情 報 保 護 學 會 誌
第17卷 第1號, 2007. 2

u-헬스케어 서비스에서의 의료정보보호

송지은*, 김신효**, 정명애***

요 약

u-헬스케어 서비스의 발달에 따라 기존의 질병 발생 후에 대응하는 방식의 병원 치료적 패러다임에서 탈피하여 환자가 무선 의료 기기를 휴대하거나 주변 환경에 설치된 의료 장치를 이용하여 일상생활 가운데 건강관리, 질병 예방, 신속한 치료 등의 서비스가 가능해지고 있다. u-헬스케어 서비스가 고도화 될수록 지능화된 의료 센서나 기기에 의한 개인 생체 정보 및 주변 환경 정보에 관한 모니터링이 가능해지고 유무선 네트워크를 통한 건강 정보의 공유가 확대될 것이다. 그러나 u-헬스케어는 개인 건강/의료 정보를 포함한 극히 개인적인 정보를 주로 다루고 있고 유무선 네트워크와 절대적으로 밀접한 연관을 맺고 있으며, 의료 정보 권한과 관련된 다양한 이해 당사자가 존재할 수 있다는 점에서 보안 및 프라이버시 측면에서 다양한 취약점과 위협이 존재할 수 있다. 따라서 안전한 u-헬스케어 서비스 연구 개발을 위해 u-헬스케어의 개요와 특성을 살펴보고, 관련 보안 이슈 및 요구사항을 분석하여 대응 가능한 합리적인 기술적 대안들을 검토코자 한다..

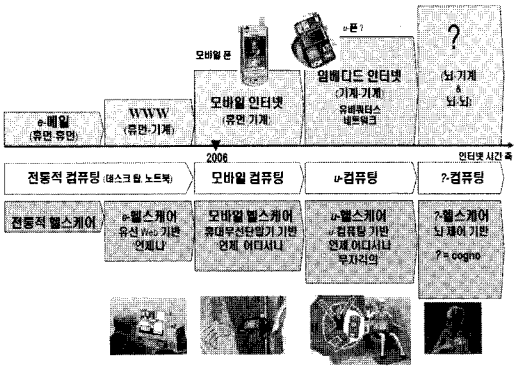
Ⅰ. 서 론

평균 수명 연장과 건강한 삶을 오래 유지하고자 하는 '건강한 삶 · 안전한 삶 · 편안한 삶 · 쾌적한 삶'등 '삶의 질' 향상에 대한 욕구는 필연적으로 고도화된 의료 서비스 발전을 야기시켰다. 아울러 유비쿼터스 컴퓨팅 기술의 발전과 IT-BT-NT를 포함한 융합기술 발전경향은 유비터스 헬스케어(이하 u-헬스케어)의 실현을 가속화하고 있다. u-헬스케어 서비스가 고도화 될수록 지능화된 의료 센서나 기기에 의한 개인 생체 정보 및 주변 환경 정보에 관한 모니터링이 가능해지고 유무선 네트워크를 통한 건강 정보의 공유가 확대될 것이다. 이와 같이 u-헬스케어는 개인 건강/의료 정보를 포함한 극히 개인적인 정보를 주로 다루고 있고 유무선 네트워크와 절대적으로 밀접한 연관을 맺고 있으며, 의료 정보 권한과 관련된 다양한 이해 당사자가 존재할 수 있다는 점에서 보안 및 프라이버시 측면의 다양한 취약점과 위협이 존재할 수 있다. 따라서 본 고에서는 u-헬스케어의 특성에 근거한 보안 이슈 및 요구사항을 분석하고 이와 관련한 합리적인 기술적 대안들을 검토해본다.

Ⅱ. 헬스케어 개요

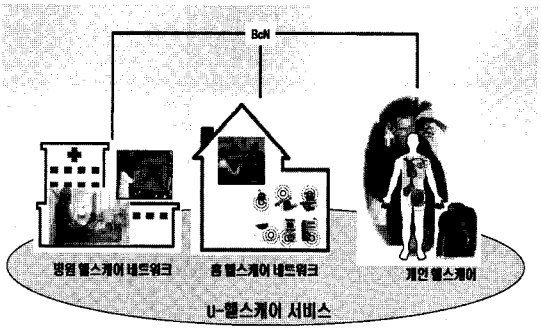
2.1 헬스케어 서비스 패러다임

u-헬스케어는 건강하고 편안한 삶에 대한 사회적 욕구 증대와 고도화된 의료 서비스 구축을 위한 정부의 전략적 정책 및 투자 증대로 주목 받고 있는 대표적인 서비스 분야이다. u-헬스케어 서비스는 바이오 센서 및 스마트 의료 기기의 발달, 유무선 네트워크의 안정화,



〔그림 1〕 헬스케어 서비스 패러다임의 진화

* 전자통신연구원 IT융합서비스부문 의료정보연구팀 연구원(happybirds@etri.re.kr)
** 전자통신연구원 IT융합서비스부문 의료정보연구팀 선임연구원(shykim@etri.re.kr)
*** 전자통신연구원 IT융합서비스부문 의료정보연구팀 팀장(machung@etri.re.kr)



〔그림 2〕 헬스케어 서비스의 분류

의료 데이터의 교환 및 처리를 위한 표준 기술 등이 뒷받침 되면서 구체적인 서비스 실체화가 가속화되고 있다. 다음 〔그림 1〕은 헬스케어 서비스의 패러다임의 진화를 나타낸 것이다.

