EHR System에서 개인정보보호를 위한 개선된 RBAC 모델에 관한 연구

안은경* · 김병훈* · 이동휘* · 김귀남*

요 약

의료기관에서 환자의 개인건강정보는 진료를 위해 의료진의 정보열람이 반드시 필요한 사항이다. 그러나 이러한 정보의 불필요한 노출은 개인정보보호와 관련이 있어 민감하게 취급되어야 하며, 의료기관에 종사하는 사용자들이라 할지라도 접근에 있어 역할에 따른 제한이 필요하다. 따라서 본 논문에서는 의료진과 그 이외의 직원들 간의 사용자 식별을 통한 개인건강정보의 접근 통제뿐만 아니라 업무에 따른 조건을 추가하여 사용자 직종 내에서도 상황에 따른 접근 통제에 대해 연구하였다. 응급상황, 담당과 여부에 따른 접근 통제, 그리고 환자가 정하는 본인의 개인정보에 대한 접근통제를 포함하여 확장된 개념의 역할기반 접근제어를 함으로써 의료기관 내에서 환자의 개인건강정보의 불필요한 접근이나 유출을 최소화 할 수 있다.

A Study on Advanced RBAC Model for Personal Information Security Based on EHR(Electronic Health Record)

Eun Kyoung Ahn* · Byung Hoon Kim* · Dong Hwi Lee* · Kui Nam Kim*

ABSTRACT

In medical Institution, Electronic Health Record (EHR) is "must access information" to medical staff considering it as medical information. However, this unnecessary exploration of personal information must be treated confidentially because the information is highly related to other's private concerns. It is necessary that medical workers should be also restricted to their access to EHR depending on their roles and duties. As the result, this article explains that "EHR access control will be executed by differentiating authorized medical staff from non medical-related staff as well as EHR access will be only permitted to authorized medical staff depending on their work status conditions. By using Advanced RBAC model on medical situation, we expect to minimize unnecessary leak of EHR information; especially, emergency medical care is needed, access control is highly required depending on a person in charge of the cases or not, and restricted medical information defined by the patient oneself is only allowed to be accessed.

Key words : EHR(Electronic Health Recode), RBAC(Role-Based Access Control)

접수일 : 2009년 6월 3일; 채택일 : 2009년 6월 18일

* 경기대학교 정보보호, 산업보안학과

1. 서 론

각 산업 분야별로 소비자 중심의 서비스로 그 형태가 전환되어 감에 따라 의료서비스에서도 기관 중심이 아닌 개인 중심의 의료정보서비스를 요구하는 목소리가 높아지고 있다. EHR(Electronic Health Recode) System은 전자건강정보로써 의료기관에서 사용되어지는 개인건강정보를 관리하는 정보체계를 말한다. 즉, 전자의무기록을 일컫는 말이다. 또한 이러한 요구에 맞추어 보건의료정보의 PHR(Personal Heath Record)로의 개념의 변화도 함께 이루어지고 있다[1].

미국의 경우 1996년 이미 의료보험과 관련하여 보건의료정보의 교환과 책임에 관해 HIPAA(Health Insurance Portability and Accountability Act)가 제정된 바 있다. HIPAA Security Rule은 전자문서 형태의 보건의료 정보의 기밀성, 무결성, 가용성을 보호하기 위한 규정으로 의료보험기관, 의료서비스 제공자, 그 외 건강관리 프로그램 등에 적용되고 있다[2].

우리나라에서는 2002년 의료법 개정을 통해 원격의료 및 전자의무기록 관련 규정이 도입되었으며, EHR 핵심공통기술 연구개발 사업단에서 보건복지가족부의 국가 보건의료 정보화 사업 추진에 따라 2006년부터 개인건강정보보호를 위한 보안체계와 지침을 개발 중에 있다. 또한, 2008년 개정된 정보통신망 이용촉진 및 정보보호에 관한 법률에 따르면, 확대된 준용기관에 의료기관이 포함되어 보건의료정보의 보안체계 정립과 시행이 매우 시급함을 알 수 있다[3].

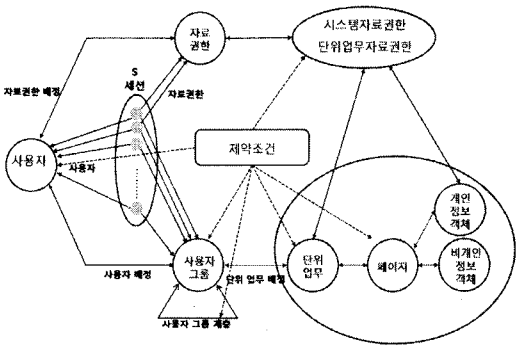
의료서비스가 진화할수록 개인의료정보의 유출로 인한 프라이버시 침해 위협, 생명 윤리 문제, 의료정보 관리 문제 등의 역기능은 현재보다 다양해지고 복잡해질 것이다. 더군다나 e-Health 및 u-Health의 진행에 따라 보안관리가 요구되는 환경의 물리적 영역이 의료기관에서 사용자의 공간으로 점차 확장될 것이다.

