情報保護學會論文誌
第20卷 第4號, 2010. 8

RBAC에 기초한 통합형 프라이버시 보호 모델*

조 혁 현,[1†] 박 희 만,[1] 이 영 록,[1] 노 봉 남,[1] 이 형 효[2‡]
[1]전남대학교, [2]원광대학교

Integrated Privacy Protection Model based on RBAC*

Hyug-hyun Cho,[1†] Hee-man Park,[1] Young-lok Lee,[1] Bong-nam Noh,[1] Hyung-hyo Lee[2‡]
[1]Chonnam National University, [2]Wonkwang University

요 약

프라이버시 보호는 기업의 온/오프-라인 데이터 처리 시스템 안에서 프라이버시 정책들을 수행할 수 있을 때에 달성될 수 있다. 프라이버시 정책 모델 중에는 P-RBAC과 목적모델, 의무모델이 있다. 그러나 이들 각각의 모델들만으로는 급변하는 기업환경에 능동적으로 대처하기 어렵다. 동일한 역할에 속해있는 사용자 중 최적의 조건을 만족하는 자만을 선발하여 일정기간 새로운 임무를 부여할 수 있어야하고, 풍부한 접근제약조건 표현을 허용하여 프라이버시 보호를 강화할 수 있어야 한다. 이를 위해 우리는 목적모델과 P-RBAC 모델, 의무모델을 통합시킨 통합형 프라이버시 보호 모델을 제안한다. 그리고 우리의 모델이 구현플랫폼과 응용에 종속적이지 않고 자동화될 수 있도록 XML 기반 정책언어모델을 정의한다.

ABSTRACT

Privacy protection can only be achieved by enforcing privacy policies within an enterprise's on and offline data processing systems. There are P-RBAC model and purpose based model and obligations model among privacy policy models. But only these models each can not dynamically deal with the rapidly changing business environment. Even though users are in the same role, on occasion, secure system has to opt for a figure among them who is smart, capable and supremely confident and to give him/her a special mission during a given period and to strengthen privacy protection by permitting to present fluently access control conditions. For this, we propose Integrated Privacy Protection Model based on RBAC. Our model includes purpose model and P-RBAC and obligation model. And lastly, we define high level policy language model based XML to be independent of platforms and applications.

Keywords: Privacy Protection, RBAC, P-RBAC

I. 서 론

프라이버시 보호 관련 법률들은 개인정보를 수집/이용하는 모든 정보통신 서비스 제공자들에게 개인정보 보호를 의무화하도록 규정한다. 따라서 그들은 프라이버시 정책들을 고객에게 알리고 고객 데이터를 보호하는 전략들을 채택해 시행한다[3,4,10]. 하지만 이익을 추구하기에 그들은 의도적이든 비의도적이든 프라이버시 정책들을 위반할 수 있기 때문에 그러한 전략들만으로 고객의 개인정보를 보호할 수 있다고 말할 수 없다. 프라이버시 보호는 기업의 온/오프라인 데이터처리시스템 안에서 프라이버시 정책들을 수행할 수 있을 때 비로소 달성된다.

최근 연구되고 있는 프라이버시 정책 모델 중에는

* 접수일(2009년 2월 26일), 수정일(1차: 2009년 4월 7일, 2차: 2009년 6월 18일), 게재확정일(2009년 6월 25일)
* 본 연구는 전남대학교 시스템보안연구센터의 지원으로 수행하였습니다.
† 주저자, hhcho@jnu.ac.kr
‡ 교신저자, hlee@wonkwang.ac.kr

P-RBAC(Privacy-Aware Role-Based Access Control)과 목적모델 등이 있다. P-RBAC은 목적, 조건, 의무 개념을 RBAC에 포함시킨 모델이고 [3,4,10], 목적모델은 한 역할에 소속된 사용자들 중 일부가 특수임무를 수행할 수 있도록 조건역할 개념을 도입한 것이다[1]. 그러나 P-RBAC 모델은 목적모델의 장점인 TFT팀 구성과 협업/협진 같은 서비스를 제공하지 못하는 단점을 지니며, 목적모델은 조건이나 의무같은 프라이버시 구성요소를 반영시키지 못하는 단점을 지닌다. 목적모델의 저자들도 P-RBAC 모델과의 통합을 남겨둔 상태다.

