https://doi.org/10.33778/kcsa.2019.19.4.151

의료기관 정보보호 인식교육을 위한 교육과정 연구

김 동 원*, 한 근 희**

요 약

세계적으로 의료분야는 스마트기기의 확산과 통신 기술의 발달로 매우 빠르게 발전하게 됨에 따라 의료보안 문제가 전면으로 대두되고 있다. 또한 진료정보교류로 개인의 민감한 의료정보가 네트워크 상에서 상호 교환되기 때문에 발생 가능한 보안위험이 매우 크다고 할 수 있다. 본 논문에서는 보건소, 보건지소, 보건진료소, 1차, 2차, 3차 병의원 등에서 운용하고 있는 의료기기와 의료시스템을 현장에서 검증한 결과를 토대로 NCS(National Competency Standards)와 국제표준, 의료기관 요구사항, 교육기관의 정보보호 학습모델을 참조하여 의료기관의 정보보호 인식교육을 위한 교육과정을 개발하였다. 이를 의료기관 종사자와 ICT 전문가 집단을 통한 타당성 검증을 진행하여 교육을 통한 의료기관의 정보보호 수준향상을 위한 방법을 연구 제안한다.

Curriculum study of information security awareness for medical institution

Dong-Won Kim*, Keun-Hee Han**

ABSTRACT

As smart devices and communication technologies have developed rapidly, the healthcare industry in the globe is seeing remarkable issues on medical security. At the same time, personal medical records are being shared in the network, which would raise the risk of information security. This thesis aims to develop the curriculum to raise the awareness of information security among workers in medical institutions by referring to NCS(National Competency Standards) International standards, medical institutions' requirements and educational institutions' curriculums on information security based on proven results from medical devices and systems introduced in the public health centers, territorial branches, community health posts and primary, secondary, tertiary hospitals. Thus, this thesis offers the method to improve information security in healthcare institutions through validation testing conducted by medical practitioners and ICT experts.

Key words : Healthcare industry, Information security awareness, Security awareness training

접수일(2019년 8월 5일), 게재확정일(2019년 9월 21일)

* 건양대학교/사이버보안공학과

** 고려대학교/정보보호대학원(교신저자)

1. 서 론

1.1 연구 배경

헬스케어 서비스는 과거와는 달리 평생동안 개인의 건강을 관리하기 위한 예방적인 의료서비스로서 진화하고 있다. 또한 기술의 발전과 산업간의 융합을 통해 초연결사회로 발전하고 있다. 예로 자동차분야는 통신과의 융합을 통해 텔레매틱스 서비스를 제공하고, 인공지능과의 융합을 통해 자율주행 자동차 시대로 발전하고 있다. 제조분야 또한 ICT와의 융합을 통해 독일의 인더스트리 4.0 등과 같이 스마트제조, 스마트 공장 등으로 변화하고 있다. 특히, 스마트 TV는 방송과 통신이 결합하고 융합하여 보다 다양한 콘텐츠를 제공하면서 헬스케어, 스마트 홈으로 서비스 영역을 확장시킬 수 있는 보다 능동적인 매체로 발전했다[1,2,5]. 현재 헬스케어 서비스는 병원을 중심으로하는 원격의료 단계에서 점차 개인 및 자택(Home) 환경에서 이용할 수 있는 환자 중심의 스마트 헬스케어(Smart Healthcare) 단계로 진화되고 있다. 개인 건강관리와 의료서비스를 보다 효율적이고 편리하게 제공받고자 하는 수요 증가와 함께 헬스케어 서비스를 통한 건강관리 서비스 기술 개발이 활발하게 진행되고 있다[3,4,5]. 이처럼 산업간의 융합과 사물인터넷, 인공지능, 클라우드 컴퓨팅, 빅데이터, 블록체인 등 기술의 발전에 따른 역기능으로서 보안문제가 사회적인 문제로 대두되고 있다. 현재 의류분야는 2005년 이후 약 300% 이상의 데이터 도난과 유출사고 건수가 증가하였다. 또한 의료기기의 해킹 사례로는 미국의 오크리지 국립연구소 내 임베디드(내장형) 시스템 신뢰성센터의 나다니엘 폴 최고과학자는 2010년에 Insulin Pump해킹 가능성을 제시하였으며,[6] 2013년 7월에는 세계적인 해킹 컨퍼런스 블랫 2013에서 발표되었다. 2016년 8월 A대학교에서는 중환자실에서 주로 쓰이는 통신기능이 없는 약물 주입기(Infusion Pump) 센서를 저가의 적외선 레이저를 이용한 해킹에 성공했다.[20] 이처럼 의료분야의 보안사고 발생가능성이 많은 연구를 통해 증명되고 있다. 이처럼 스마트의료 환경에서 정보보호에 대한 위험도가 지속적으로 증가하고 있다. 본 논문에서는 의료분야 종사자들(의사, 약사, 간호사 등)에 대한 정보보안 인식수준 실태를 조사/분석하여 정보보호 인식 수준을 강화하기 위한 효과적인 정보보호 교육 교육과정을 연구하고자 한다.

1.2 연구방법 및 구성

본 연구에서는 스마트의료 환경에서 의료분야 종사자들의 보안인식제고를 위한 NCS 기반의 효과적인 정보보호 인식교육을 위한 교육과정을 연구한다. 본 논문의 II장에서는 의료분야 보안사고 사례 및 관련 연구와, III장에서는 의료분야 정보보안 실태조사를 통해 문제점과 연구대상인 의료기관 정보보호 인식교육을 위한 교육과정과 타당성 분석을 연구하였으며, IV장에서는 활용방안, 마지막으로 V장에서는 본 논문의 결론으로 끝을 맺는다.

