TTA Technical Report

기술보고서

TTAR-xx.xxxx

(개)정일: 2018년 xx월 xx일

의료기관내 무선 의료기기 활용서비스의 보안참조 모델

Security Reference Model for Wireless Medical Devices in Healthcare Organization

표준초안 검토 위원회 바이오인식 프로젝트그룹(PG505)

표준안 심의 위원회 정보보호 기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	이병기	삼성의료원	교수	-	
	한태화	연세의료원	교수	-	
표준 초안 작성자	한태화	연세의료원	교수	-	
	김순석	한라대학교	교수	-	
	조영창	전자부품연구원	수석연구원	-	
	황인정	명지병원	책임연구원	-	
표준 초안 에디터	이병기	삼성의료원	교수	-	
	최민용	BSI Korea	실장	-	
	한근희	건국대학교	교수	-	
표준 초안 검토	김재성	KISA	수석	PG505 의장	
	전동훈	슈프리마	팀장	PG505 부의장	
	전명근	충북대	교수	PG505 부의장	
	한승진	경인여대	교수	PG505 간사	
	김학일	인하대	교수	PG505 특별위원	
	이필중	포항공대	교수	PG505 특별위원	
	정창신	TTA	팀장	PG505 위원	
사무국 담당	김재웅	TTA	단장	-	
	문서연	TTA	전임	-	

본 기술보고서 발간 이전에 접수된 지식재산권 확약서 정보는 본 기술보고서의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 기술보고서와 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 : 2018.xx

서 문

1 기술보고서의 목적

이 기술보고서의 목적은 무선 의료기기에 중점을 두며 헬스케어 제공자들이 보건의료 서비스 기관 내의 네트워크 환경에서 의료기기 도입 시 이에 대한 환경적 지원을 목표로 한다. 의료기기를 다루는 의사, 간호사, 의공기사 등의 사용자를 식별하는 것을 시작으로 사용자들과 시스템 간의 상호작용에 대한 정의, 위험 평가, 보안요건을 차등적으로 적용할 항목 검토 및 구현 사례를 제시하고자 한다.

2 주요 내용 요약

이 기술보고서는 체액 및 약물의 안전하고 정확한 관리를 위해 의료진들과 환자들의 안전한 무선 의료기기 사용법에 대해 제시한다. 위험 평가 및 분석, 논리적 설계, 개발 과정, 시험과 평가 및 보안 규제 매핑을 포함하며 보안과 관련된 업무에 대한 참조 솔루션을 제시하고자 한다.

3 인용 기술보고서와의 비교

3.1 인용 기술보고서와의 관련성

이 기술보고서는 NIST Special Publication 1800-8 문서 및 NIST Framework for Improving Critical Infrastructure Cybersecurity 문서를 기반으로 작성되었으며 인용 표준과의 관련성은 다음과 같다.

3.2 인용 표준과 본 기술보고서의 비교표

Framework for Improving Critical Infrastructure Cybersecurity	TTAR-xx.xxxx	비고
1. Framework Introduction	7. 보안 통제 맵	수정(내용 반영)
2. Framework Basics	7. 보안 통제 맵	수정(내용 반영)
3. How to Use the Framework	7. 보안 통제 맵	수정(내용 반영)
부록 I. Framework Core	7. 보안 통제 맵	수정(내용 반영)
부록 II. Glossary	-	제외(해당 없음)
부록 III. Acronyms	-	제외(해당 없음)

Preface

1 Purpose

This technical report has its objective on the emphasis of wireless medical device for the provision of assistance towards the healthcare providers within the organizational network. By starting with the identification of stakeholder who interacts with wireless medical device, it provides the definition of interaction between stakeholder and system, the review of risk evaluation and the example of implementation of security technologies.

2 Summary

This report provides the safe use of wireless medical devices among medical professionals and patients for the safe and accurate management of the device functions. It also includes the risk evaluation and analysis, logical design, development process as well as the mapping between standards and controls. It aims to provide the reference solution regarding the security tasks.

3 Relationship to Reference Standards

The standard is based on the draft version of NIST healthcare use case's draft documentation (SP 1800-8 document) and NIST's Framework for Improving Critical Infrastructure Cybersecurity. The relevancy with reference standard is the following.

Framework for Improving Critical Infrastructure Cybersecurity	TTAR-xx.xxxx	Note
1. Framework Introduction	7. Security control map	Revise(Inclusive)
2. Framework Basics	7. Security control map	Revise(Inclusive)
3. How to Use the Framework	7. Security control map	Revise(Inclusive)
Appendix I. Framework Core	7. Security control map	Revise(Inclusive)
Appendix II. Glossary	-	Eliminate(Not Applicable)
Appendix III. Acronyms	-	Eliminate(Not Applicable)

목 차

의료기관내 무선 의료기기 활용서비스의 보안참조 모델 (Security Reference Model for Wireless Medical Devices in Healthcare Organization)

1 적용 범위

본 기술보고서의 적용범위는 특정 기기구매의 기획부터 해체까지의 전 주기를 따른다. 전 주기 관리는 다음을 포함한다.

