

클라우드 기반 의료영상저장전송시스템(PACS)의 보안성

향상 연구

정명섭

고려대학교 컴퓨터정보통신학과

e-mail : kisersoge@gmail.com

Improvement of security of cloud-based medical image storage transmission systems (PACS)

Myoung-Seop Jung

*Dept. of Computer Science, Korea University

요약

다른 IT 분야에 비해 헬스케어 IT 분야는 의료정보의 중요성이 매우 높으나 현재 의료정보 보관, 데이터 전송에 대한 보안 부분이 매우 취약하며 보안관리에 대한 인력 또한 매우 부족한 상태이다. 향후 클라우드 발전법으로 인한 의료영상저장전송시스템의 환경 변화로 보안에 대한 취약성은 더욱 두드러질 것이며 사고 또한 급증할 것이다. 이에 대한 보안성 향상에 대한 방안을 제시 하고자 한다.

1. 서론

정부는 2015년 3월 27일 클라우드 산업 진흥을 목적으로 특별법 클라우드 발전법을 제정 하였으며 9월 28일 시행 예정이다. 현재 의료정보의 데이터 보관은 의료법 시행규칙 제 16 조 3 항 “의료인이나 의료기관의 개설자가 전자의무기록을 안전하게 관리 보존하기 위하여 갖추어야 할 장비는 전자의무기록의 생성과 전자서명을 검증할 수 있는 장비, 전자서명이 있은 후 전자의무기록의 변경 여부를 확인할 수 있는 장비, 네트워크에 연결되지 아니한 백업저장시스템” 이를 바탕으로 클라우드 환경에 의료정보를 등록하거나 다운로드 하는 부분을 금지하고 있다. 클라우드 발전법의 시행은 PACS 시스템의 변화를 줄 것으로 예상된다. 또한 보건복지부는 현재 의료기관 내에만 저장하도록 한 의료정보를 클라우드 환경에 등록이 가능하도록 하는 방안을 협의하고 있다. 향후 변화할 수 있는 클라우드 환경에서의 PACS 시스템의 보안은 필수적인 요소가 될 것이다.

2. 관련 연구

2.1 의료정보의 중요성

기존에 의료정보의 의미는 인체의 구조에 대한 정보와 질병에 관련된 정보 등으로 의료인에 초점이 맞춰진 정보였다. 그러나 기존의 의미는 의료기관이 정보화 되어짐에 따라 의미가 변화되어 왔다.

환자의 진료정보, 유전적인 특징, 가족력, 정신적 상태, 성생활 등 많은 부분에 있어 범위가 광범위 해졌다.

이러한 의료정보를 바탕으로 개인의 민감한 상태를 파악할 수 있으며 또한 약물주입 데이터의 조작, 수술정보 조작 등 환자 생명에 직접적인 피해를 줄 수 있는 악의적인 사고도 발생하였다.

즉 의료정보는 기존에 개인의 금융정보에 대한 중요성만큼 보안의 중요성 및 개인의 프라이버시 보장에 대해 크게 부각되고 있으며 이에 대한 보안가이드라인 제작과 연구활동이 활발해지기 시작하고 있다.

2.2 DICOM

의료장비부터 의료영상에 대한 디지털 통신에 사용하고 있는 다양한 표준을 지칭하는 용어다. DICOM은 현재 버전이 3.0 까지 제정되었으며 지속적인 보완 및 수정이 이뤄지고 있다. DICOM은 PACS 시스템을 구성하는데 있어 필수적인 표준으로이며 각 의료장비 및 의료영상에서 DICOM 표준이 지켜지지 않는다면 환자정보 및 의료영상정보를 각각의 의료정보 기준에 맞게 PACS 시스템을 별도로 구성해야 하며 이는 시스템 구성상의 혼란을 초래할 수 있다.

총 DICOM 20 장 15 장에서 “보안 및 시스템 관리 프로필(Security and System Management Profiles)”에서는 하기의 내용으로 보안에 대한 부분을 제시하고 있다.

