情 報 保 護 學 會 誌
第 16 卷 第 6 號, 2006. 12

홈-헬스케어 서비스의 정보보호 소고

송 지 은, 김 신 효, 정 명 애, 정 교 일

요 약

단순 병원 전산화 수준이었던 의료 정보 서비스는 지능화된 의료 기기를 통하여 언제 어디서든 의료 서비스를 제공받을 수 있는 u-헬스케어 서비스 형태로 진화하고 있다. 특히, 홈-네트워크 기술의 성숙과 고도화된 유무선 의료기기의 발달은 홈-헬스케어 서비스의 확대를 촉진시키고 있다. 그러나 홈-헬스케어 서비스는 거주자의 생명이나 안전과 매우 밀접할 뿐 아니라 주로 매우 개인적인 정보를 다룬다는 점에서 정보보호 문제에 매우 민감하다. 따라서 본 고에서는 신뢰성과 안전성을 보장하는 홈-헬스케어 서비스를 제공하기 위한 정보보호 요구사항 및 이슈들을 살펴보고 아울러 이와 관련된 대안 기술들을 구체적으로 살펴본다.

Ⅰ. 서 론

언제 어디서나 서비스 이용이 가능한 유비쿼터스 기술의 등장으로, 의료 서비스 역시 질병 발생 후 대응하는 병원 중심 치료 패러다임에서 탈피하여, 병원이 아닌 환자의 집, 사무실 또는 이동 중에도 의료서비스를 받을 수 있는 u-헬스케어 서비스 연구가 활발히 진행되고 있다. 특히 최근 들어 u-헬스케어 서비스의 실체화 모델로서 홈-헬스케어 서비스를 위한 기술 연구가 활발히 진행되고 있다. 근래 수명 연장 및 참살이에 대한 욕구 증대에 따라 건강 의료 서비스에 대한 수요가 증가하고 있고 홈-헬스케어 서비스가 의료 건강 서비스의 효율성과 편리성, 경제성 등을 보장 할 수 있을 것으로 기대되어 관련 서비스와 기술 개발이 지속적으로 확대될 것으로 전망된다..

홈-헬스케어 서비스는 홈-네트워크의 대표적인 서비스 모델로서 기존의 홈-네트워크와 유사한 서비스 구조를 갖는다. 즉, 다양한 유무선 네트워크를 통하여 수집된 생체 및 의료 정보가 교환 될 뿐만 아니라 다양한 접근 경로를 통해 댁내 의료 기기 및 시스템을 제어 할 수 있다. 뿐만 아니라 건강 정보를 이용한 의료 서비스에 따라 다양한 정보 소비자가 발생 및 개입 될 수 있다. 그러나 이와 같은 홈-헬스케어 서비스 구조는 다양한 보안상 취약성과 공격에 노출 될 수 있다. 유무선 네트워크를 통해 의료 정보의 도청 및 위변조, 악의적 데이터 오염, 위장 사용자 진입 등이 발생 할 수 있고 불법적인 데이터 접근 및 활용과 같은 보안상 위협과 취약점이 발생할 수 있다. 특히, 홈-헬스케어 네트워크에서 발생 및 교환되는 정보는 극히 개인적인 건강정보, 생체 정보, 신체적 특징, 생활 습성 등과 같이 프라이버시에 민감한 정보들이 대부분이고 거주자의 건강 혹은 생명에 밀접하게 관련된 정보들이므로 홈-헬스케어 서비스에서의 정보보호는 안전하고 신뢰성을 보장하기 위해 필수적으로 고려되어야 할 기술 요소이다.

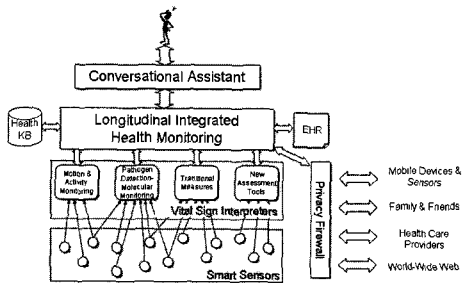
본 고에서는 홈-헬스케어 서비스의 모델을 정의하고 정보보호 이슈 및 요구사항에 대해 살펴본다. 뿐만 아니라 안전한 홈-헬스케어 서비스를 위한 정보보호 기술들을 보다 상세히 살펴본다.

