https://doi.org/10.33778/kcsa.2023.23.1.079

정밀의료 병원정보시스템(P-HIS) 정보보호모델 개선 방안에 관한 연구★

김 동 원*

요 약

개인 건강정보, 유전자정보, 임상정보 등을 활용한 정밀의료(Precision Medicine)는 차세대 의료산업으로 성장하고 있다. 국내에는 의료기관과 정보통신 기업이 협력하여 지난 5년간 약 90여개 1차 의료기관을 대상으로 클라우드 기반 정밀의료 병원정보시스템(P-HIS)을 보급하였으며, 향후 4년간 1·2차 의료기관을 중심으로 보급 및 확산을 진행하고 있다. 정밀의료는 사람의 건강과 생명에 직결되기 때문에 정보보호 및 보건의료정보 보호 문제가 매우 중요하다. 이에 따라, 본 논문에서는 클라우드 기반의 정밀의료 병원정보시스템에서 활용 가능한 정보보호 모델의 선행연구 분석을 통하여 최종적으로 정밀의료 병원정보시스템(P-HIS)의 정보보호 개선 방안을 연구 제안한다.

A Study on the Improvement of Information Security Model for Precision Medicine Hospital Information System(P-HIS)

Dong-Won Kim*

ABSTRACT

Precision Medicine, which utilizes personal health information, genetic information, clinical information, etc., is growing as the next-generation medical industry. In Korea, medical institutions and information communication companies have coll aborated to provide cloud-based Precision Medicine Hospital Information Systems (P-HIS) to about 90 primary medical ins titutions over the past five years, and plan to continue promoting and expanding it to primary and secondary medical insti tutions for the next four years. Precision medicine is directly related to human health and life, making information protecti on and healthcare information protection very important. Therefore, this paper analyzes the preliminary research on inform ation protection models that can be utilized in cloud-based Precision Medicine Hospital Information Systems and ultimately proposes research on ways to improve information protection in P-HIS.

Key words : Precision medicine, Healthcare Information Security, Information Security, Cloud computing security, Big data security

접수일(2023년 1월 12일), 수정일(1차: 2023년 3월 17일), (2차: 2023년 3월 24일), 게재확정일(2023년 3월 28일)

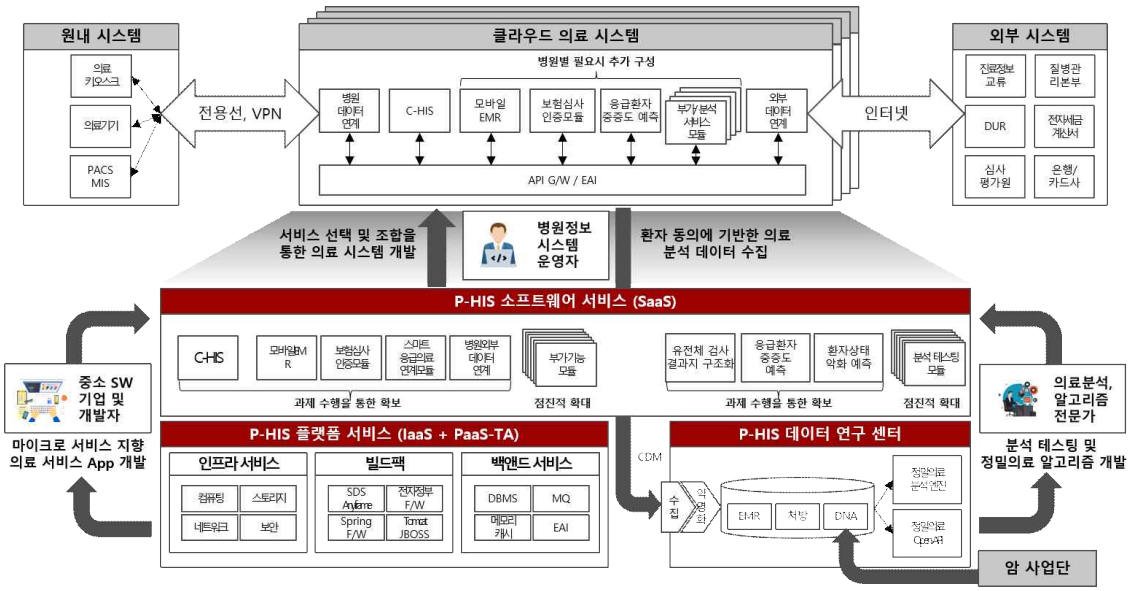
★ 이 논문은 2022년도 건양대학교 학술연구비 지원에 의하여 이루어진 것임.