e-헬스케어의 경우 기존의 의료 장비에 디지털 및 네트워크 기능을 추가한 수준이며 단순한 홈 헬스케어용 진단 장치나 원격 진료 정도의 서비스를 포함한다. 보다 발전된 형태의 서비스로서 기존 의료 장비에 무선 네트워크 기능을 추가한 m-헬스케어 서비스를 들 수 있다[2]. 이동성이 보장되는 휴대용 단말기에 진단 및 분석 기능을 부여하여 사용자가 '언제, 어디서든' 간편하게 의료 진단 서비스를 받도록 하는 것이 그 목적이다. 실제로 Pulse Oximeter, 휴대용 혈압측정기, 당뇨 폰 등 다양한 FDA 승인 휴대용 의료 기기들이 연구 개발 되었다. u-헬스케어는 기존의 e-헬스케어와 m-헬스케어의 장점을 모두 포함하고 더 나아가 무자각, 무구속적 의료 진단 및 분석을 추구한다. 즉, u-헬스케어 서비스는 모바일 의료서비스의 진화된 모델로서 공간적, 시간적 제약을 없애고 환자가 생활 공간 속에서 다양한 의료 센서 및 기기를 통해 수집된 생체 정보와 환경 정보를 기반으로 중앙의 원격 의료 서비스 시스템을 통해 언제 어디서나 의료 피드백을 받을 수 있는 서비스를 총칭한다. 대표적인 u-헬스케어 서비스 예로서 좌변기를 이용한 체지방 측정, 착복형 진단 셔츠, 체내 이식형 의료기기 등이 개발 되었으며 미국의 로체스터 대학이나 EU 및 미국, 일본 등을 중심으로 u-헬스케어 비즈니스 프로젝트가 활발히 진행되고 있다[3]. 향후, 보다 고도화된 헬스케어 패러다임이 등장하게 될 것이다. 뉴런 센서 기술이나 나노 생체 센서의 개발 및 이를 이용한 제어/진료 시스템이 연구될 경우 보다 정확하고 신뢰성 높은 헬스케어 서비스가 실현될 것이다.

2.2 u-헬스케어 서비스의 분류

헬스케어 서비스는 응용 환경에 따라 〔그림 2〕와 같이 병원 헬스케어 홈헬스케어, 그리고 BAN(Body Area Network) 중심의 개인 헬스케어로 분류할 수 있다. 병원 중심의 헬스케어는 기존 아날로그형식의 병원 기록을 EHR이나 EMR 혹은 PACS와 같은 디지털 시스템을 구축한 것에서부터 출발한다. 또한 더 나아가 의료 업무에 사용되는 의료 기기에 모바일 의료 기기를 도입, 진료 서비스의 효율화를 꾀하고 질병 예측 및 진단 시스템, 약물 반응 시스템 등 진료자의 업무를 보조 혹은 대체 할 만한 수준의 다양한 응용 서비스들에 관하여 활발한 관련 연구가 진행되고 있다. 홈-헬스케어 서비스의 경우 가장 활발하고 구체적인 u-헬스케어 서비스 모델로서, 기존의 홈-네트워크와 유사한 구조를 띈다. 즉, 댁내에 설치된 다양한 유무선 의료 센서 및 장비를 이용해 수집된 생체 및 의료 정보를 토대로 댁내 독자적으로 혹은 외부 병원 정보 시스템과의 연계를 통해 실시간 의료 서비스를 제공할 수 있다. 미국의 로체스터 대학의 스마트 메디컬 홈 프로젝트가 대표적 예이다[1]. 해당 프로젝트에서는 스마트 의료 센서부, 측정 및 분석부, 정보 교환 인터페이스 부 등을 포함하는 홈헬스케어 프레임워크와 댁내에서 피부암 등의 상태를 상시 체크할 수 있는 smart mirror, 상처의 병원체 감염 유무를 상시 감시 보고하는 smart bandage, 복용약에 대한 정보와 복용 유무를 알려주는 smart drug 등의 응용 서비스를 개발하였다.

이 외에도 체내 삽입 혹은 체내 부착형 초소형 의료기기를 이용하여 심전도, 혈압 등의 생체 신호를 측정하고 BAN을 구성하여 환자의 위치, 건강 상태 등을 실시간 모니터링 및 진료 서비스를 수행하는 개인 헬스케어 프로젝트 또한 활발히 수행중이다. 대표적으로 독일 Berlin 대학의 Microelectronics 연구소에서는 센서를 체내에 이식한 후 센서로부터의 신호를 무선으로 측정하는 시스템에 대한 연구를 수행하여 인공관절 응력 측정, 뇌압 측정, 심장심박 측정 등에 응용한 바 있다. 그 외에 많은 EU의 외국 대학 및 기업의 연구진들이 소형 센서시스템 및 소형 무선전송 및 처리장치에 대한 연구 개발을 진행 중에 있다.

이와 같이 u-헬스케어 서비스는 BINT 기술의 융합을 도모할 뿐 아니라 응용 서비스에 따라 보다 정확하고 다양한 의료 서비스를 제공하기 위해 관련 기관 및 사

용자간 의료 데이터의 교환과 공유를 필요로 한다. 이와 관련하여 최근 데이터에 대한 권한 관리와 프라이버시 보호가 큰 이슈로 대두되면서 다양한 이해 당사자(stakeholder)들이 존재 할 수 있다. 즉, u-헬스케어 서비스는 타 유비쿼터스 컴퓨팅 기술 분야에 비해 다루어지는 정보 속성이 매우 민감하고 이질적인 서비스 도메인 간 혹은 다양한서비스 관계자 간 정보 공유가 빈번하게 이루어질 수 있다는 점에서 심각한 보안 우려사항이 존재한다. 따라서 신뢰성 높은 u-헬스케어 서비스의 확대를 위해 다양한 보안 이슈와 합리적인 대안들을 충분히 고려해야 한다.

