체크리스트 기반 의료기기 보안 사전검증 시뮬레이터 설계 및 적용 프레임워크 제안

우정현[1], 전성민[1], 무니브 무하마드[1], 고광만[1]
[1]상지대학교 컴퓨터공학과
[1]2025015001@sj.sangji.ac.kr, [1]2025015104@sj.sangji.ac.kr,
[1]2019015001@sj.sangji.ac.kr, [1]kkman@sangji.ac.kr

Design and Implementation Framework of a Checklist-Based Security Pre-Evaluation Simulator for Medical Devices

Jung-Hyun Woo[1], Sung-Min Jeon[1],
Muhammad Muneeb[1], Kwang-Man Ko[1]
[1]Dept. of Computer Engineering, Sang-Ji University

요 약

본 연구는 의료기기 사이버보안 평가의 체계적 수행을 지원하기 위한 방안으로, 식품의약품안전처(MFDS)의 「의료기기 사이버보안 허가·심사 가이드라인(2024)」을 기반으로 한 체크리스트 기반 보안 사전검증 시뮬레이터의 설계 프레임워크를 제안한다. 제안된 시뮬레이터는 웹 기반 구조를 따르며, 보안 요구사항에 대한 체크리스트 응답을 시작으로 CWE 기반 위험 시나리오 매핑, SBOM 기반 정량적 취약점 분석, 자동 보고서 생성을 하나의 흐름으로 통합한다. 또한 본 시스템은 FastAPI, React, PostgreSQL 등 오픈소스 기술을 활용하여 아키텍처를 설계하였고, 외부 보안 정보 연동을 위해 NVD, GitHub Advisory, MITRE CWE DB API의 통합 방안을 포함한다. 본 연구는 이를 통해 의료기기 보안 내재화를 위한 개발 초기단계 자가진단 도구의 필요성을 충족하고, 향후 실제 구현과 적용 사례 연구를 위한 기초 설계를 제공하는 데 목적이 있다.

1. 서론

최근 의료기기의 디지털화와 연결성 증대에 따라, 의료기기를 대상으로 한 사이버보안 위협이 현실적인 문제로 부상하고 있다. 특히 원격 진단, 인공지능 기반 분석, 사용자 앱 연동 기능 등을 포함한 디지털 헬스케어 기기 및 Software as a Medical Device(SaMD)는 해킹, 데이터 유출, 비인가 접근 등의 위험에 노출될 가능성이 크다.

이러한 배경 속에서 세계 주요 규제기관은 사이버보안을 의료기기 인허가의 핵심 평가 요소로 반영하고 있으며, 한국 식품의약품안전처(식약처) 또한 2024년 11월 「의료기기 사이버보안 허가·심사 가이드라인」을 개정하여, 기존보다 확대된 35개의 보안설계 요구사항을 인허가 심사 시 적용하도록 하고 있다.

그러나 현실에서는 이러한 보안 항목에 대한 개발자 또는 제조사의 사전 자가진단 도구가 부족한 상황이며, 보안 수준의 정량적 평가나 인허가 문서 초안 작성을 지원하는 체계도 미비한 상태이다. 특히 디지털트윈 기반으로 설계되는 의료기기의 경우, 물리적 하드웨어와 가상 소프트웨어가 결합된 형태로 복잡성이 높아짐에 따라, 보안성 검증의 구조적 어려움이 더욱 심화되고 있다.

본 연구는 이러한 문제 인식을 바탕으로, 식약처 사이버보안 요구사항을 기반으로 하는 체크리스트형 보안성 평가 시뮬레이터의 설계 방안을 제안한다. 제안된 시스템은 디지털트윈 기반 의료기기 또는 SaMD 개발자가 자가적으로 보안수준을 점검하고, 인허가 제출을 위한 보안 문서를 구조화할 수 있도록 지원한다. 또한 보안 시나리오 기반의 정성적·정량적 평가 기능을 통해 제품 설계 초기단계에서의 보안 내재화를 가능하게 한다 [1][2].