- 물품 조달
- 자산의 입고
- 사용을 위한 환경 준비
- 구성
- 사용
- 유지
- 오염 제거
- 장비 사용 종료

2 인용 표준

- NIST‘s concept and draft documentation for Special Publication 1800-8 (2017)
- NIST’s Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 (2014)

3 용어 정의

3.1 안전(Safety)

재산 또는 환경에 대한 손상이나 사람의 건강에 대한 물리적인 부상 또는 손상의 부적절한 위험이 없는 상태

3.2 제3자(Third Party) [1]

논의 중인 쟁점과 관련하여 관련 당사자들과 독립적인 것으로 인정된 개인이나 단체

3.3 위험(Risk)

위해 발생 확률과 이 위해의 심각도의 조합

3.4 위험 평가(Risk Assessment) [2]
위험식별, 위험분석, 위험산정으로 이루어진 전체 프로세스

3.5 인증(Authentication) [3]
어떤 실체에 주장된 특성이 정확하다는 것을 보장하는 것

3.6 이해관계자(Stakeholder) [2]
어떤 의사결정이나 활동에 영향을 미칠 수 있는, 이에 의해 영향을 받을 수 있는, 또는 이에 의해 영향을 받을 것으로 스스로 인지할 수 있는 개인이나 조직

3.7 위험 관리(Risk Management) [2]
위험에 관하여 조직이 지시하고 통제하는 협조 활동들

3.8 아키텍쳐(Architecture) [4]
시스템의 근본적인 조직으로 시스템 구성요소, 이들 간의 관계, 구성요소와 환경과의 관계, 시스템의 설계 및 진화의 지표가 되는 원칙

3.9 형상 관리(Configuration Management) [KS X IEC 80001-1:2010 2.4항]

3.10 접근 통제(Access Control) [3]
자산에의 접근이 기업 및 보안 요구사항을 토대로 승인 및 제한되도록 하는 수단

3.11 자산(Asset) [3]
조직에게 가치가 있는 어떤 것

비고 자산에는 다음을 포함해 많은 유형이 있다.

- 정보
- 컴퓨터 프로그램 등 소프트웨어
- 컴퓨터 등 물리적 자산
- 서비스
- 사람들, 그리고 그들의 자격, 기능 및 경험
- 명성, 이미지 등 무형 자산

3.12 가용성(Availability) [3]
공인 기관의 요구시 접근 가능하며 사용 가능한 성질

3.13 이벤트(Event) [2]
특정한 일련의 환경들이 발생한 것 또는 그 환경들이 변한 것

비고 1 한 이벤트는 하나 이상 발생할 수 있으며 그 원인은 몇 가지가 될 수 있다.
비고 2 이벤트는 발생하지 않은 어떤 것으로 구성될 수 있다.
비고 3 이벤트는 “사건” 또는 “사고”라고도 한다.

3.14 무결성(Integrity) [3]
자산의 정확성과 완전성을 보호하는 성질

3.15 생명주기(Life Cycle) [5]
개념(conception)으로부터 용도폐기(retirement)까지 시스템, 제품, 서비스, 프로젝트 또는 사람이 만든 개체의 점진적 변화(evolution)

3.16 보안(Security)
시스템의 보안성, 무결성, 가용성, 지속, 책임, 권한, 신뢰성을 정의, 달성, 유지하는 것과 관련된 모든 분야

3.17 감사(Audit) [6]
감사 기준의 만족 정도를 객관적으로 결정하기 위해 감사 증거를 확보하고 객관적으로 평가하기 위한 체계적이고, 독립적이며, 문서화된 프로세스

3.18 건강 데이터(Health Data) [KS X IEC/TR 80001-2-2:2015 3.7항]

3.19 모니터링(Monitoring) [KS X IEC/TR 80001-2-1:2015 3.21항]

4 시나리오

4.1 구성요소

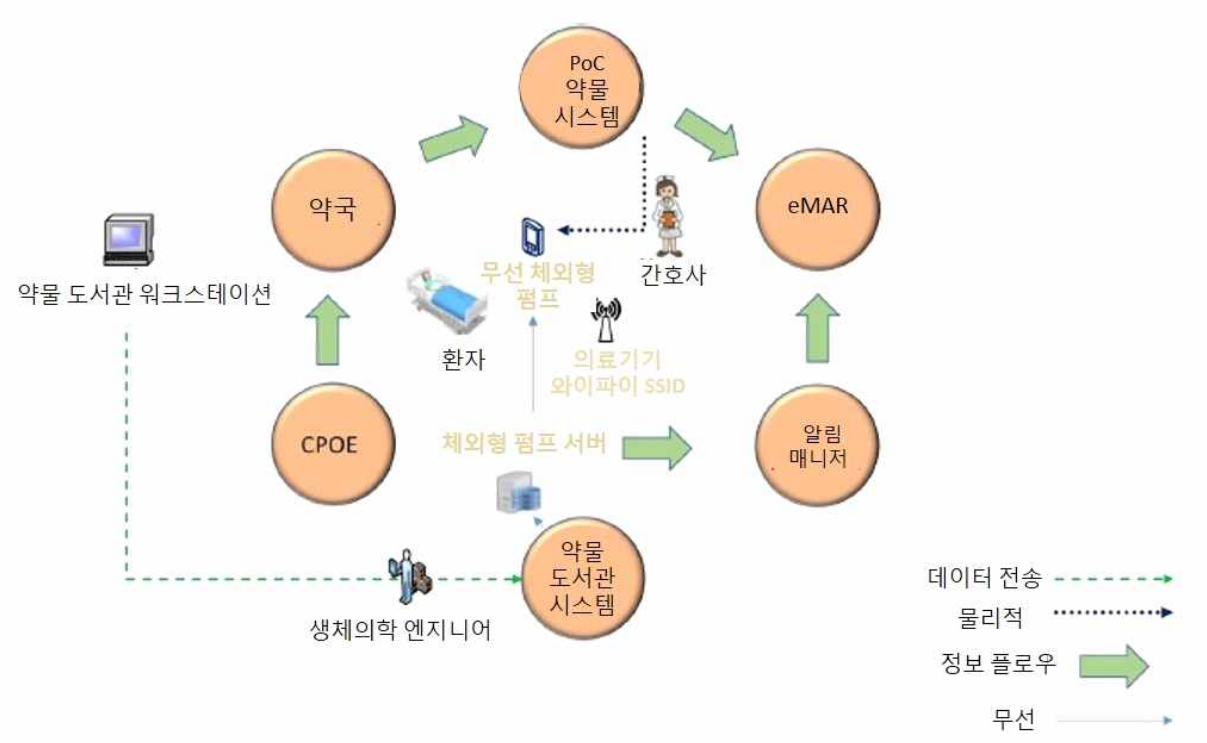
의료기기 사용사례는 기기와 상호작용하는 여러 명의 관계자들이 포함된다. 관계자들은 환경 내에서 환자의 케어를 전달하기 위하여 관련된 시스템과 상호작용한다. 하지만, 환경 내 좋지 않은 관계자들을 포함할 수도 있다. 관계자들은 다음과 같다.

