의료기기 정보보호 요구사항

한근희 TTA 바이오인식(PG505) 부의장, 고려대학교 정보보호대학원 연구교수

1. 머리말

개인, 기업, 국가 수준에서의 건강관리 비용이 증가하는 가운데, 일상생활에서의 건강한 습관이 만성질환을 예방할 수 있다는 인식이 확대되고 있다. 이와 같은 건강에 대한 인식 전환은 건강 및 의료기술의 발달에 힘입어 의료정보시스템(HIS, Health Information System)을 구축함으로써 원격에서 의료 전문가의 컨설팅을 받아 지속적으로 개인건강정보를 모니터링하는 수준으로까지 발전되고 있다.

의료기관에서는 오래전부터 정보통신기술(ICT, Information Communication Technology)과 의료기술이 융합·발전하고, 사물인터넷기술을 활용한 각종 IoT 기기를 활용하여 민감한 신체 건강정보를 포함한 개인건강정보가 집적되어 유통되는 네트워크 집속 기반의 의료기기가 폭발적으로 증가하고 있다.

HIS와 달리 의료기기(IoMD, Internet of Medical Things)는 규모와 종류, 입출력 데이터, 기술적 난이도 등에서 영역이 매우 다양하고, 인체에 위해를 가할 위험이 있으며, 민감한 정보와 밀접하게 연관되어 있으면서도 의료인과 일반인(환자, 간병인, 방문객, 기타 병원종사자 등)이 공유하는 경우가 많다.

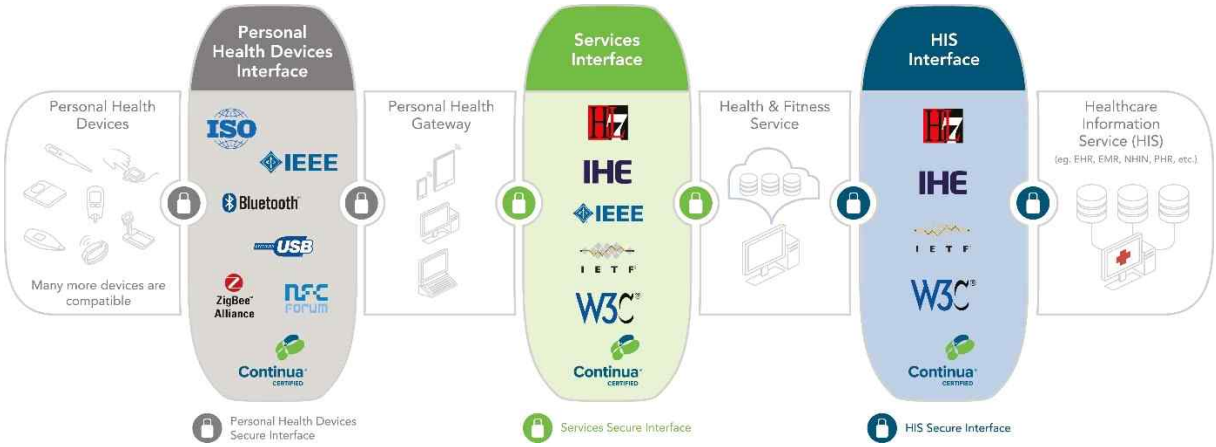
CT, MRI, 심전도기, 초음파기 등 글로벌 제조사의 고가 장비는 사용연한이 10~20년 이상인 경우가 많고 기기의 운용, 교체, 개선 등 작업을 제조사나 납품업체에서 수행하는 경우가 매우 많은 상황이다. 이러한 기기들을 운용하면서 기기 내에서 혹은 주변 장비에서 범용 운영체제(MS Windows)를 사용하는 경우가 많은데도 의료기기의 동작이 방해받을 우려로 인해서 기본적인 보안대책인 컴퓨터 바이러스 백신조차설치·사용하지 못하거나, 설치하였어도 최신 버전으로 업그레이드하거나 새로운 공격 유형에 대응하기 위한 패치 등을 설치하지 못하고 사용하는 경우가 다반사이다.

의료기관에 사이버침해가 발생할 경우 진료 서비스가 중단되거나 기기의 오작동으로 인하여 환자의 생명과 건강에 치명적인 손상이 발생할 수 있다. 의료정보시스템과 의료기기를 대상으로 한 사이버 위협과 공격 가능성이 증가하고 있어 정보보호의 필요성과 대응이 중요하게 되었다.