2.3 u-헬스케어를 위한 의료 정보화

u-헬스케어 서비스의 구성 기술로서 지능화된 바이오/메디컬 센서를 포함한 스마트 의료 디바이스가 존재한다. 뿐만 아니라 가용성과 신뢰성이 높은 유무선 네트워크 기술과 생체 신호 및 환자 정보, 임상 진료 데이터 등을 의료 정보로 가공 및 처리 할 수 있는 의료 정보 시스템이 필수적으로 요구된다. 보다 구체적으로, 바이오 칩 혹은 센서를 포함한 스마트 의료 디바이스를 이용한 데이터 수집 기술, 수집된 의무 데이터의 표기 기술, 메시징 및 의료데이터 교환 기술, 의료 정보 데이터 관리 및 가공서비스를 위한 정보 서버 기술과 안전한 의료 서비스 제공 및 프라이버시 보호를 위한 의료 정보보호 기술 등이 이에 속한다. 이 외에도, 의료 전문 용어의 정의, 비즈니스 의료전자카드 기술, 전자 투약 처방 및 전달 기술 등이 기본 의료정보화 기술과 통합 및 연동되어야 한다.

이와 같이 물리적 디바이스 단에서 측정된 생체 및 의료 데이터를 헬스케어 서비스 차원에서의 의미 있는 정보로 활용 가능하도록 하기 위해서는 의료 정보 표기 및 처리, 의료 용어, 의료 데이터의 교환 방식 등에 대한 표준화가 선행되어야 한다. 실제로 그간 의료 정보화와 관련하여 국가 간 혹은 국가 내 의료 서비스 기관 및 관련 업체 간에 협력 및 긴밀한 상호 협의 없이 산발적이고 독립적으로 개발 되어 호환 및 통합에 있어 큰 한계에 부딪혀왔다. 이를 개선하기 위하여 캐나다, 미국 및 유럽 등에서는 상호 호환 가능한 의료 정보 서비스를 보장하기 위해 국내 표준 및 법제, 기술 권고안 등을 제정해왔으며, CEN, ISO, IEEE, DICOM, HL7, IHE 등에서도 활발히 국가 간 의료 정보 교류 및 공유, 시스템 통합 등을 염두 한 국제 표준을 활발히 개발 중에 있다. 국내에서도 최근, 보건복지부 및 국내 산업표준위원회를 중심으로 전자 의무 기록 표준 및 관련 법안 마련 등에 박차를 가하고 있다.

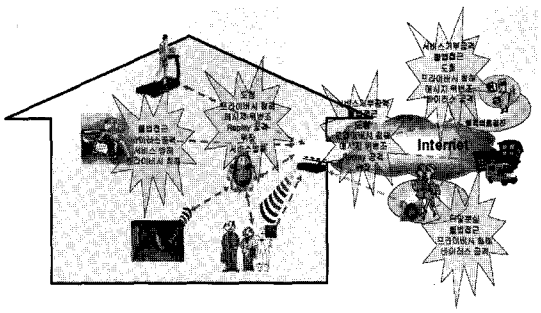
또한, 현재로서는 의료 서비스 혹은 헬스케어 시장에서 의료 정보의 전산화 및 전산 통합 수준의 의료정보화가 대형 병원을 중심으로 활발히 이루어지고 있다. 의료정보화는 의료영상정보시스템(PACS), 처방전달 시스템(OCS)과 전자의무기록(EMR)을 연동함으로써, 비용절감 효과 이외에 진료의 안정성 및 서비스 질 향상, 환자 대기시간 절감, 정보 저장의 편의성, 환자 기록에 대한 의료진의 접근성이 용이해졌다. 특히, 지금까지 병.의원에서 독자적인 형태로 관리되었던 EMR은 최근 개인의 평생 전자 건강 기록인 EHR의 개념으로 발전하게 되었다. 이러한 EMR은 사용자 중심의 u-헬스케어 서비스를 위해서 선행되어야 할 가장 기본적인 서비스이며, 국가적 차원으로 국가 보건 의료 정보 인프라(NHII: National Healthcare Information Infrastructure) 구축에 필수적이므로, 이에 대한 기술 표준화 및 상용 수준의 시스템 개발이 지속적으로 확대될 것으로 전망된다[4][5].

이와 같이 EMR 혹은 EHR 중심의 의료 정보화 및 u-헬스케어 서비스 모델 등에 대한 활발한 연구가 수행되고 있으나 반면, 보안 및 프라이버시와 관련된 연구는 아직까지는 연구는 미비한 실정이다. 이 같은 보안 문제 측면에서 HIPAA에서 주도적으로 수행하고 있는 보안 및 프라이버시에 대한 논의는 큰 의미를 가진다[6]. 다음 장에서 보다 상세하게 헬스케어 정보화와 관련한 보안 이슈를 분석해보고 국내외 의료 정보 보안 법제 및 관련 기술 표준, 및 합리적 대안으로서 주목할 만한 기술들에 대해 보다 상세히 살펴본다.

Ⅲ. u-헬스케어 환경의 의료 정보 보호

3.1 u-헬스케어 정보보호 이슈

최근 개인 정보의 남용에 관한 '빅 브라더(big brother)' 문제와 같은 프라이버시 보호 의식이 확산되면서 u-헬스케어 분야에서도 최근, 데이터 보호 및 프라이버시 보호 문제를 중요 이슈로 간주, 법제도적, 기술적 측면 등 다각적 차원에서 대응 방안을 간구하고 있다[8]. u-헬스케어 환경에서는 다음 〔그림 3〕과 같은 다양한 보안 위협 및 취약성이 존재한다.



