정 보 보 호 학 회 지
제25권 제5호, 2015. 10

의료정보공유 서비스의 전송데이터 보안 기술 동향

한 성 화*, 양 현 모**, 임 성 호***, 홍 정 욱****, 김 학 범*****

요 약

현재 의료기관간의 의료정보 공유는, 상호 협의된 의료기관간 DICOM(Digital Imaging and Communication in Medicine) 및 HL7(Health Level 7)에서 제시한 표준 Protocol을 사용하거나 각 기관별 별도의 Protocol을 사용하고 있다.[1] 현재의 의료정보공유는 특정 의료기관들 끼리만 이루어지며, 해당 기관 간 전송구간 보안은 대부분 IPSec VPN을 적용하고 있다. 법적으로 요구되는 보안 요구사항을 만족하기 위해 사전 보안 제휴를 맺은 의료기관들만 의료정보를 공유하고 있기 때문인데, 이는 의료정보교류 범위를 제한하기 때문에 의료서비스의 발전을 보안이 저해하고 있다고 판단 할 수 있다. 본 논문은 의료정보공유 서비스와 의료정보 전송데이터 보호기술을 조사하여, 현재의 문제점을 확인 후 범국가적인 의료정보공유 서비스에 대한 전송데이터 보안 아키텍처의 수립을 지원하는데 그 목적이 있다.

Keywords: Medical Information Communication, Medical Information Security, Medical ICT Security Architecture

Ⅰ. 서 론

국내 의료기관은 각 지역별 단과 병원으로 대표될 수 있는 1차 의료기관 부터 지역 종합병원인 2차 의료기관, 대도시 대형 종합병원 및 대학병원을 예로 들 수 있는 3차 의료기관으로 구분된다.

특정 질환에 의해 1차 의료기관이나 2차 의료기관에서 치료 할 수 없는 경우에는, 부득이 환자가 원하는 3차 의료기관에서 진료를 받게 된다. 이때, 보통 CD나 담당 의사간 합의에 의해 E-mail로 하위 의료기관에서 수집된 진료 기록과 각종 영상 정보를 Digital 정보로 변환하여 상급기관에 전달한다. 여기서 CD를 활용할 경우 환자가 분실 할 수 있으며, 의료정보를 담은 전송 E-mail을 사용할 때 평문으로 전송 될 경우 비인가자가 이를 취득하여 악용 할 수 있다. 환자의 경우 심리적으로 매우 취약한 상태이기 때문에, 악의적 사용자가 이를 취득하여 악용한 경우 환자는 사회공학적인 피해를 입을 수 있다.

이를 보완하고 의료서비스 발전을 도모하며 환자 편의성을 높이기 위해 의료기관간 정보공유를 하고 있다. 진료기록 및 영상정보는 민감한 정보이므로 전송 데이터에 대한 보호가 필요하며, 실제로 법적으로도 이를 요구하고 있다.

의료정보를 공유하기 위해서는, 의료정보를 공유 할 대상과 상호 협약을 맺고, 전송데이터를 보호하기 위한 암호 알고리즘 및 Hash 알고리즘, 보안 프로토콜 등의 사전 보안 연계(Security Association)를 수립한 후 제휴된 보안 채널을 통해서 정보를 전송하는 것이 일반적이다.

여기서 문제가 발생한다. 환자는, 자신이 진료를 받고 싶은 의료기관을 선택 할 권리가 있다. 그러나 사전에 상호 협약되어 있지 않은 의료기관에는 해당 진료정보를 전달 할 수 없으므로 부득이 CD를 사용하게 되며, 앞서 기술한 보안 취약점이 그대로 환자에게 전가되어 정보 분실 및 유출에 의한 악용의 위험에 노출되게 된다. 이는 환자 개인적으로도 위험하지만, 다른 관점으로는 의료서비스의 발전을 저해하는 것이다.

본 논문에서는 이러한 개인 진료정보의 유출 및 분실의 위험을 보완하고 의료정보공유의 활성화를 통한 의료서비스 발전을 위해, 현재의 의료정보전송 서비스를

* 동국대학교 국제정보대학원 (taifanz@naver.com, 010-3943-1247)
** 동국대학교 국제정보대학원 (yhmyang@naver.com, 010-2249-9469)
*** 동국대학교 국제정보대학원 (rebirth555@gmail.com, 010-5551-9661)
**** 동국대학교 국제정보대학원 (hjw1219@gmail.com, 010-9871-8233)
***** 디지큐코리아㈜/동국대학교 국제정보대학원 (khb0305@dongguk.edu, 010-3993-0707)

조사하고 의료정보의 전송데이터 보안 기술 동향을 조사하고자 한다.