2. 의료기기 보안 위협

2.1 의료기기 구성

국제표준이나 사실표준에서의 의료기기 관련 적용 범위 분류 기준은 아래 [그림 1]과 같다. 의료기기(PHD, Personal Healthcare Device), 의료기기와 연결된 게이트웨이(Personal Healthcare Gateway), 유선·무선 네트워크, 각종 서버(인터페이스 서버, OIS, PACS 등)와 의료정보시스템(EHR, EMR) 및 의료정보 데이터베이스로 구성되어 있다.



[그림 1] IEEE PHD Cyber Security Working Group 정의

2.2 의료기기 사이버보안 위협 사례

2017년 5월 발생한 워너크라이(Wanna Cry) 랜섬웨어 공격으로 영국의 '국민건강서비스(NHS)' 산하 40여 개 병원 PC가 감염되어 모든 의료서비스가 중단된 사태는 의료기관의 정보보호 취약성과 위험성을 단적으로 보여주는 예라 할 수 있다.

FDA는 2017년 1월 세인트 주드 메디컬사의 인체 이식 심장박동기(implantable pacemaker)와 가정용 심장박동기 게이트웨이에서 심각한 보안 취약점을 발견했다고 'safety communication'을 통하여 발표하였다. FDA는 가정용 게이트웨이인 Merlin@Home을 원격에서 공격함으로써 체내 삽입된 심장박동기의 배터리를 순식간에 고갈시키거나 심박수를 위험 수준까지 급상승시키는 오작동을 발생시킬 수 있다는 사실을 확인하였다. 이미 전 세계적으로 수십만 대가 보급되었던 해당 제품에 대한 보안 경고는 의료기기를 겨냥한 사이버 공격의 위험성에 대한 경각심을 불러일으키는 계기가 되었으며, 2017년 말까지 50만 대에 대한 리콜 조치가 있었다.

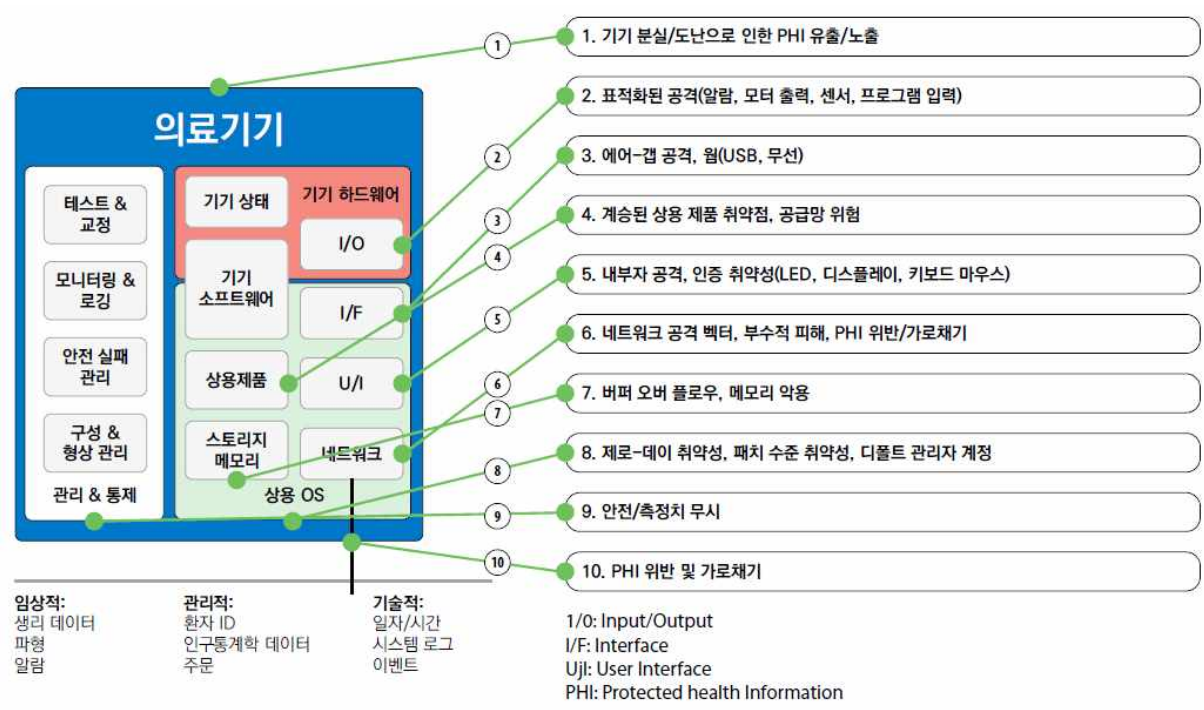
의료기관에서는 보안패치와 업데이트가 불가능할 정도로 노후한 의료기기와 네트워크 기반의 최첨단 의료기기 및 의료시스템이 공존하면서 운용되고 있다. 규모나 특성, 용도가 다양한 수만대의 의료기기들이 IT 담당자는 물론 의료기기 담당자의 관리 범위 밖에서 사용되고 있는 상황이다. 기기들이 어떻게 운용되고 관리되는지 현황 파악이 되지 않은 채로 사용됨에 따라, 가장 취약한 잠재적 사이버 공격표면(attack surface)으로서의 위험성을 내포하고 있다.