〔그림 3〕 u-헬스케어 환경의 보안 취약성 및 위협

u-헬스케어 서비스 또한 기존의 유무선 네트워크 기반 서비스와 유사한 형태의 보안 위협을 보유하고 있다. 서비스 도메인 내 유무선 네트워크를 통한 도청이나 사용자의 단말에 대한 불법 접근, 네트워크를 통한 의료정보 시스템에 대한 불법 접근, 헬스케어 관련 주요 정보에 대한 위변조, 서비스 시스템에 대한 서비스 거부 공격 등이 대표적인 예이다. 따라서 이와 같은 보안 위협으로부터 신뢰성 있고 안전성 높은 u-헬스케어 서비스를 위해 데이터 보호 및 기반 네트워크 보호 등의 관련 보안 서비스 기술이 요구된다.

이 외에도 기존 서비스와는 다른 u-헬스케어 특성에 기인한 보안 위협이 존재한다. 의료서비스 즉, 정확한 진료를 받기 위해서는 생체 정보를 포함한 개인의 질병 내력, 가족력, 신체적 특징 등의 개인 의료 정보를 충분히 제공해야 하며, 이 정보는 환자가 이동함에 따라 중복된 검사와 의료 조치가 반복되는 것을 막기 위해 선택적으로 다른 의료 기관(병.의원 또는 보건소 등)에 위임 및 제공되어야 한다. 이와 같이 개인의 정보가 공유되는 환경에서 환자의 의도된 목적에 맞게 정당한 사용자에 의해 유효한 방법으로 활용되도록 강제 및 권고할 수 있는 제도와 기술이 필요하다. 또한, 수집된 상황 정보 등을 통해 새로운 형태의 개인 프라이버시 침해 가능성이 존재한다. 즉, 수집 및 활용 대상에 속하는 생체 정보, 개인 건강 및 병력 정보, 헬스케어 서비스 정보, 개인 행동 특성이나 생활 습성 등에 대한 방대한 정보는 서로 유기적 결합에 의해 방대한 개인 정보로 전이할 수 있기 때문이다. 이는 개인의 사생활에 대한 침해 사례를 충분히 초래할 수 있다. 또한, 개인 인증 및 식별 방법이 다양화 되면서 유일무이한 개인 생체 정보가 한 대안으로서 고려되고 있다. 이와 같은 생체 정보의 경우 노출 및 위변조 되었을 경우 새로운 생체 정보로의 변경이 쉽지 않고 신체 손상으로 인하여 의지적, 자각적인 생체 정보의 제공이 불가능 할 경우에 대해서도 원활히 인증 및 식별할 수 있는 방안이 간구되어야 한다. 이 외에도 보다 향상된 수준의 의료 서비스와 개인의 의료 건강 정보에 대한 접근성을 용이하게 하기 위하여 향후, 이질적인 병원 정보 서버 간 환자에 대한 건강 정보 공유가 빈번하게 이루어질 것이다. 이질적 의료 도메인 간 개인의 건강/의료 정보를 교환 시 인증된 도메인 간에 안전하게 가용한 정보만을 송수신 하도록 지원할 수 있는 보안 기술이 필요하다. 이와 같은 보안 기술적 요구사항들은 유비쿼터스 컴퓨팅 기술을 활용한 u-헬스케어 시스템의 초기 설계 시 동시에 반영되어야 한다.

3.2 의료 정보 보호 표준 기술 및 법제도

미국의 경우 2003년 4월 HIPAA(The Health Insurance Portability and Accountability Act)의 Privacy & Security Rule 적용을 시작으로 의료정보 보안에 대한 요구가 급증하고 있으며, 이미 많은 의료솔루션 업체들이 PKI 또는 데이터 암호화 등을 중심으로 보안 기술들을 제품에 적용하고 있다[6][7]. HIPAA의 적용을 기점으로 하여, 적어도 미국에서 개발 운용되는 모든 의료정보 관련 솔루션에 보안기능이 필수적으로 추가되어야 한다. HIPAA 프라이버시 규칙이 가지는 의미는 특히 환자 개인에 대하여 개인건강기록 공개 제한 요구 권리, 비밀연락과 건강 기록수정 요청 권리, 공개 내역에 대한 권리, 개인 건강 기록 조사 및 사본 입수 권리 및 침해 발생 시 진정서를 제출할 수 있음을 명시하고, 환자의 허가나 동의가 필요한 경우를 분명히 정의함으로써 의료정보의 제공 시 프라이버시 침해를 최소화하고 법적 분쟁 소지를 없애는 효과를 주었다는 점이다. 또한 HIPAA의 보안 규칙에서는 관리상의 안전장치(Administrative Safeguard), 물리적인 안전장치(Physical Safeguard), 기술적인 안전장치(Technical Safeguard)를 정의하고 있으며 다음 〔표 1〕과 같다[7].

이 외에, 의료 정보보호 관련 인증 기준으로서 CCHIT (Certification Commission for Healthcare Information Technology)가 제정한 EHR 보안 기준이 있다[10].

미국 정부가 건강 정보 기술(Health Information Technology)의 광범위한 사용과 EHR의 일상적 사용을 촉구하면서, 미 HIT 산업협회는 HIT 제품을 인증하기 위한 자발적인 민간 조직으로서 CCHIT를 설립하였다.