본 논문의 구성은 다음과 같다. 1장은 서론으로서 본 논문의 배경과 의료정보공유 현황의 문제점에 대해 기술한다. 2장에서는 의료정보교류 활성화를 위한 각종 정부 과제, 시책 및 의료정보교류에 대한 전송 데이터 보안을 요구하는 관계 법령에 대해 기술한다. 3장에서는 의료정보공유 서비스 현행 아키텍처에 대해 기술하고, 4장에서는 의료정보 표준 별 전송데이터 보안 기술에 대해 설명한다. 5장에서는 문제점 및 이를 보완하기 위한 방향에 대해 기술한다.

Ⅱ. 의료정보교류 정부 시책 및 의료정보 관련 법

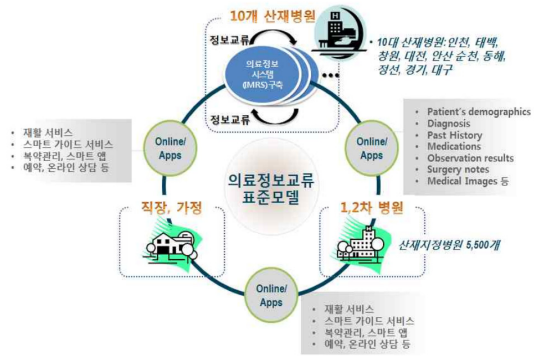
2.1. 의료정보교류 정부 시책

의료정보교류에 대한 정부기관의 노력은 꾸준히 계속되어 왔다. Pilot 형태로 의료기관간 정보교류 뿐만 아니라, 의료서비스 발전을 위한 중장기 프로젝트를 지금도 진행하고 있다.

2.1.1. K-Health 3.0 프로젝트

미래창조과학부에서 추진한 K-Health 3.0 프로젝트는 '근로복지공단병원 대상 의료시스템 혁신 시범사업'(2014.1~2015.3)으로, 근로복지공단 병원 및 산재지정병원을 대상으로 의료정보교류 사례를 창출하고 의료정보교류 확산을 위한 기술적 토대를 마련하기 위하여 시작되었다.

의료기관의 서로 다른 의료정보시스템 간 상호 운영성을 보장하는 국제 표준 기반의 공통 의료정보교류 플랫폼을 개발/시범 운영하여, 기존의 여러 정보교류 관련 시범사업에서 제시되었던 표준적용 도구를 포함하고 환자 식별체계를 정립한다.



〔그림 1〕 K-Health 3.0 프로젝트 개념도

그간 대형병원과 협력 1차 의료기관 간에 이루어졌던 1:N 방식의 제한된 의료정보교류에서 한걸음 더 나아가 대형병원-대형병원, 대형병원-1차2차병원, 1차2차병원-1차2차병원 등 다자간(N:N) 의료정보 교류 방식을 검증한다.[2]

2.1.2. 국제표준 의료정보교류시스템 시범운영

대구시는 2014년 11월 30일부터 전국 최초로 국제표준 기반의 의료정보교류 시스템을 시범운영 하였다. 의료정보교류시스템은 경북대학교병원과 대구의료원을 중심으로 협력관계에 있는 40개 병의원들로 구성된 2개의 의료정보교류 커뮤니티를 구성하고, 이를 서로 연계해 병의원 간 진료 의뢰 및 회신을 네트워크를 통해 전자적으로 처리하는 시스템이다.

이러한 일환으로 의료서비스 혁신의 근간이 되는 의료정보 인프라를 구축하고자 여러 병원으로 분산돼 있는 환자의 진료정보를 국제 표준방식에 따라 효과적으로 관리 및 활용하는 의료정보교류 시스템을 시범사업으로 선정하였다.[3]

2.1.3. 의료정보화 2020

보건복지부에서는 의료정보서비스를 발전시키기 위한 중장기 프로젝트로 "의료정보화 2020"을 수립하여 추진 중이다. 이 프로젝트는 [표 1]과 같이 단계적으로 진행되고 있으며 각 단계별 목표와 과제를 수립하여 추진중이다.

〔표 1〕 의료정보화 2020 추진과제 단계별 목표

연도	2015 ~ 2017	2018 ~ 2019
목표	보건의료 정보화 기반 강화	보건의료 정보화 연계 조성
과제	기존 의료정보시스템 개선 의료정보 표준화 정보인증 체계 구축 운영 의료정보 보호, 보안체계 구축 중점육성 운영사업 실시	수요자 중심 연계서비스 지원 공급자 중심 연계서비스 지원 정부 중심 연계 서비스 지원 서비스 운영 최적화

상기에서와 같이, 1단계에서는 의료정보화에 대한 기초를 다지는데 집중하고 있고, 2단계에서는 이를 바탕으로 의료서비스 발전을 도모하고 있다.[4]

2.2. 의료정보 관련 법

의료정보가 공인망에서 유통 될 경우 앞서 기술한 바와 같이 악의적 사용자에 의해 환자의 피해가 발생 할 수 있기 때문에, 법적으로 의료정보 전송에 대한 보호조치를 요구하고 있다.

