의료기기의 사이버보안 허가·심사 가이드라인 (민원인 안내서)

2022. 1. 21

식품의약품안전처
식품의약품안전평가원
의 료 기 기 심 사 부

지침서 · 안내서 제 · 개정 점검표

명칭	의료기기의 사이버보안 허가·심사 가이드라인(민원인 안내서)

아래에 해당하는 사항에 체크하여 주시기 바랍니다.

등록대상 여부	□ 이미 등록된 지침서・안내서 중 동일・유사한 내용의 지침서・안내서가 있습니까?	□ 예 ■ 아니오
	☞ 상기 질문에 '예'라고 답하신 경우 기존의 지침서・안내서의 개정을 우선적으로 고려하시기 바랍니다. 그럼에도 불구하고 동 지침서・안내서의 제정이 필요한 경우 그 사유를 아래에 기재해 주시기 바랍니다. (사유 :)	
	□ 법령(법・시행령・시행규칙) 또는 행정규칙(고시・훈령・예규)의 내용을 단순 편집 또는 나열한 것입니까?	□ 예 ■ 아니오
	□ 단순한 사실을 대외적으로 알리는 공고의 내용입니까?	□ 예 ■ 아니오
	□ 1년 이내 한시적 적용 또는 일회성 지시・명령에 해당하는 내용입니까?	□ 예 ■ 아니오
	□ 외국 규정을 번역하거나 설명하는 내용입니까?	□ 예 ■ 아니오
	□ 신규 직원 교육을 위해 법령 또는 행정규칙을 알기 쉽게 정리한 자료입니까?	□ 예 ■ 아니오
	☞ 상기 사항 중 어느 하나라도 '예'에 해당되는 경우에 지침서・안내서 등록 대상이 아닙니다. 지침서・안내서 제・개정 절차를 적용하실 필요는 없습니다.	
지침서・안내서 구분	□ 내부적으로 행정사무의 통일을 기하기 위하여 반복적으로 행정사무의 세부기준이나 절차를 제시하는 것입니까? (공무원용)	□ 예(☞지침서) ■ 아니오
	□ 대내외적으로 법령 또는 고시・훈령・예규 등을 알기 쉽게 풀어서 설명하거나 특정한 사안에 대하여 식품의약품안전처의 입장을 기술하는 것입니까? (민원인용)	■ 예(☞안내서) □ 아니오
기타 확인 사항	□ 상위 법령을 일탈하여 새로운 규제를 신설・강화하거나 민원인을 구속하는 내용이 있습니까?	□ 예 ■ 아니오
	☞ 상기 질문에 '예'라고 답하신 경우 상위법령 일탈 내용을 삭제하시고 지침서・안내서 제・개정 절차를 진행하시기 바랍니다.	

상기 사항에 대하여 확인하였음.

2022 년 1 월 21 일

담당자 김 현 수

확 인(부서장) 강 영 규

개정 이력서

의료기기의 사이버보안 허가·심사 가이드라인(민원인 안내서)

제·개정번호	승인일자	주요 내용
안내서-0995-01	2019.11.28	의료기기의 사이버보안 허가·심사 가이드라인(민원인 안내서) 제정
안내서-0995-02	2022.01.21	IMDRF '의료기기 사이버보안 원칙 및 기준'의 적용범위, 정의, 시판 전 고려사항을 적용

이 안내서는 사이버보안 허가·심사 시의 적용범위 및 판단기준 등에 대해 알기 쉽게 설명하거나 식품의약품안전처의 입장을 기술한 것입니다.

본 안내서는 대외적으로 법적 효력을 가지는 것이 아니므로 본문의 기술 방식('~하여야 한다' 등)에도 불구하고 참고로만 활용하시기 바랍니다. 또한, 본 안내서는 '22년 1월 현재의 과학적·기술적 사실 및 유효한 법규를 토대로 작성되었으므로 이후 최신 개정 법규 내용 및 구체적인 사실관계 등에 따라 달리 적용될 수 있음을 알려드립니다.

※ "민원인 안내서"란 민원인들의 이해를 돕기 위하여 법령 또는 행정규칙을 알기 쉽게 설명하거나 특정 민원업무에 대한 행정기관의 대외적인 입장을 기술하는 것(식품의약품안전처 지침서등의 관리에 관한 규정 제2조)

※ 본 안내서에 대한 의견이나 문의사항이 있을 경우 의료기기심사부 첨단의료기기과(디지털헬스기기팀)에 문의하시기 바랍니다.

전화번호: 043-719-3948
팩스번호: 043-719-3940

목 차

Ⅰ 일반사항

1. 배경 및 목적

정보통신기술의 발달로 유·무선 통신하는 의료기기의 개발이 증가하고 있다.

이러한 의료기기는 원격진료 목적으로 사용되는 '유헬스케어 의료기기'에서부터 생명 유지 기능 목적의 '이식형심장박동기'에 이르기까지 매우 다양하며, 기술의 발전으로 통신 가능한 다양한 유형의 의료기기가 개발될 것으로 예상된다.

그러나 의료기기의 해킹, 정보 유출 등 사이버보안 위협사례가 꾸준히 보고되고 있고, 이러한 위협사례는 재산적 손실뿐만 아니라 환자 생명에 직접적인 위해를 줄 수 있어 의료기기의 사이버보안에 대한 중요성이 부각되고 있다.

이에 본 가이드라인에서는 의료기기 허가·심사 시 사이버보안이 요구되는 의료기기의 적용 대상을 명확히 하고 제품의 특성에 따라 적용할 수 있는 보안 요구사항과 허가·심사 시 제출해야 하는 자료의 범위를 정하여 통신이 가능한 의료기기의 안전관리를 확보하고자 한다.

