비대면 원격의료 환경에 적용할 수 있는 사이버 보안 프레임워크 제안

진정하, 이인혜, 한근희
고려대학교 정보보호연구원
nemoda75@korea.ac.kr, ihlee5937@gmail.com, khhan1@korea.ac.kr

Proposal of a cybersecurity framework applicable to non-face-to-face telehealth environments

Jungha Jin, Inhye Lee, Keunhee Han
Dept. of Institute of Cyber Security & Privacy, KOREA University

요 약

특정 환경에서 환자에게 제한된 범위의 서비스만 제공하던 원격의료가 모바일, 클라우드, 인공지능 등 첨단 ICT를 통해 급속도로 확산하고 있다. 또한 2019년부터 시작된 글로벌 팬데믹으로 인하여 환자와의 대면 접촉 없이 질병 및 부상의 진단, 예방, 모니터링, 치료 또는 완화에 대한 요구가 높아짐에 따라 원격의료가 일반 의료행위의 한 방식으로 자리매김하는 중이다. 하지만, 네트워크를 통해 건강정보를 교환해야 하는 원격의료의 경우 정보의 기밀성, 무결성 및 가용성을 확보하는 것이 매우 중요하다. 이는 비대면 환경을 대상으로 하는 사이버 공격이 점차 증가하고 있으며, 특히 건강정보가 악성 사이버 공격의 주요 대상이라는 점에서 원격의료 산업의 성장을 위해서는 보안의 신뢰성 확보가 필수 조건임에는 의견이 없는 현실이다. 원격의료의 사이버 보안을 이해하기 위해서는 원격의료 행위자와 환자 간의 상호 작용, 이를 가능하게 하는 관련 기술 및 서비스 환경을 정의해야 하고 이를 바탕으로 다양한 형태의 원격의료 서비스에서 발생할 수 있는 사이버 보안 위협을 도출하기 위한 참조모델 구축이 필요하다. 모델 수립을 통해 서비스 공급자와 서비스 수신자가 준수해야 하는 사이버 보안 요구 사항을 도출을 통해 원격의료 환경에 적용 가능한 사이버보안 프레임워크 수립이 가능하다고 판단된다. 본 논문에서는 원격 의료 행위자, 환경 및 변수를 포함하여 원격 의료 사이버 보안 프레임워크의 전반적인 개념과 구조를 설명하고자 한다.

Ⅰ. 서 론

비대면 원격의료 환경이란 난민캠프, 오지, 해외근로자, 군부대 및 교정시설, 원양어선, 간호 등 실제 의료 인프라에 접근하기 어려운 사람을 대상으로 의료진과 환자 간의 혹은 의료진과 의료진 간의 원격상담 및 원격교육, 원격모니터링, 원격진료 등의 행위를 의미한다. 여기서 발생하는 원격상담 및 원격처방, 원격치료 및 원격수술, 처방 등의 의료활동을 제공하는 의료서비스 모델을 비대면 원격의료라 칭한다. 이러한 비대면 원격의료에 기존 IT 기반의 보안모델을 적용할 경우 비대면 원격의료 서비스 환경 구축 시 확인되지 않은 취약성으로 인해 발생하는 위협이 발생할 수 있다. 앞서 정의한 바와 같이 원격의료 서비스에는 의료 및 건강 영역을 다루는 다양한 활동과 기능이 포함되게 된다. 이러한 서비스는 다른 국가 및 문화에서 상이하게 표시되며 한 국가에서 사용되는 용어가 다른 국가에서는 동일한 의미로 해석되지 않을 수 있다. 따라서 일관되고 체계적인 원격의료 참조 모델과 공통 언어를 구축하는 것은 원격의료 사이버 보안 위험을 분석하는 중요한 기반 중 하나가 될 것으로 판단된다. 현재 진행중인 코로나-19와 같은 글로벌 팬데믹에서의 원격의료 의존도는 매우 높아졌으나 이를 신뢰하고 안전하게 사용할 수 있는 환경의 제공은 요원한 상황이다. 이를 위해서는 원격의료 환경에 적용할 수 있는 사이버 보안 프레임워크 수립이 필요하다고 판단되어 본 논문을 통해 해당 개념과 구조를 제안하고자 한다.

