https://doi.org/10.33778/kcsa.2022.22.3.069

클라우드 기반 안전한 정밀의료 실현을 위한 보건의료정보 보호 적용 방안에 관한 연구

김 동 원*

요 약

세계적으로 의료분야는 기술의 발전과 ICT 기술과의 융합으로 매우 빠르게 성장하고 있으며, 개인 건강정보, 유전자정보, 임상정보 등을 활용한 정밀의료(Precision Medicine)는 차세대 의료산업으로 성장하고 있다. 정밀의료는 개인의 건강과 생명을 다루기 때문에 개인정보보호 및 보건의료정보 보호 문제가 전면으로 대두되고 있다. 이에 따라, 본 논문에서는 클라우드 및 의료분야 국내·외 관련 표준, 법·제도 등의 기준에 맞추어 보안 개선사항을 제시하고 있으며, 이를 통해 안전한 정밀의료 실현을 위한 보건의료정보 보호 방안을 제안하고 있다.

A Study on Applications of Healthcare & Medicine Information Protection for Cloud-Based Precision Medicine

Dong-Won Kim*

ABSTRACT

Globally, the medical field is growing very fast with technology development and convergence with ICT technology, and Precision Medicine using personal health information, genetic information, and clinical information is growing into a next-generation medical industry. Since Precision Medicine deals with individual health and life, the issues of personal information protection and health and medical information protection are emerging.Accordingly, this paper presents security improvements by domestic and foreign standards, laws, and systems in the cloud and medical field, and proposes a plan to protect healthcare and medicine information protection for safe Precision Medicine.

Key words : Healthcare industry, Precision Medicine, Healthcare & Medicine Information Security

접수일(2022년 07월 26일), 수정일(2022년 09월 15일), 게재확정일(2022년 09월 26일)

* 건양대학교/사이버보안학과

1. 서 론

1.1 연구 배경

정밀의료(Precision medicine)는 유전체, 임상정보, 생활환경 및 습관정보 등을 토대로 보다 정밀하게 환자 각 개인을 분류하고 이를 고려한 최적의 맞춤형 의료(예방, 진단, 치료)를 제공하는 차세대 의료 패러다임이다. 정밀의료란 “환자의 특성에 맞는 의학적 치료 방식을 재단하는 것“으로, ”궁극적으로 생명을 살리기 위한 질병의 뿌리와 치료법 개발에 대한 새로운 이해를 위해 기술, 과학, 의료기록을 이용하는 것“으로 정의하고 있다[1]. 정밀의료는 개인에게 최적화된 의료서비스를 제공하는 데 목적이 있으므로, 개인의 유전자정보, 임상 정보, 환경정보, 라이프로그 등 일상생활 속 다양한 정보뿐만 아니라 개인의 건강에 영향을 줄 수 있는 모든 정보를 수집·분석하는 서비스이다. 이러한 정밀의료정보 및 데이터는 해킹으로 인하여 유출, 노출, 변조 등으로 인한 보안위협은 생명과 직결될 수 있으므로 보안성(Security)과 안전성(Safety)을 반드시 보장하여야 한다.

전 세계적으로 클라우드 컴퓨팅을 활용하여 원격의료를 수행하고 환자 데이터를 공유하는 등 클라우드를 의료 및 헬스케어 산업에 도입하는 것에 대하여 많은 관심을 가지고 헬스케어 클라우드 프로젝트를 진행하고 있다. 빅데이터, 인공지능, 클라우드 컴퓨팅 등을 중심으로 축적된 빅데이터를 활용하여 인공지능이 학습하고 이를 통해 기존의 지식체계에서는 불가능한 새로운 문제해결 방안이 실시간으로 제공되고 있다. 의료-헬스케어 분야에서는 클라우드 서비스 도입이 활발하게 이루어지고 있으며, 정밀의료 실현을 위해 개인 맞춤형 의료 빅데이터를 클라우드를 활용한 서비스가 활성화되고 있다. 국내에서는 정밀의료 병원정보시스템(P-HIS)이 개발되어 개방형 클라우드 플랫폼인 파스타(Paas-TA) 환경에서 제공되고 있다[2].

