정 보 보 호 학 회 지
제25권 제3호, 2015. 6

국외 의료기기 보안위협 사례 및 보안 동향 조사

최 성 호*, 곽 진**

요 약

정보시스템 산업의 발전은 다양한 서비스 분야에서 많은 편의성을 증가시키고 있다. 또한, IT 산업이 IoT 환경으로 집중됨에 따라 다양한 서비스가 개발 되고 있으며, 다양한 IoT 제품들은 의료기기를 포함한다, 의료 환경에서는 네트워크에 연결되는 의료기기를 통해 환자를 위한 다양한 건강관리 서비스, 생명유지 서비스 등을 제공할 수 있다. 그러나 의료기기에 대한 보안 위협이 부각되면서, 인명 피해로 확산되는 것을 막기 위한 보안 관리 체계가 필요한 실정이다. 따라서, 본 논문에서는 의료기기에 대한 보안 현황을 조사하기 위해 의료기기 관련 보안 위협 사례를 분석하고, 미국, 유럽, 일본의 의료기기 정보보호 대책 및 국제 표준화 현황을 분석한다.

Ⅰ. 서 론

최근 IoT에 대한 관심이 급증함에 따라 다양한 IoT 서비스 분야의 연구가 이루어지고 있다. 그 중 의료 환경을 개선하고 환자를 위한 다양한 서비스를 제공할 수 있는 IoT 의료기기들도 다양하게 개발되고 있다. 이러한 의료기기들은 네트워크에 접속되어 원격의 진료 등의 서비스를 제공하는 등의 다양한 서비스를 제공할 수 있다. 하지만 이러한 의료기기는 환자에 대한 생명과 근접하게 연결될 수 있기 때문에 보안관리가 적절히 이루어져야 한다[1].

미국의 경우 의료기기에 대하여 기관별로 체계적인 프로세스를 구축하여 제품에 대한 안전성 및 보안성을 관리하고 있으며, 유럽의 경우 EU 지침에 따라 유형별 의료기기에 대한 지침을 만족하고 인증이 완료된 제품에 한하여 EU 회원국에 출시할 수 있도록 관리하고 있다. 일본의 경우 각종 산업회로부터 의료기기의 안전성 및 보안성을 위한 가이드를 제시하는 등의 의료기기 보안을 위한 관리를 시행하고 있다.

본 논문에서는 의료기기와 관련된 보안 위협 및 사고사례를 분석하고 미국, 유럽, 일본을 대상으로 국가별 의료기기를 위한 보안 현황에 대하여 조사 분석한다. 또한 추가적으로 의료기기 보안을 위한 국제 표준현황에 대한 분석을 시행한다.

본 논문의 구성은 다음과 같다. 2장에서 보안 취약점 및 사고사례를 분석하고 3장에서 국가별 의료기기 관련 보안 현황 및 의료기기 관련 보안 표준화 개발 현황을 분석한다. 마지막으로 4장에서 결론을 내린다.

Ⅱ. 보안 취약점 및 사고사례

의료기기는 환자의 상태를 체크하고 생명을 유지하는 등의 목적을 가지고 개발된 제품이다. 의료기기들은 악의적인 공격자에 의해 노출될 경우 환자의 생명과 직결되어 인명피해를 발생시킬 수 있다. 또한 최근 IoT에 대한 연구가 활발히 진행되며 다양한 헬스케어서비스를 제공하는 의료기기들이 개발되고 있다. 이러한 기기들은 기본적으로 네트워크에 연결되어 환자에게 서비스를 제공해 주는 환경을 제공한다. 다양한 의료기기들이 네트워크에 연결되어 보안위협이 증가할 것으로 예상된다.