Ⅱ. 홈-헬스케어 개요

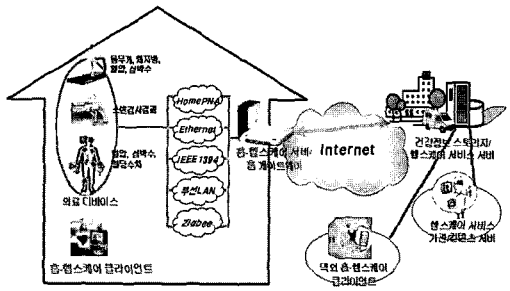
1. 홈-헬스케어 서비스

홈-헬스케어 서비스는 댁내에 설치된 유무선 의료기기를 이용하여 거주자의 생체 정보 및 환경 정보를 주기적 혹은 수시로 측정, 분석하여 언제 어디서나 의료 피드백을 받을 수 있도록 하는 서비스를 의미한다. 이와 관련한 대표적인 프로젝트로서 로체스터 대학 미

* 한국전자통신연구원 정보보호연구단(happybirds@etri.re.kr, shykim@etri.re.kr, machung@etri.re.kr, kyoil@etri.re.kr)



〔그림 1〕 스마트 메디컬 홈 서비스 프레임워크



〔그림 2〕 홈-헬스케어 서비스 아키텍처

래 건강 센터의 스마트 메디컬 홈(Smart Medical Home) 프로젝트가 있다[10]. 스마트 메디컬 홈 프로젝트는 'Your house is your personal health system'의 실현을 위해 자동화된 건강 정보 수집, 개인 정보 교환 인터페이스 정의, 타 시스템과의 통합 분야를 중심으로 활발히 연구 수행 중이다. 다음 〔그림 1〕은 스마트 메디컬 홈 프로젝트의 서비스 프레임워크로서 스마트 의료 센서부, 수집된 각종 생체 신호 분석부, 지속적인 건강 데이터 모니터링 및 축척부, 응용 서비스를 위한 정보 교환 인터페이스 및 댁내 시스템 및 서비스와 안전하게 통신하기위한 사설 방화벽 등으로 구성된다. 이 같은 서비스 프레임워크를 기반으로 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.

댁내에서 수집된 각종 생체 정보는 홈-서버 내에 집합 및 저장된 후 댁내 질병 시스템에 의해 자체적으로 질병 예측 및 피드백 서비스를 제공하거나 홈 게이트웨이를 통해 클리닉 센터나 종합 의료 정보 센터 등과 같은 댁외 의료 서비스 기관과 연계함으로서 다양한 헬스케어 서비스 제공이 가능하다. 홈-헬스케어 서비스의 아키텍처는 다음 〔그림 2〕와 같이 구성될 수 있으며 홈-헬스케어 서비스 아키텍처를 구성하는 시스템 종류 및 각 기능과 특징은 다음과 같다.

- 의료 디바이스 : 혈당, 혈압, 심박수, 움직임 등 각종 생체 신호를 측정 및 분석한 후 유무선 네트워크를 통해 홈-헬스케어 서버에 전송.
- 홈-헬스케어 클라이언트 : 댁내에서 거주자가 홈-헬스케어 서버를 통해 의료 서비스를 이용하거나 의료 디바이스를 제어할 수 있는 시스템.
- 건강정보 스토리지/헬스케어 서비스 서버 : 홈 게이트웨이를 통해 전달된 모니터링 건강 정보를 EHR(Electronic Health Record) 혹은 PACS(Picture Archiving and Communication System) 등의 표준 데이터 형태로 저장하고 관리.
- 헬스케어 서비스 기관/컨텐츠 서버 : 수집된 의료 건강 정보를 토대로 원격 진료 서비스나 개인 맞춤 건강 서비스, 각종 컨텐츠 서비스 등과 같은 서비스 기관이 이에 해당됨.
- 댁외 홈-헬스케어 클라이언트 : 헬스케어 서비스 기관 및 컨텐츠 서버로부터 관련 서비스를 제공받거나 댁내 의료 디바이스를 제어 및 관리할 수 있는 댁외 클라이언트 시스템.

홈 네트워크 기술이 성숙도에 들어섰고 대표적인 서비스 분야로서 홈-헬스케어 서비스가 큰 주목을 받고 있으나 생체 및 의료 데이터에 대한 보안 위협과 프라이버시 침해 등의 우려는 홈-헬스케어 서비스의 확대와 지속적인 성장의 저해 요인으로 지적되고 있다. 이는 관련 정보들이 대부분 거주자의 생명이나 안전과 밀접한 관계가 있을 뿐 아니라 극히 개인적인 정보가 대부분을 차지하기 때문이다. 따라서 안전한 홈-헬스케어 서비스를 보장하기 위하여 관련한 보안 이슈 및 요구사항들을 분석하고 적용 가능한 보안 기술의 간구가 선행되어야 한다.

