http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.24, No.1, February 2019, pp.17-27
https://doi.org/10.7838/jsebs.2019.24.1.017

# 스마트 의료환경에서 보안체계 구축을 위한 이해관계자 역할 분석

## An Analysis on Role of Stakeholders for Security System in Smart Healthcare Environment

김양훈(Yanghoon Kim)*, 정원후(Wonwho Jeong)**

### 초 록

4차 산업혁명의 몰입과 함께 산업의 전반적인 흐름이 ICT 기반의 비즈니스 환경으로 나아감에 따라 의료산업에도 환경변화가 일어나고 있다. 공공재 성격을 지닌 의료산업에서는 의료서비스의 신뢰성과 지속성을 요구하고 있으나, 스마트 환경으로 전환하기에 기존 시스템들의 호환성, 확장성 문제로 인하여 보안에 대한 도입이 늦춰지고 있다. 이에 따라, 본 연구에서는 신속하게 스마트 의료환경에서 보안체계를 구축하기 위하여, 필요로 하는 보안기술을 도출, 분석하고 도입하기 위한 이해관계자들이 관심을 가져야하는 부분과 역할에 대하여 설계하였다. 이를 통하여 의료보안체계를 구축하기 위한 이해관계자들의 다차원적인 노력에 대하여 확장성 있는 가능성을 제시하였다.

### ABSTRACT

With the occurrence of the 4th Industrial Revolution, environmental change is happening in the healthcare industry as overall flow of Industry heads to ICT-based business environment. Healthcare Industry, which has the characteristic of public goods, is requiring a reliability and continuity of healthcare industry, however, the introduction of security is being delayed due to the problem of compatibility and extendability of existing system. Accordingly, in this research, we have built a section and role for stakeholders to be concerned in order to induce, analyze and introduce a needed security technology for rapidly building a security system in a smart healthcare environment. We have suggested a possibility of extendability regarding a multi-dimensional effort of stakeholders for establishing a healthcare security system.

**키워드** : 의료산업, 의료정보 보안, 스마트 의료보안 플랫폼, 병원정보시스템
Medical Industry, Smart Healthcare Security Platform, Hospital Information Systems, Medical Industry Stakeholders

이 성과는 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2018R1C1B5046760).

* First Author, Department of Industrial Security, Far East University(yhkim@kdu.ac.kr)
** Corresponding Author, Department of Convergence Security, Chung-Ang University(nugudosa@naver.com)
Received: 2018-11-27, Review completed: 2018-12-26, Accepted: 2018-12-29

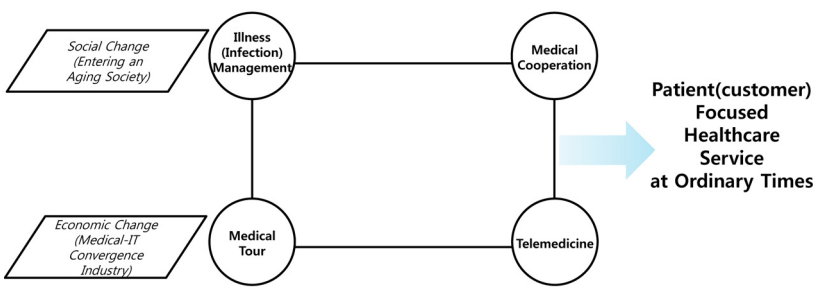
## 1. 연구배경

4차 산업혁명의 도래와 함께 융합서비스 환경이 전반적인 산업에 구축되면서 차별적인 비즈니스 환경 및 4차 산업기술에 따른 융복합적의 새로운 보안위협이 발생하고 있다[7, 18]. 의료산업 내 환경 또한 인프라로써의 ICT 구축이 진행되면서 ICT 인프라 내 정보유출 등과 같은 역기능으로 인해 비즈니스 환경을 고려한 특화된 보안기술 및 역할이 중요한 화두로 떠오르고 있다. 질병의 방지와 건강증진을 위한 진단, 치료, 재활과정에서 사용되는 의료기술 및 서비스, 의료기기, 의약품, 의료조직 체계 등을 포함하는 산업은 의료산업으로 정의되며[1] 최근 발생되고 있는 사회적 환경변화에 따라 의료산업의 경계와 영역이 확대되고 있다.

