TTA Technical Report

정보통신단체표준(국문표준)

*

TTAx.xx-xx.xxxx 제정일: 2019년 10월 xx일

의료기기 사이버보안 요구사항(기술보고서)

Medical Device Cybersecurity Requirements (Technical Report)

한국정보통신기술협회
Telecommunications Technology Association

기술보고서 초안 검토 위원회 바이오 인식 프로젝트그룹(PG505)

기술보고서안 심의 위원회 정보보호 기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위	표준번호
기술보고서(과제) 제안	한근희	건국대학교	교수	PG505 특별위원	TTAX.xx-xx.xxxx
기술보고서 초안 작성자	방지호	(재)한국기계전기 전자시험연구원	센터장	-	TTAX.xx-xx.xxxx
	정원석	(재)한국기계전기 전자시험연구원	전문위원	-	TTAX.xx-xx.xxxx
	안은주	(재)한국기계전기 전자시험연구원	연구원	-	TTAX.xx-xx.xxxx
	한근희	건국대학교	교수	PG505 특별위원	TTAX.xx-xx.xxxx
사무국 담당	김재웅	TTA	단장	사무국	
	문서연	TTA	선임	사무국	

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2019.12

서 문

1 표준의 목적

이 표준의 목적은 의료기기 개발시 고려해야 하는 사이버보안 보안요구사항을 설명하여 의료기기 개발자들이 안전하게 의료기기를 개발할 수 있도록 하는데 목적이 있다.
이 표준은 의료기기 사용간 발생할 수 있는 보안취약점 발생을 최소화하는데 기여할 것이다. 이에 따라, 의료기기의 안전성 및 신뢰성을 확보하여 안전한 스마트의료 서비스 활성화에 기여할 것으로 기대된다.

2 주요 내용 요약

이 표준은 국내·외 의료기기 표준[1][5][6][7]을 기반으로 알려진 위해요인 및 대응기능을 사이버보안 관점으로 분석하여 의료기기 사이버보안 요구사항을 제시한다.

3 인용 표준과의 비교

해당 사항 없음

Preface

1 Purpose

The purpose of this standard is to describe the cyber security requirements that should be considered when developing medical devices, so that medical device developers can safely develop medical devices.
This standard will help to minimize the occurrence of security vulnerabilities that can occur between medical devices. Accordingly, it is expected to secure the safety and reliability of medical devices, thereby contributing to the activation of safe smart medical services.

2 Summary

This standard addresses the medical device cybersecurity requirements based on Hazards and requirements provided by domestic and International standards for medical device [1][5][6][7].

3 Relationship to Reference Standards

None

목 차

의료기기 사이버보안 보안요구사항 기술보고서
Medical Device Cybersecurity Requirement(Technical Report)

1 적용 범위

이 표준은 스마트의료 서비스의 안전성 및 신뢰성을 제고를 위해 스마트의료 서비스 보안위협(TTAR-12.0026)을 기반으로 이에 대한 보안대책으로 의료기기 사이버보안 요구사항을 제시한다.

2 인용 표준

해당 사항 없음

3 용어 정의

3.1 비밀성(Confidentiality)
정당한(합법적인) 사용자가 아닌 사용자들은 컴퓨터 시스템상의 데이터 또는 컴퓨터 시스템 간에 통신 회선을 통하여 교환, 전송되는 데이터의 내용을 볼 수 없게 하는 기능

3.2 무결성(Integrity)
네트워크를 통해 송수신되거나 정보 시스템에 보관되어 있는 정보가 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보장하는 성질

3.2 가용성(Availability)
네트워크 또는 서버가 해커의 공격을 받더라도 사용자에게 지속적으로 서비스를 제공할 수 있는 능력

3.4 스마트의료(Smart Healthcare)
정보통신 기술을 활용하여 원거리에 의료정보와 의료서비스를 전달하는 모든 활동으로 원격의료의 동일 개념

3.5 바이오 정보
가공되지 않은 원본정보와 그로부터 추출되어 생성된 특징정보를 포함하여 지문, 얼굴, 홍채, 정맥, 음성, 서명 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말하며, 생체인식 정보, 유전정보, 건강관련 정보로 구분할 수 있음

3.6 위해 (HARM)
사람이나 동물에 대한 물리적 신체부상 또는 건강손상, 또는 재산이나 환경에 대한 손실.