2. 관련 연구

2.1 스마트의료 의의

현재 의료분야는 스마트의료, 원격의료 및 진료, 진료정보 교류를 통해 상호 작용하는 멀티미디어로써 ICT 기술 및 통신 수단을 활용하여 의료인이 원격에서 환자를 대면하지 않고서도 진찰・검사・처방 등의 의료행위가 가능해지면서, 비대면 진료의 성질을 지니고 있다[1,2,5]. 스마트의료 유형으로는 다음과 같이 크게 5개의 형태로 분류할 수 있으며, ①대형병원 내의 PACS(Picture Archiving Communications System) 통신망을 이용한 원격자문, ② 유무선 정보통신을 이용한 원격의료, ③재택지에서 원격의료시스템을 활용한 재택진료, ④의료지식 전달을 의한(의료인, 환자 등) 원격교육, ⑤ 의료상담 및 진료정보 교류 등이 논의된다[9].

2.2 의료보안 사고 사례

최근 기술의 발전과 산업간의 융합을 통해 의료분야의 ICT화가 매우 빠르게 진행되면서, 크고 작은 의

료정보 유출사고를 경험하고 있다(Table 1). 미국의 신용도용범죄정보센터(Identity Theft Resource Center)의 발표자료에 따르면, 2016년에는 보건의료 관련 정보는 269건의 데이터 침해사고가 발생했다. 이처럼 의료분야의 데이터 도난과 유출사고 건수는 2005년 이후 약 300% 가량 증가했다[15]. 또한 SANS는 2014년 2월 19일 의료산업에 대한 해킹위협 진단 연구보고서에서 의료정보 해킹에 대한 심각성을 제기하였다[16]. 의료분야가 최첨단 ICT 기술과 결합되면서 개인의 건강정보 및 민감정보(생체정보, 투약정보, 병력 등)들이 데이터화 되어 외부로 전송되거나, 데이터베이스 등에 집적되고 있다. 물리적인 공간에서만 존재하던 중요한 개인의 의료정보가 사이버세상으로 집중화 되면서, 비교적 쉽게 접근할 수 있게 되었다. 의료정보는 단순한 정보주체인 개인의 문제로 국한되는 것이 아니라 전 사회적인 위험이 될 수 있기 때문에 전 사회적 차원에서 의료정보 위험관리(Healthcare Risk Management) 방안과[15] 의료기관 종사자들에 대한 의료정보 및 개인의료정보 보호를 위한 인식제고 방안이 모색되어야 할 것이다.[23-25]

〈Table 1〉 Accidents and case in medical security

Year	Description	Ref
2009	For Medical Secrets, Try Facebook	[10]
2011	A Review of the Security of Insulin Pump Infusion Systems	[6]
2012	Hacker Shows Off Lethal Attack By controlling Wireless Medical Device	[11]
2013	Froedtert Hospital hacked, patients alerted of illegal access	[12]
2014	HealthSource of Ohio data leak exposed 8,800 patients information	[13]
2014	Hospital database hacked, patient info vulnerable	[14]
2016	This ain't your dose: sensor spoofing attack on medical infusion pump	[20]

2.3 의료분야 보안 요구사항

2.3.1 Health Level7

Health Level7(이하 HL7)의 정보 인프라 기능은 의료서비스 제공에 관여하지 않지만, 업무의 효율성과 상호 운용성을 위한 최소한의 기준 뿐만 아니라 환자의 안전, 개인정보보호 및 정보 보안을 위해 필요한 보장을 제공하는지 확인하기 위해 필요하다. HL7에서는 보안과 관련된 IN.1 Security와 IN.2 Health Record Information and Management 중 보안과 관련된 인증 요건이 포함되어 있다. IN.1 Security는 엔티티의 인증, 권한, 접근통제, 사용자 정보접근, 부인방지, 데이터 교환 보호, 데이터 라우팅 보호, 정보서명, 그리고 환자의 프라이버시와 기밀성에 대한 내용으로 구성되어 있다. IN.2 Health Record Information and Management는 보안과 관련된 데이터의 유지, 가용성, 파괴 및 감사 기록에 대한 내용으로 구성되어있다.

2.3.2 HIPPA

HIPAA(Health Insurance Portability and Accountability Act)는 미국 환자의 의료정보에 대한 프라이버시권 강화를 위해 의료정보와 같은 민감한 개인정보가 적절한 프라이버시 보호책이 없이 공개되지 않을 수 있도록 하는 의료정보의 비밀보장에 관한 법률로서 대표적인 것이다. HIPAA의 보안규칙은 데이터 무결성, 기밀성 및 가용성을 보호하기 위해 관리적, 물리적, 기술적 보안대책으로 분류된다. 보안규칙은 18개의 HIPAA 표준과 36개의 구현사양이 포함되어 있다.

2.3.3 ISO/IEC 27001:2013

ISO/IEC 27000(Information technology - Security techniques - Information security management systems - Overview and vocabulary)는 ISMS 수립 및 인증에 관한 원칙과 용어를 규정하는 표준이며 ISO/IEC 27001:2013에서는 11개 정보보호 대책, 39개 보안통제항목에 대한 정보보호관리체계 구축을 위한 요구사항을 제시하고 있다.

2.3.4 ISO 277799:2016

ISO27799:2016 (Health informatics -- Information security management in health using ISO/IEC 27002)은 ISO에 의해 개발된 정보보안표준으로서 의료기관 및 개인건강 주체인 개인에게 ISO/IEC 27002의 구현을 통하여 어떻게 이러한 정보들을 보호할 수 있는지 가이드를 제공하는 것이다. 11개 정보보호 대책, 39개 보안통제항목에 대한 의료정보 보호관리체계 구축을 위한 요구사항을 제시하고 있다.

