사물인터넷 시대의 의료보안 기술 현황

김순석 (한라대학교)

목차

1. 개 요
2. Use Case 및 관련 기술 분류
3. 주요 중점 기술 현황
4. 결 론

1. 개 요

최근 사물인터넷 시대의 등장 및 성장과 더불어 의료서비스가 진화할수록 개인의료정보의 유출로 인한 프라이버시 침해 위협, 의료정보 관리의 문제 등의 역기능이 현재보다 훨씬 심각해 질 전망이다. 특히 e-Health 및 u-Health의 진행과 함께 보안관리가 요구되는 물리적 영역은 개별 병원에서 의료서비스의 사용자 공간으로 보안 영역이 확장되는 추세이다. 뿐만 아니라 기존 수기로 작성되던 의료정보가 전산화되면서 네트워크 기반의 중앙 집중 시스템에 저장되어 관리 및 처리되며 진료와 상관없는 병원 사무직원이 환자의 전자의무기록 열람이 가능하다거나 진료차트 관리 프로그래머가 담당하는 병원의 진료 차트를 유출하는 등 내부자의 고의나 과실로 인한 개인의료정보 유출은 병원정보화의 가장 큰 위협이 되고 있다.

원격의료로 대표되는 e-Health에서는 의료정보의 이동성이 증가하고 이동양도 많아지면서 의료정보에 대한 외부로부터의 공격가능성이 증가하고 있다. 인터넷을 활용한 건강정보 제공 사이트에 회원으로 가입하여 건강정보를 주고받는 의료서비스의 경우는 축적된 개인의 의료정보가 외부의 공격자에게 공격당해 개인의 민감한 의료정보가 유출될 수 있다. 또한 원격지 환자를 진료하는 원격의료에서 교환 및 저장되는 데이터에 대한 보안장치가 허술하면 해커 등 공격자들로부터 쉽게 공격을 받아 민감한 개인의료정보가 유출될 수 있다. 특히 현행 의료법에서는 원격의료를 위한 시스템에 대한 제도적 규정이 확립되지 않아 보안위협 가중되고 있는 실정이다. 뿐만 아니라 센싱과 모니터링 기능으로 대표되는 u-Health의 경우는 센싱 기능의 부정확성으로 인한 진단 오류, RFID 등을 이용한 과도한 개인정보 수집으로 인한 프라이버시침해 등의 가능성 또한 점차 증가하고 있다.

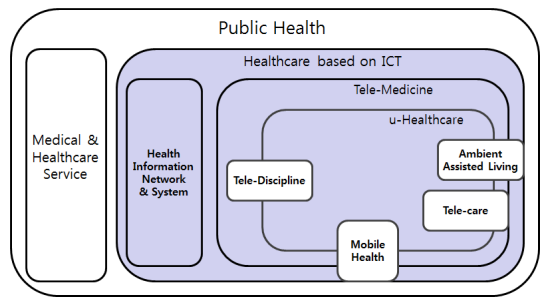
한편 세계보건기구의 TBT(Technical Barriers

to Trade) 협정에서처럼 회원국이 국가표준을 새로이 제정하거나 개정할 경우 국제표준을 기초로 사용할 것을 규정하고 있어 의료 보안 관련 표준 역시 예외 없이 지역적인 표준이 ISO(국제 표준화 기구)를 통해 국제 표준화되면서 단일 표준화되고 있으며 역으로 국제 표준이 곧 지역적인 표준화로 추진되고 있다. 따라서 국제적인 표준화는 기업들 간 논의를 통하여 서로의 이익을 극대화하면서 위험을 최소화 하는 상황이며 이러한 표준화 작업에 참여하는 기업만이 미래 시장에서 생존이 보장되는 시대가 이미 도래 하고 있다. 특히 u-Health를 위하여 EMR과 PHR의 Mobile 환경의 연계가 필요하고 따라서 의료정보의 획득, 전송, 저장시의 의료정보의 무결성과 안전성을 위한 의료보안 표준화는 향후 반드시 필요하다. 또한 국가적 규모의 공통 의료 보안 기술체계 및 서비스 플랫폼 표준 구축은 신규 서비스를 창출하려는 기업의 진입 문턱을 낮추어 의료 분야의 관련 기술발전을 촉진시켜 산업 활성화에 크게 기여할 수 있다.