3.7 위해요인 (HAZARD)
위해의 잠재적인 원천.

3.8 위해상황 (HAZARDOUS SITUATION)
사람, 재산 또는 환경이 하나 이상의 위해요인에 노출되는 상황.

3.9 의료용전기시스템 (MEDICAL ELECTRICAL SYSTEM), ME시스템 (ME SYSTEM)
ME기기가 하나 이상이면서 기능접속 또는 다중소켓아웃렛을 사용해서 제조자가 규정한 대로 서로 결합된 기기 아이템들의 조합

3.10 프로그램가능의료용전기시스템 (PROGRAMMABLE ELECTRICAL MEDICAL SYSTEM, PEMS)
한 개 이상의 프로그램가능전기부시스템(PESS)를 포함하는, ME기기 또는 ME시스템

3.11 프로그램가능의료용전기부시스템 (PROGRAMMABLE ELECTRIC SUBSYSTEM, PESS)
소프트웨어 및 인터페이스를 포함하는, 하나 이상의 중앙처리장치 기반의 시스템

3.12 IT-네트워크 (IT-NETWORK, INFORMATION TECHNOLOGY NETWORK)
두개 또는 그 이상의 통신노드 사이를 유선 또는 무선으로 연결하기 위한 통신노드 및 전달링크로 구성된 시스템 또는 시스템들.

4 약어

PEMS PROGRAMMABLE ELECTRICAL MEDICAL SYSTEM
PESS PROGRAMMABLE ELECTRIC SUBSYSTEM

5 의료기기 보안위협

5.1 스마트의료 서비스 모델의 의료기기 보안위협

스마트의료 서비스 보안위협 기술보고서[1]는 스마트의료 서비스 모델을 다음과 같이 서비스 사용자, 서비스 중개자, 서비스 제공자로 제시하고 있다.

(그림 5-1) 스마트의료 서비스 모델

스마트의료 서비스 구성요소 중 의료기기와 관련된 구성요소는 네트워크 기반의 서비스 사용자 및 서비스 제공자로 볼 수 있다.

<표 5-1> 스마트의료 서비스 구성요소

구간	명칭	역할	예시
서비스 사용자	센서	사용자의 건강정보 측정 및 획득	혈압센서, 혈당센서 등
	앱	사용자 센서로부터 획득한 건강정보를 유무선 통신 방식으로 인터넷을 이용하여 전송	스마트폰 앱 등
서비스 중개자	플랫폼	스마트의료 서비스 제공 및 정보 저장을 위한 플랫폼 제공	서비스 서버, 클라우드, 데이터베이스(DB) 등
	서비스	사용자에게 제공하는 스마트의료 기반 서비스	인증, 과금, 정보서비스(분석, 저장, 표출) 등
서비스 제공자	디지털병원	의료기관 내의 의료정보시스템들을 기반으로 각종 의료정보서비스들과 디지털 장비, 기기들을 서로 연동 및 운영하는 기반을 갖춘 의료기관으로, 사용자의 건강정보를 이용하여 진료행위 등을 수행	병원 등
	분석기관	사용자의 바이오정보를 다양한 기법을 이용하여 사용자에게 분석 서비스 제공	병리연구소, 건강증진센터, 기타 분석 기관/기업 등
	기타기관	사용자의 건강정보 및 바이오정보를 이용하여 서비스 제공	보험, 연금, 규제기관 등
네트워크	PAN/통신	센서와 앱이 설치된 단말을 연결하는 통신 수단 제공	Bluetooth, Zigbee, NFC, Wi-FI
	인터넷/ISP	스마트의료 서비스 각 구성 구간간의 정보 전송 서비스 제공	이동통신(3G/LTE등), Ethernet

