e-Healthcare 환경 내 개인정보 보호 모델☆

Privacy Information Protection Model in e-Healthcare Environment

김 경 진* 홍 승 필**
Kyong-Jin Kim Seng-Phil Hong

요 약

인터넷 등의 정보기술의 발전은 기존의 의료기술에 빠른 변화를 가져오면서 e-Healthcare가 사회적 이슈로 등장하고 있다. 의료정보화 패러다임의 새로운 전환점이라 할 수 있는 e-Healthcare는 국내에서 의료정책방안이나 기술개발을 하고 있지만, 아직 의료정보화의 기반이 되는 인프라는 부족한 수준이며 개방된 인터넷 환경 내 역공학적 측면으로 민감한 의료정보 유출 및 프라이버시 침해에 대한 문제가 대두되는 실정이다.

본 논문에서는 앞서 제시한 문제점의 해결방안으로 e-Healthcare환경 내 개인의 의료정보 보호를 위한 역할기반의 접근제어 시스템(HPIP - Health Privacy Information Protection)을 네 가지 주요 메커니즘(사용자 신분확인, 병원 권한확인, 진료기록 접근제어, 환자진단)으로 제안하였으며, 실 환경에서 효과적으로 활용될 수 있도록 프로토타이핑을 통해 그 가능성을 타진해 보았다.

Abstract

The development of information technology such as the internet has brought about rapidly changes the old medical technology, e-Healthcare has been to raise social issue. The e-Healthcare which new turning point of paradigm in the medical information develops the medical policy in Korea and the technology, the prospective of reverse engineering in internet environment is incurring problems such as distribution of critical information and invasion and infringement of privacy, etc.

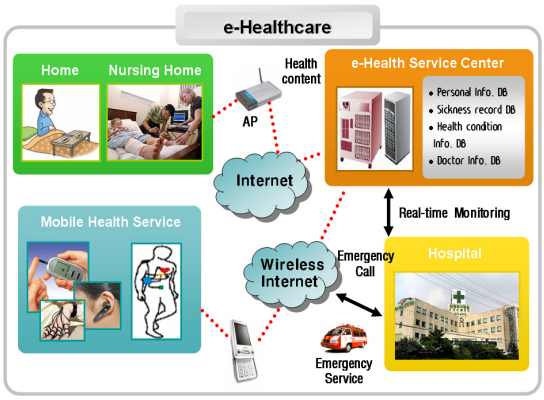
In this research, we suggest the Role Based Access Control System, HPIP - e-Healthcare Privacy Information Protection, for solving above problem. The HPIP is composed 4 mechanisms such as Consolidate User Identity, Hospital Authorization, Medical Record Access Control, Patient Diagnosis and we are also prototyping the HPIP for feasible approach in the real computing environment.

☞ keyword : 접근제어, 프라이버시 보호, 개인정보보호

1. 서 론

e-Health는 진료예약을 자동화하는 가장 단순하고 사무적인 HIT(Health Information Technology)에서부터, 환자의료정보에 대한 안전한 접근을 위해 개발된 다양한 의료정보기술이나 체계뿐만 아니라, 의사의 진료를 돕기 위한 복잡한 임상적인 적용에 이르기까지 다양한 형태의 의료정보기술의 적용을 의미한다. 이는 인터넷을 통해 보건의료제품 및 서비스가 전달되는 상태 또는 환경으로 정의할 수 있다.[1][2]

* 준 회 원 : 성신여자대학교 대학원 전산학과 석사과정
kyongjin@sungshin.ac.kr(주저자)
** 종신회원 : 성신여자대학교 미디어정보학부 교수
philhong@sungshin.ac.kr(교신저자)
[2008/07/10 투고 - 2008/07/11 심사 - 2008/09/18 심사완료]
☆ 본 연구는 서울시 산학연 협력사업(NT070103)의 지원을 받아 수행된 연구임



(그림 1) e-Healthcare 환경

그림 1의 e-Healthcare 환경은 정보통신기술을 활용하여 의료, 보건 정보를 온라인으로 제공하고 공유하는 때와 장소를 가리지 않는 건강관리 기법으로 보건 의료부문과 인터넷과의 만남으로 발생한 보건의료의 새로운 패러다임이다.[3][4]

e-Healthcare는 지금까지의 의료산업과 달리 시간적, 공간적 제약을 넘어서 모든 사람들이 편리하게 자신의 건강상태를 체크하고, 치료할 수 있는 시스템을 제공한다. 이러한 e-Healthcare 환경은 인터넷을 통하기 때문에 병원 간 환자의 진료정보를 공유할 수 있어 환자진료 및 개인건강관리 시 효율적이고 합리적인 의사결정을 지원할 수 있다.[6] 인터넷의 이용은 개인정보 활용과 사용이 편리해진 반면, 유통되는 정보의 검증이 어렵고 민감한 개인정보까지 유출되는 피해가 발생하면서 프라이버시의 침해가 중요한 위험으로 대두되고 있다.

본 논문의 구성은 다음과 같다. 1장에서는 논문의 개요를 간략히 소개하고, 2장에서는 e-Health의 국내외 동향과 정책을 알아본다. 3장에서는 관련 기술 및 e-Health의 기능별 유형과 HIPAA(Health Insurance Portability and Accountability Act of 1996)의 사례연구를 살펴보고, 국내의 e-Healthcare의 개인정보침해 문제점과 이를 보호하기 위한 대응방안을 제안한다. 4장에서는 개인정보보호 및 안전한 정보 공유의 대안으로 e-Healthcare의 개인정보보호 시스템 모델인 HPIP(e-Healthcare Privacy Information Protection)를 제안하였으며, 주요 관련 메커니즘을 소개한다. 마지막으로, 5장에서는 결론 및 향후 연구 방향을 기술하였다.