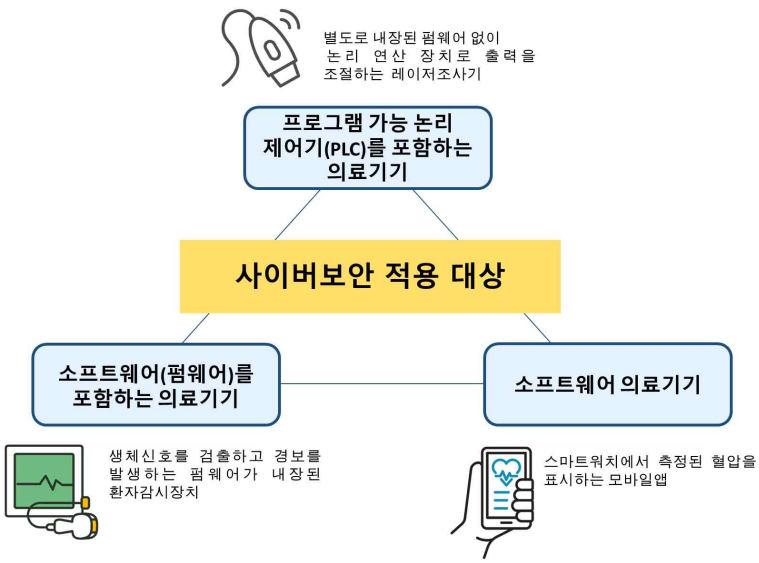
본 가이드라인은 국제조화를 이루기 위해 국제의료기기규제당국자포럼(International Medical Device Regulators Forum, IMDRF) '의료기기 사이버보안 원칙 및 지침'(Principles and Practices for Medical Device Cybersecurity, IMDRF(2020))의 2.0 적용범위, 3.0 정의, 5.0 시판 전 고려사항을 차용하여 적용하였다.

2. 적용 범위

본 가이드라인은 의료기기의 사이버보안 확보를 위한 것으로 소프트웨어를 포함하는 의료기기[펌웨어(Firmware) 및 프로그램 가능 논리 제어기(Programmable Logic Controller(PLC)를 포함하는 의료기기) 또는 소프트웨어로만 존재하는 의료기기(소프트웨어 의료기기(Software as a Medical Device, SaMD)]중 유·무선 통신(Wi-Fi, 블루투스, USB, RS-232, LAN 등)을 사용하거나 통신 경로가 존재하는 의료기기에 적용한다.

본 가이드라인은 의료기기 허가·심사 시 사용자의 건강에 직접적인 영향을 미칠 수 있는 사이버보안 위협에 대하여 적용할 수 있는 최소한의 권고사항을 제시한다.

다만, 의료기기 허가 후 관리나 사용자(의료기관 등)의 관리적 보안 또는 사용자의 건강에 직접적으로 영향을 미치지 않는 개인정보유출 등은 의료법 및 개인정보보호법 등 타 법령을 준수하도록 권장한다.



[그림 1. 의료기기 사이버보안 적용 대상]

3. 용어의 정의

가. 가용성(Availability)

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

나. 기밀성(Confidentiality)

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

다. 무결성(Integrity)

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

라. 부인방지(Non-repudiation)

제기된 이벤트나 행동의 발생 및 그것이 시작된 실체를 입증할 수 있는 능력(KS X ISO/IEC 27000:2019)

마. 소프트웨어 의료기기(Software as a Medical Device, SaMD)

하드웨어에 종속되지 않고 의료기기의 사용목적에 부합하는 기능을 가지며 독립적인 형태의 소프트웨어만으로 이루어진 의료기기

바. 사이버보안(Cybersecurity)

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

사. 암호화(Encryption)

정보보안을 유지하기 위하여 그 정보를 특정한 규칙에 따라 변형하여 저장함으로써 해독방법을 모르면 그 정보의 내용을 알아볼 수 없도록 하는 기술

아. 인증(Authentication)

어떤 실체에 주장된 특성이 정확하다는 것을 보장하는 것(KS X ISO/IEC 27000:2019)

자. 진본성(Authenticity)

어떤 실체가 무엇이라고 주장하는 성질(KS X ISO/IEC 27000:2019)

차. 취약성(Vulnerability)

하나 이상의 위협에 의해 촉진될 수 있는 자산 또는 통제의 불충분 보안 경영시스템(KS X ISO/IEC 27000:2019)

※ 의료기기 위험관리 관련 용어는 「의료기기 제조 및 품질관리 기준(식약처 고시)」 및 「의료기기 위험관리 가이드라인(2017)」을 참조한다.

Ⅱ 의료기기 사이버보안 기본원칙

의료기기 사이버보안은 가용성(Availability), 기밀성(Confidentiality), 무결성(Integrity) 을 고려하여야 한다.

가용성은 데이터가 승인된 사용자에게 즉시 제공되어야 하며, 필요한 때에 필요한 곳에서 필요한 형태로 존재되어야 함을 의미한다.

기밀성은 데이터가 허가되지 않은 사람에게 공개되거나, 허가되지 않은 용도로 사용되지 않아야 함을 의미한다. 제조자는 데이터의 송·수신 과정 또는 비인가자의 조회 등 비합법적인 방법이나 오류에 의해 데이터가 노출되더라도 해독하기 어렵도록 암호화하고 인가된 자에 한해 정보의 접근이 가능하도록 하며, 정보이용자도 목적과 그 권한에 따라 접근범위를 제한하여야 한다.

무결성은 데이터가 허가되지 않은 방법으로 변환되거나 파괴되지 않아야 함을 나타낸다. 정보는 정확하고 완전해야 하며, 위·변조를 통해 왜곡되지 않도록 해야 한다. 정보 변경 시 인가된 사용자에 의해서만 이루어지고, 로그 및 변경 이력이 관리되어야 한다.

의료기기의 사이버보안을 보장하기 위하여 가용성, 기밀성, 무결성이 준수되어야 하며, 의료기기 위험관리와 같이 「의료기기 제조 및 품질관리 기준」에 따라 의료기기 제조자가 품질시스템에서 수립한 위험관리 프로세스 내에서 적용되어야 한다.