의료기기는 서비스 사용자 및 서비스 제공자에 의해 사용되므로, 스마트의료 서비스 보안위협 기술보고서[1]에 기술된 스마트의료 서비스 및 관련 보안위협을 고려하여 다음과 같이 의료기기 관련 보안위협을 도출할 수 있다.

<표 5-2> 의료기기 주요 보안위협

구분		보안위협 및 관련 보안 요구사항
바이오 정보	생성	사용자의 의도와 상관없이 바이오 정보가 임의로 생성될 수 있는 보안위협 - 무결성 검증 : 실행파일 및 설정파일에 대한 무결성 검증
		바이오 정보가 잘못 생성될 수 있는 보안위협 - 무결성 검증 : 실행파일 및 설정파일에 대한 무결성 검증
	저장	권한이 없는 사용자가 바이오 정보에 접근할 수 있는 보안위협 - 인증 및 접근통제 : 사용자 인증, 권한이 있는 사용자에게 접근 허용
서비스 유형	의료기기 사용	사용자의 바이오정보를 잘못 생성할 수 있는 보안위협(예, 기능오류 등) - 무결성 검증 : 실행파일 및 설정파일에 대한 무결성 검증
		사용자의 바이오정보가 사용자 동의 없이 임의의 저장소에 저장될 수 있는 보안위협 - 무결성 검증 : 실행파일 및 설정파일에 대한 무결성 검증
		사용자의 바이오정보가 사용자 동의 없이 임의의 사용자에게 전송될 수 있는 보안위협 - 무결성 검증 : 실행파일 및 설정파일에 대한 무결성 검증
	의료기기 기반 의료서비스 이용	사용자의 바이오정보가 외부에 유·노출될 수 있는 보안위협(예, 기밀성 등) - 전송데이터보호 : 중요정보 전송시 안전한 암호화 채널(예, SSL/TLS) 또는 암호화(예, AES/SHA 등) 전송
		개인 바이오정보가 임의로 변조될 수 있는 보안위협(예, 무결성 오류 등) - 무결성 검증 : 중요 정보(예, 개인 바이오정보)에 대한 무결성 검증
		서비스를 제공받는 사용자가 해당 서비스를 이용할 수 없는 보안위협(예, DoS 공격 등) - 가용성 보장 : DoS/DDoS 대응
서비스 구성요소 (서비스 사용자)	사용자 센서	센서의 오동작으로 사용자의 스마트의료 정보가 잘못 생성되거나 생성되지 않을 수 있는 보안 위협 - 무결성 검증 : 실행파일 및 설정파일에 대한 무결성 검증
	어플리케이션 (앱)	안전하지 않은 플랫폼(예, 루팅, 탈옥 등)을 통해 개인의 바이오 정보가 변조될 수 있는 보안위협 - 루팅/탈옥 검사 : 루팅/탈옥 여부 확인을 통한 앱 서비스 통제 - 무결성 검증 : 중요 정보(예, 개인 바이오정보)에 대한 무결성 검증
		안전하지 않은 플랫폼(예, 루팅, 탈옥 등)을 통해 개인의 바이오 정보가 권한이 없는 사용자에게 전송 또는 유출될 수 있는 보안위협 - 루팅/탈옥 검사 : 루팅/탈옥 여부 확인을 통한 앱 서비스 통제 - 무결성 검증 : 실행파일 및 설정파일에 대한 무결성 검증
		단말기에 설치된 다른 어플리케이션에 의해 개인의 바이오 정보가 임의로 공유되거나 접근될 수 있는 보안위협 - 접근통제 : 권한이 있는 사용자에게 접근 허용

5.2 의료기기 관련 국제표준에 식별된 위해요인

의료기기와 관련된 국제표준[6][7]에서는 다음과 같이 알려진 위해요인 및 요구사항을 식별하고 있다.

