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

The Journal of Society for e-Business Studies
Vol.23, No.1, February 2018, pp.89-102
https://doi.org/10.7838/jsebs.2018.23.1.089

중소형 의료기관 보안관리 평가모델 설계 연구

A Study on Design Security Management Evaluation Model for Small-Medium size Healthcare Institutions

김자원(Ja Won Kim)*, 장항배(Hang Bae Chang)**

초 록

최근 4차 산업혁명의 도래로 인해 융합서비스 환경으로 변화함에 따라 융·복합적인 새로운 보안위협이 나타나고 있다. 이에 중소형 의료기관 또한 비즈니스 환경을 고려한 특화된 보안을 필요로 하고 있는 실정이다. 따라서 본 논문에서는 선행연구 분석을 통해 의료기관 보안 특성을 도출하고 중소형 의료기관의 현장조사를 통해 중소형 의료기관 보안 특성과 현황을 조사하였다. 이러한 중소형 의료기관 보안 특성을 기반으로 중소형 의료기관을 위한 보안관리 평가모형을 설계하고 검증하였다. 설계를 위해 현존하는 의료기관 관련 보안관리체계, 평가 인증 체계 비교분석을 수행하였고 본 논문에서 제안한 보안관리 평가 모형과 공유정도 또한 확인하였다. 또한 제안하는 중소형 의료기관을 위한 보안관리 평가모형의 통계적 검증을 위해 적합 ·타당성 검증을 수행하였고, AHP 분석을 통한 상대적 우선순위 분석을 수행하여 항목별 가중치를 도출하였다. 본 연구의 결과를 통해 중소형 의료기관이 실제 수행 가능한 보안관리 평가모형의 기준으로 활용될 수 있을 것으로 기대된다.

ABSTRACT

In this paper, the security characteristics of healthcare institutions were derived through analysis of previous research, and the characteristics and status of small and medium sized healthcare institutions were surveyed through field surveys of small and medium sized healthcare institutions. The security management evaluation model for small and medium sized healthcare institutions was designed and verified based on the security characteristics of small and medium healthcare institutions. For the design, we compared and analyzed existing security management system and evaluation certification system of healthcare institutions. We also confirmed the proposed security management evaluation model and the degree of sharing. In addition, we conducted validation for the statistical verification of the proposed security management evaluation model for small and medium sized healthcare institutions, and we performed the relative priority analysis through AHP analysis to derive the weight for each item. The result of this study is expected to be used as a standard of security management evaluation model that can be practiced in small and medium sized healthcare institutions.

키워드 : 의료보안, 중소형 의료기관, 보안관리체계
Healthcare Security, Small-Medium Size Healthcare Institutions, Security Management System

이 논문은 2016년도 중앙대학교 CAU GRS 지원에 의하여 작성되었음.

* First Author, Dept. of Security Convergence, Graduate School, Chung-Ang University(jjawon@cau.ac.kr)
** Corresponding Author, Dept. of Industrial Security, Chung-Ang University(hbchang@cau.ac.kr)
Received: 2018-01-08, Review completed: 2018-01-12, Accepted: 2018-02-01

1. 서 론

과거 종이로 환자의 의료 정보를 기록하던 의료 환경은 IT의 눈부신 발전으로 종이 대신 디지털 환경에서 기록과 관리를 하는 환경으로 변화되었다. 이러한 의료 환경의 변화로 이용자는 원격 진료나 웨어러블 디바이스를 활용한 헬스케어와 같은 환자들의 진료 편의성을 높이는 서비스를 제공받을 수 있게 되었으며 의료기관 중심이었던 보건의료의 패러다임이 이용자 중심으로 바뀌게 되었다.

의료IT 융합 환경에서 디지털화된 의료정보는 환자의 개인정보를 포함하며, 의료기관 뿐만 아니라 보험회사를 포함한 다양한 기관들과 네트워크를 통해 공유되고 있다. 따라서 의료정보 유출은 환자 개인의 금융 기록, 생체정보 등과의 조합을 통해 2차 피해로 이어질 수 있다. 또한 의료정보는 개인의 건강 정보, 치료 기록을 비롯한 민감 정보를 포함하고 있기에 단순 의료 정보 유출만으로도 막대한 피해를 끼칠 수 있는 실정이다. 하지만 의료 기관에서의 높은 IT 기술 활용도와 개인정보의 중요도에 비해 보안 수준은 여전히 미비한 것이 사실이다.

보안 전문업체에 의하면 의사의 99%가 모바일 기기를 보유하며 이를 환자 정보 공유에 적극 활용함에도 불구하고 의사들이 사용하는 모바일 기기의 14%에는 단 하나의 암호조차 설정되지 않은 것으로 조사되었다. 또한 최근 미국의 대형 병원 세 곳은 랜섬웨어 '록키(Locky)'에 감염되어 엄청난 피해를 입은 바 있다. 점점 증가하는 의료보안 사고에 대비하기 위해 우리가 대면하고 있는 보안 이슈와 위협 동향을 알아보고 기술적 및 관리적 차원에서의 의료보안과제에 대한 연구가 필요한 시점이다.

