u-헬스케어 보안 이슈 및 기술 동향

Security Issues and Its Technology Trends in u-Healthcare

u-IT839의 정보보호 이슈 특집

송지은 (J.E. Song) 의료정보보호연구팀 연구원
김신효 (S.H. Kim) 의료정보보호연구팀 선임연구원
정명애 (M.A. Chung) 의료정보보호연구팀 팀장
정교일 (K.I. Chung) 정보보호기반그룹 그룹장

목 차

평균 수명 연장과 건강한 삶을 오래 유지하고자 하는 안락한 삶에 대한 욕구는 필연적으로 고도화된 의료 서비스 발전을 야기시켰다. 아울러 유비쿼터스 컴퓨팅 기술의 발전과 IT-BT-NT를 포함한 기술간 컨버전스 경향은 유비쿼터스 헬스케어(이하 u-헬스케어)의 실현을 가속화하고 있다. u-헬스케어 서비스가 고도화될수록 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 측면에서 다양한 취약점과 위협이 존재할 수 있다. 따라서 본 고에서는 u-헬스케어의 특성에 근거한 보안 이슈 및 요구사항을 분석하고 이와 관련한 합리적인 기술적 대안들을 검토해 본다.

Ⅰ. 서론

유비쿼터스 컴퓨팅 환경의 특징은 이질적 기술간 융합, 정보의 개방성 및 공유성, 사용자 지향의 서비스 확대 등을 들 수 있다. 특히, u-헬스케어는 건강하고 윤택한 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, 의료 데이터의 교환 및 처리를 위한 표준 기술 등이 뒷받침되면서 구체적인 서비스 실체화가 가속화되고 있다. u-헬스케어 서비스는 BINT 기술의 융합을 도모할 뿐 아니라 보다 정확하고 다양한 의료 서비스를 제공하기 위해 관련 기관 및 사용자간 의료 데이터의 교환과 공유를 필요로 한다. 뿐만 아니라 진료 서비스에 관하여 병원 종속적 패러다임을 탈피하고 능동적이고 자주적인 건강 관리를 위한 사용자 욕구가 증대되면서 관련 응용 서비스 또한 증대될 것이다. 실제 IDC의 2006년 IT 세계 시장 전망 자료에서도 향후 5년간 가장 높은 성장률을 보일 IT 분야로 통신/미디어와 함께 헬스케어 분야를 선정하였다[1].

반면, u-헬스케어 서비스는 타 유비쿼터스 컴퓨팅 기술 분야에 비해 다루어지는 정보 속성이 매우 민감하고 이질적인 서비스 도메인 간 혹은 다양한 서비스 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. 따라서 이와 같은 정보가 불법적으로 노출 및 조작, 악용될 경우 개인 프라이버시 침해 및 안전하고 정확한 의료 서비스 위협 등을 초래할 수 있다. 이와 관련하여 최근 온라인상에서 개인 신상 정보 도용이나 매매 등으로 인해 피해 사례가 급증하고 있고 정부차원에서 이를 범죄 행위로 간주, 법적 제재 조치를 취한 사례는 프라이버시 보호의 중요성을 잘 나타내주는 예이다. 또한, 최근 미국에서 발생한 의료정보에 대한 해킹 및 악용 사례는 사회적으로 큰 반향을 일으켰을 뿐 아니라 의료정보보안에 대한 필요성을 사회적으로 재고시키는 계기가 되었다. 따라서 u-헬스케어 서비스의 지속적인 발전과 안정화를 위해서는 정보보호 이슈에 대한 고찰과 기술적 대안의 모색이 요구된다.