2. 홈-헬스케어에서의 정보보호 필요성

홈-헬스케어에서는 다음과 같은 정보보호 필요성이 요구된다. 첫 번째는 프라이버시 보호의 필요성이다. 프라이버시 훼손이라 함은 개인 정보의 유출 또는 정보 위변조에 따른 피해로 볼 수 있으며, 이러한 피해를 사전에 예방하는 것이 프라이버시 보호이다. 홈-헬스케어에서의 프라이버시 정보는 댁내에서 모니터링 된 생체

및 건강 정보, 주변 환경 정보와 이에 대한 피드백 서비스 정보 등이 해당된다. 홈-헬스케어에서의 프라이버시 침해는 비인가된 홈-헬스케어 클라이언트 시스템이나 관련 서비스 기관 및 사업자에 의해 유출, 남용에 의해 발생될 수 있다. 또한 댁내에 잠입한 불법 유무선 모니터링 디바이스나 바이러스 및 악성 코드에 의해 손상을 입은 기존 의료 디바이스에 의해 불법적으로 수집될 수 있다. 개인 건강 정보 노출은 개인의 명예나 사회적 지위에 대해 영향을 끼칠 수 있을 뿐 아니라 심지어 관련 의료 서비스 사업자에게 동의 없이 제공되어 상업적으로 이용되는 등 개인의 의사와 무관하게 불법적인 거래로 이어지기 쉽다는 점에서 각별한 주의가 요구된다[7]. 이와 같은 우려를 반영하여 최근 의료 정보 보호를 법률로 권고 및 의무화하는 움직임이 활발히 일어나고 있다. 미국의 HIPPA(The Health Insurance Portability and Accountability Act)는 개인 사생활과 보안을 포함하는 개인 의료 정보보호에 관한 사항을 명시하고 있다[3][4]. 국내에서도 [표 1]과 같이 개인보건의료 정보의 수집, 처리, 이용 및 제공, 정보주체의 권리, 보건의료정보취급자의 의무, 전자의무기록, 전자처방전, 원격의료 분야에서의 의료 정보보호 규정을 제정하였다. 뿐만 아니라 의료정보보호 관련 법률의 제정 필요성이 제기되어 '건강 정보보호 및 관리 운영에 관한 법률'이 입법 예고된 상태이다.[7].

두 번째는 댁내 홈-헬스케어 서버와 원격 헬스케어 서비스 서버 간에 혹은 서비스 서버와 다양한 서비스 기관 간의 상호 인증 및 안전한 정보 공유를 위한 문제 해결이 필요하다. 이질적인 도메인 간에는 서로 다른 사용자 정보 디렉토리와 인증 방법이 사용될 수 있다. 이질 도메인마다 Keberos나 PKI, Token, Biometric 등과 같은 서로 다른 인증 방법이 사용될 수 있다. 이와 같은 이질적인 인증방식에 대한 서비스 독립성을 보장하고 도메인 간 교환 및 공유되는 트랜잭션에 대해 책임(accountability) 부여를 위한 기술이 필요하다. 이를 위해 다중 도메인 간 교환되는 사용자 식별 정보는 사용자 인증 수행 방법과, 접근제어 및 보안 감사를 위해 필요한 사용자 속성 정보 등을 충분히 포함하도록 해야 한다. 홈-헬스케어 서비스 환경에서도 마찬가지로 홈-헬스케어 서버와 원격 헬스케어 서비스 서버 간 공중망을 통해 거주자의 건강 모니터링 정보를 공유하는 경우, 다량의 건강 정보를 집약적으로 보관 및 관리하는 헬스케어 정보 서버와 서비스 사업자간에 개인 건강 정보가 교환 되는 경우 상호 인증 및 접근제어, 보안 감사 등을 반드시 수행해야 한다.

[표 1] 국내 의료정보보호 관련 규정

조 항	내 용
개인보건의료정보의 수집, 처리, 이용 및 제공 등	동의에 의한 수집, 수집 시 고지의무, 개인보건의료정보 수집의 제한, 개인보건의료정보의 처리, 이용 및 제공, 연구목적에 의한 개인보건의료정보의 처리, 이용 및 제공, 개인보건의료정보의 파기
정보주체의 권리	자기결정권, 개인보건의료정보에 대한 접근 권리, 개인보건의료정보에 대한 수정 요청의 권리, 제3자 제공 내역서를 받을 권리, 제한 요청의 권리, 비밀 의사소통 요청의 권리, 동의철회의 권리
보건의료정보취급자의 의무	보건의료정보취급자의 책임, 개인보건의료정보관리책임자의 지정,개인보건의료정보의 보호조치, 비밀유지, 요청 및 불만의 처리
전자의무기록	전자의무기록의 보존, 전자의무기록의 관리, 보존에 필요한 장비,전자의무기록의 타 기관 전송 등
전자처방전	전자처방전 등의 공개제한
원격의료	비밀누설금지

