의료융합 환경에서 수용성을 고려한 비용 효율적 보안체계구축 방안 연구: 중소의료기관을 중심으로★

김 양 훈*, 안 병 구**

요 약

근래에 산업이 융합됨에 따라, 산업 간 융합 도구 활용이 조직 내 보안성에 미치는 영향이 증가하고 있다. 그러나, 조직 구성원들은 기존의 시스템을 중심으로 비즈니스를 활동하기 때문에 새로운 시스템 도입에 대한 적응력이 부족하고, 이에 따라서, 보안에 대한 고려는 후 순위로 나타날 수 밖에 없는 환경이다. 본 연구에서는 의료융합산업에서 중소형 의료기관을 대상으로 보안 체계를 구축하기 위해 우선적으로 고려해야 할 요소들에 대한 비용 효율적인 선택방안에 대하여 연구하였다. 구체적으로 선행연구들을 통하여 현재의 법제도 체계를 고려하고 보안현황을 분석하였을 때, 중소형 의료기관에서 필요한 보안 솔루션/시스템/체계에 대하여 도출하였다. 그리고, 실제 비즈니스 환경에서 중소형 의료기관 관련자들을 대상으로 비용 효율적으로 보안 체계를 구축하기 위한 상대적 우선순위에 대하여 분석하고 전반적인 보안체계를 구축하기 위한 방안을 제시하였다.

A Study on the Cost-Effective Security System for SME Hospital Acceptability in Convergence Medical Environment

Yanghoon Kim*, Byung-Goo Ahn**

ABSTRACT

As industries converge in recent years, the impact of the use of convergence tools among industries on the security of the organization is increasing. However, organizational members lack the ability to adapt to introduction of new system because they are operating business around existing systems, and thus, security considerations are an environment that will inevitably emerge as a follow-up priority. In this study, we studied cost-effective options for factors that should be considered first in order to establish a security system for small and medium-sized healthcare institutions in the healthcare convergence industry. Specifically, the current legal system was considered and the security status was analyzed through prior research, and the necessary security solution/system was derived from small and medium-sized healthcare institutions. In addition, it analyzed relative priorities for cost-efficient deployment of security systems to those involved in small and medium-sized healthcare institutions in actual business environments and presented measures to establish a overall security.

Key words : Convergence Medical Environment, SMEs Hospital, Security Acceptability, Medical Security System

접수일(2018년 12월 5일), 게재확정일(2018년 12월 26일)

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

* 극동대학교 산업보안학과
** 중앙대학교 융합보안학과

1. 서 론

최근 ICT 기술이 급변화됨에 따라, 다양한 산업에 활용되어 기존의 제품 및 서비스의 효용성을 극대화시킬 수 있는 IoT, 클라우드, 빅데이터 등의 기술들이 대두되고 있다. 이러한 혁신적인 ICT 기술들은 기존의 기업들의 제품 생산과 서비스 제공의 수준을 향상시키고 있으며, 비즈니스 환경을 융합 생태계로 변화시키고 있다.

한편, 최근 인구의 고령화와 함께 생활양식 및 환경의 변화로 인하여 건강에 관한 관심이 높아지고 있다[8]. 또한, ICT 기술의 융합으로 인하여 언제 어디서나 의료서비스에 대한 접근성이 높아지게 되었고, 병원 외부에서부터 병원 내부까지 환자의 의료정보 전 과정에 이르는 진료 및 건강관리 중심의 의료서비스에 대하여 기대가 높아지게 되었다. 이에 따라, 의료서비스 품질 향상에 대한 요구와 관심이 증가되고 있으며, 의료비 절감과 서비스 제고의 시도가 활발히 나타나고 있다[3].