환자의 건강 및 의료 정보는 개인정보보호의 대상이 되므로 매우 민감하게 취급되어야 하며, 철저한 보안 정책이 요구 된다. 의료정보 보안관련 사고에 대처하기 위한 요구조건을 충족시키기 위해서는 사용자의 행위를 통제할 수 있는 수단이 필요하다. 따라서 의료기관에 개인정보보호의 관리감독 규제를 위하여 개선된 RBAC 모델을 적용할 것을 제안한다.

2. 관련 연구

2.1 확장(형) RBAC 모델

개인정보보호를 위한 확장(형) RBAC 모델의 장점은 법 문헌상 제시하는 개인정보보호 개념을 시스템에 반영하여 보안성이 향상되었다는 점이다. 그러나 이 연구에서는 정보 객체의 관점에서 개인정보 접근 흐름과 어떤 업무에서 누가 정보를 활용하였는지를 감시하는 방법을 세분화하지 못하였다. 이 모델에서 개인정보의 흐름을 정교하게 제어하지 못한 점이 아쉬운 부분이다[4].



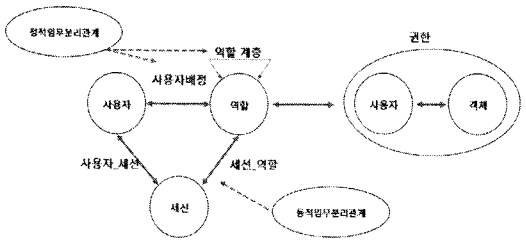
(그림 1) 확장(형) RBAC 모델

2.2 RBAC 환경에서 접근권한 기반 임무 분리 모델

이 모델은 초기 RBAC 모델에서 제약조건의 한

유형으로 언급된 임무 분리를 적용한 모델이다. 역할이 아닌 접근권한 기반의 임무분리 모델과 새로운 역할 활성화 규칙 및 안전한 위임 규칙을 제안하였다.

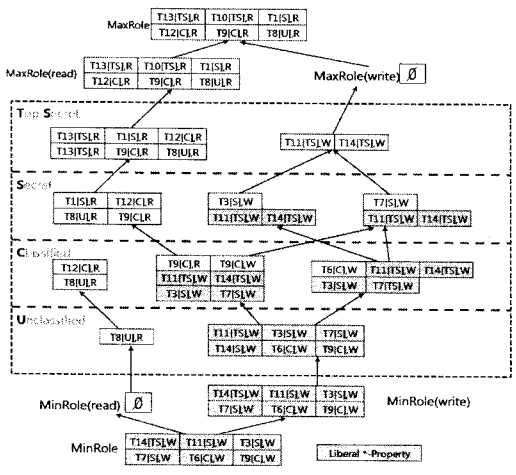
그러나 여기에서도 하위역할로부터 접근권한을 계승 받게 되어 발생하는 임무분리의 원칙에 위배되는 RBAC 모델이 가지는 근본적 문제를 가지며 이를 해결하기 위해서는 모델 자체를 변경해야 하는 제한점을 가진다[5].



(그림 2) 역할기반 접근제어 환경에서 접근권한 기반 임무 분리 모델

2.3 RBAC을 기반으로 한 데이터베이스 보안모델

다중 등급을 가진 데이터베이스와 사용자 간의 상·하위 사용자를 구분하여 등급에 따른 접근제어를 하여 데이터의 무결성을 유지하기 위한 역할 그래프를 설계하였다. 등급이 설정되어 있는 table을 각 등급에 맞는 사용자가 접근할 수 있도록 등급별로 구분하여 MAC의 simple security property를 적용하고, 각 등급별 객체의 한계를 설정하여 관리자가 역할 그래프를 탄력적으로 유지할 수 있도록 하였다.



(그림 3) RBAC을 기반으로 한 데이터베이스 보안모델

그러나 관리자가 등급을 관리함으로 인해 권한의 계층의 설정에 있어 주관성이 개입될 소지가 있는 것이 문제이다[6].

