자료를 제출하여야 한다.

‘의료기기 사이버보안 요구사항 체크리스트’는 요구사항에 대한 적합성 여부를 검증할 수 있는 자료가 필요하며, 필수원칙 체크리스트 양식을 사용하여 제품의 특성에 맞게 기재한다. 사이버보안 요구사항을 검증하기 위한 자료에는 소프트웨어 검증 및 유효성 검토 자료, 성능시험 성적서, 사이버보안 위험관리문서가 있으며 사이버보안 위험관리 문서의 경우 해당 보안 기준의 미적용 사유를 입증할 수 있는 자료로도 사용한다.

2023년 11월, 가장 최신 개정 이력으로 사이버보안 제출자료 요건을 좀 더 명시화하였으며 변경 시 제출자료, 허가신청서 기재방법을 명확화하였다.

“의료기기 허가심사 시 자주 묻는 사이버보안 질문집(FAQ)(민원인 안내서)”(2021)은 사이버보안 자료 제출대상 여부와 체크리스트 적용 및 안전성 입증 자료에 대한 질문 및 답변을 중심으로 내용을 구성하였으나 ‘19년도 버전의 가이드라인 내용을 중심으로 질문·답변이 구성되어 있어 현 가이드라인 내용을 기준으로 적용하기에 일부 내용의 업데이트가 필요한 상황이다.

2.3.2. 국외 규제 동향

(1) 의료기기규제당국자포럼(IMDF)의 사이버보안 지침 사항

IMDRF는 사이버보안 측면에서 의료기기의 안전과 성능이 보장될 수 있도록 전 세계적으로 접근 가능한 워킹그룹을 만들어 의료기기 수명주기 전반에 걸친 이해관계자들을 위한 사이버보안 지침을 발간하고 있다. “Principles and Practices for Medical Device Cybersecurity”를 발간하여 국내 사이버보안 가이드라인에 적용된 내용의 토대가 되는 지침서가 되었다. 의료기기 사이버보안 적용을 위한 기본 원칙 및 지침이 기술되어 있으며, 국내 사이버보안 가이드라인에서 참조함에 따라 요구사항 또한 동일하게 기술하고 있다.

최근 사이버보안의 지침이 강화됨에 따라 기존에 개발되었던 의료기기 및 사이버보안 업데이트를 더이상 제공하지 않게 되는 legacy medical device에 대해 기존의 지침으로 대응하기 힘들었다.

의료기기는 제품 출시 이후에도 의도한 성능에 문제가 없으면 시장에서 계속 사용될 수 있으며 제조사의 판매/관리 범위 밖에서도 거래되어 사용될 수 있는데, 이는 사이버보안이 보장되지 않은 상태에서 환자에게 사용되게 됨으로써 사이버보안 측면의 잠재적인 위험을 끼칠 수 있는 요소로 작용할 수 있다.

“Principles and Practices for the Cybersecurity of Legacy Medical Devices” 지침은 legacy medical device에 대해서 제조사(Manufacture)와 의료 서비스 제공자(Healthcare Provider)가 Total Product Life Cycle(TPLC) 동안 의료기기로부터 환자의 안전이 확보될 수 있도록 책임을 이관하는 방법에 대해서 제공한다.

최근 소프트웨어 개발 추세는 제조사가 자사의 기술로만 개발하는 것이 아닌 각종 3자 소프트웨어 및 라이브러리를 포함하여 의료기기의 다양한 기능들을 개발하고 있다. 제조사가 사용하게 되는 3자 소프트웨어 및 라이브러리의 제조사 및 개발자 또한 다시 다른 3자 소프트웨어와 라이브러리를 참고하여 개발하게 되면서, 소프트웨어의 타 개발

제품에 대한 의존성(dependency)이 높아진 상황이다.

“Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity[16]” 지침은 제조사가 개발에 사용된 소프트웨어 자재들이 투명하게 공유를 통해 소프트웨어 개발 시 참조하는 최초 단계부터 의료기기를 통해 서비스까지 SBOM이 유기적으로 연결됨으로써 의료기기 사이버보안의 확보를 위한 방법을 제공한다.

(2) 미국 식품의약국((Food and Drug Administration, FDA)의 사이버보안 현황

미 FDA에서는 ‘14년 “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices” 최초 draft 버전인 가이드라인을 발간하였으며, 여러 번의 업데이트를 거쳐 ‘23년 9월 최종 버전을 제시했다.

국내 사이버보안 가이드라인은 출시 전 설계에 적용해야 하는 사이버보안 요구사항을 위험관리 관점에서 기록되어 있다면, FDA 사이버보안 가이드라인은 사이버보안을 QSR(Quality System Regulation)의 일부로 보고 있다.

보안을 위한 설계와 의료기기 수명주기 동안 투명한 정보 공개 및 위험관리 관점에서 가이드를 제시하고 있다.

특히, 국내 사이버보안 가이드라인에는 언급하지 않은 소프트웨어 자재 명세서(SBOM)에 대한 내용도 제시하고 있어 의료기기의 사이버보안 관리를 강조하고 있다.

주요 의료기기 사이버보안 관리 치짐은 <표 3>과 같으며, 의료기기 제조업체 및 의료기기를 사용하는 의료기관에 권고되는 보안 유의사항이다.

표 3. 의료기기 사이버보안 주요 보안관리 지침 사항[17)]

구분	보안 사항
의료기기 제조업체	· 의료기기 사이버보안 위험 점검 · 사이버보안 문제 발생 후 대응 및 복구 방안 안내 · 각 의료기기별 보안 관리 계획 수립 · 의료기기 비인가 접근 차단 기술 검사 · 접근 제어 기술로 의료기기 접근 관리
의료기관	· 네트워크 경유 무단 접근 차단 · 바이러스 및 방화벽 업데이트로 악성코드 예방 · 네트워크 감시 활동 · 보안 업데이트 및 네트워크 부분 보호 조치 · 의료기기 사이버보안 문제 발생 시 제조사 문의, 불가능할 경우 FDA, DHAS ISC-CERT로 취약성 지원 요청

미국에 공개된 의료기기 개발 관련 지침 및 위협 방지 분석은 다음과 같다. DOD(Department of Defense)는 STIG(Security Technical Implementation Guides)와 DIACAP(DoD Information Assurance Certification and Accreditation Process) 문서를 공개하여 의료기기 개발에 활용할 수 있도록 지침을 제공하고 있으며, STIG는 컴퓨터 하드웨어 및 소트프웨어의 설치 및 유지보수에 대한 표준화된 보안 절차과 세부적인 요구사항을 규정하며 의료기기에 적용 가능한 항목을 포함한다.

HIMSS(Healthcare Information and Management System Society)는 의료기기 판매 보안 선언서인 MDS2(Manufacturer Disclosure Statement for Medical Device Security)를 공개하였고. 이는 의료기기 제조업자가 구매 사업자에게 의료기기의 보안 정보를 제공하도록 한다.

DHS(Department of Homeland Security)는 의료기기 하드코드에 대한 문제점을 제시하는 'ICS-CERT Alerts' 문서를 공개하였는데, 다수 의료 장비에서 고정된 비밀번호가 확인되었고, 이 정보로 공격자가 의료 장비를 조작할 수 있다는 위험이 지적되었다.

HITRUST(Health Information Trust Alliance Common Security Framework)는 의료기기의 보안성을 평가하기 위해 'CyberRX'라는 모의 해킹 테스트를 시행하고 있으며, 헬스케어 산업에 대한 포괄적인 공격 상황을 확인하고 공격 데이터를 조사하여 정보 공유 및 활동에 대한 개선을 목적으로 하는 사이버 관련 훈련이다.

(3) 유럽 EU MDR(Medical Device Regulation)의 사이버보안 현황

유럽 MDR는 최근 의료기관과 의료기기를 대상 해킹 공격으로 인해 환자, 개인 정보 및 전체 의료시스템이 위험에 노출되고 있다고 판단하고 있다. 이에 대응하기 위해 EU MDR은 사이버보안 규칙을 엄격하게 적용하고자 '19년 12월에 MDCG 2019-16 Rev.1 'Guidance on Cybersecurity for medical devices'를 제정하였으며, '20. 07 업데이트를 진행하였다.

ANNEX I - Mapping of IT security requirements to NIS Directive Cooperation Group measures를 통해 상세 요구사항과 관련한 규정을 확인할 수 있으며, 주요 내용은 <표 4>와 같다.