이러한 ICT를 중심으로 활용되는 융합환경은 기존의 산업에 다양한 변화를 일으켰다[1]. 그러나, 기존의 산업에서는 새로운 기술들에 대한 적용이 구성원들의 수용성 측면에서 능동적이지 못한 문제점이 있다. 또한 새로운 기술들의 비즈니스 적용에 있어서 보안에 대한 고려가 없고, ICT 시스템들의 초기 구성형태가 활용성 중심이듯 보안에 대한 고려가 없어 오래된 보안적 취약성 및 위협이 그대로 나타나는 형태가 되고 있다. 특히, 국내에서 공공재 성격을 갖고 있으며, 국민의 건강을 책임지는 다양한 의료기관의 ICT 시스템들은 보안에 대해 고려할 수 없는 래거시 시스템에서 운영되고 있거나, 독립적인 시스템 환경으로 인하여 기존의 보안솔루션 및 시스템들과 융화되기 어려운 환경에 있다[7].

이에 따라, 본 연구에서는 의료융합산업을 대상으로 의료기관의 조직 구성원들이 내/외부적으로 보안환경을 갖추기 위한 비용 효율적인 선택방안에 대하여 연구하고자 한다. 세부적으로 선행연구와 환경분석을 통하여 의료융합환경의 ICT 현황을 분석하고, 이러한 환경에서 필요한 보안 체계 요소에 대하여 도출하며, 비용 효율적으로 선택하기 위한 상대적 중요도에 대하여 분석하여 제시하고자 한다.

2. 선행연구

2.1 의료융합환경 및 보안현황

통계청에 따르면, 상급종합병원에서부터 소규모의 의원, 그리고 치과, 한의원, 약국 등 국내의 의료기관은 최종발표년도인 2016년도 기준 8만 9천여개로 나타나고 있다. 구체적으로 병의원부터 대형병원으로 분류되는 상급종합병원, 종합병원, 병원, 의원들의 수는 3만3천여개 이며, 중대형 병원(상급종합병원, 종합병원)의 수는 1%에 불과한 것으로 나타났다[5].

지역에서 환자진료와 건강관리를 담당하는 중소형 병의원들은 주로 병원 내부에서는 전자의무기록시스템(EMR, Electronic Medical Record), 처방전달시스템 OCS(Order, Communication System)등의 의료정보시스템을 중심으로 의료영상저장전송시스템(PACS, Picture Archiving Communication System) 등으로 구성되어 있다. 또한, 일부 도서 산간지역 등 의료접근성이 어려운 곳을 포함하여 국민의 만성질환 및 건강관리를 위하여 병원 외부에서 혈압계, 체중계, 혈당계, 체성분계 등의 개인건강정보기기(PHD, Personal Health Device)를 활용한 정보수집체계를 갖추고 있다[2, 9].

국내 의료기관에서 활용되는 의료기기의 90%는 외산이며, 병원의 개원시기에 맞춰 사용기한이 10년 이상된 기기들이 많은 상황이다. 또한, 의료기기의 적합성에 맞추어 운영체제가 Windows XP 등 오래된 래거시 형태에서 동작하고, 최신 운영체제로 업데이트하거나 악성코드 탐지 시스템을 설치하면 동작하지않는 등 문제점이 많은 상황이다[10]. 특히, 의료서비스는 진료 중심에서 환자 중심으로 변화됨에 따라, 새로운 의료IT시설에 대한 투자를 요구하고 있으며, 중소의료기관은 이에 대한 비용적, 물적 요소가 부족하여 도입이 어려운 상황이다[5].

이와같은 방향으로 국내의 의료보안을 위한 시스템, 솔루션, 체계는 전방위적으로 갖춰져 있지 않으며, 2018년도에서야 스마트 의료보안 가이드라인이 나온 상태이다[2]. 그러나 가이드라인에서는 사물인터넷 환경을 중심으로 의료서비스 제공자가 아닌 의료시스템 제공자 측면에서 보안을 갖추기 위한 방안을 다루고 있다. 예를 들어 기본적인 기술적 보안과 관리적보안 그리고 물리적 보안의 영역까지 다루고 있다. 이러한

광범위한 체계는 상급 종합병원에서도 모두 갖추기는 어려운 실정이며, 중소형 의료기관(병원)에 적용하기에는 매우 어려운 상황이다[5]. 또한 취약점과 위협을 식별하기 위하여 기존의 동일한 시스템적인 내용들을 추상화 시키면서 기존의 동일한 문제점을 도출하고 해결책을 야기하여 스마트 환경에 대한 고려가 적고, 중소형 기관에 대한 적용, 수용성이 부족한 상황이다.