본 기고문에서는 이러한 맥락에서 의료보안과 관련한 개괄적인 소개와 참조모델 및 Use Case, 그리고 관련한 주요 중점 기술 현황에 대해 소개하고자 한다.

2. Use Case 및 관련 기술 분류

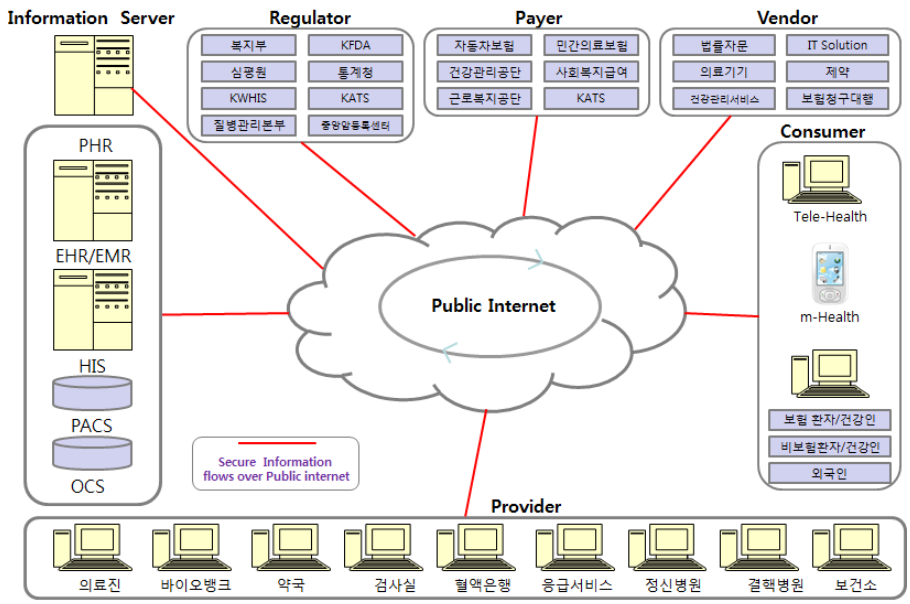
컴퓨터와 정보통신 네트워크를 기반으로 보건의료, 건강 정보 공유 및 서비스를 제공함으로서 환자 또는 소비자에게 지속적이고 상시적인 건강관리를 가능하게 해주는 기술 및 제반 서비스를 가리켜 우리는 Health ICT(Information Communication Technology)라 부른다[1]. 이는 건강 정보를 다루는 EMR(Electronic Medical Record), EHR(Electronic Health Record), PHR(Personal Health Record), u-Health, e-Health, smart Care, smart Healthcare 등과 같은 네트워크 기반 의료정보시스템 및 관련 서비스를 포함한다. 따라서 의료보안 또한 이들의 범위((그림 1) 참조) 내에 있으며 (그림 2)의 시스템 내에 존재한다고 볼 수 있다. (그림 2)에서 실선으로 표기된 부분은 각 개체들 간에 통신부분으로 안전한 전송이 보장되어야 함을 의미한다.



(그림 1) Health ICT의 범위[1]