- 환자
- 헬스케어 전문인
- 약사
- 특정 기기 판매 엔지니어
- 생체의학 엔지니어
- 의료정보 기술 네트워크 위험관리자
- IT보안 엔지니어
- IT네트워크 엔지니어
- 중앙 공급자
- 환자 방문객
- 해커

본 보고서의 시나리오는 관계자 및 각각의 관계자들이 의료 기기와 갖는 상호작용에 기반 하므로, 도출시나리오는 개발팀으로부터의 입력 정보를 기반으로 수정가능하다. 가장 일반적인 시나리오는 IT 네트워크 엔지니어가 무선 네트워크를 공급하는 것과 생체의학 엔지니어가 의료기기를 획득 및 네트워크에 연결하는 것에서 시작된다. 헬스케어 전문인은 환자의 사용을 위해 기기를 설정한다. 의사는 환자를 위해 약물을 처방하며 약사는 약물을 조제한다. 기기가 준비되고 설정된 후에는 헬스케어 전문인이 환자에게 사용한다. 지원활동은 특정 기기가 이용가능하고 안전한지 확인하는 IT 보안 엔지니어와 중앙 공급자가 제공한다. 환자 방문객은 그들 혹은 환자가 질문이나 걱정이 있을 시에 헬스케어 근로자와 간접적으로 상호작용할 수 있다. 해커는 특정 기기, 특정 기기 서버, 무선 네트워크, 임상시스템 및 병원 IT 시스템과 같은 다양한 영역을 통해 특정 기기를 공격할 수도 있다. 추가적인 활동은 일반적인 유지와 최종적으로 기기의 해체와 처리를 포함한다. 또한, 병원에서 제공하는 장비가 아닌 것은 병원의 네트워크에 접속되는 장비인 경우, 병원 내에 적절한 등록 및 허가절차를 거쳐야 한다.

4.2 구성 아키텍쳐

아래의 그림은 환자의 의료 기기와 직접적 혹은 간접적으로 상호작용할 수 있는 병원의 기술 인프라 내에서의 고차원적인 항목들을 나타낸다. 사용사례를 구현하는 실험환경의 개발과정 동안, 아래의 그림은 구성요소 플로우로 재정의 되며 실험환경에서의 물리적 아키텍처와 매핑 될 것이다.



(그림 4-1) 구성 아키텍처

그림 4-1의 구성 아키텍처는 다음의 사항을 포함한다.

- 환자
- 헬스케어 전문인
- 무선 의료기기
- 특정 기기 서버
- 무선 네트워크
- 알람 매니저
- 전자 약물 관리기록 시스템 (Electronic Medication Administration Record, eMAR)
- Point of Care 약물 시스템
- 약국
- 컴퓨터화된 의료진 주문 입력(CPOE)
- 약물 도서관
- 생체의학 엔지니어

4.3 의료 기기에 대한 이슈

다음의 난제는 실험연구 동안 다루어질 것이며 실용적인 가이드에서 문서화될 것이다. 프로젝트 동안 다른 난제들이 확인될 수도 있다.

- 접근 코드
- 접근 포인트 / 무선네트워크 구성
- 알람
- 자산 관리 및 모니터링
- 인증 및 자격인정
- 유지 및 보수
- 특정 기기 상이성
- 사용
- 응급사용

4.4 관리적 가치

이 사용사례는 무선 의료기기를 사용하는 헬스케어 기관에게 경영가치를 제공할 것이다. 또한, 의료기기 판매업자에게 취약점을 확인시켜줌으로써 참고 솔루션으로서 경영가치를 제공한다. 추가적인 가치는 다음과 같다.