- Secure connection Media
- 의료영상을 촬영 후 PACS Server로 전송 시 네트워크 단계에서의 보안
- 외부 저장장치인 Media를 이용하여 DICOM 파일을 저장할 때의 보안

- 의료영상의 무결성 보장과 영상의학과 의사의 판독 사인을 대신할 전자서명

2.3 ISO27001&ISO27799

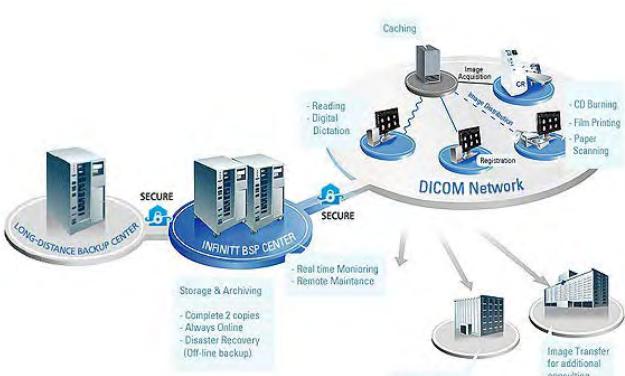
ISO27001은 국제표준 정보보호 인증으로 세계적으로 통용되고 있는 정보보호 인증이며 인증범위는 정보보호정책, 자산관리, 암호화, 운영보안, 통신보안 등 11개 영역, 133개 항목에 대하여 내부적으로 잘 계획하고 실현, 점검하고 이를 통해 관리적인 부분을 개선하였는지 평가하고 ISO27001 인증을 전달한다.

ISO27799는 ISO27001 표준을 보완하고 있으며 의료정보 보안에 대해 세부적으로 나열하여 구성하였으며 12개 영역 45개의 항목으로 구성되어 있다.

2.4 클라우드 PACS 시스템 구성

기존에는 의료기관 내에서만 의료정보를 보관함으로 환자가 다른 병원으로 이동하여 진료를 보거나 수술할 경우 의료정보를 보관하고 있던 기관에 요청하여 CD 또는 외부 미디어를 통해 복사 후 이동했던 시스템이었다. 향후 클라우드 PACS 시스템으로의 변화 시 클라우드에 보관되어 있는 의료정보를 협진 병원에서 손쉽게 확인이 가능하게 될 것이며 이는 진료 의견 교환 또한 쉬워질 것이다. 또한 클라우드 기반 PACS 시스템의 구축으로 인하여 원격판독, 이중 원격지 백업이 가능하게 될 것이다.

하기의 그림은 클라우드 PACS 시스템의 구성이다.



[그림 1] 클라우드 기반 PACS 시스템 1

3. PACS 시스템의 대표적 보안 위협요소

의료기관은 의료법 3조 1~5항을 기준으로 구분하였으며 설문 병원은 샘플링 하였으며 설문항목은 ISO27001 통제항목을 바탕으로 병원담당자 또는 PACS 유지 보수업체 직원을 인터뷰하여 조사하였다.

항목	3차 A 병원	2차 B 병원	1차 C 병원	보건소
의료장비-PACS Server 간 암호화 통신	취약	취약	취약	취약

Client-PACS Server 간 암호화 통신	취약	취약	취약	취약
응용프로그램 접속권한 통제	안전	안전	취약	취약
네트워크 통제	안전	안전	취약	안전

[표 1] 병원 별 취약점 조사

3.1 의료장비 → PACS Server 통신 보안

의료장비에서 PACS Server로 의료영상 및 의료정보 전송 시 암호화 통신을 해야 한다. 그러나 제품상의 암호화 통신 옵션이 있음에도 불구하고 대부분의 병원에서 해당 옵션을 사용하지 않고 있으며 이에 대한 의료기관 내에 인식이 되어 있지 않고 있다. 통신간 환자 의료영상 및 촬영정보가 탈취될 소지가 있어 보안에 취약하다.

3.2 PACS Client - PACS Web Server 통신 보안

PACS Client에서 PACS Web Server 간에 암호화 통신을 해야 한다. 그러나 제품상의 암호화 통신 옵션이 있음에도 불구하고 대부분의 병원에서 해당 옵션을 사용하지 않고 있으며 이에 대한 의료기관 내에 인식이 되어 있지 않고 있다. 통신간에 PACS Client에서 의료정보 조회 또는 의료영상에 대한 판독내용을 조회 시에 평문으로 노출될 소지가 있으며 탈취될 소지가 있어 보안상에 취약하다.