표 4. CE MDR MDGC 사이버보안 요구사항 관련 주요규정

MDR 규정	요구사항 항목
개인정보 보호와 데이터 보호:	장치의 일치성을 입증하기 위해 실시된 임상
제 62.4(h) 조	조사에 대한 일반 요구사항
제 52 조	일치성 평가 절차
제 83 조	제조업체의 시장 감독 시스템
제 84 조	시장 감독 계획
제 85 조	시장 감독 보고서
제 86 조	주기적 안전 업데이트 보고서
제 87 조	심각한 사고와 현장 안전 수정 조치의 보고
제 88 조	추세 보고
제 89 조	심각한 사고와 현장 안전 수정 조치의 분석
부록 II	기술 문서
부록 III	시장 감독에 대한 기술 문서
MDR 제 VI 장 및 부록 XIV	임상 평가 및 시장 팔로업

(4) 기타 주요국의 사이버보안 현황

일본 후생노동성은 의료법 시행 규칙의 일부 개정을 발표했으며, 사이버보안 강화에 초점을 맞춘 가이드북을 구성하였다. '23년 4월에 시행되었으며 국제의료기기규제포럼 가이드라인과 권고 사항을 기반으로 하며, '18년도 7월에 발표된 의료기기 사이버보안 지침을 대체한다. 일본 외 호주TGA 및 캐나다 역시 의료기기 사이버보안을 위한 가이드라인 및 시판 전 요구사항을 제정하여 위협에 대응하고 있다.

3. 의료기기 분야에서의 소프트웨어 자재명세서(SBOM) 적용

3.1. SBOM 개요 및 프레임워크

3.1.1. SBOM 정의 및 개요

소프트웨어 사이버보안 문제는 국가적으로 중요한 이슈로 인식되고 있으며, 이에 따라 각국은 ICT 공급망의 위험을 관리하는 정책을 구축하고 실행하고 있다.

소프트웨어가 포함된 제품을 조달할 때 취약점을 진단하고 조치를 완료한 제품을 공급할 수 있도록 하고 인증된 공급업체를 활용하는 것을 권장한다. 또한, 보안 요구사항을 충족하고 인증된 정보보호 제품군을 사용하여 ICT 제품의 안전성을 검증한다. 그럼에도 불구하고, 공격자들은 소프트웨어 공급망을 악용하여 불안정한 환경의 소프트웨어 개발 및 업데이트 과정에 침투하고 악성코드를 배포하는 등의 공격을 수행한다.

해킹에 대비하기 위해 인증된 제품에 대한 추가적인 보안성 검증이 필요하게 되었으며, 공급망 침해 탐지와 선견적 대처, 손상 발생 지점 확인, 피해 규모 추정, 신속한 대응책 마련을 위해 공급망의 투명성 및 정합성 확보의 중요성이 강조되었다.

IT 응용 프로그램 소프트웨어의 품질 개선 및 기술 공급 기업인 CISQ사 는 신뢰 가능한 시스템은 추척성이 확보되어야 하며, 이를 위해 소프트웨어 구성요소와 함께 출처가 공급망 전체에 공유되어야 한다고 제언했다. 외에도 MITRE 등 국가 안보 공급망에 대한 주제로 소프트웨어 구성요소의 중요성을 강조하고 각 요소의 위험을 바탕으로 총체적 위험을 추정할 수 있음을 주장했다. 이처럼 소프트웨어 자재명세서(SBOM)는 소프트웨어 공급망의 무결성 검증, 정보 공유, 그리고 가시화를 위한 중요한 도구로서, 사이버보안 관련 문서에서 꾸준히 언급되었다.

SBOM 작성, 유지, 갱신의 부분에서 의료기기의 사이버보안 측면의 직접적인 효용은 다음과 같다.

- 투명성 증가: SBOM을 통해 조직은 사용 중인 소프트웨어의 정확한 구성을 파악할 수 있고, 이는 잠재적인 취약점을 식별하고 평가하는 데 필수적임.

- 위험 관리 개선: 소프트웨어 구성 요소에 대한 명확한 이해를 바탕으로 조직은 보안 취약점과 관련된 리스크를 보다 효율적으로 통제할 수 있음. 취약점이 발견될 경우, SBOM을 사용하여 해당 구성 요소를 빠르게 파악하고 대응 가함.능

- 신속한 대응: 사이버 보안 사고가 발생했을 때, SBOM은 문제의 원인을 빠르게 찾아내고 해결할 수 있음. 소프트웨어 구성 요소의 정확한 목록이 있으면 보안 팀은 취약점을 통한 공격 경로를 더 쉽게 추적 가능함.

- 규제 준수: 여러 국가와 산업에서는 사이버보안 관련 규제를 준수하기 위해 SBOM의 작성 및 유지 관리를 요구하고 있어, 법적 요구사항을 충족하는데 필수적인 도구가 될 수 있음.

- 보안 운영 효율성 향상: SBOM은 보안 운영의 효율성을 향상시킬 수 있고, 구성 요소의 목록을 파악 가능한 상태로 새로운 취약점에 대한 알림을 받았을 때, 해당 취약점이 조직 내 어떤 시스템에 문제를 발생시키는지 신속히 파악할 수 있음.

NTIA(National Telecommunication and Information Administration)는 '18년 다양한 이해관계자를 소집하여 소프트웨어 투명성에 대해서 논의를 진행하였다. 그 결과물 중 하나로 소프트웨어 자재명세서(Software Bills of Materials)개념이 탄생하였으며, '하나 이상의 식별된 구성요소와 그 관계 및 기타 관련 정보의 목록'이라고 정의했다.

NTIA의 SBOM 정의는 <표 5>와 같다.

표 5. SBOM 기준 속성[18)]

기준	설명
작성자명	SBOM 작성자
타임스탬프	SBOM 가장 최근에 업데이트된 날짜 및 시간
공급업체명	SBOM 항목에 포함된 구성요소의 공급업체명 및 식별자
구성요소명	구성요소명 및 식별자
버전 스트링	구성요소의 버전
구성요소 해시	구성요서 암호화 해시
고유 식별자	구성요소를 고유하게 정의하는 추가 정보
관계성	SBOM 구성요소 간의 관계

미국 행정명령 14028에 따라 공급망의 보안성을 검증하는 도구로써 SBOM의 가치와 필요성을 강조하였고 정부기관이 ICT 제품을 조달할 때 SBOM의 제공을 의무화하였다. 이 같은 움직임은 전 세계적으로 확산되어 여러 국가에서도 SBOM을 기반으로 공급망 보안을 강화하는 정책을 추진하고 있다.

소프트웨어 동향에 맞추어 디지털화하고 있는 의료기기 분야에 SBO 적용 필요성이 제기되고 있다. 소프트웨어에서 발생하는 사이버보안의 잠재적인 취약점은 제조사가 의료기기 제조에 사용한 소프트웨어 구성요소로부터 비롯될 수 있으며 보안과 관련이 없는 기능을 구현하더라도, 나중에 취약점이 발견되면 다양한 장치에 영향을 미칠 수 있다.

최근의 개발 트렌드는 다양한 구성요소들이 서로 의존하며 참조를 반복하게 되는데, 이는 추적성을 낮추고 복잡성을 증가시키는 결과를 가져온다. 복잡성은 공급망 공격에 대한 더욱 복잡한 도전을 제기하며 적절한 대응 전략을 마련하는 것이 중요하다.
NTIA활동을 통해 SBOM 개발 및 채택을 위한 초석이 마련되었으며, IMDRF 또한 해당 내용을 기반으로 SBOM에 대한 내용을 정리하고 있다.

SBOM은 시판 전부터 시판 후까지 즉, 총 제품수명주기에서 사이버보안 위험관리 프로세스를 개선하는 자료로 사용될 수 있다. 제조사는 기기를 개발하며 SBOM을 통해 알려진 소프트웨어 및 라이브러리의 취약성을 추적하고 사이버보안 위협으로 안전한 기기를 출시할 수 있다. 시판 후에는 SBOM을 사용하여 지속적으로 모니터링을 함으로써 시장에 출시 후에 사이버보안 위험에 노출된 기기를 식별할 수 있다.

국내 “의료기기 사이버보안 허가·심사 가이드라인(민원인 안내서)”에서는 SBOM에 대해서 직접적으로 언급하고 있지는 않으나 체크리스트의 소프트웨어 유지보수 분류에 있는 요구사항의 적용을 위하여, SBOM을 사용한다면 총 제품수명주기에서 제조자와 의료서비스 제공자 모두에게 도움이 될 수 있다.