- 에러 감소
- 사용성 및 정보보호와 보호된 네트워크 내 데이터간의 균형을 맞추는 보장된 의료기기 제공
- 환자 안전성과 보안 관련 기능간의 균형을 맞추는 의료기기 제공
- 의료기기의 보안성 향상을 통해 불필요한 기업 네트워크 보안 시스템 내 총 경비 감소
- 관리능력 접근과 확인을 개선하기 위해 기업 건강관리 네트워크 접근 및 작업하는 사용자 행동의 가시성 확대
- 기관의 명성에 미치는 부정적인 영향 감소
- 기관에 미치는 영향에 대해 고위급의 관리직 교육 지원
- 개발 시간 감축 및 제조사들의 수용성 증가

4.5 실제 사례

- 보안 시스템 위협 사례 1

2017년 5월 영국 내 많은 지역의 국민보건서비스(National Health Services, NHS) 산하 병원 40여개 곳이 WannaCry 공격을 받은 사례이다. 16개의 병원이 폐쇄되었으며 영국

언론기관인 BBC에 따르면 적어도 6,900건의 국민건강서비스 진료 예약이 취소되었으며 1만 9,000건의 예약이 랜섬웨어 공격에 영향을 받은 것으로 보도되었다. 원인으로는 병원 시스템 상당수가 마이크로소프트(MS)가 지원 중단한 윈도 XP 기반으로 운영되고 있다는 점으로 추정되어 향후 IT 담당 부서에서 주요 사이버 보안 업데이트를 시행할 계획이다.

- 보안 시스템 위협 사례 2

2018년 2월 26일자로 보고된 의료기관 내 발생한 의료기기 오작동 사고이며 환자의 사망으로 이어진 사례이다. FDA의 의료기기 관련 안전성 및 이상징후 보고 프로그램인 MedWatch 데이터베이스에 등록된 사건으로 Carefusion사의 인퓨젼 펌프 SW 오작동이 원인인 경우이다. 의료기관 내 활용되는 의료기기의 안정성 및 유효성 이슈가 대두된 사례이다.

- 의료기관 내 예방 사례

2018년 시카고 대학교 산하 생물과학 학과는 NIST의 사이버보안 프레임워크를 참고하여 학과 내 23개의 부서에 걸쳐 사이버보안 프로그램을 수정한 사례이다. 총 4개의 프레임워크 구현 과정을 통해 기존의 부서 내 관련 방침 및 절차를 미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)의 사이버보안 프레임워크의 항목과 부합화시켰다. 결과로는 사이버보안을 효율적으로 관리하게 되었으며 전 부서 차원에서의 의사소통을 실시하여 네트워크 보안의 중요성을 상기시킨 경우이다.

5 보안 요구사항

5.1 의료기기 및 관련 시스템

- 무선 의료 기기
- 특정 기기 서버
- 특정 기기 서버는 적어도 개발 시 사용된 무선 의료 기기 중 하나 이상과 상호호환이 되어야만 한다.

관련 표준:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule http://www.nist.gov/customcf/get_pdf.cfm?pub_id=890098

5.2 네트워크

- 확장된 서비스 세트 기능이 있는 엔터프라이즈급 무선 AP

관련 표준:

- FDA, Radio Frequency Wireless Technology in Medical Devices – Guidance for Industry and Food and Drug Administration Staff Document issued on August 12, 2013
  http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077272.pdf

- NIST SP 800-48 Rev 1, Guide to Securing Legacy IEEE 802.11 Wireless Networks
  http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf

- NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i
  http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf

- IEEE 802.1x, Port Based Network Access Control
  http://www.ieee802.org/1/pages/802.1x.html

- IEEE 802.11, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
  http://www.ieee802.org/11/

- 가상 개인 네트워크(VPNs)

관련 표준:

- NIST SP 800-114, User's Guide to Securing External Devices for Telework and Remote Access
  http://csrc.nist.gov/publications/nistpubs/800-114/SP800-114.pdf

- NIST SP 800-46 Rev 1, Guide to Enterprise Telework and Remote Access Security
  http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf

- NIST SP 800-77, Guide to IPsec VPNs
  http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf

- NIST SP 800-52 Rev 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

- 스위치/라우터와 같은 엔터프라이즈급 네트워크 구성요소

관련 표준:

❍ IEEE 802.1x, Port Based Network Access Control
http://www.ieee802.org/1/pages/802.1x.html

❍ IEEE 802.3, IEEE Standard for Ethernet
http://www.ieee802.org/3/

❍ IEEE 802.1Q, Bridges and Bridged Networks
http://www.ieee802.org/1/pages/802.1Q.html

❍ Internet Engineering Task Force (IETF) Request for Comments (RFC) 4301, Security Architecture for the Internet Protocol
https://tools.ietf.org/html/rfc4301

- 침입차단시스템

관련 표준:

❍ NIST SP 800-41 Rev 1, Guidelines on Firewalls and Firewall Policy
http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

- 어플리케이션 게이트웨이

관련 표준:

❍ NIST SP 800-95, Guide to Secure Web Services
http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf

- 침입 탐지 및 예방 시스템

관련 표준:

❍ NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS)
http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

5.3 IT 시스템

- 암호화 도구

관련 표준:

❍ NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices
http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

❍ NIST Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules
http://csrc.nist.gov/groups/STM/cmvp/standards.html

❍ NIST FIPS 197, Advanced Encryption Standard (AES)
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

• 패치, 암호 및 구성요소 관리

관련 표준:

❍ NIST SP 800-118, Guide to Enterprise Password Management (Draft)
http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

❍ NIST SP 800-40 Rev 3, Guide to Enterprise Patch Management Technologies
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