현재 우리나라의 의료정보보호와 관련된 법률의 적용은 의료법에 규정이 있는 경우 의료법을 우선적으로 적용하고, 규정이 없는 경우 개인정보보호법을 적용하고 있으며 주요 내용은 [표 2]와 같다.

〔표 2〕 의료정보 관련 주요 법률

법, 시행규칙	주요내용
의료법 제18조의 2(처방전의 작성 및 교부)	누구든지 전자처방전에 저장된 개인정보를 탐지하거나 누출, 변조 또는 훼손 금지
의료법 제21조 (기록 열람 등)	의료법에서 지정하는 경우 이외에는 의료정보 제공이나 열람할 수 없음
의료법 시행규칙 제18조의 2 (전자의무기록의 관리, 보존에 필요한 장비)	법 제21조의2 제2항의 규정에 따라라 의료인 또는 의료기관의 개설자가 전자의무기록을 안전하게 관리,보존하기 위하여 갖추어야 할 장비는 다음 각 호와 같다. 1.전자의무기록의 생성과 전자서명을 검증 할 수 있는 장비 2.전자서명이 있은 후 전자의무기록의 변경여부를 확인할 수 있는 장비 3.네트워크에 연결되지 아니하는 백업저장시스템
의료법 제22조 시행규칙 제14조 (진료기록부 등의 기재사항)	진료정보는 본인의 동의 없이 수집 가능하며 진료목적으로만 사용가능하지만 일반개인정보는 동의 없이 수집 불가
개인정보보호법 제29조 (안전조치의무)	안전한 관리를 위해 접근통제, 암호화, 접속기록 보관, 물리적 보호조치 등 안전성 확보조치를 하여야 함
개인정보보호법 제18조 (개인정보 목적 외 이용, 제공 제한)	개인정보보호법에서 지정하는 경우 이외에는 개인정보를 제공할 수 없음

기본적으로 의료정보에 대한 보안 요구사항은 외부에 대한 유출 금지 및 변조, 훼손 금지인데, 이에 대한 책임은 의료기관이 갖는다. 지자체별 조례 등에 의해 법적인 보장을 받은 경우에 대해서만 의료정보공유 서비스가 구축되며, 이 경우 의료기관은 전송되는 의료정보에 대해 비인가 접근을 차단하거나 변조/훼손으로부터 보호하기 위한 보호조치를 강구하고 이를 적용해야 한다.[5]

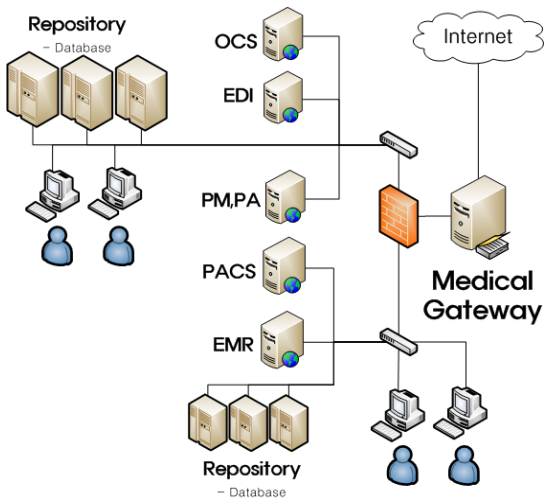
Ⅲ. 의료정보교류 서비스 아키텍처

3.1. 의료정보교류 시스템 구성

의료정보시스템은 의료기관마다 독자적으로 구성하고 있고, 각 의료기관에 맞게 별도의 특화 시스템을 운영하고 있다. (그림 2)는 가장 기본적인 의료정보시스템의 구성을 나타낸다.

의료정보시스템은 OCS나 PACS, EMR 등 다수의 시스템으로 구성되며, 상급 의료기관으로 갈수록 시스템 구성은 더욱 복잡해진다. 의료정보시스템은 기본적으로 접근통제를 매우 철저하게 적용하고 있다. HL7이나 DICOM 뿐만 아니라 의료정보 관련 법 등에서도 의료기관 내/외부의 접근통제를 매우 강조하고 있기 때문이며, 이는 내부자에 의한 의료정보 유출을 방지하는데 매우 효과적으로 적용되고 있다.

상기 그림에서 의료기관간 정보교류가 발생 할 경우,



〔그림 2〕 의료정보시스템 구성

교류대상 데이터는 병원 Repository에 존재하는 EMR과 PACS에 연관된 Data이다. 현재의 많은 의료기관에서는 각기 서로 다른 Data Format을 사용하기 때문에, 실질적인 정보교류를 위해 Repository에 앞단에 정보교류를 위한 송수신 시스템인 Medical Gateway를 배치한다.

