MPIS 2024
(제11회 2024 의료기관 정보보호 컨퍼런스)

의료기기 SBOM 동향

2024년 05월 21일

방지호 박사

스마트의료보안포럼 의료기기보안분과장

(KTC 디지털·정보보안사업단장, jhbang@ktc.re.kr)

목차

1. "SBOM" 이란?

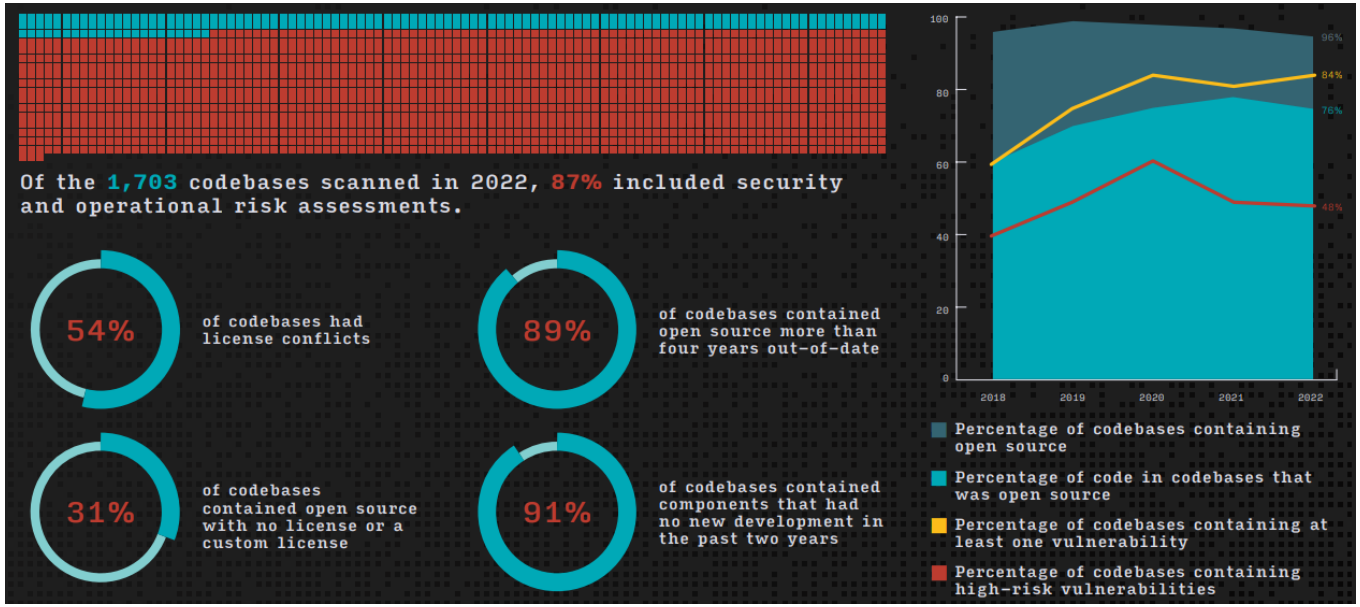
2. 국내외 의료기기 SBOM 활용 및 규제 동향

3. 의료기기 SBOM 도입

(출처) 5 Questions About SBOMs for Healthcare Organizations, HealthTech, 2023.07.10.,
https://healthtechmagazine.net/article/2023/07/5-questions-about-sboms-healthcare-organizations

1. "SBOM" 이란?

1. 공개 소프트웨어의 위험성



(출처) Synopsys, 2023 Open Source Security and Risk Analysis Report

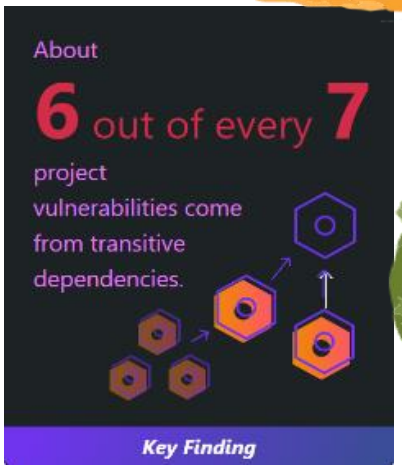
- 2022년에 스캔된 1,703개의 코드베이스* 중 87%가 보안 및 운영 위험 평가를 포함함
  - 코드베이스 54% 에 라이센스 충돌 발생
  - 코드베이스 31% 가 라이센스 또는 사용자 지정 라이센스가 없는 오픈 소스를 포함함
  - 코드베이스 89% 가 out-of-date가 4년 이상 지난 오픈 소스를 포함하고 있음
  - 코드베이스 91% 는 지난 2년 동안 새로운 개발이 없었던 구성 요소를 포함하고 있음

* 특정 소프트웨어 시스템, 응용 소프트웨어, 소프트웨어 구성요소를 빌드하기 위해 사용되는 소스 코드의 모임

1. 공개 소프트웨어의 위험성

12억 개의 취약한 오프소스 소프트웨어가
매달 다운로드 됨

2019년 이후 소프트웨어 공급망 공격은
지난 3년 동안 연평균 742% 증가



프로젝트 취약점 7개 중 6개는 (85%)
전이 종속성에서 발생

※ 출처 :sonatype, https://www.sonatype.com/resources/2023-software-supply-chain-report

2. "SBOM" 이란?