실제 국내외 의료기관의 사고 사례를 확인하기 위해 미국의 신용도용범죄정보센터(Identity Theft Resource Center, 이하 ITRC)의 통계분석 보고서, IT 보안연구소 SANS Institute (SysAmin, Audit, Network and Security, 이하 SANS)의 연구보고서, 미국 회계감사원(Goverment Accountability Office, 이하 GAO)의 조사보고서를 포함한 3개의 해외 선행연구와 국내 선행연구를 통하여 의료기관의 보안 위협 및 이슈에 대해 확인하였으며, 그 중 ITRC의 최근 통계 자료에 의하면 아래 <Table 1>과 같이 총 데이터 침해 건수 614건 중 보건의료 관련 정보는 269건으로 이는 전체에서 43.8%에 달하는 수치임을 확인하였다. 다른 산업분야에서 발생하는 데이터 침해 건수와 비교해본다면 금융관련 정보 중 23건의 데이터 침해 사고가

〈Table 1〉 The Number of Data Threat Incident

Industrial Type	2005	2006	2007	2008	2009	2010	2011	2012	2013
Management	28	69	130	243	208	279	198	172	211
Education	75	80	111	131	78	65	60	65	55
Government/Army	21	98	110	110	90	104	48	53	56
Healthcare	**13**	**43**	**64**	**94**	**65**	**160**	**87**	**165 (34.9%)**	**269 (43.8%)**
Financial	20	31	31	78	57	54	28	18	23
Total	157	321	446	656	498	662	421	473	614

발생한 점을 미루어볼 때, 의료 관련 정보에 대한 해커들의 관심이 매우 높다는 사실을 확인할 수 있다.

이와 같이 의료분야 보안사고가 빈번하게 발생되고 그 피해규모도 커짐과 동시에 국내외에서는 ISO 27799, KISA-ISMS 등 정보보호 관리체계 인증을 통해 의료기관 정보보호 관리 및 평가에 초점을 두고 정책을 시행하고 있다. 특히 최근 정보통신망 이용촉진 및 정보보호 등에 관한 법률의 개정으로 연매출 1,500억 원 이상인 의료법상 상급종합병원은 ISMS(정보보호 관리체계) 의무 인증 대상이 되었다. 하지만 국내에서 시행하고 있는 정보보호 관리체계의 경우 일반 기업을 대상으로 하는 범용의 정보보호 관리체계만을 보유하고 있으며, 의료기관의 특성이 고려되지 않은 채 시행되고 있다. 이에 대해 의무 인증 대상 의료기관의 항의가 빗발치고 있으며 실제로 2016년 첫 시행당시에는 정보보호 범위를 의료기관이 보유하고 있는 홈페이지에 국한되어 시행한 실정이다. 그럼에도 불구하고 대형 의료기관의 정보보호 관리체계 도입으로 인해 국내 의료기관 보안 수준 향상에 큰 영향을 미치고 있는 것은 사실이다. 하지만 중소형 의료기관의 경우 대형 의료기관에 비해 인적·경제적 한계로 인해 보안활동 수행에 제약이 있으며, 조직 구성원들의 보안 수준이 현저히 낮아 의료보안의 필요성 또한 충분히 느끼지 못하는 실정이다. 상대적으로 많은 기관을 차지하고 있는 중소형 의료기관의 보안 수준 향상을 위한 대책 마련이 시급한 실정이다.

따라서 본 논문에서는 중소형 의료기관을 위한 보안관리 평가모형을 설계하고자 한다. 보안관리 평가모형 설계를 위해 문헌분석을 통하여 의료기관이 가지고 있는 비즈니스 요소와 보안 특화 요소를 도출하고 의료분야 관련 관리체계, 평가, 인증 체계 내용을 비교분석하고 통계적 검증을 통해 보안관리 모형을 구축한다. 추후 AHP 분석을 통하여 각 항목별 우선순위(가중치)를 도출하는 것을 목표로 한다.

제 1장에서는 앞서 언급한 바와 같이, 본 연구의 배경 및 필요성에 대하여 기술하고 있으며, 연구의 목표 및 추진 방법 및 절차에 대해 작성하였다. 제2장에서는 관련 선행연구 분석을 통해 중소형 의료기관의 현황 및 범위를 선정하고 의료기관의 특화적인 보안 특성을 도출하였다. 추가적으로 중소형 의료기관 현장조사 내용을 통해 현재 중소형 의료기관이 가지고 있는 환경을 반영할 수 있도록 하였다. 제 3장에서는 중소형 의료기관만이 가지고 있는 보안 특성이 반영된 중소형 의료기관 보안관리 평가 항목을 도출하고, 기 도출한 평가 항목에 대해 국내·외 의료분야 관련 관리체계, 평가, 인증 체계 세부 조항을 기반으로 비교분석하여 항목별 공유 정도를 확인하고 중소형 의료기관 보안관리 평가모형을 설계한다. 이를 기반으로 제 4장에서는 설계한 평가모형을 통계적 검증을 통해 적합도, 타당성 검토를 수행하며, 통계적 적합도 및 타당도를 검증한 항목에 한하여 AHP 분석을 수행해 항목별 우선순위(가중치)를 도출한다.

2. 선행 연구

2.1 중소형 의료기관 현황

국내에서 현행되어지고 있는 의료기관의 규모 구분 기준은 크게 2가지로 의료법에 의한 구분,

국민건강보험법에 의한 구분으로 나누어진다. 의료법[9]에 의해 구분으로는 크게 의원급, 병원급으로 나누어지며 병원급 의료기관 중 일정 기준에 따라 종합병원과 상급 종합병원으로 나누어 구분되어진다.

국민건강보험법[12]에 의한 구분으로는 의료전달체계를 기반으로 구분되어 지고 1차, 2차, 3차 의료기관으로 구분하고 있다. 1차 의료기관은 의원, 보건소를 포함하며 외래환자 진료를 수행하는 30병상 미만의 의료기관으로 한정한다. 2차 의료기관은 병원, 종합병원 급으로 필수 진료과목 요건을 갖춘 병원을 대상으로 하며 30병상 이상 규모를 보유한 의료기관으로 한정한다. 3차 의료기관은 상급 종합병원을 대상으로 구분되어진다.