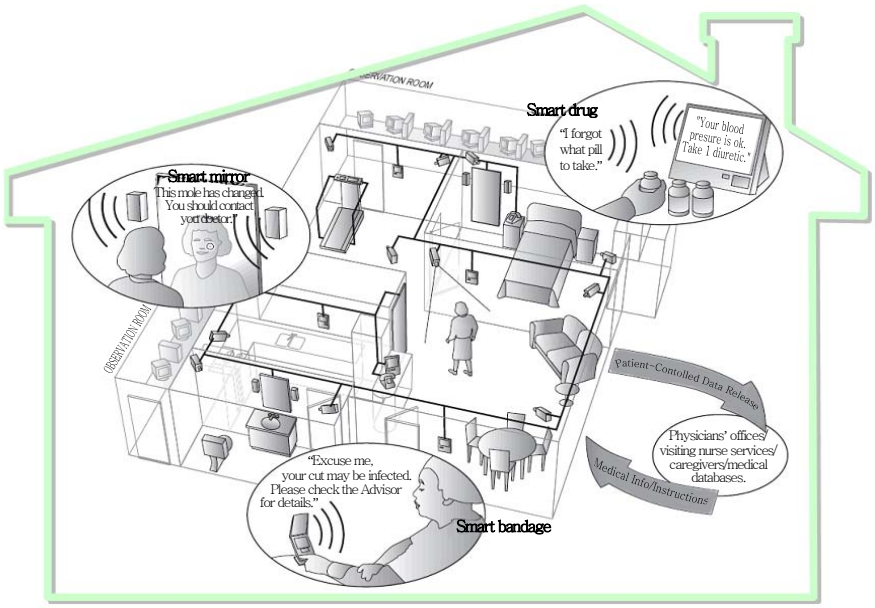
이와 관련하여 본 고에서는 u-헬스케어 서비스의 프라이버시 및 데이터 보호 등에 관련한 보안 이슈를 중점적으로 논하고 안전한 u-헬스케어 서비스를 보장하기 위해 지원 가능한 기술적 방안들에 대해 기술한다.

Ⅱ. u-헬스케어 서비스

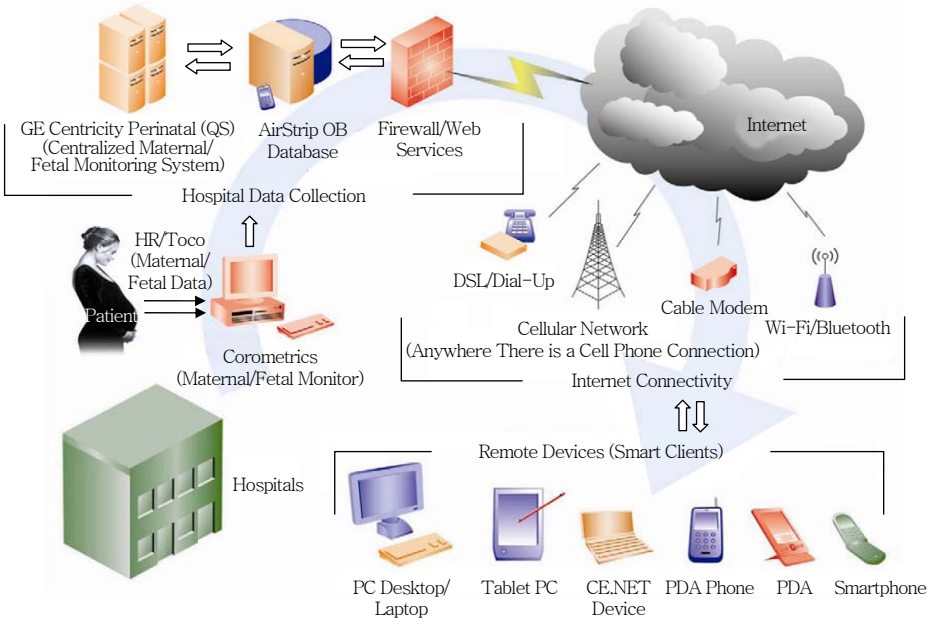
언제 어디서나 서비스 이용이 가능한 유비쿼터스 기술의 등장으로 병원이 아닌 환자의 집, 사무실 또는 이동중에도 의료서비스를 받을 수 있는 u-헬스케어 서비스의 기술 연구가 활발히 진행되고 있다. 즉, u-헬스케어 서비스는 모바일 의료서비스의 진화된 모델로서 공간적, 시간적 제약을 없애고 환자가 생활 공간 속에서 다양한 의료 센서 및 기기를 통해 수집된 생체 정보와 환경 정보를 기반으로 중앙의 원격 의료 서비스 시스템을 통해 언제 어디서나 의료 피드백을 받을 수 있는 서비스를 총칭한다. 이러한 u-헬스케어 서비스의 대표적인 예로는 로체스터 대학의 미래 스마트 메디컬 홈 프로젝트가 있다[2].

스마트 메디컬 홈 프로젝트는 스마트 의료 센서부, 수집된 각종 생체 신호의 분석부, 지속적인 건강 상태 모니터링 및 데이터 축적부, 응용 서비스를 위한 정보 교환 인터페이스 및 사설 방화벽 등으로 구성된다. 이와 같은 프레임워크를 기반으로 (그림 1)과 같이 댁내에서 피부암 등의 피부상태를 상시 체크할 수 있는 smart mirror, 상처의 병원체 감염유무를 상시 감시·보고하는 smart bandage, 복용 약에 대한 정보와 복용 유무를 알려주는 smart drug 등의 서비스를 개발하였다.