2. 국내외 동향

2.1 국외 e-Health 현황

미국의 경우, 연방법, 주법에 걸쳐서, e-medicine, e-Health에 관한 규정이 다양하게 규정되고 있고, 또한 그 존재형태도 법, 시행령, 시행규칙, 지침 등 여러 가지 형태로 존재하고 있다. 또한 영국은 데이터보호법(Data Protection Act, 1998)을 제정하여, 개인정보보호에 힘쓰고 있다.[2]

주요국의 e-Health의 동향을 표1로 나타내었다.[9][12]

(표 1) 해외사례

국가	세부 내용
유럽연합	○'eEurope의 e-Health'는 e-Europe의 목표 중 하나로 EHTEL을 중심으로 홍보를 수행하고 있음 ○유럽 19개국 e-health 관련 장관급 회의 개최(2003.5, 브뤼셀)
미국	○미국 정부는 국가 수준의 의료 정보화 정책 등을 추진 - HIPAA 법제화 ○부시대통령은 2004년 향후 e-Health에 대한 집중적 투자의 의료정보화계획을 공포 ○Elite care 의 Oatfield Estates는 은퇴한 고령자를 대상으로 양로원을 운영하며, 건강체크 변기센서, 침대센서, 약 복용 알림 시스템 운영
영국	○'99년 e-Health협회(UKeHA)를 설립하여 e-Health산업 활성화 - NHS는 '98년 'Information for Health'라는 국가차원의 정보화 전략계획을 수립
일본	○고령자 복지10개년 계획, New Gold Plan 등 정부의 적극적인 정책을 통해 u-Health 시장을 개발하고 있음 ○'06년부터 치매성 노인 주거시설, 소규모 요양소 등에 홈네트워크를 이용한 헬스케어 시스템을 도입할 예정

미국정부는 국가 수준의 의료 정보화 정책 등을 추진하여 의료 정보화 분야에서 가장 앞서 있으며, 매년 투자액이 증가하는 추세이다. 미국 시장은 기업들의 자유로운 경쟁과 기술발전을 통한 시장주의 형태로 발전할 것으로 보이며 향후 세계 시장을 견인할 전망이다.[2]

2.2 국내 e-Health 현황

우리나라 병원정보화는 1990년대 초부터 추진되기 시작해 '93년 37%에 불과하던 종합병원의 업무전산화가 '00년 거의 100%에 달하였고 최근들어 대형종합병원을 중심으로 전자의무기록시스템(EMR) 도입 및 자매병원/협력병원 간의 진료정보 공유 등이 이루어지고 있다.[13] 정책적으로는, 2004년부터 정부육성 정책의 일환으로 정통부, 산자부, 복지부 등 홈 네트워크 산업에 헬스 케어 사업 육성 및 의료 정보화를 추진 중에 있다.[9][12]

(표 2) 국내 e-Health 동향

부	추진 정책
정통부	◎ 정통부와 한국전산원은 '2006년 디지털홈구축활성화 사업'의 일환으로 e-Health산업을 기획하고, 중앙정부와 지방자치단체, 민간기업 공동으로 재원을 마련하여 u-Health 선도 사업 추진 - '04년 추진한 홈 네트워크 시범사업에 SK텔레콤컨소시엄과 KT컨소시엄이 사이버 아파트를 중심으로 원격진료가 가능한 미래형 홈 네트워크 서비스를 시행
산자부	◎ 스마트 홈 부문의 헬스 케어 품목, 전자의료기기분야 실버의료기기, 영상진단기기, 모바일 헬스 케어 등을 육성
복지부	◎ 보건의료분야, 보건산업분야, 사회복지분야, 사회보험분야의 정보화 추진 - '05년 총22개 정보화 과제에 646억 원의 예산 투입 - e-헬스케어와 전체 병원 간 진료정보 공유를 위한 전자건강기록사업(EHR)등을 추진 중

헬스케어 사업 육성 추진은 사업간 중복 및 이해당사자간의 갈등으로 정책효과가 아직 미미한 수준이지만, 병원들의 의료화가 활발해짐에 따라 다국적 기업들의 진출함으로써 의료정보화 시장의 경쟁은 심화되고 있다.

현재 기술적으로는 health 서비스 시장형성의 초기단계이며 혈압, 맥박, 혈당 등에 국한된 홈 원격진료 서비스가 위주이다. 정책은 e-Health 전체를 포괄하는 전 국가적 차원의 정책이라기보다는 각 부처의 특성만을 실어 기술개발자체만을 목적으로 산업 활성화에 중점을 두어, 보건의료서비스의 질 향상 및 관련 산업발전 등과 같은 e-Healthcare의 궁극적 목적 달성과는 거리가 있다.[5]

3. 관련 연구

3.1 e-Health의 5가지 유형

e-Health는 인터넷과 정보 기술의 발전으로 보건의료서비스를 새로운 시각에서 조망하기 시작한 개념으로 다음의 5가지 유형이 Eng(2001)가 제시한 5C에 근거하여 content, community, commerce, connectivity, care로 나누어 살펴볼 수 있다.[8]

(표 3) Eng(2001)가 제시한 5C

유 형	설 명
Content형	웹을 통해 접근 가능한 건강 및 질병과 관련된 정보를 말함. 즉, 인간의 행동변화, 의사결정 및 원거리 교육/훈련을 미치는 정보의 전자적 제공과 함께 이러한 정보 접근을 도와주는 표현 및 검색 기능을 포함.
Community형	동료 간 및 전문가 등과의 메시지 전달, 정보교환, 정서적 후원 및 커뮤니티의 구축을 포함함. 커뮤니티를 구축하는 고객 및 참여자들은 네트워크 외부성 효과를 가지며 그 자체로써 가치창출의 한 요소가 됨
Commerce형	온라인 약국, 의료기기의 온라인 구매 등 의료와 관련된 모든 전자상거래와 쇼핑을 포함하며, 크게 B2B 시장과 B2C 시장으로 나눌 수 있음.
Connectivity형	임상 및 보건 정보 시스템, 보건의료서비스와 시스템의 통합 및 행정적 거

	래 등 보건의료 시장에 속하는 여러 참여자들을 연결하는 인터넷 기초와 재화와 서비스를 칭함
Care형	자가 진료, 진료조정, 전자 건강기록, 협동형 임상 의사결정, 전문가 시스템, 질병관리 및 원격의료/원격건강 등을 포함함.