의료산업은 공공재 성격을 지닌 고부가가치 산업으로써 의료서비스 자체에 대한 신뢰성은 매우 중요한 가치로 여겨지며 사회적 고령화와 경제적 산업융합으로의 환경변화에 따라 언제 어디서나 지속가능한 상시의 의료서비스에 대한 요구가 증가하고 있다[8].

스마트 의료서비스에서는 병원에서 받은 MRI CD에 심어진 악성코드가 발견되고, 심박조절기 등의 의료장비에 내장된 소프트웨어에 악성코드가 침입한 등의 보안위협 사례가 발생할 수 있다[5]. 그러나 국내 의료기관의 보안현황 실태를 조사한 결과 국내 중소형 의료기관은 국내 의료기관의 절대다수를 차지하고 있음에도 불구하고 보안이 매우 미흡한 것으로 나타나 개발될 기술의 실중 범위를 확대할 필요가 있다. 특히 중소 의료기관은 규모가 작을수록 기술적인 보안이 부재하며 보안 인식이 낮은 중소형 의료기관의 보안 수준 제고에 대한 시급성을 강조할 필요가 있는 것으로 나타났다. 이에 따라 특화된 보안관리 모델 및 플랫폼이 필요한 것으로 나타났으며 전통적인 의료산업 보안기술 적용의 한계를 극복하고 보안이 강화된 고품질의 융복합 4차 산업 서비스 제공이 필요하다[16].

미래 의료산업은 고령화 사회로의 진입으로 인한 사회적 변화와 의료-IT 산업의 융합으로 인한 경제적 변화에 따라 의료서비스가 고객으로 지칭할 수 있는 환자중심의 상시적인 건강관리 서비스의 방향으로 진화될 것으로 예상된다. 이렇듯 의료기관에서 ICT와 융합되는 스마트 의료보안 환경으로 진입하여 보안체계를 구축하기에 기존의 서비스, 시스템들과의 호환성, 확장성 문제에 대한 해결이 필요한 시점이다. 이에 따라, 본 연구에서는 신속하게 스마트 의




〈Figure 1〉 The Aspect about the way of Healthcare Services Evolution

료환경에서 보안체계를 구축하기 위하여, 필요로 하는 보안기술을 도출, 분석하고 도입하기 위한 이해관계자들이 관심을 가져야하는 부분과 역할에 대하여 설계하고자 한다.

## 2. 선행연구

### 2.1 의료정보 생애주기 기반 보안요구사항

환자중심의 체계적이고 능동적인 서비스로 대표되는 의료와 IT 활용의 융합서비스는 개인화된 의료정보 수집, 병원 등의 의료기관 사이에 정보공유, 의료기관과 환자사이에 소통 및 연결 등을 통해 혁신적인 의료서비스로 진화하고 있다. 그러나 국내 의료기관의 다수를 차지하고 있는 중소형 의료기관의 보안전담 인력은 거의 전무하며 보안에 대한 투자 비율도 현저히 낮은 수준이다[4].

의료정보 생애주기는 의료정보의 생성-수집-저장-내부유통과 외부제공-폐기의 과정으로 이루어지며 각 단계에서 정보보호의 취약점이 도출되고 있다.

의료정보의 생성과 수집과정에서는 의료정보의 제공과 이용과 관련해 정보 관리자가 고의로 특정 부분의 동의를 누락하거나 수집한 환자의 개인정보를 본래의 목적 이외에 다른 용도로 악용할 수 있다. 또한 환자의 개인정보가 의료기관을 통해 제공될 경우 홈페이지 외부 공격자에 의해 시스템이 해킹되거나 중간과정에서 환자의료와 IT 간의 융합서비스에 따른 편익과 함께 의료정보 생애주기 과정에서 환자의 개인정보가 유출될 수 있는 취약점이 존재한다[11].

의료정보의 저장과정에서는 중요 정보에 대한 암호화가 누락되거나 데이터베이스에 접속한 사용자의 로그 기록을 발견하지 못할 수도 있다. 정보접근에 대한 권한이 없는 사용자는 암호화되지 않은 정보에 대한 접근이 가능하며 로그 파일이 기록되지 않을 시 비인가 사용자에 대한 감사 및 추적을 진행할 수 가 없다[3].