Ⅱ. 원격의료 개요

가. 원격의료 관련 용어

비대면 원격의료의 개념은 1970년부터 80년대에 전화를 이용한 원격의료를 기본으로 하여 정의되었으며, 관련한 용어가 현재까지 사용되고 있다. 또한, 각 국가에서는 다양한 원격의료에 대한 용어를 사용하고 있는데, 다양한 의료계의 용어와 같이 혼용되어 IT 기술에 접목되어 사용되고 있음에 따라 원격의료 용어와 개념에 대한 혼동이 발생할 수 있다. 원격의료를 나타내는 Telehealth에서 포함하는 의료 서비스의 예를 들어보면, Telemedicine과 Teleconsultation, 그리고 Telecare가 구분되게 된다. 우선 Telemedicine은 의료 행위가 동반되는 의료진과 환자간의 원격의료 행위를 의미하며 의료진이 플랫폼을 통해 환자와 소통하면서 의료 행위를 하는 것을 의미한다. Teleconsultation은 의료진과 의료진 사이에서 발생하게 되며, 의료진이 원격지에 있는 의료진과 환자에 대해서 처치에 대한 상담을 중점적으로 수행하는 형태로 볼 수 있다. Telecare는 앞선 Telemedicine이나 Teleconsultation보다 협소한 원격의료 행위로 볼 수 있으며, 의료진과 환자의 연결을 목적으로 하는 것이 아니기 때문에, 의료진 혹은 의료기기 제조사, 또는 개인용 건강기기 제조사 등과 환자 혹은 기기 사용자를 대상으로 수행하게 되어, 환자 및 사용자의 건강 관리를 중점적으로 다루고 있다.

나. 원격의료 보안 위협

비대면 원격의료를 포함하여 일반적인 의료 환경에서 포괄적으로 사용중에 있는 의료기기를 대상으로 하는 사이버 공격의 위험성이 크게 증가하는 추세이다. 2013년 6월 13일, 미국 식품의약청(FDA)은 사이버 공격에 의해 일부 의료기기들이 손상됐다는 보고에 따라 의료기기 및 병원 네트워크를 위한 사이버 보안 지침서를 발간한 사례가 존재한다. [1] 발간된 지침서의 내용에 따르면, 의료기기를 대상으로 하는 사이버 공격의 유형은 다음과 같이 정의하고 있다.

- 컴퓨터 악성 바이러스에 의한 감염으로 광범위하게 연결된 병원 전체 네트워크와 연결되어 동작하는 의료기기들의 고장 발생 위험이 증가
- 환자 관련 정보, 모니터링 시스템, 또는 환자 이식장치에 대한 액세스를

얻기 위해 병원 컴퓨터, 스마트폰, 테블릿 등 모바일 기기에 악성코드를 감염시킴

- 악성코드의 예로 특정 그룹에만 암호를 부여하기 위해 만들어진 소프트웨어가 실제 비밀번호, 유효하지 않은 암호 또는 하드코딩 된 암호를 무분별하게 배포해 피해를 발생시킴
- 많은 의료기기 업체는 의료기기에 대한 적절한 보안 소프트웨어 업데이트 및 패치를 제공하지 못하고 있어 사이버 공격 위험성에 노출됨

Ⅲ. 원격의료 환경에서의 사이버 보안 프레임워크

원격의료 사이버 보안 프레임워크는 환자, 의료진, 의료시설 및 장비 등이 포함되는 다양한 환경에서의 비대면 서비스를 안전하게 제공하기 위한 사이버 보안 문제를 해결해야 한다. 원격의료에서의 사이버 보안 문제는 의료진과 환자나 의료진과 의료진, 의료진과 개인용 의료기기 등의 서로 다른 보안 수준이 존재함에 따른 상호 간의 작용을 중점적으로 고려해야 한다. 동일한 환경에서 수행되는 일반적인 의료서비스와 달리 비대면 원격의료 서비스를 제공한 환경에서는 높은 보안성을 제공하고 있는 병원의 의사가 낮은 보안성을 갖거나 혹은 아예 보안성을 확보하지 못하는 어선이나 구급차에 탄 환자 및 구급대원을 포함하는 간병인 간에 원격의료 서비스가 가능해야 한다는 문제를 갖게 된다. 원격의료 서비스의 각 참여자는 시설, 장비 및 시스템에서 완전히 다른 환경에 위치하게 되며, 각 참여자의 보안 수준은 주변 환경의 보안 수준에 따라 차이가 발생하게 되는 것이다. 이러한 참여자 간 보안 수준의 차이는 취약한 환경의 맬웨어가 더 높은 보안 영역의 참여자에게로 침투할 기회를 제공할 수 있는 위험성을 갖게 된다. 다음의 그림 1은 원격의료 서비스의 사이버 보안에 영향을 미치는 참여자와 다양한 요인에 대한 개념도이다.

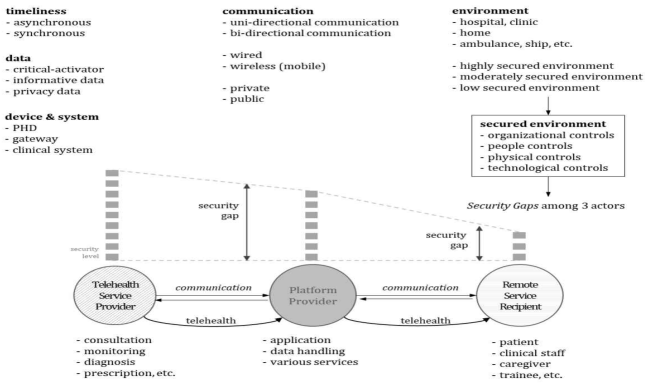

그림 1 원격의료 사이버 보안 프레임워크 개념도

상기 그림에서 나타내는 바와 같이 원격의료 활동과 관련하여 원격의료 서비스 제공자, 플랫폼 제공자 및 원격의료 서비스 수신자로 주요 참여자를 구분할 수 있다.