특히, SBOM은 제품의 단종(End Of Life)을 추적하고 대비하는데 투명성을 보장하는 효과적인 도구이며 이를 통해 제조사는 총 제품수명 단계별로 의료서비스 제공자로 하여금 사이버보안 위협을 체계적으로 맞서 처리하도록 보조할 수 있다.

의료서비스 제공자는 각 제조사별로 SBOM을 제공받으므로 의료시스템 구축 및 유지관리 시 좀 더 사이버보안 위험을 평가하여 환자에게 사이버보안으로부터 안전한 의료서비스를 제공할 수 있다. 또한, SBOM은 제조사가 성숙한 사이버보안 체계를 구축했음을 나타내는 지표로 사용될 수 있기에, 규제 및 평가기관은 SBOM을 통해 의료기기에 사용된 소프트웨어에 대해 사이버보안 위험에 대해 객관적인 평가를 수행하는데 유용하다.

국내 인허가과정에서 SBOM 제출을 의무화하고 있지 않으나 국외 규제기관에서는 SBOM 제출을 요망하고 있어 이에 대한 선제적 대응이 필요한 상황이다.

3.1.2. SBOM 활용과정 및 프레임워크

SBOM에 사용되는 콘텐츠는 제조사에 의해 수집되어 소프트웨어 구성요소 저장소에 보관된다. 제조사는 자사에서 작성한 프로그래밍 코드 및 SBOM 콘텐츠를 빌드 과정을 통해 최종 소프트웨어 실행파일 또는 실행을 위한 스크립트로 생성하여 배포를 위한 릴리즈 과정을 거치게 된다.

배포 버전의 최종 검수 이후에는 의료서비스 제공자에게 제공되어 의료행위에 활용되게 된다.

아래 <그림 3>은 SBOM의 유기적인 연계를 통한 제조사와 의료서비스 제공자의 프레임워크를 나타낸 것이다. 해당 과정을 통해 제조사와 의료서비스 제공자는 소프트웨어의 높은 투명성을 바탕으로 의료기기의 안전을 확보할 수 있다.

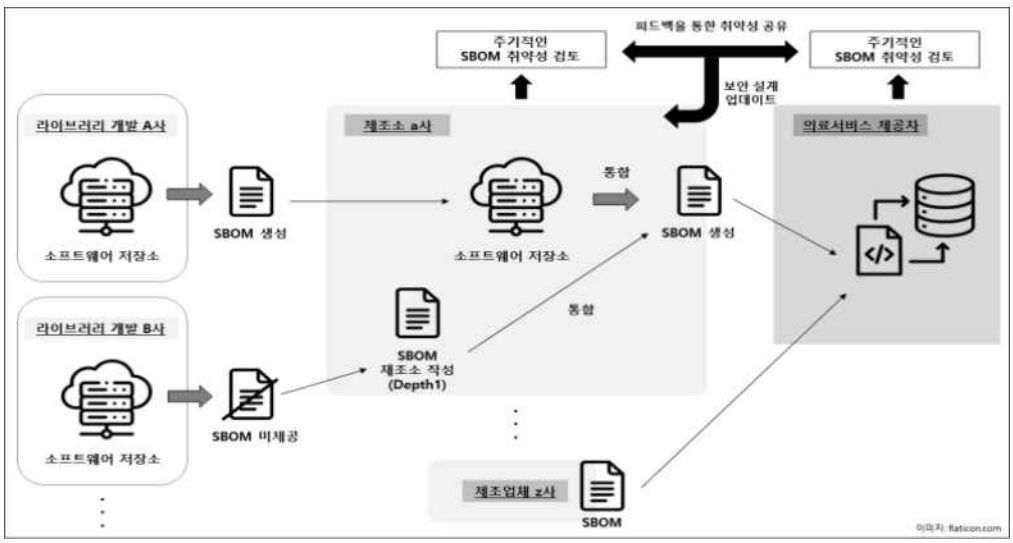

그림 3. SBOM 활용을 위한 프레임워크

3.2. SBOM 적용 방안

NTIA에서 기술한 “Roles and Benefits for SBOM Across the Supply Chain” 보고서에서는 SBOM 적용방안을 소프트웨어의 생성, 선택, 운영의 관점에서 서술하였다.

소프트웨어 생산(Produce)에 있어서 SBOM을 활용할 때, 소프트웨어 취약점 구성요소 모니터링이 용이하며 새로운 위험 발견 시 잠재적 취약 요소를 예측할 수 있다.

소프트웨어 선택(Choose)은 소프트웨어 전체의 잠재적 위험 요소를 파악하고 사전에 위험을 분석하는 것이 가능하고 아웃소싱된 구성요소의 정보를 검증하여 도입할 수 있다.

SBOM은 소프트웨어 적용(Operate)은 새로운 취약점을 신속하게 파악하고 처리할 수 있으며, 특정 소프트웨어가 영향을 받는지를 평가하고 해당 위치를 손쉽게 파악할 수 있다. 비용, 라이센스 위험, 규정 준수 위험의 요소를 고려하여 효율적으로 소프트웨어를 운영할 수 있도록 한다. <표 6>을 통해 SBOM 적용 시에 발생할 수 있는 이점을 명시하였다.

표 6. 소프트웨어 관점에서의 SBOM 적용 시 효과성

효과성	생산(Produce)	선택(Choose)	적용(Operate)
비용	적은 계획성 및 예측되지 않은 작업	보다 정확한 소요비용 파악가능	관리 효율성 증진
보안 리스크	예측된 취약점 방지	간편한 심사	빠른 식별 및 해결, 특정 소프트웨어의 문제지점 파악 가능

라이센스 리스크	라이센스와 관련된 위험을 정량화하고 관리할 수 있음	간편한 심사	라이센스 요구에 대한 효과적인 정확한 응답 가능
컴플라이언스 리스크	위험 평가의 간편화, 라이프사이클 초기에 규정 요구사항 식별 가능	정확한 심사 및 라이프사이클 초기에 문제 파악 가능	간소화 과정
고 보증	사용된 아티팩트, 소스, 프로세스에 대한 Assertion 생성 가능	구성요소에 대한 정보를 바탕으로 공격에 저항력 생성	변화하고 적대적인 조건 하에 검증

SBOM의 효과성을 통해 소프트웨어 공급망 내 제조소, 사용자 등 다양한 이해관계자가 존재함으로 의사소통 및 운용에 일관성 있는 정보의 제공이 가능할 것으로 보인다.

3.3. 국외 SBOM 적용 및 정책 추진 동향

소프트웨어 자재명세서는 무결성 및 투명성을 입증할 수 있는 도구로, 공급망 보안 관리 방안으로 효과적으로 할 수 있다. SBOM의 효과성은 구성요소 식별을 통한 인지와 가시성 제고이고, 여러 데이터의 상관관계 파악이 가능하여 지속적인 모니터링이 가능하다는 점이다.

국외 정책 사항으로 미국과 유럽을 주요 골자로 확인할 수 있으며, SBOM을 소프트웨어 라이프사이클에 맞춰 적용하고 취약점을 식별하고 보안 계획 수립에 반영하는 것을 강조하였다.

의료기기 분야에서의 SBOM 적용 사례는 미국 FDA의 “의료기기 사이버보안법(Ensuring Cybersecurity of Devices, Section 524B(a) of the FD&C Act)”에 따른 SBOM의 작성 의무화이다. SBOM은 의료기기 소프트웨어 컴포넌트의 수명종료를 추적하여 대비할 수 있게 하는 등의 이해관계자들에게 향상된 투명성을 제공해 줄 수 있으며 규제기관에게는 SBOM이 제조업체의 사이버보안 역량을 평가하는 지표로 사용할 수 있다. ‘23년 10월에 새로운 “사이버 장치” RTA 지침을 발표했고, 해당 지침에 따르면 의료기기 제조업체(MDM)는 자신의 장치를 구축하는 데 사용한 모든 소프트웨어 컴포넌트에 대한 문서화(SBOM)를 가져야 한다.[19]

FDA SBOM 의무 사항에 따른 내용은 행정명령(EO 14028)으로 비롯되었으며, 소프트웨어 공급망 보안 강화를 공표함에 따라 고려되었다.