또한, 건강·진료정보는 빅데이터 속성인 대량(Volume)으로, 급속도(Velocity)로, 다양한 형태(Variety)로, 가치 있는(Valuable) 정보로 생산되고 있으며, 빅데이터 위험 중 개인정보(Privacy) 침해는 매우 중요한 최우선 과제이며[3], 정밀의료는 개인의 유전정보 등 개인에 대한 민감정보를 활용하므로 정보유출과 개인정보(Privacy) 침해에 보호가 매우 중요하게 다루어 지고 있다[4, 5]. 이에 따라, 본 논문에서는 클라우드 환경에서의 안전한 정밀의료 실현을 위하여 클라우드와 의료분야의 국내·외 보안 요구사항을 조사/분석하여 클라우드 환경에 적용 가능한 안전한 정밀의료 정보보호 방인 도입이 필수적이며, 개인의 맞춤형 의료를 위한 많은 정보를 활용하는 정밀의료 분야는 더욱더 면밀하게 살펴보아야 한다.

1.2 연구방법 및 구성

본 연구에서는 클라우드 환경에서 정밀의료를 실현하기 위한 방안으로 II장에서는 선행연구로서 클라우드 및 정밀의료 분야 국내외 표준 동향 조사·분석 및 관련 연구, III장에서는 정밀의료 에서의 정보보안 문제점과 정보보호 요구사항을 통해 클라우드 기반 정밀의료에서의 보건의료정보 보호 적용 방안을 제시하고, 마지막으로 V장에서는 본 논문의 결론으로 끝을 맺는다.

2. 선행 연구

2.1 정밀의료 정보보호

현재까지 질병에 대한 치료는 오랜 기간의 치료 경험의 축적을 통해 표준화되고 체계화된 방법을 통해 이루어졌다. 하지만 이러한 치료법이 모든 환자에게 항상 같은 효과를 보이는 것은 아니다. 개개인의 유전정보와 환경정보 등을 수집하고 통합 분석하여 적용되는 개인맞춤형 치료는 매우 효과적이다[7]. 대표적으로는 폐암 EGFR 유전자 변이에 따른 표적치료제가 있다[6]. 정밀의료를 통한 진료 및 연구 과정에서 수집·분석된 빅데이터를 활용하며, 이러한 통합 정보는 향후 질병에 대한 더 적합한 치료 방법을 개발하는데 핵심적인 자료가 된다[8, 9]. 개인에게 최적화된 의료서비스를 제공하는데 목적이 있으므로, 개인의 민감정보를 수집하여 활용한다[10,11]. 정밀의료 분야에서 수집되는 개인정보는 Table 1과 같다.

<Table 1> 정밀의료에서 수집될 수 있는 개인정보[11]

구분	내용	수집 가능 정보
신체차원	개인의 신체 구조적 특징을 뜻하며 건강을 이루는 핵심 요소 (ex. 몸무게, 체력, 지구력, 면역력 등)	진료정보, 검사정보, 유전 정보, 각종 건강정보 등
감정차원	신체차원에 의해 인간의 건강에 많은 역할을 미치는 요소 (ex. 스트레스, 불안감, 행복감 등)	SNS정보, 라이프로그, 문진정보 등
사회차원	사교력과 문화 감수성을 의미 (ex. 가족과의 교류, 이웃과의 활동, 직장생활 등)	SNS정보, 구매정보 기록정보, 위치정보 등
지성차원	정보를 처리하고, 행동에 옮기는 능력 가치관이나 믿음을 정리하고 결정을 내리는 능력을 의미	학력정보, 두뇌기능정보 등
영성차원	생명체에 대한 태도, 인간의 본성, 타인을 태하는 태도 등과 같은 넓은 믿음체계 (ex. 종교적 가치관 등)	SNS정보, 종교정보 등
직업차원	현대사회에서 직장은 소득을 얻는 장소를 넘어 분쟁조절, 업무분배, 지성성장 등의 기술을 익힐 수 있는 존재로서의 의미	직업정보, 위치정보, 직무분야 등
환경차원	Dale B.Hahn 등은 전인적 건강에서 환경차원을 제외하였지만, 일부학자들은 개인이 생활하고 있는 지역 내지 공간의 환경적 영향도 중요한 지표로 여기고 있음	기온, 기후 정보, 대기의 질 정보, 오염정보 등

2.2 정밀의료분야 보안 요구사항

정밀의료에서의 보안 요구사항 분석을 위해 국내·외 법과 제도를 비교하고 분석하여 주요한 정보보호 문제점을 연구한다. 정밀의료는 최첨단 ICT 기술과 결합 되면서 개인의 건강정보 및 민감정보(생체정보, 투약정보, 병력 등)들이 데이터화 되어 외부로 전송되거나, 데이터베이스 등에 집적되고 있다[12]. 특히, 정밀의료에서는 개인의 사생활 침해 문제[13], 유전정보 누출로 인한 피해[14]는 개인 뿐만 아니라 전 사회적인 위험이 될 수 있기 때문에 의료정보 위험관리[15] 방안 등과 법·제도적인 측면에서의 연구가 매우 필요하다.