<표 5-3> 알려진 위해요인 및 요구사항

항목		주요 위해요인 및 관련 보안 요구사항
위해요인	의료기기 소프트웨어 및 하드웨어 관련 위해요인	바람직하지 않은 피드백 [물리적 및 데이터의] (가능성에 포함되는 것 : 요구되지 않은 입력, 범위 외 또는 상반되는 입력 및 전자파 장해로부터 발생된 입력) - 입력데이터 검증: 시큐어코딩(SW개발보안)
		입수 불가능한 데이터 - 입력데이터 검증: 시큐어코딩(SW개발보안)
		데이터의 무결성 결여 - 무결성 검증 : 데이터 무결성 검증
		잘못된 데이터 - 입력데이터 검증: 시큐어코딩(SW개발보안) - 무결성 검증 : 데이터 무결성 검증
		데이터의 잘못된 타이밍 - 타임스탬프 : 신뢰할 수 있는 타임스탬프
		PESS 내 및 그들 사이의 의도하지 않은 상호작용 - 인증 : 상호인증
		제3자 소프트웨어의 알려지지 않은 측면 또는 품질 - 해당사항 없음
		제3자 PESS의 알려지지 않은 측면 또는 품질 - 해당사항 없음
		데이터 비밀에 대한 영향을 포함한 데이터 보안의 부족, 특히 부당변경에 대한 취약성, 기타의 프로그램 및 바이러스에 의한 의도하지 않은 상호작용 - 암호화 : 데이터 암호화 및 무결성 검증
		PEMS가 기본안전 또는 필수성능을 성취하기 위해 필요한 특성을 제공하는 IT-네트워크의 고장 - 해당사항 없음(임시 저장 후 재전송)
IT-네트워크 관련 위해요인 원인	IT-네트워크 시스템에서, 위해상황의 가능성이 있는 원인	데이터의 상실 - 백업
		부적절한 데이터 교환 - 인증 : 상호인증 - 입력데이터 검증: 시큐어코딩(SW개발보안)
		오류 있는 데이터 - 입력데이터 검증: 시큐어코딩(SW개발보안)

항목		주요 위해요인 및 관련 보안 요구사항
		- 무결성 검증 : 데이터 무결성 검증
		데이터의 부적절한 타이밍 - 타임스탬프 : 신뢰할 수 있는 타임스탬프
		데이터의 예기치 못한 취득 - 해당사항 없음
		데이터에의 무허가 접근 - 접근통제 : 사용자 인증, 권한이 있는 사용자에게 접근 허용
	IT-네트워크와 관련한 위해상황을 초래할 수 있는 환경이나 초기 이벤트	원격 서비스(네트워크에의 외부 접근) - 보안관리 : 원격접속 통제
		운영체제(운영체제의 호환성) - 해당사항 없음
		소프트웨어(운영체제, 어플리케이션 등)의 수정/업그레이드 - 업데이트 : 안전한 업데이트 보장(인가된 사용자 업데이터 기능 허용, 업데이트 파일 배포자 확인 후 적용 등)
		인터페이스 호환성(데이터 충돌, 데이터 형식) · 접속(하드웨어, 네트워크 커넥터의 수정) · 네트워크 인터페이스 기판(호환성) · 네트워크 프로토콜(DICOM, HL7 등) - 입력데이터 검증 : 시큐어코딩(SW개발보안)
		패킷 어드레스 구조 / 타이밍 - 입력데이터 검증 : 시큐어코딩(SW개발보안)
		정상적인 네트워크 부하 /대역폭 - 서비스거부 : DoS/DDoS 대응
		피크 네트워크 부하 - 서비스거부 : DoS/DDoS 대응
		데이터 매체(수명 및 검색 가능성) - 해당사항 없음
		보안(바이러스, 웜, 무허가 소프트웨어 갱신 또는 업그레이드) - 안티바이러스 설치, 안전한 업데이트 보장
		최대 허용가능 응답시간 - 해당사항 없음
		네트워크의 허용가능 고장률 - 해당사항 없음
		네트워크의 유효성(계획적 및 임시 보수) - 해당사항 없음
		정보 이동 중에 충실도의 손상을 발생시키는 인터페이스/포맷의 불일치 - 입력데이터 검증 : 시큐어코딩(SW개발보안)