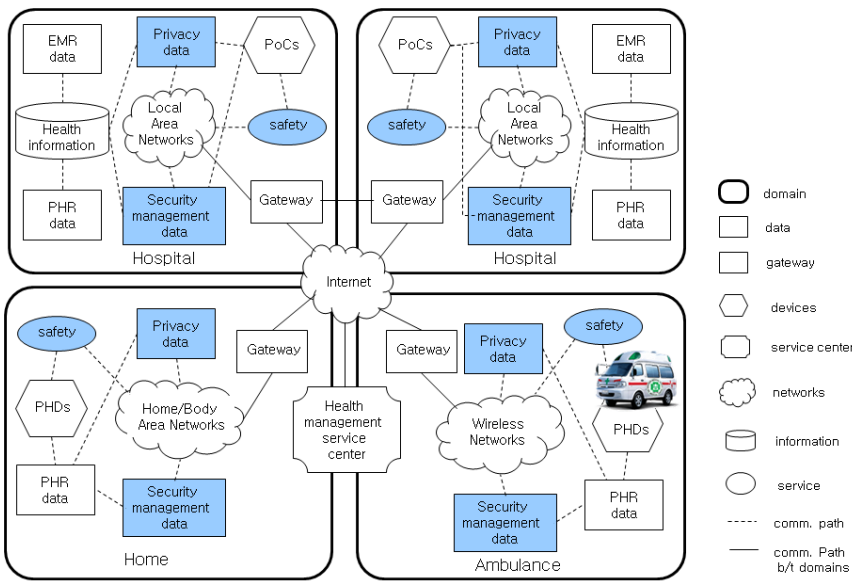
2.1 참조모델 및 Use Case

본 참조모델은 병원 내 또는 병원과 병원 사이 또는 병원 외부(각 가정 혹은 응급 구조차량)의 상황을 각 도메인으로 가정한 것이다. 이들 중 보안과 프라이버시가 고려되어야 할 건강 정보의 주 대상을 병원 내의 경우 각각 전자의무기록과 개인평생건강기록인 EMR과 PHR 데이터로 한정하였고 병원 외부의 경우는 PHR 데이터로 한정하였다. 병원 내부의 경우 건강정보 데이터베이스로부터 추출된 EMR과 PHR 데이터들 가운데 보안과 프라이버시가 보장되어야 할 대상 정보를 프라이버시 데이터와 보안관리 데이터로 분리하여 별도로 병원 내부에서 안전하게 이용하거나 LAN(Local Area Network) 망을 거쳐 게이트웨이를 통해 외부 또는 내부로 안전하게 전송될 수 있



(그림 2) Health ICT 시스템 및 체계[1]

도록 해야 한다. 또한 병원 내부에 설치되어 있는 현장진료형 의료장비(PoC)들의 경우 기기 안전성이 우선 고려되어야 하며 그리고 의료장비로(부터) 전송되는 생체 정보의 경우 또한 앞서와 마찬가지로 보안과 프라이버시가 보장되어야 할 대상 정보를 프라이버시 데이터와 보안관리 데이터로 분리하여 별도로 병원 내부에서 안전하게 이용하거나 LAN망을 거쳐 게이트웨이를 통해 외부 또는 내부로 안전하게 전송될 수 있도록 해야 한다. 가정 내의 경우 보안성과 프라이버시가 고려되어야 할 대상 정보는 혈당, 혈압, 등 PHD(Personal Health Device)로(부터)의 생체 정보인 PHR 데이터들로 이들 정보 또한 기기적인 안전성이 우선 고려되어야 하며 PHD 장비로(부터) 전송되는 생체 정보의 경우 역시 대상 정보를 프라이버시 데이터와 보안관리 데이터로 분리하여 BAN(Body Area Network) 망을 거쳐 게이트웨이를 통해 외부 또는 내부로 안전하게 전송될 수 있도록 해야 한다. 응급의료 상황을 가정한 구급차 내부의 경우 보안성과 프라이버시가 고려되어야 할 대상 정보는 가정 내와 마찬가지로 PHD로(부터)의 생체 정보인 PHR 데이터임으로 이들 정보 또한 기기적인 안전성이 우선 고려되어야 하며 이 경우 역시 대상 정보를 프라이버시 데이터와 보안관리 데이터로 분리하여 이동 또는 무선망을 거쳐 게이트웨이를 통해 외부 또는 내부로 안전하게 전송될 수 있도록 해야 한다. 단, 모든 각 도메인 내에서 외부 전송 시에는 보안성이 고려된 즉, 각종 전송보안 기술이 탑재된 가상사설망이나 IP 보안, SSL(Secure Socket Layer) 등이 이용되어야 한다. (그림 3)의 Use Case는 지금까지 언급한 참조모델의 개요와 설명을 바탕으로 모든 상황을 고려한 것이다. (그림 3)에서 각 가정의 경우 원격진료가 가능할 수 있으며 진료가 아닌 일반 건강관리의 차원에서 PHD로부터의 생체정보는 안전하게 게이트웨이를 통해 건강관리서비스센터로 전송될 수 있다. 또한 필요에 따라서는 응급상황의 경우 구급차 내에서는 해당 정



(그림 3) 의료보안관련 Use Case

보가 가정 내의 PHR 데이터와 연동될 수 있을 것이며 이들 정보들은 병원 내의 응급의료센터와도 상호 연동될 수 있을 것이다. 이러한 상황에서 각 도메인 내외부에서 다루어지는 프라이버시 데이터와 보안관리 데이터는 반드시 보호되어야 하며 전송 시에도 안전할 수 있도록 보안 기술이 반드시 탑재되어야 한다.