* 건양대학교/사이버보안학과

1. 서 론

현재 의료서비스의 패러다임은 기존과 동일한 질환 환자에게 일률적으로 적용하던 방법과는 다르게 개인별로 유전정보 및 생활환경 등에 따라 적용되는 개인맞춤형 의료서비스인 정밀의료로 변화될 것이다[1]. 정밀의료(Precision medicine)란 임상정보, 유전체 정보, 생활환경 정보, 습관 정보 등을 활용하여 정밀하게 환자 각 개인을 분류하고 이를 고려한 최적의 맞춤형 의료(예방, 진단, 치료)를 제공하는 차세대 의료 패러다임이다. 또는, 환자의 특성에 맞는 의학적 치료 방식을 재단하는 것으로, 궁극적으로 생명을 살리기 위한 질병의 뿌리와 치료법 개발에 대한 새로운 이해를 위해 기술, 과학, 의료기록을 이용하는 것으로 정의하고 있다[2]. 병원 지능화를 위한 핵심요소인 데이터의 확보를 위해 병원은 병원정보시스템(Hospital Information System, HIS)을 통해 다양한 형태의 데이터를 수십년 간 디지털화 하려고 노력해 왔다[3].

정밀의료는 개인에게 최적화된 의료서비스를 제공하기 위하여 개인의 민감정보, 개인정보, 의료정보 뿐만 아니라 환경정보, 라이프로그 등 일상생활 속 다양한 정보 등 개인의 건강에 영향을 줄 수 있는 모든 정보를 수집·분석한다. 정밀의료 서비스는 개인의 의료정보 및 데이터 등의 해킹으로 인한 유출, 노출, 변조 등으로 인한 보안 위협은 생명과 직결될 수 있으므로 보안성(Security)과 안전성(Safety)을 반드시 보장하여야 한다[4]. 전 세계적으로 정밀의료 실현을 위해 개인 맞춤형 의료 빅데이터를 활용한 서비스가 클라우드 컴퓨팅 기술을 통해 활성화되고 있다. 국내에서는 정밀의료 병원정보시스템(P-HIS)이 개발되어 개방형 클라우드 플랫폼인 파스타(PaaS-TA) 환경에서 제공되고 있다[5]. 빅데이터를 활용한 정밀의료는 빅데이터 속성인 대량(Volume), 급속도(Velocity), 다양한 형태(Variety), 가치 있는(Valuable) 정보로 생산되고 있으며, 빅데이터 위험 중 개인정보(Privacy) 침해는 매우 중요한 최우선 과제이며[6], 개인의 유전정보 등 개인에 대한 민감정보를 활용하는 정밀의료 병원정보시스템은 정보유출과 개인정



(Figure 1) 정밀의료 병원정보시스템(P-HIS) 구성 및 아키텍처

보(Privacy) 침해에 따른 보호가 매우 중요하게 다루어 지고 있다[7]. 따라서 본 연구에서는 안전한 정밀의료 병원정보시스템(P-HIS)의 실현을 위하여 클라우드와 의료분야의 국내·외 보안 요구사항을 조사/분석하여 클라우드 환경에 적용 가능한 정보보호 요구사항을 분석하고 정밀의료 병원정보시스템(P-HIS)에서 발생가능한 정보보안 문제점과 정보보호 개선을 위한 정보보호 모델의 개발 방향을 제시하고자 한다. 또한, 정보보호 모델의 개발 방향의 신뢰성을 검증하기 위해 하기 위해 관련 실무자와 전문가를 대상으로 설문조사를 통해 정밀의료 병원정보시스템 구축 시 정보보호모델에서 제시된 각각의 영역별 보호활동이 얼마나 중요한 영향을 미치는지 각 7점 척도로 측정하여 본 연구를 검토하고자 한다.