3. 의료기관 정보보호 인식교육 교육과정 개발

3.1 의료기관 정보보호 인식교육을 위한 교육과정 개발 연구 방법

의료기관 정보보호 인식교육을 위한 교육과정 개발을 위하여 “ISO/IEC 27001 Information security management systems", "ISO/IEC 27799 Health informatics - Information security management" 를 기반으로 HL7 및 HIPPA, IHE 등에서 요구하는 보안 요구사항을 포함하여 ISO 27001:2013의 14개 영역 114개 기준으로 설문지를 작성하여 배포하고, 의료기관 담당자 인터뷰를 진행하였다. 또한 보건의료분야 기관이 개인정보를 안전하게 보호하기 위한 통제항목으로 “개인정보의 안전성 확보조치”, “개인정보의 기술적·관리적 보호조치”, “의료법”과 함께 의료기관, 약국, 사회복지시설 개인정보보호 가이드라인을 비교/분석하여 점검항목을 도출하였다. 마지막으로 설문대상의 규모에 따라 1차·진료소·약국 등 소규모를 대상으로 “업무연속성, 준거성 및 정보보호 투자가 어려운 환경 등의 여건을 고려하여 12개 영역 47개 항목을 도출하여 대상 의료기관의 정보보호 실태조사를 실시하였다. 실태조사는 의료·보건·약국 등 18개 기관을 대상으로 현장조사를 수행하였다. 실태조사는 인터뷰와 설문, 현장실사 등을 통해 자산과 정보를 식별하고 정보보호 수준을 측정하였다.

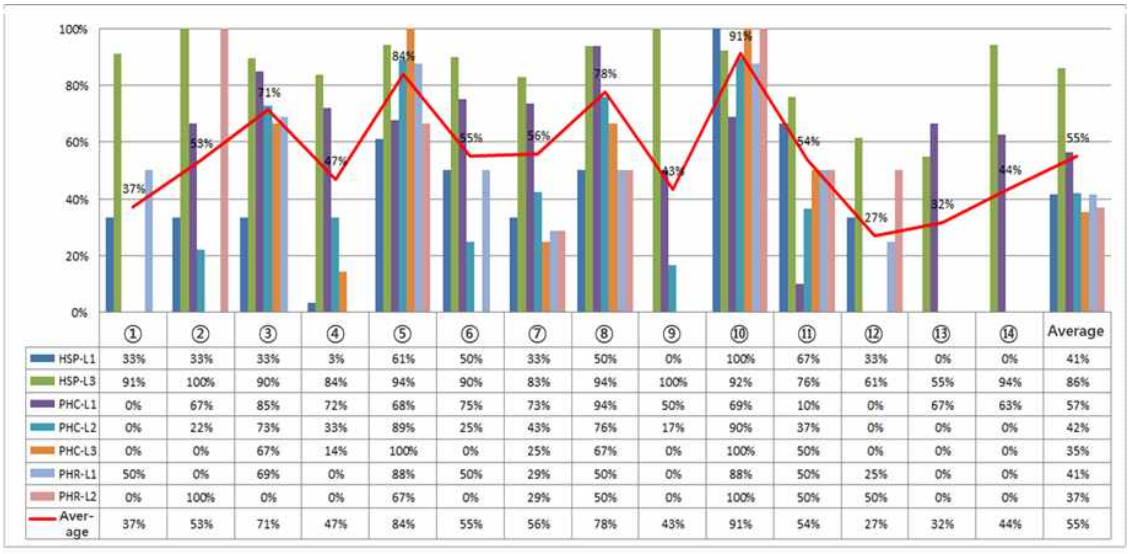
〈Table 2〉 Actual condition survey subject

code	mdeical institutions
HSP-L1	Primary hospital
HSP-L2	Secondary Hospital
HSP-L3	Third Hospital
PHC-L1	Public Health
PHC-L2	Health center
PHC-L3	Health clinic
PHR-L1	Small pharmacy
PHR-L2	Large pharmacy

의료기관 정보보호 인식교육을 위한 교육과정은 “국가직무능력표준(NCS, National Competency Standards)"을 기반으로 ISO 국제표준의 요구사항과 의료분야 정보보호 요구사항, 교육기관의 정보보호 교육과정을 참조하여 작성하였다. 또한 NIST 800-16(Information Technology Security Training Requirements:A Role-and Performance-Based Model), 800-50(Building an Information Technology Security Awareness and Training Program)의 정보보호 교육 프레임워크 참조하였다[21, 22]. 실태조사 결과에 따른 의료기관의 정보보호 수준 및 의료종사자의 수준에 따라 교육을 진행할 수 있도록 크게 4단계(Lv1 ~ 4)로 구분하였다. 교과목을 단계별로 배치하여 중복교육을 방지하였다. 연구된 의료기관 정보보호 인식 교육과정은 정보보호 전문가 및 의료분야 전문가를 통해 타당도 비율(Content Validity Ratio, CVR) 방법론을 적용하여 타당성 분석을 진행하였다.

3.2 의료기관 정보보호 수준 측정

의료기관 정보보호 수준을 측정하기 위한 실태조사 기준은 ISO/IEC 27002:2013을 준용 하여, “정보보안 정책(2)”, “정보보안 조직(7)”, “인적자원 보안(6)”, “자산관리(10)”. “접근통제(14)”, “암호통제(2)”, “물리적 및 환경적 보안(15)”, “운영보안(14)”, “통신보안(7)”, “정보시스템 취득 개발 및 유지보수(13)”, “공급자 관계(5)”, “정보보안 사고관리(7)”, “업무연속성 관리(4)”, “준수(8)” 114개 통제항목을 기준으로 의료분야 정보보호관리체계 표준인 ISO/IEC 27799:2016의 정보보호 요구사항을 맵핑하여 비교/분석을 통해 중