위에 살펴본 e-Health 기능별 유형은 상호 독립적이지 않고, 상당부분 겹쳐져 있어서 e-Health 비즈니스모델들은 다양한 기능들이 혼재되어 새로운 모형을 창출하고 있다. 이는 초기단계에서 content 유형을 중심으로 성장하며, commerce 유형이 대세를 이루다가 점차 care 유형으로 성숙하는 발전단계를 밟고 있어 의료서비스의 범위가 병원에서 환자의 생활공간인 가정이나 이동 중의 공간으로까지 확대되는 것을 말한다.

3.2 사례연구 - HIPAA

'Health Insurance Portability and Accountability Act of 1996'에서는 의료정보를 저장 및 처리하는 의료기관의 개인정보보호에 관한 사항을 법률로 규정하고 있다.

HIPAA는 의료정보를 취급하는 기관에서 준수해야 할 프라이버시와 보안에 관한 사항을 다루고 있으며 이를 간략히 요약하면 다음과 같다.

① 보안 책임자 혹은 보안조직을 지정하여야 한다.
② 건강정보의 프라이버시와 보안에 대한 주요 위협들을 파악하고 위험요인을 평가하여야 한다.
③ 보안사고 대응, 재해복구 대책, 물리적, 이적, 기술적 보안을 포함하는 보안 관리 프로그램을 구성해야 한다.
④ 신규 혹은 기존 보안통제수단의 효과성을 확인해야 한다.
⑤ 프라이버시 담당자 지정 및 프라이버시에 관한 불만처리업무을 수행한다.
⑥ 프라이버시 정책을 채택하고 공표하며, 프라이버시 정책은 동의 획득 및 건강정보의 이용 권한에 대해 구체적 규정을 보유하여야 한다. [5][7]

HIPAA 프라이버시 규정에 포함된 환자 권리의 주요내용은 표4와 같다.[11]

(표 4) HIPAA 프라이버시 규정에 포함된 환자의 권리

환자의 권리	주요 내용
프라이버시 관행의 통지	- 법적용 대상기관은 특별한 예외상황을 제외하고는 반드시 프라이버시 관행(practice)을 알려주어야 함
접근의 권리	- 특별한 예외상황을 제외하고 개인은 자신의 지정된 의료정보(designated record set)에 대한 검토 및 사본 획득 권리를 가짐 - 정신과 상담노트(psychotherapy notes), 법률 소송을 위해 준비한 정보 등은 예외로 함
수정의 권리	- 자신의 지정된 의료정보가 부정확하거나 완전하지 않은 경우 개인은 이를 수정할 권리를 가짐
공개 내역서를 받을 권리	- 개인은 최대 6년 치의 자신의 PHI 공개 내역을 알아 볼 권리가 있음
제한요청의 권리	- 개인은 자신의 PHI 사용 제한을 요청할 권리가 있음
비밀 의사소통 요청의 권리	- 지정된 주소나 전화번호를 통한 의료정보 제공 요청 등과 같이 개인은 자신의 PHI에 관한 비밀 의사소통 요청권리가 있음

HIPAA가 명확하게 프라이버시 규정과 보안 규정을 제시하고 있는 것에 비해 국내 의료 분야의 정보보호 법제도에서는 의료개인정보보호에 관한 일반법이 제정되지 않아 정보통신망이용촉진및정보보호등에관한법률 제4장의 동법에 의해 의료개인정보가 규율될 것이나, 그 근거 규정이 미흡하다.

3.3 관련 기술

P3P(Platform for Privacy Preferences)

P3P(Platform for Privacy Preferences)는 지난 2002년 국제 웹 표준화 기구인 W3C(World Wide Web Consortium)가 웹사이트 이용 시 프라이버시를 보호하기 위해 정한 표준 기술 플랫폼으로, 개

인 사용자는 자신의 개인정보 보호 Preference를 주어진 프로그램이나 에디터 등을 통해 명시하고 사용자 브라우저는 이 보호정책과 맞지 않는 웹 서버를 차단하여 개인정보유출을 사전에 방지하는 기술이다[10].

APPEL
(A P3P Preference Exchange Language)

W3C(World Wide Web Consortium)는 웹 사이트 이용시 사용자 개인정보 보호 preference를 APPEL(A P3P Preference Exchange Language)언어를 통해 명시하도록 제안하고 있다. APPEL은 W3C에서 공식적으로 제안하는 언어는 아니지만, Privacy Bird와 P3P 사용자 agent를 통한 개인정보 보호를 위한 기능을 수행하고 있다. 또한 APPEL은 P3P 정책과 사용자 agent 수행을 통제를 평가하고 XML언어를 기반으로 Privacy preferences를 규칙에 맞게 정의할 수 있다.[14]

PKI & PMI

공개키 기반구조 (PKI - Public Key Infrastructure)란 개방형 네트워크 또는 분산형 네트워크 환경 하에서 보안 요구사항을 만족시키기 위해 사용자가 보유한 암호를 이용하여 거래자의 신원을 확인하는 방식이다. 하지만, 공개키 기반구조에서 권한 인증 서비스를 제공하는 데는 한계를 가지므로 이러한 점을 보완하기 위해서는 권한관리 기반구조 (PMI - Privilege Management Infrastructure)와 같은 부가적인 구조가 필요하게 되었다. 여기서 권한관리 기반 구조란 권한 관련 자원과 이의 소유자간의 관계를 신뢰기관이 보증하고 유지하는 구조를 일컫는다.[15]