❍ NIST SP 800-53 Rev 4, Recommended Security and Privacy Controls for Federal Information Systems and Organizations
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

• 본인 확인, 접근 규제 및 자격인정

관련 표준:

❍ NIST SP 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure
http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf

❍ NIST SP 800-57 Part 1 - Rev 3, Recommendation for Key Management: Part 1: General (Revision 3)
http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf

❍ NIST SP 800-57 Part 2, Recommendation for Key Management: Part 2: Best Practices for Key Management Organization
http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf

❍ NIST SP 800-57 Part 3 Rev 1, Recommendation for Key Management: Part 3: Application-Specific Key Management Guidance
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf

- 자산/위험 관리 및 모니터링 시스템

관련 표준:

❍ NIST SP 800-30, Guide for Conducting Risk Assessments
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

❍ NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

❍ NIST SP 800-39, Managing Information Security Risk Organization, Mission, and Information System View
http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

❍ American National Standards Institute (ANSI)/Association for the Advancement of Medical Instrumentation (AAMI)/International Electrotechnical Commission (IEC) 80001-1:2010, Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsibilities and activities

❍ IEC Technical Report (TR) 80001-2-1, Edition 1.0 2012-07, TECHNICAL REPORT, Application of risk management for IT-networks incorporating medical devices - Part 2-1: Step-by-step risk management of medical IT-networks - Practical applications and examples

❍ IEC TR 80001-2-2, Edition 1.0 2012-07, TECHNICAL REPORT, Application of risk management for IT Networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls

❍ IEC TR 80001-2-3, Edition 1.0 2012-07, TECHNICAL REPORT, Application of risk management for IT-networks incorporating medical devices - Part 2-3: Guidance for wireless networks

❍ IEC TR 80001-2-4, Edition 1.0 2012-11, TECHNICAL REPORT, Application of risk management for IT-networks incorporating medical devices - Part 2-4: Application guidance - General implementation guidance for healthcare delivery organizations

❍ IEC TR 80001-2-5, Edition 1.0 2014-12, TECHNICAL REPORT, Application of risk management for IT-networks incorporating medical devices - Part 2-5: Application guidance - Guidance on distributed alarm systems

6 보안 통제 맵

표 6-1은 보안 요구사항과 관련하여 National Cybersecurity Center of Excellence(NCCoE)가 적용되는 제품의 보안 특성을 매핑한다. 중요한 인프라 사이버보안(Cybersecurity Framework, CSF) 향상, 다른 NIST 활동 및 미국 건강보험 양도 및 책임법(Health Insurance Portability and Accountability Act, HIPAA)와 같은 특수적인 분야 표준 향상을 위한 프레임워크를 활용한다. 이 초기 매핑은 표준 및 모범 사례의 실제 상황에서의 적용성을 나타내기는 하지만 이러한 특성들이 규제적 승인 및 인증에 대한 요구사항을 충족시킨다는 것을 의미하지는 않는다.

<표 6-1> 보안 통제 매핑

<table>
<tr><th colspan="2">특성 예(IEC TR 80001-2-2 기반)</th><th colspan="3">보안 프레임워크 및 모범 사례</th><th>도메인 표준 및 모범 사례</th></tr>
<tr><th>보안 특성</th><th>기능 예</th><th>CSF 기능</th><th>CSF 유형</th><th>CSF 하위유형</th><th>IEC TR 80001-2-2</th></tr>
<tr><td>자동 로그오프</td><td>헬스 데이터에 관해 승인되지 않는 접근 위험 감소. 시스템 혹은 workspot이 일정 기간 동안 작동되지 않을 경우, 다른 사용자에 의한 악용 예방. 기기/시스템 구성요소 데이터 및 설정에 대한 접근 예방</td><td>보호 (PR)</td><td>접근 규제 (PR.AC)</td><td></td><td>ALOF</td></tr>
<tr><td rowspan="6">감사 규제</td><td rowspan="6">헬스데이터를 가지고 누가 무엇을 하는지에 대한 신뢰성 있는 감사에 대한 통일된 접근법 정의를 함으로써 헬스케어 제공 기관의 IT 부서가 공공 프레임워크, 표준 및 기술을 사용하는 것에 대한 모니터링을 가능케 함</td><td>보호 (PR)</td><td>데이터 보안 (PR.DS)</td><td>PR.DS-4</td><td rowspan="6">AUDT</td></tr>
<tr><td rowspan="3">탐지 (DE)</td><td>문제 및 이벤트 (DE.AE)</td><td>DE.AE-2, DE.AE-3</td></tr>
<tr><td>보안의 지속적인 모니터링 (DE.CM)</td><td>DE.CM-1, DE.CM-3, DE.CM-7</td></tr>
<tr><td>탐지 과정 (DE.DP)</td><td>DE.DP-4</td></tr>
<tr><td rowspan="2">응답 (RS)</td><td>통신 (RS.CO)</td><td>RS.CO-2</td></tr>
<tr><td>분석 (RS)</td><td>RS.AN-1, RS.AN-3</td></tr>
</table>