2.3 의료기기 보안 위협 요소

의료종사자들이 의료기기에 대한 사이버보안 위협 요소를 살펴보는 것은 중요하다. 아래 3가지 요소를 기반으로 의료기기에 대한 위험성을 고려해 보면 좋을 것이다.

(1) 의료기기가 병원 네트워크에 연결되어 작동하는가?
(2) 의료기기가 사이버침해를 당했을 경우, 그로 인하여 환자나 의료종사자들에게 직접적인 손상이 발생할 수 있는가?
(3) 의료기기에 혹은 의료기기를 통해서 얼마나 많은 보안 위협이 발생할 수 있는가?

위의 사례를 바탕으로 [그림 2]와 같이 선진 의료 현장에서 기본적으로 적용하고 있는 'IHE PCD(Patient Care Device) White Paper - Cybersecurity'에서 제시하는 보안위협 사례를 바탕으로 의료기기의 각 구성요소를 중심으로 위협 요소를 살펴서 대응하면 좋을 것이다.



[그림 2] 의료기기 구성과 사이버 보안 위협 요소 (IHE PCD White Paper를 재구성)

3. 의료기기 보안 요구사항

3.1 의료기기 분류

의료기기 분류의 가장 중요한 기준은 의료기기법상 기준 의료기기 품목 및 품목별 등급에 관한 규정이지만, 이 기준은 제품의 허가와 심사의 관점에서 규정되었기 때문에 진료대나 수술대, 주사기 등 재료나 용품들도 의료기기 분류에 포함되어 있다. 반면 본 표준에서 제시하는 분류체계는 네트워크에 접속 가능하면서 소프트웨어에 의해 작동되는 의료기기들을 대상으로 한다. 이런 의료기기들은 사이버 해킹 공격이 가능하기 때문에 보안과 개인정보보호 관점이

중요하게 처리되어야 할 필요가 있다는 차이점이 있다.

실제로 의료기관에서는 재료와 같은 소모성 의료기기는 자산으로 관리하지 않으며 기계나 장치들과 같은 의료기기를 자산(고정자산)으로 관리하고 있다. 고정자산으로 관리하는 의료기기도 의료기관의 규모에 따라 수천에서 수만 대에 달한다. 기구와 같은 의료기기를 소모성 자산으로 분류하여 관리하는 곳도 있는 것처럼 의료기관마다 의료기기를 분류하는 기준과 체계가 모두 달라서 어느 하나로 정의하기가 어려운 것이 현실이다.

또한 의료기기 소프트웨어(SaMD)와 같은 최첨단 의료기기 산업 발전으로 하드웨어 위주로 인식되던 기존 의료기기의 개념이 소프트웨어적 부분까지 확장되는 한편, 하나의 의료기기 내에서 여러 가지 기능 중 질병, 상해, 장애를 직접적으로 진단, 치료, 경감, 예방 및 보정하는 기능만을 한정하여 의료기기로 한정하려는 경향도 있다.

따라서 의료기관에서 의료기기를 담당하는 의공부서에서 관행적으로 분류 및 관리되고 있는 의료기기에 한정하여 고유한 기능과 사용목적에 따라 'TTAK.KO-12.0372 의료기기 정보보호 요구사항' 표준에서 <표 1>과 같이 8가지 종류로 분류하였다. 의료기기 소프트웨어(SaMD)의 의료기기로서의 기능과 사용 목적은 표의 1번~7번으로 분류가 가능하나, 보안과 관리의 관점에서 소프트웨어적인 특징이 존재하는 것을 고려하여 8번에 별도로 분류하였다.