GE 헬스케어는 (그림 2)와 같이 의료용 단말과 병원 내 데이터베이스를 이용하여 원격지에서 임산



(그림 1) 스마트 메디컬 홈 서비스[2]



(그림 2) GE사 u-헬스케어 서비스 구성도[3]

부의 상태(태아의 심장박동, 산모의 자궁 수축도 등)를 살피고 원격지에서도 충분히 진찰할 수 있는 시스템을 자사의 통합 의료정보시스템과 연동이 가능하게 함으로써[3], u-헬스케어 시대가 먼 미래의 희망사항이 아니라 가까운 장래에 실현될 기술임을 보여주고 있다.

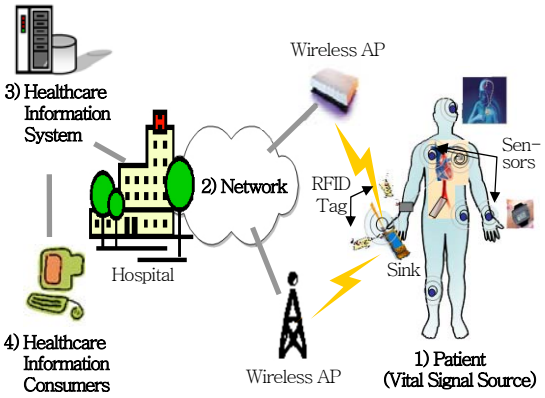
이 외에, EU 및 미국, 일본 등에서도 u-헬스케어 비즈니스 프로젝트가 활발히 진행되고 있다. EU의 MobiHealth (Mobile Healthcare) 프로젝트는 고위험도의 임산부, 만성 질환자, 심장 질환자 등을 대상

〈표 1〉 헬스케어 관련 정부 출자 사업 현황

정보통신부	• 홈네트워크 산업에 포함하여 e-Health 산업을 육성 - 2004년 추진한 홈네트워크 시범사업에 SK 텔레콤 컨소시엄과 KT 컨소시엄이 사이버 아파트를 중심으로 원격진료가 가능한 미래형 홈네트워크 서비스를 시행
산업자원부	• 스마트홈 부문의 헬스케어 품목, 전자의료기기분야, 실버의료기기, 영상진단기기, 모바일헬스케어 등을 육성
보건복지부	• 보건의료분야, 보건산업분야, 사회복지분야, 사회보험분야의 정보화 추진 - 2005년 총 22개 정보화 과제에 646억 원의 예산 투입 - e-헬스케어와 전체 병원간 진료정보 공유를 위한 전자 건강기록사업(EHR) 등을 추진중

으로 일상 생활 속에서 지속적인 환자 모니터링을 통해 질병 판단 및 예측, 응급상황 대처 등의 서비스를 제공하는 플랫폼과 비즈니스 모델에 관한 연구를 진행하고 있다[4]. 또한 암, 신생 질병의 집중 치료를 받은 후, 댁내에서 원격 모니터링 및 진단 서비스를 받는 지속적인 의료 케어(MCC) 프로젝트[5]와 RFID를 응용하여 환자의 이동, 현 위치, 이상 징후 등의 데이터를 실시간으로 의료 기기에 전송하는 RFID 센서 응용 프로젝트 등도 활발히 진행중이다. 실제 우리나라도 정부적 차원에서 적극적으로 헬스케어 사업을 육성하고 있는 가운데 의료정보 업체나 대기업 간에 다양한 u-헬스케어 서비스 모델 개발과 특허 출원 등의 경쟁이 심화된 상태이다. <표 1>은 헬스케어 산업과 관련한 정부 출자 사업 현황을 도시하고 있다[6].

u-헬스케어는 다양한 기술들이 집약 및 융합된 서비스 기술로서 (그림 3)과 같이 생체 및 환경 정보를 센싱, 모니터링 하기 위한 의료 센서나 기기, 센서 간 통신 및 데이터 송수신을 위한 유무선 네트워크, 생체 데이터 분석과 건강 피드백을 담당하는 의료 정보 서버, 그리고 생성된 의료 정보를 소비하는 다양한 정보 소비자 집단, 즉 환자나 의료진 및 관련 응용 서비스 등으로 구성될 수 있다. 환자 이식형 혹은 이동형 센서는 환자 식별 정보를 포함하여 혈당, 당뇨, 심박 수, 동작 탐지 등에 관한 생체 정보를 측정하고 필요에 따라 주변 환경 정보 등을 감지하여