SBOM 정의

- **SW를 이루는 구성요소의 세부 정보와 의존관계**에 대한 정형화된 기술(description)을 의미함
  - SW 빌드에 사용된 다양한 구성요소의 상세 정보와 공급망 관계를 포함한 형식적인 기록 - 美행정명령 EO14028 Sec.10.(j)
  - SW구성요소 정보와 계층적 의존관계를 형식적이고 기계가독적인 형태로 기술한 목록 – NTIA
  - SW 구축에 사용되는 다양한 구성요소의 세부사항 및 공급망 관계를 포함하는 공식 기록으로, SW 개발자와 공급업체는 종종 기존 오픈소스와 상용SW 구성요소를 조합하여 제품을 만들며, SBOM은 제품에서 이러한 구성요소를 열거함 - NIST
  - 한 개 이상 식별된 컴포넌트 목록과 다른 관련된 정보 – IMDRF
  - SW를 구성하는 부분을 설명하는 전자문서 또는 기계가독적 파일 - 네덜란드 국가사이버보안 센터

SBOM 최소요소 (NTIA)

- 데이터 필드 : 필수적으로 추적해야 할 각 구성요소의 기준 정보 문서화 – **구성요소의 공급자 · 이름 · 버전 · 식별자 · 의존관계, SBOM 작성자 · 작성일시**
- 자동화 지원 : SW생태계 상에서의 적용을 위한 자동 생성 · 기계가독성 등을 포함한 자동화 지원, SBOM 생성 · 소비를 위한 데이터 포맷으로는 SPDX, CycloneDX, SWID tags 포함
- 지침 및 절차 : SBOM 요청 · 생성 · 사용에 대한 운영 정의 - 생성 빈도수, SW구성요소 분석 깊이, 알려진 언노운(Known Unknowns), 배포 및 전달, 접근 제어, 오류에 대한 양해

(출처) '미국 SBOM 정책 분석 및 시사점(Issue Report IS-144, SPRI, 2022.12.16.)' 내용에 추가

3. SBOM 표준

SBOM 포맷 표준

- SPDX : 리눅스재단의 오픈소스 프로젝트 기반으로, SBOM 정보를 주고 받기 위한 공개 표준(2021년, ISO/IEC 5962). 라이선스 관리를 주요 목적으로 설정해 라이선스명에 대한 모호함 제거를 위해 별도 명칭 목록을 관리함
  * 라이선스에 대한 모호함 해소를 위해 별도의 목록(SPDX License list)을 관리하고 지적재산권 및 라이선스 관련 정보 기술을 위한 항목을 풍부하게 제공
- SWID : 미국 상무부 지원 프로젝트 기반으로, SW제품을 설명하는 구조화된 메타데이터 포맷 표준(2012년, ISO/IEC 19770-2)으로, SW 자산/보안 관리에 활용이 권고됨
  * SW제품의 설치·패치·설정·삭제 등에서의 SW식별 정보 관리 기능 제공
- CycloIneDX : OWASP에서 표준 개발을 위해 추진한 프로젝트로, 앱 보안과 공급망 구성요소 분석을 위한 경량 SBOM 표준임. SBOM 뿐만 아니라 서비스, 운영, 취약점 등에 대한 정보 교환 및 공급망 관리 측면에서의 활용을 위한 확장성 제공
  * SaaSBOM, HBOM(HW BOM), VEX(취약점 정보) 등으로 확장·활용 가능

- SBOM 필수항목에 대한 SPDX, SWID, CycloneDX 포맷 비교 ⇒

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

(출처) '미국 SBOM 정책 분석 및 시사점(Issue Report IS-144, SPRI, 2022.12.16.)' 내용에 추가

2. 국내외 의료기기 SBOM 활용 및 규제 동향

1. 의료기기 SBOM 관련 국내외 동향

미국

- (`22.12) **`23년 통합 세출법**(Omnibus)이 법률로 서명됨
  - ✓ 3305절(의료기기의 사이버보안 보장)에 **524B절(기기의 사이버보안 보장)을 추가**하여 FD&C 법을 개정함
  - ✓ `14년부터 의료기기 사이버보안에 대한 구속력 없는 지침을 발표했으나, 새로운 법안은 **의료기기가 최소 사이버보안을 충족하도록 FDA에 공식적으로 권한을 부여**함
  - ✓ 의료기기 사이버보안을 충족하기 위해 **SBOM 제출 의무화**

국내

- (`19.12) 식약처에서 "의료기기의 사이버보안 허가·심사 가이드라인 " 을 발표하면서 **네트워크에 연결된 의료기기에 대하여 사이버보안 적용을 요구**하고 있음
- (`22.01, '23.07) IMDRF의 사이버보안 가이드라인을 국내 환경에 맞게 **개정하여 발표**
- (`24.05) 국정원, 과기정통부, 디지털플랫폼정부위원회에서 '**SW 공급망 보안 가이드라인 v1.0**' 발표