본 장에서는 최근 발생한 의료기기에 대한 보안 사례를 및 보안 취약점에 대한 분석을 시행한다. 대표적인 사례로 심장 박동기 및 인슐린 펌프에 대한 해킹 사례가 있다. 해당 사례는 보안 컨퍼런스로부터 발표된 취약점 사례이며, 공격자가 원격의 취약점을 이용하여 의료기기에 대한 서비스를 조작하거나 전류를 통해 기기를

이 논문은 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2014R1A2A1A11050818).
* 아주대학교 컴퓨터공학과 (csha123@ajou.ac.kr)
** 아주대학교 정보컴퓨터공학과 (security@ajou.ac.kr)

〔표 1〕 보안 취약점 및 사고 사례

유형	사례	내용
취약점	· 심장박동기 / ICD 취약점	- 2008 년 Medical Device Security Center 의해 심장 박동기 / ICD (Implantable Cardioverter Defibrillator)에 전류를 흘려 기기를 정지 시키킬 수 있다는 연구 결과가 발표
	· 인슐린 펌프 해킹	- 2011 년 Black Hat에서 당뇨병 환자의 인슐린 펌프에 무선 기능의 취약점을 이용하여 투여되는 인슐린의 양을 외부에서 조작하는 등 '치명적인 공격'을 감행 할 수 있는 것을 발표
	· 인슐린 펌프 해킹(McAfee)	- 2011 년 McAfee FOCUS 11에서 인슐린 펌프에 대한 해킹 시연.
	· 맥박 조정기 해킹	- BreakPoint security conference 2012에서 맥박 조정기에 해킹에 대해 발표 - Black Hat 2013에서 맥박 조정기 해킹에 대한 발표가 진행될 예정 이었지만, 발표 되지 않음
	· Roche 만들어진 여러 의료기기에 사용되는 Symantec pcAnywhere 취약점 발견	- 여러 의료기기에 사용되는 Symantec pcAnywhere에 취약점이 발견
	· 생화학 자동 분석 장치에 이용되는 Oracle 소프트웨어의 취약점 발견	- 생화학 자동 분석 장치 COBAS INTEGRA 400/400 plus Analyzer에서 사용되는 Oracle 소프트웨어의 취약점. 장치의 데이터베이스에 대한 원격 액세스 취약점. FDA가 2013 년 1 월에 Enforcement Report를 발표
	· 의료기기의 하드 코드 된 암호	- 2013 년 6 월에 ICS-CERT에서 의료 디바이스 내부에 하드 코드 된 암호 에 대한 경고 발표 - 수술 장비와 마취 기계 인공호흡기 약물 주입 펌프 등이 관계하고 있으며, 기기에 따라 원격 조작이 가능함
사고사례	· Beth Israel Deaconess Medical Center에서 태아 모니터링 시스템 감염	- 고위험 임신 여성을 위한 태아 모니터링 시스템이 악성 코드에 감염되어 장치의 기능이 느려진 사례 보고
	· 네트워크 취약점을 통한 인터넷에서 의료기기에 접근	- ICS-CERT Monthly Monitor (2012 년 8 월호)에서 의료기기의 원격 모니터링에 대한 경고 발표 - 실제로 인터넷에서 액세스 할 수 있는 의료기기가 대학에서 발견
	· 가나자와 대학 부속 병원에서 의료기기의 바이러스 감염	- 가나자와 대학 부속 병원에서 각 부서에 개별적으로 도입한 시스템이 다른 종류의 기기에 바이러스 감염을 확산 시켜 진료 업무에 영향을 미침. 바이러스 검색 · 제거 도구 설치 후 바이러스 검사는 1000 건 정도의 악성 프로그램이 발견 된 장비도 발견 됨
취약점 / 사고사례	· 의료기기를 겨냥한 악성코드 발표	- 2013년 6월 FDA에서 네트워크에 연결된 의료기기가 악성 코드에 감염된 사례 발표 - 환자의 정보 및 모니터 시스템, 임플란트 장비에 무선으로 연결되는 모바일 기기를 겨냥한 악성 코드 발표

정지시키는 등 다양한 악의적인 공격이 가능하다는 것을 보여준 사례이다. 또한, Beth Israel Desconess Medical Center에서는 태아를 모니터링하는 시스템이 악성코드에 감염되어 의료기기에 대한 정상적인 활동을 방해하는 사례가 보고된 바 있으며, 인터넷 상에서 네트워크의 취약점을 이용하여 대학 내부의 의료기기에 접속할 수 있는 취약점이 발견된 사례도 있다. 이러한 사례들은 취약한 의료기기를 사용한 사람에게 공격을 시행할 경우 인명적인 피해를 발생시킬 수 있으며, 다양한 보안 문제를 발생시킬 것이다.