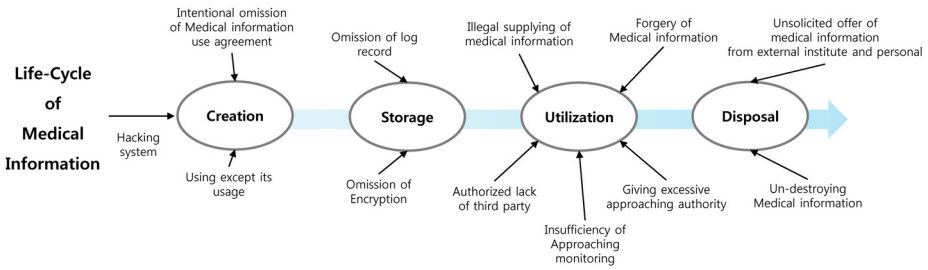
의료정보의 활용과정, 즉 내부유통에서 발생하는 보안취약점은 의료기관 내부 각 부서에게 의료정보에 대한 과도한 접근권한을 부여하고 접근에 대한 모니터링이 미흡할 시 직급 혹은 부서에 상관없이 내부직원이 개인정보를 열람할 수 있도록 되어있다.

의료정보를 활용하는 과정인 외부제공 부분에서는 외부 유관기관으로 해당 정보를 전송하는 과정에서 정보 자체의 위변조가 나타날 수 있으며 의료법에 따른 의료정보의 보호범위에서 벗어나 있는 외부기관 또는 개인에게 의료정보가 불법으로 제공되어 저장될 수 있는 문제점을 가지고 있다.

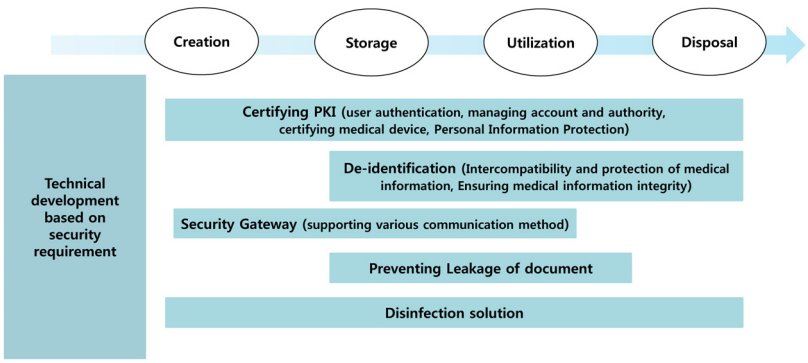
의료정보의 폐기과정에서는 의료정보를 파기해야함에도 불구하고 이를 파기하지 않고 저장하거나 다른 외부기관 또는 개인에게 의료정보를 제공할 수 있다는 취약점이 존재한다.

<Figure 2>에서는 정보보호 취약점을 의료정보 생애주기별로 나누어 그림으로 보여주고 있다. 이와 같은 취약점을 해결하기 위해서는 법적, 관리적, 기술적 관점에서의 다차원적인 정보보호의 요구사항이 설계되어야 하며 각 과정과 요소에 관계되는 이해관계자들과 그들이 활용 및 사용하는 정보에 대한 분석이 필요하다.

<Figure 3>에서는 앞서 도출된 취약점들을 구분하고 이에 따른 의료정보 보안 요구사항들에 대한 기술개발 사항들을 그림으로 정리하고




〈Figure 2〉 Information Security Vulnerability According to Healthcare Information




〈Figure 3〉 Smart Medical Security Platform based on Healthcare Information Life Cycle

있다. 보안요구사항에 대한 통합기술개발은 의료정보 생애주기의 전 과정에 걸쳐 개발되어야 하며 의료정보를 식별할 수 없게 만드는 비식별화 기술개발은 저장과정부터 폐기과정에 걸쳐 개발되어야 한다. 보안게이트웨이 기술개발은 의료정보가 생성되는 과정부터 활용되는 과정에 걸쳐 개발되어야 하며 악성코드에 대한 방역솔루션은 보안요구사항 통합기술개발과 마찬가지로 전 주기에 걸쳐 개발하여 도출된 취약점을 해결할 수 있도록 해야 한다.