Medical Gateway는, 각 의료기관에서 정보를 요청시, 해당 요청에 해당하는 정보를 Repository에서 확인하여 요청한 기관으로 전달하거나 특정 의료정보를 다른 의료기관의 ITS로 요청하는 역할을 수행한다. 보안 관점에서의 역할로는, 암호화 채널을 형성하여 전송 의료정보를 보호하거나 비인가자의 Repository내 의료정보에 대한 직접적인 접근을 차단하기 위한 Air Gap 역할을 수행한다.[6]

3.2. Medical Gateway 시장 현황

Medical Gateway는 국내외 모두 독자적인 기술을 앞세워 각국/각 의료기관에 제공하고 있다.

국내 네오젠소프트(Neozensoft)의 NeoHIE는 의료정보 시스템간의 데이터 송수신을 위한 솔루션으로 HL7, CDA(표준화된 콘텐츠 교환주소[임상문서구조]) 기반의 데이터 전송 및 MLLP를 이용한 표준 전송규약을 준수하며, 각종 데이터 포맷을 지원하여 이기종간의 병원 데이터를 실시간으로 변환하여 원하는 형태로 전송이 가능하다. 또 다른 국내 기업인 INFINITT Healthcare에서 개발한 INFINITT PACS는 DICOM, HL7, HIPPA, IHE 등의 국제표준을 준수하여 의료정보를 교류 할 수 있다.

해외 Medical Gateway 개발사는 MACH7 TECHNOLOGIES과 Epic System이 있다. MACH7 TECHNOLOGIES의 VNA Solution는, DICOM을 준수하고 있으며 영상자료에 대한 공유를 가능하게 한다. Epic System의 EpicCare EMR도 마찬가지로 다른 EMR 시스템에서도 정보를 전달할 수 있다.[7,8,9,10]

Ⅳ. 의료정보전송표준 별 전송데이터 보호 방법

대표적인 의료정보 전송 표준인 HL7과 DICOM에서 제시한 전송데이터 보호 방법은 다음과 같다.

4.1. HL7

HL7은 의료기관 간 데이터 교환을 위한 표준 프로토콜로서, 1987년에 개발되어 현재는 전 세계적으로 활용되고 있는 의료정보의 전자적 교환 표준이다.[11,12]

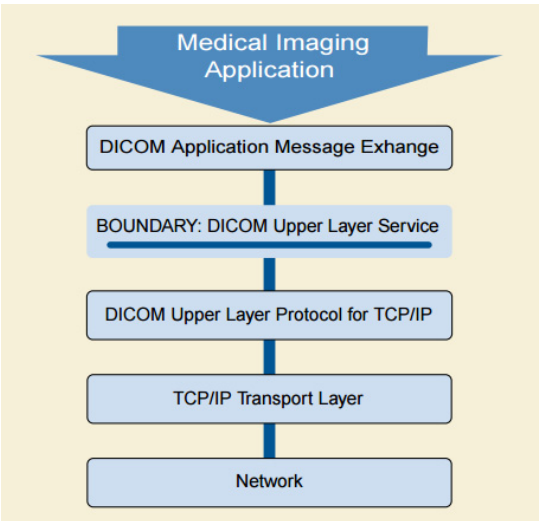
HL7의 보안은 "Security Working Group"에서 개발중이며, IEEE나 ASC 및 NIST 등의 각종 국제 표준을 준용하고 있다. Security Working Group에서는 HL7에서 요구되는 인증, 무결성, 암호화, 감사 등의 보안 서비스와 이를 구현하기 위한 메카니즘을 제시하고 있다.

HL7에서 권장하고 있는 의료정보 전송 시 데이터 보호 기법으로, DES에 의한 데이터 암호화 후 전송을 수행하거나, HTTPS등의 SSL Protocol을 적용, 보안 메일 전송에 의한 Secure EDI(Electronic Data Interchange)를 사용하는 방법의 세가지 방식을 제안하고 있다.[13]

현재는 “HL7 Version 3 Standard: Transport Specifications-MLLP”에서 의료정보 전송을 보안 Framework 및 Protocol을 개발하고 있다.[14]

4.2. DICOM

ACR과 NEMA이 공동 개발한 DICOM은 진료 영상정보 전송을 위한 표준으로서, 20개의 PS(Parts of the Standards)로 구성되어 있다. 이중 의료정보 교환은 PS 3.7에서 정의하였고 PS 3.8에서는 이를 위한 네트워크



〔그림 3〕 DICOM Network Protocol Architecture〔16〕

통신 지원 사항에 대해 정의하였다.[15]

DICOM에서는 의료정보의 전송을 위한 Network 서비스 계층구조를 제시하였는데, 세부 구조는 [그림 3]과 같다.

Medication Imaging Application Layer는 실제 병원에서 사용되는 의료정보인 RIS 등의 영상정보를 나타내며, DICOM Application Message Exchange Layer는 DICOM Service를 위한 Messaging Protocol을 의미한다. DICOM Upper Layer Service는 일종의 Middle Layer로서 물리적인 DICOM System을 논리적으로 분산/통합하는 기능과 함께 보안 전송 채널(Secure Transport Connection) 제공 역할을 담당한다. 나머지 Layer는 의료정보시스템에서 제공하는 일반 Network Stack을 나타낸다.