추가적으로 통계청 자료에 따르면 의료기관 구분에 따른 의료기관 보유현황은 상급종합병원 43개소, 종합병원 301개소, 전문병원 1,516개소, 일반병원 1,462개소, 의원 30,689개소를 보유하고 있는 것으로 나타났으며, 본 논문에서는 전체 34,011개소 의료기관 중 32,151개소(약 94.53%)를 차지하는 일반병원과 의원을 대상으로 중소형 의료기관의 범위를 설정하였다. 전문병원은 요양병원과 정신병원 등 특수 진료과목에 해당하는 병원을 포함하며, 일반병원은 병원급에 해당하는 병상 수를 가지고 있지만 전문병원이 아닌 병원으로 한정한다.

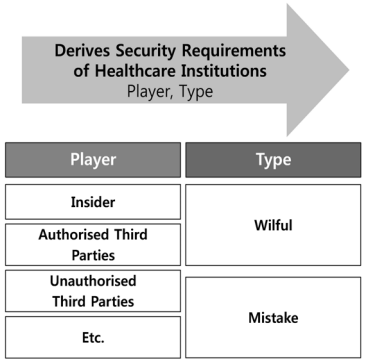
전문병원의 경우 국내에서 시행되고 있는 별도의 인증체계를 보유하여 운영하고 있으며, 상급종합병원의 경우 정보통신망법 개정에 따라 K-ISMS 인증을 의무화하고 있는 실정이다. 하지만, 일반병원과 의원에 해당하는 중소형 의료기관의 경우 인적·경제적 한계로 인하여 별도의 인증을 의무화하지 않고 있다. 하지만 중소형 의료기관은 전체 의료기관 중 큰 비중을 차지하고 있으며, 특히 의료전달체계로 인해 종합병원 혹은 상급종합병원으로 방문하기 전 필수적으로 중소형 의료기관에서 진료를 받아야 하는 특성을 지니고 있어 방문자 수 또한 상대적으로 많은 수를 차지하고 있다.

2.2 의료기관 보안 특성 선행연구

보안특성 분류 기준을 설계하였다. 먼저, 보안을 사람이 행하는 범죄행위로부터 조직의 안녕과 질서를 유지하는 것으로 바라볼 때, 의료보안은 의료기관(병원)에서 Player(행위자, 사람)와 범죄행위의 고의성 여부(Type)를 확인하는 것으로 기준을 설계하였다.

설계한 기준은 <Figure 1>과 같으며, 해당 기준을 기반으로 의료기관에 특화된 보안 특성을 도출하기 위해 선행연구를 통하여 의료기관에서 발생하는 보안사고 시나리오를 분석하였다.

ISO 27799[4]의 Annex-A와, Nicole van Deursen[17]의 연구를 기반으로 의료기관에서 빈번히 발생하는 보안특성을 도출하였다.



〈Figure 1〉 Classification of Security Incidents of Healthcare Institutions

Player(행위자, 사람)은 내부자, 인가된 제3자, 비인가 제3자, Etc. 총 4가지로 분류하였으며, 각 Player(행위자, 사람)들 각각 고의(남용)와 실수(오용)에 의해 발생할 수 있는 위험요소를 비교하여 결과를 도출하였다.

이와 같이 선행연구를 분석한 결과 내부자에 의해 발생하는 보안사고 시나리오가 가장 많은 것으로 나타났으며, 해당 시나리오의 발생빈도 또한 가장 높은 것으로 확인했다. 의료기관 내에서 사용되어지고 있는 IT 시스템 관련 보안사고 시나리오는 굉장히 많은 양을 차지하고 있었지만, 실제 발생빈도를 확인하였을 때 5개의 시나리오가 실제 의료기관에서 발생하는 보안사고이며, 발생 빈도를 5점 척도로 구분할 때 1(거의 없음), 2(없음)에 해당하는 시나리오만 존재하는 것을 확인하였다. 이를 통해, 실제 의료기관에서 빈번히 발생되고 있는 보안사고는 내부인에 의한 오・남용에 의한 사고임을 확인 할 수 있었다.

2.3 중소형 의료기관 현장조사

중앙대학교 의료보안연구소가 수행한 중소형 의료기관의 보안 수준 실태조사를 참고하여 중소형 의료기관 경영환경 특성, 의료IT서비스 환경 특성, 의료보안특성에 대해 분석하였다. 해당 조사는 의원과 병원 200개소를 대상으로 조사를 진행하였으며, 총 29개의 문항으로 구성되어져있다[3].

중소형 의료기관의 경영환경 특성 기술통계 분석의 주요 결과로는 첫째, 의료IT서비스를 사용하는 국내 의료기관에 대한 설문 분석 결과, 현재 84%에 해당하는 의료기관이 진료중심의 운영방식을 따르는 것으로 나타났으며 둘째, 의료부서(진료 등을 포함한 의료행위를 수행하는 부서)에 종사하는 구성원 비율은 평균 72%로 나타났다. 셋째, 의료지원부서(원무과, 전산실 등을 포함한 의료행위를 수행하지 않는 부서)의 구성원 비율은 평균 28%로 확인되어 진료 위주의 의료서비스를 실시하고 있는 것을 확인하였다. 넷째, 원장(의사) 중심의 수직적 의사결정 구조로 운영되는 기관이 82%로 나타나 대다수의 의료기관이 수직적 경영 구조로 운영되는 것을 확인하였다. 다섯째, 현재 중소형 의료기관은 치료・진료 중심의 병원 운영방식을 따르며 구성원 비율 또한 의료부서에 치중된 것을 알 수 있었음 대다수의 의료기관이 원장(의사) 중심의 수직적 의사결정 구조로 운영되어 독단적 경영환경을 가지고 있음을 확인한 것이 있다.