## 2.2 적용 가능한 스마트 의료보안 플랫폼 구축을 위한 이해관계자 도출

대・중소 의료기관에 모두 적용이 가능한 국제 표준기반의 국제 스마트 의료보안 플랫폼 구축을 위해서는 의료분야의 이해관계자들에 대한 정의가 필요하다. 의료산업 분야는 타 산업과 달리 해당 산업에 얽힌 이해관계자가 다양하다. 따라서 정보에 접근하고자 하는 사용자들이 각각 어떤 의료정보를 활용하고 사용하는지에 대한 분석이 필요하다.

의료정보학에서 정의하고 있는 의료분야의 이해관계자들에는 환자, 의사와 간호사, 지원인력, 공공의료기관, 정부, 의료 교육자, 보험회사, 의료기관, 의학 연구자, 기술 업체가 있다. 환자는 인터넷을 통해 병원, 보험, 의료진에 대한 정보 같은 의료정보, 진료예약, 처방받은 약의 제조제등과 같은 개인의료정보, 개인 의료기록에 대한 정보를 활용고자 한다[10]. 의사와

간호사는 전자 의약품 투여에 대한 기록, 원격 제어를 포함한 전자 의료 기록, 전자처방 등에 대한 정보를 활용하고자 하며 지원 인력들은 환자 등록, 전자 예약, 전자 청구 등에 대한 정보를 사용하고자 한다. 공공의료기관에서는 사고 보고, 바이오 테러 및 증후군과 관련한 정보를 사용하고자 하며 정부는 의료산업에 대한 표준, 서비스 개방, 질병관리 등을 활용하고자 한다. 의료 교육자는 온라인 의료 자원을 얻고자 하며 보험회사는 의료 산업의 트렌드 분석, 의료진 프로파일, 전자 청구, 의료기관은 EHR, 지출, 입원기간, 질병관리, 의학 연구자는 질병, 인구 등의 연구정보와 연구대상에 대한 정보, 기술 업체는 신기술, 데이터마이닝, 상호운용성 인증에 대한 정보를 활용하고자 한다[6].

## 3. 스마트 의료보안 환경에서 이해관계자 역할 분석

본 연구의 기반이 되는 스마트 의료보안 플랫폼인 병원정보시스템(Hospital Information System)은 보안게이트웨이, 방역솔루션, 문서 유출방지, 데이터 익명화, PKI 인증의 다섯 가지 요소를 포함하고 있으며[9], 이에 따라 각 보안 요소기술에 대한 구체적인 필요성을 분석하여 각 요소들을 실행하는 이해관계자들과의 관계를 도출하고자 한다.

### 3.1 의료기관 보안 요소기술 분석

중소형 의료정보시스템은 현재 환자의 민감정보 보호를 위한 인증기반권한관리, PC/DB/문서에 대한 표준화된 보안기술이 적용되어야 하며 전담인력과 투자여력이 없는 중소병원을 위한 표준화된 보안프레임워크가 적용된 통합/경량형 EMR이 필요하며 의료보안인증서를 이용한 안전한 키 관리인증과 권한관리 및 정보유출 방지기능이 탑재된 의료정보시스템으로 개발되어야 한다.

보안게이트웨이는 의료정보시스템(EMR, EHR, PACS 등)의 의료정보시스템과 직접 데이터를 송수신할 수 있는 의료기기가 아닌 경우에 다른 의료기기나 의료정보시스템의 통신을 위한 국제표준기반의 스마트의료기기용[2]으로 해당 기술은 타 산업분야에서는 게임, 홈 등 한정분야에서 한정적인 보안 모듈로 적용되고 있으며 온도, 습도, 동작 등의 일반 센서로 쓰이는 경우 보안 모듈은 적용되지 않는다. 해당 개발기술은 의료산업 내에서 일부 의료용의 게이트웨이로 쓰일 경우 보안은 낮은 수준으로 적용되며 의료용 센서와 같은 의료기기에 대해서는 보안이 적용되지 않는 한계를 가진다. 이에 따라 병원정보시스템에서 의료용 보안게이트웨이는 위변조 및 해킹이 방지되어야 하며 백신, 구간암호화 등과 같은 고수준의 보안이 적용되어야 한다. 또한 혈압계, 혈당기 등의 다양한 의료기기 및 웰니스케어 기기에 대한 보안도 추가적으로 적용되어야 할 필요가 있다[15].