DICOM에서는 보안에 대한 구체적인 요구사항을 PS 3.15에서 적용 영역과 보안 기술, 관리 방법에 대한 알고리즘 및 기술 등의 상세 Spec을 제시하고 있으며, 그 세부내용은 [표 3]과 같다.

의료정보 전송 데이터 보안에 해당하는 Profile은 Secure Transport Connection Profile 과 Digital Signature Profile 이다. 각각은 일반적인 의료정보 전송 시 적용되어야 할 보안 기술과 전자서명 시 필요한 보안 Spec을 구체적으로 제시하였으며, 권장되는 적용 Service나 Data Field까지 제시하였다.

〔표 3〕Security and System Management Profile

Secure Use Profiles
Secure Transport Connection Profiles
Digital Signature Profiles
Media Storage Security Profiles
Network Address Management Profiles
Time Synchronization Profiles
Application Configuration Management Profiles
Audit Trail Profiles

4.3. 국제표준의 보안 요구사항

HL7이나 DICOM에서 제시된 전송 데이터 보안 기술은 의료정보에서 요구되는 보안 요구사항을 근간으로 제안되었으며, 이는 국내 의료정보관련 법령에서도 유사한 보안 요구사항을 제시하고 있다. [표 4]는 HL7 및 DICOM에서 요구하고 있는 의료정보에 대한 보안 요구사항은 나타낸다.

〔표 4〕 국제표준별 보안 요구사항

보안 요구사항	HL7	DICOM
Authentication	O	O
Authorization	O	
Data Confidentiality	O	O
Audit	O	
Secure Communication	O	
Availability	O	
Integrity	O	O
Key Management		O
Digital Signature		O

두 표준 및 국내 의료정보 법, HIPAA(미국 건강보험 이전과 책임에 관한 법) 모두, 명시적으로 요구하고 있는 보안 요구사항은 명칭으로는 차이가 있으나, 내용적으로는 모두 대동소이하다. 기본적으로 의료정보 보호를 위해 암호화 및 인증, 무결성 검증, 부인방지, 권한관리(접근통제)를 모두 요구하고 있다.[17]

4.4 의료정보의 전송데이터 보호 기법

특정 기관에 존재하는 의료정보를 다른 의료기관에 전송할 때 적용되는 기법은 [표 5]와 같다. 각 전송데이터 보호 기법은 HL7 뿐만 아니라 DICOM에서도 제시하고 있으며, 실제로 국내 뿐만 아니라 미국, 일본, 유럽 등 다수의 국가에서도 대동소이하게 적용되고 있다.[13]

이중 가장 많이 사용되고 있는 방식은 IPSec VPN을

〔표 5〕 HL7 전송 데이터 보호 기법

기법	내용
IPSec VPN 적용 방식	Medical Gateway 앞단에 IPSec VPN을 적용하여, Center/Remote 지점간 암호화 통신을 적용하는 방식
SSL Protocol 적용 방식	Medical Gateway에서 의료정보 요청 및제공 Server에 SSL Protocol을 적용하는 방식 주로 Web Server에 HTTPS 설정으로 제공
EDI 방식	Electronic Data Interchange 의료정보 전송 담당자간의 합의에 의해, 의료정보 전송 E-mail을 S-MIME/PGP로 암호화 하는 방식
전자서명 방식	공인 인증서를 사용하여 Message Digest를 생성, 전송 데이터에 대해 비대칭키 암호 알고리즘을 적용하는 방식

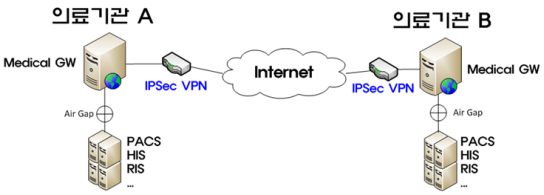
적용하는 방식과 SSL Protocol을 적용하는 방식, 전자서명 방식이며 그 구조는 각각 다음과 같다.

4.4.1. IPSec VPN 적용 방식

IPSec VPN을 적용할 경우에는 Medical Gateway와 공인망 사이에 VPN 장비를 배치하여 VPN 장비간 제휴된 SA를 적용하여 의료정보 전송데이터를 보하는 방식이다.

IPSec VPN을 적용할 경우, ESP/AH Protocol을 적용 할 수 있는데, 이 Protocol은 내부적으로 암호 알고리즘 및 Hash 알고리즘을 적용하고 있다. 이러한 암호 알고리즘 적용에 의해 IPSec VPN간 송수신 데이터는 기밀성 및 무결성을 보장받을 수 있기 때문에 많은 의료기관간 의료정보교류 시 기본 Network Infra요소로 선택되고 있다.

IPSec VPN을 사용할 경우에는, 의료기관이 전송데이터에 대한 보호 메카니즘을 VPN에 일임하기 때문에 서비스 구축/운영상의 보안 업무는 감소되지만, 별도의 장비 도입에 대한 부담이 발생한다.