세 번째는 네트워크 보호의 필요성이다. 홈-헬스케어 네트워크는 생체 신호 및 환경 정보를 측정하거나 전송하기 위해 [그림 2]에서 보는 바와 같이 HomePNA, Ethernet, IEEE1394, 무선 LAN, Zigbee 등 다양한 통신 프로토콜이 이용될 수 있다. 그러나 최근, 센서 네트워크 기반의 의료 기기 서비스가 발달하고 무선 LAN 이나 블루투스 등 무선 통신 서비스가 보편화되면서 무선 네트워크를 통한 보안상 공격 및 위협이 가중화되었다. 무선 LAN이나 Zigbee, RFID 등 무선 프로토콜 자체의 보안상 취약점(vulnerability)을 이용한 세션 가로채기, 중간자 공격, DoS(Denial of Service) 공격으로 인한 서비스 무력화, 위장 디바이스 공격 등이 발생할 수 있으며 웜/바이러스 등에 의한 시스템 장애 유발이 가능하다. 특히, 유무선 네트워크 환경 모두에서 가장 심각한 보안 위협은 네트워크 전체에 대한 DoS 공격이다. 지난 1.25 인터넷 침해사고에서 경험하였듯이 이러한 위협은 광범위한 사용자들에게 영향을 주게 된다. 전달매체 사이에서의 정보수집과는 달리 취약 지점을 집중 공격하는 DoS 공격으로 인한 비정상적인 데이터 폭주 등은 네트워크 가용성을 파괴하기 때문에 원활하고 안정된 홈-네트워크 서비스를 방해하는 주요인이 될 수 있다. 따라서 안전한 홈-헬스케어 서비스를 보장 하기 위하여 발생 가능한 위협이나 공격들을 능동적으로 감지하고 대응할 수 있는 정보보호 기술이 요구된다.

3. 홈-헬스케어 정보보호 요구사항

안전하고 신뢰성 있는 홈-헬스케어 서비스를 보장하기 위하여 다음과 같은 정보보호 요구사항이 충족되어야 한다. 일반적인 정보보호 요구사항으로는 악의적인 공격자가 개인의료 정보를 얻고자 시도하는 공격을 막는 인증 기술, 정상적인 무선 센서와 센서 사이의 데이터를 공격자가 엿듣는 경우를 방어하는 도청 방지 기술, 공격자가 정상적인 데이터를 위조 혹은 오염시킴으로써 서비스의 무결성을 손상키는 공격을 방어하는 데이터 기밀성과 무결성 보장기술과 정당한 권한이 있는 시스템이나 사용자에게 의료 기기 제어나 의료 정보 접근, 관련 서비스 이용 등을 보장하는 서비스 접근 제어 기술 등이 있다.

이 외에도, 사용자가 원하는 때에 정확한 서비스를 제공할 수 있는 서비스의 신뢰성 및 가용성 또한 매우 중요한 정보보호 요구사항이다. 특히, 홈-헬스케어 서비스의 경우 서비스의 가용성 뿐 아니라 보안상 공격, 시스템 장애나 오류 등이 발생했을 시에도 적절한 수준의 가용성, 무결성, 기밀성을 보장하면서 중요 서비스를 지속적으로 제공할 수 있는 생존성까지 보장 받을 수 있어야 한다. 이는 응급 상황을 포함한 모든 일상생활 가운데서 거주자의 건강과 안전을 보장하기 위해서이다. 그리고 또한 개인의 프라이버시 보호 기술이 보장되어야 한다. 개인의 생체 및 위치, 환경 정보 등이 불법적으로 수집 되지 않도록 방지되지 않도록 해야 하며 비록 이와 같은 정보가 노출 되더라도 소유자와의 연관 관계를 파악하지 못하도록 하거나 이전의 관련 건강 정보를 추측 및 습득 할 수 없도록 해야 한다. 또한 개인 건강 정보에 대한 이용 목적 및 방법에 대해 인지하고 접근 권한을 직접 설정 및 제어할 수 있는 서비스가 지원 되어야 한다[11].