3.3 PACS 시스템의 접속권한 통제

PACS 프로그램 접속하여 의료정보 및 의료영상을 로컬로 저장하는 접속 권한이 의료기관 내에 사용자 별로 권한이 분류되어 있지 않아 불특정 사용자에 의해 외부로 유출될 소지가 있다. 1차 병원, 보건소의 경우 사용자 권한을 관리하는 관리자가 따로 존재하지 않아 의료정보 및 의료영상 유출 및 보안사고에 대한 사후관리가 더욱 취약한 상태이다.

3.4 PACS 시스템의 네트워크 통제

3차, 2차, 보건소의 경우 의료기관 내에 네트워크 보안이 IPS, IDS 등을 통해 대체로 잘 관리되고 있으나 1차 병원의 경우에는 공유기를 통해 인터넷을 사용하고 있는 환경이 많아 외부 네트워크로부터의 침입에 매우 취약하다. 또한 의료기관 내에 물리적, 논리적 망 분리가 되어 있지 않아 네트워크를 통한 악성코드 감염에 취약한 상태이다.

4. 클라우드 PACS 시스템의 보안 예상 위협요소

클라우드 환경에서 변하게 될 PACS 시스템의 보안 위협을 예상하여 기술하였다.

4.1 클라우드 PACS Server- 협력병원 의료 영상 공유

환자가 병원을 이동할 때마다 의료 영상을 수동으로 이동했던 일들이 클라우드 환경으로 변화 시에 의료 영상 공유가 협력 병원 간에 손쉽게 변화 될 것이다. 기존에 설문조사 했던 내역 중 1 차 병원의 네트워크 통제항목 미약한 부분으로 인하여 클라우드 환경에 있는 의료영상을 다운로드 시에 외부네트워크로부터의 탈취될 수 있는 소지가 있다.

4.2 클라우드 PACS Server- 원격판독 의료정보 공유

기존에 1 차, 2 차 병원에서 영상의학과 전문의의 부족으로 인하여 의료영상에 대한 판독이 어려운 점이 존재했다. 이는 클라우드 환경으로 변화됨에 따라 로컬 의료기관 내에서 판독이 어려웠던 의료영상을 손쉽게 확인하고 판독 또한 손쉽게 가능해 질 것이다. 원격판독기관 또한 1 차 병원과 마찬가지로 소규모로 운영되는 병원이기에 정보보안에 매우 취약하다. 이는 원격판독기관에서 클라우드에 저장되어 있는 의료영상을 다운로드하여 판독 시에 외부네트워크로부터의 탈취 될 수 있는 소지가 있으며 또한 판독 시에 전자서명 시스템이 구성되어 있지 않아 판독내용에 대한 무결성이 훼손될 소지가 있다.

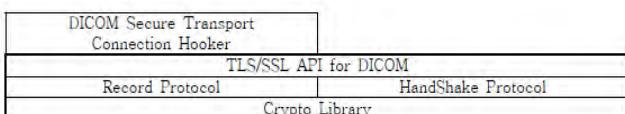
5. 클라우드 PACS 시스템의 보안 위협 대응방안

5.1 ISO 27001&27799 를 통한 보안관리 인식의 변화

ISO27001&ISO27799 의 관리항목을 통해 의료기관 내에 보안관리 및 운영에 대한 전반적인 인식전환이 필요하며 특히 1 차 병원 및 보건소는 관리항목 중 운영보안, 네트워크보안, 통신보안등을 중점으로 하여 의료정보 보안의 관리적 측면을 강화해야 한다.

5.2 의료장비 → 클라우드 PACS Server 통신보안

DICOM 표준 중에 15장 “보안 및 시스템 관리프로필 (Security and System Management Profiles)”에서는 ‘Secure Transport Connection Profiles’ 을 총족하는 모듈을 지원하고 있다.



[그림 2] DICOM TLS API Architecture

해당 모듈을 통해 로컬의료기관에서 클라우드 PACS Server로 의료영상을 전송 시 안전한 암호화 전송 모듈을 사용하여 통신 보안을 강화해야 한다.