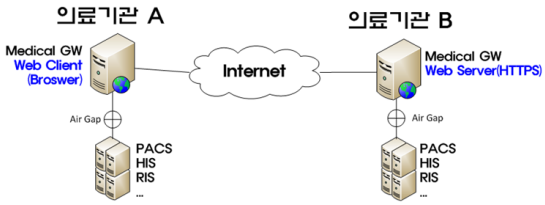


〔그림 4〕 IPSec VPN 적용한 전송데이터 보호

4.4.2. SSL Protocol 적용 방식

SSL Protocol 적용 방식은 전송 Protocol의 Socket Layer에서 암호 알고리즘을 적용하는 방식이다. Medical Gateway에서 의료정보를 전송 할 경우 Web Server를 사용 할 수 있는데, 이 경우 Web Server의 Protocol Type을 HTTPS로 설정하면, 간단하게 SSL Protocol을 적용 할 수 있다.

이 경우, Local Medical Gatewal는 Web Browser를 사용하여 원격지에 존재하는 Medical Gateway에 접속하게되며, 이때 Web Browser와 원격지의 Web Server는 SSL Protocol을 적용하여 암호 채널을 사용하게 된다.



〔그림 5〕 HTTPS를 활용한 전송데이터 보호

HTTPS 방식을 적용할 경우에는, 의료기관의 전송데이터에 대한 보안 아키텍처는 간단해 지지만, Medical Gateway에 대한 자체 보호를 직접 구현해야 한다는 부담이 발생한다.

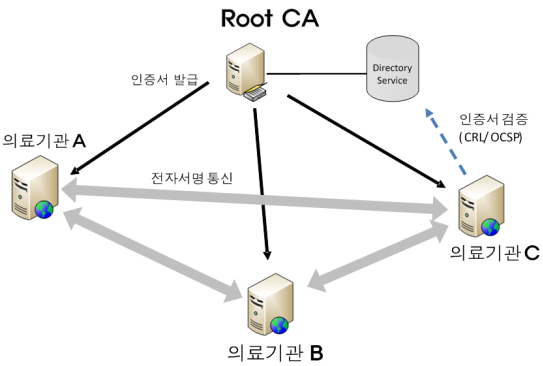
4.4.3. 전자서명 방식

전자서명 방식은, PKI 기반에 의해 공인인증서를 사용하는 방식이다.

각 Medical Gateway에서 공인인증서를 발급받고, 전송되는 데이터에 대해 전자서명을 적용하는 방식이다.

전송데이터에 전자서명을 적용 할 경우, 내부적으로 전송데이터에 대해 대칭키/비대칭키 암호알고리즘을 적용하며 Message Digest를 생성/검증 할 때 Hash 알고리즘을 사용하게 되어 데이터에 대한 기밀성과 무결성을 보장하게 된다. 또 Message Digest 생성시 송신자 개인키를 사용하고, 대칭키 암호알고리즘에 적용되는 암호키를 송신자 공개키로 암호화하여 수신자에게 전송하기 때문에 송수신 부인방지 기능을 제공한다.

상기 구조를 조금 더 확장한다면, 인증서 로그인 방식을 적용하여 식별 및 인증 과정에 적용할 수 있으며,



〔그림 6〕 H-PKI 보안 아키텍처 구성

CRL/OCSP를 사용하여 공인인증서의 유효성을 검증 받을 수 있다.

전자서명을 적용 할 경우에는 전송데이터에 대해 강력한 보안 메커니즘을 적용할 수 있으나 복잡한 Protocol 구조에 의해 성능이 저하되는 단점과, 의료기관에서 PKI Infra를 구축해야 하는 부담이 발생한다.

Ⅴ. 결 론

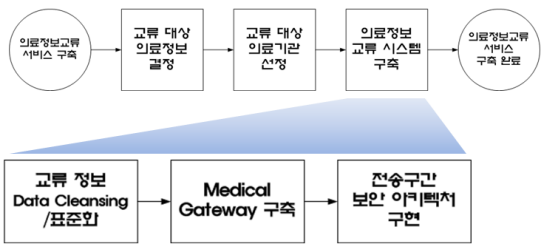
5.1. 의료정보교류 서비스의 현황 분석

HIPAA에서 권장하는 의료정보 전송보안 기법과 국제표준인 HL7과 DICOM 모두 모두 거시적인 보안 아키텍처는 제시하지 않고 있으며 P2P 통신에 Focus를 두고 있는데, 신뢰된 대상에 한해 서로 의료정보를 공유하는 방식으로, 일반적으로 [그림 7]의 순서로 구축된다.