향후 네트워크를 통해 다양한 서비스를 제공하는 의료기기가 발전함에 따라 의료기기에 다양한 공격이 발생될 수 있으며, 생명과 연관된 공격 행위 및 의료데이터 유출에 대한 위협이 점차 증가할 것이다.

[표 1]은 다양한 보안 취약점 및 사고사례에 대한 내용을 정리한 것이다[2].

Ⅲ. 국가별 의료기기 관련 보안 현황 및 의료기기 보안 표준화 개발 현황 분석

3.1 미국의 의료기기 관련 보안을 위한 현황

미국의 의료기기에 대한 관리는 HHS(Department of Health and Human Services) 산하의 FDA(Food and Drug Administration)가 시행하고 있다.

FDA 및 DSH(Department of Homeland Security), GAO(Government Accountability Office) 등이 협력하여 의료기기에 대한 보안사고 및 위협, 대책방안에 대한 지침 및 권고를 연구하고 있다. 2013년 6월에는 FDA, DHS에서 의료기기 보안지침 및 권고사항을 공개하였다. 미국의 기관별 의료기기 보안을 위한 현황은 다음과 같다[2].

3.1.1 FDA

FDA는 미국식품의약국으로 의료기기에 대한 사이버 보안 관리 지침, 산업체 및 FDA 지원에 대한 지침(의료기기의 무선기술), FDA Safety Commucation 권고사항에 대한 문서를 공개하였다[2].

〔표 2〕 의료기기 사이버 보안 관리 지침

유형	내용
의료기기 제조업체	· 의료기기 관련 사이버 보안 위험 확인 · 사이버보안 사후대책을 위한 대응방안 및 복구방법 제공 · 의료기기별 보안관리 전략 구축 · 의료기기에 대한 무단 액세스 방지 기술 검토 · 접근제어기술을 통한 의료기기 액세스
의료기관	· 네트워크를 통한 무단 액세스 제한 · 악성코드에 방지를 위한 백신 및 방화벽 최신화 · 네트워크 모니터링 · 보안 패치 최신화 및 개별 네트워크 요소 보호 · 의료기기 사이버 보안 문제 발생시 제조업체에 대한 문의. 연락 불가시 FDA, DHAS ISC-CERT가 취약성 해결 지원

❒ 의료기기 사이버 보안 관리 지침

본 문서는 의료기기 제조업체가 사이버 보안 문제에 대한 지원을 목적으로 작성되었다. 주요 보안관련 내용은 [표 2]와 같다.

❒ 무선 주파수 의료기기, 산업 및 식약청 직원을 위한 지침

본 문서는 권고사항이며, 무선 의료기기의 설계, 테스트, 사용 및 유지 관리에 대한 고려사항을 제시하고 있다. 세부 사항으로 무선 기술을 통한 의료기기의 안전하고 효과적인 사용 방안에 대하여 기술하고 있으며, 설계, 테스트 및 무선 의료기기 사용에 대한 고려사항으로 보안관련 무슨 신호 및 데이터 보안, 유지보수와 같은 항목이 추가되어 있다.

❒ FDA Safety Communication(의료기기 및 병원 네트워크에 대한 사이버 보안)

본 문서는 의료기기에 악성코드 감염 등의 사이버 공격에 의한 기기 고장의 위험을 줄이기 위한 안전한 네트워크 환경을 구축할 수 있도록 하는 권고사항을 발표하는 커뮤니티이다.

❒ FDA 시스템 품질 규정

의료기기 소프트웨어 및 의료기기의 설계, 개발, 제조과정에서 보안에 대한 장애 안전모드 구현, 논리 및 물리적 보안의 정의 데이터 무결성에 대한 내용이 포함되어있다.

3.1.2 GAO

GAO는 행정기관과는 독립적인 의회로써, 행정기관의 업무 효율성에 대한 감시를 시행하는 역할을 한다. 해당 의회에서는 의료기기의 정보보안 대책에 대한 FDA에 권고사항을 제시하였다[2].

❒ 의료기기의 정보보안 대책에 관하여 FDA에 권고

해당 권고는 미세동기 등의 이식형 의료기기의 무선통신에 대한 보안위협을 제시하며 대책에 대한 권고를 나타내는 문서이다. 보안위협으로 무선통신으로 베터리 소모공격 등의 가능성을 나타내고 있다.