항목		주요 위해요인 및 관련 보안 요구사항
		이질적인 네트워크 위상 - 해당사항 없음
의료기기 소프트웨어 요구사항	소프트웨어 요구사항	기능(functional) 및 능력(capability) 요구사항 (예) - 성능 (예, SW 목적, 타이밍 요구사항) - 물리적 특성 (예, 코드 언어, 플랫폼, 운영체제) - SW 수행되는 컴퓨팅 환경 (예, 하드웨어, 메모리 크기, 프로세싱 유닛, 시간존, 네트워크 구조) - 업그레이드 또는 다수 SOUP/다른 기기 버전과 호환성에 대한 필요 - 안전한 업데이트 보장
		소프트웨어 시스템 입력(inputs) 및 출력(outputs) (예) - 데이터 특성 (예, 숫자(numerical), 영숫자(alpha-numeric), 형식(format)) - 범위(range) - 한계(limits) - 디폴트(defaults) - 입력데이터 검증 : 시큐어코딩(SW개발보안)
		소프트웨어 시스템과 다른 시스템 간의 인터페이스 - 입력데이터 검증 : 시큐어코딩(SW개발보안)
		소프트웨어 기반의 알람(alarms), 경고(warnings), 운영자(operator) 메시지 - 보안경고
		보안(Security) 요구사항 (예) - 민감한 정보의 손상과 관련된 것 - 인증(authentication) - 인가(authorization) - 감사 추적(audit trail) - 통신 무결성 - 시스템 보안 및 멀웨어 보호 - 데이터 무결성 검증, 인증 및 권한관리, 감사기록 생성, 전송데이터 보호, 접근통제
		SW로 구현된 사용자 인터페이스 요구사항 (예) - 수동 조작 지원(support for manual operations) - 사람-장비 상호작용(human-equipment interactions) - 인적 제약들(constraints on personnel) - 집중된(concentrated) 사람의 주의가 필요한 영역

항목		주요 위해요인 및 관련 보안 요구사항
		- 입력데이터 검증 : 시큐어코딩(SW개발보안)
		데이터 정의 및 데이터베이스 요구사항 - 입력데이터 검증 : 시큐어코딩(SW개발보안)
		운영 및 유지보수 사이트(site) 또는 사이트들(sites)에서 배포된 의료기기 소프트웨어의 설치 및 수용 요구사항 - 안전한 업데이트 보장
		운영 및 유지보수 방법과 관련된 요구사항 - 안전한 업데이트 보장
		IT-네트워크 측면과 관련된 요구사항 (예) - 네트워크로 연결된 알람, 경고, 운영 메시지 - 네트워크 프로토콜 - 네트워크 서비스의 비 가용성(unavailability) 처리 - 보안경고, DoS/DDoS 대응
		사용자 유지보수 요구사항 - 안전한 업데이트 보장
		규제(regulatory) 요구사항 - 개인정보보호
의료기기 소프트웨어 관련 위험한 상황에 대한 잠재적 원인	위험 상황에 기여하고 있는 소프트웨어의 잠재적인 원인	부정확하거나 불완전한 기능 명세 - 설명서/매뉴얼 : 보안기능 사용 및 설정에 대한 명확한 서술
		식별 된 소프트웨어 항목 기능의 소프트웨어 결함 - 입력데이터 검증 : 시큐어코딩(SW개발보안)
		SOUP에서의 실패 또는 예기치 않은 결과 - 3rd party : 안전한 3rd party 제품/라이브러리 사용
		예기치 않은 소프트웨어 작동으로 이어질 수있는 하드웨어 오류 또는 기타 소프트웨어 결함 - 실행파일 및 설정파일에 대한 무결성 검증
		합리적으로 예측 가능한 오용 - 설명서/매뉴얼 : 보안기능 사용 및 설정에 대한 명확한 서술