유럽

- **의료기기 규정(MDR) 745/2017** 부속서 I에 일반 안전 및 성능 요구사항이 나열되어 있으며, 부속서에는 6개의 명시적인 **사이버보안 요구사항도 포함**되어 있음
  - ✓ 745/2017(MDR) 및 746/2017(IVDR)이 2017년 5월 25일에 채택되어 발효
  - ✓ 의료기기의 경우 2021년 5월, 체외진단 의료기기의 경우 2022년 5월까지 점진적으로 적용 → 2021년 5월에 발효됐지만 업체 준비 미흡과 코로나19 등을 이유로 2024년 5월 26일까지 시행 연기

    * 고위험군 의료기기 전환은 2027년 말까지, 중위험 및 저위험 기기 전환은 2028년 말까지 연장
- 사이버보안 요구사항은 Medical Device Coordination Group에서 게시한 **"MDCG 2019-16 의료기기 사이버보안 지침"**에 자세히 설명되어 있음
  - ✓ (4.2 사용 설명서) 특정 보안정보의 경우 사용 설명서가 아닌 별도 문서를 통해 공유된다고 언급하고 있으며, 특정 보안정보 예시로 **SBOM을 명시**하고 있음

(참고) "옴니버스" 3305절(의료기기 사이버보안 보장) 내용

SEC. 3305. 의료기기의 사이버보안 보장

(a) 일반 – FD&C법(21 U.S.C. 351 이하)은 마지막에 다음을 추가하여 개정됩니다. :

Sec. 524B. 기기의 사이버보안 보장

(a) 일반- 신청서를 제출하는 사람 또는 510(k), 513, 515(c), 515(f) 또는 520(m)에 따라 제출하는 경우, 이 절에 따른 사이버 기기의 정의를 충족하는 기기의 절에는 사이버 기기가 (b)항에 따른 사이버보안 요구사항을 충족하는지 확인하기 위해 장관이 요구할 수 있는 정보가 포함되어야 합니다.

(b) 사이버보안 요구사항 - (a)항에 명시된 신청서 또는 제출물의 스폰서는 (a)항에 설명된 신청 또는 제출의 스폰서는 다음을 수행해야 합니다.

(1) **협동적 취약성 공개(coordinated vulnerability disclosure, CVD) 및 관련 절차**를 포함하여 적절한 시기에 **시판 후 사이버보안 취약성 및 악용을 모니터링, 식별 및 해결하기 위한 계획**을 장관에게 제출합니다;

(2) 기기 및 관련 시스템이 **사이버공격으로부터 안전(cybersecure)하다는 합리적인 보증을 제공하기 위한 프로세스 및 절차를 설계, 개발 및 유지**하고, 기기 및 관련 시스템에 대한 **시판 후 업데이트 및 패치를 제공**하여 다음을 해결합니다.

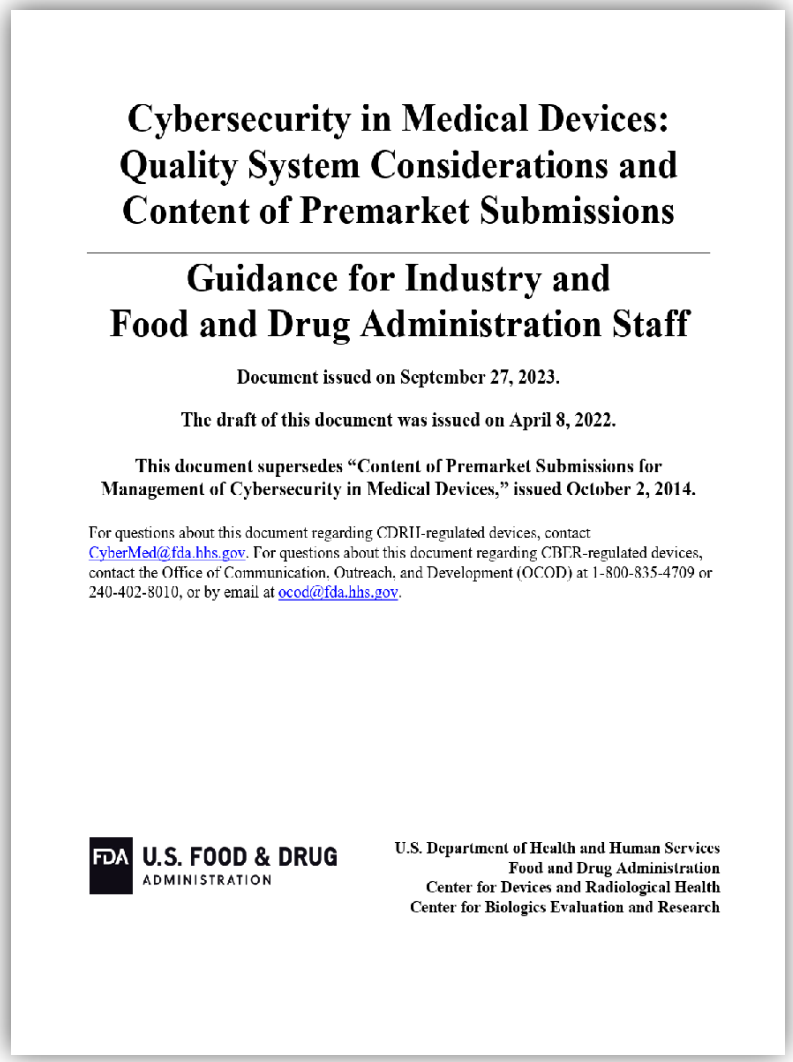
(A) 합리적으로 정당화되는 정기적인 주기로, 허용할 수 없는 것으로 알려진 취약점; 그리고

(B) 통제할 수 없는 위험을 초래할 수 있는 중대한 취약점을 주기에서 벗어나 가능한 한 빨리 해결합니다;

(3) **상용, 오픈소스 및 기성 소프트웨어 구성요소를 포함한 소프트웨어 자재 명세서(SBOM)**를 장관에게 제공합니다.

