원격의료보안표준 기반에 관한 연구

이인혜*, 박상선*, 한근희*
*고려대학교
ihlee5937@gmail.com, sitcs@naver.com, khhan1@korea.ac.kr

A Study on the Basis of Telehealth Cybersecurity Standards

In Hye Lee*, SangSeon Park*, Keunhee Han*
*Korea University

요 약

팬데믹 시대를 맞아 전세계적으로 원격의료에 대한 수요가 높아졌고, 이에 따라 원격의료의 보안 위험도 급증하고 있다. 원격의료는 각각의 원격의료 참여자가 서로 보안수준이 상이한 물리적 공간에 있으면서 의료행위에 참여하고, IT와 의료기기 비전문가인 개인이 자신의 공간에서 다수의 의료기기를 운용해야 하는 경우가 많으며, 서비스형태에 따라 실시간 데이터 교환이 이루어져야 한다는 점에서 일반적인 의료와 다른 보안 이슈가 발생한다.
이와 같은 특성의 원격의료 보안 위험 대응방안 연구를 위하여 관련 표준을 검토해 보았으나, ISO/IEC 및 미국 NIST의 일반보안 표준으로부터 분기한 의료 일반에 대한 보안표준이나 의료기기 보안 가이드는 존재하지만 원격의료보안을 포괄적으로 정립한 표준을 찾을 수 없었다.
이에 따라 국제적으로 통용될 수 있는 원격의료보안 표준의 개발이 시급하며, 이를 위하여 원격의료에 대한 용어 정의, 원격의료 참조모델 규정, 원격의료 보안모델 개발이 필요하다. 향후 이와 같은 원격의료 구성 요소들을 정의하고 구성 요소들 간의 상호작용과 환경적 보안 취약성 및 위협, 보안 요구사항을 정립한 원격의료 보안프레임워크 수립이 수행되어야 할 것이다.

1. 서론

최근까지의 원격 의료는 주로 특정 환경의 환자에게 제한된 범위의 서비스를 제공해 왔다. 그러나 세계적 전염병의 대유행으로 인하여 비대면 원격 의료 서비스는 일시적이고 특별한 의료 행위가 아닌 보편적 의료 관행의 한 형태로 부상하고 있다.

McKinsey & Company의 자료에 따르면 COVID-19 이전과 비교했을 때 원격의료 사용이 38배 증가하였다[1]. 우리나라 국회에서도 2020년 12월 '감염병 예방에 관한 법률'을 개정해, 의사-환자 간 비대면 진료를 감염병 확산 종료 시 까지 허용하여, 2020년 2월부터 2021년 8월 까지 전국 10,695개 의료기관에서 265만 건의 원격진료를 시행하였고 전체 70,969개 의료기관 중 16.5%인 11,687개 의료기관이 비대면 진료를 수행하였다[2].

한편, 원격 근무가 불가피하게 증가할 수밖에 없었던 2020년 3월 이후 모든 국가에서 원격데스크톱(RDP)에 대한 사이버공격이 급증하였다. 특히 국내 의료기관의 경우 2020년~21년 발생한 랜섬웨어 초기 침투와 내부전파 방법으로 RDP가 지속적으로 악용되고 있다[3].

또한 2021년 서울대병원과 서울성모병원의 해킹 공격으로 인한 개인정보 유출 피해[4], 안산 A병원의 2021년 8월 랜섬웨어 해킹으로 인한 데이터 소실[5] 등 의료기관에 대한 피해가 끊이지 않고 있다.

이와 같은 사회환경과 보안환경의 동향은 원격지 환자 및 의료진과 네트워크를 통해 민감한 의료정보, 영상정보 등을 주고받아야 하는 원격의료 서비스의 사이버 보안 위험이 지속적으로 증가할 것이라는 것을 예측하게 한다[6][7].

그러나, 원격의료보안에 대하여 정립된 국내외 표준이나 지침이 아직 부재하기 때문에 일반적인 보안 표준이나 의료보안 표준을 준거해야 하는 실정이다. 이로 인하여 원격의료서비스의 기기, 시스템, 환경적

특성에 따른 보안요구사항을 반영하여 적절히 대응하는 것에 어려움이 존재한다.

이에 따라, 원격의료보안 침해에 효과적으로 대응하기 위한 선제적 방안 수립이 시급하며 이를 위하여, 본 논문에서는 관련 국제 표준과 지침들을 분석하여 향후 발전 방향을 제시하고자 한다.

2. 원격의료보안의 주요 이슈

원격의료는 동일한 물리적 공간에서 이루어지는 일반적인 의료행위와 달리 원격의료 행위가 이루어지는 양 당사자의 환경이 상이하다는 점에서 보안적 측면의 특이성이 존재한다. 물리적 공간의 상이함은 원격의료행위가 이루어지는 환경과 해당 환경의 보안 수준을 고려해야 한다는 의미이다.