〔표 1〕 HIPAA Security Technical Regulations

기준	조항	(R)=의무, (A)=권고	
기술적 보장조항			
접근제한	164.312(a)(1)	개별 이용자의 신원확인	(R)
		비상시 접속 절차	(R)
		자동 로그오프	(A)
		암호화와 디코딩	(A)
검사 관리	164.312(b)		
정보의 보전	164.312(c)(1)	전자기밀의료정보 인증을 위한 메커니즘	(A)
개인 혹은 단체 인증	164.312(d)		
전송 보안	164.312(e)(1)	정보보전성관리	(A)
		암호화	(A)

CCHIT는 기능, 상호연동, 보안과 신뢰성, 인증 프로세스 등 4개의 WG을 운영하고 있고 보안 WG의 경우, 외래 환자용 EHR(Ambulatory EHR) 보안 기준과 입원 환자용 EHR(Inpatient EHR) 보안 기준을 개발하고 있다. CCHIT가 제정한 외래 환자용 EHR 2006년 보안 기준의 경우, 접근 통제, 보안 감사, 인증, 보안 기술 서비스, 백업/복구, 보안 기술 문서 제공 등의 내용을 골자로 하고 있다. 그러나 여전히 해당 법 제도 들이 프라이버시나 보안에 대해서 언급하고 있으나, 데이터의 소유권에 대해서는 언급하지 않아, 진료자료의 소유권 문제가 발생의 소지가 존재한다. 따라서 국내 의료 관련 정보보호 법.제도 제정 및 보완 시에 의료 데이터의 보안 및 프라이버시 뿐 아니라 소유권에 관한 문제도 반드시 심각하게 고려해야 한다.

의료 정보 기술 표준의 경우, 그 범위는 의료 행위를 나타내는 용어 및 참조 모델, 진료 기록의 형식 및 서식, 정보의 메시징 방법 및 의료 정보 보안과 같은 인프라 기술에서부터 의료 기기 규격 및 인터페이스 혹은 비즈니스 모델 요구사항 등에 이르기까지 다양하다. 또한, 의료정보 기술의 표준 이슈는 지역별 블록화 추세 강화, 적합성 및 상호운용성에 관한 관심의 증대, 지적재산권과 표준화간의 조화 문제, 표준 제정 과정에의 이용자 참여 증대 등과 같은 양상을 띄고 있다. 현재, 의료 정보와 관련된 대표적인 국제 표준 기구(Global SDOs: Standard Development Organizations)및 해당 개발 기술은 〔표 2〕과 같다.

〔표 2〕 의료 정보 관련 표준화 기구

DICOM	Digitized Image Communication in Medicine	Medical Image
IEEE	Institute of Electrical and Electronic Engineering	Network and Device Communication
CEN	Committee for European Normalization	As ISO
ISO	International Organization for Standardization	Health Informatics in general
HL7	Health Level 7	EHR, Messaging and Communication
WHO	World Health Organization	Classification of Diseases, pharmacy
SNOMED	Systematized Nomenclature of Medicine	Classification of Diseases, pharmacy

대표적인 의료 정보 보안 표준은 ASTM E31.25과 ISO/TC215 WG4에서 활발히 제안중이다. ASTM (American Society for Testing and Material)은 미국에서 유통되는 거의 모든 제품 및 재료에 대한 용도와 특성을 시험하고 제품의 품질을 규격화함으로써 제품 생산자와 사용자가 손쉽게 이와 같은 재료를 사용할 수 있도록 인증을 다루는 표준 기구로서, 현재 E31 기술 위원회에서 헬스케어 관련 표준화를 주도하고 있다〔9〕. ASTM의 E31 Healthcare Informatics 기술 위원회는 특정 환자 정보나 지식을 포함한 의료정보 및 의사 결정에 사용될 시스템 구조 및 기능, 내용, 저장장치, 보안 및 기밀성 보장과 정보 전달 등에 관한 표준 개발을 주목표로 하고 있으며, 특히 E31.25 WG의 경우, 'E31.25: Healthcare Data Management, Security, Confidentiality, and Privacy' 와 같이 환자 및 의료 식별, 의료 데이터에 대한 인증 및 인가, 보안 감사 등의 내용을 골자로 표준화를 추진 중이다. 다음은 해당 ASTM E31.25에서 개발한 주요 보안 표준 기술들이다.

- E1714-00, Standard Guide for Proper-ties of a Universal Healthcare Identifier (UHID)
- E1762-95(2003), Standard Guide for Electronic Authentication of Health Care Information
- E1869-04, Standard Guide for Confidentiality,

Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records
- E1985-98(2005), Standard Guide for User Authentication and Authorization
- E1986-98(2005), Standard Guide for In-formation Access Privileges to Health Information
- E1987-98, Standard Guide for Individual Rights Regarding Health Information
- E2084-00, Standard Specification for Authentication of Healthcare Information Using Digital Signature
- E2085-00a, Standard Guide on Security Framework for Healthcare Information
- E2086-00, Standard Guide for Internet and Intranet Healthcare Security
- E2147-01 Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems
- E2212-02a Standard Practice for Healthcare Certificate Policy

또한, ISO/TC215는 의료장비 간 데이터의 상호연계성 및 호환성 확보, 의료기록의 디지털화에 필요한 표준을 개발을 목표로 하는 의료정보기술위원회이며, 다음과 같이 8개의 WG이 활발히 활동 중에 있다. WG4에서 주로 논의하고 있는 보안 기술을 다음과 같이 분류할 수 있다[11].

〔표 3〕 ISO/TC215 WG4 의료 정보 보안 표준

▸ 공개키 기반 구조(PKI)
- ISO/DIS 17090-1/2/3 : Public key infrastructure-1/2/3
▸ 권한 관리 및 접근 제어 (PMAC)
- ISO/NP TS 22600-1/2/3 : Privilege management and access control : part 1/2/3 - ISO/CD TS 21298 : Functional and structural roles
▸ 보안 관리(Security Management)
- ISO/DIS 27799 : Security management in health using ISO/IEC 17799 - ISO/IEC 17799 Code of practice for information security Management(2005-revised version)
▸ 보안 아카이빙(Secure Archiving)
- ISO/WD 21547-1/2 : Security requirements for archiving and backup : part 1/2
▸ 익명화(Pseudonymisation)
- ISO/NP TS 25237 : Pseudonymisation
▸ 보안 감사(Audit Trail)
- ISO/27789 Audit tails for electronic health records
▸ 안전성 평가(Safety Assessment)
- ISO/DTR 27809 : Measures for Ensuring Patient Safety of Health Software - ISO/PRFTS 25238 : Classification of safety risks from health software
▸ 위험 관리(Risk Management)
- ISO/NP TS 29321 : Risk Management in manufacture domain - ISO/NP TR 29322 : Risk Management in user domain

3.3 u-헬스케어 의료 정보 보안 기술

본 절에서는 앞서 살펴본 u-헬스케어의 보안 요구사항을 반영하고 개인 건강/의료 정보에 대한 프라이버시 및 데이터 보호, 유무선 헬스케어 네트워크 보호 기술, 그리고 의료 정보 데이터의 안전한 공유 및 멀티 도메인 간 인증을 위한 대안 기술들을 보다 상세히 검토한다.