중소형 의료기관의 의료IT서비스 환경적 특성의 주요 기술통계 결과는 총 3가지로 첫째, 설문에 응답한 의료기관 99%가 의료IT서비스를 사용하고 있지만, 의료기관 내부 의료IT서비스 전담부서가 존재하지 않거나 외부 아웃소싱으로 운영되고 있는 기관은 전체 97%로 나타났다. 둘째, 전체 매출액 대비 의료IT서비스 투자율이 1%가 채 되지 않는 기관이 절반 이상을 차지함을 확인하였다. 셋째, 의료IT서비스는 보급화 되어있으나, 서비스 도입 이후 유지보수 및 최신화에 있어 의료기관이 무관심한 상황이며 이에 대한 투자 또한 거의 이루어지지 않는 상황임을 알 수 있었다.

중소형 의료기관 의료보안 특성의 주요 기술통계 분석 결과는 첫째, 의료기관 내부 의료정보보호 전담부서가 존재하지 않거나 외부 아웃소싱으로 운영되고 있는 기관은 전체 97%로 나타났으며 둘째, 의료IT서비스 투자 대비 의료정보보호 투자율이 1%가 채 되지 않는 기관이 절반 이상을 차지하였다. 의료IT서비스 투자율을 1%가 되지 않는 기관이 절반 이상을 차지한 것을 미루어 볼 때에, 의료정보보호에 대한 투

자가 전혀 이루어지지 않고 있음을 확인할 수 있었다. 마지막으로, 설문에 응답한 기관 중 전체 86%에 해당하는 기관이 의료보안활동의 중요성을 인지하고 있으며, 83%에 해당하는 기관이 중소형 의료기관을 위한 정보보호 관리체계의 필요성을 인지하고 있었다. 하지만, 전담인력부족(62.5%)/예산부족(54.2%)의 이유로 의료보안 활성화가 힘든 실정임을 확인하였다.

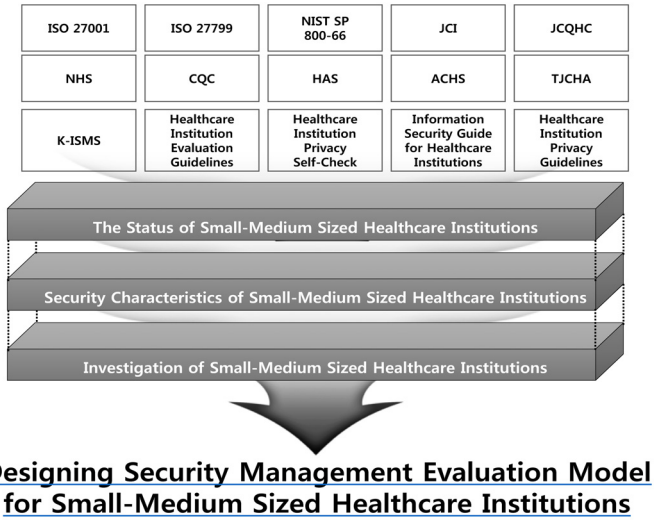
3. 중소형 의료기관 보안관리 평가모형 개발

3.1 중소형 의료기관 보안관리 평가모형 설계

본 논문에서는 아래 <Figure 2>와 같이, 선행연구를 통해 분석한 의료기관의 비즈니스 특성과 의료기관 특화 보안요소를 반영하고 중소형 의료기관을 대상으로 한 보안 수준 설문 내용을 반영하여 중소형 의료기관의 보안 특성을 도출하고자 한다.

3.2 중소형 의료기관 보안관리 평가모형 개발

본 연구에서는 앞서 분석한 의료기관 보안 특성 선행연구와 중소형 의료기관 현황 및 실정 분석 내용을 기반으로 중소형 의료기관을 위한 보안관리 평가모형의 세부항목을 도출하였다. 도출한 세부항목과 기존 범용 보안관리 체계(ISO 27001: 2013 & 27002: 2013[5])와 의료기관용 보안관리체계 ISO 27799: 2016[4]을 포함하여 국내외 의료기관을 대상으로 하는 보안 점검 지표 비교분석을 수행하였다. 중소형 의료기관의 특성이 반영된 보안관리 모델 구축을 위해 국내외 의료보안 관련 표준을 포함한 선행연구를 비교분석하였으며, 본 연구에서 분석한 선행연구 목록은 <Table 2>와 같다.



〈Figure 2〉 Designing Security Management Evaluation Model for Small-Medium Sized Healthcare Institutions

〈Table 2〉 The List of Certification Related with Small-Medium Sized Healthcare Institutions

No.	Title
①	ISO/IEC 27001: 2013. Information Technology-Security Techniques-Information security management systems-requirements(2013)
②	Health informatics-Information security management in health using ISO/IEC 27002(2016)
③	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act(HIPAA) Security Rule, NIST Special Publication 800-66 revision 1(2008)
④	Joint Commission International Accreditation standards for hospitals 5th edition(2014)
⑤	Japan Council for Quality Health Care, Hospital Accreditation Standards by Functional Category Hospital Type 1
⑥	Quality and Outcomes Framework guidance for GMS contract 2013/14, NHS Commissioning Board(2013)
⑦	CQC The state of health care and adult social care in England: An overview of key themes in care 2010/11. London: Care Quality Commission (2011)
⑧	de Sante, H. A. Haute autorite de Sante. Grossesses à risque: orientation des femmes enceintes entre les maternités en vue de l'accouchement, 2010-04(2008)
⑨	The Australian Commission on Safety and Quality in Health Care, National Safety and Quality Health Service Standards(second edition)(2017)
⑩	Joint Commission of Taiwan, Evolution of Hospital Accreditation Standards(2015)
⑪	KISA, Information Security Management System(ISMS) Certification Standard(2013)
⑫	Healthcare Institution Evaluation Guidelines, Ministry of Health and Welfare, Korea Health Industry Development Institute(2017)
⑬	Security of Privacy self-checklist(medical institution), Korean Hospital Association(2017)
⑭	Information Security Guide for Healthcare Institutions(Hospital), Ministry of Health and Welfare, Korea Health Industry Development Institute(2016)
⑮	Guidelines for Security of Privacy(Healthcare Institutions), Ministry of Health and Welfare, Ministry of Government Administration and Home Affairs(2016)