2. 배경 및 관련 기준

의료기기의 사이버보안은 과거에는 기능 안전성이나 개인정보 보호에 비해 상대적으로 후순위로 다루어졌으나, 최근 원격 진단, 모바일 앱 연동, 클라우드 기반 분석 등 디지털 기술의 접목이 확대되면서 사이버보안 위협이 중요한 이슈로 부상하고 있다. 최근 보고된 해킹, 악성코드 감염, 비인가 접근

사례 등은 의료사고로 이어질 수 있는 실질적 위협으로 부상하고 있으며, 각국 규제기관은 보안성을 의료기기 인허가의 필수 요소로 포함시키고 있다.

이에 따라 미국 FDA, IMDRF, 유럽연합, 일본 등은 의료기기의 설계 단계부터 폐기까지 전 생애주기를 고려한 사이버보안 요구사항을 가이드라인을 통해 제시하고 있으며, 보안 문서화 요구도 점차 강화되는 추세이다. 예를 들어, 미국 FDA는 2023년 최종 가이드라인에서 총 12종의 보안 산출물을 요구하며, 여기에 SBOM(Software Bill of Materials), 위협모델링, 보안 테스트 결과, 취약점 대응 계획 등이 포함된다 [3]. IMDRF 또한 2020년 N60 문서를 통해 기술적·관리적 보안 요구사항을 규정하고 있다. 한국 식약처 역시 2024년 개정 「의료기기 사이버보안 허가·심사 가이드라인」을 통해, 기존 15개였던 보안 요구사항을 35개 항목으로 확대하고, 이를 6개 핵심 영역으로 구조화하였다. 이 기준은 IEC 62443-4-2, ISO/IEC 81001-5-1 등 국제 표준과 정합성을 유지하면서도 국내 실정에 맞춰 자율평가 방식을 도입하고 있다. 제조사는 설계 문서, 보안 체크리스트, 기술적 증빙자료, 미적용 사유 등을 포함한 인허가 문서를 직접 준비해야 하며, 이에 따라, 사전 구조화 및 자동 점검이 가능한 디지털 기반 시스템 도구의 필요성이 더욱 부각되고 있다 [4].

식약처가 제시한 사이버보안 평가 기준은 다음의 6개 영역으로 구성되며, 각 항목별로 세부 점검 요소 및 예시 키워드가 함께 제공된다.

<표 1> 식약처 사이버보안 평가 기준의 6대 분류 및 항목 예시

분류	주요 항목 요약	예시 키워드
식별 및 인증	사용자 및 기기 식별·인증 구현	비밀번호, 인증서, MFA 등
사용 통제	권한 기반 접근 제한	관리자/사용자 권한, 포트 비활성화
시스템 무결성	소프트웨어 위변조 방지	해시 검증, Secure Boot
데이터 기밀성	저장/전송 중 개인정보 보호	AES 암호화, 씬, 최소 수집 원칙
이벤트 대응 및 감사	보안 사고 감지 및 기록, 대응 절차 구비	보안 로그, 사고 알림, 감사 추적
자원 가용성	서비스 유지 및 보안 업데이트 체계 마련	OTA, 백업/복구, Dos 대응

이 기준은 단순한 기술 보안 요구를 넘어, 자산 식별부터 사용 통제, 무결성 확보, 데이터 보호, 이벤트 대응, 지원 가용성까지 포괄하고 있다. 따라서 개발 초기 단계부터 체계적인 보안 요구사항 반영이 필요하며, 자가진단 기반의 시스템적 검토 도구가 절실한 상황이다. 본 연구는 이러한 배경을 바탕으로, 식약처 기준을 디지털화한 시뮬레이터 설계 방안을 제안하고자 한다.

3. 시뮬레이터 설계 및 구성 모듈

3.1 설계 개요

본 연구에서 제안하는 시뮬레이터는 식약처의 「의료기기 사이버보안 허가·심사 가이드라인(2024)」을 기반으로, 의료기기 개발자 및 보안 평가자가 보안 요구사항을 자가진단하고 결과 보고서를 자동 생성할 수 있도록 구성된 웹 기반 플랫폼이다.

시뮬레이터는 사용자가 체크리스트에 응답한 내용을 바탕으로, CWE(Common Weakness Enumeration) 기반 위험 시나리오 분석과 SBOM(Software Bill of Materials) 기반 정량적 취약점 분석을 자동 수행하며, 인허가 문서로 활용 가능한 보고서를 PDF, Word, Excel 형식으로 출력할 수 있다. 이 과정을 통해 보안 설계의 내재화와 인허가 문서 준비를 동시에 지원한다.