3.3.1 의료 정보의 프라이버시 보호 기술

개인정보보호 방법으로는 개인정보를 자신의 통제 영역 안에 포함시켜 개인정보의 유통을 개인이 관리하도록 하는 개인정보 자기통제권 확보 기술과 개인 정보를 전송 하고자 하는 대상자만이 해석할 수 있도록 암호화하는 방법 및 정보 활용 시 개인 정보를 통해 개인을 식별하지 못하도록 하는 익명화 방법을 들 수 있다.

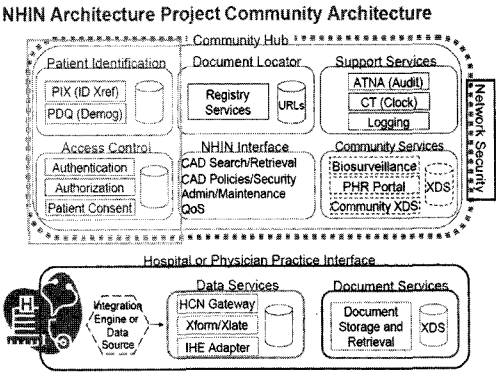
P3P는 웹사이트 접속 시 프라이버시를 보호하기 위해 국제 웹 표준화 기구인 W3C 권고안으로 2002년 승인되었으며 대표적인 개인정보 자기통제권 기술이다[11]. 이 기술은 사용자가 요구하는 정보보호 요구 수준에 부합하는 경우에만 해당 정보를 제공함으로써 사용자 스스로 본인의 정보를 관리하고 제공할 수 있도록 한다. P3P의 보다 상세한 동작방법은 다음과 같다. 즉 사용자 PC의 웹 브라우저에 설치된 에이전트가 자동으로 사용자의 개인정보 보호정책과 서비스 제공업체의

개인정보 사용정책을 비교해 약관 동의 여부 등을 결정하며, 이용하는 서비스 종류에 따라 개인정보 노출 수준을 조절할 수 있고, 자신의 정보가 서비스 제공자 또는 관련된 제3자에게 어떤 목적으로 사용되는지를 모니터링 할 수 있도록 도움을 준다. 프라이버시 보호의 적극적인 표현인 개인정보의 자기통제권 강화에 기여할 수 있는 장점을 P3P가 지니고 있음에도 불구하고, 웹 브라우저와 서버 간 통신 시 개인정보 노출 가능성이 존재하는 한편, 서비스 제공자가 개인정보 사용정책을 표현하기 매우 어렵다는 기술적인 문제를 안고 있는 것도 현실이다. 또한 이 기술을 의료 분야에서 사용하기 위해서는 금치산자나 한정치산자 등 자기통제권 행사가 불가능한 사람에 대한 대비책이 필요함은 물론이다. 하지만 P3P가 인터넷상의 불필요한 개인정보 노출을 막을 수 있는 방안 중 하나로 여겨져 왔으며, 이는 인터넷과 연동되는 의료분야의 개인정보보호에서도 유용하게 적용될 수 있을 것이다[16].

또한 프라이버시 보호를 위한 익명성 보장은 의료정보화에서의 가장 중요한 이슈중의 하나로서 와 같이 IHE에서 Liberty Alliance(이하 리버티 얼라이언스)와의 협조를 통해 구체화 시킨바 있다[12]. HE는 새로운 의료정보화 표준의 개발보다는 기존의 다양한 표준 간의 상호 호환성을 논의하기 위한 벤더들의 촉진기구로서 익명성 보장기술로 활용 가능한 ID-federation 기술을 의료분야에 적용하기 위해 리버티 얼라이언스와 협력관계를 맺고 이에 대한 활발한 논의를 진행 중이다. 이들이 추구하는 의료서비스에서의 구체적인 익명성 보장 기법은 다음 절에서 IHE의 데이터 공유(XDS)와 상호인증(XUA)을 통해 좀 더 자세히 설명하도록 한다[12][13][14].

3.3.2 유무선 헬스케어 네트워크 보호 기술

의료정보보호 기술은 타 정보보호 시스템 기술과 마찬가지로 독자적으로 존재하는 기술이 아니라 의료정보 시스템(또는 의료기기 제품)에 보안기술이 내재된 형태로 운용되고 있다. 또한 TCP/IP 기반의 인터넷 프로토콜이 의료장비에 필수적으로 지원되면서 기존의 네트워크 장비 회사는 네트워크 정보보호 솔루션을 의료분야 정보보호에 그대로 사용할 수 있을 것으로 판단되고 있다. 즉, 헬스케어 네트워크에 대한 보안 장비는 네트워크 장비(스위치나 라우터 등) 내장용 안티바이러스, 침입탐지, VPN 장비 및 보안 관리, 사용자 인증을 위한 AAA 장비, PoC 장비와 의료단말용 타블렛 PC 또는 PDA에 적용하기 위한 무선 보안 구간 인증 및 암호 툴 등으로 구성될 수 있다. [그림 4]는 대표적인 헬스케어 시스템 및 네트워크 보안 기술 구성 예를 나타낸다[17].