의료기기 사이버보안의 위험관리 프로세스는 위험분석(Risk analysis), 위험평가(Risk evaluation), 위험통제(Risk control), 잔여위험 허용평가(Evaluation of overall residual risk acceptability), 위험관리보고서

(Risk management report), 생산 및 생산 후 정보(Production and post-production information)의 단계로 진행된다. 이러한 사이버보안 위험관리는 정보의 생명주기 전체에 걸쳐 통신이 가능하거나 통신 경로가 존재하는 의료기기에 적용한다.

[그림 2. 의료기기 사이버보안 위험관리 프로세스]

의료기기 사이버보안 위험분석 단계에서는 가용성, 기밀성, 무결성이 파괴되어 환자에게 미치는 위해요인을 식별한다. 또한 이러한 과정에서 식별된 위해요인이 현실화된 결과의 잠재적 영향을 평가하고, 실제적인 발생 가능성을 평가하여 위험 수준을 결정한다.

의료기기 사이버보안 위험평가 단계에서는 식별된 각 위해요인에 대하여 위험관리 계획서에 정의된 위험 수용기준을 바탕으로 산정된 위험이 위험감소를 하지 않아도 될 만큼 낮은지를 결정하여야 한다.

의료기기 사이버보안 위험통제 단계에서는 위험평가 결과를 감안한 적절한 사이버보안 위험통제 방안을 선택하고, 선택한 방안의 구현에 필요한 모든 통제를 결정 및 실행하여야 한다.

그리고 위험통제 수단을 적용한 후 잔여위험들에 대하여 허용 평가를 하여야 한다.

제조자는 이러한 일련의 사이버보안 위험관리 프로세스에서의 절차들을 위험관리보고서에 기록하여야 한다.

생산 및 생산 후 정보 단계에서는 사이버보안에 대한 정보를 검토하기 위한 체계적인 절차를 수립하고 유지하여야 한다.

또한, 제조자는 사이버보안 위험관리 프로세스를 적용하기 위해 적절한 기능과 수준으로 사이버보안 목표를 수립하여야 한다. 사이버보안 목표는 사이버보안 정책과의 일관성을 유지하고, 실현가능한 수준에서 측정이 가능하며 적용 가능한 사이버보안 요구사항과 위험평가 및 위험처리 결과를 감안하여야 한다.

아울러, 의료기기 생명주기 전체에 걸쳐 내부 및 외부 고객들의 의견을 지속적으로 수집·분석하여 의료기기 사이버보안 위험관리에 반영한다.

의료기기 사이버보안 위험관리보고서의 구체적인 작성방법은 「의료기기의 사이버보안 적용방법 및 사례집(2019)」을 참조할 수 있다.

Ⅲ 의료기기 사이버보안 요구사항

유·무선 통신이 가능하거나 통신 경로가 존재하는 의료기기는 정보의 위변조, 오작동 또는 의료기기에 승인되지 않은 접근 등을 방지하기 위한 대책을 마련하여야 한다.

제조자는 표 1을 참고하여 의료기기의 잠재적 결함으로 인해 사용자에게 발생할 수 있는 위해(Harm)의 정도, 의료기기의 통신방법 및 사용환경을 종합적으로 고려하여 표 1의 요구사항 적용 여부를 식별하고, 식별된 요구사항에 대해 사이버보안 안전을 확인할 수 있는 검증자료를 제출하여야 한다.

다만, 제품의 특성 상 적용할 수 없는 일부 요구사항에 대해서는 해당 항목의 미적용 사유를 확인할 수 있는 근거자료(위험관리문서, 사용설명서, 설계문서 등)를 제출할 수 있다.

[표 1. 의료기기 사이버보안 요구사항 적용을 위한 고려사항의 예]

고려사항	종류	설 명
사이버보안 침해로 인한 위해도	상 (major)	의료기기 사이버보안 침해로 사용자의 심각한 상해 또는 사망, 신체기능의 영구적 장애, 신체구조의 영구적 손상의 가능성이 있음
	중 (moderate)	의료기기 사이버보안 침해로 사용자의 일시적이고 경미한 상해, 의학적 중재가 필요할 수 있음
	하 (minor)	의료기기 사이버보안 침해로 사용자의 일시적인 불편, 의학적 중재 없이 가역적이거나 경미하고 단시간의 불편이 있을 수 있음
통신방법	유선 통신	유선 케이블(USB, RS-232, HDMI 등)을 이용하여 다른 기기 및 시스템과의 통신을 수행
	무선 통신	무선 통신 모듈(Wi-Fi, 블루투스, NFC, RF 통신 등)을 이용하여 다른 기기 및 시스템과의 통신을 수행

사용 환경	병원 내 사용	병원 내에서만 사용되는 의료기기로 사이버보안 침해를 위한 제3자의 접근이 어렵고, 보안이 갖춰진 병원 폐쇄망 내에서 사용됨
	병원 외 사용	병원 외에서 사용이 가능한 의료기기(개인용 의료기기 등)로 제3자의 접근이 용이함
	공용 네트워크망 사용	시공간의 제약없이 언제, 어디서나 공용 네트워크망(인터넷 등)에 접속하여 기기 및 시스템과의 통신이 가능함

아래의 사이버보안 요구사항은 IMDRF '의료기기 사이버보안 원칙 및 지침'(Principles and Practices for Medical Device Cybersecurity, IMDRF(2020)) 5.1 보안 요구사항 및 아키텍처 디자인의 사이버보안 설계 원칙을 적용한 것으로 현 시점에서 사용되고 있는 제품들의 기술적 특성을 반영하였다.

추후 새로운 제품이 개발되거나 기능, 통신 특성 등이 차이가 있는 경우 사이버보안 요구사항 일부가 제외되거나 추가될 수 있다. 이러한 요구사항은 제품의 허가 이후에도 지속적인 사후관리를 통해 제품에 반영하여야 한다.