2. 관련 연구

정밀의료는 유전정보, 생활습관 등 개인 건강정보를 토대로 최적화된 진단 및 치료를 적용하는 헬스케어 패러다임이다. 인간 유전체 프로젝트(Human Genome Project, HGP)의 완성으로 인류는 스스로를 규명하는 생물학적 근간인 유전자 염기서열 정보를 확보했고, 이를 기반으로 다양한 생명현상을 이해하고 혁신적인 치료 방안을 고안하는 데 활용하고 있다. 정밀의료의 실현 가능성 중 핵심요인은 유전체 염기서열 해독 비용의 하락이며, HGP 완료로 약 1/20,000인 5,000 달러로 낮아졌으며, 2015년 10월 기준으로 1,245 달러로 낮아져 염기서열 백만 개를 해독하는 데 필요한 비용은 고작 0.014 달러이다. 이는 빅데이터 분석 기술로 다량의 데이터를 처리할 수 있으므로 실현이 가능하게 되었다[8]. 현재까지 질병에 대한 치료는 오랜 기간의 치료 경험의 축적을 통해 표준화되고 체계화된 방법을 통해 같은 질병인 모든 환자들에게 경우 동일한 방식으로 이루어졌으나, 개개인의 유전정보와 환경정보 등을 빅데이터를 통해 수집·분석하여 적용되는 개인맞춤형 치료는 매우 효과적임이 입증되었다[9]. 정밀의료를 통한 대표적인 사례로는 폐암 EGFR 유전자 변이에 따른 표적치료제가 있다[10]. 정밀의료는 진료 또는 연구 과정에서 빅데이터를 활용하여 수집·분석된 데이터를 활용하며, 이러한 통합 정보는 향후 질병에 대한 더 적합한 치료 방법을 개발하는 데 핵심적인 자료가 된다[11]. 정밀의료는 개인에게 최적화된 의료서비스를 제공하는데 목적이 있으므로, 개인의 의료정보, 민감정보, 건강정보, 사생활 정보, 환경정보 등을 수집하여 활용한다[12]. 정밀의료에서는 유전체 분석과 관련된 표준이 중요한 이슈 사항으로 떠오르고있어 이에 따른 국제표준과기구(Inter

〈Table 1〉 정밀의료/정보보호 관련 표준 현황[4,13]

구분	표준명
ISO 25720	Health informatics - Genomic Sequency variation Markup Language(GSVML)
ISO/TS 22220	Health informatics - Identification of subjects of health care
ISO 8601	Data elements and interchange formats - information interchage - Representation of dates and times
ISO/TS 27527	Health informatics - Provider identification
ISO 11615:2012	Health inforatics - identification of medicinal products - data elements and structures for the unique identification and exchange of regulated medicinal product information
ISO/TS 20428	Health informatics - Data elements and their metadata for describing structured clinical genomic sequence information in electronic health records
ISO 27799	Health informatics -- Information security management in health using ISO/IEC 27002
NIST	Cybersecurity Framework ver 1.1
HIPAA	Health Insurance Portability and Accountability Act
HITRUST	Common Security Framework
FISMA	Federal Risk and Authorization Management Program(FedRAMP)
CSA	Cloud Security Alliance - Open Certification Framework(CSA OCF)

〈Table 2〉 주요 5개국 정밀의료 추진 현황[15]

구분	정밀의료 플랫폼	정책	중점질환	단기 목표	장기 목표
한국	Dr.Answer PaaS-TA	정밀의료 사업단	폐암, 위함, 대장암	·2만명 규모의 데이터 구축 ·정밀의료 병원정보시스템 (P-HIS) 기관 90여개 보급	·암, 희귀·난치 질환 환자 40만명, 일반인 60만명 데이터 확보 ·향후 4년간 1·2차 의료기관 중심으로 클라우드 기반 병원정보시스템 보급·확산
미국	All of US (All of Us Research Program	정밀의료 추진계획(PMI)	암	100만명 이상의 데이터 수집	건강 및 헬스케어 전반에서 정밀의료 활용
영국	UK Biobank	2020 개인 맞춤형 헬스케어 구상 프레임워크 보고서	암, 희귀질환	500만병의 유전체 정보 확보	정밀의료의 실현, 유전질환, 희귀질환, 암, 전염병의 유전학적 원인 규명
일본	PeOPLe	질병 극복을 위한 게놈 의료 실현화 프로젝트	질병 극복을 위한 게놈 의료 실현화	40만명의 유전체 정보 취합해 연구에 활용	의료혁신 5개년 전략 수행
중국	정밀의료 지식뱅크 및 공유 플랫폼	정밀의료 5개년 발전계획	암(간, 위)	100만명의 유전체 분석	2030년까지 정밀의학에 약 107조원 투자