방역솔루션 기술은 고가의 어플라이언스와 연동이 되는 서비스 형태로, 초기에는 도입 및 유지보수 비용이 높아 도입의 장벽이 존재한다. 또한 일부는 산업별 특성으로 한정적인 특수목적 전용의 폐쇄망 환경으로 도입되어 사용하고 있는 기술이다. 이는 국내 의료서비스 현장에서는 구형 시스템을 계속해서 사용하고 의료산업 종사자들의 보안인식이 결여에 따른 낮은 보안수준의 환경으로 랜섬웨어 감염 등의 보안

침해사고가 발생하는지 확인하는 기술이며 특히 의료분야의 경우에는 짧은 지연의 발생에도 많은 피해가 발생할 수 있기 때문에 기존의 전통적인 보안과 다른 보안정책의 적용이 필수이다. 따라서 의료 방역시스템은 허용 가능한 목록을 기반으로 스마트 의료보안 플랫폼과 연동 및 호환이 가능하도록 개발되어야 하며 기존의 악성코드에 대하여 헤더의 코드를 활용하는 시그니처 기반 검사 기능을 통해 하이브리드형의 의료 보안 방역 기술의 적용이 가능한 소프트웨어가 개발되어야 한다.

문서의 유출방지 기술은 의료기록이 외부 또는 침입자에 의한 유출을 막기 위한 기술로 의료 관리자의 권한의 사용자가 설정한 기간이 지난 로그를 자동으로 삭제하는 기능, 보안모듈에 오류가 발생할 시 로컬에 로그를 기록하도록 하는 기능, 보안 문서에 손상이 있을 경우에 대비한 자동 백업 기능, 보안 문서의 수정 후 저장/종료 시 해당 문서를 백업하는 기능에 대한 개발이 필요하다.

데이터의 비식별화 기술이란 해당 정보만으로는 특정 개인을 식별할 수 없게 만드는 기술을 의미하며[14] 안전한 개인정보 보호의 수단으로 주목받고 있는 기술이다. 현재 재식별이 불가능한 비식별처리 정보를 데이터 손실에 포함하고 있다. 빅데이터 분석과 활용 가능한 정보로써의 가치는 저하되는 것으로 보고 있다[13]. 의료분야에서는 비식별 조치를 위해 k-anonymity를 적용 중에 있으며 이는 의료 민감정보들에 대해 동질성, 배경지식에 대한 공격 등의 취약성을 보였으며 데이터의 유효성 검증에 취약하다는 문제점을 가진다. 이에 따라 이러한 문제를 해결할 수 있는 기술을 통해 의료정보의 비식별화 원천기술을 개발해야 하며 기술개발과 실증의 반복수행을 통해 빅데이터 활용에 대한 유효성 검증 방안을 마련해야 한다.

마지막 요소인 PKI 인증은 공개키 기반구조(Public Key Infrastructure)의 약자로 공개키 알고리즘인 비대칭키암호화 방식으로 인증, 암호화, 전자서명을 제공하는 인프라로 볼 수 있다. 의료분야의 PKI 인증은 공인인증체계의 연계를 통해 개발되어야 한다. 현재 중소형 병원 종사자를 신뢰할 수 있는 권한 정보와 의사라이센스 번호, 환자번호 등과 같은 신원 확인정보는 사용되고 있지 않으며 의료 환경에 적합한 인증서의 발급 및 배포에 대한 관리가 부족한 실정이며 국제 의료용 PKI의 표준에 준수하지 못하고 있다. 이에 따라 PKI 인증기술은 의료보안 인증서의 발급 주체에 따른 권한관리와 신원 확인 정보에 대한 관리를 포함해야 하며 의료 환경에 적합한 인증서 발급 및 배포 프로토콜을 개발할 필요가 있으며[12] 국제 표준 기반의 ISO 17090-1/2/3을 준용하여 서비스가 확산되도록 개발되어야 한다[9].