2.2.1 45 CFR 46

미국 보건복지수(HHS)와 15개의 연방기관이 참여하여 인간을 보호하기 위해 마련된 45 CFR 46 규칙이 발표되었으며[16], 이는 미국에서의 정밀의료 연구 분야에 직접적인 영향을 미치고 있다. 주로 정보주체의 이해 향상을 위한 동의와 프로세스, 공동 연구에 대한 sIRB 검토 요구, 2차 연구를 위해 저장된 식별 가능 자료에 대한 포괄적 동의, 건강 관련 임상시험의 정의 등이 주요 내용으로 구성된다[11,16].

2.2.2 HIPPA Security Rule

정밀의료에서의 개인정보 이슈와 연관성이 매우 높은 미국의 건강보험 이동성 및 책임의 법인 HIPAA(Health Insurance Portability and Accountability Act)가 있다. 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 구현 사양이 포함되어 있다[12].

2.2.3 GINA

2008년에 제정된 유전자 차별 금지에 관한 법률로 유전자정보차별금지법(Genetic Information Non-discrimination Act, 이하 GINA)이 있다. 장차 질병으로 발전할 수 있는 유전자를 소지한 경우에 대한 차별 금지, 근로자의 유전자정보를 고용, 해고, 인사, 승진 등에 반영 금지 등을 포함하고 있다[11,17].

2.2.4 HITRUST Common Security Framework

HITRUST(Health Information Trust Alliance)는 보건의료분야, 기술분야, 정보보호 분야 지도자들의 민간조직으로 공통보안프레임워크(Common Security, Framework, CSF)인 의료기술보안을 위한 인증 프레임워크를 수립하여 민감한 데이터 및 규제된 데이터에 접근, 저장 또는 교환하는 모든 조직에서 사용 가능한 공통 보안 요구사항은 제시하고 있다.

2.2.5 NIST Cyber Security Framework

미국은 국가안전보장과 경제 안보를 위한 주요 사회기반시설에 대한 공통보안프레임워크를 제공한다. 사회기반시설에 공통되는 정보보안 대책 우수사례, 기대되는 성과, 참고 정보가 제시되고 있으며, Frameork Core, Framework Profile, Framework Implementation Tier의 3가지 요소로 구성되어 있다. 2014년 2월 초판 발표된 후 2018년 4월 CSF v.1.1이 발표되었으며, Supply Chain Risk Management 보안 요구사항이 포함되어 제시하고 있다[18].

2.2.6 FedRAMP

공공분야의 클라우드 도입에 따른 보안 인증제도로서 FISMA(Federal Information Security Management Act)에 적용하는 방식을 표준화 하는 미국 정보의 프로그램이다. 클라우드 기반 서비스에 대한 보안평가, 인증, 지속적 모니터링을 제공하는 표준화된 프로그램으로, FedRAMP는 FISMA 준수 비용을 줄이고 정부 데이터를 보호하고 사이버보안 취약점을 탐지할 수 있다[19].

2.2.7 ISO 277799

ISO에 의해 개발된 정보보안표준으로서 의료기관 및 개인건강 주체인 개인에게 ISO/IEC 27002의 구현을 통한 정보보호 가이드를 제공한다. ISO27799 (Health informatics -- Information security management in health using ISO/IEC 27002)는 11개 정보보호 대책, 39개 보안통제항목에 대한 의료정보보호 관리체계 구축을 위한 요구사항을 제시하고 있다[12,20].