	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	Average
HSP-L1	33%	33%	33%	3%	61%	50%	33%	50%	0%	100%	67%	33%	0%	0%	41%
HSP-L3	91%	100%	90%	84%	94%	90%	83%	94%	100%	92%	76%	61%	55%	94%	86%
PHC-L1	0%	67%	85%	72%	68%	75%	73%	94%	50%	69%	10%	0%	67%	63%	57%
PHC-L2	0%	22%	73%	33%	89%	25%	43%	76%	17%	90%	37%	0%	0%	0%	42%
PHC-L3	0%	0%	67%	14%	100%	0%	25%	67%	0%	100%	50%	0%	0%	0%	35%
PHR-L1	50%	0%	69%	0%	88%	50%	29%	50%	0%	88%	50%	25%	0%	0%	41%
PHR-L2	0%	100%	0%	0%	67%	0%	29%	50%	0%	100%	50%	50%	0%	0%	37%
Aver-age	37%	53%	71%	47%	84%	55%	56%	78%	43%	91%	54%	27%	32%	44%	55%

①Security Policies	⑥Cryptography	⑪Supplier relationships
②Organization of Information security	⑦Physical and environmental security	⑫Information security incident management
③Human resource security	⑧Operations security	⑬business continuity management
④Asset management	⑨Communications security	⑭Compliance
⑤Access control	⑩System acquisition, development and maintenance	

(Fig. 1) Survey on the level of information security of medical institutions

복되는 항목과 의료정보보호에 고유한 통제항목을 도출하는 1차 필터링 과정을 통해 의료기관에 필요한 정보보호 통제항목을 도출 하였다. 또한 “HIPPA”, “IHE”, “HL7”, “개인정보보호법”, “의료기관 인증기준”, “보건의료분야 개인정보보호 가이드라인” 등을 분석하여 1차병원·진료소·약국 설문항목은 12개 영역 47개 항목을 도출하고, 2차·3차·보건소·지소 설문항목은 14개 영역 178개 점검항목을 도출하였다. 이를 기반으로 실태조사는 의료기관에서 반드시 준수해야 하는 정보보호 요구사항을 도출하고 정보호호 수준을 측정하여 교육과정에 활용하였다. 정보보호 수준을 측정하기 위한 분석방법으로 설문지를 작성하여 의료기관에 방문하기 전 담당자에게 사전 배포하여 인터뷰 내용을 사전에 인지할 수 있도록 하였다. 또한 의료기관 담당자의 인터뷰를 설문지 기반으로 하여 문서검토, 의료기관 실사 등을 진행하였다. 실태조사 점검결과는 의료기관 정보보호 수준측정을 위해 활용한다. 각 의료기관의 정보보호 현황을 분석하여 14개 영역의 평균은 Fig 1. 의료기관 영역별 보안수준 평가결과와 같이 전반적으로 전체 영역별 평균에 비해 1차 병원, 보건지소, 진료소의 경우 보안수준이 매우 미흡한 것으로 조사되었다. 조사한 의료기관의 정보보호 현황은 의료기관의 규모 및 매출에 따라서 정보보호 투자 예산의 차이가 크기 때문에 규모별로 정보보호 수준을 분류하였다. 정보보호 전문조직 및 전담인력을 보유한 의료기관과 전담인력 없이 겸직을 하고 있는 의료기관 간의 보안수준의 차이가 발생하고 있었으며, 의료기관의 안전성(Safety)을 확보하기 위해서는 정보보호 전담조직 과 정보보호 인력 확보, 정보보호 인식, 적절한 예산편성이 매우 중요한 것으로 확인되었다. 특히, 정보보호 인식교육은 추가 예산이나 비교적 적은 노력으로 의료기관의 정보보호 수준을 빠르게 강화할 수 있으므로, 의료기관의 효과적인 정보보호 인식교육을 위한 방법의 연구가 필요하다. 실태조사를 통한 수준측정 결과는 의료기관에 필요한 정보보호 교육 교육과정 도출에 활용한다.

3.3 의료기관 정보보호 교육과정 개발 범위

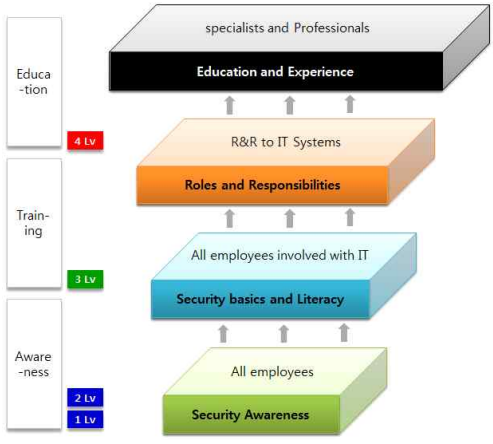
의료기관은 스마트화가 매우 빠르게 진행되고 있는 실정이다. 국내는 원격의료 및 진료정보교류를 통한 활성화 방안을 모색하고 있다. 또한 의료정보의 악용은 생명에 영향을 끼칠 수 있으므로 높은 수준의 정보보호가 필요하다. 하지만 ICT 도입을 통한 스마트의료 분야는 정보보호 대한 교육이나 관리체계가 매우 미흡한 것이 실태조사를 통해 확인되었다. 정보보호를 위해 가장 필요한 부분은 인적자원에 대한 정보보호 인식교육이다. 의료기관 정보보호 수준 측정 결과에서도 정보보호의 필요성은 인지하고 있으나, 그 방법과 정보보호 분야의 전문성으로 인한 접근이 매우 어려워 정보보호 가이드에 대한 필요성이 의료산업 현장의 요구사항으로 존재하였다.

현재 미국 같은 경우, 정보보호 인식제고 프로세스 및 프레임워크를 구성하기 위해 인식, 훈련, 교육에 대한 명확한 정의를 내리고 있으며, 특히 정보보호 교육에 대한 프레임워크는 “NIST 800-16 Information Technology Security Training Requirements:A Role-and Performance-Based Model”의 프레임워크가 가장 잘 구성되었다고 알려져 있다[19]. 정보보호 교육은 인식, 훈련, 교육 3단계로 나눌 수 있으며, 교육 대상에 따라 구성이 달라진다[19]. IT시스템에 관련된 모든 직원들에게는 “보안의 기초” 교육이 필요하며, IT시스템과의 생명주기와 관련된 각각의 역할을 담당하는 직원에게는 각 단계별 구체적인 보안 훈련이 필요하며, 또한 보안전문가들에게는 “교육과 경험”이 필요하다[16, 19]. 또한, “NIST 800-50 Building an Information Technology Security Awareness and Training Program”에서 인식, 훈련, 교육을 다음과 같이 정의하고 있다[19].