승인	최소한의 데이터 및 특권에 대한 원칙에 따라 헬스데이터에 관한 접근 규제 제공 및 사용의도에 부합하여 HDO가 행하는 업무에 요구될 시에 필요한 기능만 작용되는 것	보호 (PR)	접근 규제 (PR.AC)	PR.AC-1, PR.AC-4	AUTH
			데이터 보안 (PR.DS)	PR.DS-5	
			정보 보호 과정 및 조치 (PR.IP)	PR.IP-3	
			보호적 기술 (PR.PT)	PR.PT-3	
			문제 및 이벤트 (DE.AE)	DE.AE-1	
			보안의 지속적인 모니터링 (DE.CM)	DE.CM-1, DE.CM-3	
보안 기능의 구성요소	HDO로 하여금 그들의 정책적 요구 그리고/혹은 워크플로우에 부합하도록 제품의 보안기능을 활용하는데 있어 판단하는 것을 지원	보호 (PR)	접근 규제 (PR.AC)	PR.AC-1, PR.AC-4	CNFS
			데이터 보안 (PR.DS)	PR.DS-5	
			정보 보호 과정 및 조치 (PR.IP)	PR.IP-3	
			보호적 기술 (PR.PT)	PR.PT-3	
		탐지 (DE)	문제 및 이벤트 (DE.AE)	DE.AE-1	
			보안의 지속적인 모니터링 (DE.CM)	DE.CM-1, DE.CM-3	
사이버보안 제품 업그레이드	일관적인 작업방식 생성. 현장서비스 스태프, 원격서비스 스태프 및 승인 받은 HDO 스태프들에 의한 제품 보안 패치에 대한 설치/업그레이드	보호 (PR)	정보 보호 과정 및 조치 (PR.IP)	PR.IP-1, PR.IP-3	CSUP
		보호 (PR)	유지 (PR.MA)	PR.MA-1, PR.MA-2	

데이터 백업 및 재난 복구	헬스케어 제공자는 데이터, 하드웨어 및 소프트웨어의 손상 혹은 파괴가 있을 시에 경영에 기여할 수 있도록 보장해야 함	확인 (ID)	자산 관리 (ID.AM)	ID.AM-5, ID.AM-6	DTBK
			경영 환경 (ID.BE)	ID.BE-1, ID.BE-4, ID.BE-5	
		보호 (PR)	데이터 보안 (PR.DS)	PR.DS-4	
			정보 보호 과정 및 조치 (PR.IP)	PR.IP-4, PR.IP-7, PR.IP-9, PR.IP-10	
			보호적 기술 (PR.PT)	PR.PT-4	
		탐지 (DE)	문제 및 이벤트 (DE.AE)	DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5	
		응답 (RS)	분석 (RS.AN)	RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4	
			응답 계획 (RS.RP)	RS.CO-1, RS.CO-2, RS.CO-3, RS.CO-4	
			향상 (RS.IM)	RS.IM-1, RS.IM-2	
			완화 (RS.MI)	RS.MI-1, RS.MI-2	
			응답 계획 (RS.RP)	RS.RP-1	
		회복 (RC)	통신 (RC.CO)	RC.CO-3	
			회복 계획 (RC.RP)	RC.RP-1	
응급 접근	보호된 헬스데이터에 대한 접근이 응급 혹은 재난상황일 경우 저장된 헬스데이터에 대해 즉각적인 것을 가능	보호 (PR)	접근 규제 (PR.AC)	PR.AC-1, PR.AC-4	EMRG
			보안의 지속적인 모니터링 (DE.CM)	DE.CM-1, DE.CM-3	

헬스데이터 비식별화	기기(어플리케이션 소프트웨어 혹은 추가적인 도구)의 환자의 신원을 알 수 있는 정보를 직접적으로 제거하는 기능. 팩토리로 보내기 이전의 데이터 정리. 헬스데이터 접근/노출 없이 원격 서비스가 가능하도록 하는 것, 인-팩토리 보관, 라벨링 및 교육	보호 (PR)	정보 보호 과정 및 조치 (PR.IP)	PR.IP-6, PR.IP-8	DIDT
헬스데이터 무결성 및 진실성	헬스데이터가 비승인된 방식으로 변경되거나 파괴되지 않게 하는 것. 비승인된 원격 접근 및 원격 프로그램으로부터의 보호를 포함하여 헬스데이터의 무결성을 보장하는 것	보호 (PR)	데이터 보안 (PR.DS)	PR.DS-1, PR.DS-2, PR.DS-6	IGAU
		탐지 (DE)	보안의 지속적인 모니터링 (DE.CM)	DE.CM-4	
			탐지 과정 (DE.DP)	DE.DP-3	
말웨어 탐지 및 보호	제품이 말웨어의 예방, 탐지 및 제거에 대해 효과적이고 일관적인 지원을 함으로써 규제, HDO, 사용자의 요구를 지원함. 보안에 있어서의 적절하고 심도 깊은 방어 접근법의 필수적인 단계임	보호 (PR)	정보 보호 과정 및 조치 (PR.IP)	PR.IP-7, PR.IP-12	MLDP
		탐지 (DE)	보안의 지속적인 모니터링 (DE.CM)	DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-4	
노드 승인	승인 정책은 지역 HDO IT 정책에 적용될 수 있도록 수용적이어야 함. 필요 시, 헬스데이터를 통신할 시에 노드 승인을 사용함	보호 (PR)	접근 규제 (PR.AC)	PR.AC-3, PR.AC-4, PR.AC-5	NAUT