각 자료의 통제항목 혹은 평가 지표 세부내용을 기반으로 매핑을 통해 분석을 수행하였다. 매핑 방법은 각 지표에서 보유하고 있는 가장 낮은 레벨인 세부내용을 기반으로 유사하거나 동일한 내용끼리 맵핑하는 과정을 거쳐서 수행하였으며, 중소형 의료기관의 특성이 반영된 보안관리 모델을 구축하기 위해 의료보안 관련 국내외 관련 문헌(ISO/IEEE 27001 : 2013, ISO/IEEE 27799 : 2016[4], KISA-ISMS[7], NIST Special Publication 800-66, Joint Commission International Accreditation Standards for Hospitals(JCI 인증), Hospital Accreditation Standards by Functional Category Hospital Type 1 (JCQHC 인증), Quality and Outcomes Framework guidance for GMS contract 2013/14, NHS Commissioning Board, 개인정보보호 자율점검표(대한병원협회), 의료기관을 위한 정보보호안내서(병원편) (보건복지부), 개인정보보호 가이드라인(의료기관편) 등을 비교분석하였다.

본 연구에서 도출한 각 세부항목의 조작적 정의는 <Table 3>과 같으며, 앞서 분석한 선행연구 내용을 기반으로 정의를 도출하였다. 세부항목의 조작적 정의에 참고한 선행연구는 <Table 2>의 순서와 동일하게 기재하였다. 추가적으로, 세부항목을 선정함에 있어 중소형 의료기관 현장조사 내용을 반영하여 현재 국내에서 운영되어지고 있는 의원급 병원과 일반병원에서 겪고 있는 의료보안 한계점과 경영현황 IT 인프라 현황 등을 최대한 반영하여 세부항목을 선정하였다.

세부항목 선정 및 도출에 있어서는 현재 운영되어지고 있는 국내병원의 한계점과 국제표준 또는 인증체계에서 우선순위가 있는 항목에 초점을 맞추었으며, 관련 선행연구의 공유정도

를 확인함으로써 해당 내용을 반영하였다. 본 논문에서 제안하는 중소형 의료기관 보안관리 평가모형의 세부항목은 <Table 3>과 같다.

본 연구에서 도출한 각 세부항목과 선행연구의 공유정도를 확인하였을 때, “의료기관(일반) 직원” 항목이 93%로 가장 높은 수치를 보였으며, 이후 “의료정보 보안관리” 87%, “의료보안 전문인력” 73%, “지속적 개선(인증)” 67% 순으로 높은 공유정도를 나타냈다. 반대로 “의료기기(특화)”, “법적 요구 규제사항” 두 항목은 40%의 공유정도로 가장 낮은 공유정도를 나타내었다.

〈Table 3〉 The List of Evaluation Items

Items	Explain	Reference
Accident management	Refers to the management of response regulations for accidents that harm business continuity, such as system malfunctions and outflow accidents at medical institutions	[1, 2, 8, 10, 11, 12, 13, 18]
Continuous improvement (Certification)	Refers to activities that continuously improve the security environment of medical institutions.	[4, 5, 6, 8, 9, 12, 14]
Healthcare equipment (General)	Refers to the IT equipment commonly used by the organization of the healthcare institution. It also manages access rights(account management), environment update(Fetch, SW update), installation and operation of security SW for personal computer(PC), service server and database And the like.	[1, 5, 10, 12, 11, 13, 18]
Healthcare equipment (Specialized)	Refers to security management such as access rights management(account management), environment update(Fetch, SW update) for devices specialized for medical activities such as CT, X-ray, scale,	[8, 12, 11, 14]
Healthcare information security management	Refers to the security management of application programs that contain medical information such as EMR, OCS, PACS, etc.	[1, 3, 5, 9, 10, 11, 12, 13, 18]
Classify and manage security areas (Equipment)	Refers to the operation of physical security systems such as access control, intrusion alarm, and detection of immigration to perform physical security activities in relation to protected areas	[1, 3, 8, 10, 13, 15]
Security system operation	Refers to performing security management by identifying / distinguishing between the protected area(Ex. treatment room, examination room, etc.) and protective equipment(Healthcare equipment, etc.)	[1, 2, 7, 10, 12, 13, 18]
Healthcare security investment (Facility)	The amount of security investment(ratio) to sales amount(or IT investment amount) *The amount of security investment(ratio): refers to the cost to invest in staff(security)+security consulting+secur*ity system construction	[1, 5, 7, 8, 10, 13, 18]
Healthcare security investment (Education)	The amount of security investment(ratio) to sales amount(or IT investment amount) *The amount of security investment(ratio): the cost of investing in security education*	[1, 5, 7, 8, 10, 13, 18]
Healthcare institutions staff (general)	Refers to security activities for employees(general) such as security pledge and security education.	[1, 2, 3, 5, 9, 10, 12, 11, 13, 18]
Healthcare security Staff	The degree of security staff(or additional staff) in the healthcare institutions	[1, 2, 3, 6, 7, 10, 11, 13, 14, 18]
Compliance	The extent to which the organization’s security regulations and activities are consistent with laws and regulations related to healthcare institutions (such as the Medical Law, the Health Care Act, the National Health Promotion Act, the medical device technique)	[1, 2, 13, 18]

이는 앞서 분석한 중소형 의료기관의 보안 현황 및 관련 선행연구들의 내용과 같이 현재 중소형 의료기관의 보안 수준 향상과 보안 사고를 막기 위해서는 “의료기관(일반)직원” 즉, 해당 의료기관에서 근무하고 있는 의료진, 원무과 관련 아웃소싱 직원을 모두 포함한 일반 직원을 대상으로 하는 보안 활동이 최우선시 되어야하는 것을 확인할 수 있다.