3. EHR System에서 개선된 RBAC 모델의 연구

EHR System에서 사용자에게 접근제어 제약을 가지는 새로운 모델을 적용하여 환자의 개인정보 보호를 도모하려고 한다. 그러나 앞에서 살펴본 기존의 RBAC 모델에서는 해답을 찾기가 힘들었다. 다수의 사용자와 대량의 데이터를 다루고 있으며, 사용자와 데이터가 계속 증가한다는 측면에서 의료정보는 학교 교무업무 시스템과 비슷한 점이 있다. 의료정보 전송에 있어 정보의 주체에게 기본적인 권한이 부여되어야 하는 것도 같은 점이다. 그러나 응급 상황, 의학적 지식의 불균형으로 인한 판단력의 차이 등 환자에게 모든 권리를 부여할 수 없는 것이 의료상황이므로 앞에서 언급된 모델을 그대로 적용하는 것은 부적절하다. RBAC 모델에서 개인정보 전송의 접근권 및 통제권을 행사하는 데 예외의 상황을 포함한 프로토콜이 필요하다. 사용자 그룹에 따라 사용자의 권한이 의사, 간호사, 약사 등 의료인에서부터 영양사, 원무팀 직원 등 접근하는 의료정보 수준과 직접적 관련성에 있어 분야 별로 차이가 있다. 그러므로 이 차이에 의한 정보 접근도 통제할 수 있어야 한다.

또한, 기존 RBAC 모델의 접근권한에 임무분리를 적용하게 되는 경우, 각 그룹별로 접근권의 범위를 따로 설정하고 역할계승을 차단할 수 있다. 따라서 역할 계층에 따른 임무 분리의 원칙에 위배되는 상황을 예방할 수 있다.

마지막으로, 데이터 보안의 측면에서, 개인의료정보의 데이터베이스는 정보의 성격에 따라 다중등급을 적용하여 관리되어야 한다.

3.1 개념의 정의 및 작업 흐름

3.1.1 정보 구분

접근통제와 관리를 용이하게 하기 위하여 보안과 통제의 대상이 되는 개인의료정보를 각 그룹별 특성에 따라 구분하고, 그 중에 정보의 주체(환자)가 정의한 비밀에 해당하는 정보를 구분하였다<표 1>.

〈표1〉 데이터베이스 정의

da01	ID, 이름, 생년월일, 연락처, 주소
da02	키, 몸무게, vital sign, 진료과, 해당병동
da03	lab data(혈액검사, 균배양검사, 혈액형 등), 검사결과(X-ray, CT, MRI 등)
da04a	의사가 내리는 질병 진단
da04b	간호사, 응급 구조사 등이 내리는 직군진단
da05a	의사가 내는 진료처방
da05b	타 직종에서 내는 진료 및 검사처방
da06	수행하여 기록된 자료(각종 처치, 수술 등)
secret	환자가 정의한 비밀

데이터 분류에 있어 의료 데이터의 경우 다른 집단과는 차별화되는 특성을 가진다. 사람의 생명을 다룬다는 특성상 응급상황에 있어 의료행위의 주체/결정권은 의료진에게 있다. 이는 데이터 생성과 관리, 정보전송에 관한 권한이 데이터 주체(환자)의 의지에 우선하여 일부 사용자(의료인)에게 우선권이 주어진다는 뜻이다. 따라서 같은 내용을 가진 데이터라 할지라도 상황(예, 응급)에 따라 사용자 권한의 구분이 필요하다.

3.1.2 사용자 그룹 구분

EHR System에서 환자 개인의료정보에 접근하는 그룹은 다양하다. 그에 따라 접근 가능한 정보를 최대한 제한하기 위하여 정보접근별 그룹으로 사용자 그룹을 구분하였다. 개별 사용자는 특정 사용자 그룹에 소속되어 그룹 별 역할을 수행할 수 있는 권한을 얻게 된다.

〈표 2〉 사용자 그룹 정의

U1	진료과 의사	U8	조무사, 보조원
U2	병동 간호사	U9	원무팀
U3	약사	U10	의무기록팀
U4	임상병리사, 검사실	U11	보험팀
U5	물리치료사	U12	행정팀(총무, 인사관리, 경리)
U6	영양사	U13	정보관리팀
U7	응급구조사		

3.1.3 권한배정

각 데이터 별로 기록하기, 수정하기, 열람하기, 관리하기의 4가지 업무권한이 주어지게 되며, 이는 사용자 그룹에 따라 복합적으로 조합되어 분배된다. 이 중 응급진료에 한해 일부 사용자에게 접근권한이 더 광범위하게 부여되게 되나, 일시적인 권한부여이므로 응급상황에 이루어졌던 의료행위와 관련된 정보는 보호가 가능하다. EHR System에서 부여받는 권한은 <표 3>과 같이 정해 두었다.