6 의료기기 사이버보안 요구사항

6.1 스마트의료 서비스 보안위협 및 위해요인 대응 보안요구사항

5장의 스마트의료 서비스 보안위협 중 의료기기에 대한 보안위협과 의료기기 관련 알려진 위해요인 대응을 위해 도출된 보안위협은 다음 표와 같이 정리할 수 있다.

<표 6-1> 의료기기 주요 보안요구사항

유형	보안 요구사항
접근통제	사용자 인증
	상호인증
	권한관리
	권한이 있는 사용자에게 접근 허용
	원격접속 통제
오작동 대응	시큐어코딩(SW개발보안)
	보안경고
	감사기록 생성
	백업
	실행파일 및 설정파일에 대한 무결성 검증
	신뢰할 수 있는 타임스탬프
암호화	데이터 암호화
	데이터 무결성 검증
	중요정보 전송시 안전한 암호화 채널(예, SSL/TLS) 또는 암호화(예, AES/SHA 등) 전송
업데이트	인가된 사용자 업데이트 기능 허용
	업데이트 파일 배포자 확인 후 적용
안전한 운영환경	루팅/탈옥 여부 확인을 통한 앱 서비스 통제
	안전한 3rd party 제품/라이브러리 사용
	DoS/DDoS 대응
	안티바이러스 설치
	(설명서/매뉴얼) 보안기능 사용 및 설정에 대한 명확한 서술
규제사항	개인정보 보호

6.2 의료기기 사이버보안 요구사항

표6-1의 의료기기 주요 보안요구사항을 기반으로 의료기기 사이버보안 요구사항을 유형별로 다음과 같이 정의할 수 있으며, 추가로 고려해야 하는 사이버보안 요구사항을 정의하였다. 의료기기 개발시 다음 사이버보안 요구사항을 고려하여 안전하게 의료기기를 개발하는 것이 필요하다.

6.2.1 접근통제

(가) 사용자 인증 : 의료기기 설정 관리, 중요정보 접근 등 중요기능 수행전 사용자 인증을 수행해야 한다.
1) (아이디/비밀번호) 비밀번호를 소프트웨어(실행파일)에 하드코딩 되지 않아야 하며, 평문으로 저장되지 않아야 한다.
2) (아이디/비밀번호) 비밀번호가 유추하기 어렵도록 비밀번호 설정규칙(예, 최소 길이, 숫자/영문자/특수문자 조합 등)이 적용되어야 한다.
3) (아이디/비밀번호) 비밀번호 입력시 화면에 평문으로 노출되지 않도록 해야 한다.

(나) 상호인증 : 의료기기가 다른 의료기기 또는 서버와 중요정보(예, 바이오정보, 의료기기 제어명령어, 보안패치 파일 등)을 송수신하기 전에 상호인증을 수행해야 한다.

(다) 권한관리 : 최소권한의 원칙에 따라 불필요한 권한을 생성하지 않아야 하며, 사용자 역할(예, 의사, 간호사, 환자, 유지보수인원 등) 에 맞는 최소한의 권한을 부여해야 한다.

(라) 권한이 있는 사용자에게 접근 허용 : 사용자 인증을 통해 인가된 사용자의 권한을 확인하여 중요정보 등에 접근이 허용된 경우만 접근을 허용해야 한다.