NTIA의 “The Minimum Elements For a Software Bill of Materials(SBOM)” 보고서에 따르면 최소 구성요소로 ‘데이터 필드, 자동화 지원, 관행 및 절차’를 제시하였고 정의는 아래와 같다.[20]

- 데이터 필드: 추적 대상 구성요소에 대한 기초 정보(공급자, 구성요소 이름, 구성요소 버전, 기타 고유식별자, 종속 관계, SBOM 데이터 작성자, 타임스탬프)를 기록해야 함.
- 자동화 지원: 자동 생성 및 기계 가독성을 이용하여 자동화를 실현하고 소프트웨어 생태계 전반으로 확대 가능함. SBOM 작성 및 사용 데이터 형식으로 SPDX, CycloneDX, SWID 태그를 활용할 수 있음.
- 관행 및 절차: SBOM 요청, 생성 및 운영 활동은 빈도, 깊이, 배포 및 제공, 접근 제어, 인지된 불확실성 정보, 오류 조정을 포함함.

유럽(EU)은 미국에 이어 유럽 시장에 납품되는 디지털 기기에 SBOM(소프트웨어 자재명세서) 작성을 의무화하는 등 사이버보안을 강화하고 있다.

EU의 사이버복원력법(Cyber Resilience Ac, CRA)은 제조업체에 설계부터 생산 단계까지 외부 인터페이스를 포함한 침범 면적 제한, 악용 완화 메커니즘·기술을 활용, SBOM 등 구성요소 문서화, 자동 보안 개선 등을 필수사항으로 제시한다.

사업자에 대해서도 필수 사이버보안 요건 준수, 제품의 사이버보안 위험분석 및 위험 경감, 적합성 평가 수행, 사고 보고, 기술문서의 보관 등의 의무를 부여하였고 수입사와 유통사에 대해서도 적합성 인증마크의 유무를 필히 검증하게 하고 있다.

미국 및 유럽 외에도 네덜란드 국립사이버안보센터(National Cyber Security Centre, NCSC)도 사이버보안 측면에서 SBOM 사용 현황을 수집하였고 “Using the Software Bill of Materials for Enhancing Cybersecurity”를 발간했다. 소프트웨어 제작, 선정 및 구매, 관리, SecDevOps 관점에서 SBOM의 보안 가치를 제공하고 취약점 탐지를 위한 방안을 소개한다.[21] 해당 보고서는 아래와 같은 요소를 핵심 사항으로 선정했다.

- SBOM의 온·오프라인 접근성
- 사용 목적에 맞는 SBOM 정보 제공

- 보안 평가에 필요한 SBOM 정보 구성요소
- 기본 SBOM 데이터 형식으로 CycloneDX 사용
- 보안 식별력 증대을 위한 자동화 및 도구 활용

이와 같이, 사이버 보안을 위한 국제적 흐름이 있으며 SBOM의 필요성을 인지하고 소프트웨어 위협 방지의 측면에서의 SBOM 규제 제안을 적용하는 과정에 있다.

3.4. 의료기기 제조소 SBOM 작성 및 관리방법

3.4.1. SBOM 콘텐츠 수집

SBOM 콘텐츠는 소프트웨어 설계 단계부터 수집 및 관리가 시작된다. SBOM 콘텐츠는 상용 소프트웨어 공급업체에서 제공하는 타사 SBOM 문서, 오픈소스 소프트웨어 공급기관/업체/개발자가 함께 제공하는 각종 문서, 소프트웨어 콘텐츠 분석 도구에서 자동으로 생성된 출력물, 제조사에서 개발 중 활용한 각종 자료와 같은 다양한 출처에서 얻을 수 있다.

해당 SBOM 콘텐츠는 설계-개발-빌드-테스트 과정 중 수집되며, 제조사가 관리하는 소프트웨어 구성요소 저장소에서 유지 관리 될 수 있다. 제조사의 소프트웨어 구성요소 저장소는 수동으로 작성한 문서부터 자동화된 툴까지 다양한 도구들이 있으나, 특정 도구 사용을 고집할 필요는 없다.

현재는 SBOM 콘텐츠 관리를 위해 국제적으로 널리 사용되는 표준화된 도구는 없으므로 제조사의 판단에 따라 도구를 선택할 수 있으며, 도구에 따른 장단점은 아래 <표 7>와 같다.

표 7. SBOM 생성 방법의 장·단점

배포방법	장점	단점
제조업체에서 보안 문서 제공	· SBOM 작성을 위한 별도 도구 필요없음	· 자동화되어 있지 않음 · 문서 업데이트 시 재배포 이슈 발생 · 제공하는 문서와 기기의 동기화 이슈 발생 · SBOM 접근 통제 어려움 (무단 확인가능)
제조업체에서 별도의 (전자)보안 문서 제공	· SBOM작성을 위한 별도 도구 필요 없음 · 기계가 판독 가능 · SBOM 접근을 일부 통제할 수 있음	· 자동화되어 있지 않음 · 문서 업데이트시 재배포 이슈 발생 · 제공하는 문서와 기기의 동기화 이슈 발생
디스플레이, 참조링크 또는 다운로드를 통해 의료기기에서 접근하도록 허용	· 항상 적합한 버전 공유 가능 · 사용자가 별도로 문서 관리하지 않아도 확인 가능 · SBOM 접근을 통제할 수 있음	· 자동화되어 있지 않음 · SBOM확인을 위해서 기기 접근이 선행되어야 함 · SBOM 추출 시 외부 포트 사용 이슈 발생 · SBOM 관리를 위해 저장 공간 사용 · SBOM 기능 사용을 위해 배터리 추가 소모 가능 (배터리로 작동하는 기기)

의료기기 API에서 접근 허용	· SBOM 접근을 통제할 수 있음 · 자동화 된 처리 가능	· API에 대한 표준이 정의되어 있지 않음
제조업체 관리 저장소 공유	· SBOM 접근을 통제할 수 있음 · 자동화된 처리 가능	· 고객이 보유하고 있는 기기들에 대한 정보 획득을 위해 여러 제조업체 저장소를 확인해야 함
중앙 저장소 공유	· 고객이 한번에 보유하고 있는 기기들에 대한 SBOM에 대한 검토 가능 · 자동화된 처리 가능	· 타사 서비스 사용 시 법적 이슈 (저작권, 책임, 기타 고려사항) 발생 · 일부 고객의 경우 같은 기기의 여러 버전을 보유할 수 있어, 추가적인 버전 관리 어려움 발생

3.4.2. SBOM 자료 생성 및 작성

제조사는 SBOM 생성 시에 소프트웨어 공급망에 대해 고려해야 한다. 의료기기에 사용된 소프트웨어에 사용된 소프트웨어 구성요소를 메이저, 마이너, 패치 버전별로 유지 관리하고 배포할 수 있어야 한다.

특히, 제조사는 타사 소프트웨어 구성요소에 대한 SBOM을 제공받지 못한 경우에는 제조사가 사용한 소프트웨어의 첫 번째 깊이의 의존성을 가진 소프트웨어 구성요소에 대해서는 유지 관리를 실시해야 한다. 예로 인공지능 의료기기 개발 시에 많은 업체들은 python 언어

기반의 다양한 패키지를 사용하게 된다. 그중 인공지능을 위해서는 필수적으로 'Tensorflow package'(또는 Pytorch package)를 사용하게 되지만, 별도로 SBOM을 제공하지 않아 Tensorflow외에는 SBOM의 컨텐츠를 관리하지 않을 수 있다.

오픈소스 소프트웨어는 상호 의존성이 매우 크므로 모든 의존된 package에 대해서 관리하는 것이 사이버보안 투명성을 크게 높일 수 있는 방법이나 제조사가 SBOM 작성에 너무 많은 시간을 소요하게 된다.

이에 제조사는 모든 의존 package를 관리하는 것이 아닌 첫 번째 깊이까지의 의존된 package를 유지·관리하여 관리의 효율과 사이버보안의 투명성을 높이는 활동을 적절한 지점을 찾아야 할 것이다.

위 내용의 연장선으로, 제조사는 Numpy, Pandas, Scipy package 등 Tensorflow가 참고하는 첫 번째 깊이까지의 패키지들을 SBOM의 콘텐츠로 정의하여 관리하도록 한다. 해당 근거자료 마련을 위해 SBOM 작성을 위한 절차를 소프트웨어 개발 계획서에 명시하고, python과 같은 보고서에 경우 requirement.txt와 같은 파일로 깊이1에 대한 SBOM의 근거자료를 작성하도록 한다.