본 논문은 위에서 언급한 각 모델들과 정책언어들을 분석하여 목적모델을 어떻게 프라이버시 모델들과 통합시킬 수 있는지, 그리고 프라이버시 보호를 보다 세밀하게 하기 위해 조건표현을 어떻게 풍부하게 할 것인지, 그리고 구현 플랫폼에 구애받지 않고 정책수행을 자동으로 할 수 있게 하기 위해 어떻게 정책표현을 고수준으로 할 것인지에 초점을 둔다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구를 다루고, 3장에서는 몇 가지 사례를 제시하고 분석을 통해 RBAC 기반 통합 프라이버시 보호 모델(Integrated Privacy Protection model based on RBAC : IPP-RBAC)을 제안한다. 4장에서는 IPP-RBAC 모델의 구성 요소들을 XML 언어로 명세하기 위한 정책언어모델을 기술하고 사례연구에 적용한다. 5장에서는 기존 접근제어 모델 및 정책언어와 제안한 모델을 비교분석 한다. 6장은 결론 및 향후 연구 방향에 대해 기술하며, 마지막 부록에는 의료정보 시스템에 적용할 수 있는 우리의 IPP-RBAC 정책 퍼미션 배정 정책을 제시한다.

II. 관련연구

프라이버시 정책과 관련된 연구로는 P3P나 EPAL, XACML 같은 프라이버시 정책 표현 언어와 프라이버시 인지 RBAC(P-RBAC) 패밀리 모델이 있다.

P3P(Platform for Privacy Preferences) [9]는 기업 웹사이트의 개인정보 수집 및 이용 정책을 컴퓨터가 읽을 수 있는 형식(machine readable format)으로 인코딩하기 위한 방법을 제공한다. 그러나 정당한 방법으로 수집된 개인정보가 어떻게 사용되는가에 대한 강제 규정이 없어 이를 추적하기 어려운 단점을 지닌다. 한편 EPAL(Enterprise Privacy Authorization Language)[6,11]는 IBM과 ZKS가 공동으로 개발한 기술로, 프라이버시 정책을 생성하기 위해 어휘(vocabulary)라는 개념을 사용한다. 그러나 어휘를 알고 있을 때에만 정책을 번역할 수 있다는 단점을 지닌다.

XACML[5]은 보안이 요구되는 자원에 대해 정교한 접근제어를 수행할 수 있는 XML기반 접근제어정책 언어로, 다양한 플랫폼에 구애받지 않고 일관된 정책설정을 허용함으로써 상호 운영성을 제공한다. 또한 XACML은 매칭기법과 조건에 사용될 수 있는 다양한 연산자와 함수들을 제공하는 장점도 제공한다. 그러나 RBAC을 XACML로 표현하려면 그의 틀에 끼워 맞춰야 하는 부담요소를 안고 있다.

최근에는 RBAC에 프라이버시 정책들을 제공할 수 있도록 프라이버시 보호 요구사항을 고려한 P-RBAC 모델[3,4,10], 조건모델, 목적기반 접근제어 모델[1,7], 의무 모델[2] 등이 연구되어 왔다. P-RBAC은 프라이버시 퍼미션을 정의하여 프라이버시를 강화하지만, 조건표현이 풍부하지 못하고 목적모델의 장점인 조건역할을 수용하지 못한다. 조건표현 언어인 LC_0는 한정된 도메인 안에서 컨텍스트 변수들과 관련된 동등성 제약만을 지원하며, 원자형식의 조건들을 논리곱(AND)으로 제한함으로써 관계연산이나 논리합을 지원하지 못한다. LC_0의 단점 중 논리합을 지원한 것이 LC_1이며, LC_1에 관계연산자를 지원한 것이 LC_2이다. 그러나 LC_2는 산술연산과 사용자 정의 함수를 지원하지 못한다.

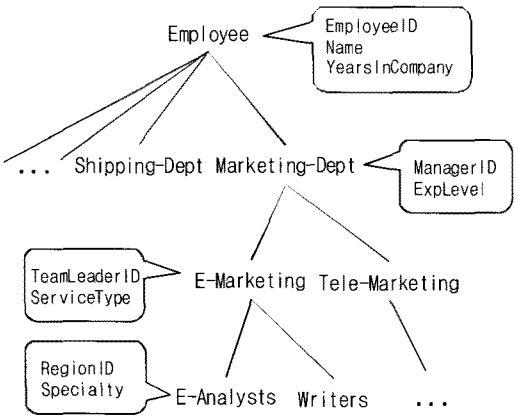
III. RBAC 기반 통합형 프라이버시 보호 모델

우리가 제안한 모델은 목적모델을 P-RBAC 모델과 통합시키는데 있다. 아울러 조건표현을 풍부하게 하기위해 XACML을 차용한다. 본 장에서는 우리가 제안한 IPP-RBAC모델을 설명한다.