뿐만 아니라, 서비스 혼란 및 무력화를 위한 악의적 공격에 대해 감지하고 감내 할 수 있는 기능과 예기치 못한 상황이 발생할 때 이를 기록하고 관리자에게 보고하여 보안 대응을 할 수 있도록 하는 보안 감사 및 보안 관리 기능도 요구된다. 또한 홈-헬스케어서 사용자 인증을 위해 ID/PWD, 인증서 외에도 자각적, 비자각적으로 수집되는 지문이나 얼굴, 홍채, 음성 인식 등과 같은 생체 정보를 기반으로 한 다양한 인증 기술들을 포괄적으로 지원할 수 있어야 한다[2][5][13]. 이와 같은 기술적 요구사항은 홈 네트워크를 활용한 헬스케어 서비스의 초기 설계 시 동시에 반영되어야 한다.

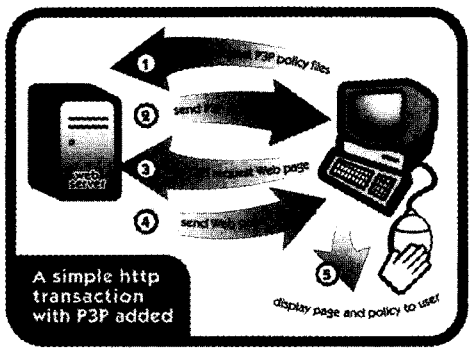
Ⅲ. 홈-헬스케어 정보보호기술

본 장에서는 홈-헬스케어 서비스의 정보보호 요구사항을 반영하고 의료 정보의 프라이버시 보호, 서비스 도메인 간 교환되는 전자 의무 기록의 보호 및 안전한 공유, 서비스의 가용성과 신뢰성을 높이기 위한 네트워크 보호 기술 등을 보장하기 위한 기술들을 보다 상세히 검토한다.

1. 의료정보의 프라이버시 보호 기술

개인정보보호 방법으로는 개인정보를 자신의 통제 영역 안에 포함시켜 개인정보의 유통을 개인이 관리하도록 하는 개인정보 자기통제권 확보 기술과 개인 정보를 전송하고자하는 대상자만이 해석할 수 있도록 암호화하는 방법 및 사용 시의 내 정보가 누구인지 알아내지 못하도록 하는 익명화 방법을 들 수 있다.

P3P(Platform for Privacy Preferences Project)는 웹사이트 접속 시 프라이버시를 보호하기 위해 국제 웹 표준화 기구인 W3C(World Wide Web Consortium) 권고안으로 2002년 승인되었으며 대표적인 개인정보 자기통제권 기술이다. 이 기술은 사용자가 요구하는 정보보호 요구 수준에 부합하는 경우에만 해당 정보를 제공함으로써 사용자 스스로 본인의 정보를 관리하고 제공할 수 있도록 한다.



[그림 3] P3P 동작과정

P3P의 동작과정은 [그림 3]에 도시하였다[14]. 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 사용 정책을 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 그대로 적용될 수 있을 것이다.

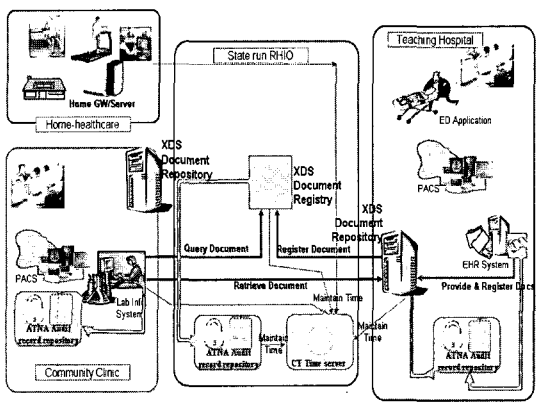
익명성 보장은 의료정보의 치료 또는 연구 목적으로 사용을 위해서는 반드시 필요한 항목이다. 익명성 보장이란 내가 정당한 사용자임을 증명하되, 나의 식별 정보를 제공하지 않을 수 있는 권리를 의미한다. 인터넷 등에서 회원가입을 위해 입력을 요구하는 주민번호는 실명확인을 위해 필요하다고 하지만 이에 의해 알려질 수 있는 개인 성별, 출생지, 나이 등 실명이외의 다양한 개인정보의 노출로 프라이버시 침해가 우려된다. 의료 서비스 시에도 자신의 사례와 비슷한 질병의 치료나 연구 또는 질병 통계 목적으로 개인의 현재 질병 및 병력이 활용될 수 있으나, 이때에도 반드시 개인의 식별 정보를 포함하지 않도록 하여 익명성을 보장하여야 한다. 이러한 익명성 보장 기술은 평상시 정상적인 활동에는 반드시 보장되어야 하지만, 응급 처치 등의 긴급 상황 에서는 개인의 신분 확인이 가능하여야 하는 양면성을 지니고 있다.