①인식 : 인식(awareness)은 훈련이 아니며 인식제고의 목적은 단순히 보안에 대한 주의를 집중시키는 것이고 개인들로 하여금 보안에 대한 염려를 인지시키는 것이며, 이에 따라 대응할 수 있도록 하려는 것이며, 이를 통해 조직의 구성원들이 IT보안에 대해 알고 발생할 수 있는 문제들에 대응할 수 있게 되며, 인식제고를 위한 프로그램이 마련되면 이를 뒷받침해 줄 수 있는 기본적인 사항들과 관련 문서들이 필요하게 됨[16, 19].

②훈련 : 훈련은 구성원들이 인식제고 프로그램을 통해 생산된 문서들을 올바르게 이해하고 보안능력을 키우며 실천할 수 있도록 해주며, 훈련은 업무와 관련된 기술을 가르쳐 개인의 원활한 업무 수행을 지원할 수 있도록 한다는 점에서 인식제고와 다르다고 볼 수 있음[16, 19]. “훈련”은 정보보호전문가가 아닌 기능적인 전문분야의 참석자로 하여금 필요한 보안스킬과 능력을 제공하는 것으로, 사람들로 하여금 특정기능을 수행하는 스킬을 가르치는 것인 반면에 인식은 어떠한 이슈에 대해 개인적인 주의를 끄는 것이 초점임[16, 19].

③교육 : 교육은 조직의 모든 기능 업무들에서 이루어질 수 있는 보안능력, 경쟁력 등을 하나의 지식으로 집약시켜 전문가를 양성하는데 초점을 맞추고 있음[16, 19].



(Fig. 2) education, training, awareness[17, 18]

의료기관의 스마트화에 따른 안전한 보호를 위해서 정보보호 수준강화를 위한 교육이 필요하고 효과적이고 효율적인 교육을 위해서는 의료분야에 적합한 정보보호 교육 교육과정 개발이 매우 필요한 실정이다[16].

3.4 의료기관 정보보호 인식교육 교육과정 개발

교육과정은 국가직무능력표준(이하, NCS)의 능력단위 “정보보호”, “보안엔지니어링”, “보건/의료” 를

기반으로 하였으며, ISO 27001:2013, ISO 27799:2016 및 정보보호 관련 교육기관과 교육과목을 참고하여 개발 하였다. 특히 NCS의 지식(Knowledge), 기술(Technology), 태도(Attitude) 개념을 적극적으로 도입하여 교과목에서 요구하는 최소 요구사항을 도출함으로써 각각의 교육과정을 수준별로 분류하고, 자가평가를 통해 개인별로 부족한 교과목을 선정하여 효율적으로 학습할 수 있는 교육과정을 연구한다.

각각의 영역에서 선정된 교육단위는 NCS의 “정보보호”, “보안엔지니어링”, “보건/의료” 직무단위에서 요구하는 기본 교과목과, 타 교육기관 및 협회 등 정보보호 전문가 교육과정을 참조하여 인식교육에 필요한 기초단계(Basic Level)를 중심으로 구성되었으나, 이는 지속적인 연구를 통해 의료기관에 최적화된 체계적인 교육과정 확보가 필요하다. 교육단위에 따라 요구하는 지식·기술·태도는 교육의 목적, 방향, 내용 등에 따라 상이할 수 있으며, 최소 요구사항이 반영되어야 효과적인 교육이 이루어 질 수 있다[19]. 이는 NCS에서 기본적으로 요구하는 교육대상자 요구사항으로 본 연구에서는 이를 적극적으로 반영하여 교육과정 구성에 활용하였으며, Table 3.와 같이 교육에서 필요한 지식·기술·태도 기준을 정의하였다[19]. 이를 통해 각 교과목 별로 교육대상자에게 필요한 기술적, 지식적, 태도적인 기준을 제시함으로써 효과적인 교육을 기대할 수 있다[19].

<Table 3> Medical information security base[19]

Div	Main contents
Knowledge	• Medical laws and policies related information protection and security • Medical privacy policy / task guideline • Key information handling outsourcing related law/regulations/procedures • Managing access authority of key information • Classification standard of information asset • Strategic planning for the development of methods of information protection services • Medical information systems proctection, security program and safety facilities • Medical classification, listing and security management of assets • Security rating method for major asset • Handling key information assets • Management method of media contained key information • Physical disposal / destruction method of key information contained in media and industrial, electronic equipment • Subjects and sort of training needed or performed in interior and exterior facility • Key information management regulations • Key information writing guide, required entry and standard of content for key information creater • Key information writing, keeping, disposal, system buildup for general staff • How to protect key information and manage security • Designing, development, utilization and management of key information protection training program • Key information educational material development methods and training techiques • Knowledge about cause of major information accident and trends • Guideline knowledge about major information accident
Technology	• Ability to analyze medical laws and policies • Ability to write a report • Ability to security plan • Security technique (OS, Server, Applicatiaon, Program, etc) • vulnerability identification ability • security development ability (Secure coding, Secure Design, etc) • Ability to use analytical tools • Ability to use security solutions(F/W, IDS, IPS, etc) • Ability to utilize medical information system (EMR, PHR, PACS, etc) • Medical information protection Security threat and risk analysis ability • Medical information system vulnerability analysis ability • Medical information security IT technology • etc
Attitude	• Law-abiding spirit for legal requirements / regulations about information security • Law-abiding spirit for legal requirements / regulations about technical security for key information • Responsible and fair attitude to key information security • Dilligent attitude to activity for medical information proctection/security • Responsible attitude as key information manager • Elaborate attitude to finding key information's vulnerability and preventing • Active and propulsive attitude to keeping information security