3.1 프라이버시 접근제어 모델 통합의 필요성

이절에서는 기존 프라이버시 모델들에 아래의 사례를 적용해 문제점을 파악하고 해결책을 도출한다.

[가정] P-RBAC이 구현된 시스템은 [그림 1][1]의 역할계층 구조를 가지며, E-Analysts 역할이 고객의 프로파일에는 접근가능하나 E-mail에는 접근할 수 없다는 퍼미션 배정이 설정되어 있다. 또한 E-Analysts 역할에 u_1, u_2, u_3가 배정되어 있다.



〔그림 1〕 역할 계층과 역할 속성들

〔사례〕 E-Analysts에 배정된 사용자 중 유일하게 새로운 태스크 포스 팀에 소속된 u_1은 13세 미만의 고객에게 맞춤형 서비스를 고객의 E-mail을 통해 알리고자 한다.

사용자 u_1은 이제 업무수행 상 o_1(13세 미만 고객의 E-mail)에 접근할 수 있어야 한다. 따라서 보안관리자는 새 퍼미션 배정을 추가해주어야 한다.

PA_1: (E-Analysts, ((read, o_1), Service- Announcement, o_1_소유자_나이==13세이하 ∧ 부모동의==Yes, ∅)

PA_1은 "Service-Announcement 목적으로 부모동의가 있는 13세 미만의 고객주소 o_1(E-Mail)을 E-Analysts 역할이 접근할 수 있다"는 의미를 갖는데, 이 결과는 사용자 u_1뿐만 아니라 u_2, u_3, u_4까지 o_1에 접근하는 부작용을 초래한다.

위의 사례 외에도 P-RBAC 모델과 목적모델이 구현된 시스템의 사용자가 자신의 신용을 담보로 프라이버시 데이터를 구입하고자 할 때에도 문제는 발생한다. 시스템은 먼저 사용자의 신용한도액과 예금 잔액을 더하고, 그 결과가 사용자의 거래규모보다 큰지를 검사해야 하는데 P-RBAC은 조건표현에 동등성 제약만을 지원하므로 산술연산을 수행할 수 없고, 목적모델은 조건 자체를 지원하지 않는다.

개인정보 소유자는 자신의 프라이버시 강화를 위해 상황에 맞게 조건들을 변경할 수 있어야 하며 TFT팀 구성과 협업을 쉽게 할 수 있어야 한다. 따라서 위의 사례를 해결하기 위해서는 RBAC과 목적모델, 그리고 P-RBAC 모델이 통합된 RBAC 기반 통합 프라이버시 보호모델이 필요하다.

3.2 RBAC 기반 통합형 프라이버시 보호 모델

우리는 기존 RBAC과의 일관성을 위해 역할과 관련된 관계(relationship)는 배정이라는 용어로, 그렇지 않으면 바인딩이라는 용어를 사용한다.

정의 1. IPP-RBAC 모델

- 사용자, 역할, 사용자 배정, 퍼미션, 세션 - 기존 RBAC 정의와 동일하다.
- 목적트리와 객체계층 - 목적과 객체는 계층을 이룬다. 접근목적과 허용목적은 동일한 목적트리를 참조한다.
- 접근목적 배정 - 접근목적 배정은 정보 사용자의 정보이용 목적을 사전에 배정한 것이다.
- 허용목적 바인딩 - P-RBAC의 목적과 같은 개념이다. 퍼미션에 허용목적을 바인딩한다.
- 프라이버시 퍼미션 배정 - 프라이버시 퍼미션 배정은 프라이버시 퍼미션과 역할 또는 조건역할의 쌍으로 구성된다.
- 역할속성 배정 - 역할과 속성의 쌍이다.