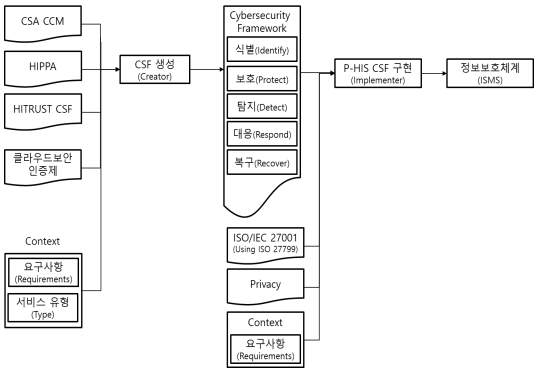
2.1.1 CSA OCF

CSA는 비영리단체인 클라우드 보안협회이며, 클라우드 보안 제어 프레임워크인 OCF(Open Certification Framework))를 제공하고 있다. CSA OCS는 3단계의 신뢰를 기반으로 구축되어 있으며, 클라두으 서비스 제공자의 높은 수준의 가시성과 투명성 제공을 보장하고 있다. 또한, CSA 최적실무(Best Practice)에 따른 컴플라이언스 상태를 보여주는 CAIQ(The Consensus Assessments Initiative Questionnaire)와 CCM 보고서를 제공한다[21.22].

3. 정밀의료 보건의료 보호체계 연구

3.1 정밀의료 보안요소 식별

정밀의료분야 보건의료 보호체계 연구개발을 위하여 “NIST Cybersecurity Framework", "ISO/IEC 27799 Health informatics - Information security management"를 기반으로 HITRUST CSF, CSA CCM, FedRAMP, HIPPA, IHE 등에서 요구하는 보안 요구사항을 식별한다. 정밀의료 보안요소 식별은 Fig 1과 같이 국내외 보건의료 및 정보보호 요구사항과 정밀의료 법·제도, 표준, 기술, 사고사례 등을 비교분석하여 클라우드 기반 정밀의료 구현으로 전개한다.



(Fig. 1) 정밀의료 보건의료 보호체계 구현 Flow

유형	카테고리	Public IaaS		PaaS-TA		SaaS	
식별 (ID)	자산 관리 / 사업환경 / 지침 / 위험평가 / 위험전략 / 공급망						
보호 (PR)	◦ 접근제어 (AC)	001	사용자 인증 및 권한 관리	001	사용자 인증 및 권한 관리	001	사용자 인증 및 권한 관리
		002	물리적 출입통제	002	API 키 관리	002	다중 인증
		003	네트워크 분리			003	API 키 관리
		004	VM 간 독립성 보장				
		005	API 키 관리				
	◦ 교육훈련 (AT)	001	내부인력 보안	001	내부인력 보안	001	내부인력 보안
	◦ 데이터보안 (DS)	001	하드웨어 멀티테넌트 환경 보안	001	컨테이너 멀티테넌트 환경 보안	001	어플리케이션 멀티테넌트 환경 보안
		002	네트워크 암호화			002	데이터 이동 흐름 파악
		003	데이터 VM 이전 보안			003	데이터 폐기
		004	백업시스템 구축			004	데이터 암호화
						005	사용 종료된 권한 해제
						006	비식별화
						007	데이터 무결성 보장
						008	데이터 통신 암호화
	◦ 절차 (IP)	001	침해사고 대응 계획 수립	001	침해사고 대응 계획 수립	001	침해사고 대응 계획 수립
		002	백업 정책 수립	002	컨테이너 관리 방안 수립	002	민감정보 접근 보안정책 수립
		003	장비 폐기 및 재사용 정책 수립			003	소프트웨어 개발보안 정책 수립
		004	네트워크 보안 정책 수립				
		005	가상자원 관리 정책 수립				
	◦ 유지보수 (MA)	001	장비 유지보수	001	소프트웨어 유지보수	001	소프트웨어 유지보수
	◦ 방어기술 (PT)	001	IaaS 인터페이스 및 API 보안	001	PaaS-TA 인터페이스 및 API 보안	001	SaaS 인터페이스 및 API 보안
		002	백업 수행	002	결함허용 및 가용성 지원	002	정보유출 차단 솔루션 적용
		003	네트워크 정보보호 시스템 운영	003	O/S 보안 강화	003	시큐어 코딩
		004	이중화	004	악성코드 통제	004	웹공격 차단
		005	하이퍼바이저 보안	005	안전한 개발환경 제공	005	앱위변조, 악성앱 차단
		006	가상 소프트웨어 보안	006	백앤드 서비스 보안		
탐지 (DE)	◦ 이상행위 및 이벤트 (AE)	001	탐지된 이벤트 분석	001	탐지된 이벤트 분석	001	탐지된 이벤트 분석
	◦ 모니터링 (CM)	001	추적 감사	001	추적 감사	001	추적 감사
		002	네트워크 모니터링	002	PaaS-TA 성능 및 용량 모니터링	002	SaaS 성능 및 용량 모니터링
		003	IaaS 성능 및 용량 모니터링	003	PaaS-TA 컨테이너 및 백앤드서비스 보안 취약점 점검	003	데이터 변경 모니터링
		004	네트워크 및 보안 장비 취약점 점검	004	O/S 취약점 점검	004	개인정보 / 민감정보 / PMI 데이터 유출 점검
		005	하이퍼바이저 보안 취약점 점검	005	악성코드 탐지	005	웹 취약점 점검
						006	모바일 악성코드 탐지
	◦ 탐지절차 (DP)	001	탐지절차의 지속적인 개선	001	탐지절차의 지속적인 개선	001	탐지절차의 지속적인 개선
대응 (RP)	대응계획 / 커뮤니케이션 / 분석 / 완화 / 개선						
복구 (RC)	복구계획 / 개선 / 커뮤니케이션						