사용자 승인	승인 정책은 HDO IT 정책에 적용될 수 있도록 수용적이어야 함. 이러한 요구사항은 헬스데이터에 대한 접근을 제공할 시에 사용자 승인을 요구하는 것은 논리적인 부분임. 기기, 네트워크 및 헬스데이터에 대한 접근을 규제하는 것과 반박 불가한 감사 과정을 생산하기 위함임. 이 기능은 명확하고 확실하게 네트워크, 기기 및 자원을 어떤 사용자가 접근하는지 확인하여야 함. 이 기능은 위에 언급된 응급/재난 상황과 일관성 있어야 함	보호 (PR)	접근 규제 (PR.AC)	PR.AC-1, PR.AC-3, PR.AC-4	PAUT
기기에 대한 물리적 잠금	허가 받지 않은 접근이 시스템 혹은 데이터 기밀성, 무결성 및 가용성을 위해하지 못하도록 함	보호 (PR)	접근 규제 (PR.AC)	PR.AC-2	PLOK
보안 가이드	시스템의 운영자 및 관리자들을 위한 보안 가이드가 이용 가능하도록 해야 함. 운영자 및 관리자들을 위한 추가적인 매뉴얼(의료기기 제조업자 판매 및 서비스를 포함한)이 바람직하며 이는 관리자들에 의해 행해져야 할 모든 관리적인 기능에 대한 이해를 하게함	이 부분은 운용 및 관리를 위한 것으로 여러 개의 영역에 매핑 될 수 있음	-	-	SGUD
시스템 및 어플리케이션 경화	의료기기 그리고/혹은 소프트웨어 어플리케이션에 대한 보안 규제 조정을 통해 사용의도를 유지하고 보안을 최대화시킴. 서비스 제거 등과 같은 포트 폐쇄를 통해 공격 벡터 및 종합적인 공격 표면 영역 최소화	보호 (PR)	정보 보호 과정 및 조치 (PR.IP)	PR.IP-1, PR.IP-2	SAHD

제품 전 주기 로드맵에서의 제3자 구성요소	목표는 제품의 전 주기 동안 구성요소 전 주기 영향을 적극적으로 관리하는 것임. 이러한 가정용 상업적 혹은 제3자 소프트웨어는 운영시스템, 데이터베이스 시스템, 리포트 생산자, 의료영상처리 구성요소 등을 포함함 (전제는 기존의 제품생산과정이 이미 하드웨어 구성요소의 진부화를 관리하는 것임). 제3자는 전용 전 주기와 지원 프로그램을 가진 보안취약 구성요소의 내부적 공급자를 포함함	확인 (ID)	경영 환경 (ID.BE)	ID.BE-1	RDMP
			위험 평가 (ID.RA)	ID.RA-1	
		보호 (PR)	인식 및 교육 (PR.AT)	PR.AT-3	
			유지 (PR.MA)	PR.MA-1	
			정보 보호 과정 및 조치 (PR.IP)	PR.IP-1, PR.IP-2, PR.IP-3	
		탐지 (DE)	보안의 지속적인 모니터링 (DE.CM)	DE.CM-6	
헬스데이터 저장 기밀성	MDM은 상품 및 제거될 수 있는 미디어에 저장된 헬스데이터의 무결성 및 기밀성에 대한 잠재적 위해를 완화시키는 기술적 규제를 행해야 함	보호 (PR)	데이터 보안 (PR.DS)	PR.DS-1, PR.DS-5	STCF
송신 기밀성	HDO의 송신된 헬스데이터 기밀성을 보장하기 위한 요구에 따라, 제조업자는 기기가 여러 개의 국내 표준 및 규정 (USA HIPPA, EU 95/46/EC, HBP 517 등)을 충족한다는 것을 제시하여야 함	보호 (PR)	접근 규제 (PR.AC)	PR.AC-2	TXCF
			데이터 보안 (PR.DS)	PR.DS-2, PR-DS-5	
송신 무결성	시스템/기기는 송신된 헬스데이터의 무결성을 보호함	보호 (PR)	접근 규제 (PR.AC)	PR.AC-2	TXIG
			데이터 보안 (PR.DS)	PR.DS-5	
		탐지 (DE)	보안의 지속적인 모니터링 (DE.CM)	DE.CM-4	
			탐지 과정 (DE.DP)	DE.DP-3	

부 속 서 A

관련 규정, 표준 및 가이드라인

A.1 개요

다음은 의료기기 및 헬스케어 분야에서의 사이버보안에 관한 표준, 가이드라인 및 지침 목록이다. 이는 사이버보안 모범사례에 관한 NIST, 국제표준 및 가이드라인을 포함한다.

규정

- FDA, Content of Premakret Submissions for Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff, Document Issued on October 2, 2014
  https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf

- FDA, Guidance for Industry – Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software, Document Issued on January 14, 2005
  http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf

- FDA, Infusion Pumps Total Product Life Cycle – Guidance for Industry and FDA Staff, Document Issued on December 2, 2014
  http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm209337.pdf

헬스케어/의료기기 특화 (국제표준화기관 [ISO]/IEC, IHE)

- Department of Homeland Security (DHS), Attack Surface: Healthcare and Public Health Sector
  https://info.publicintelligence.net/NCCIC-MedicalDevices.pdf

- Health Insurance Portability and Accountability Act (HIPAA) Security Rule
  http://www.hipaasurvivalguide.com/hipaa-regulations/hipaa-regulations.php

- Department of Health and Human Services (HHS) HIPAA Administrative Simplification Statue and Rules
  http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html