national Organization for Standardization) 기술위원회 215(보건의료정보)에서는 관련 표준을 제안하고 있으며, 클라우드 기반 병원정보시스템 구현을 위한 클라우드 보안 표준과 정보보호 표준을 함께 고려하여야 할 필요가 있다. 주요 정밀의료 및 정보보호 관련 표준 현황은 Table 1.과 같다[13]. 또한, 국내에서는 과학기술정보통신부와 보건복지부에서 클라우드 기반 정밀의료 병원정보시스템(P-HIS)이 2017년부터 2021년 까지 총 308,55억원을 투자하여 현재까지 약 90여 개의 1차 의료기관에 보급되어 운영되고 있다. 정밀의료는 미국과 한국 외에도 전 세계적으로 활발히 연구·개발되고 있으며, 주요 5개국 정밀의료 현황은 다음 Table 2.와 같다[14,15].

NIST “Cybersecurity Framework"는 미국의 국가안전보장과 경제 안보를 위한 주요 사회기반시설에 대한 공통 보안프레임워크로서 사회기반시설에 공통되는 정보보안 대책 우수사례, 기대되는 성과, 참고 정보가 제시되고 있으며 Frameork Core, Framework Profile, Framework Implementation Tier의 3가지 요소로 구성되어 있다[4]. 2014년 2월 초판 발표된 후 2018년 4월 CSF v.1.1이 발표되었으며, Supply Chain Risk Management 보안 요구사항이 포함되어 제시하고 있다[16]. 보건의료 분야는 ISO/IEC 27799 ”Health informatics - Information security management"에서 정보보호관리체계를 요구하고 있다. 또한, 미국이 1996년에 의료정보보호법이라 할 수 있는 HIPAA(Health Insurance Portability and Accountability Act)를 제정하여 시행하고 있다[1]. 정밀의료는 복잡하고 정교한 예측 모형을 구현하기 위해서 방대한 양의 데이터 확보와 데이터를 구성하고 관리하고 해석하는 능력을 필요로 하기 때문에 클라우드 기반의 정밀의료는 빅데이터가 필연적 관계이다[17]. 또한, 정밀의료를 활용한 맞춤형 의료는 개인 환자의 맞춤화된 치료 전략을 현실화 하기 위해서는 클라우드 컴퓨팅 기반의 정밀의료가 필요하다[17]. 의료분야는 HITRUST CSF, HIPPA, IHE 등과 클라우드 보안 분야의 CSA CCM, FedRAMP에서 요구하는 보안 요구사항을 비교 분석하고 국내외 보건의료 및 정보보호 요구사항과 정밀의료 법·제도, 기술, 사고사례 등을 비교 분석하여 정밀의료 병원정보시스템(P-HIS)의 클라우드 서비스 별 표준내용을 구성하며 Table 3.과 같다.

〈Table 3〉 NIST CSF를 활용한 Cloude 기반 서비스 별 P-HIS 정보보호 요구사항

유형	카테고리	Public IaaS	PaaS-TA	SaaS
식별	자산 관리, 지침, 사업환경, 위험평가, 공급망			
보호	접근 제어	사용자 인증 및 권한 관리	사용자 인증 및 권한 관리	사용자 인증 및 권한 관리
		물리적 출입통제	API 키 관리	다중 인증
		네트워크 분리		API 키 관리
		VM 간 독립성 보장		
		API 키 관리		
	데이터 보안	하드웨어 멀티테넌트 환경 보안	컨테이너 멀티테넌트 환경 보안	어플리케이션 멀티테넌트 환경 보안
		네트워크 암호화		데이터 이동 흐름 파악
		데이터 VM 이전 보안		데이터 폐기
		백업시스템 구축		데이터 암호화
				사용 종료된 권한 해제
				비식별화
				데이터 무결성 보장
				데이터 통신 암호화
	유지보수	장비 유지보수	소프트웨어 유지보수	소프트웨어 유지보수
	교육훈련	내부인력 보안	내부인력 보안	내부인력 보안
	절차	침해사고 대응 계획 수립	침해사고 대응 계획 수립	침해사고 대응 계획 수립
		백업 정책 수립	컨테이너 관리 방안 수립	민감정보 접근 보안정책 수립
		장비 폐기 및 재사용 정책 수립		소프트웨어 개발보안 정책 수립
		네트워크 보안 정책 수립		
		가상자원 관리 정책 수립		
	방어 기술	IaaS 인터페이스 및 API 보안	PaaS-TA 인터페이스 및 API 보안	SaaS 인터페이스 및 API 보안
		백업 수행	결함허용 및 가용성 지원	정보유출 차단 솔루션 적용
		네트워크 정보보호 시스템 운영	O/S 보안 강화	시큐어 코딩
		이중화	악성코드 통제	웹공격 차단
		하이퍼바이저 보안	안전한 개발환경 제공	앱위변조, 악성앱 차단
		가상 소프트웨어 보안	백앤드 서비스 보안	
탐지	이상행위 및 이벤트	탐지된 이벤트 분석	탐지된 이벤트 분석	탐지된 이벤트 분석
	모니터링	추적 감사	추적 감사	추적 감사
		네트워크 모니터링	PaaS-TA 성능 및 용량 모니터링	SaaS 성능 및 용량 모니터링
		IaaS 성능 및 용량 모니터링	PaaS-TA 컨테이너 및 백앤드서비스 보안 취약점 점검	데이터 변경 모니터링
		네트워크 및 보안 장비 취약점 점검	O/S 취약점 점검	개인정보 / 민감정보 / PMI 데이터 유출 점검
		하이퍼바이저 보안 취약점 점검	악성코드 탐지	웹 취약점 점검
				모바일 악성코드 탐지
	탐지 절차	탐지절차의 지속적인 개선	탐지절차의 지속적인 개선	탐지절차의 지속적인 개선
대응	대응계획, 완화, 분석, 개선, 커뮤니케이션			
복구	복구계획, 개선, 커뮤니케이션			