2.2 의료융합환경 보안기술

보안을 위한 의료정보시스템은 의료기관에서 활용하는 의료정보의 생성(수집)~저장~활용(내부유통과 외부제공)~폐기과정에 따라 위협 및 취약점을 분석하여 설계될 수 있다. 분석된 취약점과 의료정보 생애주기에 대하여 시나리오를 기반으로 의료융합보안 프레임을 설계하면, 병의원 외부에서는 PHD 보안기술, 통신구간암호화기술(PHD에서 보안게이트웨이 구간, 보안게이트웨이에서 의료정보시스템 구간), 보안게이트웨이기술로 구분할 수 있다. 그리고, 병의원 내부에서는 사용자 인증기술, 권한관리 기술, 방역화 기술, 문서유출방지기술, 익명화기술 등으로 나타낼 수 있다[7].

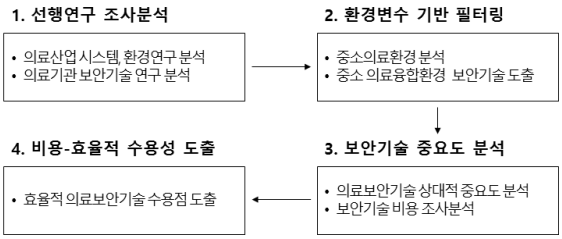
그리고 역할 중심의 보안 에이전트 기반 의료융합환경 보안기술을 살펴보면, 사용자 인증기술(전자서명), 접근제어 기술, 권한관리 기술 등으로 구분할 수 있다[4, 6].

한편, 미국 등의 해외 사례와 국내 ISMS를 참조하여 보건의료환경에 필요한 보안기술을 구분하면 매체관리 기술, 악성코드 방지 기술, 접근관리 기술, 통신보안 기술, 사용자인증 기술, 네트워크/운영체제/AP 접근통제 기술, 원격지 근무 관리기술 등으로 나타낼 수 있다[3, 9].

3. 의료융합환경 핵심 보안기술 도출 및 연구방향 설계

3.1 연구방법론 및 흐름

근래에 산업이 융합됨에 따라, 산업 간 융합 도구 활용이 조직 내 보안성에 미치는 영향이 증가하고 있다. 그러나, 조직 구성원들은 기존의 시스템을 중심으로 비즈니스를 활동하기 때문에 새로운 시스템 도입에 대한 적응력이 부족하고, 이에 따라서, 보안에 대한 고려는 후 순위로 나타날 수 밖에 없는 환경이다. 이에 따라, 본 연구에서는 의료융합산업에서 중소의료기관들이 비용 효율적으로 보안체계를 수용하기위한 방안을 도출하기 위하여 그림 1과 같은 연구방법론을 설계하였다.



(그림 1) 연구방법론(흐름)

3.2 중소 의료기관 보안기술

앞서 분석한 의료산업시스템과 환경의 현황과 다양한 의료보안 기술, 그리고 중소의료환경을 종합하여 중소 의료융합환경에서 필요한 보안기술을 표 1과 같이 도출하였다.

<표 1> 중소 의료기관을 위한 보안기술

분류	보안기술	설명
의료기관 외부	PHD 보안기술	개인 건강정보기기 자체를 안전하게 활용할 수 있게 해주는 보안기술
	통신구간 암호화기술	PHD와 보안게이트웨이, 보안게이트웨이와 의료정보시스템 사이의 통신구간 암호화 기술
	보안 게이트웨이 기술	다종, 다인, 다량 PHD의 데이터를 수집하여 중개하는 게이트웨이에 대한 안전성을 담보하는 보안기술
의료기관 내부	사용자 인증기술	의료정보시스템에 접근하는 개인대상에 대한 검증 기술
	권한관리기술	의료정보시스템에 접근하는 개

		인대상이 활용할 수 있는 정보의 범위를 관리하는 기술
	방역화기술	의료정보시스템을 활용함에 있어 외부 악성코드나 비인가 프로세스에 대해서 동작하지 못하도록 환경을 구성하는 보안기술
	문서유출방지기술	의료정보시스템에서 생성되는 외부 전달용 문서, 영상 등에 대한 안전성을 담보하기 위한 보안기술
	익명화기술	생성되는 다량의 의료정보 활용(임상 등)을 위하여 개인을 식별할 수 없도록 하는 기술