〈표 3〉 권한 정의

RC	Recoding
AD	Adjustment
RD	Reading
MN	Management(not reading informations, but adjustment database)

3.1.4 역할 배정

정보 구분에 따라 사용자는 각 역할 별 권한에 따른 데이터 접근 역할분리가 되어 있다. 기본적으로 직군에 따라 사용자 그룹이 정해졌으므로, 정적 임무분리가 적용된다. 각 단위업무에 따른 사용자 권한은 그룹별로 정해지게 되며, 권한이 부여된 상태에서 해당 직무를 수행하게 된다. 다만, 사용자 그룹 중 U1과 U2 집단은 예외의 경우를 가진다. 환자가 소속된 과의 경우 두 그룹은 그들이 가진 권한을 모두 사용할 수 있지만, 환자가 소속되지 않은 과의 사용자는 모든 권한을 가질 필요가 없다.

응급 진료에 있어 환자 진료에 차질이 생기지 않도록 응급 진료에 관한 조건은 별도로 설정해 두어야 한다. 이를 위해 모델에서는 동적 임무분리를 적용한 역할 배정의 과정이 한 번 더 포함되게 된다. 사용자들은 자신이 속한 그룹이 가지는 권한으로 데이터에 접근할 수 있으며, 이는 불필요한 접근을 최소화한다. 이러한 분리는 원활한 업무를 보장하여 모델의 유용성을 유지한다.

(1) 역할 배정 I(정적임무분리)

사용자가 로그인 하였을 때, 사용자 그룹을 지정하기 위한 역할 배정이다. 로그인을 하게 되면, 사용자 정보 데이터베이스에 있는 자료를 확인하여, 사용자가 권한을 부여받게 된다. EHR System에 있어 사용자 그룹별 역할 배정은 <표 4>와 같다.

(2) 역할 배정 II(동적임무분리)

응급 진료와 담당과 경우를 구분하기 위한 역할 배정이며, 사용자가 U1, U2 그룹에 속하는 경우가 이에 해당된다. U1의 경우, 응급진료와 담당의 여부를 알아보기 위하여 조건 함수를 적용하여 특정 키 값을 부여한다. 응급실에 환자가 도착한 경우, 응급실에서 로그인을 하는 U1 그룹의 사용자는 키 값 '^'을 부여받지 않게 되고 U1의 권한을 가지고 환자에 대한 업무를 수행하게 된다. 그런 다음 상황이 진행되어 환자가 특정 진료과에 배정이 되면, 응급진료 상황이 종료된 것이므로, 응급실에서 로그인했던 사용자는 키 값을 부여받아 U1이 가지는 권한을 상실하게 된다. 이처럼 담당과가 아닌 의사는 키 값 '^'을 가지게 되고 이 사용자 그룹은 'U1+^'의 권한을 배정받아 그에 해당하는 일부 권한을 부여받게 된다.

〈표 4〉 사용자 그룹별 역할 배정

그룹	데이터(업무) 구분	권한 RC	AD	RD	MN	그룹	데이터(업무) 구분	권한 RC	AD	RD	MN
U1	da01, da02, da03, da04a, da05a, da06, scr.	O	O	O	X	U7	da01, da02, da03, da04a, da05a	X	X	O	X
	da04b, da05b	X	X	O	X		da04b, da05b, da06	O	O	O	X
U1+^	da01, da02, da03, da04a, da04b, da05a, da05b, da06, scr.	X	X	O	X	U8	da01, da02	X	X	O	X
U2	da01, da02, da04b, da05b, da06	O	O	O	X	U9	da01, da02, da04a, da05a	X	X	O	X
	da03, da04a, da05a, scr.	X	X	O	X						
U2+^	da01, da02	X	X	O	X	U10	da01, da02	X	X	O	X
U3	da01, da02, da03, da04a, da05a	X	X	O	X	U11	da01, da02, da04, da05a, da05b, da06	X	X	O	X
	da06	O	O	O	X						
U4	da01, da02, da03, da04a, da04b, da05a	X	X	O	X	U12	모든 환자 정보	X	X	X	X
	da05b, da06	O	O	O	X						
U5	da01, da02, da03, da04a, da04b, da05a, da05b	X	X	O	X	U13	da01, da02, da03, da04a, da04b, da05a, da05b, da06, scr.	X	X	X	O
	da06	O	O	O	X						
U6	da01, da02, da03, da04a, da04b, da05a, da05b	X	X	O	X						
	da06	O	O	O	X						

〔응급구분함수〕

user(a) ∈ Emergency state, user(a) ∈ U1 ⇒ user(a) = 'U1'