익명성 보장은 의료정보화에서의 가장 중요한 이슈 중의 하나이고 IHE(Integrating the Healthcare Enterprise)에서 Liberty Alliance(이하 리버티 얼라이언스)와의 협조를 통해 구체화 시킨바 있다. IHE는 새로운 의료정보화 표준의 개발보다는 기존의 다양한 표준간의 상호 호환성을 논의하기 위한 벤더들의 촉진기구이다. 익명성 보장기술로 활용 가능한 ID-federation 기술을 의료분야에 적용하기 위해 리버티 얼라이언스와 협력관계를 맺고 이에 대한 활발한 논의를 진행중이다. 리버티 얼라이언스 역시 e-Health SIG(Special Interesting Group)를 구성하여 활동하고 있으며 이들이 추구하는 의료서비스에서의 익명성 보장 기법은 다음 절에서 IHE의 데이터 공유(XDS, Cross-Enterprise Document Sharing)와 XUA(Cross-Enterprise User Authentication - User Identity Federation)에 대해 좀 더 자세히 설명하도록 한다.

2. 전자 의무 기록의 보호 및 안전한 공유

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[8][16][17]. 따라서 교환할 환자/의료 데이터 식별 방법과 교환할 메타 데이터 문서 구조와 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 부여하기위하여 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.



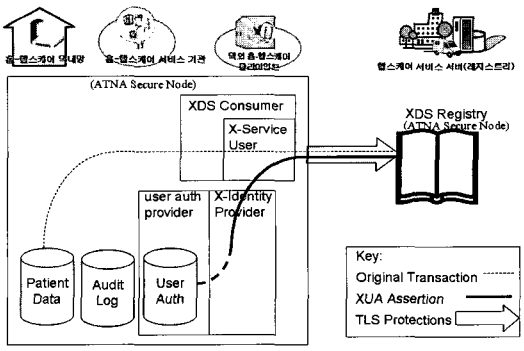
[그림 4] 홈-헬스케어 환경에서의 IHE-XDS

이 같은 IHE-XDS는 댁내 홈-헬스케어 도메인과 댁외 건강 정보 서비스 기관 간 거주자의 건강 정보가 교환되는 홈-헬스케어 서비스 환경에서도 적용 가능하다. [그림 4]와 같이 홈-헬스케어 서버와 클리닉 센터, 중대형 병원 내의 XDS Document Repository 간에 건강 정보 요청 및 접근이 수행 될 경우, 각 Repository와 Registry는 IHE-XDS 모델에서 지원하는 DSIG (Digital Signature Content Profile), CT(Consistent Time), ATNA(Audit Trail and Authentication) 등을 이용하여 건강 정보 요청자의 식별, 접근 제어, 교환 데이터의 기밀성과 무결성 보장, 발생하는 정보 이벤트에 대한 보안 감사 등을 지원함으로서 안전한 건강 정보 공유를 보장 할 수 있다. IHE-XDS에서 제시하는 보안 모델을 구성하기 위한 구체적 보안 솔루션들은 다음과 같다.

- Affinity Domain Policy : 모든 Actor, 즉 건강 정보 교환을 동의한 도메인들은 보안 정책의 생성 및 수행에 대해 사전에 동의한다.
- ATNA : 데이터의 기밀성, 무결성 등을 보장하고 개인에게 민감한 정보의 경우 접근 제어를 실행한다. 또한 보안 감사를 통해 책임의 불법 행위를 방지하고 책임의 소재를 분명히 한다.
- DSIG : 요청자의 식별 및 데이터 요청과 제공에 대한 부인 방지를 지원하기 위하여 사용해야 한다.
- 그 밖에 접근제어를 위한 RBAC(Role Based Access Control)이나 PMAC(Privilege Management and Access Control) 등 응용 레벨에서의 접근 제어 정책 정의가 필요하다.

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 필요한 인증와 속성 정보, 보안 감사 속성 정보 등을 포함하고 있다[8][15]. 앞서 언급한 바와 같이 다중 도메인 간 교환되는 트랜잭션에 대해 Accountability를 부여하기 위하여 피 요청기관이 접근 결정 및 보안 감사를 수행하는 데 사용 가능한 방법으로 요청자를 식별해야 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



[그림 5] 홈-헬스케어 환경에서의 IHE-XUA

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

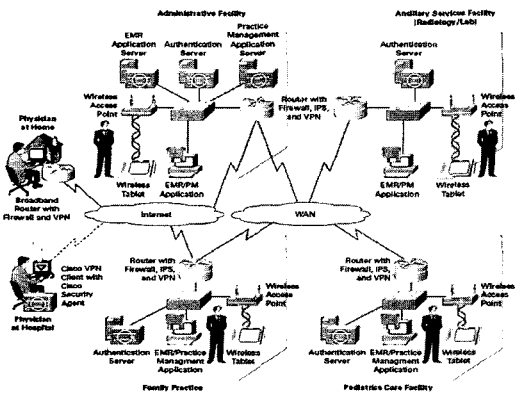
홈-헬스케어 환경에서 IHE-XUA를 이용한 도메인 간 인증 수행 예는 다음 [그림 5]와 같다.