[표 2. 의료기기 사이버보안 요구사항]

항목	요구사항
보안 통신	제조자는 의료기기가 다른 기기나 네트워크와 어떻게 접속(유·무선 통신 등)하여야할지를 고려하여야 한다. ※ 예: Wi-Fi, 이더넷, 블루투스, USB 등
	제조자는 내·외부의 모든 입력에 대한 유효성을 확인하는 설계 특성을 고려하여야 하며, 보안이 취약한 통신(예. 가정용 네트워크 혹은 기존 기기)만을 지원하는 기기 및 환경에서 이루어지는 통신도 고려한다.
	제조자는 비인가 접근/변경/반복을 방지하기 위한 의료기기의 보안이 보장된(secured) 데이터 송·수신 방법을 고려하여야 한다. ※ 예: 기기/시스템 간 통신 시 상호인증방법, 암호화 필요 여부, 과거에 전송된 명령어 및 데이터의 비인가 반복에 대한 방지, 사전에 정의된 통신 종료 시점의 적절성 여부 등

데이터 보호	제조자는 안전(safety)과 관련된 데이터가 저장되거나 기기와 송·수신될 때 암호화와 같은 일정 수준의 보호가 요구되는지 고려하여야 한다. ※ 예: 비밀번호(passwords)는 암호화된 보안(secure)이 확보된 해쉬(hash)로 저장되어야함
	제조자는 기밀성에 대한 위험 통제 수단이 요구될 때, 통신 프로토콜의 컨트롤(control)/시퀀싱(sequencing) 필드의 메시지를 보호하거나 암호화의 키 관련 자료가 손상되는 것을 방지하도록 고려하여야 한다.
기기 무결성	제조자는 데이터 부인방지(non-repudiation)를 보장하기 위한 설계 특성이 필요한지를 결정하기 위해 시스템 레벨에서의 아키텍쳐를 평가하여야 한다. ※ 예: 감사 로그 기록 기능 제공
	제조자는 기기 소프트웨어의 비인가된 변경과 같은 기기의 무결성에 대한 위험을 고려해야한다.
	제조자는 바이러스, 스파이웨어, 랜섬웨어 등 기기에서 실행될 수 있는 악성코드를 막기 위해 안티 멀웨어 프로그램과 같은 통제조치를 고려하여야 한다.
사용자 인증	제조자는 기기의 사용이 입증된 사용자이거나, 다른 역할의 사용자에게 사용권한을 부여를 허용하거나, 응급상황에서 접근을 허용하는 사용자 접근 통제에 대해 고려하여야 한다. 추가적으로 동일한 자격증명은 기기와 고객들에게 공유되지 않아야한다. ※ 접근 통제의 예: 비밀번호, 하드웨어 키, 생체인증 등
소프트웨어 유지보수	제조자는 주기적인 업데이트의 구현과 배포를 위한 수행절차를 수립하고 통보하여야한다.
	제조자는 운영 체제(OS) 소프트웨어, 제3자 소프트웨어, 오픈 소스 소프트웨어가 업데이트나 통제될 경우에 대해 고려하여야 한다. 또한 제조자는 외부의 통제에 의한 소프트웨어의 업데이트나 운영환경 만료에 대한 대응 계획을 수립하여야 한다. ※ 예: 보안이 보장되지 않은(unsecure) 운영체제 버전에서 운영되는 의료기기 소프트웨어
	제조자는 새로운 사이버보안 취약성에 대응할 의료기기 업데이트 방안을 고려하여야 한다. ※ 예: 업데이트 시 사용자 개입/ 자동 업데이트 여부, 기기의 안전(safety)과 성능에 영향을 보장할 수 있는 업데이트 유효성 검증
	제조자는 업데이트의 수행하기 위해 어떤 연결이 필요한지와 코드 서명 및 기타 비슷한 수단을 통한 연결이나 업데이트의 진본성을 고려하여야 한다.
물리적 접근	제조자는 비인가된 개인이 의료기기에 접근하는 것을 방지하기 위한 통제수단을 고려하여야 한다. ※ 예: 물리적 잠금 혹은 포트(port) 접근의 물리적 제한, 인증이 필요없는 물리적 케이블의 접근제한 등
신뢰성 및 가용성	제조자는 의료기기가 필수 성능을 유지하기 위해 사이버보안 공격을 탐지, 저항, 대응 및 복구하도록 허용하는 설계 특성을 고려하여야 한다.

Ⅳ 허가·심사 첨부자료

1. 제출 자료의 범위 및 요건

유·무선 통신이 가능하거나 통신 경로가 존재하는 의료기기는 허가 신청 시「의료기기 허가·신고·심사 등에 관한 규정」(식약처 고시) 제29조(첨부자료의 요건) 제8호 성능에 관한 자료 중 '소프트웨어 검증 및 유효성 확인 자료'를 제출하여야 하며, 제출 시 정보의 위변조, 오작동 또는 의료기기에 승인되지 않은 접근 등으로부터 방지하기 위한 대책으로 표 2의 의료기기 사이버보안 요구사항을 적용하여야한다.

제조자는 의료기기 사이버보안 요구사항에 대한 준수 여부를 확인할 수 있도록 표 3의 '의료기기 사이버보안 요구사항 체크리스트'와 체크리스트의 요구사항을 실제로 검증한 자료를 제출하여야한다. 다만, 제조사의 위험분석을 통해 요구사항 일부를 제외하거나 수정하여 적용하는 경우에는 제26조 제1항 제4호에 따른 시험규격 및 그 설정근거를 제출하여야하며, 해당 자료로 '사이버보안 위험관리문서'를 제출할 수 있다.

< 사이버보안 제출 자료 예시 >

1. 의료기기 사이버보안 요구사항 체크리스트

2. 사이버보안 요구사항을 검증한 자료

- 소프트웨어 검증 및 유효성 확인 자료
- 사이버보안 위험관리문서
- 성능시험성적서

3. 사이버보안 요구사항 미적용 근거를 확인할 수 있는 자료

- 사이버보안 위험관리문서 등

‘의료기기 사이버보안 요구사항 체크리스트’는 의료기기 사이버보안 요구사항에 대한 적합성 여부를 확인할 수 있는 자료로 의료기기 허가·심사 시 의료기기 사이버보안 요구사항 체크리스트 양식을 활용하여 제품의 특성에 맞게 작성하여 제출한다.