RBAC (Role Based Access Control)

역할 기반 접근제어 모델은 사용자에게 직접 권한을 할당하던 기존의 모델들과는 달리 기업 환경뿐만 아니라 데이터베이스. 운영체제 등에 적용될 수 있는 매우 유연한 접근 통제 정책으로 현실세계에서 수행하는 업무적 역할에 따라 인가권한을 역할에 할당하고, 사용자들은 적당한 역할에 소속되도록 함으로써 사용자들의 권한 관리를 효율적으로 할 수 있도록 지원한다.[16]

3.4 e-Healthcare 환경 내의 문제점

e-Healthcare는 인터넷을 통하기 때문에 정보공유 및 사용이 편리하여, 최근 대형종합병원을 중심으로 전자의무기록시스템(EMR) 도입 및 자매병원/협력병원 간의 진료정보 공유 등이 이루어지고 있다.[11]

하지만, 이는 일부이고 국내 일반 의료기관은 단일 병원 시스템 구축 수준으로 의료정보화의 기반이 되는 인프라는 아직 미흡하여 병원 간 정보의 공동 활용 및 네트워크화에 기본진료 정보가 공유되지 않아 중복검사, 대기시간 증가 등 사용자(환자) 중심적인 서비스가 부족한 실정이다.

또한, 의료업무전산화의 발전으로 병원의 운영업무와 진료 업무가 정보시스템에 의존하는 비중이 점점 높아지고, 정보의 사용 범위가 넓어짐에 따라 정보보호 위협은 더욱 커지면서 유통되는 정보의 질에 대해 검증이 어렵고, 환자의 개인정보 유출로 프라이버시를 침해할 우려가 있다. 아래 표는 의료이용자별 문제점 및 이슈에 대해 분류해 보았다.

(표 5) 보안 및 프라이버시 문제점과 이슈

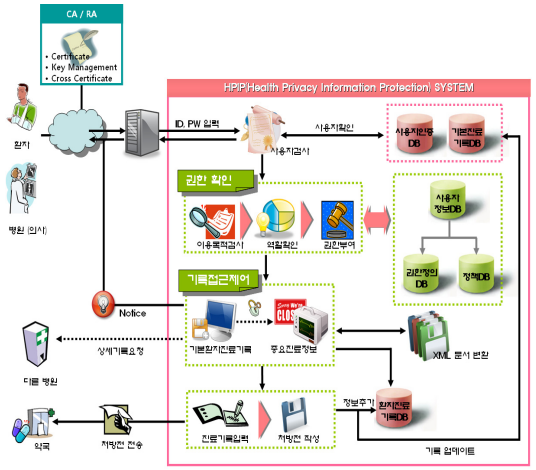
분류	이슈	문제점
병원 / 의료 기관	- 환자의 개인진료정보를 이용하기 위해서는 무조건 환자의 동의가 필요하다. - 정보 수정 시에 오류 없는 정확한 데이터를 보장해야 한다. - 환자의 개인진료정보의 유출 및 남용피해에 대해 강화된 법적 제재가 필요하다. - 개인 건강/진료정보를 취급하는 사이트는 수집 방법, 수집	- 프라이버시 보안 기술 부족 - 소유자(환자) 동의 없이 개인정보 수집 및 유통 - 명백하지 않은 개인정보 수집에 대한 약관(목적) - 개인정보는 정보요청자의 인증 확인 없이도 쉽게 유출 가능

	범위 등에 대해 이용자에게 공지 의무화가 필요하다.	
약국	- 누구든 쉽게 환자의 개인정보와 진료기록을 접근할 수 있다. - 필요한 정보 이외의 정보도 습득이 가능하다.	- 허가받지 않은 자가 민감한 정보에 접근이 가능
환자	- 환자는 자신의 정보가 어떻게 수집되고 사용되는지 알 수 없다. - 환자는 자신의 의료기록정보를 접근하기 어렵다.	- 사용자들이 프라이버시의 위험성에 대한 인식 부족
병원 대 병원	- 일반 의료기관은 인프라의 미흡으로 정보 공유 어려움이 있다. - 일부, 대형종합병원만이 환자의 기본 진단 기록과 질병정보를 공유하고 있다. - 경우에 따라 프라이버시 제약 없이 민감한 정보를 사용할 경우 정보공유는 제한적인 범위 내에서 공유해야 한다.	- 잘못된 개인정보 유출 - 수집된 개인정보의 남용 및 도용 - 정보 공유 시, 민감한 질병기록까지 노출되면서 프라이버시 침해가 발생

4. Health Privacy Information Protection 시스템

4.1 HPIP 구성도

HPIP(Health Privacy Information Protection) 시스템은 의료정보화의 진전으로 인해 노출 위협이 증가된 환경에서 사용자(환자)가 자신의 의료정보를 편리하게 확인할 수 있도록 하는 반면, 사용자가 아닌 병원이나 약국이 환자의 기록을 이용할 경우에는 제한된 권한을 부여하여 환자의 동의에 따라 진찰 및 치료 내역을 이용할 수 있도록 한다. 이는 병원과 환자, 약국의 임무를 분리하여 최소한의 권리를 줌으로써 허가받지 않은 자들이 쉽게 환자의 민감한 의료기록 및 개인정보에 접근하지 못하도록 하여 환자의 프라이버시를 보장하고, 필요한 경우에 따라 민감한 진료정보에 대해 안전하게 공유하는 방법이다. HPIP 시스템 모델은 4가지의 주요 구성요소(1.사용자 신분확인, 2. 병원 권한 확인, 3.환자기록 접근제어, 4.환자진단)를 제시하였으며 기본 아키텍처는 그림2와 같다.