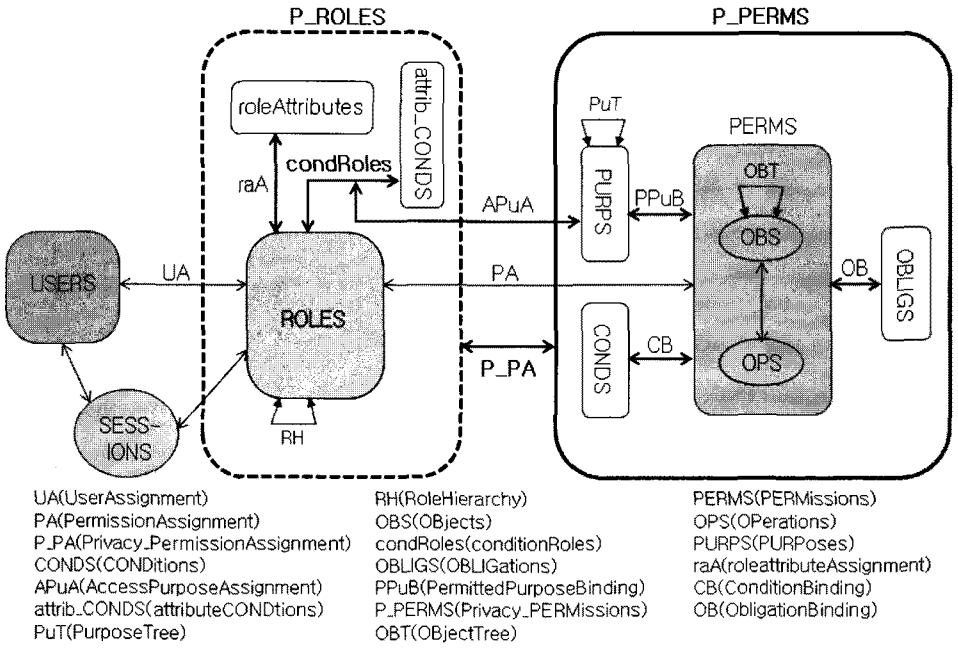
IPP-RBAC 모델을 구성하는 요소들은 〔그림 2〕와 같이 사용자 집합(USERS), 역할 집합(ROLES), 역할 계층(RH), 역할속성 집합(roleAttributes), 역할속성들로 구성된 조건집합(attrib_CONDS), 조건역할 집합(condRoles), 역할속성 배정(raA), 퍼미션 집합(RERMS), 조건 집합(CONDS), 목적 집합(PURPS), 의무 집합(OBLIGS), 목적 트리(PuT), 데이터 객체 계층(OBT), 접근목적 배정(APuA), 허용목적 바인딩(PPuB), 조건 바인딩(CB), 의무 바인딩(OB)으로 구성된다.

3.2.1 IPP-RBAC 모델의 조건 표현

우리의 IPP-RBAC 모델은 XACML의 조건 표현을 수정하여 정의한다. XACML을 선택한 이유는 산술, 관계, 논리연산은 물론이고, XPath2.0 함수와 XQuery1.0 함수, 그리고 사용자가 정의한 비표준 함수들도 허용하기 때문이다. IPP-RBAC의 조건 표현은 부록에 기술되어 있다.

3.2.2 접근목적 배정과 허용목적 배정

접근목적은 조건역할 뿐만 아니라 역할에도 배정될



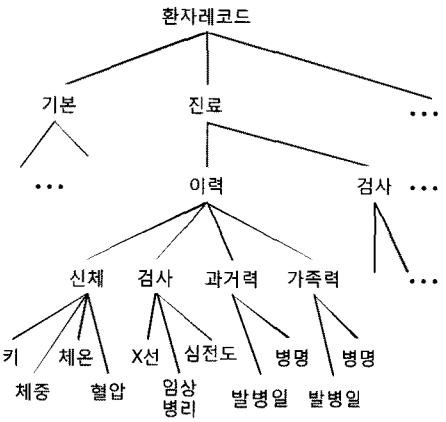
〔그림 2〕 IPP-RBAC 모델

수 있다. 허용목적 바인딩 정의는 다음과 같다.

정의 2. 허용목적 바인딩

허용목적 바인딩은 허용목적과 퍼미션들의 다대다 사상이다. 다시말해 PPuB⊆PURPS×PERMS이다. binded_purposes() 함수를 이용해 한 퍼미션에 바인드된 허용목적들을 구할 수 있다. 정형적으로 표현하면, binded_purposes(p:PERMS) ={pu∈PURPS|(pu, p)∈PPuB}. 또한 한 퍼미션에 인가된 허용목적들은 다음 함수로 구해진다.

authorized_permitted_purposes:(p:PERMS)→2^{PURPS}



〔그림 3〕 환자 진료기록 트리구조

3.2.3 데이터 객체 트리

본 모델은 보호하는 개인정보를 XML로 기술하므로 데이터의 중요도에 따라 각 엘리먼트에 연산을 묶는 퍼미션을 정의하고, 그 퍼미션에 허용목적을 바인딩한다. 〔그림 3〕은 데이터 객체의 트리구조이다.