(그림 3) u-헬스케어 서비스 구성 요소

동기식 혹은 비동기적인 방법으로 유무선 네트워크를 통해 건강 정보 서버에 전송한다. 이 때, 무선 의료 기기 및 센서 간에는 Zigbee나 UWB 방식의 센서 통신 프로토콜이 사용될 수 있으며 WLAN이나 3GPP, 이더넷 등을 포함한 유무선 인터넷을 통해 수집된 데이터들이 전송된다. 건강 정보 시스템에 수집 및 축적된 데이터로부터 건강상태, 생활패턴 등에 관한 건강 자료(wellness index)를 분석하고 이와 관련된 경고(alarm), 현장진단처방(PoC), 단순 주지 등의 피드백(feedback)이 응용서비스의 한 형태로 사용자에게 전송된다. 이 외에도 u-헬스케어 정보에 대한 다양한 소비자와 서비스 형태가 존재함에 따라 정보 권한이나 서비스 효율성, 경제적 이득 관점에서 조정 및 타협이 필요한 이해 당사자(stakeholder)들이 존재할 수 있다[7].

이와 같이 u-헬스케어는 개인의 생체 정보 및 주변환경에 관한 모니터링 정보 등 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 충분한 보안 이슈 검토와 합리적인 기술적 대안의 강구가 이루어져야 한다.

Ⅲ. u-헬스케어 보안 이슈

미국의 경우 2003년 4월 HIPAA의 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[8],[9]. HIPAA의 적용을 기점으로 하여, 적어도 미국에서 개발 운용되는 모든 의료정보 관련 솔루션에 보안기능이 필수적으로 추가되어야 한다. 뿐만 아니라 최근 개인정보의 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 강구하고 있다[10]. u-헬스케어 환경에서는 (그림 4)와 같이 다양한 보안 취약점과 위협 요소들이 존재한다. 유무선 네트워크 기반 서비스에서 발생 가능한 보안상 취약점 및 공격이 u-헬스케어 환경에서도 유사하게 전이되는 형태를 보인다. 따라서, 기반 네트워크 및 시스템에 대한 안전성, 신뢰성 보장 및 데이터 보호를 위한 기술적 대안이 기본적으로 요구된다.

한편, u-헬스케어 서비스는 다음과 같이 기존 유비쿼터스 컴퓨팅 서비스와는 다른 보안 요구사항들이 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. 즉 개인 정보가 여러 기관들에 의해 공유되어야 하며 정확한 진료를 위해서는 정보 공유가 필수적이다. 그러나 개인의 입장에서는 이러한 개인 정보가 타당한 대상자에 의해 의료 서비스 목적에 맞게 최소한의 공유만 이루어지기를 기대할 것이다. 반면, 현 의료 정보 보안 정책 및 기술로는 정보 공유의 대상과 그 범위를 명확하게 파악하거나 결정할 수 없다는 큰 문제를 안고 있다. 따라서 의료 정보에 대한 프라이버시 보호적 차원에서의 개인 의료 정보권한 관리 및 위임, 활용에 관한 기술적, 법제도적 지원책이 요구된다[11]. 또한, 불법적인 의료 정보 열람과 이용을 막고 그 책임 소재를 판단하기 위하여 보안 감사 체계가 보완되어야 한다. 현재, 대부분의 병원에서는 요청자의 단순 서비스 요청에 관한 로그만 남길 뿐, 데이터 습득 이후 활용, 폐기 등에 관한 의무사항 준수에 관련한 감사 체계가 부재한 상황이다. 이는 최근 심각한 보안 취약점으로 거론되고 있는 내부자에 의한 정보 유출의 위험성을 가중시킬 수 있다.

(그림 4) u-헬스케어 환경의 보안 위협

또한, 보다 향상된 수준의 의료 서비스와 개인의 의료 건강 정보에 대한 접근성을 용이하게 하기 위하여 향후 이질적인 병원 정보 서버간 환자에 대한 건강 정보 공유가 빈번하게 이루어질 것이다. 실제로, 현재 보건 복지부에서는 국내 EHR 정보 교류 시스템 모델로서, 국립 보건소 및 국립 병원의 데이터에 대해서는 정부에서 중앙 집중적으로 통합 관리하고 일반 사설 병원에서 보유하고 있는 환자 정보에 대해서는 환자의 요청에 따라 서로 공유 및 활용 가능하도록 하는 분산/집중 혼합형 정보 시스템 모델을 검토하고 있다. 이와 같이 이질적 의료 도메인 간 개인의 건강/의료 정보를 교환 시, 인증된 도메인 간에 안전하게 가용한 정보만을 송수신하도록 지원할 수 있는 보안 기술이 필요하다. 즉, 이질적인 인증 방식에 대한 인증 서비스 독립성을 보장하고 도메인 간에 교환 및 공유되는 트랜잭션에 대해 책임(accountability)을 부여하기 위한 기술이 필요하다.