(마) 원격접속 통제 : 원격접속을 허용하지 않아야 한다.
1) 불가피하게 필요한 경우 사용자 인증을 통해 인가된 사용자만 접근하도록 해야 한다.
2) 네트워크로 연결된 세션이 일정시간 동안 사용되지 않는 경우 세션이 자동으로 종료(또는 잠금) 되어야 하며, 재접속시 사용자 인증후 접속을 허용해야 한다.

6.2.2 오작동 대응

(가) 시큐어코딩(SW개발보안) : 입력데이터 검증을 통해 유효한 데이터를 기반으로 의료기기가 동작할 수 있도록 안전하게 개발하여야 한다.
1) 보안약점 및 보안취약점이 존재하지 않도록 안전하게 개발해야 한다.
2) 의료기기 소프트웨어의 경우, IEC 62304에 따라 의료기기 소프트웨어의 전체 개발생명주기를 대상으로 의료기기 소프트웨어의 안전등급을 기반으로 적절한 수준의 기능요구사항 분석 및 위험관리를 통해 안전하게 개발해야 한다.

3) 국내 시판을 목적으로 하는 의료기기의 경우, 식품의약품안전처의 '의료기기의 사이버 보안 허가·심사 가이드라인'을 준수하여 개발해야 한다.
4) 미국 등 해외수출을 목적으로 하는 의료기기의 경우, 미국 FDA의 'Content of Premarket Submissions for Management of Cybersecurity in Medical Devices' 및 'Postmarket Management of Cybersecurity in Medical Devices' 등 보안가이드라인을 준수하여 개발해야 한다.

(나) 보안경고 : 의료기기의 보안기능 오동작, 오류발생, 악성코드(바이러스) 감염 등이 발생한 경우 보안경고(예, 팝업, 이메일/SMS, 소리, 점등 등)를 생성해야 한다.

(다) 감사기록 생성 : 보안사고 등 추적을 위해 감사기록을 생성해야 한다.
1) 감사기록은 사건발생 일시, 유형, 사건을 발생시킨 주체의 신원(가능한 경우), 보안이벤트 내용 및 결과(성공/실패) 등을 포함하고 인가된 사용자가 검토할 수 있는 기능을 제공해야 한다.
2) 감사기록은 비인가된 삭제로부터 보호되어야 한다.

(라) 백업 : 중요정보(예, 바이오정보, 설정값 등)의 유실을 방지할 수 있도록 백업기능을 제공해야 한다.

(마) 무결성 검증 : 기기 동작에 영향을 주는 설정값과 주요 실행파일(프로세스)에 대해 무결성을 보장(예, 의료기기 구동시/주기적으로 무결성 점검 등)해야 한다.

(바) 타임스탬프 : 중요정보 생성, 감사기록 생성 등 데이터의 신뢰성 보장 및 발생시점 추적을 위해 신뢰할 수 있는 타임스탬프를 사용해야 한다.

6.2.3 암호화

(가) 전송데이터 보호 : 중요정보(바이오정보) 전송시, 중요정보의 기밀성 및 무결성이 보장되도록 안전한 암호화 채널(예, SSL/TLS) 또는 암호화(예, AES/SHA 등)하여 전송해야 한다.

(나) 저장데이터 보호 : 의료기기 내에 중요정보(바이오정보) 저장시, 중요정보의 기밀성 및 무결성이 보장되도록 안전하게 저장(예, 암호화, 난독화/분산 저장 등)해야 한다.

(다) 안전한 암호화 알고리즘 사용 : 전송/저장데이터 보호를 위해 암호화 알고리즘을 사용하는 경우, 국가정보원의 암호검증필제도의 요구사항을 준수하여 112bit 이상 강도의 안전한 암호알고리즘(국제표준으로 등재되어 검증된 암호알고리즘)을 사용하여야 한다.