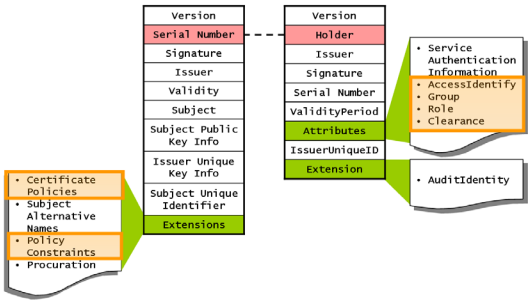


(그림 2) HPIP Architecture

4.1.1 속성인증을 이용한 신분확인 메커니즘

사용자 신분확인은 신원을 검증하고 기본 속성을 저장할 수 있는 메커니즘이다. 인증서를 통해 신분 확인 후 개인 정보 보호 정책에 준한 사용자의 속성을 그림 3과 같이 PKI의 확장 필드와 PMI를 활용하여 구현한다. 이는 사용자의 접근 권한, 임무, 역할 등의 속성 정보만을 따로 관리하는 속성 인증서를 생성하고 관리하여 시스템이 신원확인 후, 신원에 따라 주어진 그룹에 할당하고 이후 설정된 정책등급과 속성정보를 가지고 권한을 부여하여 정책 기반의 접근 제어가 이루어지도록 한다. 사용자(환자)가 요청할 경우에는 사용자 신분검사를 통해 신분을 확인함으로써 사용자는 자

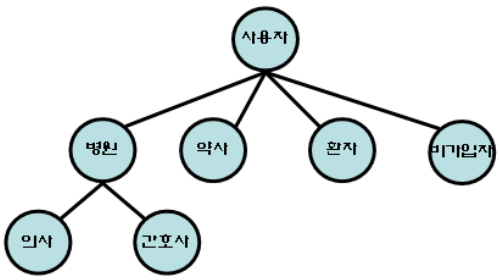
신의 개인정보(신분, 재산 및 병력)와 진료 및 처방 기록을 모두 볼 수 있다.



(그림 3) PKI와 PMI 연동방안

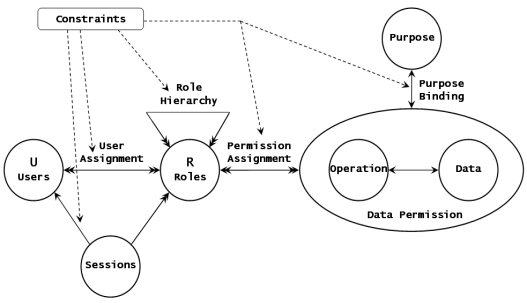
4.1.2 병원 권한확인 및 제어 메커니즘

신분확인에서 주어진 그룹에 분류되고 그룹 내에 있는 세부적인 역할에 할당이 되어서 적합한 권한이 주어진다. 권한은 조직의 구조를 유연하게 반영할 수 있는 역할기반의 접근제어(RBAC - Role Based Access Control)를 이용하여 사용자의 역할에 맞는 제한된 권한을 갖는다. 이는 권한을 개인에게 직접 부여하는 것이 아니라 조직에서 필요한 역할을 분류하여 의료업무 권한을 부여하는 것으로 시스템을 이용하는 사용자들을 편리하게 관리할 수 있고 사용자에게 할당되는 업무나 기능을 추가 및 삭제하기 용이하다. 제시된 그림4는 사용자의 역할을 계층적으로 보여준다.



(그림 4) 역할 분류

이러한 계층적으로 분류된 역할을 기반으로 접근하는 사용자 U는 PKI와 PMI의 속성값을 확인하여 R에 따라 역할을 분류하고 이 역할에 따라 개인정보 데이터를 접근할 수 있는 제한적인 권한이 부여된다. 데이터의 접근은 개인정보 요청 목적과 조건에 따라 접근이 제한되고 이용할 수 있는 권한이 달라진다. 그림 5의 제안한 RBAC 모델 적용은 의료 환경에 필요한 역할을 구분하여 시스템 사용자들을 유연하게 관리할 수 있고 의료 업무에 대해 권한을 부여하여 시스템 사용자에게 할당되는 업무 및 기능을 융통성 있게 처리할 수 있다. 또한, 병원 간의 의료 정보전달의 상호 호환성을 갖춘 시스템이 구축될 경우 환자는 병원을 방문하고 기다리는 시간/비용을 절감하면서 보다 편리하고 체계적인 의료서비스를 이용가능하다.



(그림 5) RBAC based Healthcare

(표 6) 구성요소

요소	설명
Users	HPIP 시스템을 이용하는 개개인의 사용자.
Roles	의료 업무의 책임과 권한에 관련 되는 의료 조직 내 직함. - 의사, 간호사, 환자, 약사 등
Sessions	동적으로 사용자와 역할을 할당할 수 있도록 관여
Operation	하나 혹은 그 이상의 보호된 RBAC 객체들(환자의 개인정보)의 집합에 접근하기 위한 특정 접근방식. - Read, Write, Delete 등

Data	HPIP 시스템에 의해서 관리되는 대상이며 환자의 개인정보를 말함.
Purpose	HPIP 시스템에서 환자의 정보를 이용하려는 목적들을 정의 - 처방, 진료 등
Constraints	사용자가 역할에 할당되는 조건, 역할 내 의료업무의 제한조건, 정보의 이용에 필요한 제약조건 등

(표 7) RBAC 정의

DEFINITION
- A set U of users, a set R of roles, a set D of data, a set P of purposes, a set O of operation, a set S of sessions.
- The set of Data Permissions $DP = \{(o, d) \mid o \in O, d \in D\}$.
- User Assignment $UA \subseteq U \times R$, a many-to-many mapping user to role assignment relation.
- The role hierarchy $RH \subseteq R \times R$ is a partial order on roles.
- $DPA \subseteq DP \times R$ is many-to-many permission to role assignment relations.
- Purpose binding $PB \subseteq P \times DP$, a many-to-many mapping data permission to purpose relation.