뿐만 아니라, u-헬스케어 환경이 되면서 종래의 ID/PWD나 공인 인증서 기반뿐 아니라, 다양한 생체 식별 정보가 사용자 인증 방식으로 활용될 것이다. 생체 인식/인증에 사용되는 유일무이(唯一無二) 생체 정보는 그 정보의 변경이 쉽지 않아 생체정보의 노출로 더 이상 사용이 불가능한 경우에 대한 대비책이 있어야 하며, 신체 손상으로 생체정보의 제공이 불가능한 경우에 대한 대체 수단의 제공 방법이 마련되어야 한다. 특히, 사용자 식별과 관련하여 지금까지 널리 쓰여왔던 주민등록번호는 그 생성 특성상 번호만으로도 개인 정보 노출이 쉽고 주민번호 생성 및 유출 또한 용이하며, 중복된 번호 존재 등으로 국가적으로도 온라인 상거래나 전자정부 행정업무에서도 사용을 지양하고 있다. 그러나 현재 병원 시스템은 환자 정보를 생성, 검색, 활용하기 위한 키로서 여전히 주민등록번호나 주민등록번호와 단순 매핑된 환자번호가 쓰이고 있다. 또한, 병원마다 서로 다른 환자 식별 체계가 사용되고 있어 환자는 다양한 형태, 다수의 ID 정보를 기억 및 관리해야 하는 불편함을 감수하고 있다. 향후, 병원간 건강/의료 정보 공유 시, 환자를 포함한 인가 받은 정보 소비 주체들이 불필요한 개인 정보 노출 없이 익명성을 보장 받으면서도 정상적으로 인증 및 식별 가능하며, 소수의 ID 계정으로 의료 서비스 이용이 가능하도록 할 수 있는 통합된 ID 관리 체계가 필요하다. 통합된 ID 관리 시스템의 구축 범위는 정책에 따라 협소하게는 모(母) 병원과 관련 협업 병원 간 구축할 수 있으며, 국가적으로 국내 모든 병원의 환자를 인증 및 관리하는 국가 통합형 ID 관리 시스템 모델이 존재할 수 있다.

마지막으로, u-헬스케어 서비스는 타 유비쿼터스 컴퓨팅 서비스에 비해 환자의 생명 및 안전에 매우 민감한 영향을 미칠 수 있다. 따라서, u-헬스케어 서비스를 구성하는 시스템 및 응용 서비스에 대한 안전성 평가는 매우 중요한 작업이다. 이는 하드웨어 장비뿐 아니라 소프트웨어 솔루션과 관리적 측면의 정책도 포함한다. 현재, 일반적인 네트워크나 컴퓨터 장비에 대한 보안 등급 평가 기준은 존재하나, 의료 시스템의 특성을 반영한 의료 시스템의 보안 관리 기준은 부재한 상황이다. 따라서 환자의 건강 상태 및 생명 위협 영향을 기준으로 재검토된 의료 시스템의 안전성 및 보안 평가 기준이 새롭게 마련되어야 한다.

u-헬스케어 서비스 구축을 위하여 국내외적으로 정보 공유를 위한 상호호환성 보장을 포함한 보안 및 프라이버시 이슈가 가장 중요한 현안으로 고려되고 있다. 이와 같은 보안 기술적 요구사항들은 유비쿼터스 컴퓨팅 기술을 활용한 u-헬스케어 시스템의 초기 설계시 동시에 반영되어야 한다.

Ⅳ. u-헬스케어 보안 기술

앞서 살펴본 u-헬스케어의 보안 요구사항을 반영하고 개인 건강/의료 정보에 대한 프라이버시 및 데이터 보호, 안전한 정보 공유, 도메인간 인증 및 ID 관리, 헬스케어 시스템의 보안 관리 등을 위한 대안 기술들을 보다 상세히 검토한다.