2.2 관련 요소 기술 분류

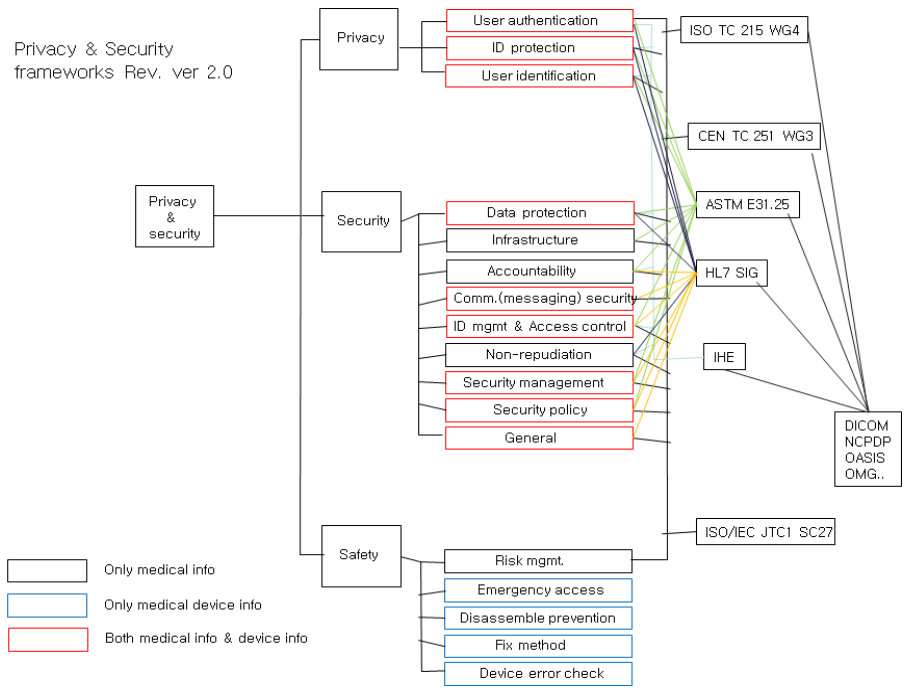
앞서 2.1절에서 기술한 참조모델을 기반으로 국제표준화기구인 ISO의 TC215 보건의료정보기술위원회[2]에서 정한 체계에 따라 관련한 보안 요소 기술들을 분류하면 (그림 4)와 같이 나타낼 수 있으며 이들은 다시 세부적으로 (그림 5)와 같이 나타낼 수 있다.

3. 주요 중점 기술 현황

본 장에서는 앞서 2.2절에서 살펴본 분류체계에 따라 국제표준화기구인 ISO의 TC215 WG4를 중심으로 각 분야별 주요 기술 현황에 대해 살펴보고자 한다.

3.1 사용자 인증기술

사용자 인증 기술과 관련하여 미국의 경우 연방법인 HIPAA Security Rule §164.308 관리적 보안조항에서 피고용인의 인증과 의료정보센터의 접근 정책과 절차, 접근 승인 등 정보접근에 대한 관리를 규정하고 있으며 이와 관련하여 NIST(National Institute of Standards and Technology)의 가이드 문서가 있다[3][4]. 캐나다의 경우 CHI(Canada Health Infoway) 주도로 가이드라인을 개발하고 있으며 CHI SCWG8 IT Privacy & Security Services에서 해당 표준화 연구를 진행하고 있다[5]. 한편 ISO TC 215에서는 의료정보시스템에서의 인증을 특화한 표준화는 진행하지 않고 있으며 다만 일반 정보시스템의 인증을 대상으로 한 ISO 표준으로 주로 전자서명에 관련된