4. 통계적 검증

4.1 연구대상 및 자료수집 방법

본 연구의 최종 목표인 중소형 의료기관을 위한 보안관리 평가모형을 검증하기 위하여 설문조사 수행을 위한 대상을 선별하였다. 실제 의료기관에서 보안활동을 수행하고 있는 관련 분야 전문가를 대상으로 설문을 진행하였으며, 중소형 의료기관의 규모적 특성상 의료기관 내・외부적으로 의료보안활동을 수행하는 담당자를 설문 대상으로 선정하였다. 세부적으로 의료기관 외(外)에서 의료보안활동을 수행하는 의료 ICT 아웃소싱 담당자와 의료기관 내(內)에서 의료보안활동을 수행하는 의료보안 담당자를 대상으로 하였으며, 실제 의료보안활동을 수행하고 있는 의료진, 원무과 직원 등을 포함하는 의료보안 관련 업무를 전・겸임으로 수행하지 않는 의료기관 일반 직원들을 대상으로 설문을 수행하였다.

설문은 대면조사를 주로 수행하여 설문에 대한 이해를 충분히 할 수 있도록 하였으며, 실제 유효 설문은 56개로 나타났다. 표본의 수가 충분하진 않지만 설문 수행 대상을 질적으로 높은 수준의 대상만을 선별하여 진행하였기 때문에, 연구 결과의 신빙성을 충분히 입증할 수 있는 결과가 나올 것으로 생각된다.

설문방식은 각 평가 항목들의 타당성(적절한 정도)을 측정하기 위해 5점 척도(1: 아주 적합하지 않다, 2: 적합하지 않다, 3: 보통이다, 4: 적합하다, 5: 아주 적합하다)로 객관식 형태로 진행하였다.

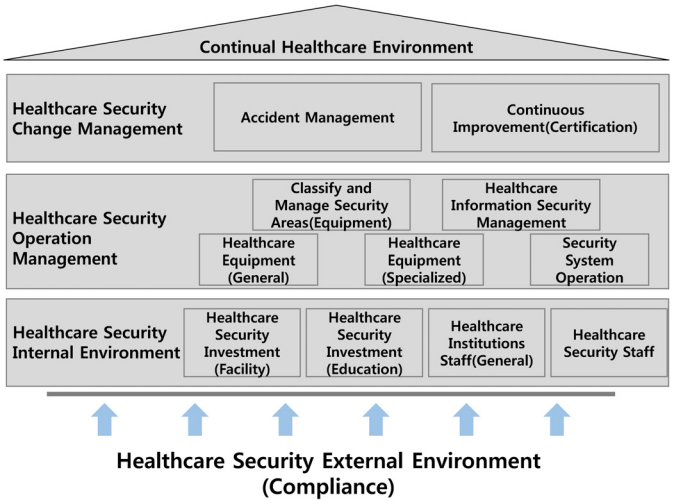
4.2 중소형 의료기관 보안관리 평가모형 적합・타당성 검증

설문조사 수행 결과, 각 세부항목의 평균값(기준 타당성은) 모두 3.5 이상으로 중소형 의료기관 보안관리 평가모형에 적합함을 나타내었다.

세부항목별 평균(기준타당성) 값과 표준편차 값은 <Figure 3>과 같다.

Descriptive Statistics Quality		
Items	Average	Standard Deviation
Accident Management	3.82	0.61
Continuous Improvement(Certification)	3.54	1.04
Healthcare Equipment(General)	3.61	1.07
Healthcare Equipment(Specialized)	3.86	0.89
Healthcare Information Security Management	3.86	0.97
Classify and Manage Security Areas(Equipment)	3.93	1.09
Security System Operation	4.04	0.92
Healthcare Security Investment(Facility)	3.86	1.15
Healthcare Security Investment(Education)	3.86	1.04
Healthcare Institutions Staff(General)	4.00	0.94
Healthcare Security Staff	3.96	1.00
Compliance	3.54	1.29

〈Figure 3〉 Feasibility Subcriteria



〈Figure 4〉 Small-Medium Sized Healthcare Security Management Evaluation Model

적합・타당성 검증 기준을 만족한 세부항목은 총 12개 항목이며, 관리모형으로 도식화하면 <Figure 4>와 같다.

각 세부항목은 크게 의료보안 변화관리, 의료보안 운영관리, 의료보안 내부환경, 의료보안 외부환경으로 4가지 영역으로 구분되어진다.

4.3 중소형 의료기관 세부항목 우선순위 분석

앞서 도출한 중소형 의료기관 보안관리 평가모형의 세부항목 12가지를 기준으로 각 항목의 가중치를 산정하기 위해 AHP 분석을 실시하였다.

각 기준들의 상대적 우선순위를 산정하기 위한 AHP 분석은 10년 이상의 경력이 있는 의료기관 실무자 또는 의료기관의 ICT 아웃소싱을 수행하는 의료보안 담당자를 대상으로 설문을 수행하였으며, 중소형 의료기관 환경을 충분히 이해할 수 있는 역량을 보유한 대상을 선별하여 설문 대상의 높은 질적 수준을 확보하였다. 10명을 대상으로 AHP 설문을 진행하였으며, 10점 척도를 사용하여 설문을 수행하였고, Consistency Index도 산정했다.