‘사이버보안 위험관리문서’와 ‘소프트웨어 검증 및 유효성 확인 자료’는 신청 제품이 의료기기 사이버보안 요구사항 체크리스트에 기재한 사이버보안 요구사항을 만족하고 있음을 확인할 수 있는 근거 자료이다.

‘사이버보안 위험관리문서’는 의료기기 전체 생명주기에서의 사이버보안과 관련된 위해요인을 파악하여 발생 가능한 위해를 최소화 및 차단하기 위한 위험관리 활동을 기록한 보고서로 신청 제품의 사이버보안과 관련된 위해요인 식별과 각 위해요인에 대한 위험분석 및 위험경감 조치의 결과를 기재하여야 한다.

‘소프트웨어 검증 및 유효성 확인 자료’는 의료기기의 위험관리 과정에서 식별된 위해요인에 대한 위험통제 조치의 결과를 검증할 수 있는 객관적인 자료로서 사이버보안 요구사항에 대한 시험 및 검증 절차, 시험결과, 시험 및 검증 도중 소프트웨어 변경이 발생한 경우 재시험 결과를 포함하여야 한다.

‘사이버보안 위험관리문서’와 ‘소프트웨어 검증 및 유효성 확인 자료’는 「의료기기의 사이버보안 적용방법 및 사례집(2019)」과 「의료기기 소프트웨어 허가·심사 가이드라인(2019)」을 참조하여 작성할 수 있다.

2. 의료기기 사이버보안 요구사항 체크리스트

의료기기 사이버보안 요구사항 체크리스트 작성 시 사용되는 통신 기술(유·무선 통신 방식 등), 사용 환경(병원 내/외 사용, 공용 네트워크망 사용 등) 등 통신 특성을 확인할 수 있는 사항을 기재한다.

이를 기반으로 하여 아래의 사이버보안 요구사항 체크리스트에 따라 요구사항 적용여부, 적합성 입증방법, 첨부자료 또는 문서번호를 기재한다.

신청 제품의 기술적 특성 상 요구사항이 제외 또는 추가될 수 있으며, 요구사항이 제외되는 경우 적절한 사유를 '적합성 입증 방법' 란에 기재하고, 추가되는 경우 사이버보안 요구사항에 추가 기재할 수 있다. 예를 들어, 소프트웨어 의료기기(SaMD)의 경우 하드웨어로만 구현할 수 있는 보안 요구사항은 제외할 수 있으며, 소프트웨어로 보안위협에 대해 통제조치를 할 수 있는 경우 요구사항을 추가 기재할 수 있다.

[표 3. 의료기기 사이버보안 요구사항 체크리스트]

< 의료기기 사이버보안 특성 기재 >

1) 사용되는 통신 기술 : *유선 통신(USB, RS-232, LAN), 무선 통신(Wi-Fi, 블루투스, RF 통신)*

2) 사용 환경 : *병원 내 사용, 병원 외 사용*

3) 공용 네트워크망 사용여부 : *Y/N*

사이버보안 요구사항		해당 기기 적용 여부	적합성 입증 방법	해당 첨부자료 또는 문서번호
보안 통신	제조자는 의료기기가 다른 기기나 네트워크와 어떻게 접속(유·무선 통신 등)하여야할지를 고려하여야 한다. ※ 예: Wi-Fi, 이더넷, 블루투스, USB 등	*적용/미적용*	*소프트웨어 검증 및 유효성 확인 자료/사이버보안 위험관리문서*	*문서번호, 페이지, 요구사항 ID, 시험항목 #*
	제조자는 내·외부의 모든 입력에 대한 유효성을 확인하는 설계 특성을 고려하여야 하며, 보안이 취약한 통신(예. 가정용 네트워크 혹은 기존 기기)만을 지원하는 기기 및 환경에서 이루어지는 통신도 고려한다.			
	제조자는 비인가 접근/변경/반복을 방지하기 위한 의료기기의 보안이 보장된(secured) 데이터 송·수신 방법을 고려하여야 한다. ※ 예: 기기/시스템 간 통신 시 상호인증방법, 암호화 필요 여부, 과거에 전송된 명령어 및 데이터의 비인가 반복에 대한 방지, 사전에 정의된 통신 종료 시점의 적절성 여부 등			
데이터 보호	제조자는 안전(safety)과 관련된 데이터가 저장되거나 기기와 송·수신될 때 암호화와 같은 일정 수준의 보호가 요구되는지 고려하여야 한다. ※ 예: 비밀번호(passwords)는 암호화된 보			

	안(secure)이 확보된 해쉬(hash)로 저장되어야 함			
	제조자는 기밀성에 대한 위험 통제 수단이 요구될 때, 통신 프로토콜의 컨트롤(control)/시퀀싱(sequencing) 필드의 메시지를 보호하거나 암호화의 키 관련 자료가 손상되는 것을 방지하도록 고려하여야 한다.			
기기 무결성	제조자는 데이터 부인방지(non-repudiation)를 보장하기 위한 설계 특성이 필요한지를 결정하기 위해 시스템 레벨에서의 아키텍쳐를 평가하여야 한다. ※ 예: 감사 로그 기록 기능 제공			
	제조자는 기기 소프트웨어의 비인가된 변경과 같은 기기의 무결성에 대한 위험을 고려해야한다.			
	제조자는 바이러스, 스파이웨어, 랜섬웨어 등 기기에서 실행될 수 있는 악성코드를 막기 위해 안티 멀웨어 프로그램과 같은 통제조치를 고려하여야 한다.			
사용자 인증	제조자는 기기의 사용이 입증된 사용자이거나, 다른 역할의 사용자에게 사용권한을 부여를 허용하거나, 응급상황에서 접근을 허용하는 사용자 접근 통제에 대해 고려하여야 한다. 추가적으로 동일한 자격증명은 기기와 고객들에게 공유되지 않아야한다. ※ 접근 통제의 예: 비밀번호, 하드웨어 키, 생체인증 등			
소프트웨어 유지보수	제조자는 주기적인 업데이트의 구현과 배포를 위한 수행절차를 수립하고 통보하여야한다.			
	제조자는 운영 체제(OS) 소프트웨어, 제3자 소프트웨어, 오픈 소스 소프트웨어가 업데이트나 통제될 경우에 대해 고려하여야 한다.			