### 3.2 의료기관 보안체계 구축을 위한 이해관계자 역할 분석

스마트 의료보안 플랫폼의 구축을 위해 앞의 선행연구에서 도출된 이해관계자를 여섯 개의 주체로 구분하여 주요 주체와 병원정보시스템의 다섯 가지 보안기술 요소와 관련된 사항을 알아보고자 한다. 선행연구와 산업 식별을 통해 도출된 이해관계자는 의료 S/W 공급사, PHD 공급사, 의료정보관계기관, 의료기관, 개인으로 구분되며 의료 S/W 공급사의 주요 주체는 HIS 및 의료기기 개발사, 헬스케어 서비스 운영사 등이며 PHD 공급사는 개인의료단말

〈Table 1〉 The Matrix of Smart Medical Security Platform Technology with Stakeholders

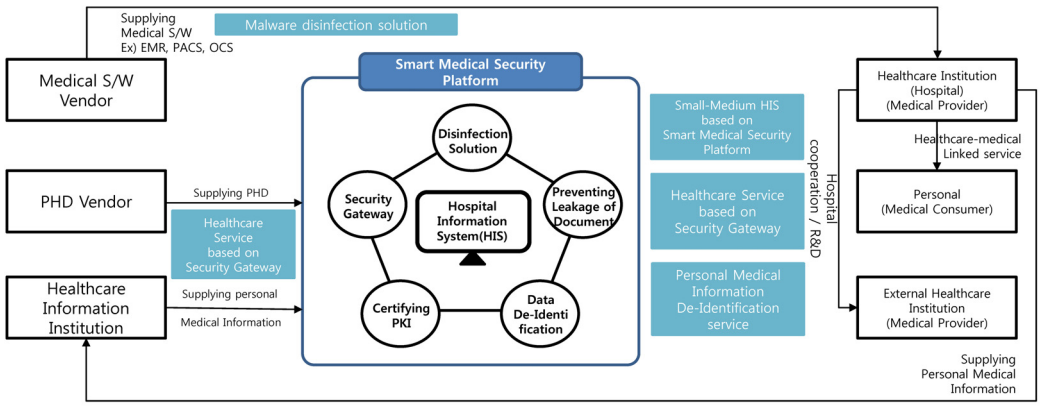
| | | Stakeholders | | | | | |
|---|---|---|---|---|---|---|---|
| | | Medical S/W Vendor | PHD Vendor | Healthcare Information Institution | Healthcare Institution (Hospital) | Personal | External Healthcare Institution |
| Smart Medical Security Platform Technology | Security Gateway | | √ | √ | | √ | |
| | Disinfection Solution | √ | | | √ | | |
| | Preventing Leakage of Document | | | | √ | | |
| | Data De-Identification | | | √ | √ | | √ |
| | Certifyiing PKI | | | | √ | | |

개발사와 웨어러블디바이스 개발사 등으로 볼 수 있다. 의료정보관계기관은 보건복지부, 건강보험심사평가원, 사회보장정보원 등이 주요 주체가 되며 의료기관에서는 대·중소 병원, 보건소 및 정부운영 의료기관, 대합병원협회 등이 주요 주체가 되며 개인, 즉 의료 수요자는 병원 환자, 헬스케어서비스의 이용자 등이 있다. 아래의 <Table 1>에서는 스마트 의료보안 플랫폼 요소와 이해관계자 간의 관계가 매트릭스로 표현되어있다.

의료 S/W 공급사는 의료서비스 협력사로써 의료기관 또는 의료공급자에게 EMR, PACS, OCS 등의 의료 SW를 제공하게 되며 의료기관은 의료수요자인 개인에게 헬스케어-의료 연계 서비스를 제공하게 된다. 이때 의료기관은 외부의료기관과 함께 의료기관 협진 및 R&D를 수행할 수 있으며 두 의료공급자는 의료정보관계기관인 의료보험 관련 정부기관에게 개인의료정보를 제공하게 되며 의료정보관계기관에서는 스마트 의료보안 플랫폼에 개인의료정보를 제공할 수 있게 된다. 아래 <Figure 4>에서는 스마트 의료보안 플랫폼의 다섯 가지 요소와 실제 의료기관 현장의 이해관계자를 역할론적으로 정리해 보았다.