(1) SBOM 구성요소 및 형식 비교

SBOM 작성을 위해서는 각 소프트웨어 구성요소를 구분할 수 있는 내용이 포함되어 있어야 한다. SBOM에 적용되는 항목은 많으면 많을수록 사이버보안 취약점 평가 및 투명한 공개 측면에서 좋을 수 있으나. 제조사의 관리 측면에서 비효율을 발생시킬 수 있다.

이에 NTIA, FDA, IMDRF에 요구하는 최소 사항에 대해서는 제조사의 필요에 따라 소프트웨어에 맞게 SBOM에 보충 정보를 추가할 수 있다. 예를 들어, 소프트웨어 컴포넌트 해시를 추가할 경우 재현성 측면에서 완성도를 높일 수 있어 취약점을 재현하고 분석하는 데 도움이 될 수 있다.

사용한 소프트웨어 컴포넌트의 지원종료(End of support)기간을 포함한다면 제조사의 소프트웨어 위험관리 측면에서 도움이 될 수 있다. 각 기관에 따른 SBOM 포함 최소 요구사항은 아래 <표 8>과 같다.

표 8. NTIA, FDA, IMDRF별 SBOM 포함 최소 요구사항

구분	내용
NTIA	· 공급자 이름(Supplier Name) : 구성요소를 만들고 정의하고 식별하는 주체의 이름 · 구성요소 이름(Component Name) : 최초 공급자에 의해 정의된 소프트웨어 단위의 명칭 · 구성요소 버전(Version of the Component) : 공급자가 이전에 식별된 소프트웨어 버전으로부터의 변경을 명시하기 위해 사용하는 식별자 · 기타 고유 식별자(Other Unique Identifiers) : 구성요소를 식별하는 데 사용되거나 관련 데이터베이스를 위한 조회 키 역할을 하는 기타 식별자. 예를 들어 NIST의 CPE 사전의 식별자일 수 있음 · 종속성 관계(Dependency Relationship) : 업스트림 구성요소 X가 소프트웨어 Y에 포함된다는 관계의 명시(오픈소스 프로젝트에서 특히 중요) · SBOM 데이터 작성자(Author of SBOM Data) : 이 구성요소에 대한 SBOM 데이터를 만든 주체의 이름 · 타임스탬프(Timestamp) : SBOM 데이터 어셈블리의 날짜 및 시간 기록
FDA	· 소프트웨어 컴포넌트가 있는 자산(assets) · 소프트웨어 컴포넌트 이름(component name) · 소프트웨어 컴포넌트 버전(component version) · 소프트웨어 구성 요소 제조업체(component manufacturer)

	· 소프트웨어 구성 요소 제조업체에서 모니터링 및 유지 관리를 통해 제공하는 소프트웨어 지원 수준(level of support)
	· 소프트웨어 구성 요소의 지원 종료 날짜(end-of-support date)
	· 알려진 취약점(any known vulnerabilities)
IMDRF	· 작성자 이름(Author name): SBOM 파일을 생성한 법인으로 개인, 조직 또는 이와 유사한 단체 포함하여 나타냄
	· 타임스탬프(Timestamp): 타임스탬프: SBOM 데이터 어셈블리의 날짜 및 시간 기록
	· 소프트웨어 컴포넌트 공급업체(Software component vendor or supplier): 컴포넌트를 생성, 정의, 식별하는 주체를 말하며, 소프트웨어 컴포넌트 공급업체 이름은 일반적으로 상용소프트웨어의 법적 비즈니스 이름을 참조해야 함
	· 소프트웨어 구성요소 이름(Software component name): 원래 공급업체가 정의한 소프트웨어 단위에 할당된 명칭임
	· 소프트웨어 구성요소 버전(Software component version): 공급업체가 이전에 식별된 버전에서 소프트웨어의 변경 사항을 지정하는 데 사용하는 식별자
	· 고유 식별자(Unique identifier): 구성요소를 식별하거나 관련 데이터베이스의 조회 키로 사용되는 식별자
	· 관계(Relation): 업스트림 컴포넌트 X가 소프트웨어 Y에 포함되는 관계 설명

3.4.3. SBOM 배포

제조사는 SBOM에 대해서 인식 제고, 접근 권한 제공, 업데이트 푸시 등 최선의 방법을 고려하여 의료서비스 제공자에게 공유해야 한다. 전달 형식은 전자파일 또는 제조사의 웹사이트의 API(어플리케이션 프로그래밍 인터페이스) 등의 형식으로 전달할 수 있다.

SBOM 전달 방법에 대해서는 유일한 방법은 없으나, IMDRF는 표준화된 자동 검색 및 교환 메커니즘을 사용하는 것을 권유하고 있다.

일반적으로 소프트웨어 개발 시 오픈소스 소프트웨어를 사용한 경우에는 참조한 오픈소스의 라이선스 규약에 따라 사용 정보를 소프트웨어에서 알리도록 명시화하고 있다.

오픈소스 소프트웨어 기반의 의료기기 규제에 맞춰 사용한 오픈소스 리스트를 공개해야 하는데, 공개내용에 SBOM의 구성요소를 포함으로써 사이버보안의 정보 공유의 투명성을 높일 수 있다. 다만, 의료기기의 경우 변경에 따른 환자의 안전이 중요하므로, 배포하는 버전마다 SBOM이 관리되어야 할 것이다.

의료기기가 존재하는 곳이면 해당 의료기기를 통해 SBOM 역시 엑세스가 가능해야 하므로 제조사는 몇 가지 방법으로 SBOM을 알릴 수 있다.

매뉴얼, 소프트웨어 의료기기의 도움말 또는 특정 메뉴를 통해 접근 확인하고 의료기기에 포함 시켜 배포하는 방법, SBOM 리스트 등 문서 직접 제공, 제조사에서 SBOM을 정리한 웹사이트 링크 제공, 제조사에서 로컬/중앙 방식으로 관리하는 저장소에 접근 권한 제공 등 링크 및 저장소 권한 허용이 있다.

SBOM의 정보는 의료기기의 사이버보안 향상을 위해 사용되지만, SBOM또한 의료기기에 포함된 민감한 정보로써 위변조와 같은 위험에 노출될 가능성이 있다. 사이버보안의 기본 원칙과 동일하게 제조사, 의료 서비스제공자에 이르기까지 기밀성, 무결성이 확보될 수 있도록 철저하게 관리 해야 한다.

3.4.4. SBOM 유지보수(재생성)

SBOM는 소프트웨어 구성요소에 취약점 여부가 명시되어 있지 않지만, 다른 리소스와 함께 의료기기 취약성을 모니터링하는 데 사용할 수 있는 유효성 있는 방법이다. 제조사는 의료서비스 제공자에게 취약성 정보를 알리도록 최선을 다해야 하는데, 방법 중 하나로 취약성 익스플로잇 가능성 거래소를 이용하는 것이다.

의료기기 사이버보안 위협 및 취약점이 발견되는 경우 제조사는 다음의 조치를 이행하고 새로운 SBOM을 생성하여 배포해야 한다. 새로운 SBOM 생성을 위한 최소 조건은 아래와 같으며 반드시 이에 국한되지는 않는다.

- 업그레이드, 업데이트 또는 패치를 통해 취약점 해결 시
- 의료기기 소프트웨어에 새로운 기능 추가 시
- 같은 기능을 하지만 소프트웨어의 구성요소가 변경된 경우
- 소프트웨어 구성요소 추가 또는 삭제 발생 시
- 수명 종료(end of life), 지원 종료(end of support) 또는 구성요소 및 하드웨어, 운영체제가 바뀐 새 버전 출시 시

새로운 SBOM 생성은 제조사의 코드가 바뀌지 않았더라도 참고하는 소프트웨어, 패키지 및 라이브러리의 변경이 발생 된 상태에서 빌드를 수행하며 배포 발생 시에도 수행되어야 한다. 이러한 변경은 정기적으로 의료서비스제공자에게 전달됨으로써 총 제품 수명전주기 동안의 양측간 신뢰를 향상시킬 수 있다.

3.5. SBOM 작성 시 고려사항

SBOM 개념은 최근 도입되었으며, 현재도 지속적으로 발전되어가고 있는 개념 중 하나이다. 시판이 완료된 구형 의료기기에 대해서 SBOM을 확보하는 것은 어려울 수 있다.