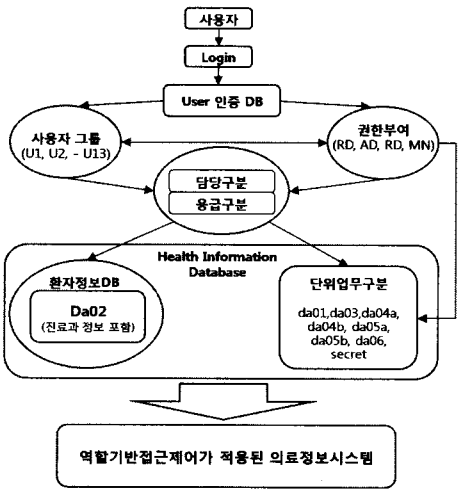
〔담당구분함수〕

user(b) ∉ Emergency state, user(b) ∈ Correct part, user(b) ∈ U1 ⇒ user(b) = 'U1'
user(c) ∉ Emergency state, user(c) ∈ Correct part, user(c) ∈ U1 ⇒ user(b) = 'U1+^'

U2의 경우도 마찬가지 방식으로 동적 임무분리가 적용되어 환자의 정보와 관련된 업무 처리에 있어 불필요한 노출을 줄일 수 있다. 또한 권한이 없는 사용자가 자료를 입력하고 수정하는 것을 제한한다.

3.2 각 단계별 권한/역할 배정을 통한 개선된 RBAC 모델

다음 (그림 4)는 권한/역할 배정을 통한 업무처리 순서를 도식화한 것이다. 사용자가 로그인을 하면, 사용자 DB에서 사용자 인증을 하고, 사용자 그룹을 확인하고 상황(담당, 응급, 비밀)에 대한 권한 통제 확인 과정을 거친다. 사용자에게 권한이 부여되면, 환자의 진료과 정보와 비교하여, 사용자는 단위업무에 대한 권한을 부여 받는다. 이에 업무를 진행할 수 있는 Page에 위의 조건을 만족한 업무만 활성화 되어, 개선된 역할기반 접근제어 기능이 적용된다.



(그림 4) 개선된 RBAC based on EHR system

기존의 EHR System에서 RBAC 모델의 경우 응급환자나, 다른 과로의 진료의뢰 환자에 있어 업무수행의 용이함을 위하여 모든 직종에 모든 권한을 부여하고 있다. 그러나 개선된 RBAC 모델을 적용하는 경우 이처럼 불필요한 정보의 노출을 줄이면서, 원활한 업무의 흐름을 보장하게 된다.

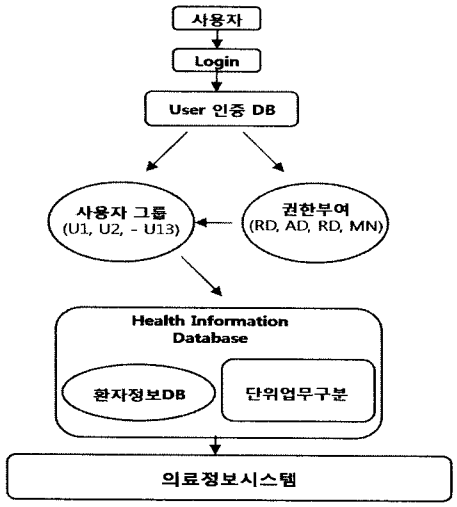
user(a) ∈ Emergency state, user(a) ∈ U1 ⇒ user(a) = 'U1'

응급실에 위급한 환자가 도착한 경우, 이 환자는 진료과의 어느 곳에도 속하지 않으나, 검사 혹은 처방을 필요로 하며, 의료 처치를 받아야 한다. 이러한 경우 응급구분에서 함수의 적용을 받아 해당과 의사가 아닌 의사, 혹은 간호사도 일시적으로 환자에게 처치를 할 수 있다. 상황이 안정되고 환자의 진료과가 정해진 다음에는 담당 구분 함수의 적용을 받아 담당 의사, 혹은 간호사가 업무를 이어받아 수행하게 되므로, 업무의 흐름이 끊어지지 않고 환자에 대한 치료는 지속되게 된다. 또한 응급실에서 이 환자를 처치했던 의료진과 담당 과에서 처치를 하게 되는 의료진 사이의 이중 처방 및 수행을 예방할 수 있어 불필요한 의료서비스를 방지할 수 있다는 부수적인 효과도 생길 수 있다.

4. EHR 환경에서의 RBAC과 개선된 RBAC 제안모델의 정보접근 비교

EHR System은 모두 RBAC 방식을 따르고 있다. 병원에 종사하는 직원이나 의료인에게 환자 정보의 일부는 불필요한 노출이 불가피하다. 이 경우 사용자가 속하는 그룹에 따라 그에 해당하는 역할과 권한을 모두 부여 받게 되므로, 의사와 간호사, 약사 등 타 직종간의 접근제어는 가능하다. 그러나 동일 그룹 내에서 환자의 담당이 아닌 의료진이 정보에 접근하는 것은 차단할 수 없었다(그림 5).