5.3 PACS Client - 클라우드 PACS Server 통신 보안

HTTPS 프로토콜은 HTTP 와 유사하지만 통신간의 내용은 모두 암호화 하는 점이 다르다.

향후 클라우드 PACS 시스템이 도입됨에 따라 기존에 로컬 의료기관에의 사용자가 Client 프로그램 접속하여 사용하는 것이 아니라 클라우드 환경에 접근 가능한 협력병원, 원격판독기관 등 다수의 사용자가 추가될 것이다. 이에 PACS Client - 클라우드 PACS Server 간에 HTTPS 프로토콜을 사용하여 환장정보 조회 및 영상 확인 시 발생할 수 있는 취약 점을 보완해야 하며 통신 보안을 강화해야 한다.

5.4 DICOM 전자서명 구현

PACS 에서 전자서명은 크게 두가지로 구분할 수 있다. 첫째 의료영상의 원본성을 위해 의료영상이 처음 발생하는 의료장비 또는 의료영상을 PACS 시스템으로 전송 후 의료영상을 보정 시에 전자서명을 한다. 둘째 영상의학과 판독의 가 의료영상을 확인 후 판독하는 리포트에 전자서명을 한다. 전자서명을 하는 내용에는 의료영상 이미지마다의 고유번호, 이미지 픽셀정보 등이 포함된다.

1	the SOP Class UID
2	the Study and Series Instance UIDs
3	all attributes of the General Equipment Module that are present
4	the Current Requested Procedure Evidence Sequence
5	the Pertinent Other Evidence Sequence
6	the Predecessor Documents Sequence
7	the Observation DateTime
8	all attributes of the SR Document Content Module that are present

[표 2] 전자서명 시 필수 정보

해당 내용을 바탕으로 클라우드 환경으로 의료영상 전송 시와 원격판독기관에서 판독 시에 전자서명을 하여 의료영상, 환자의 판독내용에 대한 무결성을 보장해야 한다.

6. 결론

클라우드 발전으로 인하여 PACS 시스템은 향후 많은 변화가 있을 것이며 의료 영상을 외부에 저장하는 부분은 현재 국내에서 논의중인 원격의료에 대한 부분 까지도 연계가 된다. 향후 국내에서 시행할 경우 의료정보의 외부 공유로 인한 보안 취약점은 급증할 것이다. 본 논문에서는 기존 PACS 를 사용하고 있는 병원의 대표적인 보안 취약점을 조사하였으며 향후 클라우드 PACS 시스템으로 변화 시에 예측되는 보안 위협 또한 파악해 보았다. 이를 근거 삼아 국제 표준을 바탕으로 클라우드 환경에서의 보안성을 향상시킬 수 있는 방안을 제시하였다.

ISO27001&27799 관리항목을 바탕으로 의료기관의 보안 인식은 꾸준히 관리되어야 하며 기술적인 보안의 위협은 위의 제시한 내용을 바탕으로 향상 시킬 수 있을 것이다.

이와 더불어 지속적으로 발생하는 보안위협의 예외사항을 효과적으로 대응 할 수 있는 방안에 대한 추가 연구가 필요하다.

참고문헌

<국내문헌>

[1] 인피니트헬스케어 Smart-Net, <http://www.infinitt.com/cms/services/cloud-bases-service/infinitt-smart-net>, 2015년 9월 13일 검색

[2] 최윤섭, 디지털 헬스케어 국내규제 무엇이 바뀌어야 하나, <http://www.slideshare.net/pelexus/ss-49056597>, pp. 3, 2015

[3] 정보통신부, 의료영상저장전송장치(PACS) 데이호환성 향상 및 보안 적용 가이드라인, pp. 40~41, 50, 2003

[4] 흥승택, 의료정보 보안 메커니즘 적용 모바일 PACS 시스템 구현, pp. 3, 2012

[5] 국가법령정보센터, 의료법 시행규칙, 제 16 조 3 항, 2015

<해외문헌>

[1] DICOM, <http://medical.nema.org/standard.html>, DICOM Part 15, 2015년 9월 13일 검색