<표 1> 의료기관의 의료기기 분류 체계

No.	분류명	고유 기능 (사용 목적)	대표 장비
1	LS (Life Support)	생명 유지 기기	인공호흡기, 심장충격기, 인슐린펌프, 심박조율기, 마취기, 신생아 보육기, 체외순환기 등
2	SR (SuRgical)	수술기기	수술내시경, 내비게이션, 로봇수술기, 전기(레이저)수술기 등
3	TR (TReatment)	치료 및 처치용 기기 (Physical Therapy and Treatment)	감마나이프, 선형가속기, 쇄석기, 운동치료기, 혈관조영장치, 혈액투석기, 레이저치료기, 약물주입기, 광선치료기, 전기자극치료기 등
4	PM (Patient Monitoring)	환자 감시 기기 (Patient Monitoring)	환자 감시장치(Patient Monitor), 중앙 감시장치, 분만감시장치(Fetal Monitor), 원격측정기(Telemetry), 심장혈류박출량감시기 (Cardiac Output Monitor), 뇌파 비디오 모니터(EEG Video Monitor), 심전도 모니터 (Holter Monitor), 맥박산소측정기(Pulse Oximeter), 생체신호감지 기기(NIBP Monitor) 등
5	DA (Diagnosis and Analysis)	진단 기기 (생체신호 측정, 분석 및 진단)	컴퓨터단층촬영기(CT), 심전도검사기(EKG), 초음파 검사기, 신체기능검사기기, X-ray, 자기공명영상장치(MRI), 감마카메라, 소화기내시경 등
6	LA (LAboratory)	검사 기기 (생체 정보 간접 측정 및 분석 기기(혈액, 조직 등))	동맥혈가스검사(ABGA), 감마계측기 (Gamma Counter), 혈구검사기(Hematology Analyzer), 효소면역장비(Immunoassay Analyzer), 혈당 측정기 등
7	AS (ASsistant)	의료 보조용 기기	자동약포장기, 현미경, 라벨부착기(Slide Labeller) 등
8	SW (SoftWare)	의료 기기 소프트웨어(SaMD)	CAD(Computer Aided Diagnosis), 3D 워크스테이션, 초음파 분석 소프트웨어 등

3.2 의료기기 보안 요구사항

의료기관에서 모니터링, 진단 진료, 치료, 처방 등에 사용하는 의료기기와 인체에 이식한 의료기기 및 개인의 건강 목적을 위해서 사용하는 기기 등 모든 의료기기에서 발생 가능한 사이버 보안 위협에 대응하기 위한 필수적인 정보보호 방안을 'TTAK.KO-12.0372 의료기기 정보보호 요구사항' 표준에서 아래와 같이 수립하였다.

(1) 시스템 하드닝
(2) OS, 펌웨어 업그레이드, 업데이트 및 보안패치
(3) 안티 바이러스 백신
(4) 백업
(5) USB 포트 관리
(6) 계정 관리
(7) 패스워드 관리
(8) 기기 인증
(9) 유지보수 정책
(10) 로깅과 모니터링
(11) 이동식 기기 관리
(12) 반출 및 폐기정책
(13) 보안사고 대응

표준 부록에서 보안 위협 요소와 보안 요구사항 간의 상호 연관 관계를 <표 2>에 나타내었다.

4. 맺음말

국내 의료계의 현실은 예산 및 인력 부족과 기술 지원 미비, 보안 인식 부재 등으로 정보보호 관점으로서의 전반적인 의료기기 실태조사가 부족하고 의료기관의 보안을 아우를 수 있는 일관성 있는 기술가이드나 지침이 부족한 형편이다.

본고에서는 의료기관에서 정보보호 관리 사각지대에 있는 의료기기의 보안 취약점을 파악하고 사이버보안 위협에 대한 대응방안을 제시함으로써 의료기기 관리와 관계된 이해관계자들, 특히 의공 담당자들의 정보보호 가시성(Visibility)과 대응력(Countermeasure)을 높이고자 하였다.

네트워크 기반 의료기기 및 의료시스템으로 인한 사이버보안 위험성에 대한 인식을 바탕으로, 의료보안 국제표준과 미국표준, 사실표준 등을 살펴서 한국 실정에 맞는 의료기기 보안 요구사항을 TTA 표준으로 개발하였다.

앞으로 의료기관의 의료기기 보안관리를 위한 분류체계 수립과 의료기기 보안가이드라인 개발을 통하여 지능화, 고도화되어 가는 사이버 공격에 대한 실용적 대응 방안 마련이 필요하다.