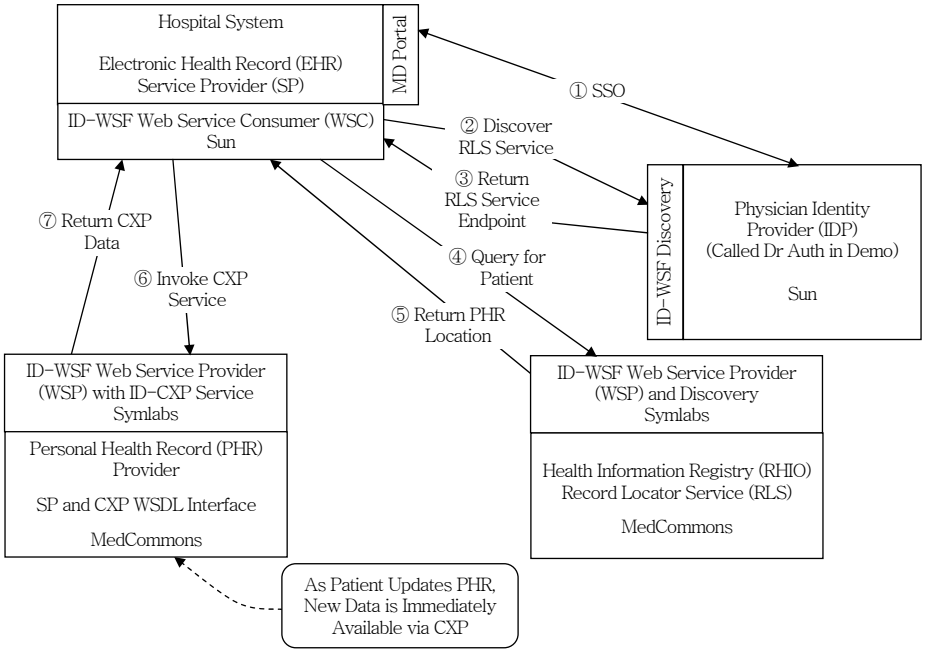
1. 건강/의료 정보에 대한 프라이버시 보호 기술

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

P3P는 웹사이트 접속시 프라이버시를 보호하기 위해 국제 웹 표준화 기구인 W3C 권고안으로 2002년 승인되었으며 대표적인 개인정보 자기통제권 기술이다[12]. 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 서버간 통신시 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.

또한 익명성 보장은 의료정보화에서의 가장 중요한 이슈 중의 하나로서 IHE에서 Liberty Alliance (이하 리버티 얼라이언스)와의 협조를 통해 구체화 시킨 바 있다[13].



(그림 5) Liberty Alliance e-Healthcare SIG[12]

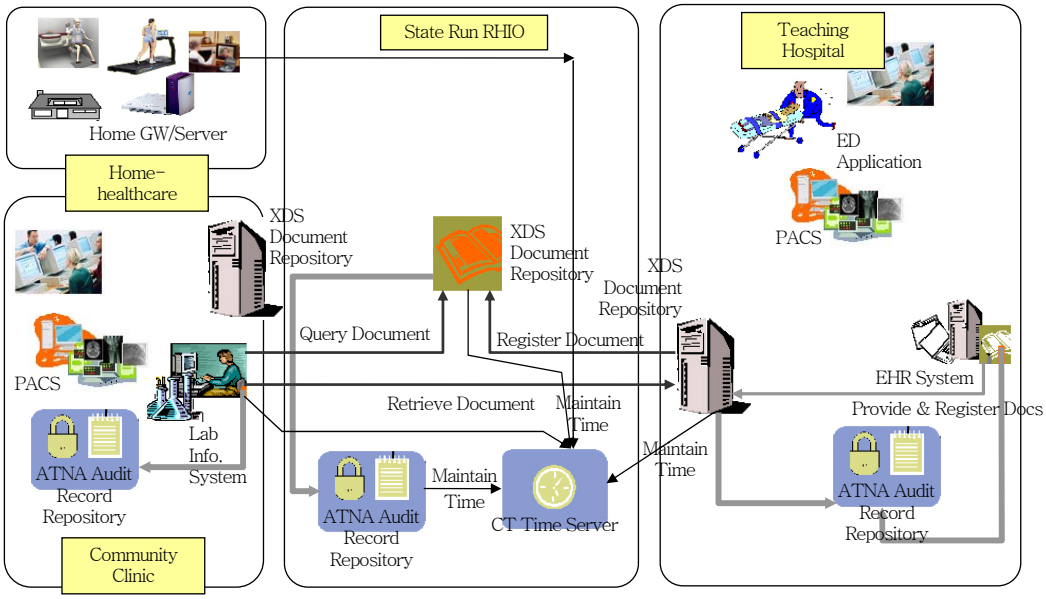
IHE는 최근 익명성 보장 기술로 활용 가능한 Federation-ID 기술을 의료분야에 적용하기 위해 리버티 얼라이언스와 협력관계를 맺고 이에 대한 활발한 논의를 진행중이다. 리버티 얼라이언스는 (그림 5)와 같이 e-Health SIG를 구성하여 활발히 활동중이다. 이들이 추구하는 의료서비스에서의 구체적인 익명성 보장 기법은 다음 절에서 IHE의 데이터 공유(XDS)와 상호인증(XUA)을 통해 좀 더 자세히 설명하도록 한다[13]-[15].