통상 Consistency Index가 0.1 이하이면 응답자들의 답변을 신뢰할 수 있다고 본다. 본 연구의 AHP 분석 수행 결과 Consistency Index는 0.043으로 0.1보다 낮은 수치를 도출하여 응답자들의 답변을 신뢰할 수 있다고 해석된다.

본 연구의 AHP 분석결과, 상대적으로 중요한 순으로 나열하면 “의료보안 투자(교육)”은 21%, “의료기관(일반) 직원”은 18%, “보호구역(장비)설정과 관리”는 11%로 상대적 우선순위를 보였다. 이는 “의료IT시스템에 의한 보안활동 보다 내부자 혹은 의료기관 관련 종사자들에 의한 보안활동에 가중을 더 해야 한다.”라는 선행연구 분석 결과와 유사하게 중소형 의료기관에서는 의료IT시스템과 관련된 보안활동을 수행하는 것 보다 의료기관 구성원 모두 의료보안의 중요성을 인지하고 그 수행방법을 학습할 수 있도록 일반 직원에 대한 관리와 의료보안 교육 투자 정도를 평가 하는 항목이 가장 높은 가중치를 보이는 것을 확인할 수 있다.

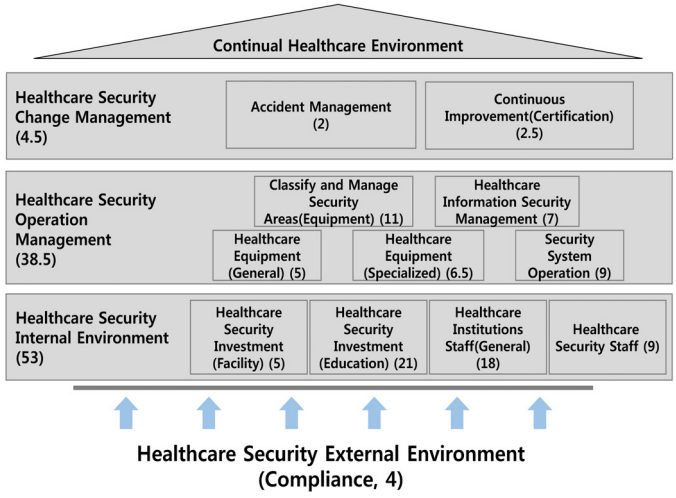
반면 “사고대응 규정관리”는 2%, “지속적 개선(인증)”은 2.5%, “법적 요구 규제사항”이 4%

로 가장 낮은 우선순위를 보였다. 설문조사 수행 당시 대면조사를 통해 확인한 결과, 대다수의 의료기관에서는 인증에 관한 부정적인 인식을 보유하고 있음을 확인할 수 있었다. 의료기관의 인증을 수행하기 위해 실제 의료기관 종사자들의 업무 가중이 필연적으로 증가함에 따라 대부분의 의료기관 종사자들은 인증 자체에 반감을 부정적 영향을 가지고 있었으며, AHP 분석 결과 또한 이와 동일하게 도출되어 “지속적 개선(인증)” 항목이 낮은 가중치를 보이는 것을 확인할 수 있다.

<Table 4>는 각 항목에 대한 가중치 및 우선순위를 확인할 수 있으며, 가중치의 경우 계산의 용이함을 위해 소수점 둘째 자리에서 반올림하여 수치를 최적화 하였다. 이어지는 <Figure 5>에서는 본 연구의 최종 결과인 중소형 의료기관을 위한 보안관리 평가모형을 도식화한 것이며, 각 항목에 대한 가중치를 괄호를 통해 나타내었다.

〈Table 4〉 The Result of AHP Analysis

Items	Weighting	Priority
Accident Management	2.1 → 2.0	12
Continuous Improvement(Certification)	2.4 → 2.5	11
Healthcare Equipment(General)	4.7 → 5.0	8
Healthcare Equipment(Specialized)	6.4 → 6.5	7
Healthcare Information Security Management	6.8 → 7.0	6
Classify and Manage Security Areas(Equipment)	11.2 → 11.0	3
Security System Operation	9.0 → 9.0	4
Healthcare Security Investment(Facility)	5.3 → 5.0	8
Healthcare Security Investment(Education)	21.0 → 21.0	1
Healthcare Institutions Staff(General)	18.3 → 18.0	2
Healthcare Security Staff	8.7 → 9.0	4
Compliance	4.2 → 4.0	10



〈Figure 5〉 Small-Medium Sized Healthcare Security Management Evaluation Model(AHP)

5. 결론 및 향후연구

최근 4차 산업혁명의 도래로 인해 융합서비스 환경으로 변화함에 따라 융・복합적인 새로운 보안위협이 나타나고 있다. 이에 중소형 의료기관 또한 비즈니스 환경을 고려한 특화된 보안을 필요로 하고 있는 실정이다. 상급 종합병원의 경우, ISMS 인증 의무화를 시작으로 보안에 대한 중요성을 인식하고 있으나, 중소형 의료기관은 인적 경제적 부담으로 보안에 대한 중요성은 인식하나 수행에 옮기지 못하고 있는 한계점이 존재한다. 따라서 본 논문에서는 선행연구 분석을 통해 의료기관 보안 특성을 도출하고 중소형 의료기관의 현장조사를 통해 중소형 의료기관 보안 특성과 현황을 조사하였다. 이러한 중소형 의료기관 보안 특성을 기반으로 중소형 의료기관을 위한 보안관리 평가모형을 설계하고 검증하였다. 설계를 위해 현존하는 의료기관 관련 보안관리체계, 평가 인증 체계 비교분석을 수행하여 공유정도 또한 확인하였다.