- Integrating the Healthcare Enterprise (IHE) Patient Care Device (PCD), Technical Framework White Paper
  http://www.ihe.net/Technical_Framework/upload/IHE_PCD_Medical-Equipment-Management_MEM_White-Paper_V1-0_2009-09-01.pdf

- IHE PCD, White Paper, Medical Equipment Management (MEM): Cyber Security
  http://www.ihe.net/Technical_Framework/upload/IHE_PCD_White-Paper_MEM_Cyber_Security_Rev2-0_2011-05-27.pdf

- IHE PCD, White Paper, MEM: Medical Device Cyber Security - Best Practice
  http://www.ihe.net/uploadedFiles/Documents/PCD/IHE_PCD_WP_Cyber-Security_Rev1.1_2015-10-14.pdf

- IHE PCD, Technical Framework, Volume 1, 10 IHE PCD TF-1 Profiles
  http://www.ihe.net/uploadedFiles/Documents/PCD/IHE_PCD_TF_Vol1.pdf

- IHE PCD, Technical Framework, Volume 2, 10 IHE PCD TF-2 Transactions
  http://www.ihe.net/uploadedFiles/Documents/PCD/IHE_PCD_TF_Vol2.pdf

- IHE PCD User Handbook - 2011 Edition - Published 2011-08-12
  http://www.ihe.net/Technical_Framework/upload/IHE_PCD_User_Handbook_2011_Edition.pdf

- Department of Veterans Affairs (VA), Medical Device Isolation Architecture Guide 2009
  http://s3.amazonaws.com/rdcms-himss/files/production/public/HIMSSorg/Content/files/MedicalDeviceIsolationArchitectureGuidev2.pdf

일반 사이버보안/위험관리 (ISO/IEC, NIST)

- NIST Cybersecurity Framework - Standards, guidelines, and best practices to promote the protection of critical infrastructure
  http://www.nist.gov/itl/cyberframework.cfm

- NIST SP 800-160, System Security Engineering, An Integrated Approach to Building Trusthworthy Resilient Systems
  http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf

- SANS 20 Critical Security Controls
  http://www.sans.org/critical-security-controls/

부 속 서 B

약어

FDA	U.S. Food & Drug Administration
NIST	National Institute of Standards and Technology
ALOF	Automatic Logoff
PR	Protect
AUDT	Audit Controls
DS	Data Security
PT	Protective Technology
DE	Detect
AE	Anomalies and Events
CM	Security Continuous Monitoring
DP	Detection Processes
RS	Respond
CO	Communications
AN	Analysis
AUTH	Authorization
AC	Access Control
IP	Information Protection Processes and Procedures
CNFS	Configuration of Security Features
CSUP	Cyber Security Product Upgrades
MA	Maintenance
DTBK	Data Backup and Disaster Recovery
ID	Identify
AM	Asset Management
BE	Business Environment
RP	Response Planning
IM	Improvements
MI	Mitigation
RC	Recovery
EMRG	Emergency Access
DIDT	Health Data De-Identification
IGAU	Health Data Integrity and Authenticity
MLDP	Malware Detection / Protection
NAUT	Node Authentication
PAUT	Person Authentication
PLOK	Physical Locks on Device
SGUD	Security Guides
SAHD	System and Application Hardening
RDMP	Third-Party Components in Product Lifecycle Roadmaps
RA	Risk Assessment
AT	Awareness and Training
STCF	Health Data Storage Confidentiality
TXCF	Transmission Confidentiality
TXIG	Transmission Integrity
OTS	Off-the-Shelf
DHS	Department of Homeland Security
HIPAA	Health Insurance Portability and Accountability Act
HHS	Department of Health and Human Services
IHE	Integrating the Healthcare Enterprise
PCD	Patient Care Device
MEM	Medical Equipment Management

부 록 I-1

지식재산권 확약서 정보

II-1.1 지식재산권 확약서(1)

해당 사항 없음

II-1.2 지식재산권 확약서(2)

해당 사항 없음

부 록 I-2

시험인증 관련 사항

II-2.1 시험인증 대상 여부

해당 사항 없음

II-2.2 시험표준 제정 현황

해당 사항 없음

부 록 I-3

본 기술보고서의 연계(family) 표준

II-3.1

해당 사항 없음

부 록 I-4

참고 문헌

[1] KS X ISO/IEC 27002:2014, 정보기술 - 보안기술 - 정보보호 경영을 위한 실무지침
[2] ISO Guide 73:2009, Risk management - Vocabulary
[3] KS X ISO/IEC 27000:2014, 정보기술 - 보안기술 - 정보보호 경영시스템 - 개요와 용어
[4] ISO/IEC 42010:2011, System and software engineering - Architecture description
[5] KS X ISO/IEC 12207:2009, 정보기술 - 시스템 및 소프트웨어 공학 - 소프트웨어 생명주기 프로세스
[6] KS Q ISO 9001:2009, 품질경영시스템 - 요구사항

부 록 I-5

영문기술보고서 해설서

II-5.1
해당 사항 없음

II-5.2
해당 사항 없음

부속서 A
해당 사항 없음

부속서 B
해당 사항 없음

부 록 I-6

기술보고서의 이력

판수	채택일	기술보고서번호	내용	담당 위원회
제1판	2018.09.	제정 TTAx.xx-xx.xxxx	의료기관내 무선 의료기기 활용서비스의 보안참조 모델	PG505