[그림 4] IBM 헬스케어 시스템 아키텍쳐

본 시스템 구성도에서 보는 바와 같이 헬스케어 시스템은 VPN이나 침입탐지 시스템 등의 네트워크 보안 장치뿐 아니라 데이터의 기밀성과 무결성, 사용자 인증 및 접근 제어와 같은 기본적인 보안 요구사항을 보장하기 위한 보안 서비스 모듈을 지원하도록 하고 있다.

대게 구체적인 보안 기술 및 보안 강도 등은 의료정보에 관한 관련 법률 준수 범위 내에서 각 의료 기관이 독자적으로 보안 정책을 수립하여 보안 서비스를 지원하도록 하고 있다. 앞서 살펴 본 HIPAA나 Canada Infoway[18] 등에서는 보안 위협 정도와, 비용적 합리성, 서비스 가용성 측면 등을 고려하여 강제 혹은 권고사항 수준의 법제도나 지침 등을 마련하여 의료 정보 서비스에 있어 사용자에게 일정 정도 이상의 정보 보호를 보장하도록 하고 있다.

3.3.3 의료 정보 데이터의 안전한 공유 및 멀티 도메인 간 인증

IHE-XDS에서는 의료 데이터의 공유를 동의한 의료 도메인(Clinical Affinity Domain) 간에 데이터 교환 상호호환성을 보장하고 데이터의 안전한 접근과 활용을 보장하기 위한 기술적 내용을 포함하고 있다[12][14][16]. IHE(Integrating the Healthcare Ente- rprise)에서 Liberty Alliance(이하 리버티 얼라이언스)와의 협조를 통해 구체화 시킨바 있다. IHE는 새로운 의료정보화 표준의 개발보다는 기존의 다양한 표준간의 상호 호환성

을 논의하기 위한 벤더들의 촉진기구이다. 교환할 환자/의료 데이터 식별 방법과 메타 데이터 문서 구조 및 포맷, 인코딩/디코딩 규칙 등에 관한 내용 뿐 아니라 데이터에 대한 접근 통제, 보안 감사 방법 등의 보안 기술도 포함하고 있다. IHE-XDS를 통해 추구하는 보안 모델 요소는 다음과 같다.

- Risk Assessment: 해당 정보 자산(Asset)은 환자/건강 정보를 저장하고 있는 레지스트리나 레파지토리로서 데이터에 대한 기밀성, 무결성, 가용성 보장을 기본으로 한다. 또한, 정보 제공의 원칙에 있어 언제나 환자의 안전(Patient Safety)이 개인 프라이버시보다 우선하도록 한다.
- Accountability: 정보 접근 및 사용에 대한 권한을 확인하고 책임을 부여하기 위하여 정보 요청자를 식별, 접근 제어를 수행하고 정보에 관련된 이벤트에 대하여 반드시 로그를 남겨 보안 감사를 수행해야 한다.
- Policy Enforcement: 정보 공유를 협의한 도메인 간에는 반드시 상호 식별이나 인증, 접근 제어 정책, 보안 감사 레벨 등의 보안 정책에 대한 설정과 시행의 동의가 이루어져야 한다.

u-헬스케어 환경에서 IHE-XDS를 이용한 정보공유 방법은 다음과 같다. 클리닉 센터 및 중대형 병원 내의 XDS Document Repository 간에 건강 정보 요청 및 접근이 수행 될 경우, 각 Repository는 IHE-XDS 모델에서 지원하는 DSIG, CT, ATNA[15] 등을 이용하여 건강 정보 요청자의 식별, 접근 제어, 교환 데이터의 기밀성과 무결성 보장, 발생하는 정보 이벤트에 대한 보안 감사 등을 지원함으로써 안전한 건강 정보 공유를 보장할 수 있다. 그 밖에 접근제어를 위한 RBAC이나 PMAC 등의 응용 레벨에서의 접근 제어 정책에 대한 정의를 추가적으로 할 수 있다.

또한, IHE-XUA는 멀티 도메인 간 사용자 인증을 지원하기 위한 통합 프로파일로서 도메인 간 교환되는 트랜잭션에 대해 사용자 (XDS Actor) ID를 부여하고 접근 제어를 수행하기 위해 요구되는 인증 및 속성 정보, 보안 감사 속성 정보 등을 포함하고 있다[12][13][16]. 다중 도메인 간 교환되는 트랜젝션에 대해 책임(Accountability)를 부여하기 위하여 피 요청기관이 접근 결정과 보안 감사를 수행하는 데 사용 가능한 방법으로 요청자를 식별할 수 있어야 한다. 그러나 도메인 간 서로 다른 인증 방법과 사용자 정보 디렉토리를 사용하고 있으므로 인증 방법의 협상, 상호 호환 가능한 인증 및 속성 정보 교환 방법 등이 요구된다. 유비쿼터스 서비스 패러다임에 대한 인식의 확산으로 원격 의료 진단 서비스 수준에 머물러 있는 u-헬스케어 서비스의 고도화 및 다양화를 위해 관계 서비스 기관간의 정보 공유와 연계가 점차 확대될 것이다. 따라서 향후, IHE의 멀티 도메인 간 전자 건강 데이터의 안전한 공유 기술들은 더욱 유용하게 적용될 수 있을 것이다.