(4) 장치 및 관련 시스템이 사이버보안에 대한 합리적인 보증을 입증하기 위해 장관이 규정을 통해 요구할 수 있는 기타 요건을 준수합니다.

2-1. 美 FDA 사이버보안 가이드 : 시판전 보안요구사항



Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

Guidance for Industry and Food and Drug Administration Staff

Document issued on September 27, 2023.

The draft of this document was issued on April 8, 2022.

This document supersedes "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," issued October 2, 2014.

For questions about this document regarding CDRH-regulated devices, contact CyberMed@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-835-4709 or 240-402-8010, or by email at ocod@fda.hhs.gov.

FDA U.S. FOOD & DRUG ADMINISTRATION

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

I. 소개
II. 범위
III. 배경
IV. 일반 원칙
V. 사이버보안 위험 관리를 위해 SPDF 사용
  A. 보안 위험 관리
    1. 위협 모델링
    2. 사이버보안 위험 평가(assessment)
    3. 상호 운용성 고려사항
    4. 제3자 소프트웨어 구성요소
    5. 미해결 이상 징후에 대한 보안 평가
    6. TPLC 보안 위험 관리
  B. 보안 아키텍처
    1. 보안통제 구현
    2. 보안 아키텍처 뷰
  C. 사이버보안 시험
VI. 사이버보안 투명성
부록 1. 보안 통제 범주 및 관련 권장 사항
부록 2. 보안 아키텍처 흐름에 대한 제출 문서
부록 3. 임상시험용 기기 면제를 위한 제출 서류
부록 4. 일반적인 시판 전 제출 문서 요소 및 위험에 따른 확장성
부록 5. 용어

2-2. 美 FDA SBOM 요소 : 기본요소(NTIA) + 추가요소

NTIA의 기본 SBOM 요소

< SBOM에 대한 메타정보를 제공하는 속성 >

- 작성자 이름(Author Name): SBOM의 저자로, 작성자가 항상 공급자가 아닐 수도 있음
- 타임스탬프(Timestamp): SBOM이 마지막으로 업데이트된 날짜 및 시간으로, 초기 생성을 포함하여 SBOM 항목이 변경되면 타임스탬프를 업데이트해야 함. 타임스탬프는 시간대와 지역에 걸쳐 일관되어야 하며 ISO 8601과 같은 일반적인 국제 형식을 사용해야 함

< 컴포넌트에 적용되는 속성 >

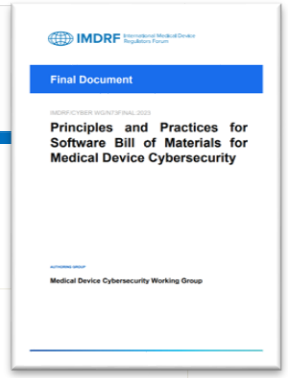
- 공급자 이름(Supplier Name): SBOM 항목에 있는 구성요소 공급업체의 이름 또는 기타 식별자
- 구성요소명(Component Name): 구성요소의 이름 또는 기타 식별자로, 공급자(또는 작성자)가 정의함
- 버전(Version String) : 구성요소 버전으로, 버전 정보는 구성요소를 추가로 식별하는 데 도움이 됨
- 구성요소 해시(Component Hash): 구성요소의 암호화 해시로, 암호화 해시는 소프트웨어 구성요소의 고유 식별자임. 해시 대신 디지털 서명을 사용할 수 있으며 더 강력한 무결성과 신뢰성을 제공하지만 키 관리 및 서명 확인을 포함한 복잡성이 추가됨. 공급자와 작성자는 구성요소를 정의하는 방법을 선택하고, 이는 다시 해시 범위를 정의함. 예를 들어 SBOM에는 소스 구성요소에 대한 해시, 해당 구성요소의 컴파일된 바이너리 형식에 대한 해시, 구성요소 컬렉션에 대한 해시가 포함될 수 있음
- 유일한 식별자(Unique Identifier): 구성요소를 고유하게 정의하는 데 도움이 되는 추가 정보로, 고유 식별자는 일부 전역적으로 고유한 계층 구조 또는 네임스페이스를 기준으로 생성되거나 기존 전역 좌표계를 참조할 수 있음
- 관계(Relationship): SBOM 구성요소 간의 연관성으로, 구성요소 간의 관계는 SBOM 모델 설계에 내재되어 있으며, 기본 관계 유형은 포함임

2-2. 美 FDA SBOM 요소 : 기본요소(NTIA) + 추가요소

FDA에서 요구하는 추가 정보

- 소프트웨어 컴포넌트 제조업체의 모니터링 및 유지관리를 통해 제공되는 **소프트웨어 지원 수준**
  - 예, 소프트웨어가 적극적으로 유지 관리됨(the software is actively maintained), 더 이상 유지 관리되지 않음(no longer maintained), 버려짐(abandoned)
- **소프트웨어 컴포넌트 지원 종료**(EoS, End-of-Support) **일자**