	• Cooperation for keeping friendly relationship with other departments for information security • Law-abiding spirit to follow fixed law / rules / regulations for information security • Resonsible attitude to keep information security • Diligent attitude to repetitive tasks for information security • Logical and creative attitude to developing curriculum and teaching materials for various educatee • Responsible attitude to careful planning for maximizing efficiency • Continued research and research will for efficiency advancement of information security education management system • Effort to apply information security guideline to work

최종적으로 도출한 의료기관 정보보호 교육과정은 교육단위 교과목 마스터는 총 26개 교육단위 요소로 구성되며, 영역별로는 산업보안(5), 의료보안 동향(2), 의료보안 위험관리(8), 의료보안감사(2), 정보보안이론(1), 의료보안기술(5), 병원 정보시스템 이해(1), 정보보안동향(2)로 개발되었다. 이는 주기적으로 의료분야 현장의 요구사항과 정보보안동향 등을 분석하여 지속적으로 연구 및 개발되어야 할 것이다.

3.5 타당성 분석

연구 및 개발된 의료기관 정보보호 인식교육과정 결과는 각 과정마다 개발된 내용의 타당성을 타당도 비율(Content Validity Ratio, CVR) 방법론을 활용하였다. CVR을 구하는 산식은 CVR = (Ne - N/2)/(N/2) (N: 응답자 수, Ne: 타당성 정도)를 활용하였다[17, 19].

$$CVR = \frac{N_e - \frac{N}{2}}{\frac{N}{2}} \quad (1)$$

$SVR : Content\ Validity\ Ratio$
$N : Nmber\ of\ response$
$N_e : (valid)\ Likert\ 4 \text{ or } (very\ valid)\ Likert\ 5$

〈Table 4〉 The minimum value of the relevant percentage[17, 19]

Personal	7	8	9	10	15	20	25	30	35
CVR minimum	0.99	0.75	0.78	0.62	0.49	0.42	0.37	0.33	0.31

현업에 종사하는 정보보호 및 의료분야 전문가 20인을 대상으로 교육과정 개발의 방법론과 결과에 대하여 리뷰를 진행하였으며, 각 항목에 대해서 타당성을 검증하였다. CVR 분석결과 교육과정에 대한 전문가의 타당도 비율(CVR)은 Table 5와 같으며, 0.42보다 높은 값으로 전체적으로 타당하다는 결론을 도출하였다.

〈Table 5〉 Educational units element CVR

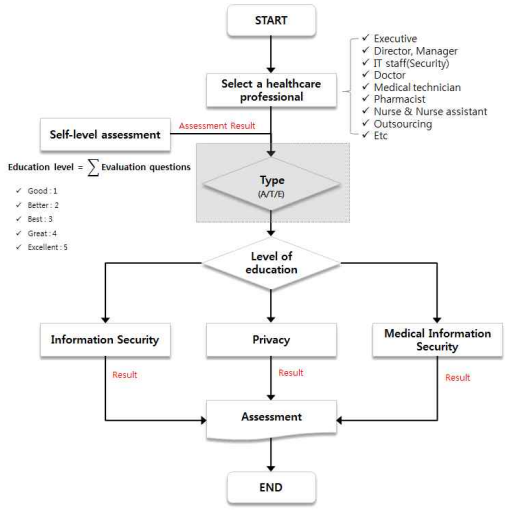
Educational distinction	Educational units element	CVR
Medical security	Medical convergence security	1
	hospital infrastructure security	1
	Medical terrorism and infrastructure security	1
	Computing platform	1
	Supply chain security	1
Medical Trends	ISO/IEC 274799 understanding	0.7
	Domestic and international trends in the Medical	0.8
Risk management	hospital environmental analysis	0.8
	To set the security range	1
	Security goals	0.9
	Asset identification	0.8
	Asset analysis	0.9
	Risk analysis	0.9
	Risk assessment	0.9
	Eliciting security requirements	0.9
	Security requirements analysis	1
	Security requirements specification	0.8
	Verification of the security requirements	0.9
	Information protection policy	1
	Protect organizational information	1
	Establishing human security measures	0.8
	Physical control of the protected areas	0.8
	System protection	1
	Office building security	0.8
	Build the application security	0.9
	Server security building	1
	Network security building	1
	Build a database (DB) security	1
	Establishment of operational security	1

	Infringement incident response	0.8
	IT established a disaster recovery system	0.9
	Information security training	1
	Security threat detection	1
	Security threat analysis	1
	In response to security threats	0.8
	Post processing	0.8
Security audit	Security audit plan	1
	Performs security audits	1
	Security audit follow-up	0.9
	Security certification preparation	1
	Security certification application	0.9
	Security certification audit	0.8
	Security authentication measures nonconformance	1
	Security certification follow-up	0.9
Security theory	Introduction to information protection	0.7
Security technologies	Network hacking and vulnerability analysis	1
	Web hacking and vulnerability analysis	0.6
	An analysis on the system hacks and weakness	0.9
	Secure coding and development security	0.8
	Database security	0.8
Understand the solution	Understanding the Medical solutions	1
Security trends	The latest trends in information security technology	1
	Information security accident case	0.9

4. 활용방안

4.1 정보보호 인식수준 자가평가

의료기관의 정보보호 실태조사 결과를 토대로 의료기관에서 가장 필요한 보안교육 분야를 분석하여 NCS 기반의 정보보호 인식교육을 위한 교육과정을 개발하였다. 이는 규모 및 환경, 직무분야에 따라 필요한 교육항목이 다를수 있다. 이를 위해 NCS에서 제공하고 있는 교육수준 자가평가 방법을 기반으로 의료기관에 정보보호 교육 유형(인식, 훈련, 교육)에 따라 수준을 평가하기 위한 자가평가 방법을 Fig 4.와 같이 연구 제안한다. 이를 활용하여 교육 대상자 스스로 자가평가를 실시하여 교육 대상자의 정보보호, 개인정보보호, 의료정보보호 교육수준을 평가 할 수 있다. 자가평가 결과는 Table 6. 교육수준 자가평가 기준에 따라 정보보호, 개인정보보호, 의료정보보호 분야에 따라 필요한 교육 유형을 선택하여 직무에 따라 필요한 정보보호 인식교육 교육과정을 개발 할 수 있을 것으로 기대한다.