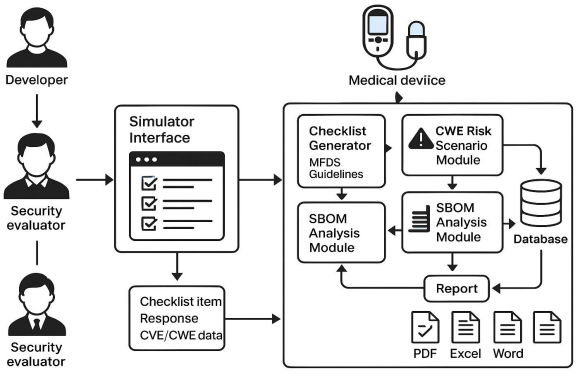
3.2 구성 모듈 및 기능

본 시뮬레이터는 다음의 다섯 가지 주요 기능 모듈로 구성된다

<표 2> 주요 기능 모듈 구성

모듈	주요기능
체크리스트 응답 모듈	MFDS보안 가이드라인 기반 자가진단 항목 제공 및 사용자 응답 수집
CWE 위험 시나리오 모듈	응답 기반으로 CWE시나리오 자동 매핑 및 정성적 분석
SBOM 분석 모듈	Syft를 통한 SBOM 파일 생성, Grype를 통해 CVE 취약점 도출
보고서 자동 생성기	PDF, Word, Excel 보고서 자동 생성 및 보안 문서화 지원
외부 API 연동 모듈	NVD, GitHub, CWE Db 등 실시간 연동으로 최신 보안 정보 반영

3.3 시스템 흐름도 기반 작동 구조

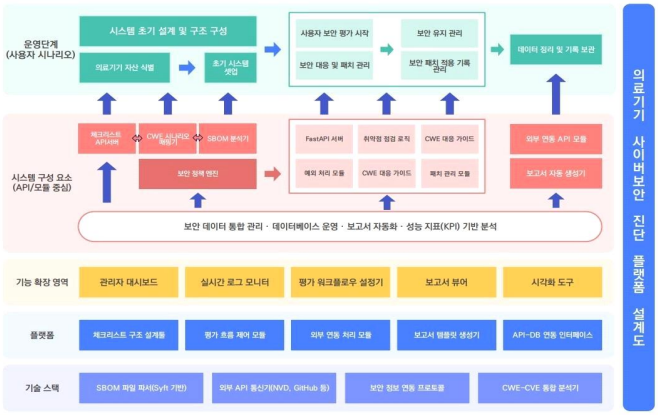


<그림 1> 시뮬레이터 전체 작동 흐름도

본 시뮬레이터는 의료기기 보안성 평가를 위한 자동화된 검증 절차를 지원하며, <그림 1>은 본 시스템의 전체 작동 흐름을 도식화한 것이다. 시스템 사용자는 개발자 또는 보안 평가자로, 웹 인터페이스를 통해 체크리스트 기반의 보안 항목에 응답함으로써 절차가 시작된다. 사용자의 응답 정보는 시스템 내 CWE 시나리오 자동 매핑 모듈로 전달되어, 해당 보안 항목과 연계된 설계 취약점을 구조화된 위험 시나리오 형태로 자동 생성한다. 이를 통해 보안 요구사항 미충족 항목에 대한 설계상 위험 인식을 가능하게 한다. 또한, 사용자는 시스템에 SBOM 파일을 업로드하게 되며, 시스템은 Syft 기반 분석 도구를 통해 소프트웨어 구성요소를 파싱하고, Grype 도구를 활용하여 구성요소별 CVE 취약점 정보를 자동 식별한다. CWE와 CVE(Common Vulnerabilities and Exposures) 간 상호 연계 분석을 통해 정량적 취약점 분석이 이루어진다 [5].