3.3 중소 의료기관 보안기술 중요도 분석방향

중소 의료기관 보안기술 중요도를 도출하기 위하여 2018년도 3월1일부터 8월31일까지 10년 이상 경력의 중소 의료기관 병원정보시스템 개발 전문가 2인, 10년 이상 경력의 건강관리 시스템 개발 전문가 2인, 의료정보 관련 교수 2인, 의료산업 관련 공공기관 전문가 2인, 보안 솔루션(개발) 전문가 2인 등 총 10인으로 구성된 전문가들을 대상으로 계층화 분석(AHP, Analytic Hierarchy Process)을 수행하였다. 그리고, 중소 의료기관에서 보안의 중요도와 대형 의료기관에서 보안의 중요도 차이를 분석하기 위하여 추가적인 조사분석을 수행하였다. 10인 전문가 개별의 의견에 대하여 일관성 지수(InConsistency Index, 0에 가까울수록 신뢰성이 높음)를 통해 검증을 수행하였고, 모두 활용할 수 있는 것으로 나타났다. 계층화 분석에서 10인의 전문가 의견을 종합하기 위하여 아래의 식인 기하평균을 이용하였으며, 소수점 넷째 자리에서 반올림하여 활용하였다.

$$GM = \sqrt[n]{\sum_{i=1}^{n} a_i} \qquad (1)$$

우선, 기술적, 관리적, 물리적 보안 등 기본적인 보안체계 구축 방법을 대상으로 중소 의료기관에서 중요시 여기는 시각을 견지하기 위하여 우선순위(중요도)를 분석하였다. 그리고, 의료기관 외부에서 활용하는 보안기술 3종과 의료기관 내부에서 활용하는 보안기술 5종에 대하여 시급성을 검토하기 위하여 우선순위(중요도)를 분석하였다.

4. 의료융합환경 비용-효율적 보안수용점 분석

4.1 의료기관 보안도구(방법) 중요도 분석

중소 의료기관 보안도구(방법)에 대한 분석 결과는 일관성 지수 0.0016으로 나타났다. 그리고 관리적 보안 50.5% > 기술적 보안 30.6% > 물리적 보안 18.9% 순으로 중요한 것으로 분석되었다. 대형 의료기관 보안도구(방법)에 대한 분석 결과는 일관성 지수 0.0011으로 나타났으며, 기술적 보안 48.9% > 관리적 보안 33.0% > 물리적 보안 18.1% 순으로 중요한 것으로 분석되었다.

인적 물적 자원이 풍부한 곳에서는 보안 체계를 도입하기 위하여 시스템을 우선적으로 고려하고 있으며, 그렇지 못한 기관에서는 의료정보시스템 유지보수 등을 통한 인적자원의 보안관리를 더욱 필요로 하는 것으로 분석되었다.

4.2 의료기관 내외부 보안기술 중요도 및 비교

의료기관 외부 보안기술을 중심으로 살펴보면, ①PHD보안기술, ②통신구간암호화기술, ③보안게이트웨이기술 형태로 나열하였다.

중소 의료기관에서는 PHD보안기술(46.1%)에 대한 도입을 가장 필요로 하고 있었으며, 보안게이트웨이 기술(35.2%), 통신구간암호화기술(18.6%)을 순차적으로 필요로 하는 것으로 나타났다.

<표 2> 중소 의료기관 외부보안기술 계층화 분석표

외부 보안기술	①	②	③
①		2.154	1.494
②			0.464
③			

그와 비교하여 대형 의료기관 역시 PHD보안기술(48.9%)에 대한 도입을 가장 필요로 하고 있었으나, 차순위로 통신구간암호화기술(33.0%), 보안게이트웨이 기술(18.1%)을 순차적으로 필요로 하는 것으로 나타났다.