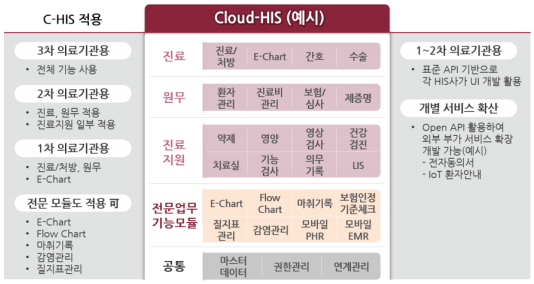
(Fig. 2) 클라우드 기반 정밀의료 보안요소

정보보호의 영역은 정책, 정형화된 절차, 표준 및 가이드라인 등을 통제하는 관리적 통제(Administrative controls), 중요 장비에 대한 작업장, 정밀의료 클라우드 컴퓨터 장치 등에 대한 감시와 통제를 위한 출입문, 잠금장치, 감시 카메라, 경비원, 네트워크 분리 등에 의한 물리적 통제(Physical controls), 정보시스템을 감시하고 통제하기 위해서 소프트웨어와 특정 데이터를 이용하는 패스워드, 방화벽, 침입탐지시스템, 접근 제어, 데이터 암호화 등에 의한 논리적 통제(Logical controls), 환경재해(자연재해, 화재, 정전)에 대한 대비 및 복구방안에 대한 환경적 통제(Environmental controls)등으로 구분된다. 정보보안은 일회성, 부분적 보안 등으로 제한적이었지만, 개인의 정밀의료정보와 같이 중요한 정보를 보호하기 위해서는 지속적 관리, 전사적 보안이 요구되며, 클라우드를 기반으로 하는 정밀의료시스템에 최적화되고 보다 높은 수준의 보안 관리 활동을 위한 정보보호 관리체계가 필요하다. NIST CSF 5개 기능, 6개 유형, 108개 세부유형과 CSA CCM의 136개 도메인, HIPAA Security Rule 136개, HITRUST CSF 149개 통제항목을 분석하여 클라우드 컴퓨팅 환경과 정밀의료정보를 보호하기 위해 필요한 보안요구사항을 식별하고 전문가 10명을 대상으로 델파이 기법을 활용하여 Fig2와 같이 안전한 정밀의료를 위한 보건의료정보 보안요소를 식별하였다[28, 29].

3.2 클라우드 기반 정밀의료 특징

최근 환자 데이터의 생성과 분석에 따른 기술발전은 정밀의료 분야의 성장을 촉진하고 있다[23]. 정밀의료와 맞춤형 의료는 개인 환자의 방대한 데이터를 이용하여 새로운 치료 전략을 제시한다. 임상데이터 외의 방대한 의료데이터를 활용하기 위해서는 클라우드 기반의 정밀의료가 필요하다[23]. 빅데이터, Wearable Health Device, 유전체 검사정보 축적 등을 통해 다양한 정밀의료가 가능하다.

국내에는 Fig 3과 같이 2017년도 과학기술정보통신부의 정밀의료 국가 전략 프로젝트의 일환으로 클라우드 HIS와 연계하여 의료기관의 규모와 유형에 맞는 SaaS 플랫폼에 적용하여 개발하였다. 다양한 HIS 환경에서도 분석서비스가 가능한 공통데이터모델(CDM) 체계를 적용하여 정밀의료 구현을 위한 기반을 마련하였다[2].