최종적으로, 분석된 결과는 보고서 자동 생성 모듈로 전달되며, 사용자 응답, CWE 시나리오, CVE 목록 등을 통합하여 PDF, Word, Excel 형식의 문서로 자동 출력된다. 생성된 보고서는 의료기기 인허가 제출 시 활용 가능한 표준화된 형태로 제공되어 문서화 효율성과 정확성을 높인다.

3.4 시스템 아키텍처 설계



<그림 2> 의료기기 보안성 검증 시뮬레이터 시스템 아키텍처 설계도

본 연구에서 제안하는 시뮬레이터는 의료기기 보안성 평가를 웹 기반에서 자동화하기 위한 목적으로 설계되었으며, 전체 시스템은 4계층 구조의 플랫폼 아키텍처를 따른다. 각 계층은 사용자 시나리오 계층, 시스템 구성 요소 계층, 기능 확장 및 플랫폼 계층, 기술 스택 계층으로 구성되며, 전체 구조는 <그림 2>에 제시하였다.

(1) 사용자 시나리오 계층

가장 상단에 위치한 사용자 시나리오 계층은 실제 사용자인 개발자 또는 보안 평가자의 업무 흐름을 반영하여 구성된 단계이다. 사용자는 '의료기기 자산 식별 → 시스템 초기 설정 → 보안 대응 및 패치 관리 → 보안 기록 저장'의 절차에 따라 플랫폼을 이용하며, 이는 실질적인 인허가 문서 준비 과정과 직접적으로 연계된다. 각 시나리오 단계는 시스템 하위 모듈과 상호 작용하며, 사용자 중심의 인터페이스를 통해 유기적인 작동 흐름을 유도한다.

(2) 시스템 구성 요소 계층 (API 및 모듈 중심)

이 계층은 시뮬레이터의 핵심 기능이 구현되는 영역으로, 주요 API 서버와 분석 모듈이 포함된다.

체크리스트 API 서버는 식약처(MFDS)의 사이버 보안 평가 기준에 따라 설계된 항목을 사용자에게 제공하고, 입력된 응답을 구조화하여 저장한다.

CWE 시나리오 매핑기는 체크리스트 응답에서 도출된 보안 취약 요소를 기반으로 CWE 시나리오를 자동 생성하여, 설계상의 보안 취약점을 시각적으로 제시한다.

SBOM 분석기는 Syft를 통해 SBOM을 파싱하고, Grype를 활용해 구성 요소별 CVE 취약점을 자동 탐지한다. 보안 정책 엔진은 사용자의 입력 응답과 취약점 분석 결과를 종합하여, 인허가 기준 충족 여부를 평가하고 보안 정책 기반의 진단 결과를 제공한다. 보고서 자동 생성기 및 외부 API 연동 모듈은 분석된 정보를 종합하여 PDF, Word, Excel 형식의 보고서를 자동 생성하며, GitHub Advisory DB, NVD, MITRE CWE DB 등의 외부 보안 데이터베이스와 실시간으로 연동되어 최신 위협 정보를 반영한다. 각 모듈 간 연결 흐름은 시스템 하위 요소에서 상위 사용자 계층으로 정보를 전달하는 방향으로 설계되었으며, <그림 2>의 파란색 화살표를 통해 이를 시각적으로 표현하였다.

(3) 기능 확장 및 플랫폼 계층

본 계층은 사용자 중심의 UI 요소와 백엔드 기능을 확장하는 구성 요소들로 이루어져 있다.

프론트엔드 기능으로는 관리자 대시보드, 실시간 로그 모니터, 평가 워크플로우 설정기, 보고서 뷰어, 시각화 도구 등이 포함되며, 보안 분석 결과를 직관적으로 확인하고 활용할 수 있도록 설계되었다.

백엔드 플랫폼 측면에서는 체크리스트 구조 설계툴, 외부 연동 처리 모듈, 보고서 템플릿 생성기,

API-DB 연동 인터페이스 등이 포함되며, 사용자 입력과 보안 분석 결과를 안정적으로 연결하는 역할을 수행한다.

(4) 기술 스택 계층

최하단에 위치한 기술 스택 계층은 본 시스템의 구현에 활용된 핵심 오픈소스 도구와 연동 API를 나타낸다.