3.1.3 DOD

DoD(Department of Defense)는 STIG, DIACAP 문서를 공개하였으며 의료기기 개발에 지침으로 활용 가능하다[2].

❒ STIG(Security Technical Implementation Guide)

해당 문서는 컴퓨터 소프트웨어 및 하드웨어의 설치 및 유지보수에 대한 표준화된 안전한 방법과 구체적인 요구사항을 규정하고 있으며 의료기기에 적용 가능한 항목을 포함한다. 세부 내용으로는 제품 개발에 응용프로그램 구성 가이드, 위협 모델, 위험 관리, 암호화 기능, 데이터 보호 등의 제품의 보안을 위한 요소들이 포함되어 있다.

❒ DIACAP(DOD Information Asurance Certification and Accreditation Process)

정보시스템에 대한 리스크 관리가 적용되는 것을 보장하기 위한 프로세스를 규정한다. DoD와 군인 병원 입찰 요구사항을 토대로 정보시스템에 대한 시스템 라이프 사이클의 정보보증관리프로세스를 DoD 전체 표준의 정의한다.

3.1.4 HIMSS

HIMSS(Healthcare Information and Management SystemSociety)는 의료기기 제품 판매에 관한 보안 선언서인 MDS2를 공개하였다[2].

❒ MDS2 (Manufacture Disclosure Statement for Medical Device Security)

해당 문서는 의료기기 제조업자가 건강관리 사업자에게 의료기기에 대한 보안관련 정보를 제공하도록 하는 보안 선언서이다. 현재 해당기술은 표준화가 완료된 상태이다.

3.1.5 DHS

DHS(Department of Homeland Security)에서는 ICS-CERT Alerts 문서를 공개하여 의료기기 하드코드에 대한 문제점을 제시하였다[2].

❒ ICS-CERT Alerts

ICS-CERT Alerts는 의료기기의 하드코드 암호에 대한 위협 정보(ICS-ALERT-13-164-01)를 공개하였다. 세부내용은 많은 의료기기에서 하드코드된 키가 발견되었으며, 공격자는 이정보를 통해 의료기기에 대한 제어를 시행할 수 있다는 문제점을 지적하였다.

3.1.6 HITRUST

HITRUST 에서는 의료기기에 대한 모의 해킹을 통한 안전성을 분석하기 위한 CyberRX를 시행하고 있다[2].

❒ CyberRX

헬스케어 산업에 대한 모의 사이버 공격을 시행함으로써 의료기기에 대한 포괄적 공격 시나리오를 검증하고 공격 정보를 분석하여 공격정보 분석센터에 의한 정보 공유 및 활동에 대한 개선을 위한 것을 목적으로 하는 의료산업의 사이버관련 훈련이다[2].

3.2 유럽의 의료기기 관련 보안을 위한 현황

유럽의 의료기기에 대한 관리는 보건소비자총국(EC:European Commission,DGHealth and Consumers)에서 시행하고 있다. 또한 의료 제품규제내용은 유럽의 약품청(EMA)이 담당한다[1]. EPHA (European Public Health Alliance)는 유럽의 의료 및 건강분야의 정책을 감시하며 의료기기 사이버 보안에 대한 관리를 시행하고 있다.

EU에서는 이러한 기관들로부터 “새로운 접근법의 생각”에 의거한 3개의 지침이 제정되었다.

❒ 의료기기 지침

의료기기 제조업자가 CE 마크를 취득하고, 제품을 판매하기 위해 필요한 필수 요구사항을 규정하고 있다. 주요 내용으로는 요구사항을 충족하기 위한 기술 문서 및 설계 관련 문서에 대한 검증을 시행하고, EU Regulation 722/2012를 따르도록 규정하고 있다. 해당 문서는 위험 관리에 대한 내용이 포함되어 제품에 대한 안전성을 향상시키는데 목적으로 한다.

❒ 능동형 이식 의료기기 지침

치료목적의 이식 의료기기에 대한 기술 문서 및 설계 관련 문서를 검토하고 시스템에 대한 품질을 검증하도록 규정하고 있다. 또한, 기기에 대한 서비스 적합성 테스트를 진행하도록 규정하고 있다.