서비스 요청자가 환자의 기록을 접근하는 병원(주치의)일 경우 병원 인증을 통해 역할을 확인한다. 병원이 환자의 진단 기록을 요청했을 때 병원의 권한을 검증하고 정보 이용목적에 대한 명시를 확인하여 정의된 의료정보정책과 일치한다면, 환자기록에 접근 가능하도록 한다. 이는 의료정보화의 진전으로 e-Healthcare의 개방된 웹 환경에서 병원의 신분 확인을 통해 병원 간의 임무분리와 최소권한을 주어 환자의 개인 정보 유출 및 진료정보의 손실을 예방하고, 권한 없는 자의 정보 접근을 제어하기 위한 기능을 제공한다.

4.1.3 진료기록 접근제어

병원에서 사용자(환자)의 이전 기록을 접근 할 때, 환자의 프라이버시 보호를 위해 해당 병원의 환자의 이전 병명 및 진료 기록만을 보여주고 개인정보는 낮은 레벨의 정보만을 보여준다.

사용자에게 다른 병원에서 진찰한 진료 기록이 있을 경우 또는 보안등급이 높은 특이 질병이 있을 경우 병원이 다른 병원에게 환자의 상세진료 기록내용을 요청하고 사용자에게 진료기록 접근 여부를 Notice 기능으로 요청하여 사용자의 전 진료기록을 볼 수 있다. 아래 표8은 민감한 중요 정보에 따라 보안등급을 설정해 놓은 예이다.

(표 8) 보안등급 정책 설정 예

사용자 정보 보안등급	
P1 (Strict)	장애 여부
P2 (Cautious)	주민번호
P3 (Moderate)	주소, 연락처, 혈액형
P4 (Flexible)	나이, 직업
P5 (Casual)	ID, 이름, 성별

진료기록 보안등급	
P1 (Strict)	정신병, 질병
P2 (Cautious)	수술기록, 입원기록
P3 (Moderate)	감기, 두통, 외상
P4 (Flexible)	-
P5 (Casual)	-

이는 의료업무별 역할을 구분하여 병원과 약국, 사용자에게 임무분리 및 최소한의 권한만을 주어 환자의 진료기록에 대해 보안등급별로 접근제어 함으로써 개인 정보 유출 및 진료정보의 손실을 예방한다.

사용자가 환자의 정보 요청 시 환자의 개인정보 이용목적, 요청한 개인정보 등을 P3P의 정책설정 언어인 APPEL로 표현한다. 이는 XML로 변환되어 정보가 전달되어 진다.

그림6은 인증된 병원이 환자의 ID를 읽어 진료기록을 공유하는 목적으로 환자의 일반적인 의료기록 정보를 요청하는 예를 APPEL를 사용하여 표현한다. 데이터의 정보는 환자의 ID와 진찰날짜 및 환자의 진단 기록을 나타낸다. 환자의 의료

정보를 요청 받은 병원은 XML 기반으로 환자의 정보를 그림7과 같이 제공한다.

```
- <appel:RULESET xmlns:appel="http://www.w3.org/2002/04/APPELv1"
    xmlns:p3p="http://www.w3.org/2000/12/P3Pv1" crtdby="W3C"
    crtdon="1999-11-03T09:21:32-05:00">
  - <appel:RULE behavior="request" description="Request general medical
      information of patient">
    - <p3p:POLICY>
      - <p3p:STATEMENT>
        - <p3p:PURPOSE appel:connective="or">
            <p3p:sharePublicMedicalInfo />
          </p3p:PURPOSE>
        - <p3p:RECIPIENT>
            <p3p:AuthenticatedHospital />
          </p3p:RECIPIENT>
        - <p3p:RETENTION>
            <p3p:indefinitely />
          </p3p:RETENTION>
        - <p3p:DATA-GROUP appel:connective="or-exact">
            <p3p:DATA ref="#hospital.publicInfo.ID" />
            <p3p:DATA ref="#patient.publicInfo.ID" />
            <p3p:DATA ref="#patient.MedicalInfo.date" />
            <p3p:DATA ref="#patient.MedicalInfo.symptom" />
            <p3p:DATA ref="#patient.MedicalInfo.checkUp" />
            <p3p:DATA ref="#patient.MedicalInfo.diagnosis" />
            <p3p:DATA ref="#patient.MedicalInfo.treatment" />
          </p3p:DATA-GROUP>
        </p3p:STATEMENT>
      </p3p:POLICY>
    </appel:RULE>
  </appel:RULESET>
```

(그림 6) APPEL 변환 예

```
<?xml version="1.0" encoding="euc-kr" ?>
- <medicalInfo>
  - <hospital>
      <ID>Hospital B</ID>
    </hospital>
  - <patientRecord>
    - <patient id="1234">
        <date>2005-02-04</date>
        <symptom>tympanitis</symptom>
        <checkUp>CTscans</checkUp>
        <diagnosis>otitis media</diagnosis>
        <treatment>tympanoplasty</treatment>
      </patient>
    </patientRecord>
  </medicalInfo>
```

(그림 7) 환자정보 XML 변환 예

4.1.4 환자 진단

병원(의사)이 사용자(환자)의 진찰내용을 입력한다. 기록된 진단내용이나 병명은 보안등급 정책 설정에 따라 등급별로 기록되고 환자의 추가된 진찰내용은 병원DB와 사용자DB에 업데이트된다.