거주자의 건강 정보를 수집하고 있는 홈-헬스케어 댁내 망이나 환자의 원격 진료 서비스를 수행하는 의료기관, 건강 정보에 대한 컨텐츠 서비스 기관 및 이동형 댁 외 헬스케어 클라이언트 등이 레지스트리를 통해 데이터를 공유할 때, 통신 트랜잭션에 대해 X-Assertion 즉, 인증 및 식별 정보, 보안 속성 정보 등을 포함하도록 함으로써 이질적 보안 프로토콜 운용 환경에 대한 상호 운용성을 보장하고 트랜젝션에 대하여 Accountability, 보안 감사 등을 시행 할 수 있는 조건을 조성한다. 또한, ID Federation를 지원함으로써 ID 중복 관리 및 익명성 보장 등을 보장할 수 있다.

최근 IHE 에서는 근래에 논의 및 제안되고 있는 ISO와 ASTM의 표준을 반영하여 SAML Assertion을 확장하는 작업을 하고 있다. X.509-ISO/TS17090, LDAP Meta data compliant-ISO/TX 21091, Functional and Structural Roles from ISO/DTS 21298 등이 대표적인 표준 예이다. 유비쿼터스 서비스 패러다임에 대한 인식의 확산으로 원격 의료 진단 서비스 수준에 머물러 있는 홈-헬스케어 서비스도 서비스 고도화 및 다양화를 위해 관계 서비스 기관들이 보다 확대될 것이므로 IHE의 멀티 도메인 간 전자 건강 데이터의 안전한 공유 기법은 향후 더욱 유용하게 사용될 수 있을 것이다.

3. 네트워크 정보보호 기술

홈-헬스케어 서비스의 무결성과 가용성을 보장하기 위해서는 홈-헬스케어 네트워크에 대한 보호가 필요하다. 그러나 사실 네트워크 보호의 문제는 홈-헬스케어 서비스에만 귀속되는 독자적인 이슈는 아니다. 실제로 네트워크 장비 회사들은 TCP/IP 기반의 인터넷 프로토콜이 의료장비에 필수적으로 지원되면서 기존의 네트워크 정보보호 솔루션을 의료분야 정보보호에 그대로 사용할 수 있을 것으로 판단하고 있다. 즉, 헬스케어 네트워크에 대한 보안 장비는 네트워크 장비 내장용 바이러스 백신, 침입탐지, VPN 장비 및 보안 관리, 사용자 인증을 위한 AAA 장비 등과 PoC(Ponit-of-Care) 장비와 의료 단말용 타블렛 PC나 PDA에 적용하기 위한 무선 보안 구간 인증 및 암호 툴 등으로 기존 보안 장비와 큰 차이가 없다. 이러한 헬스케어 네트워크 보안 구성 예시는 [그림 6]과 같다[6].



[그림 6] 시스코 헬스케어 네트워크 보안 구성 예

그러나 홈-네트워크가 점차 활성화 되면서 홈-헬스케어 댁내망은 홈-헬스케어 서버나 게이트웨이 외에도 다양한 유무선 의료 기기 센서, 서비스 클라이언트 터미널이 혹은 단말들로 구성되고 사용자가 다양해짐에 따라 공격 형태 및 피해 양상이 보다 다양하게 나타날 수 있다. 또한 댁내 망을 구성하는 무선 통신 프로토콜들은 WLAN, 블루투스, Zigbee, RFID 등으로써 대부분 MAC 계층에서 발생하기 때문에 기존의 침입 탐지 시스템으로 대응하는 데는 한계가 있다. 따라서 이들 무선 통신 망에서의 보안상 취약점 및 발생 가능한 보안 위협 등의 시나리오를 보다 상세히 분석하여 이를 기반으로 한 홈-헬스케어 게이트웨이 내외장용 침입 탐지 및 대응, 더 나아가 지속적인 서비스 가용성을 보장하는 침입 감내 기술에 대한 연구가 지속적으로 요구된다[9].