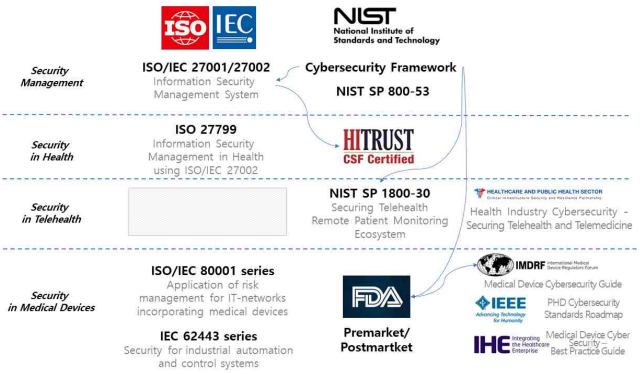
또한, 원격의료 환경에는 환자인 개인이 사적인 공간에서 사용하고 관리해야 하는 다수의 의료기기가 포함된다는 특징이 존재한다. 다양한 제조사, 프로토콜, 데이터 형식의 의료기기들이 비전문가인 환자나 케어기버(caregivers)들에 의해 관리 및 운용되어야 한다는 것이 보안의 논점이다.

서비스형태에 따라 실시간 통신을 통해 환자와 의료진간의 데이터교환이 필요하다는 것이 중요한 보안 이슈가 될 수 있다[9]. 기술이 발전하고 비대면 환경이 확대될수록 실시간 교환 데이터의 가용성, 무결성, 기밀성의 확보가 서비스 성패의 관건이 될 것이다.

이에 따라 원격의료보안의 계보는 일반적인 보안에서 출발하여 의료분야의 특성을 반영한 보안, 기기보안까지 일관성 있게 적용될 필요가 있다.

3. 국제표준 기반에서의 원격의료보안

원격의료보안과 관련한 국제 표준의 계보는 보편적인 정보보안관리체계와 보안통제를 규정한 'ISO/IEC 27001 Information Security Management Systems – Requirements'와 'ISO/IEC 27002 Code of Practice for Information Security Controls'에서 시작한다고 볼 수 있다. 또한, 미국의 국가 표준이지만 점차 영향력이 확대되어 국제 표준과 같은 파급력을 미치고 있는 표준이 미국 국가표준원(NIST)에서 발간한 표준이고, ISO/IEC 27001/27002와 동급으로 언급될 수 있는 표준이 EO13636 기반 NIST CSF'Cybersecurity Framework'와 'NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations'이다.



(그림 1) 국제표준 기반에서의 원격의료보안

보편적으로 적용될 수 있는 보안통제항목에서 의료분야에 특화된 통제항목과 적용가이드를 제시하는 표준이 ISO 계열에서는 'ISO 27799 Information Security Management in Health using ISO/IEC 27002'이고 미국에서는 민간기관인 HITRUST에서 개발한 'HITRUST CSF(Common Security Framework)'이다. 다만, HITRUST CSF는 NIST CSF의 의료분야 특화된 프레임워크로 언급하지만, 제시된 보안통제항목을 고려할 때 ISO/IEC 27002의 영향을 더 많이 받은 것으로 보인다. ATA(American Telemedicine Association)를 통해 가이드 출간 등 꾸준히 원격의료를 지원해왔던 미국은 HSCC(The Health Sector Coordinating Council)와 미 보건복지부(HHS)가 함께 'Health Industry Cybersecurity – Securing Telehealth and Telemedicine'을 2021년 발간하여 보급하고 있다.

의료기기보안과 관련된 문제는 IEC 62443 시리즈 'Security for Industrial Automation and Control Systems'과 'ISO/IEC 80001 시리즈 'Application of risk management for IT-networks incorporating medical devices'를 참조할 수 있다. 또한, IEEE PHD WG의 IEEE 11073 시리즈 표준은 다양한 개인건강기기 통신에 대한 이해를 높일 수 있고, 특히 2019년 출간된 'PHD Cybersecurity Standards Roadmap' 는 PHD의 위협 모델과 완화방안을 제시했으며, 이를 기반으로 몇 가지 사례를 보여주고 있다. IHE의 'IHE Patient Care Device (PCD) White Paper, Medical Equipment Management(MEM): Medical Device Cyber Security – Best Practice Guide' 일반적인 의료기기 아키텍처와 보안 고려사항, 모범 사례를 제시하고 있다.

미국에서는 FDA를 중심으로 NIST CSF의 관점에서 의료기기의 사이버보안 문제를 다루고 있다. FDA에서 발간한 'Content of Premarket Submission for Management of Cybersecurity in Medical Devices'와 'Postmarket Management of Cybersecurity in Medical Devices'는 미국 시장에 진입하기 위한 전 세계 모든 의료기기 제조사의 주목을 받았고 FDA가 회원국으로 되어 있는 IMDRF(국제의료기기규제자포럼)의 'Medical Device Cybersecurity Guide'에도 영향을 미치고 있다.