진료가 끝난 사용자의 처방내용은 약국으로 전송되고 약국은 자신의 역할에 따라 제한된 권한만 부여되어 사용자의 처방약에 대해서만 접근이 가능하다.

4.2 시스템 구현

HPIP(Health Privacy Information Protection) 시스템은 e-Healthcare의 웹 환경 내에서 개인정보보호 기반의 의료정보 접근제어를 구현하였다.

먼저, 사용자가 로그인을 하여 신분을 검증한다. 로그인시 PKI와 PMI의 정책속성 필드값을 이용하여 사용자의 역할과 권한을 확인한다. 그림 8은 개인정보 소유자(환자) 자신임이 인증되었다면 사용자 DB에 신분 확인된 사용자의 개인정보를 보여준다. 이는 크게 사용자의 신원정보 부분과 의료 진단 기록이 명시된 부분으로 구분되어 있다. 자신의 정보에 대해서는 모두 접근이 가능하다.

User ID	8502052345678
Name	Kim Kyong Jin
Sex	F
Resident Number	8502052345678
Age	23
Address	Changu-dong, Hanam Si, Gyeonggi-Do
Job	Graduate student
Academic Clique	in university
Telephone	01234567890
Payment Infomation	Credit card
Mark	0

> Medical Treatment

Date	Hospital ID	Diagnosis	Pharmacy ID
20050204	Hospital B	chronicity tympanitis	-
20040301	Hospital A	common cold	Pharm A
20030306	Hospital B	hypertension	Pharm A
20030305	Hospital A	cardiac failure	Pharm B

(그림 8) 개인정보 소유자의 진료정보 - View

인증이 된 시스템 사용자에 한에서 환자의 진료정보를 요청한다. 시스템은 필요한 최소한의 신원정보만을 제공하며 이전에 병원A에서 진료 받은 기본적인 진료기록들을 병원A에게 보여준다.

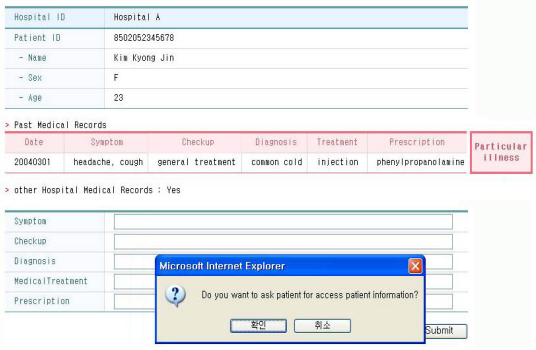
병원 내에서 진료했던 특이진단(민감한 질병)이 있을 경우 “Particular illness”를 선택하여 상세한 진료기록을 요청할 수 있다. 이 때, 개인정보가 이용되고 있는 소유자(환자)에게 confirm message를 전송하여 자신의 민감한 진료정보를 공개하는 것에 대해 알려준다. 소유자가 병원에게 자신의 정보의 접근을 허용했다면, 한 번 더 병원A의 신

```
struct PatientData
{
    Date        date;       // 진찰날짜
    PatientInfo ID;         // 환자ID
    MedicalInfo symptom;    // 증상
    MedicalInfo checkUp;    // 검사
    MedicalInfo diagnosis;  // 진료
    MedicalInfo treatment;  // 처방
}

// 민감한의료정보 요청 시
void Request_SensitiveMedicalInformation(patientID)
{
    PatientData     *medicalInfo;

    Authentication();
    Authorization();

    if (ConfirmNotice(patientID))
    {
        medicalInfo = Search_MedicalInformation(patientID);
        XMLFile(medicalInfo);
    }
}

// 확인 Notice
bool ConfirmNotice(patientID)
{
    string  contactPhone;
    bool    result;

    contactPhone = Search_PatientInformation(patientID);
    result = Notice(contactPhone);

    return result;
}
```

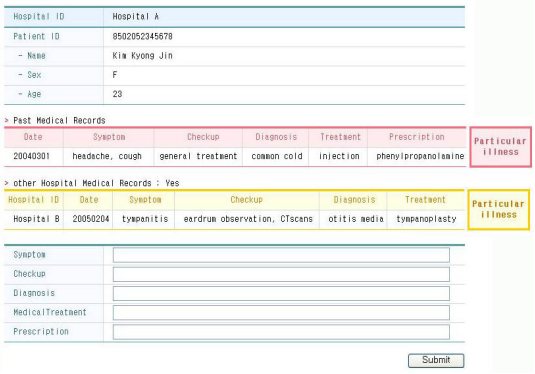
(그림 9) 민감한 진료정보 요청 - Notice

원을 확인하고 민감한 특이진단의 상세정보를 보여준다. 아래 소스코드는 Request_SensitiveMedicalInformation모듈과 ConfirmNotice모듈의 핵심적인 코드의 일부분을 보여준다. 민감한 진단정보를 요청했을 경우 환자의 동의를 얻고 상세정보를 제공한다.

환자가 병원 B에서 진료 받은 기록이 있다면 병원 A는 병원 B에게 환자의 의료정보기록을 요청하여 환자의 진료정보를 공유한다. 병원의 권한에 따라 일반적인 진료기록만을 접근하게 하고, 허가된 병원에 한하여 특이질병(민감한 진료정보)을 보여준다. 이 때, 환자에게 confirm message를 전송하여 동의를 얻고 민감한 진료정보기록을 제공한다. 그림10은 병원 A에서 보는 환자의 일반적인 진료기록이다. 여기서 Other Hospital Medical records가 있을 경우에 다른 병원에 환자의 이전 진료 기록을 요청할 수 있다. 그림11은 다른 병원에서 환자의 일반적인 진료정보를 제공한다.