<표 2> 의료기기 보안 위협과 보안 요구사항 적용표

보안 위협	보안 요구사항											
	하드닝	업데이트	백업	USB	계정관리	패스워드	기기인증	유지보수	로깅/ 모니터링	이동식	반출 / 폐기	사고대응
보안기능 미비	√		√		√	√	√		√			
보안설정 미비	√		√		√	√	√		√			
초기설정 유지	√				√	√						
입력설정 오류	√											
잘못된 구매계약								√				
계정 공유					√							
권한설정 오류					√							
취약한 패스워드						√						
개인정보 유출	√			√		√	√	√	√	√	√	
악성코드 감염	√	√	√	√	√	√	√	√	√	√		√
오염된 USB				√				√				
미검증 S/W	√											
안티바이러스 미설치	√	√	√									
레거시 기기	√	√	√						√			
미검증 패치		√							√			
패치 미비		√										
응급 시 보안대책 미비					√				√			
외부 반출	√										√	
법규 미준수												√
모니터링 미실시									√			
로그데이터 유실	√		√						√			
백업 미비	√		√									√
폐기정책 미준수											√	
기기분실 및 도난	√		√							√		
기기인증 부재					√		√					
공유폴더 사용	√								√			

※ 본 연구는 정부(과학기술정보통신부, 산업통상자원부, 보건복지부, 식품의약품안전처)의 재원으로 범부처전주기의료기기연구개발사업단의 지원을 받아 수행된 연구임 (과제고유번호: 1711138615, KMDF_PR_20200901_0272)

[주요 용어 풀이]

• 의료정보시스템(HIS)

의료기관에서 일어나는 제반 업무를 정보통신기술(ICT)을 이용하여 관리하는 시스템. 의사나 간호사의 일상적인 기록 작업이나 계산업무부터 의사 및 간호사의 업무현황, 작업지시, 내원하는 고객(외래, 입원환자 등)의 건강정보, 과거 병명에서 현재 병의 진행과정, 치료 방법 등과 의료기관의 관리정보, 경영정보, 원무관리시스템 등의 병원 전체 운영을 위한 시스템을 포함하여 제반적인 모든 정보를 다룬다. [출처(3.6~3.7)] TTAK.KO-12.0305R1. 디지털 병원 정보보호 요구사항

• 전자의무기록(Electronic Medical Record, EMR)

병원 진료 지원 업무 중 의료 기록 업무를 전산 처리하는 것. 의료 기록은 수작업 처리가 많은데, 전자의무기록(EMR)은 종이 없는 기록 방식이라는 측면에서 광디스크나 CD로 기록을 보관하는 방법에서 발전하여, 현재는 의료 기기에 내장된 컴퓨터가 중앙의 주 시스템과 상호 연계되고, 원격 진료에 이용됨. 전자의무기록(EMR)으로 신속한 업무 처리와 인력 및 비용 절감의 효과가 있으며 기록의 신속한 전달과 활용이 가능하고 환자의 대기 시간 단축 등 서비스 향상의 효과도 있음 [출처(3.1~3.3, 3.5, 3.8)] TTA 정보통신망 용어사전

• 의료기기 소프트웨어 (SaMD, Software as Medical Device)

의료기기에 해당하는 목적으로 사용하기 위해 개발된 소프트웨어로 독립형 소프트웨어와 내장형 소프트웨어, 모바일 의료용 앱 등을 포함 [출처] 의료기기 소프트웨어 허가·심사 가이드라인, 식품의약품안전처 식품의약품안전평가원, 2018

[참고문헌]

[1] 의공사가 꼭 알아야 할 의료기기 보안, 한근희, 의공협회, 2019.

[2] 의료기기의 사이버보안 허가·심사 가이드라인, 식품의약품안전처 식품의약품안전평가원 의료기기심사부 첨단의료기기과, 2019.11

[3] IHE Patient Care Device(PCD) White Paper, Medical Equipment Management (MEM): Medical Device Cyber Security-Best Practice Guide rev.1.1, IHE, 14 Oct. 2015

[4] TTAK.KO-12.0372 의료기기 정보보호 요구사항, TTA, 2021.6.30.

[5] TTAK.KO-12.0305R1 디지털 병원 정보보호 요구사항, TTA, 2020.12.10

※ 출처: TTA 저널 제197호

(코로나 이슈로 각 표준화기구의 표준화회의가 연기・취소됨에 따라 TTA 저널로 대체합니다)