IV. IPP-RBAC 정책언어 모델

기업의 보안 정책은 여러 부서에서 독립적으로 관리하므로 정책 수정은 고비용과 신뢰문제를 야기하며 기업전반의 통합정책 수립을 어렵게 한다[5]. 따라서 공통된 표준의 정책 언어개발이 필요하다[8].

4.1 IPP-RBAC 정책의 논리적 표현

USERS, ROLES, OBS, OPS, CONDS, raA, condRoles, roleAttributes, CB, OB, attrib_CONDS, PURPS, OBLIGS, APuA, PPuB, P_PA를 각각 사용자, 역할, 데이터 객체, 연산, 조

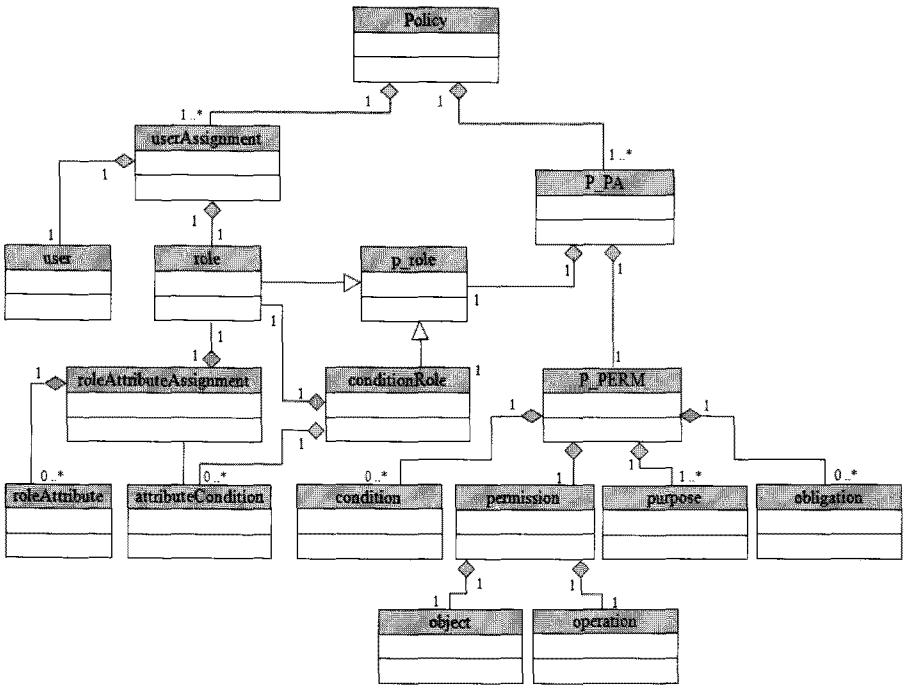
건, 역할속성배정, 조건역할, 역할속성, 조건바인딩, 의무바인딩, 속성기반 조건, 목적, 의무, 접근목적 배정, 허용목적 바인딩, 프라이버시 퍼미션 배정 집합이라 하자.