(그림 10) 다른 병원에서 환자의 진료정보 요청



(그림 11) 환자의 진료정보 공유

환자진료 기록은 환자의 사생활 보호뿐만 아니라 의료 과실에 관한 법적 소송에서 매우 중요한 요소이므로 병원이 사용자의 진료기록을 이용하려 할 경우 Notice 기능으로 사용자에게 요청함으로써 사용자에게 개인정보에 관한 권리를 갖게 하고, 정보의 위·변조 및 프라이버시 침해를 예방할 수 있다.

5. 결론 및 향후 계획

의료정보화의 발전으로 정보 사용범위가 넓어지면서 프라이버시 침해가 증가하고 있음에도 현 국내 법적으로나 정보보호 인프라의 기술이 미흡한 상태이며 이를 해결하기 위해서는 새로운 해

결책이 필요하다는 인식이 점차 확산되고 있다. 의료정보화 패러다임의 새로운 전환점이라 할 수 있는 e-Healthcare는 현재 국내에서 새로운 기술들의 개발과 함께 정책 및 법제도를 추진 중이고, 일부 대형 종합병원에서 EMR 도입 및 진료 정보 공유가 이루어지고 있지만, 정보보호 위협이라는 문제점을 해결해야 올바른 발전을 할 것이다.

그 기반시스템으로 제안한 HPIP(Health Privacy Information Protection) 시스템은 역할기반의 접근제어를 통해 민감한 정보에 대한 프라이버시 침해 및 권한 남용 예방에 효과적이며, 사용자 승인에 따른 병원간의 정보공유는 안정적인 e-Healthcare 서비스로 확대되는데 기여할 수 있다.

향후, e-healthcare 시스템 구축을 뒷받침하는 국내 개인정보보호법 기반의 정보이용 방안을 역할기반 접근제어 모델에 적용함으로써, 프라이버시 접근통제 방안에 대해 연구를 계속하여, e-Healthcare가 안정적인 서비스를 할 수 있게 한다.

참 고 문 헌

[1] 정영철, “e-Health 정책동향 및 대응방안”, 보건복지포럼, 2006.

[2] 주지홍, “e-Health 산업발전을 위한 법제도 검토”, 한국법정책학회, 2006.

[3] Song Han, Geoff Skinner, Vidyasagar Potdar, Elizabeth Chang, ″A Framework of Authentication and Authorization for e-Health Services″, SWS’06, 2006.

[4] Kart, Firat Miao, Gengxin Moser, L. E. Melliar-Smith, P. M., ″A Distributed e-Healthcare System Based on the Service Oriented Architecture″, SCC 2007. IEEE International Conference on, Vol. 9, pp.652-659, 2007.

[5] David T. Fetzer, O. Clark West, ″The HIPAA Privacy Rule and Protected Health Information: Implications in Research Involving DICOM Image Databases″, Academic Radiology, Vol. 15, pp.390-395, 2008.

[6] Jun Choe, Sun K. Yoo, ″Web-based secure access from multiple patient repositories″, International Journal of Medical Informatics, Vol. 77, pp.242-248, 2008.

[7] 정영철, 최은진, “e-Health 유형분류 및 국내현황”, 보건복지포럼, 2006.

[8] 김동수, “의료정보화 패러다임의 전환: 병원정보화에서 e-Health, u-Health로”, Information Industry, 200.

[9] 이승현, “미국 Healthcare Information Technology 정책 및 추진현황”, 『정보통신정책』, 제18권, 제10호 통권 394호, 2006.

[10] A list of privacy surveys, Available at http://www.w3.org/P3P/p3pfaq.html.

[11] 김동수, 김민수, “e-Health 시대의 진전에 따른 의료정보보호 쟁점 및 정책방향”, 『정보화정책』, 제13권, 제4호, pp. 128-148, 2006.

[12] 이재영, 유선실, 권지인, “디지털 컨버전스 환경에서의 신산업활성화 전략연구”, 정보통신정책, 2007.

[13] David F. Frraiolo, Ravi Sandhu, Servan Gavrila, D. Richard Kuhn, Ramaswamy Chandramouli, “Proposed NIST Standard for Role-Based Access Control″, ACM Transaction on Information and 시스템 Security, Vol. 4, No. 3, pp. 224-274, 2001.

[14] Lorrie Cranor, Marc Langheinrich, ″A P3P Preference Exchange Language 1.0(APPEL 1.0)″, W3C Working Draft, 2002.

[15] ITU-T, “ITU-T Recommendation X.509. Information Technology : Open Systems Interconnection - The Directory : Public Key And Attribute Certificate Frameworks″, ITU-T, 2000.

[16] DAVID F.FERRAIOLO, RAVI SANDHU, SERVAN GVRILA. “Proposed NIST Staandard for Role-Based Access Control″, ACM Transactions on Information and System Security, Vol. 4, No. 3, 2001.

◐ 저 자 소 개 ◑

김 경 진 (Kyong-Jin Kim)
2007년 성신여자대학교 컴퓨터정보학부 졸업 (학사)
2007년~2009년 성신여자대학교 대학원 전산학과 (석사)
2009년~현재 성신여자대학교 대학원 전산학과 박사과정
관심분야 : 접근제어, 프라이버시 보호
E-mail : kyongjin@sungshin.ac.kr

홍 승 필 (Seng-Phil Hong)
1993년 Indiana State University (학사)
1994년 Ball State University (석사)
1997년 Illinois Institute of Technology (박사수료)
2002년 KAIST(구 ICU) (박사)
1997년~2005년 LG CNS Systems, Inc.
2005년~현재 성신여자대학교 IT학부 조교수
관심분야 : 접근제어, 통합인증, 정보보호 아키텍처, 유비쿼터스 보안, 프라이버시 보호
E-mail : philhong@sungshin.ac.kr