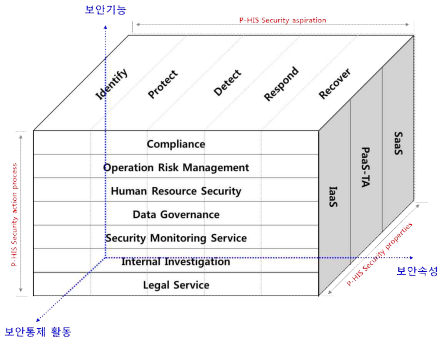
3. 정밀의료 병원정보시스템(P-HIS) 정보보호모델 개선방안

3.1 P-HIS 정보보호 모델 개념

본 연구에서 제시한 P-HIS 정보보호 모델은 국내 정밀의료 병원정보시스템 확산을 위해 필요한 안전성과 보안성을 강화하고 관리하기 위한 정보보호 모델로서 이는 다른 일반 분야의 정보시스템과 달리 의료정보보호, 개인정보보호, 클라우드 서비스 별 보호를 함께 정의하고, 사회기반시설에 대한 공통 보안프레임워크인 NIST “Cybersecurity Framework" 의 개념을 적용하여 정의한다. 본 정보보호모델은 기존 모델과 비교하여 보안활동을 고려하기 위한 전략연계모형을 기반으로 연구되었으며, 이에따라 정밀의료의 비즈니스와 IT측면을 함께 고려하여 연구한다.

3.2 P-HIS 정보보호 모델의 구성

P-HIS 정보보호 모델은 ISO/IEC 27001, HIPAA, 정보보호표준표델을 준용하고, 비즈니스 및 IT와 조화로운 보안활동을 고려하기위해 전략연계모형인 Henderson, J. and N. Venkaraman의 Strategic Alignment Model을 활용하여 구성한다[18]. 모형을 구성하는 3개의 축은 목적(Aspiration), 프로세스(Action Process), 특성(Properties)으로 전략연계모형의 원론적인 의미를 반영하여 정보호호 관점에서 목적은 보안기능으로 프로세스는 보안통제활동으로 특성은 보안유형으로 투영하여 세 축을 Figure 2.와 같이 구성한다.



(Figure 2) P-HIS 정보보호 모델 구성

의료분야는 정보보호만을 강조하다 보면 효율성을 강조하는 IT와 대립하게 되며 결과적으로 비즈니스 성과를 저하하는 결과를 초래할 가능성이 높다[19]. 비즈니스 및 IT와 조화로운 보안활동을 정의하기 위한 전략연계 모형에 정보보호 요건을 투영한 전략연계 모형 세 축의 구성은 다음과 같다.