정의 3. IPP-RBAC 정책 표현

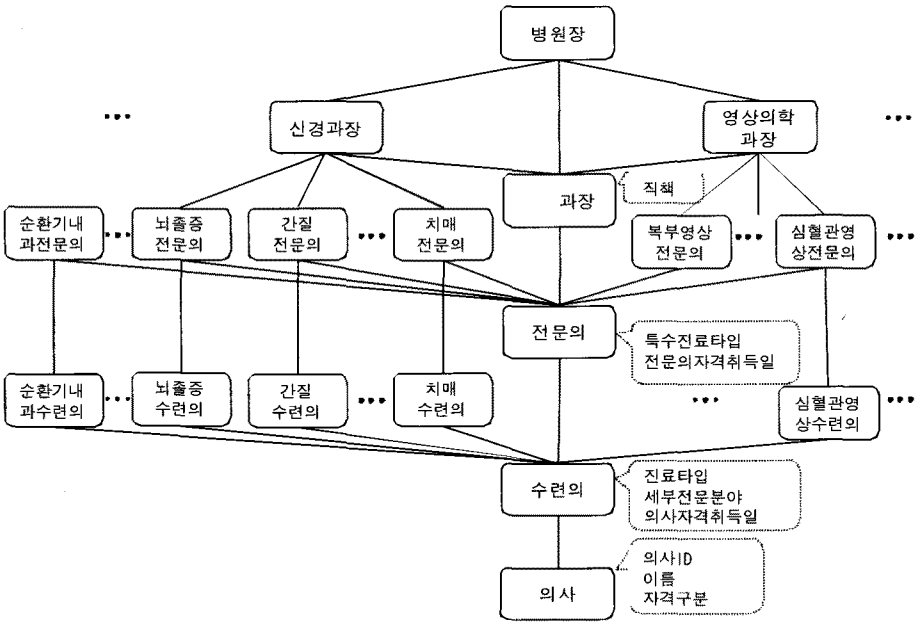
- Policy: (UA, P_PA) 정책(policy)은 사용자 배정과 프라이버시 퍼미션 배정 쌍으로 구성된다.
- UA: 기존 RBAC과 동일하다.
- P_PA: (P_ROLES, P_PERMS) 프라이버시 퍼미션 배정은 조건역할이나 역할에 프라이버시 퍼미션을 배정한 것이다. P_ROLES는 조건역할이나 일반역할로 대체될 수 있는 추상역할이다.
- condRoles: (ROLES, attrib_CONDS) 조건역할(condition role)은 역할과 역할속성기반 조건의 쌍으로 구성된다.
- attrib_CONDS: 속성기반 조건은 역할속성들의 값을 피연산자로 하는 명제논리식이다.
- raA: (ROLES, roleAttributes) 역할속성 배정은 역할과 역할속성의 쌍으로 구성된다.
- P_PERMS: (PERMS, PURPS, CONDS, OBLIGS) 프라이버시 퍼미션은 기존 퍼미션에 허용목적과 조건, 그리고 의무를 추가한다.
- PERMS: (OBS, OPS) 퍼미션(permission)들은 객체들과 연산들의 쌍으로 구성된다.
- CB: (CONDS, PERMS) 조건 바인딩은 조건들과 퍼미션의 쌍이다.
- PPuB: (PURPS, PERMS) 허용목적 바인딩은 허용목적과 퍼미션의 쌍이다.
- OB: (OBLIGS, PERMS) 의무 바인딩은 의무와 퍼미션의 쌍이다.
- APuA: (PURPS, condRoles) 접근목적과 조건역할의 쌍이다.

4.2 IPP-RBAC 정책언어 모델

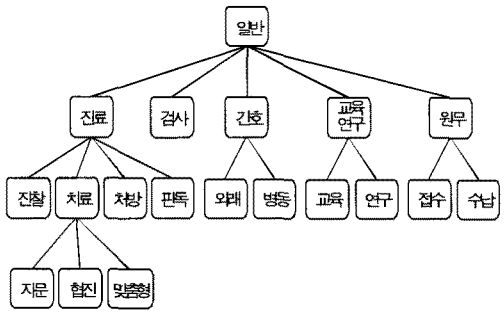
XML기반 IPP-RBAC 정책언어 모델의 클래스 다이어그램은 〔그림 4〕와 같다. IPP-RBAC 정책언어로 명시한 의료정보시스템의 퍼미션배정정책 도큐먼트 인스턴스는 부록에 제시한다.



〔그림 4〕 XML기반 IPP-RBAC 정책언어 모델



〔그림 5〕 역할속성이 배정된 역할 계층



〔그림 6〕 목적트리

4.3 적용사례

이절은 우리모델에 다음 시나리오를 적용할 때 접근제어 과정을 설명한다. 〔그림 5〕는 속성기반 역할계층을, 〔그림 6〕은 목적트리, 〔그림 7〕은 조건역할, 그리고 〔그림 8〕은 프라이버시 정책을 나타낸다. 또한 표1은 접근목적 배정, 〔표 2〕는 허용목적배정을 나타낸다.

〔시나리오1〕

환자 p는 두통을 호소하며 담당의사 u_1(두통전문의)에게 진료를 요청한다. 담당의사 u_1은 치료를 목적으로 환자 p의 치료데이터를 읽고자 한다.

결 론: 읽을 수 있다.