전송 데이터에 대한 보호 기능은 “의료정보 교류시스템 구축” 단계에서 구현되는데, 초기에 의료정보를 구축 할 대상들만 전송구간에 대한 보안 시스템을 구축하게 된다. 이는, 보안 아키텍처의 구현이 의료기관에 일임되어 있기 때문에 발생한다. 의료기관에서는 제한된 비용으로 효율적인 구축해야하기 때문에, 상호 협약된 의료기관들만 전송구간에 대한 보안 체계를 적용하게 된다.

분명 이 과정은 적절한 접근 방법이다. 다만 이 절차대로 구축할 경우, 국가/사회 등의 거시적인 관점에서 본다면 [표 6]와 같은 단점이 발생한다.

국가 전체적인 관점에서, 안전한 통신 인프라를 통한 임의의 의료기관간 의료정보교류는 의료서비스의 발전을 위한 하나의 필요조건이다. 현재는, 의료정보교류에 필요한 보안 아키텍처 구현을 특정 의료기관이나 Vendor가 부담을 갖고 있다. 그러나 안전한 의료정보



(그림 7) 의료정보교류 시스템 구축 Process

〔표 6〕 현행 의료정보공유 시스템의 문제점

문제점	설명
제한적 통신	신뢰된 대상에 대해서만 정보공유가 가능하여 임의의 의료기관에 의료정보 전달이 불가능하므로, “환자” 입장에서는 큰 의미가 없다.
Vendor 종속성 발생	IPSec VPN이나 Medical Gateway를 개발한 Vendor의 '제품'에 종속되며, 이로 인해 정보공유의 수평 확장의 어렵다.
개발/구축 비용 증가	IPSec VPN 도입시에는 의료기관별 전송구간 보호를 위한 시스템 구축비용 이 증가한다. 반대로, Medical Gateway에 보안 서비스를 개발하기에는 개발사의 개발 부담 비용이 증가한다.
보안강도 Gap발생	의료정보공유 Group(Site)별 적용 Cipher Suite 상이하여 보안 강도 Gap이 발생한다.

공유를 위한 표준 보안 아키텍처를 국가에서 제시하고 의료기관과 의료정보시스템을 개발하는 Vendor가 이를 수용하여 시스템에 적용시킨다면, 전송 구간에 대한 보안 부담이 줄고 공통 Protocol을 사용하여 임의의 의료기관간 의료정보교류가 자연스럽게 활성화 될 수 있다.

5.2. 의료정보 전송 보호 메카니즘에 대한 연구 방향

환자가 원하는 의료기관에서 진료를 받을 수 있게 하고 진료비용의 중복을 방지하기 위해서는, 임의의 의료기관간 의료정보를 전송 할 수 있어야한다. 또한, 의료정보교류에 대해 법적/사회적인 요구사항을 만족하기 위해 기술적으로 [표 4]에서 제시한 보안 요구사항을 만족해야 한다. 이를 통하여, 현재의 의료정보공유 서비스에서 발생하는 제한적 의료기관간 정보교류와 Vendor 종속성의 문제, 보안 강도의 Gap 발생 등의 문제를 해결 할 수 있어야 한다.

이러한 기술적/사회적/법적 만족을 위해, 범국가적인 의료정보 전송에 대한 보안 아키텍처를 제시하여 의료기관이 이를 자발적으로 수용하고 현장에 손쉽게 적용시킬 수 있어야 한다.

국가기관에서 제시한 전송 데이터 보안 표준을 Medical Gateway에 적용한다면, VPN과 같은 전송 데이터 보호를 위한 별도의 보안 시스템을 도입하기 위한 비용을 절감 할 수 있게 된다. 또 국가 전체적인 의료정보보안 아키텍처를 통합 관리 할 수 있기 때문에 의료정보교류 Site별 보안 강도를 동일하게 적용 할 수 있그쳐. 장기적으로는 의료정보교류와 관련된 기업/기관의

부담이 줄어들어 의료정보교류가 활성화 될 수 있으며, 의료 서비스가 발전 할 수 있다.

다만, 국가기관에서는 각 의료정보시스템을 개발하는 Vendor의 의료정보 전송시스템이, 국가가 제시한 보안 체계를 정확히 수용하였는지에 대한 검증이 뒷받침되어야하는 후속 인증도 요구된다.

원칙적으로 의료법에서는 환자에 대한 진료기록을 의료기관 외부로의 유출을 금지하고 있다. 이에 대한 의료법과 관련된 법제 정비가 필요하며 의료용어 및 의료정보전송을 위한 표준 Protocol을 정착시키고 환자의 개인 진료정보의 활용에 대한 인식을 개선한다면 의료정보교류는 활성화 될 것이다.

참 고 문 헌

[1] Ik-Sung Cho, Hyeog-Soong Kwon. “Implementation and Design of WISD(Web Interface System based DICOM) for Efficient” *The journal of the Korea Institute of Maritime Information & Communication Sciences*, pp. 501-507, Dec. 2007.

[2] Creation Fusion Planning Part, “K-Health 3.0 Project”, *Ministry of Science, ICT and Future Planning*, May. 2104.