(라) 안전한 암호키 관리 : 암호연산을 위해 암호키가 사용되는 경우, 암호키 생성, 배포, 사용, 저장, 폐기 등 암호키 생명주기를 고려하여 안전하게 암호키를 관리해야 한다.

6.2.4 업데이트

(가) 안전한 업데이트 : 안전한 업데이트를 보장해야 한다.

5) 인가된 사용자가 업데이트를 수행할 수 있도록 해야 한다.
6) 업데이트 파일의 신뢰성 확보를 위해 배포자 확인(예, 업데이트 파일 해쉬값 검사, 업데이트 파일의 전자서명값 검사 등) 후 업데이트를 적용해야 한다.
7) 업데이트 실패시 롤백 기능을 제공해야 한다.

6.2.5 안전한 운영환경

(가) 모바일 앱 서비스 통제 : 휴대용 단말기에 의료기기 소프트웨어(모바일 앱)이 설치되어 운영되는 경우, 루팅/탈옥 여부를 확인 후 설치 또는 구동되도록 해야 한다.

(나) 3rd party : 안전한 3rd party 제품/라이브러리를 사용해야 한다.

1) 최신 보안패치된 3rd party 제품/라이브러리를 사용해야 한다.

(다) DoS/DDoS 대응 : 의료기기의 서비스 가용성 보장을 위해, DoS/DDoS 대응기능이 적용되어야 한다.

1) 또는, 운영환경(보안장비 등)의 지원을 받아 DoS/DDoS 대응을 할 수 있다.

(라) 안티바이러스 : 의료기기의 안전한 운영을 위해 안티바이러스를 설치해야 한다.

(마) 서비스 : 불필요한 서비스는 제거하거나 비활성화해야 한다.

1) JTAG, UART, USB 등의 인터페이스를 통해 인가되지 않은 사용자가 접근할 수 없도록 비활성화(또는 제거) 시키거나 사용자 인증 후 제한적으로 접근을 허용해야 한다.

(바) 설명서/매뉴얼 : 의료기기의 오용을 방지하기 위해, 설명서/매뉴얼에 의료기기를 안전하게 사용할 수 있도록 보안기능 사용 및 설정에 대한 명확하게 서술해야 한다.

1) 주의사항 경우, 사용자가 명확하게 식별할 수 있도록 그림, 글씨크기, 글씨 색깔 등을 이용하여야 한다.

6.2.6 규제사항

개인정보 보호 : 의료기기를 통해 생성·처리되는 환자의 바이오정보는 개인정보로서 국내 개인정보보호법에 따라 안전하게 관리되어야 한다.

부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

해당 사항 없음

부 록 Ⅰ-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

해당 사항 없음

부 록 Ⅰ-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

해당 사항 없음

부 록 Ⅰ-4
참고 문헌

[1] TTAR-12.0026, ‘스마트의료 서비스 보안 위협(기술보고서)’, 2017.11.
[2] 방송통신위원회 및 한국인터넷진흥원, ‘바이오정보 보호 가이드라인’, 2017.12.
[3] 국가인권위원회, ‘바이오 정보 수집·이용 실태조사’, 2016년도 인권상황실태조사 연구용역보고서(발간번호: 11-1620000-000634-01), 2016.11.
[4] TTA정보통신용어사전, 2016.01., http://word.tta.or.kr/noticeView.do?public_no=35
[5] ISO 14971 : 2007, ‘의료기기 - 의료 기기에 대한 위험 관리의 적용’
[6] IEC 60601-1 : 2012, ‘의료기기의 전기·기계적 안전에 관한 공통기준 및 시험방법’
[7] IEC 62304 : 2015, ‘의료기기 소프트웨어-소프트웨어 라이프사이클 프로세스’

부 록 Ⅰ-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

해당 사항 없음

부 록 Ⅰ-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2019.10.xx	TTAx.xx-xx.xxxx	의료기기 사이버보안 요구사항	바이오인식 프로젝트그룹 (PG505)