본 논문에서는 정보의 노출을 최소화 하여 개인정보보호의 제도적 흐름에 발맞추어 갈 수 있도록 접근제어 조건을 추가한 개선된 RBAC 모델을 제안하였으며 기존의 모델과의 비교를 통해 그 유의성을 검증해 보겠다.

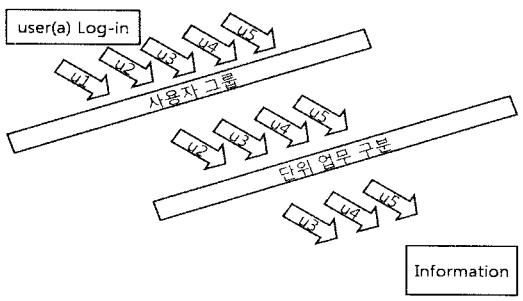


(그림 5) 기존 EHR system에서의 RBAC 모델

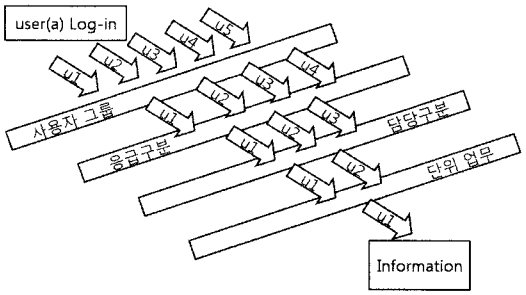
4.1 정보접근 비교 환경

RBAC 모델을 사용하고 있는 EHR system과 개선된 RBAC 모델을 적용할 수 있는 환경은 기본적으로 동일하다. 로그인을 통한 사용자 인증과정 후 시스템에 접근하게 되며, 이에 사용자 그룹별 업무에 적합한 권한을 부여받아 직무를 수행한다. RBAC 모델에서 사용자 그룹에 따라 권한과 역할의 부여가 이루어졌다면, 개선된 RBAC 모델에서는 담당과 응급이라는 상황에 따라 사용자의 권한과 역할이 달라진다.

동일한 의료 환경에서 환자 정보에 접근함에 있어 임의의 사용자는 정보사용이 가능한 그룹의 소속 여부와 단위업무에 따라 특정 다수의 접근이 가능하다. 그러나 개선된 RBAC 모델을 적용한 경우, 임의의 사용자 접근에 있어 기존의 통제 뿐 아니라 상황에 따라 소수의 특정인만이 접근이 가능하다.



(그림 6) 동일 환경 내 RBAC 모델 적용 시 사용자 접근 정도



(그림 7) 동일 환경 내 개선된 RBAC 모델 적용 시 사용자 접근 정도

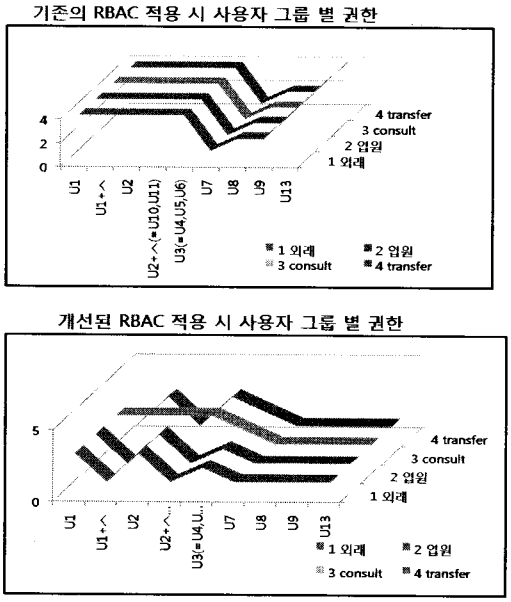
4.2 정보접근 비교

기존의 RBAC 모델과 개선된 RBAC 모델에서 각 사용자별 정보 접근 시도를 상황별로 비교한 결과는 다음과 같다.

먼저, 일반적인 상황에 대한 비교이다. 외래를 경유하여 병원에 입원하게 되는 경우, 환자가 외래에 도착하였을 때 기존의 RBAC 모델은 각 직군별 사용자에 있어 권한의 변동이 거의 없다. 외래를 경유하여, 입원하고, 환자가 타과 진료의뢰, 전과되는 과정에 있어 담당 의사여부, 해당 병동 간호사 여부에 상관없이 동일한 권한을 가지게 된다. 또한 행정, 원무, 보험팀의 사용자는 부서와 상관없이 EHR system에 접속하면 환자의 정보를 볼 수 있는 권한이 부여된다. 정보관리자의 경우 환자의 정보와 관련된 모든 권한을 가지고 있으며, 타 사용자의 요청에 따라 정보 수정이 가능하다.