(Fig. 3) Curriculum utilization flow chart

〈Table 6〉 Self-assessment Criteria in Education Level

Lv	Self-assessment criteria			Type
	Information Security	Privacy	Medical Security	
1	10~20	30~45	10~20	Awareness
2	21~30	45~60	21~30	
3	31~40	51~75	31~40	
4	41~50	76~90	41~50	Training
5	51~60	81~110	51~60	
6	61~70	111~120	61~70	
7	71~80	121~130	71~80	Education
8	81~100	131~150	81~100	

4.2 활용방안

본 연구결과는 의료기관에서 효율적인 인식제고 교육을 통한 정보보호 수준 강화를 위한 교육과정을 제시하였다. 또한 스스로 자가평가를 통해 부족한 부분을 확인할 수 있는 도구 활용을 통해 필요한 부분을 빠르게 학습하여 의료기관에서 효율적으로 정보보호 인식수준을 강화하기 위한 방법을 연구 제안하였다. 본 연구결과는 1차, 2차, 3차 병의원, 보건소, 보건지

소, 보건진료소, 약국 등에서 정보보호 인식교육을 위해 수준별, 직급별 등으로 필요한 수준에 따라 교과목을 배치함으로써 수준별 커리큘럼을 구성하는데 활용 가능 할 것으로 기대한다.

5. 결 론

스마트의료는 매우 빠른 속도로 확산되고 있다. 수많은 산업이 ICT 기술과 융합하면서 발전하고 있다. 특히, 사물인터넷(IoT) 기술의 발전으로 인하여 스마트의료는 그 확산속도가 매우 빠르다. 의료분야 특성상 사람의 생명을 다루기 때문에 정보보호는 매우 중요한 요소이다. 본 연구에서는 의료기관의 보안성을 향상시키기 위한 의료기관 정보보호 인식교육 교육과정을 연구하여 제안하였다.

앞으로 나아갈 방향으로, 먼저 본 연구에서 제시한 의료기관의 인식교육 교육과정을 토대로 실 환경에서의 교육을 통해 보안성 향상을 검증하고 우선순위를 설정하여 효과적으로 보안위협에 대처할 의료보안 인식교육 프로세스 및 보안검증 방법에 대한 연구가 필요할 것이다. 또한 안전하게 스마트의료가 확산되고 정착이 되기 위해서는 주기적으로 의료현장의 요구사항과 보안기술 동향을 파악하여 지속적으로 개발되고 개선되어야 할 것이다. 또한 현재 의료분야는 정보보호 인식의 초기단계이며, 가장 기초적인 정보보호 인식교육이 선행적으로 적용되어야 할 필요가 있다. 실효성 있는 교육을 위해서는 의료분야(1차, 2차, 3차 병의원, 보건소, 보건지소, 보건진료소, 약국 등) 별 정보보호 교육을 의무화·강제화 하고, 직급별·직무별에 따른 인식·훈련·교육을 위한 체계 연구가 필요하다.

<Table 7> medical information security awareness curriculum

Educational distinction	Education	Type	Lv	Educational units element
Medical security	Medical convergence security	Education	7	Medical convergence security
	hospital infrastructure security	Awareness	3	hospital infrastructure security
	Medical terrorism and infrastructure security	Awareness	2	Medical terrorism and infrastructure security
	Computing platform	Education	7	Computing platform
	Supply chain security	Education	8	Supply chain security
Medical Trends	Medical standard trend	Awareness	2	ISO/IEC 27799 understanding
	The Medical trends	Awareness	1	Domestic and international trends in the Medical
Risk management	Security planning	Training	5	hospital environmental analysis
		Training	4	To set the security range
		Education	7	Security goals
	Security risk assessment	Awareness	2	Asset identification
		Training	4	Asset analysis
		Training	5	Risk analysis
		Training	5	Risk assessment
	Define security requirements	Training	5	Eliciting security requirements
		Training	5	Security requirements analysis
		Training	4	Security requirements specification
		Training	4	Verification of the security requirements
	Administrative security building	Education	7	Information protection policy
		Training	4	Protect organizational information
		Training	5	Establishing human security measures
	The physical security of the building	Training	4	Physical control of the protected areas
		Training	4	System protection
		Awareness	1	Office building security
	Technical security provisioning	Training	4	Build the application security
		Training	4	Server security building
		Training	4	Network security building
		Training	4	Build a database (DB) security
	Security system management	Training	5	Establishment of operational security
		Training	6	Infringement incident response
		Education	7	IT established a disaster recovery system
		Training	4	Information security training
	Security threat management control	Training	5	Security threat detection
		Training	6	Security threat analysis
		Training	5	In response to security threats
		Training	4	Post processing
Security audit	Security audit	Training	4	Security audit plan
		Training	4	Performs security audits
		Training	4	Security audit follow-up
	Security certificate management	Training	4	Security certification preparation
		Training	4	Security certification application
		Training	4	Security certification audit
		Training	4	Security authentication measures nonconformance
		Training	4	Security certification follow-up
Security theory	Introduction to information protection	Awareness	1	Introduction to information protection
Security technologies	Network hacking and vulnerability analysis	Training	5	Network hacking and vulnerability analysis
	Web hacking and vulnerability analysis	Training	5	Web hacking and vulnerability analysis
	An analysis on the system hacks and weakness	Training	5	An analysis on the system hacks and weakness
	Secure coding and development security	Training	6	Secure coding and development security
	Database security	Training	5	Database security
Understand the solution	Understanding the Medical solutions	Awareness	2	Understanding the Medical solutions
Security trends	The latest trends in information security technology	Awareness	1	The latest trends in information security technology
	Information security accident case	Awareness	1	Information security accident case

참고문헌

[1] Seung-hwan Kim, “Trend of personal health-device standardization for u-health service,” Journal of KIISE Vol.29-1, pp.31-37, 2011.