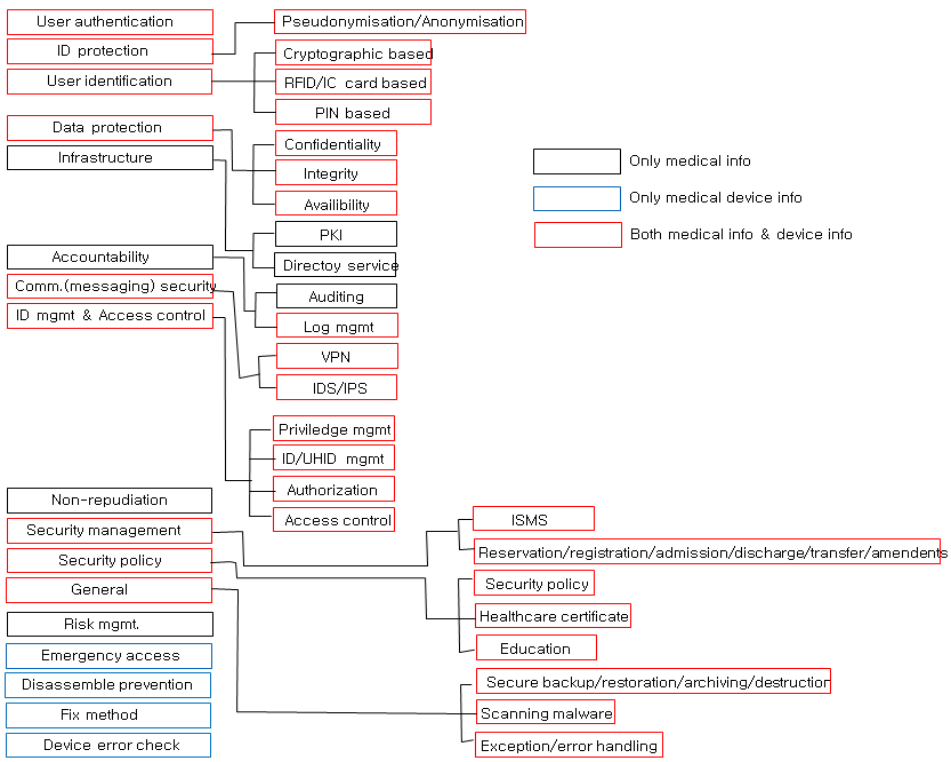
(그림 4) 의료보안관련 기술 및 표준화 분야

기술이나 암호화 알고리즘 및 해쉬 알고리즘을 이용한 인증 기술에 대한 표준이 제정되어 있다. 유럽 표준의 경우도 마찬가지 상황으로 인증 메커니즘 중 하나인 전자서명에 대한 표준 중심으로 표준 제정 및 진행 중이다. 국내 표준 현황 또한 일반 정보 보안기술에 대한 전자서명 기술 중심으로 표준화 진행되어 왔다. 따라서 의료정보시스템의 경우 전자서명, 타임 스템프, 암호화 알고리즘 등 특정 보안 기술에 대한 메커니즘은 크게 다르지 않을 것이나 향후 의료정보시스템에 참여하는 주체별 인증방법에 대한 표준화의 필요성이 있다.

3.2 사용자 ID보호기술

미국의 경우 HIPAA에 의해 정의된 18개 PHI (Personal Health Information)[1]를 모두 제거하는 safe harbor 원칙에 의해 익명화가 진행되고 있다. 그러나 다만 Direct identifier를 제거하는 것에만 집중하고 있으며, Quasi identifier에 관해서는 현재 개별 연구자 수준에서 진행되고 있는 실정이다. 캐나다의 경우 CHI에서 주도적으로 가이드라인을 개발, 제시하고 있으며 주민등록번호 등과 같은 직접적인 개인식별 코드에 대한 제거는 표준화되어 있다. 다만, 의료 정보의 특징상 진료기록에 텍스트 형태로 기록된 개인 정보들에 대해서는 현재 기술로 제거하는 것이 쉽지 않은 실정이다. 현재 텍스트 마이닝과 역할기반 시스템 등을 통해 여러 가지 방법들이 제안되고 있으나 아직 기술 개발이 초기화 단계이며 특히 앞서 언

1) ①이름, ②주소정보(우편번호 등), ③개인과 직접 관련된 날짜정보(생일, 자격 취득일 등), ④전화번호, ⑤팩스번호, ⑥이메일 주소, ⑦사회보장번호, ⑧의료기록번호, ⑨건강보험번호, ⑩계좌번호, ⑪자격취득 번호, ⑫자동차 번호, ⑬각종 장비 식별 번호, ⑭URL정보, ⑮IP주소, ⑯생체정보(지문 등), ⑰얼굴사진, ⑱기타 고유 특징 등



(그림 5) 의료보안관련 세부 기술 및 표준화 분야

급한 Quasi identifier를 제거하는 기술은 심각성에도 불구하고 학술적 측면에서의 연구도 많이 진행되지 않고 있어 향후 시급히 연구되어야 할 필요성이 있다.