(Fig 3) 클라우드 기반 병원정보시스템[2]

클라우드 기반의 정밀의료는 환자의 질병상태, 생활 방식, 환경에 대한 다차원적인 데이터를 수집을 통해 다음 Table 2와 같은 장점을 가진다.

<Table 2> 클라우드 기반 정밀의료의 장점[23]

고급 데이터 관리 도구 필요
무제한 데이터 저장 및 공유
데이터 수집 프로세스 자동화
데이터 체계적 검색이 가능한 형식으로 저장함
복잡한 데이터 분석 수행
다차원 데이터를 쉽게 검색, 수집, 분석
실시간 데이터 모니터링
빠른 추세 식별
많은 정보에 근거한 의사결정성

3.3 클라우드 기반 정밀의료를 위한 정보보호 개선사항

안전한 정밀의료를 위한 보안활동이 의료기관내 조직에서 효과적으로 작용하기 위해 IT와 정보보안과의 전략적 연계가 필수적인 요소이다. 보안만 강조하다 보면 효율성을 강조하는 IT와 대립하게 되면 결과적으로 성과를 저하해는 결과를 초래할 수 있다. Henderson, J. and N. Venkaraman의 전략연계 모형[24]에 따라 목적, 프로세스, 특성을 고려한 정보보호체계 적용이 필요하다. 정밀의료에서 고려해야할 사항인 무결성(정밀/의료정보 변조로 인한 잘못된 처방), 신뢰성(정밀의료 시스템을 활용한 의료활동 중 오류로 인한 훼손), 회복성(오류로 인한 의료활동 중단)을 고려하여야 한다[26, 27]. 의료행위에 활용되는 정밀의료는 정보보안의 훼손으로 개인의 건강과 궁극적으로는 생명에 위협을 초래할 수 있다.

(1) IaaS 클라우드 환경에서 정밀의료 정보보호 개선사항

아래의 Table 3은 정밀의료 IaaS와 관련된 보안통제항목이다. 보안통제항목은 목적, 적용내용, 법적 요구사항으로 구성되어 있다. 특히 국내 관련 법(개인정보보호법, 정보통신망법, 의료법)에서 요구하는 항목은 "필수(14)", 국내 관련 법에서는 요구하지 않으나 클라우드 보안인증제에서 요구하는 항목은 "권고(17)", 그 외 항목은 "선택(11)"으로 분류한다. IaaS 플랫폼에서는 Infra에 해당하는 네트워크, 스토리지, 시스템, 하이퍼바이저 등과 관련된 범주의 통제항목들로 구성된다.

<Table 3> IaaS 정밀의료 보안통제의 보안등급 개요

Type	Essential	Recommen-dation	Optional
Identify	2	4	0
Protect	11	5	6
Detect	1	3	2
Respond	0	3	2
Recover	0	2	1
Total	14	17	11

주요한 필수 요구사항으로는 사용자 인증 및 권한 관리, 물리적 출입통제, 네트워크 분리, 하드웨어 멀티테넌트 환경 보안, 네트워크 암호화, 침해사고 대응계획 수립, 네트워크 보안 정책 수립, 네트워크 정보보호 시스템 운영, 가상소프트웨어 보안 등과 같이 Infra 보호에 중점을 두고 있다.

(2) PaaS 클라우드 환경에서 정밀의료 정보보호 개선사항

국내 정밀의료 PaaS는 PaaS-TA 플랫폼을 적용하고 있다[2]. 국내 환경에 맞도록 확장 개발한 컨테이너 기반 오픈소스인 PaaS-TA는 국산 소프트웨어를 지원하고 사용자 편의성 및 관리 효율성을 향상시켰다. 주로 Platform에 해당하는 운영체제(컨테이너), 미들웨어(개발환경), 런타임(로드밸런스) 등과 관련된 범주의 요구사항들로 구성된다. 보안 통제항목은 Table 4와 같이 PaaS-TA 정밀의료 목적, 적용내용, 법적 요구사항으로 구성되어 있다. IaaS와 동일하게 국내 관련 법에서 요구하는 항목은 "필수(4)", 클라우드 보안인증제에서 요구하는 항목인 "권고(15)", 그 외 항목은 "선택(12)"으로 분류한다.