반면, 개선된 RBAC 모델의 경우에는 환자가 외래를 거쳐 입원, 타과 진료의뢰 과정까지 외래, 병동, 진료의뢰 받는 과에 해당하는 각 과 담당 의료진만이 해당 권한을 가진다. 일단 다른 과로 전

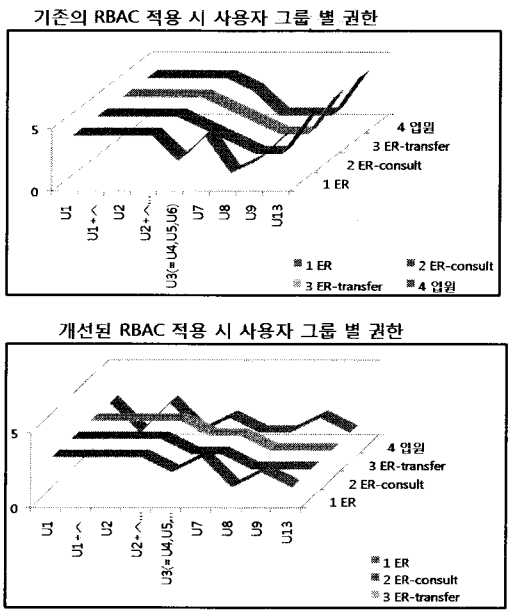
과가 되고나면, 기존의 담당 사용자는 권한을 잃게 되고, 변경된 과의 의사가 담당의 권한을 새로 가지게 된다. 다른 사용자 그룹에 관해서도 마찬가지 규칙이 적용된다.



(그림 8) 외래 경유 입원 환자에 대한 두 모델의 권한 비교

다음으로, 환자가 응급실을 거쳐 입원하게 되는 상황에 대한 비교이다. 환자가 도착한 경우 기존의 RBAC 모델에서는 일차적으로 모든 의료진이 해당 환자 정보의 접근이 가능하였으며, 권한을 모두 가질 수 있다. 이 때, 응급 구조사, 응급실 의사, 간호사의 경우 환자가 응급실을 나가 특정 과로 입원을 하게 되면 더 이상 환자정보에 접근할 필요가 없다. 그럼에도 불구하고 환자 정보 접근 권한을 가지고 있다. 또한 응급의학과 소속이 아닌 다른 과 의료진 및 실습 학생도 환자의 정보조회가 가능하다.

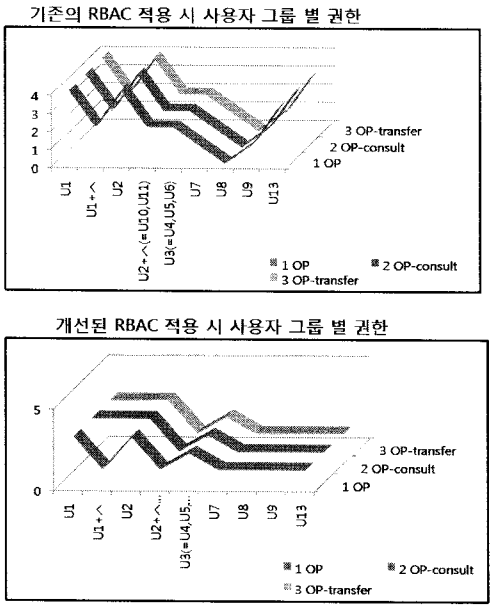
반면, 개선된 RBAC 모델은 환자가 응급실을 경유하여 해당과로 입원하는 경우 각 역할에 따른 권한을 변경시킨다. 그 환자를 담당하는 의료진만이 해당 권한을 행사할 수 있게 된다. 환자가 응급의학과에서 응급처치가 끝난 후 담당과가 결정이 되면, 환자에 대한 권한은 다시 담당과에 속하는 사용자에게 넘어가게 된다. 만약 다른 과로의 진료의뢰가 필요하여 환자 정보를 공유해야 하는 경우라면, 진료의뢰를 받은 과에서도 같은 권한을 가지게 된다. 이는 정보접근을 기준으로 보았을 때 보안등급이 높아지는 것으로 볼 수 있으며, 개인의료정보의 보호를 위해 필요한 부분이다[7].



(그림 9) 응급실 경유 입원 환자에 대한 두 모델의 권한 비교

마지막으로, 병원에서 특수 상황인 수술에 있어 환자에 대한 사용자 그룹의 권한에 대한 비교이다. 수술은 스케줄에 따른 담당 진료과가 정해져 있다. 그러므로 환자에 접근하게 되는 사용자 그룹도 정해져 있다. 수술실에서 사용자 그룹이 환자 정보에 접근하는 형태는 매우 제한 적이다. 그러나 수술 중 환자 상태의 변화나 질환에 의한 연합수술(combine op), 타과에 일부수술 의뢰 혹은 전과가 되는 경우 다시 해당 의료진에 한해 접근이 가능하게

된다. 이에 기존의 모델과 개선된 RBAC 모델에 있어 비교한 내용은 다음과 같다.