(참고) IMDRF, 의료기기 SBOM 요소



기본 SBOM 요소

- 작성자 이름(Author name) : SBOM 파일을 생성한 개체(예, 개인, 조직, 또는 유사) 참조
- 타임스탬프 : SBOM 데이터 어셈블리 날자 및 시간 기록
- 소프트웨어 컴포넌트 벤더(공급자) : 컴포넌트를 생성하고 정의하고 식별하는 개체. SW컴포넌트 벤더 이름은 일반적으로 상업 SW에 대한 법적 비스니스 이름을 참조해야 함
- 소프트웨어 컴포넌트 이름 : 오리지널 공급자에 의해 정의된 소프트웨어 유닛에 할당된 명칭
- 소프트웨어 컴포넌트 버전 : 이전에 식별된 버전에서 소프트웨어의 변경을 명세하기 위해 공급자에 의해 사용되는 식별자
- 유일한 식별자 : 컴포넌트를 식별하는데 사용되거나 관련 데이터베이스 조회 키 역할을 하는 식별자
- 관계(Relationship) : 업스트림 컴포넌트 X가 소프트웨어 Y에 포함되는 관계를 설명

추가 정보

- 컴포넌트 해시 : 컴포넌트의 존재를 관련 데이터 소스에 매핑하는 데 도움이 될 수 있음
- 디바이스의 생명주기와 관련된 고려사항(예, 소프트웨어 컴포넌트의 EOS(End-of-Support) 날자)

(참고) 국내외 사이버보안 가이드라인 GAP 분석 : SBOM 관점

구분	국내 식약처 가이드 (2023.07)	IMDRF (2020.03)	美 FDA 가이드 (2023.09)	MDR / MDCG 2019-16 rev.1 (2020.07)
SBOM (시판 전, 시판 후 업데이트/보안패치 등)	-	- (별도문서, [IMDRF/CYBER WG/N73, 2023.04.] **Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity**)	**V. A. 4. Third-Party Software Components (제3자 SW 구성요소)** **(a) SBOM** **(b) Documentation Supporting SBOM**	4. Documentation and Instructions for use (문서화 및 사용 설명서) **4.2 instructions for use (사용 설명서)**