설계한 <Figure 4>의 내용은 새로운 이해관계자의 식별이나 새로운 스마트 의료보안 플랫폼 기반 요소기술이 발생된다면 기술의 위치와 이해관계자의 시각, 규칙(Rule)에 따라 포함될 수 있는 확장성 있는 프레임워크의 성격을 갖출 수 있게 나타내었다.

마지막으로 여서 분류의 이해관계자가 다섯 분류의 스마트 의료보안 플랫폼기반 요소기술에 대한 필요성에 따른 개발 의향을 갖출 수 있는지 적합 타당성을 조사 분석하였다. 구체적으로 의료 S/W 공급사, PHD 공급사, 의료정보관계기관, 중소형 중심 의료기관, PHD 사용자 및 진료환자를 지칭할 수 있는 개인을 대상으로 각 5명씩 인터뷰 방식을 통하여 적합 타당




〈Figure 4〉 Security Perspective by Stakeholders on Smart Medical Security Platform

성을 <Table 2>와 같이 조사분석 하였다. 보안 또는 의료산업과 관련된 전문지식을 보유한 조사자들을 대상으로 표적 집단면접법을 통하여 분석하였으며, 중소 의료기관의 환경과 스마트 의료보안 플랫폼 기반 보안요소 기술에 대한 이해도가 높으며 필요성을 제기한 전문가들을 대상으로 5점 척도 기반의 적합타당성을 조사 분석 진행하였다. 그 결과 모든 이해관계자들은 해당 요소기술에 대한 이해와 적용에 대하여 필요성을 갖고 있는 것으로 나타났다.

〈Table 2〉 Stakeholders Security Element Technology Feasibility Analysis

| Stakeholders | Feasibility Point |
|---|---|
| Medical S/W Vendor | 4.4 |
| PHD Vendor | 4.6 |
| Healthcare Information Institution | 4.2 |
| Healthcare Institution (Hospital) | 4.4 |
| Personal | 4.0 |
| External Healthcare Institution | 4.4 |

## 4. 결 론

의료산업 내 인프라로 ICT가 활발하게 구축됨에 따라 해당 정보를 유출시키고 위협하는 행위 또한 증가하고 있다. 타 산업 분야에 비해 더욱 민감한 정보를 가지는 의료분야에서는 비즈니스 환경을 고려한 보안의 역할이 중요하다. 이에 따라 본 연구에서는 제시된 스마트 의료보안 플랫폼인 병원정보시스템의 다섯 가지 요소를 분석하고 이와 관련한 역할을 수행하는 이해관계자들과 각각 활용 및 사용하는 정보에 대해 살펴보았다.

의료산업 현장에 특화된 의료정보보호의 기술 개발과 의료와 IT의 융합을 통한 의료서비스의 선진화를 추진할 수 있도록 병원정보시스템의 요소들을 분석하고 보안 인식 수준이 매우 낮은 중소형 의료기관과 스마트 의료보안 플랫폼의 실증 범위를 확대시키기 위해 의료산업 내 각 이해관계자들에 대한 분석을 실시하였다. 그리고, 스마트 의료보안 플랫폼의 보안요소기술과 이해관계자의 시각 분석을 통해 지속가능한 스마트 의료서비스 시행을 위한

설계방안을 제시하였다. 마지막으로, 실제 의료산업 현장에서 개별 이해관계자들이 이러한 시각을 견지하여 보안체계 구축을 위한 노력을 수행할 수 있을지에 대한 적합 타당성을 검증하였으며, 그 결과 모두 타당한 것으로 나타났다.

향후 연구로는 개별 이해관계자들과 의료산업의 특색을 갖출 수 있는 보안요소기술들에 대한 심층적인 개발연구를 수행하고자 한다.

## References

[1] Barrow, R. C., "Privacy, Confidentiality, and Electronic Medical Record," Journal of the American Medical Informatics Association, Vol. 3, No. 2, pp. 139-148, 1996.