우선 중소형 의료기관의 보안 활동을 위한 새로운 보안관리 평가모형 설계를 위해 국내 의료기관 현황, 의료기관 보안특성, 중소형 의료기관 현장조사 등을 통해 세부항목 12개를 도출하였다. 이를 토대로 설계된 모형을 검증하기 위해 실제 의료기관에서 보안활동을 수행하고 있는 관련분야 전문가를 대상으로 적합도 설문을 진행하였으며, 기술통계량 분석을 토대로 타당성을 확인하여 세부항목의 적합・타당성을 검증하였다. 최종적으로 중소형 의료기관 보안관리 평가모형으로써 제시한 12가지 항목이 적절함을 입증되었다.

마지막으로 12개로 도출된 항목을 합리적으로 수행할 수 있는 방안을 마련하기 위해, 상대적 우선순위 분석을 통해 가중치를 산정하였다. 분석 결과, “의료보안 투자(교육)”이 21%, “의료기관(일반)직원”이 18%로 가장 높은 가중치를 보였으며, “의료보안 사고대응 규정관리”는 2%, “의료보안 지속적 개선(인증)”이 2.5%로 가장 낮은 우선순위를 보였다.

상급종합병원을 대상으로 하는 ISMS 인증이 의무화되어 시행되어지고 있지만, 상대적으로 많은 개소를 가지고 있는 중소형 의료기관에 대한 보안인증과 평가체계는 전무한 실정에서 본 연구의 결과를 통해 중소형 의료기관의 비즈니스 환경과 제약조건을 반영한 평가모형을 제안함으로써 실천 가능한 의료기관 보안활동 및 대책 수립방안을 제시할 수 있을 것으로 기대된다.

본 연구의 한계점으로는 설계한 모형을 실제 조직에 적용해보는 사례연구를 수행하지 못한 점이다. 사례연구를 수행하지 못해 기 제안한 모형의 실제 적용 타당성을 확인하기 어려우며, 실제 중소형 의료기관의 적용 및 활용에 있어 한계점을 가진다.

References

[1] Bae, J.-M., Kim, S. G., and Chang, H. B., “A Study on Design Direction of Industry-Centric Security Level Evaluation Model through Analysis of Security Management System,” Society for e-Business Studies, Vol. 20, No. 4, pp. 177-191, 2015.

[2] Choi, Y.-S., Moon, S.-Y., Kang, H.-J., and Jun, H.-J., “A Study on t-he Development

of a Model to Measure the Knowledge Based Information Utilization Level in Architectural Design Work Environment," Journal of the Architectural Institute of Korea, Vol. 29, No. 4, pp. 59-70, 2013.

[3] ETNews, [cited 2018 Jan 26], Available from: URL: http://www.etnews.com/20170728000514.

[4] ISO 27799 Annex A Threats to health information security, 2016.

[5] ISO/IEC 27001 : 2013, Information Technology Security Techniques Information security management systems requirements, 2013.

[6] Korean Hospital Association, Personal Information Protection Self-Checklist, 2016.

[7] Korean Internet & Security Agency(KISA), Information Security Management System(ISMS) Certification Standard, 2013.

[8] Liu, C. H., Lin, F. Q., Chiang, D. L., Chen, T. L., Chen, C. S., Lin, H. Y., Chung, Y. F., and Chen, T. S., "Secure PHR Access Control Scheme for Healthcare Application Clouds," in Proceeding of 42nd International Conference on Parallel Processing, pp. 1069-1076, 2013.

[9] Medical Law, [cited 2017 Oct 27], Available from: URL: http://www.law.go.kr.

[10] Ministry of Government Administration and Home Affairs, Privacy control level indicator, 2015.

[11] Ministry of Health & Welfare & Korea Health Industry Development Agency, Information Protection Guide for Medical Institutions-Hospital, 2016.

[12] Ministry of Health & Welfare & Korea Health Industry Development Agency, Information Protection Guide for Medical Institutions-Medical Center, 2016.

[13] Ministry of Health and Welfare & Ministry of Government Administration and Home Affairs, Privacy Guidelines-Medical Institutions, 2013.

[14] National Intelligence Service: Information security management status index, 2015.

[15] Pharmacy personal information self-checklist, 2015.

[16] Shin, E. H. and Chang, H. B., "A Study on the Method of Security Industrial Classification through the Review of Industrial Special Classification," *Society for e-Business Studies*, Vol. 22, No. 4, pp. 175-191, 2017.

[17] Van Deursen, N., Buchanan, W. J., and Duff, A., "Monitoring information security risks within health care," Computer & Security, 2013.

[18] Veiga, A. D. and Eloff, J. H. P., "An Information Security Governance Framework," Information Systems Management, Vol. 24, No. 4, pp. 361-372, 2007.

[19] York, T. W. and MacAlistrer, D., Hospital & Healthcare Security, Butterworth Heinemann, 6th Edition.

저 자 소 개

김자원 (E-mail: jjawon@cau.ac.kr)
2012년~2016년 성결대학교 컴퓨터공학과 (학사)
2016년~현재 중앙대학교 일반대학원 융합보안학과 산업보안전공 (석사과정)
관심분야 의료보안, 산업보안, 중소형 보안관리체계

장항배 (E-mail: hbchang@cau.ac.kr)
2006년 연세대학교 정보시스템관리 (박사)
2007년~2012년 대진대학교 경영학과 조교수
2012년~2013년 상명대학교 경영학과 조교수
2014년~현재 중앙대학교 산업보안학과 부교수
관심분야 산업보안, 의료보안, 연구보안, 보안 데이터 분석