3.3 사용자 식별기술

사용자 식별 및 인증 기술은 시스템의 안전성과 원활한 서비스를 위해 반드시 필요한 기술로서 현재 대부분 의료시스템의 경우 지식기반 기술 즉, 암호나 PIN의 유효성을 확인하여 사용자를 식별하는 방법을 사용하고 있다. IC카드의 경우 오프라인 전자진료카드로서 내원환자 및 직원에게 발급되어 대상을 식별 및 인증할 뿐 아니라 수납, 처방전 발급, 진료안내 및 출입통제 등 다방면에 활용 가능하여 이미 국내외적으로 많은 병원에서 이를 도입 및 활용하고 있다. RFID 기술의 경우 환자식별 및 의약품관리, 의료장비, 감염성 폐기물 관리 등에 활용되고 있다. 현재 사용자식별 및 인증방법과 관련하여 개별적 표준이 따로 정해져 있지는 않으나 많은 표준들에서 이에 대해 부분적으로 다루고 있다.

3.4 데이터 보호 및 보안 기반구조

데이터 보호 기술은 이미 오랜 시간 동안 연구개발되어 있으며 많은 상용 제품들이 현재 출시되어 있다. 또한 본 기술의 여러 세부 기술들이 독자적인 표준안으로 현재 제정되어 있는 상태이다. 한편 공개키기반구조 및 디렉토리 기술의 경우 원천기술은 이미 전통적인 보안 분야에서 기업뿐만 아니라 정부기관 등에서 다양하게 보유되

고 상용화되어 있어 새로운 기술은 아니나 ISO를 중심으로 병원이나 보건관련 기관 등에서 건강정보보호를 위해 공개키기반구조(PKI)에 관한 ISO 국제 표준이 제정된 바가 있으며 현재 국내 표준으로의 부합화가 진행 중이다.

3.5 책임추적성 보장 및 통신보안 기술

책임추적성 보장 기술은 현재 ISO를 통해 이미 국제 표준화가 진행되어 있으며 우리나라의 경우 지난 2012년에 국내 부합화가 진행된 바가 있어 올해부터 해당 병원이나 관련 업체에서 실질적인 개발 및 구현이 이루어져야 할 것으로 전망된다. 한편 가상사설망이나 침입탐지 등 통신보안기술은 기존 전통적인 보안 분야에서 이미 ISO IEC를 통해 표준이 제정된 바 있으나 의료정보 분야와 관련해서는 현재 ISO를 중심으로 건강정보기반구조를 위한 동적요구 가상사설망에 관한 표준 및 EHR 통신 부분의 보안 표준화가 진행 중에 있다. 또한 전송부분에 있어 메시징 보안 분야는 HL7 Ver 3.0이 발표된 바가 있으며 국내와 유럽의 경우 자국의 부합화가 이미 이루어진 상태이다. 우리나라에서도 해당 표준에 대해 병원 및 업계, 관련 학계를 중심으로 실질적인 개발 및 구현이 이루어져야 할 것으로 전망된다.

3.6 ID관리 및 접근통제 기술

현재 이 분야에 대해 EMR, OCS(Order Communication System), HIS(Hospital Information System) 등 전반적인 의료시스템에 대한 접근 통제를 효율적으로 관리할 수 있는 통합인증 및 권한관리 기술이 주를 이루고 있다. 특히 의료정보의 교류에 대한 요구가 높아지면서 병원 등 기관 내부뿐 아니라 기관 외부의 사용자의 ID관리 및 접근정책에 대한 연구도 진행되고 있다. 또한 모바일 환경 등 다양한 접근 및 사용 환경을 고려한 적합한 의료정보시스템 역할기반 접근제어 기술이 활발하게 진행되고 있다. 현재 ISO TC215 WG4에서는 데이터 레코드 및 기능에 대해서 사용자의 역할에 따라 접근이 통제 가능하도록 역할에 대한 기능 구조적 집합 및 모델을 정의하고 있다. 특히 의료 응용 서비스 모델에서 환자 및 의료 서비스 관계자에 대한 역할 정의에 더욱 중점을 두고 각 역할 들은 구조적(정적구조)이거나 기능적인 타입(동적인 역할모델)으로 분류가능하다고 보고 있다.