❒ 체외 진단용 의료기기 지침

체외 진단용 의료기기 지침은 의료기기에 대한 안전성에 대한 요구사항을 주로 규정하고 있으며, EU Regulation 722/2012를 따르도록 규정하고 있다.

EU 회원국은 모두 EU의 지침을 준수하기 위해 국내법을 제정해야 하며, 의료기기에 대한 평가는 회원국이 아닌 EU 인증기관에 의해 안전성이 평가되어야 한다. CE 평가마크를 받은 의료기기 제조업체는 유럽 경제지역(EEA:European Economic Area)내에서 의료기기를 판매할 수 있다[2].

3.2.1 CE 마크

유럽경제지역(EEA)과 터키, 스위스 등에서 의료기기를 판매하기 위해서는 모든 EU 회원국의 기준을 충족한 것을 증명하는 CE 마크가 표시되어야 한다. CE 마크는 의료기기뿐만 아니라 다양한 제품에 대한 안전, 건강, 환경보호에 대한 요구를 만족하는 평가 제도이다. 의료기기 종류에 따라 EU 지침으로 내세운 3가지의 지침을 만족해야 한다[2].

3.3 일본의 의료기기 관련 보안을 위한 현황

일본에서는 “의료정보시스템의 안전 관리에 대한 가이드라인”을 작성하는 등의 업무를 수행하는 경제 산업성을 중심으로 보안위원회를 설치하고 3개의 산업협회(JIRA,JAHIS, JEITA)등에 따라 의료기기보안관련 작업을 진행하고 있다.

일본 후생노동성에서는 의료정보시스템을 대상으로 한 지침으로 “의료정보시스템의 안전관리에 대한 가이드라인”을 공개하였으며, 의료기관의 책임자, 정보시스템 관리자, 시스템 도입 업체 등을 위한 보안관련 항목을 포함한 요구사항과 권장사항을 보여주고 있다. 또한 경제산업성에서 “의료정보를 위탁 관리하는 정보처리 사업자 안전 관리 지침”을 공개하고 총무성으로부터 “ASP·SaaS 사업자가 의료정보를 다루기 위한 안전관리 가이드라인”을 공개하였다[2]. 일본의 각 기관별 의료기기 보안을 위한 현황은 다음과 같다.

3.3.1 일본 화상의료시스템 공업회(JIRA)

화상의료시스템에 대한 기술 표준화 추진 및 품질에

〔표 3〕 국가별 의료기기 관련 보안 현황 정리

국가	기구	내용
미국	FDA	· 의료기기 사이버 보안 관리지침 공개 · 무선 주파수 의료기기, 산업 및 식약청 직원을 위한 지침 공개 · FDA Safety Communication 운용 - 의료기기 및 병원 네트워크에 대한 사이버 보안 등의 권고사항 제시 · FDA 시스템 품질 규정 제시
	GAO	· 의료기기의 정보보안 대책에 대한 FDA 권고
	DOD	· Security Technical Implementation Guid 공개 · DoD Information Asurance Certification and Accreditation Process 공개
	HIMSS	· Manufacture Disclosure Statement for Medical Device Security 공개
	DHS	· ICS-CERT Alerts 운용 - ICS-ALERT-13-164-01 발표
	HITRUST	· CyberRX 운용 - 의료기기에 대한 모의 사이버 공격 시행
유럽	EU	· EC, EPHA, EMA의 기관을 운용하며 EU 관리 하에 3개의 의료기기 지침 발표 · 의료기기 지침, 능동형 이식 의료기기 지침, 체외 진단용 의료기기 지침
일본	JIRA	· 제조업자에 의한 의료정보보안 개시 설명서 공개 · 원격 서비스 보안 가이드라인 공개
	JEITA	· 의료기기의 개발 및 보급 촉진 정책, 기술 과제 대응 등의 활동
	JAHIS	· JIRA와 합동으로 원격 서비스 보안 가이드라인, 제조업자에 대한 의료 정보보안 개시 설명서 작성

대한 안전성 등에 관한 연구를 진행하고 있다. 해당 기관에서는 다음과 같은 문서를 공개하였다[2].

❒ 제조업자에 의한 의료정보보안 개시 설명서

의료기기 제품에 대한 보안 관련 설명의 표준 서식이다. 해당 문서는 의료 영상 시스템에 대한 보안 관한 설명을 작성할 수 있도록 서식을 표준화한 것이다.