(참고) 국내 ´SW 공급망 보안 가이드라인 v1.0´ NIS-SBOM

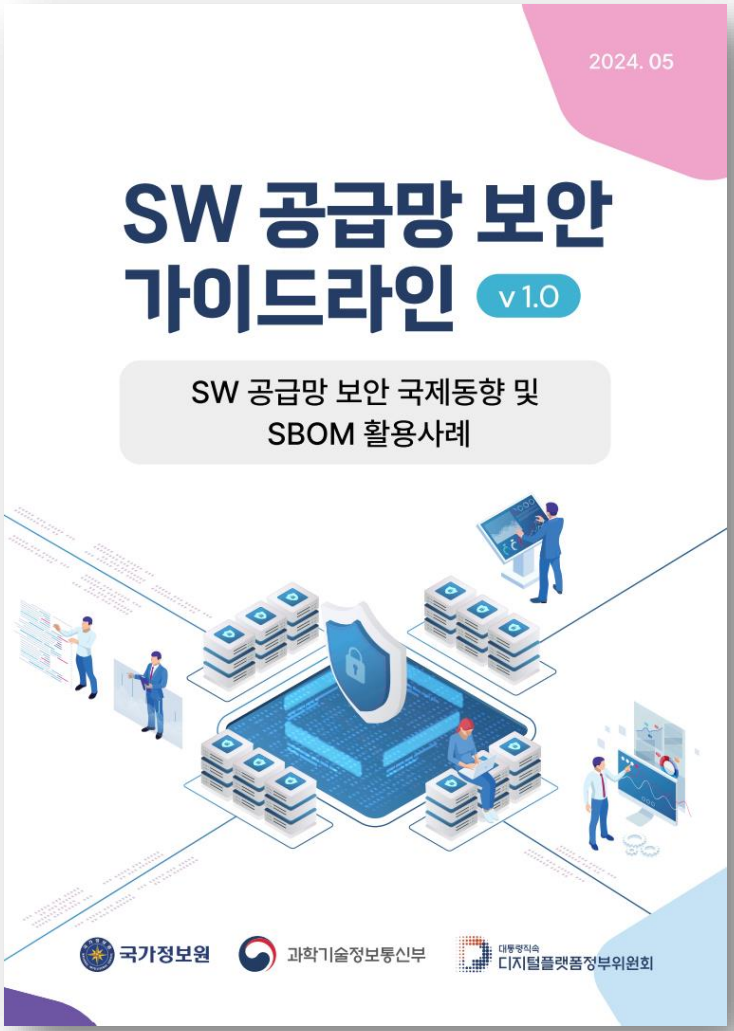
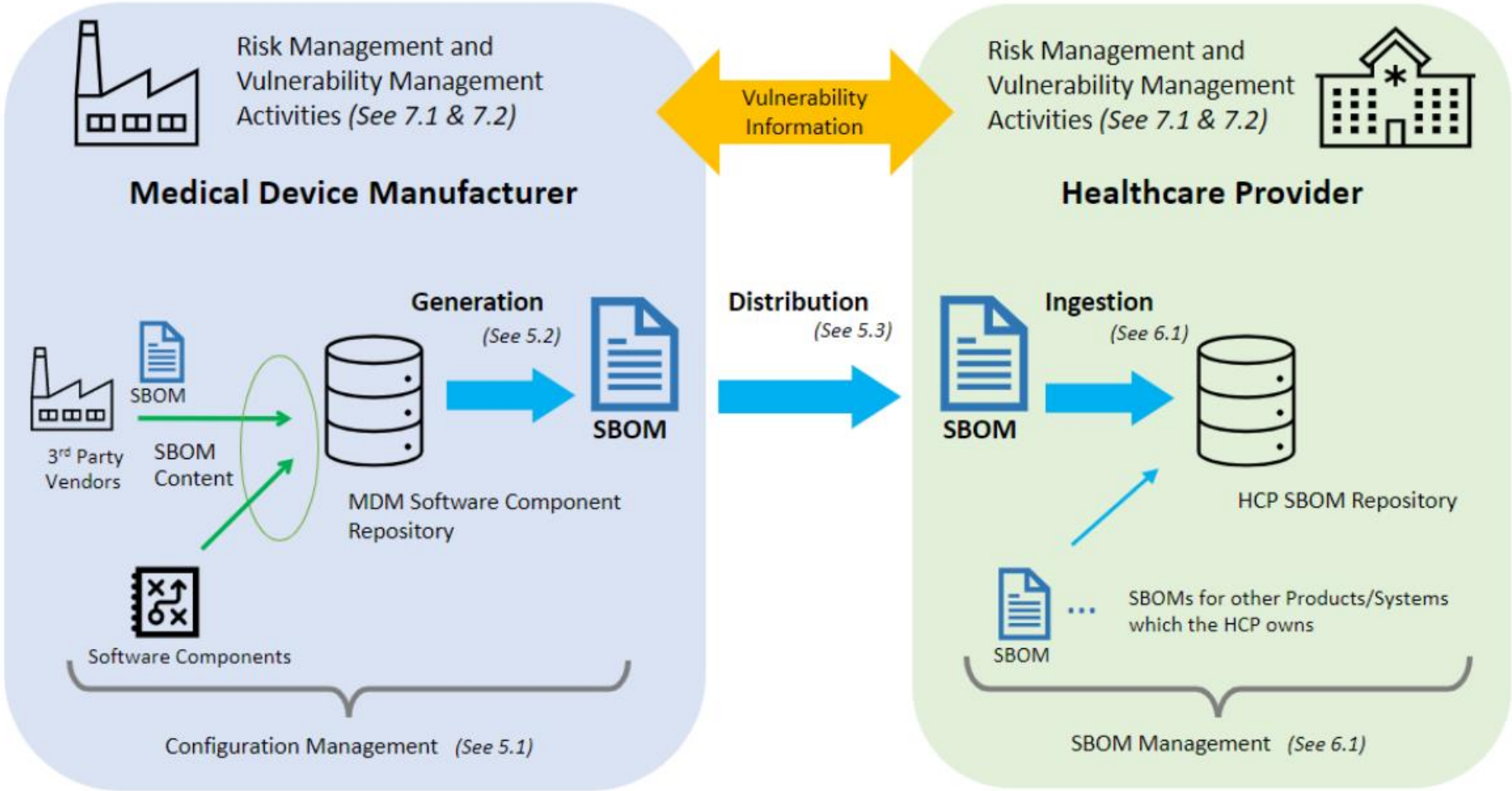


표 35 NIS-SBOM 기본항목 (* : 자체 선정)

구분	속성
① SBOM Standard*	NIS / SPDX / CycloneDX / TTA 등 SBOM 표준
② SBOM Type*	개발 / 유통 등 SBOM 생성단계
③ CycloneDXNo.	CycloneDX번호
④ SPDX Doc. ID	SPDX 문서번호
⑤ SBOM ID*	SBOM 문서번호
⑥ Product Name*	제품 이름
⑦ Product Version*	제품 버전
⑧ Component Name	컴포넌트 이름
⑨ Component Alias*	컴포넌트 별칭
⑩ Component Version	컴포넌트 버전
⑪ Component Supplier Name	컴포넌트 공급자 이름
⑫ Component Hash	컴포넌트 해시(SHA-256 이상 사용)
⑬ Component Path*	컴포넌트 경로(컴포넌트 실제 위치 식별)
⑭ SBOM Author Name	SBOM 작성자
⑮ Unique Identifier	컴포넌트 버전 외에 조회가 가능한 고유 식별자 (CPE, PURL 등)
⑯ Dependency Relationship	상위 컴포넌트와의 종속 관계
⑰ Timestamp	SBOM 생성일시
⑱ License Name · Version	라이선스 이름 · 버전
⑲ Vul. DB	NVD(CVE), CISA(KEV) 등 보안취약점 DB
⑳ Vul. Info	CVE 식별자 및 CVSS 보안취약점 등급