[2] Cao, F., Huang, H. K., and Zhou, X. Q., "Medical Image Security in a HIPAA Mandated PACS Environment," Computerized Medical Imaging and Graphics, Vol. 27, No. 2, pp. 185-196, 2003.

[3] "Cyber Security Guide for Smart Medical Service," Korea Internet & Security Agency, 2018.

[4] Glemm, A. L., Scott, R., Robert, M. S., and Nitesh, R. T., "If Electronic Medical Records are so Great, Why aren't Family Physicians Using Them?," Journal of Family Practice, Vol. 51, No. 7, 2002.

[5] Gollakota, S., Hassanieh, H., Ransford, B., Katabi, D., and Fu, K., "They Can Hear Your Heartbeats: Non-Invasive Security for Implantable Medical Devices," ACM SIGCOMM Computer Communication Review, Vol. 41, No. 4, pp. 2-13. 2011.

[6] Halperin, D., Thomas, S. H., Fu, K., Tadayoshi, K., and Maisel, W. H., "Security and Privacy for Implantable Medical Devices," The Community for Technology Leaders, Vol. 17, No. 1, 2008.

[7] Jung, Y. S., "Implementation Plan of Integrated Medical Information System for Ubiquitous Healthcare Service," Korea Society of Industrial Information Systems, Vol. 15, No. 2, pp. 115-126, 2010.

[8] Kim, D. W. and Han, K. H., "Recent Research Trends for Responding to Security Threats in Smart Healthcare Environment," Information & Communications Magazine, Vol. 35, No. 2, pp. 95-99, 2018.

[9] Kim, Y. H. and Chang, H. B., "The Change of Future Environment and The Task of Healthcare Security," OSIA S&TR Journal, Vol. 31, No. 2, pp. 4-9, 2018.

[10] Koo, C. C., Shyy, Y. M., iMedica Corp., "Medical Records Data Security System," U.S. Patent 6,874,085, 2005.

[11] Kumar, P. and Lee, H. J., "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey," Sensors, Vol. 12, No. 1, pp. 55-91, 2012.

[12] Lee, Y. H. and Jung, C. S., "Design of Privilege Authentication for Secure OS based on PKI," Korea Institute of Information Scientists and Engineers, Vol. 34,

No. 1, 2007.

[13] Oh, K. Y., “The Point of Issue and Blind on a Debate Concerning De-identification of Data,” Korean Public Law Association, Vol. 45, No. 2, 2016.

[14] Park, S. H., Kim, Y. H., Park, G. M., Na, O. C., and Chang, H. B., “Research on Digital Forensic Readiness Design in a Cloud Computing-Based Smart Work Environment,” Sustainability, Vol. 10, No. 4, pp. 1-24, 2018.

[15] Williams, P., “A Practical Application of CMM to Medical Security Capability,” Information Management & Computer Security, Vol. 16, No. 1, pp. 58-73, 2008.

[16] Yang, C. M., Lin, H. C., Chang, P., and Jian, W. S., “Taiwan’s Perspective on Electronic Medical Records’ Security and Privacy Protection: Lessons Learned from HIPAA,” Computer Methods and Programs in Biomedicine, Vol. 82, No. 3, pp. 277-282, 2006.

[17] Lee, K. K., Jung, Y. S., and Han, C. H., “A Study on Consumer’s Acceptance of Medical Internet Marketing According to Medical Departments,” The Journal of Society for e-Business Studies, Vol. 14, No. 1, pp. 121-142, 2009.

[18] Kim, J. W. and Chang, H., “A Study on Design Security Management Evaluation Model for Small-Medium size Healthcare Institutions,” The Journal of Society for e-Business Studies, Vol. 23, No. 1, pp. 89-102, 2018.

## 저 자 소 개

김양훈 (E-mail: yhkim@kdu.ac.kr)
2011년 대진대학교 소프트웨어공학전공 (박사)
2014년~현재 극동대학교 산업보안학과 조교수
관심분야 융합보안, 산업보안, 소프트웨어 프레임워크

정원후 (E-mail: nugudosa@naver.com)
2014년~현재 중앙대학교 융합보안학과 박사과정
관심분야 산업보안, 융합보안, 경제방첩