- 목적(Aspiration)-보안기능: 클라우드 컴퓨팅을 IT활동으로 본다면 정보보호 측면에서는 보안역할(식별, 보호, 탐지, 대응, 복구)을 의미함
- 프로세스(Action Process)-보안통제 활동: P-HIS 보안 측면에서는 목적(위협요소 제거)을 달성하기 위한 활동인 보안통제 활동으로 설명되며, P-HIS 보안 측면에서는 P-HIS 유형(IaaS, PaaS-TA, SaaS)에 따라 보안통제 활동이 달라지기 때문에 중요한 요소로서, 보안유형을 의미함
- 특성(Properties)-보안속성: P-HIS는 클라우드 컴퓨팅 환경과 의료분야가 접목된 형태의 시스템으로 클라우드 컴퓨팅의 특성과 의료분야의 특성을 고려한 정보보호 속성을 의미함

보안기능 축은 P-HIS의 제거대상 보안위협 요인을 나타내며 세계적인 산업체 표준으로 CSA(Cloud Security Alliance)에서 설문조사를 통해 도출한 항목과 NIST CSF(CSF)들을 모델링하여 P-HIS 환경의 5개 보안기능(식별, 보호, 탐지, 대응, 복구)을 기준으로 한다. 보안통제 활동 축은 위협요인을 감소시킬 목적으로 수행하는 활동을 나타내며, NIST SP 500-299에 언급된 CSA TCI-RA(Trusted Cloud Initiative -. Reference Architecture)의 비즈니스 운영 지원 서비스(BOSS: Business Operation Support Service)를 참조하며 7개의 정보보호 유형에 따른 통제활동(운영 리스크 관리, 인적자원 보안, 데이터 거버넌스, 모니터링, 내부 사고조사, 재해복구, 준거성)을 정의한다. 정보보안 속성 축은 인간의 건강정보, 의료정보를 클라우드컴퓨팅 환경을 통해 의료행위에 활용하기 때문에 악의적인 공격을 통해 개인의 건강과 궁극적으로는 생명에 위협을 초래할 수 있으

므로 전통적인 정보보호 속성인 기밀성(Confidentiality), 무결성(Integrity), 가용성(availability)을 보장하고, 정밀의료정보의 안전한 보호를 위한 보다 높은 차원의 무결성, 신뢰성, 회복성을 보장하기 위한 정보보호 체계가 필요하다.

3.3 P-HIS 정보보호 통제항목

국내 정밀의료 병원정보시스템은 클라우드를 기반으로 구성되며, 특히 PaaS 플랫폼은 국내 환경에 맞도록 확장 개발한 컨테이너 기반 오픈소스인 국산 소프트웨어를 지원하고 사용자 편의성을 향상시킨 PaaS-TA 플랫폼을 적용하고 있다[5]. 클라우드 서비스별로 식별, 보호, 탐지, 대응, 복구 유형에 따라 국내 관련 법에서 요구하는 항목은 "필수" 요구사항이며, 국내 관련 법에서 요구하지 않으나 클라우드 보안인증제 등에서 요구하는 항목은 "권고", 그 이외 항목은 선택으로 분류하여 구성한다[4].

〈Table 4〉 IaaS 정밀의료 보안통제의 보안등급 개요

Type	Essential			Recommen-dation			Optional		
	IaaS	PaaS-TA	SaaS	IaaS	PaaS-TA	SaaS	IaaS	PaaS-TA	SaaS
Identify	2	2	2	4	4	4	0	0	0
Protect	11	2	7	5	3	3	6	7	7
Detect	1	0	0	3	3	3	2	2	3
Respond	0	0	0	3	3	3	2	2	2
Recover	0	0	0	2	2	2	1	1	1
Total	14	4	9	15	15	15	10	12	13

4. 통계 검증 방법

4.1 조사 방법

본 연구에서 제시한 P-HIS 정보보호 모델은 온라인 설문조사 방식을 사용한다. 설문지의 배포는 개인별 전자우편이나 SNS 등을 활용하여 설문조사 링크를 송신하고 응답자가 PC, 스마트폰 등 다양한 환경에서 참여가 가능하도록 자가기입식 방식으로 데이터를 수집한다. 설문표본대상자는 Table 5와 같이 정보보호 전문가 및 병원 담당자, 관련 산업체 담당자 등 정보화 담당자와 기관 등의 정밀의료 관련 전문가를 대상으로 한다. 설문조사를 통해 P-HIS 정보보호 모델에서 제시된 각각의 정보보호활동이 얼마나 중요한 영향을 미치는지에 대해서 각 7점 척도로 측정한다. 본 설문조사를 통해 제안된 정보보호 모델이 정밀의료 병원정보시스템에 더 적합한 모델이라는 것을 통계적으로 검증하고자 한다.