Ⅳ. 결 론

홈-헬스케어 서비스는 거주자의 건강이나 생명에 관련된 정보를 주로 다룬다는 점에서 타 홈-헬스케어 서비스보다 건강 정보 보안 및 프라이버시 보호 등을 포함한 정보보안 문제에 대해 더욱 민감한 성향을 띈다. 건강 정보의 보안은 환자의 생명이나 안전과 관련된 중요한 사항이다. 뿐만 아니라 개인 건강 정보 노출은 개인의 명예나 사회적 지위에 대한 악영향, 상업적인 불법 이용 등 개인의 의사와 무관하게 타인에 의한 사생활 침해로 이어지기 쉽다는 점에서 각별한 주의가 요구된다. 또한 댁 내외 홈-헬스케어 도메인 간, 그리고 이질적 서비스 기관 간 건강 정보의 공유 및 교환이 확대됨에 따라 안전한 정보 공유를 위한 기술이 보장 될 수 있어야 한다. 안전한 홈-헬스케어 서비스 환경을 구축하기 위해 홈-네트워크 특성을 고려한 유무선 네트워크 보안 기술 또한 기본적으로 뒷받침 되어야 함은 물론이다. 따라서 본 고에서는 홈-헬스케어 서비스 특성을 고려하여 기존 프라이버시 보호 및 네트워크 보호 기술 등을 적용 및 확대할 수 있는 방안을 모색하였으며 EHR 시스템이 구축된 서비스 도메인 간 안전한 정보 교환을 위해 IHE 기술을 홈-헬스케어 네트워크 환경에 적용 및 활용하는 모델을 제시하였다. 바이오 칩이나 센서, 무선 의료 기기 등 보다 지능화된 의료 장비들이 거미줄처럼 얽혀서 다양한 서비스가 제공되는 보다 고도화된 u-헬스케어 서비스는 정보보안 및 프라이버시 보호 등이 보장되는 안전한 홈-헬스케어 시스템 구축으로 그 실현이 보다 구체화, 가속화 될 수 있을 것이다.

참 고 문 헌

[1] 한국전산원,"의료정보화의 현황 및 과제", 2005
[2] 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
[3] CMS, "HIPPA Security series: Security

Standards, Technical Safeguards", 2005
[4] "Summary of the HIPPA Privacy Rule", http://www.hhs.gov/ocr/hipaa/privrulepd.pdf
[5] "Final Criteria: Security and Reliability For 2006 Certification of Ambulatory EHRs ", 2006
[6] Cisco Systems, Inc., "Medical-Grade Networks-Cisco Protected Healthcare Solutions for Physician Groups and Clinics"
[7] 박건희, "보건의료정보화와 개인정보보호", 서울대 의대 2006년 상반기 토픽 리뷰, 2006.6.
[8] IHE 홈페이지, http://www.himss.org/ASP/topics_ihe.asp
[9] 홍만표, "Intrusion Tolerance System for Home Network Security.pdf"
[10] University of Rochester, " Letting the home interface with the healthcare system: New paradigms for consumers and providers", Though Leader's workshop white paper, 2004
[11] 한종욱, "홈네트워크 사용자 인증 및 접근제어 솔루션", HNFocus vol.10, 2005
[12] 소프트포럼, "홈네트워크에서의 SSO" Soft-Forum. 2005
[13] 국내 e-Health 발전에 따른 정책대응방안 연구 - 한국보건사회연구원, 2005
[14] Australia, 'National Privacy Principles (Extracted from the Privacy Amendment (Private Sector) Act 2000', Available at http://www.privacy.gov.au/publications/npps01.html
[15] IHE, "IHE IT Infrastructure Technical Framework : Cross-Enterprise User Authentication(XUA) Integration Profile", White Paper, 2006
[16] Robert Horn, "Audit Trail and Node Authentication / Consistent Time", IHE, 2005
[17] ITI Technical Committee, "IHE Security-XDS as a case study", IHE, 2006

〈著者紹介〉

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

김 신 효 (Shin-hyo Kim)
1990년 2월 : 전남대학교 전산학과 (이학사)
2000년 2월 : 충남대학교 컴퓨터과학과(이학석사)
1990년 ~ 현재 : 한국전자통신연구원 정보보호연구단 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 고분자 연구소 Prof. W Knoll 그룹 근무
2000년 ~ 현재 : 한국전자통신연구원 의료정보보호팀 팀장
관심분야 : 나노 바이오 센서, 뉴런 칩, u-헬스케어, 의료정보보안

정 교 일 (Koy-il Chung)
1981년:한양대학교 전자공학과 (공학사)
1983년:한양대학교 산업대학원 전자계산학과 (공학석사)
1997년:한양대학교 대학원 전자공학과 (공학박사)
1982년~현재: 한국전자통신연구원 정보보호연구단 정보보호기반그룹장/책임연구원
관심분야 : IC Card, Security, Biometrics, 국가기반보호, 신호처리