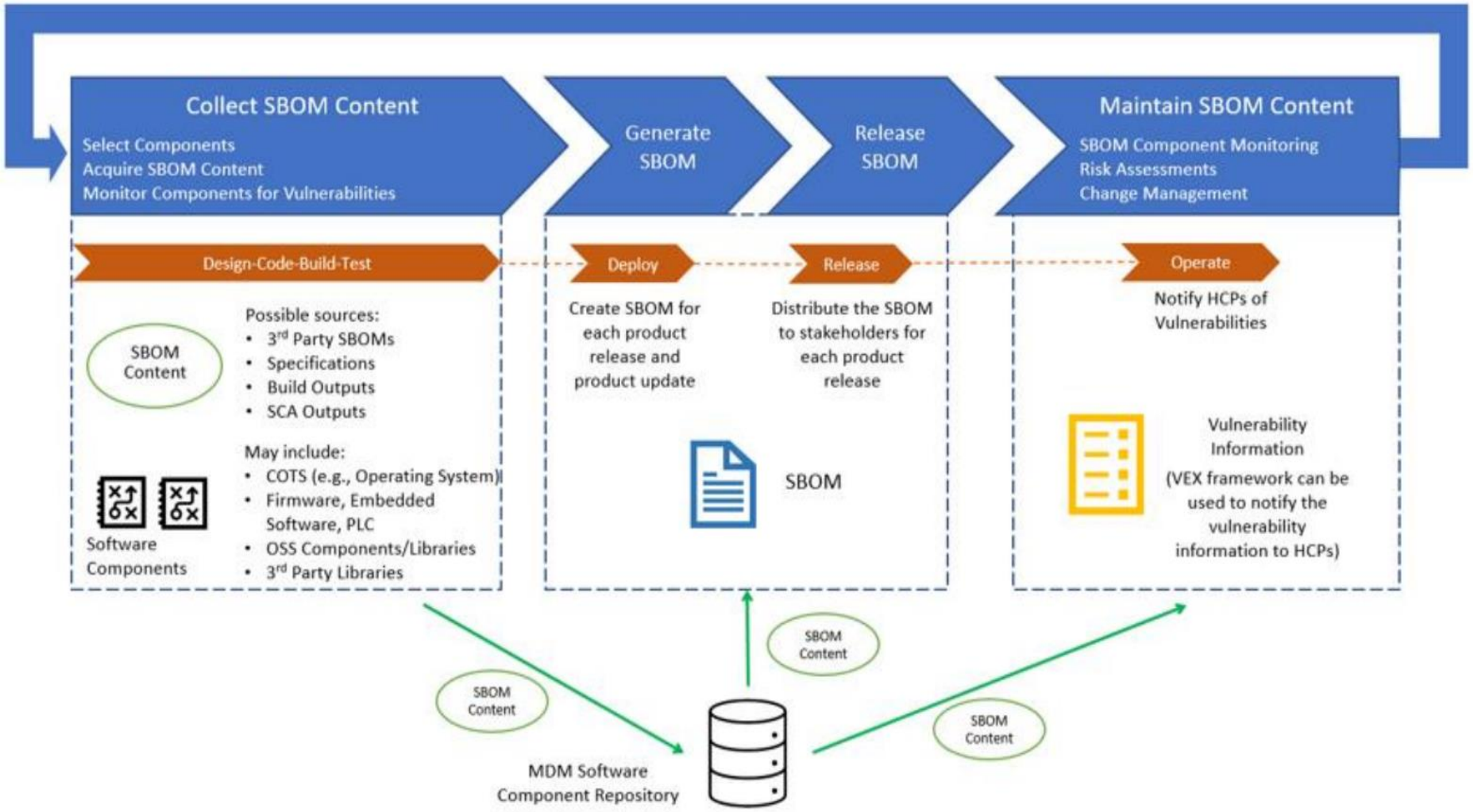
3. 의료기기 SBOM 도입

1. SBOM 프레임워크



(출처) Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity

2. 제조자 고려사항



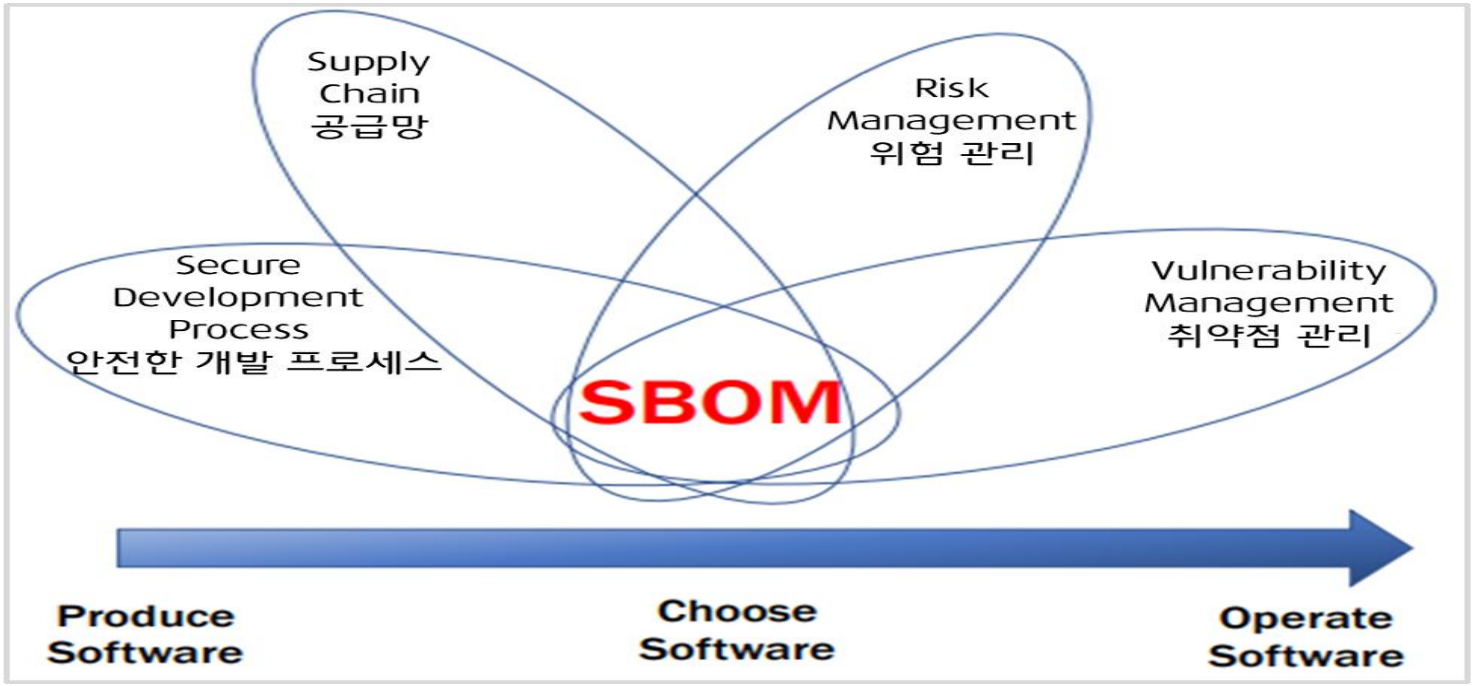
(출처) Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity

3. SBOM 배포

배포 방법	장점	단점
제조자가 제공하는 **고객 보안 문서**에 포함	▪ 특별한 도구가 필요하지 않음	▪ 자동화되지 않음 ▪ 문서는 자주 업데이트되고 사용자에게 배포되어야 함 ▪ 문서를 장치 자체에 다시 연결할 수 있는 방법 필요 (강력한 자산 관리) ▪ SBOM 접근에 대한 통제 감소
별도(전자) 문서로 제조자에 의해 제공	▪ 특별한 도구가 필요하지 않음 ▪ SBOM 접근에 대한 더 많은 통제 ▪ 가급적(preferably) 컴퓨터로 읽을 수 있음	▪ 자동화되지 않음 ▪ 문서는 자주 업데이트되고 사용자에게 배포되어야 함 ▪ 문서를 장치 자체에 다시 연결할 수 있는 방법 필요 (강력한 자산 관리)
디스플레이, 참조(간접) 또는 다운로드를 통해 의료기기에서 접근 가능	▪ 항상 정확한 버전 ▪ 사용자의 통제하에 있음 ▪ SBOM 접근에 대한 더 많은 통제	▪ 자동화되지 않음 ▪ 정보에 접근하려면 장치에 대한 접근 권한 필요 ▪ 장치에 정보 추출 수단이 없을 수 있음(예, 사용자 인터페이스, USB 포트, 네트워크 연결) ▪ 장치에 충분한 공간 필요