(그림 10) 수술실 환경 환자에 대한 두 모델의 권한 비교

5. 결 론

EHR System에서 생성되는 개인의료정보는 그 특성상 의료 전문가와 의료기관에서 관리되어 왔다. 자신의 정보라 할지라도 일정한 절차 없이 열람하거나 사용할 수 없도록 제한되었다. 의료정보는 수동적으로 받아들여지고 타인 의해서 생성되는 것이기 때문에 EHR System에서 개인건강정보의 보안문제는 더욱 중요해지고 있다[8].

본 연구에서 제안된 개선된 RBAC 모델은 기존의 EHR System에서 통제할 수 없었던 사용자 그룹의 역할에 따른 접근제어 기능을 개선시켰다. 이는 EHR System에서 개인의료정보 보호 정책을 강화시키는 것이며, 보안등급을 향상 시킬 수 있는 방안이다. 병원에서 다루어지는 환자(개인)의 극히 비밀스러운 건강정보는 다른 개인정보와 마찬가지로 정보에 대한 보호 정책이 반드시 필요하다. 본 연구가 제안하는 개선된 RBAC 모델은 2008년 개정된 정보통신망 이용촉진 및 정보보호에 관한 법률이 제시한 의료기관에서의 개인정보보호의 개념을 강화시켰다. 또한 그에 따른 개인건강정보 유출을 예방하는 방안으로 제안하였다.

기관의 시스템 보안을 적용하는 경우 한 가지 보안 정책으로 기관의 모든 개인정보 보안이 강화되지 않는다. 점차 보완적 모델을 적용해 가야하며, 기관 내에서 정보보호 조직을 활성화해야 한다. 또한 정책적 차원에서 통합된 가이드라인이 제시되어 모델이 보완되고 보편화 적용되는 것이 필요하다.

참 고 문 헌

[1] 정혜정, 김남현, "보건의료의 정보화와 정보보호관리 체계", 정보보호학회지, 제19권, 제1호, 2009.

[2] 김동수, 김민수, "e-Health 시대의 진전에 따른 의료정보보호 쟁점 및 정책방향", 정보화정책, 제13권, 제4호, pp. 128-148, 2006.

[3] 보건복지가족부, 보건복지정보화촉진시행계획(안). 2009.

[4] 김보선, 홍의경, "교무업무 시스템에서의 개인정보보호를위한 역할기반 접근 제어 확장", 정보과학회논문지 : 컴퓨팅의 실제 및 레터, 제14권, 제2호, 2008.

[5] 오세종, "역할기반 접근제어 환경에서 접근권한 기반의 임무분리 모델", 정보처리학회논문지, 제11-C권, 제6호, 2004.

[6] 박기홍, 김응모, "역할기반 접근제어를 기반으로 한 데이터베이스 보안모델 설계", 성대논문지, 제52권, 제1호, 2001.

[7] 이동희, "의료정보의 프라이버시 보호를 위한 확장 RBAC 설계", 충북대학교 대학원 전자계산학과 박사학위논문, 2006.

[8] Vicky Liu, William Caelli, Lauren May and Peter Croll, "Open Trusted Health Informatics Structure(OTHIS)", 2nd Australasian Work -shop on Health Data and Knowledgement, Wollongong, Australia, 2005.

[9] Calvin S. Powers, Paul Ashley, Matthias Schunter, "Privacy Promise, Access Control and Provacy Management", Proc. of the 3rd International Symposium on Electronic Commerce, IEEE, pp. 13-21, 2002.

[10] J. B. D. Joshi, B. Shafiq, A. Ghafoor, and E. Bertino, "Dependencies and separation of duty constraints in GTRBAC", Proc. of the 8th ACM symposium on Access control models and technologies, 2003.

안 은 경

2003년 아주대학교 간호학부 (간호학사)

2009년 아주대학교 보건대학원 보건정책과 관리(보건학 석사)

2009년 경기대학교 산업보안학과 박사과정

김 병 훈

2008년 안양대학교 전기전자 공학과(공학사)

2008년 경기대학교 정보보호학과 석사과정

이 동 휘

2000년 경기대학교 전자계산학과 (이학사)

2003년 경기대학교 정보보호 기술공학과(공학석사)

2006년 경기대학교 정보보호 학과 박사

현재 경기대산업기술보호특화센터 연구교수

김 귀 남

미국 캔자스대학교(공학사)

미국 콜로라도주립대학 (공학석사)

미국 콜로라도주립대학 (공학박사)

현재 경기대산업기술보호특화센터 센터장

현재 경기대학교 정보보호학과 교수