<표 3> 대형 의료기관 외부보안기술 계층화 분석표

외부 보안기술	①	②	③
①		1.4142	2.8284
②			1.7321
③			

의료기관의 외부 보안기술 중요도와 관련하여 심층적으로 분석한 결과, 외부 건강관리 기기(PHD)에 대한 보안은 현재 개발은 되어있으나 실제 상품에 탑재되어 판매되지 못하고 있으나 향후 보안을 위하여 반드시 필요한 것으로 나타났다. 중소 의료기관에서는 직접 방문 등을 통한 데이터 이관으로 보안게이트웨이에 대한 수요가 많았고, 대형 의료기관에서는 다량의 건강정보들이 모바일, 웹, 접수처 등을 통하여 들어오기 때문에 통신구간암호화기술에 대한 필요성이 높은 것으로 나타났다.

의료기관 내부 보안기술을 중심으로 살펴보면, 상세한 중요도를 분석하기 위하여 앞서 도출된 주요 보안기술에 대하여 ①사용자인증기술, ②권한관리기술, ③방역화기술, ④문서유출방지기술, ⑤익명화기술 형태로 나열하였다. 그리고, 개별 기술에 대한 계층화 분석표를 표2와 표3으로 제시하였다. 이를 통하여 분석한 결과는 다음과 같다.

중소 의료기관에서는 권한관리 기술에 대한 도입 필요성이 가장 높게 분석되었으며, 문서유출방지기술에 대한 수요가 가장 적을 것으로 나타났다. 상세하게는 ②권한관리기술 35.9% > ①사용자인증기술 20.9% > ⑤익명화기술 19.2% > ③방역화기술 15.5% > ④문서유출방지기술 8.4% 순으로 나타났다. 심층적으로 인터뷰를 통하여 분석한 결과, 개별 의료인들에 대한 권한관리를 통하여 개인정보보호법 등에 대한 이행을 만족시키고자하는 필요성이 강했으며, 새로운 기술의 일환인 익명화 기술들에 대한 접근을 원하는 것으로 나타났다.

<표 4> 중소 의료기관 내부보안기술 계층화 분석표

내부 보안기술	①	②	③	④	⑤
①		0.585	1.842	2.714	0.693
②			1.957	3.557	2.714
③				2.154	0.843
④					0.511
⑤					

이와 비교하여 대형 의료기관에서는 익명화기술의 도입 필요성이 가장 높게 분석되었으며, 방역화기술에 대한 수요가 가장 적을 것으로 나타났다. 상세하게는 ⑤익명화기술 35.7% > ②권한관리기술 23.5% > ④문서유출방지기술 20.1% > ①사용자인증기술 12.7% > ③방역화기술 8.1% > 순으로 나타났다.

<표 5> 대형 의료기관 내부 보안기술 계층화 분석표

내부 보안기술	①	②	③	④	⑤
①		0.577	2.000	0.408	0.447
②			1.732	2.000	0.577
③				0.333	0.224
④					0.447
⑤					

심층적으로 인터뷰를 통하여 분석한 결과, 대량의 데이터를 보유한 대형 의료기관의 경우 임상실험 등 다양한 부분에 데이터를 기존에 활용하고 있었으며, 이를 자동화하여 더욱 많은 연구와 데이터분석을 위한 시스템을 요구하고 있는 것으로 나타났다. 한편, 방역화기술과 같이 호환성과 확장성에 저해되는 요소들에 대해서는 제한적인 것으로 나타났다.

5. 결 론

혁신적인 ICT 기술들은 기존의 기업들의 제품 생산과 서비스 제공의 수준을 향상시키고 있으며, 비즈니스 환경을 융합 생태계로 변화시키고 있다. 이러한 과정에서 국내에서 공공재 성격을 갖고 있으며, 국민의 건강을 책임지는 다양한 의료기관의 ICT 시스템들

은 보안에 대해 고려할 수 없는 래거시 시스템에서 운영되고 있거나, 독립적인 시스템 환경으로 인하여 기존의 보안솔루션 및 시스템들과 융화되기 어려운 환경에 있다.