제조사는 자동화 컨텐츠 분석 도구를 통해 분석 결과를 활용하여 구형 기기에 대한 SBOM을 구축할 수 있으나 호환이 원활히 되지않는 경우에는 직접 SBOM을 작성해야 할 수 있다. 이런 경우에는 가능하면 범위와 깊이를 줄인 최소한의 SBOM을 만들고 점진적으로 컨텐츠를 확장함으로써 사이버보안의 투명성을 높이는 것이 필요하다.

SBOM 수집, 생성, 배포 및 사용을 위해 표준 및 도구들을 사용할 수 있다. 표준과 도구는 계속하여 발달하는 단계에 있지만, 제조사는 변화하는 상황에 맞추어 표준과 도구를 선정하여 보안문서 형태의 SBOM을 구축해야 할 것이다.

제조사는 SBOM 생성 시 개발하는 소프트웨어 기준으로 참조하는 오픈소스 소프트웨어의 깊이를 설정해야 한다. 운영체제와 같이 비용을 지출하는 소프트웨어는 제공사에서 제시한 수명종료가 있어 깊이를 설정할 필요가 없으나, 오픈소스 소프트웨어의 경우에는 깊이 설정에 어려움이 있다.

SBOM의 깊이가 깊어지면 의료서비스제공자에게 고가치와 투명성을 제공하지만, 제조사는 명세서 구축과 작성에 복잡성과 어려움을 안게 된다.
제조사는 개발하면서 필요한 오픈소스 소프트웨어를 정리하게 되는데, 개발에 사용한 오픈소스와 오픈소스가 첫 번째 참조하는 깊이에 대해 관리하여야 하며 해당하는 다른 소프트웨어 구성요소들에 대해 재현성에 크게 영향을 미친다.

SBOM을 배포하는 빈도를 늘릴 경우, 제조사는 의료기기 사이버보안에 대한 높은 품질과 투명성을 확보할 수 있지만 제조사의 관리 어려움을 발생시키므로 적절한

배포 시점에 대해서 GMP에 소프트웨어 개발 계획서에 이를 명시하고 보고서에 배포한 이력을 남겨야 할 것이다.

3.6. SBOM 데이터 형식

SBOM은 표준화된 형식이 따로 존재하지 않으며, 일반적으로 사용되고 있는 SBOM 데이터 형식은 SPDX, SWID, CycloneDX가 있다.

리눅스 사가 개발한 SPDX(Software Package Data Exchange)는 오픈소스 및 라이센스 정보교환의 산업 표준이다. 릴리스의 이름, 버전, 구성요소, 저작권 등으로 구성되어 있어 SBOM의 요소와 일맥상통한다.

SPDX는 중복 작업을 줄이고 배포 및 컴플라이언스를 간소화하는 공통형식이며 ISO/IEC 5692:2021를 기반으로 한 국제 오픈 표준이다.

SPDX 라이선스 목록은 SPDX 명세의 중요한 부분이다. 오픈소스 또는 협업 소프트웨어, 데이터, 하드웨어, 문서에서 흔히 발견되는 라이선스와그 밖의 목록이며, 표준화된 짧은 식별자, 전체 이름, 라이선스 텍스트, 각 라이선스와 예외에 대한 공식적인 영구 URL이 포함되어 있다.

SWID(Software Identity)는 ISO/IEC19770-2 표준에 의해 정의되었고, 소프트웨어 정보에 대한 태그를 생성하여 오픈소스 소프트웨어의 인벤토리를 지원하는 장치이다.

SWID 태그 파일은 특정 소프트웨어 제품의 릴리스에 대한 설명 정보를 포함하며 SWID 태그 문서는 다음과 같은 데이터 요소로 구성된다.

- 소프트웨어 제품 식별
- 제품 버전 특성화
- 제품 생산 및 배포에 관련된 조직과 개인 식별
- 소프트웨어 제품을 구성하는 아티팩트 나열
- 소프트웨어 제품 간의 관계 설정
- 기타 설명 메타데이터 제공

이 같은 태그 정보는 SBOM 데이터로 활용할 수 있으며, 타 SWID 태크에 링크하여 사용가능해 소프트웨어의 종속 관계를 나타낼 수 있다. 현재는 용량 크기가 큰 XML 형식으로 제공되며, 앞으로 CBOR(Concise Binary Object Representation)을 바탕으로 경량화된 CoSWID의 사용도 가능할 것으로 보인다.[22)]

CycloneDX는 애플리케이션 보안 및 공급망 구성요소 분석에 활용되도록 설계된 경량 SBOM 표준이다.[23)] 소프트웨어 보안 요구사항과 위험 분석을 위해 설계되었고 JSON, XML 언어로 작성할 수 있다. 제공업체의 정보, 라이센스, 구성요소 종속성 등 자재명세서에 대한 데이터를 제공한다. <표 9>는 NTIA에서 제시한 각각의 데이터 형식에 대한 비교이다.

표 9. 기존 형식에 기반한 SBOM 기본 구성요소 정보의 매핑 방법(NTIA)

속성	SPDX	SWID	CycloneDX
작성자명	(2.8) Creator:	<Entity> @role (tagCreator), @name	metadata/authors /author
타임스탬프	(2.9) Created:	<Meta>	metadata /timestamp
공급업체명	(3.5) PackageSupplier:	<Entity> @role (softwareCreator /publisher), @name	Supplier publisher
구성요소명	(3.1) PackageName	<softwareIdentity> @name	name
버전 스트링	(3.3) PackageVersion:	<softwareIdentity> @version	version
구성요소 해시	(3.10) PackageChecksum: (3.9) PackageVerification Code:	<Payload>/../<File> @[hash-algorithm]: hash	Hash “alg”
고유 식별자	(2,5) SPDX Document Namespace (3.2) SPDXID:	<softwareIdentity> @tagID	bom/serialNumber component/bom-ref
관계성	(7.1) Relationship: DESCRIBES CONTAINS	<Link> @rel, @href	(Inherent in nested assembly/ subassembly and/or dependency graphs)

4. 결과

4.1. SBOM 데이터 반영 요소

보안 문서로 제공하는 SBOM의 경우, Word, Excel, 한글 등 다양한 문서 작성 프로그램을 사용할 수 있으며 표준 및 도구가 존재하지 않는다.

다만 작성 시 향후 개발되는 기기 및 품목의 확장을 고려하여 SBOM Migration 이슈에 쉽게 대응할 수 있도록 자동으로 parsing 할 수 있는 문서 형태로 작성하는 것을 권고한다. 기본 구조는 <표 5>의 내용을 반영하였다.

4.2. 적용 소프트웨어별 SBOM 작성예시 제안

NTIA, FDA, IMDRF에서는 각각 SBOM의 최소한의 구성요소를 제안하였으나, 제조사에서는 구성요소 선정 및 작성에 어려움이 있다. 이에, 최근 수요가 많은 인공지능 소프트웨어 의료기기에 대해 작성예시를 들어 소프트웨어 자재명세서 작성 및 평가에 도움이 되고자 한다.

본문 3. 소프트웨어 자재명세서(SBOM)에서 언급한 SBOM 데이터 형식별 적용 예시는 <표 9>를 참고하여 코드를 작성하였으며, 아래와 그림과 같다.