- SBOM 파싱 : Syft 기반으로 구성 요소 정보를 구조화.
- 취약점 탐지 : Grype를 사용하여 CVE 탐색 및 CWE 매핑.
- 보안 연동 프로토콜 : GitHub Advisory DB, NVD API, MITRE CWE DB 등과의 API 연동.
- 보고서 자동화 출력 : python-docx, WeasyPrint, xlsxwriter를 통해 다양한 문서 형식의 결과물 생성

이와 같은 구조는 의료기기 개발자 또는 제조사가 보안성 요구사항을 사전 평가하고, 결과를 자동 문서화함으로써 실제 인허가 문서 제출에 활용할 수 있도록 지원한다.

4. 시스템 구현 및 적용 시나리오

본 장에서는 제안된 시뮬레이터 시스템의 실제 구현 방식과, 이를 기반으로 한 보안성 평가 시나리오 적용 사례를 소개한다. 구현은 오픈소스 기반 기술 스택을 중심으로 이루어졌으며, 시스템의 각 계층은 독립적으로 설계되어 모듈화된 방식으로 통합되었다.

<표 3> 개발 환경 및 사용 기술 도구

항목	내용
개발 프레임워크	FastAPI(Python 3.10 기반)
프론트엔드	React.js(TypeScript)
데이터베이스	PostgreSQL
문서 자동화 도구	python-docx, WeasyPrint, xlsxwriter
보안 취약점 분석 도구	Syft, Grype
외부 연동 API	NVD API, GitHub Advisory API, MITRE CWE DB API

시스템은 클라우드 환경 (예: AWS EC2 또는 GCP VM 인스턴스)을 기반으로 구축되며, RESTful API 구조를 통해 각 기능 모듈이 유기적으로 연동된다. SBOM 분석은 Syft를 통해 구성요소를 추출하고, Grype를 통해 CVE 취약점을 자동 탐색하는 방식으로 구현되었다.

4.2 적용 시나리오

의료기기 제조사가 SaMD 제품을 개발 중인 상황을 가정하여 시뮬레이터 적용 흐름은 다음과 같다.

- 초기 시스템 셋업 : 사용자는 시스템에 접속하여 의료기기 식별 정보 및 자산 분류 정보를 입력한다.
- 체크리스트 기반 자가진단 수행 : MFDS 보안 기준에 따른 항목에 응답하여 현재 보안수준을 진단한다.
- 위험 시나리오 도출 : 시스템은 CWE 데이터베이스를 기반으로 보안 미흡 항목에 대한 위험 시나리오를 자동 생성한다.
- SBOM 기반 정량 평가 수행 : 제품 내 포함된 소프트웨어 구성요소를 SBOM 파일로 업로드하면, 자동으로 취약점(CVE) 분석이 수행된다.
- 보고서 자동 생성: 모든 분석 결과는 PDF, Word, Excel 형식의 보고서로 통합되어 인허가 문서 초안으로 활용된다.

4.3 기대 효과

자가진단 기능 강화: 개발자 또는 제조사가 제품 보안 수준을 사전에 구조적으로 검토할 수 있음.

인허가 대응 효율성 제고: 자동화된 보고서 생성 기능을 통해 제출 문서 작성 시간을 대폭 단축.

국내외 기준 동시 대응: MFDS 기준뿐 아니라 CWE, CVE 등 국제 보안 기준까지 반영되어 추후 글로벌 시장 진출을 위한 기반 마련.

참고문헌

[1] 식품의약품안전처, 「의료기기 사이버보안 허가·심사 가이드라인」, 2024년 11월 개정.

[2] 한승희, 박건우, “의료기기 사이버 보안 측면에서의 사후 관리 방안 마련 연구,” 『FDC법제연구』, 제16권, 제1호, pp. 27-35, 2021.

[3] 식품의약품안전처, “의료기기 사이버보안 적용 및 심사 사례,” 2023.

[4] International Medical Device Regulators Forum (IMDRF), Principles and Practices for Medical Device Cybersecurity, IMDRF/MDCE WG/N60 FINAL:2020, 2020.

[5] Scherb, C., Hadayah, A., & Heitz, L., “CyMed: A Framework for Testing Cybersecurity of Connected Medical Devices,” arXiv preprint, arXiv:2310.03583, 2023.