원격의료보안 요구사항에 대한 접근은 미국 NIST에서 더욱 활발하게 나타나고 있다. NIST SP 1800-30 'Securing Telehealth Remote Patient Monitoring Ecosystem'에서는 원격의료의 한 형태인 원격 모니터링에 대한 아키텍처와 보안 특성, 가이드를 제시하고 있다. 반면 ISO와 IEC에서는 아직 원격의료를 다루고 있는 보안 표준이 개발되지 않았다.

따라서 디지털 대변혁과 비대면 생활화가 확대되는 현 상황에서 의료행위 참여자, 의료 환경, 의료정보 및 정보시스템 뿐 만 아니라 의료기기까지 고려한 포괄적인 원격의료 보안 기준 정립이 절실히 필요하다.

4. 원격의료보안 표준 고려사항

원격의료보안에 대한 표준은 다음 사항을 제시해야 한다.

가. 용어 정의

ISO에서는 원격의료를 'use of telecommunication techniques to provide telemedicine, medical education, and health education over a distance'로 정의한다 [9]. 그러나, 각 국가와 환경에 따라 다양한 형태의 서비스로 발전하고 있는 원격의료는 원활한 의사소통과 모델 정립을 위하여 공통의 언어로 개념화할 필요성이 존재한다. 따라서 원격의료의 범위와 대표적인 서비스 모델을 규정함으로써 원격의료 보안 분야에서 통용될 수 있는 용어 정의가 필수 불가결하다.

나. 원격의료 참조모델

원격의료 참조모델 수립은 용어 정의와 밀접한 연관성이 있다. 원격의료는 각 원격의료 서비스의 목적과 기준에 따라 다양하게 분류된다. telemedicine, tele-consultation, tele-education 등 원격의료 행태에 따라 분류되기도 하고 telemedicine 또한 tele-diagnosis, tele-monitoring, tele-counseling 등 다양한 종류로 세분되기도 한다. 상이한 기준에 따른 분류는 상황에 대한 융통성이 가능하지만 포괄적이고 보편적인 기준을 정립하는 데에는 어려움이 있다.

따라서 다양한 원격의료의 목적과 성격을 분석하여 보안의 관점에서 유의미한 참조모델을 기준점으로 상정함으로써 이에 따른 보안요구사항의 도출과 대응방안 수립을 체계적으로 할 필요성이 있다.

다. 원격의료보안모델

원격의료 참조모델을 통해 각 참조모델에 내재되어 있는 보안취약점과 위협을 도출하여 이를 분석하고 통합함으로써 상위 개념의 원격의료 보안모델을 수립할 수 있다. 원격의료보안모델은 원격의료 보안 환경, 보안과 관련된 변수들, 이에 따른 취약점과 위협, 보안요구사항과 대응방안이 포함된다.

5. 결론

COVID-19로 인하여 물리적 환경에서의 생활이 급격하고 광범위하게 논리적 환경으로 변화함으로써 미처 준비할 여유도 없이 원격의료 보안성 강화에 대한 필요성 또한 급증하였다. 이에 따라 각 국가에서는 자국의 니즈에 맞는 원격의료의 모델을 발전시키겠지만, 네트워크와 디지털로 연결된 환경에서 운용되는 원격의료의 보안적 취약성은 국지적 대응만으로 방어하기 어려운 측면이 있다.

따라서, 본 논문에서 제시한 고려사항을 참고하여 보편적으로 적용될 수 있는 원격의료 보안 프레임워크를 개발하고 국제적으로 통용될 수 있도록 제도화하는 것이 원격의료산업 성장에 중요한 밑거름이 될 것이다.

본 연구는 정부 (과학기술정보통신부, 산업통상자원부, 보건복지부, 식품의약품안전처)의 재원으로 범부처전주기 의료기기연구개발사업단의 지원을 받아 수행된 연구임 (과제고유번호: 1711138615, KMDF_PR_20200901_0272)

참고문헌

[1] https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality
[2] http://www.dailymedi.com/detail.php?number=874696&thread=22r01
[3] 한국사회보장정보원 진료정보침해대응센터, 원격데스크톱(RDP) 터널링 공격 분석 및 대응방법, KHCERT-TR-2021-01, 2021.4.2.
[4] http://news.kmib.co.kr/article/view.asp?arcid=0016225479&code=61121111&cp=nv
[5] https://www.kyeonggi.com/news/articleView.html?idxno=2379314
[6] ECRI, 2019 Top10 Health Technology Hazards, 2018.10.18.
[7] ECRI, 2020 Top10 Health Technology Hazards, 2020.5.11.
[8] Healthcare & Public Health Sector Coordinating Councils, Health Industry Cybersecurity - Securing Telehealth and Telemedicine, 2021. 4
[9] ISO TR 16056-1 Interoperability of telehealth systems and networks – Part 1: Introduction and definitions, 2004. 07