<Table 4> PaaS 정밀의료 보안통제의 보안등급 개요

Type	Essential	Recommen-dation	Optional
Identify	2	4	0
Protect	2	3	7
Detect	0	3	2
Respond	0	3	2
Recover	0	2	1
Total	4	15	12

주요한 필수 요구사항으로는 사용자 인증 및 권한 관리, 내부 인력 보안 등 같이 Platform 보호에 중점을 두고 있다. PaaS-TA의 경우에는 국내 법에서 요구하는 항목이 적고 주로 클라우드보안인증제에서의 요구사항이 많다. 사업환경에 따라 "필수" 요구사항을 적절하게 고려하여 개선하여 적용할 필요가 있다.

(3) SaaS 클라우드 환경에서 정밀의료 정보보호 개선사항

국내 정밀의료 SaaS의 보안 통제항목은 Table 5와 같이 구성되며 국내 관련 법에서 요구하는 항목은 "필수(9)", 클라우드 보안인증제에서 요구하는 항목인 "권고(15)", 그 외 항목은 "선택(13)"으로 분류한다. SaaS 플랫폼에서는 주로 Service에 해당하는 데이터, 어플리케이션(Web, App)등과 관련된 범주의 통제항목들로 구성된다.

<Table 5> SaaS 정밀의료 보안통제의 보안등급 개요

Type	Essential	Recommen-dation	Optional
Identify	2	4	0
Protect	7	3	7
Detect	0	3	3
Respond	0	3	2
Recover	0	2	1
Total	9	15	13

주요한 필수 요구사항으로는 사용자 인증 및 권한 관리, 내부 인력 보안, 어플리케이션 멀티테넌트 환경 보안, 데이터 폐기, 데이터 보호, 사용 종료된 권한 해제, 민감정보 접근 보안정책 수립 등 같이 Service 보호에 중점을 두고 있다.

본 연구를 통해 클라우드 기반의 안전한 정밀의료 실현을 위한 개선방안으로 Fig 2와 같이 IaaS 클라우드 환경에서는 필수(14)", "권고(17)", "선택(11)"의 보안 요구사항과 PaaS 클라우드 환경에서는 필수(4)", "권고(15)", "선택(12)"의 보안요구사항, SaaS 클라우드 환경에서는 "필수(9)", "권고(15)", "선택(13)"의 보안요구사항을 연구 제안하였으며, 이를 활용하여 기술적·환경적·제도적 여건을 고려하여 적용할 필요가 있다.

4. 결 론

의료분야는 ICT 기술과의 융합을 통해 매우 빠른 속도로 발전하고 있다. 정밀의료는 개인의 맞춤형 의

료로서 방대한 개인정보와 민감정보를 활용한다. 빅데이터 기술과 ICT 기술을 활용한 의료산업은 고부가가치 분야로 주목되고 있으며, 의료산업에서 화두고 되고 있는 정밀의료는 차세대 의료산업으로 성장하고 있다. 정밀의료 특성상 사람의 생명을 다루기 때문에 정보보호는 매우 중요한 요소이다. 클라우드 기반 정밀의료는 병원정보시스템과 더불어서 정밀의료를 통한 의료서비스 품질 향상, 비용절감, 편리성 증대 및 산업경쟁력을 향상시킬 수 있을 것이다. 본 연구에서는 보건의료 및 클라우드 기반 정보보호 현황 분석과 관련 법·제도, 국내·외 표준 등을 연구하여 정보보호 요구사항을 분석하였다. 식별, 보호, 탐지, 대응, 복구를 기반으로 한 NIST Cybersecurity Framework를 기본 축으로 CSA CCM, HIPAA, HITRUST의 정보보호 요구사항을 IaaS, PaaS-TA, SaaS에 적용하였다. 또한 클라우드 기반 정밀의료에 따른 정보보호 개선사항을 도출하여 제시하였으며, 이를 통해 국내의 정밀의료 정보보호 방안을 개선 발전시킬 수 있는 기반을 마련하였다.

향후에는, 정밀의료에서 다루고 있는 데이터(의료정보, 유전정보, 생체데이터, 임상정보, 생활습관 정보 등)의 종류에 보안위협 분석과 사례, 데이터 보호기술을 중심으로 정보보호 요구사항과 적용방법에 대한 연구가 필요하다.

참고문헌

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

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

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

[4] 장성원. "빅데이터 시대 개인정보의 형법적 보호." 비교형사법연구 24.1 (2022): 1-28.