3.7 보안관리 및 위험관리

보안관리와 관련하여 조직의 정보보호관리 체계에 대한 외부기관의 객관적 평가로 정보보호관리 체계 인증이 있으며 국내에서는 한국인터넷진흥원(KISA)이 시행하는 ISMS인증이 있고 국제적으로는 ISO27001인증 등이 있다. 미국의 경우 연방법인 HIPAA Security Rule에서 정보보호관리체계 별 명세를 정의(§164.308, §164.310, §164.312)하고 있으며 환자 등록, 입원, 퇴원 등의 의료기관 프로세스 별 정보시스템에 대한 객체 중심 모델을 정의한 ASTM 표준(ASTM E1715)이 있다. 한편 최근 ISO TC 215에서는 ISO27000 시리즈를 의료분야에 접목한 표준(ISO 27799)을 발표하였으며 이 표준은 2015년 3월 현재 최종 단계의 투표가 진행 중이다.

한편 의료기기를 포함한 의료 소프트웨어의 위험관리 부분에 있어 국제적으로 ISO를 중심으로 현재 ISO 80001 등 상당부분 표준화가 이루어져 있는 실정이며 국내에서도 지난 2011년 12월 위험분류 및 환자 안전 부분에 대해 일부 표준 문건에 대해 국내 부합화가 이루어진 상태이다. 그러

나 국내의 의료 소프트웨어를 포함한 의료기기 분야의 위험관리는 현재 이루어지고 있지 않아서 향후 시급히 이루어져야 할 것으로 전망된다.

3.8 기타 보안 기술

부인방지 기술과 관련하여 현재 HL7의 Ver 3.0내에서 주고받는 메시지에 있어 부인방지가 적용되고 있어 지금부터 해당 병원이나 관련 업체에서 실질적인 개발 및 구현이 이루어져야 할 것으로 전망된다.

자료 백업, 저장, 아카이빙, 그리고 폐기와 관련하여 ISO 국제 표준화에 따른 국내 부합화가 지난 2011년 12월 29일에 제정됨에 따라 해당 병원이나 관련 업체에서는 빠른 시일 내에 개발이나 구현이 이루어질 것으로 전망된다.

한편 건강정보의 프라이버시 보호와 관련한 정책이나 교육측면에서 우리나라가 현재 국제적으로 선점 및 선도하고 있으며 이미 우리나라 산업체(병원) 및 협회가 주도하여 지난 2012년 5월 ISO TC215 WG4에 new work item으로 제안하여 국제표준을 주도하고 있는 상태이다.

4. 결 론

본 기고문에서는 국제표준화기구인 ISO의 보건의료정보기술위원회인 TC215의 보안분야 워킹그룹인 WG4를 중심으로 의료 보안과 관련한 개괄적인 소개와 참조모델 및 Use Case, 그리고 주요 중점 국내외 기술 현황에 대해 살펴보았다. 향후 의료보안 분야가 국내외 특히 국내에서 주요 비즈니스 이슈로 자리 잡기 위해서는 기술적인 문제는 차체하고서라도 먼저 원격의료와 관련한 의료법의 제도 개선이 반드시 선행되어야 할 것이다. 만일 제도 개선이 점진적으로 이루어 질 경우 앞서 언급한 기술적인 개선을 통해 독거노인이나 고령자 혹은 섬이나 도서산간지역의 소외계층에 의료 복지의 실현이 앞당겨질 것이라 미루어 짐작해 본다.

감사의 글

이 논문은 2013년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2013R1A1A2006745).

참 고 문 헌

[1] Health-ICT 국가전략보고서, 기술표준원, 2012.
[2] ISO TC215, http://isotc.iso.org/livelink/livelink/open/tc215
[3] HIPAA(Health Insurance Portability and Accountability Act), http://www. hhs.gov/ocr/privacy/
[4] NIST(National Institute of Standard and Technology), http://www.nist.gov/
[5] CHI(Canada Health Infoway), https://www.infoway-inforoute.ca/

저 자 약 력

김 순 석
이메일 : sskim@halla.ac.kr

- 2003~현재 한라대학교 컴퓨터공학과 조교수
- 2011~현재 ISO TC215 보건의료정보 전문위원
- 2010~현재 TTA PG419 유헬스 프로젝트그룹 특별위원
- 관심분야 : 의료보안, 유헬스보안 등