의료기기에 **API**로 접근 가능	▪ SBOM 접근에 대한 더 많은 통제 ▪ 자동화된 프로세스에서 사용할 수 있음	▪ API 표준은 정의되지 않은 상태로 남아 있음 ▪ 도구 필요 ▪ 연결 필요
제조자가 **관리하는 저장소**	▪ SBOM 접근에 대한 더 많은 통제 ▪ 자동화된 프로세스에서 사용 가능	▪ 고객은 정보를 위해 여러 제조업체 사이트/저장소를 확인해야 함
중앙 집중식 저장소	▪ 고객이 정보에 접근할 수 있는 보다 간소화된 방법(즉, 많은 개별 제조업체 사이트/저장소를 확인할 필요 없음) ▪ 자동화된 프로세스로 사용 가능	▪ 제3자 서비스를 사용할 때 제조업체에 대한 지적 재산권, 책임 및 기타 고려 사항 ▪ 일부 조직에는 업데이트 상태가 다른 동일한 장치의 여러 버전이 있을 수 있으므로 최신 버전뿐만 아니라 모든 적용 가능한 SBOM에 접근해야 하므로 버전 관리 문제

(출처) Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity

4. SBOM의 중요성



SBOM은 소프트웨어 개발과 유지보수 과정에서 공급망 투명성을 제공하고, 위험 관리를 강화하며, 취약점을 식별하고 관리하며, 안전한 개발 프로세스를 지원하는 중요한 도구

이를 통해 기업은 보안과 안전성을 강화하고 소프트웨어 라이프사이클 전반에 걸쳐 안전한 결과를 달성 가능하게 함

※ 출처 : 공급망 보안 워크숍 "Efforts to Secure the Software Supply Chain in the U.S."

KTC는 고객과 함께

미래를 만들어 나가겠습니다.