2. 전자 의무 기록의 안전한 교환 및 공유 기술

IHE-XDS에서는 의료 데이터의 공유를 동의한 의료 도메인(clinical affinity domain) 간에 데이터 교환 상호호환성을 보장하고 데이터의 안전한 접근 및 활용을 보장하기 위한 기술적 내용을 포함하고 있다[13],[15]. 따라서 교환할 환자/의료 데이터 식별 방법과 메타 데이터 문서 구조 및 포맷, 인코딩/디코딩 규칙 등에 관한 내용뿐 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 registry나 repository로서 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 정보 공유 방법은 (그림 6)과 같다. 클리닉 센터 및 중대형 병원 내의 XDS document repository 간에 건강 정보 요청 및 접근이 수행될 경우, 각 repository는 IHE-XDS 모델에서 지원하는 DSIG, CT, ATNA



<자료>: ITI Technical Committee, "IHE Security-XDS as a Case Study," Aug. 2006.

(그림 6) u-헬스케어 환경에서의 IHE-XDS

[16] 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.

3. 멀티 도메인 간 인증 및 ID 관리 기술

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[13], [14]. 다중 도메인 간 교환되는 트랜잭션에 대해 책임(accountability)을 부여하기 위해 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. IHE-XUA는 다음과 같은 국제 표준을 이용 및 확장하여 이와 같은 문제를 해결하고 있다.

- SAML 2.0 Profiles
- SAML Browser SSO Profiles
- Enhanced Client/Proxy Profiles
- SAML Profile with XDS
- Extended SAML 2.0 Profiles into HL7

뿐만 아니라, SAML 2.0을 기반으로 Federation-ID를 지원함으로써 협력관계를 맺은 관련 서비스 기관 간 웹 SSO 및 single logout을 지원할 수 있으며, 중복 ID 제거와 ID 도용 및 유출 관리 등과 같은 ID 관리 체계 방법도 지원 가능하다. 리버티 얼라이언스에서도 HIPAA 규약에 호환 가능한 적절한 인증 방법으로서 Federation-ID 기술을 이용한 인증 방법을 구체적 대안으로서 제시하고 있다. u-헬스케어 시스템에서 Federation-ID 기술 도입을 할 경우,

〈표 2〉 u-헬스케어의 Federation-ID 기술 효과

장점	구체적 예
보안	• 사용자 인증 • 다중 접근 제어 레벨 설정 가능
HIPAA 호환	• 인증 레벨 설정 지원 • 데이터 접근에 대한 상세 보안 감사 지원
운영 효과 개선	• 싱글 사인 온-중복 ID 관리 방지 • 애플리케이션에 따른 구별된 UserID 관리 • 새로운 구성원 추가 및 확장성 용이
비용 절감	• ID 관리자를 위한 운영관리자 지원 • 개발 시간 감소 • 표준 준수 개발-상이한 인터페이스에 대한 중복 개발 낭비 방지
상호 호환성	• 기존 시스템간 통합 지원 • 새로운 시스템 구축 및 통합 용이

<표 2>와 같은 효용성을 얻을 수 있을 것이다.

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.

4. 헬스케어 시스템 위험 평가 및 보안 관리 기술

헬스케어 시스템의 오류 및 결함, 사용 부주의 등으로 인한 의료 사고 등으로부터 환자의 건강 및 생명에 대한 악영향을 최소화하기 위하여 헬스케어 시스템에 대한 안전성 평가 및 위험 관리 기술이 요구된다. 현재, ISO/TC215 WG4에서는 ISO 27809 - Measures for ensuring patient safety of health software, ISO 25238 - Classification of safety risks form health software, ISO 29321-Application of risk management to the manufacture of health software 등의 표준 기술을 활발히 개발 중이다[17]. 특히, ISO 27809의 경우 현재 기술표준 ballot 단계로서 의료 시스템으로 인한 환자 위협의 치명성(영향 정도) 및 영향 받는 환자 규모 등을 기준으로 위협도를 분류한 후, 각 위협의 발생 가능

한 빈도수를 반영하여 시스템의 위험등급을 A부터 E까지 분류하는 체계를 띄고 있다. 또한, ISO 29321에서는 헬스케어 시스템의 위험 평가 결과에 따라 시스템 접근 권한 관리 및 발생 가능한 사고 대응 등에 관련한 보안 관리 기술을 활발히 개발중이다.