	또한 제조자는 외부의 통제에 의한 소프트웨어의 업데이트나 운영환경 만료에 대한 대응 계획을 수립하여야 한다. ※ 예: 보안이 보장되지 않은(unsecure) 운영체제 버전에서 운영되는 의료기기 소프트웨어			
	제조자는 새로운 사이버보안 취약성에 대응할 의료기기 업데이트 방안을 고려하여야 한다. ※ 예: 업데이트 시 사용자 개입/ 자동 업데이트 여부, 기기의 안전(safety)과 성능에 영향을 보장할 수 있는 업데이트 유효성 검증			
	제조자는 업데이트의 수행하기 위해 어떤 연결이 필요한지와 코드 서명 및 기타 비슷한 수단을 통한 연결이나 업데이트의 진본성을 고려하여야 한다.			
물리적 접근	제조자는 비인가된 개인이 의료기기에 접근하는 것을 방지하기 위한 통제수단을 고려하여야 한다. ※ 예: 물리적 잠금 혹은 포트(port) 접근의 물리적 제한, 인증이 필요없는 물리적 케이블의 접근제한 등			
신뢰성 및 가용성	제조자는 의료기기가 필수 성능을 유지하기 위해 사이버보안 공격을 탐지, 저항, 대응 및 복구하도록 허용하는 설계 특성을 고려하여야 한다.			

V 참고문헌

1. 개인정보의 기술적·관리적 보호조치 기준, 방송통신위원회 고시, 행정안전부
2. 의료기기 소프트웨어 허가·심사 가이드라인, 식품의약품안전처(2015)
3. 의료기기 위험관리 가이드라인, 식품의약품안전처(2007)
4. 홈·가전 IOT 보안가이드, 한국인터넷진흥원(2017)
5. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, FDA(2018)
6. Framework for Improving Critical Infrastructure Cybersecurity, NIST(2014)
7. ISO 14971, Medical devices - Application of risk management to medical devices(2019)
8. ISO 81001-1, Health software and health IT systems safety, effectiveness and security -- Part 1: Principles and concepts(2021)
9. KS X ISO/IEC 27000, 정보기술 - 보안기술 - 정보보호 경영시스템 - 개요와 용어(2019)
10. KS X ISO/IEC 27001, 정보기술 - 보안기술 - 정보보호 경영시스템 - 요구사항(2019)
11. KS X ISO/IEC 27002, 정보기술 - 보안기술 - 정보보호 경영을 위한 실무 지침(2019)
12. KS X ISO/IEC 27032, 정보기술 - 보안기술 - 사이버보안에 대한 가이드라인(2019)
13. KS X IEC TR 80001-1, 의료기기가 통합된 IT네트워크에 대한 위험관리의 적용 - 제1부 : 역할, 책임 및 활동(2017)
14. KS X IEC TR 80001-2-1, 의료기기가 통합된 IT네트워크에 대한 위험관리의 적용 - 제2-1부 : 단계별 의료용 IT네트워크 위험관리 - 실제적용과 사례(2020)
15. KS X IEC TR 80001-2-2, 의료기기가 통합된 IT네트워크에 대한 위험관리의 적용 - 제2-2부 : 의료기기의 보안 요구사항, 위험, 통제에 대한 공개 및 통신을 위한 지침(2020)
16. KS X IEC TR 80001-2-3, 의료기기가 통합된 IT네트워크에 대한 위험관리의 적용 - 제2-3부 : 무선 네트워크에 대한 지침(2020)
17. Postmarket Management of Cybersecurity in Medical Devices, FDA(2016)
18. Principles and Practices for Medical Device Cybersecurity, IMDRF(2020)

별첨 의료기기 사이버보안 요구사항 예시

표 2의 의료기기 사이버보안 요구사항에 적용할 수 있는 상세한 예시를 아래에 제시하였으며 제조자는 상세 예시를 참고하여 각 요구사항에 대한 적합성을 입증할 수 있다. 다만, 해당 예시는 참고 사항일 뿐이며 반드시 이를 따를 필요는 없다.

[표 5. 사이버보안 요구사항에 대한 상세 요구사항 예시]

<table>
<tr><th>항목</th><th>사이버보안 요구사항</th><th colspan="2">상세 요구사항 예시</th></tr>
<tr><td rowspan="4">보안
통신</td><td>제조자는 의료기기가 다른 기기나 네트워크와 어떻게 접속(유·무선 통신 등)하여야할지를 고려하여야 한다.
※ 예: Wi-Fi, 이더넷, 블루투스, USB 등</td><td colspan="2">[1] 통신 구성
제품의 위해도 및 사용환경을 고려하여 통신을 구성하여야한다.
※ 입증 예시 : 제품의 통신 구성 및 방법을 확인할 수 있는 통신구성도, 사용설명서 등</td></tr>
<tr><td rowspan="3">제조자는 내·외부의 모든 입력에 대한 유효성을 확인하는 설계 특성을 고려하여야 하며, 보안이 취약한 통신(예. 가정용 네트워크 혹은 기존 기기)만을 지원하는 기기 및 환경에서 이루어지는 통신도 고려한다.</td><td rowspan="3">[2] 접근통제 및 인증 : 식별 및 인증에 기반하여 의료기기 역할에 따른 접근 권한을 부여가 가능하고 접근 권한에 따라 인가된 데이터에만 접근 가능해야 한다.</td><td>[2-1] 통신 시 인가된 기기 또는 네트워크를 인식할 수 있는 수단을 갖추어야한다.</td></tr>
<tr><td>[2-2] 의료기기 접속 인식 : 비인가된 의료기기가 접속될 시 이를 인식하여 구분할 수 있어야 한다.</td></tr>
<tr><td>[2-3] 비인가된 의료기기 접속 제한 : 비인가된 의료기기의 접속 시 접속을 제한할 수 있어야 한다.</td></tr>
</table>