설 명: 시스템은 담당의사 u_1이 접근하려는 치료데이터와 관련 있는 정책 P_PA_1을 찾아낸다. 정책

CanConsult:(수련의, reqAttrID.clinic_type='자문')
CanCoWork:(수련의, reqAttrID.clinic_type='협진')
CanSpecialClinic: (전문의, reqAttributeID.doctor_licence='전문의'∧reqAttributeID.clinic_type='담당'∧reqAttributeID.special_clinic_type='선택진료'∧(reqAttributeID.detail_major='순환기내과'∨reqAttributeID.detail_major='뇌졸중'∨reqAttributeID.detail_major='두통'∨reqAttributeID.detail_major='심혈관영상')∧(system.today-reqAttributeID.specialist_licence_day〉= 10))
CanStrokePatientTailored: (전문의, reqAttributeID.doctor_licence='전문의'∧reqAttributeID.special_clinic_type='맞춤형 진료'∧(reqAttributeID.detail_major='뇌졸중'∨reqAttributeID.detail_major='감마나이프수술'∨reqAttributeID.detail_major='심혈관영상'∨reqAttributeID.detail_major='심장내과'∨reqAttributeID.detail_major='뇌신경재활')∧(system.today-reqAttributeID.specialist_licence_day〉= 10))

〔그림 7〕 조건 역할

UA_1:(u_1,두통전문의) UA_2:(u_2, 순환기내과수련의)
UA_3:(u_3,순환기전문의) UA_4:(u_4, 소화기내과수련의)
UA_5:(u_5,수면장애수련의) UA_6:(u_6, 소화기전문의)
UA_7:(u_7, 두통전문의) UA_8:(u_8,뇌졸중전문의)
UA_9:(u_9,감마나이프전문의) UA_{10}:(u_{10},심혈관전문의)
UA_{11}: (u_{11}, 심장전문의) UA_{12}:(u_{12},뇌신경전문의)
P_PA_1:(두통전문의,((환자p의 데이터,R),진료,∅,))
P_PA_2:(두통전문의,((환자p의 데이터,R),진료,∅,0))
P_PA_3:(CanConsult,((환자p의 과거력,R),진료, 자문의뢰='yes',0))
P_PA_4:(CanCoWork,((환자p의 검사데이터,R), 진료, 협진의뢰='yes', 0))
P_PA_5: (CanSpecialClinic, ((환자p의 가족력, R), 진료, 선택진료신청='yes', 0))
P_PA_6: (CanStrokePatientTailored, ((환자p의 진료데이터, R), 진료, 맞춤형진료신청='yes', 0))

〔그림 8〕 프라이버시 정책

P_PA_1은 "두통전문의가 환자 p의 치료데이터를 진료 목적으로 읽을 수 있다"고 되어 있는데, 접근목적 치료는 목적트리에서 진료목적보다 상위에 있으므로 허용목적인 진료를 포함하므로 담당의사 u_1은 치료를 목적으로 환자 p의 데이터를 읽을 수 있다.

〔표 1〕 접근목적 배정

조건역할	목적
CanConsult(자문)	자문
CanCoWork(협진)	협진
CanSpecialClinic(선택진료)	진료
CanStrokePatientTailored (뇌졸중맞춤형)	맞춤형

〔표 2〕 허용목적 배정

퍼미션	목적
(식별데이터, RW)	원무
(접속데이터, RW)	진료, 간호, 원무
(이력데이터, R)	진료, 연구
(진찰데이터, R)	진료, 연구
(진찰데이터, W)	진료
(치료데이터, R)	진료, 연구
(치료데이터, W)	진료
(수술데이터, R)	진료, 연구
(수술데이터, W)	진료
(간호데이터, R)	진료, 연구, 간호
(간호데이터, W)	간호
(검사데이터, R)	진료, 연구, 검사
(검사데이터, W)	진료, 검사

〔시나리오 2〕

두통환자 p는 두통전문의 u_7에게 선택진료를 요청한다. 선택 진료를 요청받은 의사 u_7(전문의자격 취득 7년)은 치료를 목적으로 환자p의 가족력을 읽으려고 한다.

결 론: 읽을 수 없다.

설 명: 시스템은 접근되는 가족력 데이터와 연관된 정책이 P_PA_5임을 검색한다. 정책 P_PA_5는 "CanSpecialClinic(선택진료)이라는 조건 역할에 속하는 사용자는 환자 p의 가족력을 진료를 목적으로 읽을 수 있음"을 말해준다. 그러나 두통전문의 u_7이 제공한 역할속성들 중 경력이 10년 미만인 관계로 u_7은 조건역할 CanSpecialClinic에 속하지 못하므로 환자p의 가족력을 읽을 수 없다.