예시는 SPDX, SWID, CycloneDX 버전으로 구성하였고 소프트웨어 개발자, 해쉬값 등 최소 요소를 포함하였다.

```
SPDXVersion: SPDX-2.2
DataLicense: CC0-1.0
SPDXID: SPDXRef-DOCUMENT
DocumentName: SYInnovate
DocumentNamespace: http://spdx.org/spdxdocs/SYInnovate-1.0
Creator: Tool: (주)SYI
Created: 2023-04-05T00:00:00Z

PackageName: SYInnovate
PackageVersion: 1.0
PackageSupplier: Organization: (주)SYI
PackageDownloadLocation: http://SYI.com/SYInnovate
FilesAnalyzed: false
PackageChecksum: SHA256: 6dcd4ce23d88e2ee95838f7b014b628e2e7e58b8b9e4b2fb1fdd3518aaf9f8e6
PackageVerificationCode:
 6dcd4ce23d88e2ee95838f7b014b628e2e7e58b8b9e4b2fb1fdd3518aaf9f8e6 (excludes: SPDXRef-DOCUMENT)
```

그림 4. SBOM SPDX 버전 예시

```
<?xml version="1.0" encoding="UTF-8"?>
<bom xmlns="http://cyclonedx.org/schema/bom/1.3" version="1">
  <components>
    <component type="library" bom-ref="pkg:maven/org.example/SYInnovate@1.0">
      <name>SYInnovate</name>
      <version>1.0</version>
      <publisher>(주)SYI</publisher>
      <hashes>
        <hash alg="SHA-
256">6dcd4ce23d88e2ee95838f7b014b628e2e7e58b8b9e4b2fb1fdd3518aaf9f8e6</hash>
      </hashes>
    </component>
  </components>
</bom>
```

그림 6. SBOM CycloneDX 버전 예시

```
<?xml version="1.0" encoding="UTF-8"?>
<SoftwareIdentity
    xmlns="http://standards.iso.org/iso/19770/-2/2015/schema.xsd"
    tagId="com.SYI.SYInnovate"
    name="SYInnovate"
    version="1.0"
    versionScheme="multipartnumeric"
    patch="false"
    media="false">
    <Entity
        name="(주)SYI"
        regid="com.SYI"
        role="softwareCreator tagCreator"/>
    <Link
        href="http://SYI.com/SYInnovate"
        rel="product"/>
    <Payload>
        <File
            name="/opt/SYI/SYInnovate/bin/example"
            size="182736"

hash="sha256:6dcd4ce23d88e2ee95838f7b014b628e2e7e58b8b9e4b2fb1fdd3518aaf9f8e6"/>
    </Payload>
</SoftwareIdentity>
```

그림 5. SBOM SWID 버전 예시

인공지능 소프트웨어 의료기기의 경우 운영체제를 기반으로 제조사에서 개발한 의료기기가 구동되게 된다. 제조사에서 개발한 의료기기 소프트웨어는 다른 소프트웨어 및 오픈소스 소프트웨어를 참고하여 개발하고 빌드되어 의료서비스 공급자에게 공급되게 된다.

(1)제조사에서 직접 개발한 SBOM 콘텐츠, (2)운영체제와 같은 상용 소프트웨어 SBOM 콘텐츠, (3)제조사가 개발에 사용한 오픈소스 소프트웨어 SBOM 콘텐츠와 같이 3가지 SBOM의 성격으로 나누어진다.

(1), (2), (3)을 한 SBOM 형식으로 담기에 호환되지 않는 부분이 있어 각 조건에 맞는 구성요소 및 작성예시를 제안하고자 한다. 제안한 예시는 수동으로 제공하는 보안문서 형태로 작성할 수 있도록 구성하였다. 각 형식별 예시는 <그림7, 8, 9>와 같다.

(1) 제조사에서 직접 개발한 SBOM(제조사 개발 Software를 기반으로 한 SBOM 예시)

ID	Supplier Name (공급업체 이름)	SW Name	Component Name (컴포넌트 이름)	Version of the Component (컴포넌트 버전)	Dependency Relationship	Author of SBOM Data	Timestamp
OP_0001_01	㈜SYI	SY Innovate	SYI-C Brain	0.9.1	OTS_OS_001, OPNSRC_0001, OPNSRC_0002	Son Yein	2024-02-01
OP_0001_02			SYI-C viewer	"			
OP_0001_03			SYI-C analysis	"			
OP_0001_04				"			
OP_0001_05				"			
OP_0002_01	㈜OOO		SYI-C Alzheimer's Predictor	0.1.0	OTS_OS_003	Son Yein	2022-03-01

그림 7. 제조사에서 직접 개발한 SBOM

SBOM 구성요소는 아래 내역을 포함하여 작성하였다.

- ID: 제조사에서 작성한 컴포넌트들에 대해서 ID를 부여한다.
- Supplier Name: 공급업체 이름을 작성한다. 제조사와 제조의뢰자가 다를 경우 및 일부 모듈에 대해서 용역을 통해 공급받을 경우 제조사 외에 다른 업체가 추가될 수 있다.
- SW Name: 제조사에서 관리하는 SW 의료기기의 이름을 작성한다.
- Component Name: 제조사에서 관리하는 컴포넌트의 이름을 작성한다.
- Component Version: 제조사에서 관리하는 컴포넌트의 버전을 작성한다. 작은 프로젝트의 경우에는 버전이 동일할 수 있으나, 대규모 팀 프로젝트일 경우에는 컴포넌트별로 버전일 별도로 존재할 수 있다.
- Dependency Relationship: 의존성이 존재하는 다른 SBOM에서 부여한 ID를 기재한다.
- Author of SBOM Data : 컴포넌트의 개발자 또는 개발팀 이름을 작성한다
- Timestamp : 컴포넌트가 완료된 시점의 날짜 또는 unique한 tag를 부여할 수도 있다.

(2) 상용소프트웨어 SBOM(제조사에서 개발 시 적용한 상용소프트웨어에 대한 SBOM 예시)

ID	software component name (이름)	software component version (버전)	software component manufacture (제조업체)	software level of support (소프트웨어 지원수준)	component's end-of-support date (지원종료일)	any known vulnerabilities (알려진 모든 취약점)	Relationship
OTS_OS_001	ubuntu	18.04.05 LTS	Canonical Ltd	Tier 1	2024-06-31	Link1(vulnerabilities) : 링크	OP_0001
OTS_OS_002	RHEL	7.9	RedHat	Tier 4	-	Link1(vulnerabilities) : 링크	
OTS_OS_003	matlab	2020a	Mathworks	Tier 1	not declared	Link1(vulnerabilities) : 링크	OP_0002

그림 8. 상용 소프트웨어 SBOM

- ID: 제조사에서 적용한 소프트웨어들에 대해서 ID를 부여한다
- Software component name: 공급사에서 명시한 소프트웨어의 이름을 작성한다.
- Software component version: 공급사로부터 획득한 소프트웨어의 버전을 작성한다.
- Software component manufacture: 공급업체(개발업체)의 업체명을 작성한다.
- Software level of support: 공급사의 소프트웨어 지원 수준을 작성한다. 공급사와의 유지보수에 따라서 tier 값이 달라질 수 있다.
- Component's end-of-support date: 공급사에서 공식적으로 공시한 지원종료일을 작성한다. 공시가 되지 않은 경우는 공시되지 않음을 명시한다.
- Any known vulnerabilities: 제조사 또는 보안 자료를 통해 알려진 취약점 링크를 작성한다.
- Relationship : 제조사에서 개발한 소프트웨어 의료기기 컴포넌트와 관련 있는 기능들에 대해서 ID를 인용하여 작성한다.

(3) 오픈소스 소프트웨어 SBOM(제조사에서 개발시 적용한 오픈소스 소프트웨어에 대한 SBOM 예시)

ID	Author name	Timestamp	Software component vendor(supplier)	Software component name	Software component version	Unique Identifier	Relationship
OPNSRC_0001	Son Yein	2024-04-08	published by github(https://github.com/ANTsX/ANTs)	ANTs	v2.4.4	d74bb06	OP_0001
OPNSRC_0002	Son Yein	2023-07-20	published by official website(https://surfer.nmr.mgh.harvard.edu/fswiki/DownloadAndInstall)	freesurfer	v7.4.1		OP_0001

그림 9. 오픈소스 소프트웨어 SBOM

- ID: 제조사에서 적용한 소프트웨어들에 대해서 ID를 부여한다.
- Author name: 제조사에서 해당 오픈소스를 사용한 개발팀 및 개발자를 작성한다(관리목적).
- Timestamp: 해당 오픈소스를 참조한 날짜를 기재한다.
- Software component vender: 해당 오픈소스를 공급한 자에 대한 정보를 기록한다. 대부분의 오픈소스는 최근 github을 통해 공유되어 있으며, 이외에도 온라인 링크를 통해 공유되고 있다. 이에 다운로드한 링크를 기록한다.
- Software component name: 오픈소스 공급자가 명시한 컴포넌트의 이름을 작성한다.
- Software component version: 오픈소스 공급자가 명시한 컴포넌트의 버전을 작성한다.
- Unique Identfier : 오픈소스에 부여된 Tag를 기록한다. (Tag는 github에서 다운로드 버전 선택 시 확인할 수 있다.)
- Relationship: 제조사에서 개발한 소프트웨어 의료기기 컴포넌트와 관련 있는 기능들에 대해서 ID를 인용하여 작성한다.