- 원격의료 서비스 제공자 : 원격의료 요청을 받아 원격의료 서비스를 제공하는 의료 주체로서 의사 및 간호사와 같은 임상 직원이거나 상담사와 같이 비의료 정보를 제공하는 단체일 수 있으며, 임상 정보 시스템을 사용하여 원격지의 환자에 대한 진단 또는 처방 지시를 내리거나 원격 의료진과 협력하거나 특정 환자에게 조언을 제공한다. 또한 원격 교육생에게 실시간 교육을 제공하거나 원격 수술 로봇으로 수술을 수행하는 등의 활동에 참여한다.
- 플랫폼 제공자 : 원격의료 서비스 제공자와 원격 서비스 수신자 간의 원격의료 서비스를 중재하며 텍스트, 오디오, 이미지, 비디오 등 다양한 데이터를 교환하면서 원격의료 참여자를 연결하고 양 당사자가 의도한 목적을 달성하도록 지원하는 역할을 한다.
- 원격의료 서비스 수신자 : 원격의료 서비스를 요청하는 참여자로서 원격의료 서비스를 제공받는 환자이거나, 요양원에서 환자 및 노인을 돌보는 간병인, 응급처치를 수행하는 구급대원, 원격지 전문가의 도움으로 수술을 시행하는 외과의, 전문 교육이 필요한 인턴 등이 해당한다.

원격의료 환경에 포함되는 각 참여자 간의 연결에서 사이버 보안에 영향을 발생할 수 있는 사항은 다음과 같이 정리할 수 있다.

- 시간에 대한 이슈 : 원격 수술이나 응급 상황에서의 비대면 진료와 같은 생명을 긴급하게 다루는 경우 동기식 방식으로 무조건 동작되어야 함
- 데이터에 대한 이슈 : 실제 의료 환경과 동일한 데이터를 사용하는 경우가 존재하여 정보보안에 보다 심각한 주의가 필요함
- 장치/기기 및 시스템에 대한 이슈 : PHD와 같은 개인용 기기부터 전문 의료용 진단 기기까지 다양한 장치들이 존재하게 되며, 이러한 기기들이 외부와의 연동을 위해 접속하게 되는 게이트웨이 시스템이 존재하게 된다. 하지만 미국에서 게이트웨이의 보안적 문제로 인한 긴급 사용 중지가 되었던 사례가 있어서 이 또한 원격의료에서 보안적인 고려 사항으로 심각하게 다루어야 함[2]
- 통신 방식 이슈 : 단방향/양방향 통신인지와 같은 장치에서 생성된 데이터를 처리하는 방식에서부터, 무선/유선과 같은 환경적 고려사항, 공용망/사설망 사용과 같은 이슈에서 정보보안을 고려해야 함
- 환경적 이슈 : 병원이나 진료소를 포함하여 환자가 거주하는 집이나 환자를 이송중인 앰블런스, 원양어선 등과 같이 다양하게 존재하며, 이러한 환경적 이슈에서 조직 구성원에 대한 통제, 사람에 대한 통제, 물리적인 통제, 기술적인 통제를 고려하여 보안의 수준을 적정하게 제공해야 함

Ⅳ. 결론

원격의료 환경은 주요 참여자가 원격의료 활동을 수행하는 물리적 또는 가상 공간을 의미하게 된다. 3가지로 구분된 참여자는 앞서 언급하는 5가지 이슈 사항을 만족하는 원격의료 사이버 보안 프레임워크 적용을 통해 적정 수준의 보안성을 제공해야 한다. 서로 다른 보안 정책 하에서 서로 다른 공간에 물리적으로 위치한 참여자 간의 상호 작용은 보안 책임 문제를 발생시킬 수 있으며, 상호 연결된 두 참여자 사이의 격차는 보안 수준이 낮은 행위자에서 보안 수준이 높은 행위자로 위협이 이동할 가능성을 높이게 된다. 각 참여자가 간의 보안 격차를 적정하게 해소하지 못하게 된다면 원격의료 서비스에서의 사이버 보안은 실패할 가능성이 높다고 판단된다. 따라서, 앞서 3장에서 제안하는 원격의료 사이버 보안 프레임워크의 적용을 통해 적정 수준의 보안성을 제공해야 신뢰성을 제공하는 안전한 비대면 원격의료 서비스의 제공이 가능하다고 판단된다.

ACKNOWLEDGMENT

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

참 고 문 헌

[1] C. for D. and R. Health, “Safety Communications - Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication,”

[2] “Implantable Cardiac Devices and Merlin@home Transmitter by St. Jude Medical: FDA Safety Communication -Cybersecurity Vulnerabilities Identified,”