❒ 원격 서비스 보안 가이드라인

의료기관내의 정보 기기 및 시스템을 원격 보수할 수 있는 원격 서비스 보안 가이드라인이다. 세부 항목으로 원격 서비스에 대한 보안 요구사항, 기본 보안 방침, 표준 사례의 위험 평가, 위험 식별, 위험 분석 및 보안 대책 등에 대한 내용으로 구성되어 있다.

3.3.2 전자정보기술산업협회(JEITA)

의료기기의 개발 및 보급 촉진 정책, 기술 과제 대응 등에 대한 활동을 시행하며, 의료기기의 보안에 대한 검토를 담당한다[2].

3.3.3 보건의료복지정시스템공업회(JAHIS)

의약분야에서 의료기기에 대한 기술 규정, 안전성, 신뢰성 기술의 개발을 추진하고 JIRA와 합동으로 원격 서비스 보안 가이드라인 및 제조업체에 의한 의료정보 보안 개시 설명서를 작성하였다[2].

3.4 국제 의료기기 보안 표준 동향

의료기기에 대한 보안관련 국제 표준은 의료기기의 기능성 안전, 위험 관리, 품질 관리 등의 관점에서 안전성을 확보하기 위한 요구사항을 규정하고 있다. [표 4]는 주요 국제 표준의 개요를 정리한 것이다[2-6]

3.4.1 IEC 62304

해당 표준은 안전한 의료기기를 위한 소프트웨어 개발관련 프로세스를 정의한다. 일반 요구사항으로 의료기기에 대한 위험 관리 항목이 추가되어 있으며, 위험 분석, 평가, 통제하는 태스크에 대한 관리 방침, 관리 절차, 관리 방법을 체계적으로 적용하도록 요구하고 있다.

〔표 4〕 의료기기 보안 관련 국제 표준

표준	개요
IEC 62304	· 의료기기 소프트웨어 - 소프트웨어 수명주기 프로세스
IEC 80001-1:2010	· 의료기기를 포함한 IT 네트워크에 대한 위험 관리의 제공
ISO 14971	· 의료기기의 품질 경영 시스템 - 규제 목적을 위한 요구 사항
ISO 13485	· 의료기기 안전 규격
IEC 60601 시리즈	· 의료기기 - 의료기기 관련 규격 사항 정의
IEC 62366	· 의료기기에 대한 분석, 설계, 검증프로세스 등 규정(2015 업데이트)
IEC/CD 82304-1	· 의료기기를 포함한 제품 안전에 대한 일반적 요구사항

또한 보안 항목으로 권한이 없는 자에 대한 데이터 접근을 방지하는 등의 내용을 정의하고 있다.

3.4.2 IEC 80001-1:2010

의료기기 대부분이 네트워크에 연결된 개별 의료기기를 직접적으로 관리하기 어려운 환경에서 IT 네트워크에 대한 위험관리를 수행하여 안전한 형태로 시스템을 관리하기 위한 요구사항을 나타낸다.

3.4.3 ISO 14971

의료기기 제조사에서 체외 진단용 의료기기를 포함한 여러 의료기기들에 대한 위험을 식별하고 위험의 추정 및 평가를 시행하며, 위험을 제어하고 모니터링 하는 방법에 대하여 규정하고 있다.

3.4.4 ISO 13485

의료기관이 사용자에 대한 요구사항 및 의료기기 관련 서비스에 적용되는 요구사항을 지속적으로 충족시키고 의료기기에 대한 안전 규격을 규정하여 품질경영시스템에 대한 요구사항을 정의 한다.

3.4.5 IEC 60601 시리즈

의료기기에 대한 안전성 시험 등에 관한 요구사항을 규정한다. 2개의 시리즈로 구성되어 IEC 60601-1에서는 의료기기에 대한 일반적인 규격을 정의하고 IEC 60601-2에서 X-선 검사장치 등의 개별 안전성 규격을 정의한다.

3.4.6 IEC 62366

의료기기의 사용성에 관한 요구사항을 규정하여 의료기기 개발자에 대한 안전성 및 유용성에 대한 분석, 설계, 검증, 검증 프로세스를 정의하고 있다. 해당 표준 문서는 2015년 2월 업데이트가 완료되었다.