V. 결론 및 시사점

u-헬스케어 서비스 환경에서는 다양한 의료 센서 및 기기의 이용과 건강 정보에 대한 연계 및 공유로 인하여 개인의 생체 정보, 헬스케어 서비스 정보, 행동특성, 생활습관 등 개인에 관한 방대한 정보수집이 가능해질 수 있다. 이는 개인의 사생활 침해를 초래할 수 있을 뿐 아니라 서비스 과정에서 정보가 왜곡 및 악의적으로 이용될 경우, 신뢰성 있고 정확한 헬스케어 서비스가 불가능해진다. 이와 같은 특성을 반영하여 현재 u-헬스케어 서비스에서는 프라이버시 보호와 멀티 도메인 간 안전한 정보 공유 및 인증 방법이 가장 큰 난제로 거론되고 있다. 이를 위하여 사용자의 자기 건강 정보에 대한 권한 관리를 제도적, 기술적으로 지원하고 내부자나 서비스기관에 의한 정보 남용을 막기 위하여 보안 감사 체계를 강화하고 있으며 개인 식별 ID에 관하여 익명성을 보장하는 방법과 편리성과 안전성의 균형을 이루는 합리적 수준의 접근제어 방법에 관한 기술 개발과 검토가 활발히 이루어지고 있다. 또한 최근 시스템의 안전성에 대한 평가 및 보안 관리 또한 시스템으로 인한 의료 사고를 미연에 방지, 피해를 최소화하기 위한 대안으로서 주목 받고 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.

● 용 어 해 설 ●

HIPAA: 미국의 건강 보험 이전 가능성 및 책임에 관한 법률로서 전자적 의료 정보의 보안 및 개인 의료 정보보호를 위한 엄격한 규정을 포함하고 있다. 일반적, 관리적, 물리적, 기술적 보안 규칙을 포함한 6개의 섹션으로 구성되며 각 섹션은 관련 기술 표준과 구현 스펙으로 구성되어 있다.

IHE: IHE는 의료정보 표준화 실현을 위한 촉진 기구로서 기존 산업 표준들을 준수하면서 의료정보 시스템 및 의료 기기 간 통신과 정보 공유에 있어 상호호환성을 보장하는 데 그 목적이 있으며, 이와 관련하여 기존 표준 기술의 검토 및 검증, 구현 가이드라인 제시, 통합 프레임워크 및 프로파일 구축 등의 활동을 하고 있다.

약 어 정 리

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

참 고 문 헌

[1] IDC, “IDC Expects Healthy Worldwide Investments in IT with Highest U.S. Growth Rates in Healthcare and Communications and Media,” 2006.

[2] University of Rochester, “Letting the Home Inter-

face with the Healthcare System: New Paradigms for Consumers and Providers," Though Leader's workshop white paper, 2004.
[3] GE 헬스케어, http://www.gehealthcare.com
[4] MobiHealth 프로젝트, http://www.mobihealth.org
[5] EU MCC 프로젝트 홈페이지, http://www.eten-mcc.org/
[6] 한국전산원, "의료정보화의 현황 및 과제," 2005.
[7] J.S. Wimalasiri, P. Ray, and C.S. Wilson, "Maintaining Security in an Ontology Driven Multi-Agent System for Electronic Health Records," *Enterprise Networking and Computing in Healthcare Industry, HEALTHCOM 2004. Proc. 6th Int'l Workshop*, 28-29 June 2004.
[8] CMS, "HIPAA Security Series: Security Standards, Technical Safeguards," 2005.
[9] HIPAA, "Summary of the HIPAA Privacy Rule," http://www.hhs.gov/ocr/hipaa/privrulepd.pdf
[10] 박건희, "보건의료정보화와 개인정보보호," 서울대 의대 2006년 상반기 토픽 리뷰, 2006. 6.
[11] Australia, "National Privacy Principles (Extracted from the Privacy Amendment (Private Sector) Act 2000," http://www.privacy.gov.au/publications/npps01.html
[12] W3C, "The Platform for Privacy Preferences 1.1 (P3P1.1) Specification," 2006. 11.
[13] IHE, http://www.himss.org/
[14] IHE, "IHE IT Infrastructure Technical Framework: Cross-Enterprise User Authentication (XUA) Integration Profile," White Paper, 2006.
[15] ITI Technical Committee, "IHE Security-XDS as a Case Study," IHE, 2006.
[16] Robert Horn, "Audit Trail and Node Authentication/ Consistent Time," IHE, 2005.
[17] ISO/TC215 http://www.iso.org/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=4720