[3] Medical Sightseeing Part, “Medical Information Exchange System Project”, *Dae-gu City Hall,* 2013.11

[4] Health Medical Policy Part, “Health IT Strategic Plan 2020”, *Ministry of Health & Welfare*, 2015.03

[5] Young-Gyu Lee. “Civil Remedies for the Infringement of Individually-identifiable medical information” *Hanyang Law Review* Vol.25 No.1 pp 135-160.

[6] Seokjin Im, Hee-Joung Hwang, “Design and Implementation of Message Format and Server for Interworking EMR System and Gateway of Medical Devices,” *The Journal of The Institute of Internet, Broadcasting and Communication*, vol. 13, issue 6, pp. 255-262, Dec. 2013.

[7] Neozensoft-Product Description, NeoHIE, 2015.

[8] Epic System-Product Description, EpicCare EMR, 2015.

[9] MACH7 TECHNOLOGIES-Product Description, VNA Solution, 2105.

[10] INFINITT Healthcare-Product Description, INFINITT PACS, 2015.

[11] Jung-Kil Song, “A message design on the Implementation of WAMIS(Wide Area Medical Information System) Based on HL7” *Hannam University*, pp. 6-17, Dec. 2003.

[12] Min-woo Kim, Jae-hwan Jeon, Gwan-hyung Kim, Sung-in Kang, Am-suk Oh, “Design of HL7 Message for HIS Integration of Healthcare Systems,” *Journal of the Korea Society of Computer and Information*, Jul 2007.

[13] Mary Kratz, Polar Humenn, Mark Tucker, Michael Nolte, Steve Wagner, Gregg Seppala, Gunther Shadrow, Wayne Wilson, Sean Auton, “Health Level Seven Security Services Framework,” *HL7 Security Group*, July 1999.

[14] Rich Ankney, “A Security Framework for Healthcare Information,” *HL7-Special Comittee-Security*, pp. 4-7, Feb. 1997.

[15] National Electrical Manufacturers Association, “Security and System Management Profiles,” *DICOM PS3.15 2015b*, pp. 63-72, 2011.

[16] National Electrical Manufacturers Association, “Part 8: Network Communication Support for Message Exchange,” *DICOM PS3.8 2015b*, pp. 23, 2007.

[17] Dongsoo Kim, Minsoo Kim, “Development of an Information Security Standard for Protecting Health Information in u-Health Environment”, *Soongsil University/ Pukyong National University*, Jun. 2007.

〈저 자 소 개〉

한 성 화 (Sung-Hwa Han)
종신회원

1998년 2월 : 단국대학교 건축공학과 졸업
2014년 9월~현재 : 동국대학교 정보보호학과 석사과정
관심분야 : 정보보호, 통신공학

양 현 모 (Hyun-Mo Yang)
정회원

2014년 9월~현재 : 동국대학교 정보보호학과 석사과정
1990년 7월~2013년 1월 : 비씨카드(주)
2013년 2월~현재 : (주)스마트로
관심분야 : 정보보호

임 성 호(Sung-ho Lim)
정회원

2010년 2월 : 천안대학교 정보보호학과 졸업
2014년 9월~현재 : 동국대학교 정보보호학과 석사과정
2010년 12월~2015년 2월 : 케이씨씨시큐리티(주)
2015년 2월~현재 : 한솔넥스지(주)
관심분야 : 정보보호, 보안운영, ISMS

홍 정 욱(Jeong-Wook Hong)
정회원

2014년 2월 : 강남대학교 전자공학과 졸업
2015년 3월~현재 : 동국대학교 정보보호학과 석사과정
관심분야 : 정보보호

김 학 범 (Hak-Beom KIM)
종신회원

1990년 8월 : 중앙대학교 대학원 전자계산학과 졸업(공학석사)
2001년 2월 : 아주대학교 대학원 컴퓨터공학과 졸업(공학박사)
1991년 10월~1996년 6월 : 한국전산원 주임연구원
1996년 7월~2001년 8월 : 한국정보보호진흥원 기술표준팀장
2001년 9월~2003년 1월 : (주)드림시큐리티 상무이사
2003년 2월~2005년 3월 : (주)장미디어인터렉티브 상무이사
2008년 4월~2009년 6월 : 인포섹(주) 수석컨설턴트
2009년 7월~2010년 12월 : 에스지에이(주) 연구소장
2011년 8월~2013년 3월 : (주)지엔에스인증원 본부장
2013년 4월~2014년 9월 : (주)이너버스 연구소장
2001년 3월~2009년 2월 : 순천향대학교 정보보호학과 겸임교수
2005년 9월~현재 : 동국대학교 국제정보대학원 겸임교수
2011년 7월~현재 : 한국정보보호학회 이사
2015년 5월~현재 : 디지큐코리아(주) 부사장
관심분야 : ISMS, PIMS, 클라우드컴퓨팅보안, 빅데이터, 개인정보보호