3.4.7 IEC/CD 82304

소프트웨어에 대한 국제 표준으로 임베디드 소프트웨어가 아닌 의료 소프트웨어 제품 규격으로 검토가 진행 중이며 현재 드래프트 단계이다.

Ⅳ. 결 론

본 논문에서는 의료기기에 대한 보안 관련 위협 사례를 분석하고 미국, 유럽, 일본에 대한 의료기기 보안을 위한 현황을 분석하였다. 의료기기는 환자에 대한 생명과 직접적으로 연결되어 있기 때문에 각종 위험으로부터 안전하게 관리되어야 한다. 국외에서는 의료기기에 대한 보안을 위해 기관별로 체계적인 관리프로세스를 구성하고 의료기기의 안전을 위한 활동을 시행하고 있다. 또한 의료기기에 대한 안전성을 위해 별도의 가이드라인을 공개하고 있으며, 국제표준으로 보안요구사항을 포함한 다양한 보안관련 표준화가 진행되고 있다.

향후 의료기기에 대한 보안 관리를 위한 체계적인 프로세스를 적용하여 향후 의료 IoT 환경으로 발전하였을 때 의료기기에 대한 보안을 위해 체계적인 프로세스 개발에 주력해야 할 것이다.

참 고 문 헌

[1] KISA, “국내외 지식정보보안 산업 동향”, 2012.08

[2] IPA, “의료기기의 정보보안에 관한 조사”, 기술본부보안센터, 2014.04

[3] 오영배, 정영은, 신석규, “의료기기 소프트웨어 기능 안전성 기술 및 표준화 동향”, TTA Journal. Vol.147, pp.87-94, 2013

[4] IEC 80001-1,“Application of risk management for IT-networks incorporating medical devices -- Part 1: Roles, responsibilities and activities”, 2010

[5] IEC 62366-1,“Medical devices -- Part 1: Application of usability engineering to medical devices”, 2015

[6] IEC/CD 82304-1,“Health software -- Part 1: General requirements for product safety”, 2014

〈저 자 소 개〉

최 성 호 (Seong-Ho Choi)
학생회원

2013년 2월 : 순천향대학교 정보보호학과 졸업
2013년 3월~2014년 2월 : 순천향대학교 정보보호학과 석사과정
2014년 3월~현재 : 아주대학교 컴퓨터공학과 석사과정
관심분야 : 네트워크 보안, 클라우드 컴퓨팅 보안, 응용시스템보안, 개인정보보호

곽 진 (Jin Kwak)
종신회원

2000년 8월 : 성균관대학교 학사
2003년 2월 : 성균관대학교 석사
2006년 2월 : 성균관대학교 박사
2006년 4월~2006년 11월 : 일본 큐슈대학교 방문연구원
2006년 8월~2006년 11월 : 일본 큐슈시스템정보기술연구소 특별연구원
2006년 11월~2007년 2월 : 정보통신부 정보보호기획단 개인정보보호팀 통신사무관
2007년 1월~현재 : 한국정보기술융합학회 이사
2007년 3월~2015년 2월 : 순천향대학교 정보보호학과 교수
2008년 1월~현재 : 한국정보보호학회 논문지편집위원
2008년 1월~현재 : 한국정보보호학회 이사
2008년 4월~현재 : 한국인터넷정보학회 논문지편집위원
2008년 12월~현재 : 정보통신산업진흥원 기술평가위원
2010년 3월~현재 : 조달청 기술평가위원
2011년 1월~현재 : 한국정보처리학회 이사
2011년 1월~현재 : JIPS 논문지 편집위원
2011년 7월~현재 : 지식경제부 지식경제기술혁신평가단 위원
2012년~현재 : 한국암호포럼 운영위원
2012년~현재 : 한국방송통신전파진흥원 평가위원
2013년~현재 : 교육부 정책자문위원
2013년~현재 : 금융보안연구원 보안기술 자문위원
2013년~현재 : 금융감독원 인증방법평가위원
2015년 3월~현재 : 아주대학교 정보컴퓨터공학과 교수
관심분야 : 자동차 보안, 암호프로토콜, 응용시스템보안, 클라우드 컴퓨팅 보안, 개인정보보호, 정보보호제품평가