〈Table 5〉 설문표본대상자

구분	설문 수	백분율(%)
계	153	100%
정보보호 전문가	58	62%
의료 전문가	51	59%
관련 산업체	44	88%

4.2 통계 검증

본 연구모델의 검증은 각 정보보호활동을 측정변수로 하고 정보보호 요구사항을 잠재변수로 하며, 정보보호 모델의 보안기능, 보안속성, 보안통제활동을 매개변수로 정의하여 각각에 대해 측정변수로 정의한다. 설문조사에 활용한 데이터의 신뢰도 평가를 위해 개념 신뢰도(composite Reliability)를 활용한다. 이는 지표의 내적 일관성을 측정하는 지표로 활용된다. 개념 신뢰도인 CR과 평균분산 추출 AVE 값을 계산하여 측정모형의 개념 신뢰도를 판단한다. 이를 계산하기 위해 측정모형을 확증적 요인분석(Confirmatory factor analysis, CFA)에 실행시켜 표준화회귀계수, 상관관계, 분산추정치 값 등을 이용하여 계산하였다. Table 6.과 같이 개별 측정 변수들의 표준화회귀계수가 0.7 이상이고, CR이 0.7 이상, AVE가 0.5 이상이면 개념 신뢰도와 판별 타당도는 확보되었다고 판단할 수 있다[1]. 또한 확인적 요인분석인 AMOS를 이용하여 측정모델에 대한 구조방정식모형의 적합도를 평가하여 검증한다. 적합도 평가 결과 값에서 카이 스퀘어(χ^2)값, p-value는 0.05 이상, $\frac{\chi^2}{DF(Q)}$ 은 3보다 작아야 하며, 기초적합지수(Goodness of fit Index, GFI), Adjust GFI, NFI(Normed fit Index) 값이 0.9이상, RMSEA는 0.08 이하, 개별 측정변수들의 표준화회귀계수 결과 값이 0.7 이상인지 확인하여 설문

결과에 대한 신뢰도를 검증하였으며, 모두 적정한 결과를 나타내어 본 P-HIS 정보보호 모델이 적합하고 신뢰도가 있다고 판단할 수 있다[1].

〈Table 6〉 P-HIS 개념신뢰도(Cronbach`s α) 측정결과

변수항목		분산추정치	Cronbach's α	분산 추정합	Cronbach's α
보안 기능	FA1	1.342	0.919	6.626	0.834
	FA2	1.748	0.895		
	FA3	1.012	0.939		
	FA4	1.079	0.935		
	FA5	1.079	0.935		
보안 통제 활동	CA1	1.375	0.948	8.522	0.850
	CA2	1.543	0.942		
	CA3	2.470	0.907		
	CA4	1.962	0.926		
	CA5	1.170	0.956		
보안 속성	AA1	1.043	0.979	10.241	0.915
	AA2	1.450	0.971		
	AA3	1.217	0.976		
	AA4	1.249	0.975		
	AA5	1.472	0.971		
	AA6	1.427	0.972		
	AA7	1.247	0.975		
	AA8	1.132	0.977		

5. 결론

현재 국내에서는 클라우드 정밀의료 병원정보시스(P-HIS)이 고려대의료원을 중심으로 14개 의료기관과 정보통신 기업이 협력하여 2017년부터 현재까지 1차의료기관 90여개에 보급되었으며, 2023년부터 4년간 1·2차 의료기관 중심으로 보급·확산이 진행되고 있다. 정밀의료는 특성상 사람의 생명을 다루기 때문에 정보보호는 매우 중요한 요소이다. 본 연구에서는 정밀의료 병원정보시스템에서 필요한 정보보호 모델을 연구 제안하였으며 이를 통해 국내의 정밀의료 정보보호 방안을 개선 발전시킬 수 있는 기반을 마련하였다. NIST CSF를 기본 축으로 CSA CCM, HIPAA, HITRUST, IHE 등 정밀의료 병원정보시스템(P-HIS)의 정보보호 통제항목을 선정하였다. 기존 연구에서는 안전한 클라우드 기반의 정밀의료를 실현하기 위한 정보보호 요구사항을 식별하였으나, 본 논문은 해당 정보보호 요구사항을 실제 정밀의료 병원정보시스템의 정보보호 모델을 제안하여 실제 검증할 모델을 제시한 것으로 의의가 있다고 할 수 있다. 본 정밀의료 병원정보시스템(P-HIS) 정보보호모델이 기존 안전한 클라우드 기반의 정밀의료 정보보호모델에 비해서 통계 검증을 통해 신뢰성이 있으며, 보안활동을 고려하기위한 전략연계모형으로 제안되어 정밀의료 분야의 비즈니스 및 IT와 조화로운 보안활동 강화를 위한 모델로서 개선되었다.