Ⅳ. 결론 및 시사점

u-헬스케어 서비스는 타 유비쿼터스 컴퓨팅 기술 분야에 비해 다루어지는 정보 속성이 매우 민감하고 이질적인 서비스 도메인 간 혹은 다양한서비스 관계자 간 정보 공유가 빈번하게 이루어질 수 있다는 점에서 심각한 보안 우려사항이 존재한다. u-헬스케어 분야에서 다루는 정보는 주로 건강이나 생명과 밀접한 관계가 있는 관련 정보로서 극히 개인적인 사항을 주로 포함한다. 이와 같은 특성을 반영하여 현재 u-헬스케어 서비스에서는 네트워크를 통한 데이터 공유 환경에서 데이터 처리 및 공유 등에 관한 상호호환성 보장, 표준화, 프라이버시 보호 및 데이터 보호 등이 난제로 거론되고 있다. 이를 위하여 사용자에 대한 안전한 의료서비스를 제공하기 위한 관련 법제도와 보안 표준 기술이 국내외적으로 개발 및 이행 중이며 데이터 보호 및 프라이버시 보호, 안전한 데이터 공유를 위한 구체적 기술 요구사항들에 대한 개발, 검토가 활발히 이루어지고 있다.

헬스케어에서의 정보보호 문제는 시스템 설계 단계에서부터 충분히 고려되어 적용되지 않는다면 그 편리성에도 불구하고 u-헬스케어 서비스 자체의 활성화를 저해할 것이다. 따라서 이러한 정보보호 우려를 해소하기 위해서는 컴퓨팅 환경의 변화에 맞춰 현재의 법제도 및 기술에 있어 지속적인 보완이 필요할 것이다.

약어정리

BAN	Body Area Network
PACS	Picture Archiving Communication System
OCS	Order Communication System
EHR	Electronic Health Record

EMR	Electronic Medical Record
HIPAA	Health Insurance Portability and Accountability Act
HIT	Health Information Technology
MCC	Medical Care Continuity
IDC	International Data Corporation
IHE	Integration of Healthcare Enterprise
P3P	Platform for Privacy Preferences Project
W3C	World Wide Web Consortium
SIG	Special Interest Group
XDS	Cross-Enterprise Domain Sharing
AAA	Authentication, Authorization and Accounting
XUA	Cross-Enterprise User Authentication
PoC	Point of Care
DSIG	Digital Signature Content Profile
CT	Consistent Time
ATNA	Audit Trail and Authentication
RBAC	Role Based Access Control
PMAC	Privilege Management and Access Control

참고문헌

〔1〕 University of Rochester, "Letting the home interface with the healthcare system: New paradigms for con-sumers and providers," Though Leader's workshop white paper, 2004

〔2〕 MobiHealth 프로젝트 http://www.mobihealth.org

〔3〕 EU MCC 프로젝트 홈페이지 http://www.eten-mcc.org/

〔4〕 한국전산원, "의료정보화의 현황 및 과제," 2005

〔5〕 Wimalasiri, J.S.; Ray, P.; Wilson, C.S., "Maintaining Security in an Ontology Driven Multi-Agent System for Electronic Health Records" Enterprise Networking and Computing in Healthcare Industry, 2004. HEALTHCOM 2004. Proceedings. 6th International Workshop on 28-29 June 2004

〔6〕 CMS, "HIPAA Security series: Security Standards, Technical Safeguards," 2005

〔7〕 HIPAA, "Summary of the HIPAA Privacy Rule," http://www.hhs.gov/ocr/hipaa/privrulepd. pdf

〔8〕 박건희, "보건의료정보화와 개인정보보호," 서울대의대 2006년 상반기 토픽 리뷰, 2006.6.

〔9〕 ASTM 표준기구, http://astm.org

〔10〕 CCHIT, http://www.cchit.org/

〔11〕 ISO/TC215 표준기구, http://www.iso.org/

〔12〕 HIMSS, http://www.himss.org/

〔13〕 IHE, "IHE IT Infrastructure Technical Framework : Cross-Enterprise User Authentication(XUA) Integration Profile," White Paper, 2006

〔14〕 ITI Technical Committee, "IHE Security-XDS as a case study," IHE, 2006

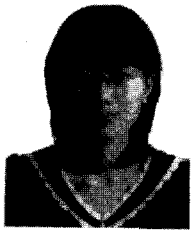
〔15〕 Robert Horn, "Audit Trail and Node Authentication / Consistent Time," IHE, 2005

〔16〕 송지은, 김신효 외, "홈-헬스케어 서비스의 정보보호 소고," 정보보호학회지, 2006

〔17〕 IBM Healthcare Solution, http://www-03.ibm.com/industries/healthcare/index.jsp

〔18〕 Canada Health Infoway, http://www.infoway-inforoute.ca

〈著者紹介〉



송 지 은 (Ji-eun Song)
2002년 2월 : 전북대학교 컴퓨터과학과 (이학사)
2004년 2월 : 전북대학교 컴퓨터정보학과 (공학석사)
2004년~현재 : 전자통신연구원 의료정보융합연구팀
관심분야 : 무선 인터넷 보안, RFID/Sensor 네트워크, 프라이버시 보호, 의료정보보호

김 신 효 (Shin-hyo Kim)
1990년 2월 : 전남대학교 전산학과 (이학사)
2000년 2월 : 충남대학교 컴퓨터과학과(이학석사)
1990년~현재 : 전자통신연구원 의료정보융합연구팀 선임연구원
관심분야 : 무선LAN 정보보호, AAA보안, DRM, 프라이버시 보호

정 명 애(Myung-Ae Chung)
1986년 2월 : 이화여자대학교 화학과 (이학사)
1988년 2월 : 이화여자대학교 화학과 (이학석사)
1997년 Clausthal 공대 물리학연구소 (공학박사)
1997년~1998년 : Clauthal 공대 물리학 연구소 (Post-Doc)
1998~1999년 : Max-Planck 고분자연구소 Prof. W Knoll 그룹 근무
2000년~현재 : 전자통신연구원 IT융합서비스부문 의료정보융합연구팀 팀장
관심분야 : 나노 바이오 센서, 뉴런 칩, u-헬스케어, 의료정보보안