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

[6] Chen, Fan, et al. "Cellular Origins of EGFR-Driven Lung Cancer Cells Determine Sensitivity to Therapy." Advanced Science 8.22 (2021): 2101999.

[7] 대석허. "Personalized cancer medicine: present status and future perspectives." Journal of the Korean Medical Association 58.11 (2015): 1021-1026.

[8] 윤혜선. "정밀의료를 위한 데이터 거버넌스에 관한 연구-미국의 All of Us Research Program 사례를 중심으로." 바이오경제연구 2 (2019).

[9] 장성재. "보건의료 빅데이터 관리시스템 최신 동향." BRIC View 동향리포트, 한국원자력의학원 (2017).

[10] 신재승, et al. "정밀의료 생태계 구축을 위한 데이터 수집 및 연계 국내 동향." 한국웰니스학회지 15.1 (2020): 73-81.

[11] 장세균, 김현창 and 김소윤. (2017). 정밀의료에서의 개인정보와 정책방향에 관한 연구 : 미국, EU, 일본과의 비교법제도 분석을 중심으로. 한국의료법학회지, 25(1), 133-154.

[12] 김동원, and 한근희. "의료기관 정보보호 인식교육을 위한 교육과정 연구." 융합보안논문지 19.4 (2019): 151-163.

[13] 임혁, and 김태성. "라이프로그 시스템 (Life log system) 의 개인정보 생명주기 (Life cycle) 단계별 프라이버시 노출에 대한 위험성." KMIS International Conference. 2014.

[14] 유호종, et al. "유전정보 기증으로 발생 가능한 피해의 유형과 확률." 생명윤리정책연구 8.2 (2014): 87-108.

[15] Kim, Dong-won, et al. "Telemedicine Security Risk Evaluation Using Attack Tree." Journal of The Korea Institute of Information Security & Cryptology 25.4 (2015): 951-960.

[16] US Department of Health and Human

Services. "Final rule enhances protections for research participants, modernizes oversight system." Retrieved February 10 (2017): 2019.

[17] Kumar, Krishali, Michael Crawford, and Katharina Clausius. "Defined, Described and Defended: The Genetic Non-Discrimination Act in the Media." (2022).

[18] White, Gregory B., and Natalie Sjelin. "The NIST Cybersecurity Framework." Research Anthology on Business Aspects of Cybersecurity. IGI Global, 2022. 39-55.

[19] Taylor, Laura. "FedRAMP: history and future direction." IEEE Cloud Computing 1.3 (2014): 10-14.

[20] Ngqondi, Tembisa G. "The ISO/IEC 27002 and ISO/IEC 27799 Information Security Management Standards: A Comparative Analysis from a Healthcare Perspective." Port Elizabeth: Nelson Mandela Metropolitan University (2009).

[21] Saxena, Swati. "Ensuring cloud security using cloud control matrix." International Journal of Information and Computation Technology (2013): 933-938.

[22] 최주영, 최은정, and 김명주. "클라우드 서비스 평가 프로그램과 ISO/IEC 27001: 2013 의 비교 연구." Journal of Digital Convergence 12.1 (2014): 405-414.

[23] 한성민. "국내 정밀의료의 현황과 방향성." 지식융합연구 3 (2020): 97-114.

[24] Henderson, John C., and Harihara Venkatraman. "Strategic alignment: Leveraging information technology for transforming organizations." IBM systems journal 38.2.3 (1999): 472-484.

[25] 진정하, 김병준, and 한근희. "클라우드 기반 국방 정보시스템 구축에서의 정보보호 적용 방안 연구." 한국통신학회논문지 46.9 (2021): 1415-1425.

[26] 전인석, 김동원, and 한근희. "의료산업에서의 랜섬웨어 대응 방법." 정보보호학회논문지 28.1 (2018): 155-165.

[27] 김동원. "보안성을 고려한 스마트 의료기기 관리 (Secure-MEMP) 방법에 관한 연구." 융합보안논문지 21.1 (2021): 63-72.

[28] Kim, Dong-won, Jin-young Choi, and Keun-hee Han. "Risk management-based security evaluation model for telemedicine systems." BMC Medical Informatics and Decision Making 20.1 (2020): 1-14.

[29] Kim, Dong-Won, Jin-Young Choi, and Keun-Hee Han. "Medical device safety management using cybersecurity risk analysis." IEEE Access 8 (2020): 115370-115382.

[저 자 소 개]

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