보안을 중심으로 한 새로운 의료IT시스템에 대한 투자가 요구되고 있으나, 인적, 물적 자원이 부족한 중소 의료기관은 도입이 어려운 상황이다. 이에 따라 본 연구에서는 중소 의료기관의 보안체계 구축을 위하여 우선적으로 도입해야 할 기술에 대한 분석을 수행하였다. 결과적으로 중소형 의료기관에서는 우선적으로 도입해야 할 보안기술은 '권한관리기술'로 분석되었으며, 외부 PHD 공급자들의 건강정보기기에 보안성 탑재에 대한 필요성이 있는 것으로 나타났다.

중소 의료기관은 현재 운영하고 있는 의료정보시스템들을 중심으로 권한관리기술 → 사용자인증기술 → 익명화기술 → 방역화기술 → 문서유출방지기술 순으로 융합설치한다면 보다 비용-효율적인 보안체계를 구축할 수 있을 것이다.

향후, 개별기술들을 중소의료기관 환경에 맞추어 개발·구축에 대한 연구를 수행하고자 한다.

참고문헌

[1] 송지은, 김신효, 정명애 (2007). u-헬스케어 서비스에서의 의료정보보호. 정보보호학회지, 제17권, 제1호, pp. 47-56.

[2] IoT보안얼라이언스, "스마트의료 사이버보안 가이드", 한국인터넷진흥원, 2018.

[3] 우성희 (2015). IoT 환경의 의료 정보보호와 표준 기술. 한국정보통신학회논문지, 제19권, 제11호, pp. 2683-2688.

[4] 윤은준, 유기영 (2010). 의료정보보호를 위한 RFID를 이용한 환자 인증 시스템. 한국통신학회논문지, 제35권, 제6호, pp. 962-969.

[5] 이난경, 이종옥 (2015). 중소형 병원의 클라우드 병원정보시스템 서비스 체계에 관한 연구. 한국전자거래학회지, 제20권, 제3호, pp. 89-112.

[6] 이대성, 노시춘 (2011) 보안 에이전트 역할 기반에 기초한 의료정보시스템 소프트웨어 보안아키텍쳐 설계방안, 융합보안논문지, 제11권 제4호, pp.78-83.

[7] 장항배, 김양훈(2018), "미래 환경변화와 의료보안 과제", S&TR Journal, 제31권, 제2호, pp. 4-9.

[8] 정원수, 오영환 (2008). U-Healthcare 기반의 환자 모니터링 시스템. 한국통신학회논문지, 제33권 제7호, pp. 575-582.

[9] 정혜정, 김남현 (2009). "보건의료의 정보화와 정보보호관리 체계". 정보보호학회지, 제19권, 제1호, pp. 125-133.

[10] "백신도 못 까는 의료기기", 지디넷코리아, 2018.5.4.

[11] Dimitris Gritzalis, Costas Lambrinoudakis (2004), "A security architecture for interconnecting health information systems", International Journal of Medical Informatics 73, pp. 305-309.

[12] Fu-Shiung Hsih(2007), "Context-aware Workflow Driven Resource Allocation for e-Healthcare," e-Health Networking, Application and Services, 2007 9th International Conference, pp.34-39.

[13] Karakış, R., Güler, İ., Capraz, I., & Bilir, E. (2015). A novel fuzzy logic-based image steganography method to ensure medical data security. Computers in biology and medicine, 67, pp. 172-183.

[14] Wang, Y., Wang, L., & Xue, C. A. (2018). Medical information security in the era of artificial intelligence. Medical hypotheses, 115, pp. 58-60.

[15] Zhang, R. and Liu, L.(2010), "Security models and requirements for healthcare application clouds," In Cloud Computing(CLOUD), 2010 IEEE 3rd International Conference on, pp. 268-275.

〔저자소개〕

김 양 훈 (Yanghoon Kim)
2005년 2월 대진대학교 컴퓨터공학 학사
2007년 2월 대진대학교 컴퓨터공학 석사
2011년 2월 대진대학교 소프트웨어공학 박사
2014년 2월 - 현재 극동대학교 산업보안학과 교수
email : yhkim@kdu.ac.kr

안 병 구(Byung-Goo Ahn)

2018년 2월 중앙대학교 융합보안학과 박사수료
2010년 - 현재 코오롱인더스트리㈜ 산업보안팀장
email : bgahn0405@naver.com