			[2-4] 비인가된 네트워크 통신 차단 : 비인가된 네트워크 통신 접속을 제한할 수 있어야 한다.
	제조자는 비인가 접근/변경/반복을 방지하기 위한 의료기기의 보안이 보장된(secured) 데이터 송·수신 방법을 고려하여야 한다. ※ 예: 기기/시스템 간 통신 시 상호인증방법, 암호화 필요 여부, 과거에 전송된 명령어 및 데이터의 비인가 반복에 대한 방지, 사전에 정의된 통신 종료 시점의 적절성 여부 등		[2-5] 원격접속 차단 : 의료기기가 의료기관의 서버에 접속할 수 있는 경우, 의료기기 도난 시 해당 의료기기가 서버에 접속할 수 없도록 접근통제를 할 수 있어야 한다.
			[2-6] 의료기기 인증 관리 : 의료기기 인증의 유효기간을 설정할 수 있어야 하며, 설정된 유효기간 만료 시 접근이 통제되어야 한다.
			[2-7] 자동세션종료 : 설정된 시간 이후에는 의료기기간의 통신 또는 접속이 종료되도록 한다.
데이터 보호	제조자는 안전(safety)과 관련된 데이터가 저장되거나 기기와 송·수신될 때 암호화와 같은 일정 수준의 보호가 요구되는지 고려하여야 한다. ※ 예: 비밀번호(passwords)는 암호화된 보안(secure)이 확보된 해쉬(hash)로 저장되어야함	[3] 의료기기 데이터 전송 또는 저장의 기밀성 및 무결성 보장 : 통신을 이용하는 의료기기의 데이터를 전송하거나 저장하는 경우적절	[3-1] 안전한 암호 알고리즘 사용 : 데이터 전송 및 저장 시 사용되는 암호 알고리즘은 112비트 이상 보안강도를 가진 검

		한 암호화 및 복호화 방식을 활용하여 기밀성과 무결성을 보장하여야 한다.	증된 암호 알고리즘 또는 모듈을 사용하여야한다. * 인증 정보: RSA, DSA, SHA 등 * 데이터 : AES 등
			[3-2] 개인의료정보 저장 관리 : 의료기관 외부에서 사용되는 측정기기 또는 게이트웨이에는 개인의료정보를 저장하지 않는 것을 권고한다.
	제조자는 기밀성에 대한 위험 통제 수단이 요구될 때, 통신 프로토콜의 컨트롤(control)/시퀀싱(sequencing) 필드의 메시지를 보호하거나 암호화의 키 관련 자료가 손상되는 것을 방지하도록 고려하여야 한다.	[4] 안전한 암호키 사용 : 암호화 시 사용되는 암호키는 안전하게 관리되어야 한다.	
기기 무결성	제조자는 데이터 부인방지(non-repudiation)를 보장하기 위한 설계 특성이 필요한지를 결정하기 위해 시스템 레벨에서의 아키텍쳐를 평가하여야 한다. ※ 예: 감사 로그 기록 기능 제공	[5] 데이터 감사를 위한 시스템 로그 기록 : 사용자가 의료기기에 접속 시 접속기록, 환자정보 조회, 데이터 생성, 변경, 삭제 등과 같은 로그가 기록되어야 한다.	
	제조자는 기기 소프트웨어의 비인가된 변경과 같은 기기의 무결성에 대한 위험을 고려해야한다.	[6] 의료기기의 정상 동작을 보장하기 위해 주요 실행파일 및 설정파일에 대한 무결성을 검증하여야하며, 무결성 오류 발생 시 대응방안을 고려하여야 한다.	
	제조자는 바이러스, 스파이웨어, 랜섬웨어 등 기기에서 실행될 수 있는 악성코드를 막기 위해 안티멀웨어 프로그램과 같은 통제조치를 고려하여야 한다.	[7] 불필요한 서비스 제거 또는 비활성화 : 불필요한 외부 접속 포트 등의 서비스 비활성화를 기본값으로 설정하고, 외부 접속 포트를 사용할 경우 비밀번호 설정, IP 제한 등의 추가적인 보안 조치를 수행하여야 한다.	

사용자 인증	제조자는 기기의 사용이 입증된 사용자이거나, 다른 역할의 사용자에게 사용권한을 부여를 허용하거나, 응급상황에서 접근을 허용하는 사용자 접근 통제에 대해 고려하여야 한다. 추가적으로 동일한 자격증명은 기기와 고객들에게 공유되지 않아야한다. ※ 접근 통제의 예: 비밀번호, 하드웨어 키, 생체인증 등	[8] 접근통제 및 인증 : 식별 및 인증에 기반하여 사용자 역할에 따른 접근 권한을 부여가 가능하고 접근 권한에 따라 인가된 데이터에만 접근 가능해야 한다.	[8-1] 인가된 사용자를 인식할 수 있는 ID/PW, 하드웨어키, 생체인증 등의 수단을 갖추어야한다.
			[8-1-1] 비밀번호를 사용하는 경우, 다음을 적용해야 한다. - 비밀번호 작성 규칙 강화 - 비밀번호 하드코드 금지 - 비밀번호 노출 금지
			[8-2] 다중접속 금지 : 동일 사용자가 다중으로 접속하지 않아야 한다.
			[8-3] 사용자 접속 인식 : 비인가된 사용자가 접속될 시 이를 인식하여 구분할 수 있어야 한다.
			[8-4] 비인가된 사용자 접속 제한 : 비인가된 사용자의 접속 시 접속을 제한할 수 있어야 한다.
			[8-5] 원격접속 차단 : 사용자가 의료기관의 서버에 접속할 수 있는 경우, 사용자