5. 고찰 및 결론

정보통신기술의 발달로 유·무선 통신을 사용하는 의료기기 개발이 증가하고 있으며, 의료기기에서의 소프트웨어 활용이 증가함에 따라 인공지능과 같은 신기술이 접목되고 있다. 사이버보안 측면에서 오픈소스의 활용 등 구성요소를 파악하고 체계적으로 관리하여 보안 취약점을 신속하게 식별하고 대응할 수 있는 SBOM이 제안되었다.

미국 행정명령(EO 14028)를 토대로 FDA의 의료기기 소프트웨어의 SBOM 필수 제출 등 필요성을 강조하고 있다. 의료기기국제포럼 역시 SBOM에 대한 원칙과 관행을 제시하였으며, 국내 식품의약안전처도 '23년 11월 '의료기기 사이버보안 가이드라인' 3종을 발간했다.

의료기기 제조소는 기존 지침을 준수하여 의료기기 소프트웨어뿐만 아니라 하드웨어도 포함하는 사이버보안 자재명세서(Cybersecurity Bill Of Materials)를 제공해야 하나 새로운 지침에 따라 의료기기에 내장된 소프트웨어만 다루는 SBOM만 제출하면 된다. 기존 CBOM은 구성요소에 하드웨어 항목까지 포함되므로 범위와 복잡성이 크게 증가되었으며, 하드웨어의 보안 취약점을 파악하고 추적하는 것이 소프트웨어보다 까다롭게 적용될 수 있다.

소프트웨어 의료기기(SaMD) 제조소는 SBOM의 등장으로 작성 부담감을 줄일 수 있을 것으로 사료된다.

<그림 4~6>에서 제시한 것처럼, SBOM의 대표적인 데이터 형식(SPDX, SWID, CycloneDX)에 따라 IMDRF에서 최소 구성요소로 코드를 구성함을 통해 국내 의료기기 제조업체에서 SBOM 생성 시 발생할 수 있는 부담을 감소시킬 수 있을 것이다. 소프트웨어 의료기기 제조업체와 직면하고 있는 사이버보안 문제를 SBOM을 통해 사전/사후에 효과적으로 관리하고 보안 위험을 표적화하여 대응할 수 있다.

데이터 형식에 따른 코딩 외에도 수기로 작성하고 보관하여 GMP 등 인허가 문제에 대응할 수 있도록 SBOM 표준 양식을 <그림 7~9>를 통해 제안하였으며, 의료기기 제조사에서

직접 개발할 수 있는 SBOM 양식, 상용소프트웨어 SBOM, 오픈소스 소프트웨어에 적용할 수 있는 SBOM으로 구분하여 작성하였다.

사이버보안 문제는 소프트웨어의 발전과 꾸준히 업데이트되는 항목으로, 현재 제시하고 있는 최소한의 구성요소를 포함하고 발생할 수 있는 보안위협 상황이 발생할 때마다 귀속시킬 필요가 있다.

이외에도 제조소는 SBO,M 작성 시 제조소가 포함하여야 하는 필수 구성수준 외에도 제조소 입장에서의 기술 깊이를 설정하여야 한다. 본문에서 기술한 NTIA 등 정부 규제로 요구하는 정보 수준을 최소 요건 외에도 알려진 취약점 정보를 바탕으로 대비할 수 있는 장치를 포함하는 것을 제안한다.

기존에 정의된 양식이 따로 없었기에, 국내 의료기기 소프트웨어의 SBOM 표준 모델을 제시했다는 점을 의의를 둔다. 안정화된 의료기기 사이버 보완 환경 및 국내 의료기기 제소업체의 국외 인허가 경쟁력 강화를 위해 국가적 표준모델 제안과 관련 학계·민간의 협력이 요구되는 바이다.

국제적인 동향과 소프트웨어 발전에 따른 보안위협의 증가로 SBOM이 더 많이 적용될 것으로 보이며, SBOM이 제공하는 구성요소의 가시성을 기반으로 제품의 품질 판단 지표로 활용될 것임을 전망한다.

본 연구를 통하여 향후 의료기기 소프트웨어의 국내 SBOM 확립을 위한 가이드라인 및 정책 수립에 본 연구 결과가 기초 연구자료로 사용될 수 있기를 기대한다.

참고 문헌

1. MarketsandMarket, Artificial Intelligence in Healthcare Market, 2020
2. Executive Office of the President of U.S.,Improving of Nation's Cybersecurity, 2021(Executive Order 14028 of May 12)
3. Security affais, MAJOR DUESSELDORF HOSPITAL INFECTED WITH RANSOMWARE, PATIENT DIED FOR CONSEQUENCES, 2020
4. BBC, Colonial hack: How did cyber-attackers shut off pipeline?, 2021, https://www.bbc.com/news/technology-57063636
5. 손효현, 김동희, 김소정, 2022, 사이버안보 강화를 위한 소프트웨어 공급망 보안 정책 연구: SBOM 정책 추진 사례를 중심으로. 디지털융복합연구, 20(2), 9-20
6. 식품의약품안전처, 의료기기 사이버보안 원칙 실무, 2023
7. 식품의약품안전처, 의료기기 사이버보안 허가·심사 가이드라인(민원인 안내서), 2023
8. IMDRF/CYBER WG/N73, Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity, 2023
9. 식품의약품안전처, 의료기기 제조 및 품질관리 기준(식약처 고시)
10. 식품의약품안전처, 의료기기 위험관리 가이드라인, 2017
11. 식품의약품안전처, 의료기기 사이버보안을 위한 소프트웨어 자재명세서 원칙 및 실무, 2023
12. 식품의약품안전처, 의료기기의 사이버보안 허가·심사 가이드라인(민원인 안내서), 2022
13. IMDRF/CYBER WG/N60, Principles and Practices for Medical Device Cybersecurity, 2020
14. Cynerio, The State of Healthcare IoT Device Security 2022, 2022
15 IoT보안얼라이언스, 의료 분야 ICT 융합 제품·서비스의 보안 내재화를 위한 스마트 의료사이버보안 가이드, 2018
16. IMDRF/CYBER WG/N73, Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity, 2023
17. 최성호, 곽진, 2015, 국외 의료기기 보안위협 사례 및 보안 동향 조사, 정보보호학회지 제25권 제3호
18. National Telecommunications and Information Administration(NTIA), Framing

Software .Common Software Bill of Materials(SBOM)-SecondEdition. Washington D.C. : NTIA., 2021

19. Food and Drug Administration, The Premarket Cybersecurity Guidance: Section 524B of the FD&C Act., 2024
20. NTIA, The Minimum Elements For a Software Bill of Materials(SBOM), 2021
21. B. Riel, S. Kuijpers & R. Koning., Using the Software Bill of Materials for Enhancing Cybersecurity. National Cyber Security Centre(NCSC), 2021
22. The Linux Foundation Projects, The Software Package Data Exchange. SPDX., https://spdx/dev, 2010
23. ISO/IEC 19770-2 Information technology-IT asset management-Part2: Software identification tag. ISO, 2015

ABSTRACT

Proposing a Standard Model for the Application of SBOM in Cybersecurity Evaluation of Medical Device Software

Through this research, in alignment with international trends in Software Bill of Materials (SBOM), recommendations will be made for the establishment of SBOM in terms of software quality management and cybersecurity for domestic medical devices.

The proliferation of digital healthcare has led to an escalation in security threats, rendering the management of security in medical device software imperative. With the expanding utilization of open-source platforms in the development of medical device software, manufacturers are increasingly susceptible to inadvertent cybersecurity vulnerabilities. In response to this challenge, the necessity for SBOM (Software Bill Of Materials) has been advocated to ensure transparency within the software supply chain. SBOM furnishes essential information required to manage and counter security threats within the software supply chain, encompassing a comprehensive enumeration of all components integrated into a software product.

International trends indicate that integrating SBOM can enhance effective risk management, serving as a foundational asset to augment cybersecurity risk management protocols across the lifecycle of a medical device product.

Given the scarcity of domestic precedents beyond the medical device realm and the absence of a government-defined framework, this study will present policy trends at the medical device software SBOM level. It will explore the applicability scope by accounting for the idiosyncrasies of medical device software.

Drawing upon domestic and foreign medical device cybersecurity regulations, IMDRF guidelines, and an analysis of SBOM policies in major foreign nations, this study has identified SBOM elements and recommendations adaptable to the domestic medical device sector. These recommendations aim to streamline the creation process for manufacturers and implementers, thereby enhancing operational efficiency and maintenance efficacy.

Keywords: Medical Software, SBOM, Software Cybersecurity