[2] u-Health Forum Korea, “2009 u-Health Industry white paper,” 2009.

[3] Don-sik Yoo, “Review & Scheme of u-Health Standardization,” TTA 20th Anniversary Seminar, Sep. 2008.

[4] Chan-young Park, jun-ho Lim, Soo-jun Park and Seung-hwan Kim, “Technical trend of u-healthcare standardization,” Electronics and Telecommunications Trends Vol. 25, pp. 48-59, Aug. 2010.

[5] Am-suk Oh, "A Study on Home Healthcare Convergence for IEEE 11073 Standard," JKIICE Vol.19 no. 2, pp. 422-427, Feb. 2015.

[6] Nathanael Paul, Tadayoshi Kohno and David C Klonfoo, “A Review of the Security of Insulin Pump Infusion Systems,” Journal of Diabetes Science and Technology, 5(6), pp. 1557-62, Nov. 2011.

[7] ISO/DIS 27799:2014(E), "Health informatics - Information security management in health using ISO/IEC 27002," ISO, Feb. 2015.

[8] ISO/IEC 27005:2011, "Information security risk management (second edition)," ISO, Dec. 2011.

[9] Kyoung-hee Baek and yun-hwa Jang, "A Legal Study on the Relationship between In-Person and Remote Medical Treatments," Seoul Law Review, Vol. 21, pp. 449-482, Feb. 2014

[10] Katherine Chretien, "For Medical Secrets, Try Facebook," Journal of the American Medical Association, vol 302, pp. 1309, Sep, 2009

[11] Barnaby Jack, "Hacker Shows Off Lethal Attack By controlling Wireless Medical Device," RSA Conference, Feb. 2012

[12] http://fox6now.com/2013/02/14/froedte rt-hospital-hacked-patients-alerted-of- illegal-access/, "Froedtert Hospital hacked, patients alerted of illegal access," fox6now.com, Feb. 2013

[13] http://www.esecurityplanet.com/network-security/health-source-of-ohio-data-breach-exposes-8800-patients-personal-info.html, "HealthSource of Ohio data leak exposed 8,800 patients information," eSecurity Planet, Mar. 2014

[14] http://www.wired.com/2014/06/hospital-networks-leaking-data/, "Hospital database hacked, patient info vulnerable," WIRED, Mar. 2014.

[15] Dong-won Kim, Keun-hee Han, In-seok Jeon and Jin-young Choi, “Telemedicine Security Risk Evaluation Using Attack Tree," Journal of The Korea Institute of Information Security & Cryptology Vol.25, No.4, pp.951-960, Aug. 2015.

[16] C. H. Lawshe, “A Quantitative approach to content validity,” Personnel Psychology, Volume 28, Issue 4, pp. 563 - 575, Dec, 1975

[17] KOSF, The Foundation for the spread of the smart plant study on spontaneous composition, 2016

[18] NIST, "Guide for Mapping Types of Information and Information Systems to Security Categories," NIST SP800-60 vol. 1, Ayg. 2008.

[19] In-seok Jeon, Dong-won Kim, Keun-hee Han and Jin-young Choi, “Curriculum Development for Smart Factory Information Security Awareness Training," Journal of The Korea Institute of Information Security & Cryptology Vol.26, No.5, pp.1335-1348, Oct. 2016.

[20] Young-seok Park, Yun-mok Son, Ho-cheol Shin, Doh-yun Kim and Yong-dae Kim, “This ain’t your dose: Sensor Spoofing Attack on Medical Infusion Pump,” usenix, WOOT'16 Proceedings of the 10th USENIX Conference on Offensive Technologies, Pages 189-199, Aug. 2016.

[21] NIST, "Building an Information Technology Security Awareness and Training Program," NIST SP800-50, Oct. 2003.

[22] NIST, "Information Technology Security Training Requirements:A Role- and Performance-Based Model," NIST SP800-16, Apr. 1998.

[23] 한국융합보안학회.융합보안논문지 제16권 제7호 (2016) pp.21-29 "의료클러스터 기반의 빅 데이터 환경에 대한 IP Spoofing 공격 발생시 상호협력 보안 모델 설계" https://www.earticle.net/Article/A301561

[24] 한국융합보안학회.융합보안논문지 제14권 제3호 (2014) pp.11-19 "체내 이식형 의료기기의 보안성 향상을 위한 3-Tier 보안 메커니즘 설계" https://www.earticle.net/Article/A224196

[25] 한국융합보안학회.융합보안논문지 제18권 제5호 (2018) pp.75-81 "의료융합 환경에서 수용성을 고려한 비용 효율적 보안체계구축 방안 연구 : 중소의료기관을 중심으로" https://www.earticle.net/Article/A346536

[著者紹介]

김 동 원 (Dong-Won Kim)
2009년 2월 서울과학기술대학교 학사
2012년 2월 건국대학교 석사
2014년 2월 고려대학교 박사 수료
2017년~현재 건양대학교 사이버보안공학과 조교수
email : blast@konyang.ac.kr

한 근 희 (Keun-Hee Han)
서울과학기술대학교 학사
한양대학교 석사
고려대학교 박사
2019년~현재 고려대학교 정보보호대학원 초빙교수
email : khhan@formal.korea.ac.kr