본 논문에서는 설문조사를 통해 수집한 데이터를 통계분석과 검증방법을 토대로 연구하였으며, 정밀의료 병원정보시스템(P-HIS) 정보보호 모델의 신뢰성이 확보되었다. 향후 본 논문에서 제시한 연구모형을 토대로 측정변수에 대하여 설문지를 구체화하고 관련 전문가 등에게 연구모형에 대한 검증을 거쳐 설문을 시행하고 분석하여 연구결과를 확인해 볼 수 있다.

참고문헌

[1] 신제수, et al. "정밀의료실현을 위한 보건의료정보 보호모델에 관한 실증적 연구." 한국 IT 정책경영학회 논문지 8.4 (2016): 209-217.

[2] Ashley, Euan. A., "The precision medicine initiative: a new national effort", JAMA, Vol. 313(21), pp. 2119-2120. Jun, 2015.

[3] 손병은, and 정성문. "의료인공지능 연구/개발 및 실용화를 위한 지능형 병원정보시스템 모델." 한국융합학회논문지 13.3 (2022): 67-75.

[4] 김동원. (2022). 클라우드 기반 안전한 정밀의료 실현을 위한 보건의료정보 보호 적용 방안에 관한 연구 . 융합보안논문지, 22(3), 69-78.

[5] 최종수, 김성은, and 이상헌. "헬스케어 클라우드 동향과 정밀의료 병원정보시스템 (P-HIS) 개발 사업." 한국통신학회지 (정보와통신) 35.2 (2018): 3-9.

[6] 정영철, "의료분야 빅데이터 활용을 위한 개인정보 비식별화 규정 현황과 과제", 보건복지포럼, pp.50-6 0, 2015.

[7] 김동원, and 한근희. "스마트의료 환경에서 보안위협 대응을 위한 최근 연구동향." 한국통신학회지 (정보와통신) 35.2 (2018): 95-99.

[8] 문세영, 장기정, 김한해. (2020). 정밀의료의 성공전략. 한국과학기술기획평가원, R&D InI

vol.15, 14-32, 2020.
[9] 대석허. "Personalized cancer medicine: present status and future perspectives." Journal of the Korean Medical Association 58.11 (2015): 1021-1026.
[10] Chen, Fan, et al. "Cellular Origins of EGFR Driven Lung Cancer Cells Determine Sensitivity to Therapy." Advanced Science 8.22 (2021): 2101999.
[11] 윤혜선. "정밀의료를 위한 데이터 거버넌스에 관한 연구-미국의 All of Us Research Program 사례를 중심으로." 바이오경제연구 2 (2019).
[12] 신재승, et al. "정밀의료 생태계 구축을 위한 데이터 수집 및 연계 국내 동향." 한국웰니스학회지 15.1 (2020): 73-81.
[13] Song, Jun-Hyeon, Il-Gon Kim, and Seon-Ju An. "표준· 시험인증 기술동향-정밀의료데이터 표준화 동향." TTA Journal (2017): 86-91.
[14] 보건복지부, 정밀의료 병원정보시스템 성과보고회, (2021),
[15] Collins, Rory. "What makes UK Biobank special?." Lancet (London, England) 379.9822 (2012): 1173-1174.
[16] White, Gregory B., and Natalie Sjelin. "The NIST Cybersecurity Framework." Research Anthology on Business Aspects of Cybersecurity. IGI Global, 2022. 39-55.
[17] 한성민(Han Seongmin). (2020). 국내 정밀의료의 현황과 방향성. 지식융합연구, 3(2), 97-114.
[18] Henderson, John C., and Nramanujam Venkatraman. "Strategic alignment: a framework for strategic information technology management." (1989).
[19] 김정덕, and 이성일. "클라우드 컴퓨팅 정보보호 프레임워크에 관한 연구." 정보보호학회논문지 23.6 (2013): 1277-1286.

〔저자소개〕

김 동 원 (Dong-Won Kim)
2009년 2월 서울과학기술대학교 학사
2012년 2월 건국대학교 석사
2021년 2월 고려대학교 박사
2017년~현재 건양대학교 사이버보안학과 교수
email : blast@konyang.ac.kr