			계정 도난 시 해당 계정이 서버에 접속할 수 없도록 접근통제를 할 수 있어야 한다.
			[8-6] 사용자 인증 관리 : 사용자 계정의 유효기간을 설정할 수 있어야 하며, 설정된 유효기간 만료 시 접근이 통제되어야 한다.
			[8-7] 자동세션종료 : 설정된 시간 이후에는 사용자의 접속이 종료되도록 한다.
소프트웨어 유지보수	제조자는 주기적인 업데이트의 구현과 배포를 위한 수행절차를 수립하고 통보하여야한다.	[9] 펌웨어 또는 소프트웨어 업데이트의 인가 : 펌웨어 또는 소프트웨어 업데이트 시 관리자의 인가를 요청 및 확인하는 절차가 있거나 관리자 또는 사용자가 인지할 수 있는 거리에서 보안이 보장되는 방법으로 수행되어야 한다.	
	제조자는 운영 체제(OS) 소프트웨어, 제3자 소프트웨어, 오픈 소스 소프트웨어가 업데이트나 통제될 경우에 대해 고려하여야 한다. 또한 제조자는 외부의 통제에 의한 소프트웨어의 업데이트나 운영환경 만료에 대한 대응 계획을 수립하여야 한다. ※ 예: 보안이 보장되지 않은(unsecure) 운영체제 버전에서 운영되는 의료기기 소프트웨어		
	제조자는 새로운 사이버보안 취약성에 대응할 의료기기 업데이트 방안을 고려하여야 한다. ※ 예: 업데이트 시 사용자 개입/		

	자동 업데이트 여부, 기기의 안전(safety)과 성능에 영향을 보장할 수 있는 업데이트 유효성 검증		
	제조자는 업데이트의 수행하기 위해 어떤 연결이 필요한지와 코드 서명 및 기타 비슷한 수단을 통한 연결이나 업데이트의 진본성을 고려하여야 한다.	[10] 펌웨어 또는 소프트웨어 업데이트의 무결성 보장 : 펌웨어 또는 소프트웨어 업데이트 파일 배포 시 버전 식별이 가능하여야 하며, 파일에 대한 배포자 및 무결성을 검증할 수 있어야 한다.	[10-1] 펌웨어 또는 소프트웨어 업데이트 시 인증방식 사용 : 펌웨어 또는 소프트웨어의 업데이트 시 코드 서명 정보를 사용하고 코드 서명 정보는 안전한 해쉬 코드로 보호하여야 한다.
물리적 접근	제조자는 비인가된 개인이 의료기기에 접근하는 것을 방지하기 위한 통제수단을 고려하여야 한다. ※ 예: 물리적 잠금 혹은 포트(port) 접근의 물리적 제한, 인증이 필요없는 물리적 케이블의 접근제한 등	[11] 물리적인 통신포트 침해의 최소화 - 통신포트의 침해를 최소화하기 위해 기기에 물리적인 잠금을 제공하여야 한다.	
신뢰성 및 가용성	제조자는 의료기기가 필수 성능을 유지하기 위해 사이버보안 공격을 탐지, 저항, 대응 및 복구하도록 허용하는 설계 특성을 고려하여야 한다.	[12] 사이버 보안 위협 탐지 시 취해야 할 대응책에 관한 정보 제공 - 의료기기의 사용 중 발생하는 사이버 보안 사고에 대하여 긴급 연락처 및 기기의 제조자와 상담을 할 수 있는 연락방식을 제공하여야 하며, 사이버 보안 위협 탐지 시 취해야 할 대응책을 수립하고 사용자에게 제공하여야 한다.	
		[13] DDoS 공격에 대한 방어 - 공용 네트워크망에 접속하여 의료기기를 실시간으로 제어 또는 환자 생명과 직접적으로 연관될 수 있는 정보를 실시간으로 송수신하는 장비의 경우 DDoS 공격에 대한 대응책이 수립되어야 한다.	

[전문가협의체 위원]

소속	직위	성명	비고
고려대학교	교수	한근희	학계
경북대학교	교수	이성기	
연세대학교	교수	유선국	
건국대학교	연구원	이인혜	
분당서울대학교병원	의공팀장	유재민	
건국대학교병원	과장	한기태	
한국기계전기전자시험연구원	선임연구원	방지호	연구기관
한국인터넷진흥원	팀장	이향진	
한국인터넷진흥원	책임연구원	임송빈	
한국인터넷진흥원	팀장	김찬일	
한국인터넷진흥원	책임연구원	이상걸	
삼성전자㈜	부장	이수관	산업계
삼성전자㈜	부장	조성호	
삼성전자㈜	책임	이기태	
LG전자㈜	책임연구원	이창희	
하이케어넷 주식회사	이사	곽봉조	
㈜지엠솔루션	대표	김명교	
㈜솔	대표	이종묵	
㈜H3 시스템	대표	김민준	
㈜인바디	부장	김경근	

의료기기의 사이버보안 허가·심사 가이드라인(민원인 안내서)

발 행 처 식품의약품안전처 식품의약품안전평가원

발 행 일 2022년 1월

발 행 인 서경원

편 집 위 원 장 이정림

편 집 위 원 강영규, 한영민, 손승호, 배영우, 김현수, 정병수, 김병남

우) 28159
충북 청주시 흥덕구 오송읍 오송생명2로 187

문 의 처 식품의약품안전평가원 첨단의료기기과(디지털헬스기기팀)

전화: 043-719-3948
팩스: 043-719-3900

28159 충북 청주시 흥덕구 오송읍 오송생명2로 187
오송보건의료행정타운
식품의약품안전처 식품의약품안전평가원
의료기기심사부 첨단의료기기과(디지털헬스기기팀)
TEL : 043)719-3948 FAX : 043)719-3900
http://www.mfds.go.kr/medicaldevice

식품의약품안전처
식품의약품안전평가원