V. 비교 분석 및 결론

프라이버시 접근제어 모델 측면에서 제안된 모델은 목적모델과 RBAC 모델 그 어느 것이라도 확장이 용이하다. 그 이유는 우리의 모델이 역할속성 배정이라는 개념을 도입하기 때문이다. P-RBAC 모델은 접근목적 개념이 없으므로 사전 필터 기능을 갖지 못한다. 그러나 우리의 모델은 접근목적을 조건역할에 배정 가능하므로 사전 필터기능을 갖는다.

P-RBAC과 우리의 모델은 저장된 데이터의 내용에 기초하여 조건표현을 할 수 있다. 우리의 모델과 목적모델은 새로운 태스크 포스 팀 구성이나 협업 환경에 아주 적합하다. 또한 제안된 모델은 정교한 제어가 가능하다. 이는 접근목적의 검증과 데이터 객체의 계층적 구조에서 그 이유를 찾을 수 있다. 우리의 모델과 다른 접근제어 모델들 간 특징별 비교를 요약하면 〔표 3〕과 같다.

〔표 3〕 접근제어 모델 비교

기능 \ 모델	P-RBAC	목적모델	제안모델
프라이버시 보호	○	○	○
확장성	○	×	○
사전필터기능	×	○	○
내용기반 조건 표현	○	×	○
TFT나 협업에 적용	×	○	○
고수준 언어표현	○	×	○
정교한 접근제어	△	△	○

본 논문은 프라이버시 모델들과 정책언어들을 분석하여 RBAC 기반 통합 프라이버시 보호 모델(IPP-RBAC)을 설계하고, 이를 기초로 한 XML 기반 정책언어 모델을 제안하였다. 그리고 제안모델을 의료정보 시스템에 적용시키고, 기존 접근제어 모델 및 정책언어 모델들과 비교분석하였다. 제안한 모델은 다음과 같은 특징을 지닌다.

첫째, 접근목적 배정과 허용목적 바인딩을 기존 P-RBAC 모델에 통합함으로써 부당한 사용자가 접근하는 것을 원천봉쇄하였다. 둘째, 프라이버시 보호를 위해 정보 제공자가 제공하는 요청정보와 보호할 데이터 내용에 기초하여 산술연산과 논리연산 등의 조건을 풍부하게 표현할 수 있게 하였다. 셋째, 본 모델은 정교한 제어가 가능하도록 데이터 객체를 계층화하여 표현하였다. 넷째, 기존 RBAC 시스템과 호환되도록 하기 위해 역할속성 배정을 정의하고, 프라이버시 퍼미션을 조건역할에 부여함으로써 제안된 모델은 기존 RBAC 시스템과 호환되도록 확장성을 제공한다. 다섯째, 제안모델은 새로운 태스크 포스 팀 구성이나 협업 환경에 적합하다. 이는 기존 RBAC의 틀을 그대로 유지하면서 협업에 필요한 조건역할 개념을 도입하고 역할속성 배정이라는 개념을 도입함으로써 가능하다.

제안된 모델은 프라이버시 보호 접근제어 시스템들에게 포괄적인 프레임워크를 제공한다. 그리고 P-RBAC의 구성요소들을 자동으로 관리할 수 있도록 프라이버시 정책에 적합한 고수준 언어를 제공한다. 그러나 향후 행해져야 할 더 많은 연구가 여전히 남아있다. 제안된 모델의 조건 표현에 XQuery를 이용하여 좀 더 풍부하게 표현하는 문제와 이벤트-기반 프라이버시 관리가 그것이다. 또한 XML 데이터베이스를 이용하여 제안된 모델을 구현하고자 한다.

참고문헌

[1] J.W. Byun and N. Li, "Purpose Based Access Control for Privacy Protection in Relational Database Systems", The International Journal on VLDB, Vol. 17, pp. 603-619, Jul. 2008.

[2] Qun Ni, E. Bertino and J. Lobo, "An Obligation Model Bridging Access Control Policies and Privacy Policies," SACMAT'08, Jun. 2008.

[3] Qun Ni, A. Trombetta, E. Bertino and J. Lobo, "Privacy-aware Role Based Access Control," The Proceedings of the 12th ACM Symposium on Access Control Models and Technologies, pp. 41-50, Jun. 2007.

[4] Qun Ni, Dan Lin, E. Bertino and J. Lobo, "Conditional Privacy-aware Role Based Access Control," The Proceedings of the 12th European Symposium on Research in Computer Security, LNCS 4734, pp. 72-89, 2007.

[5] P. Kumaraguru, L.F. Cranor, J. Lobo and S.B. Calo, "A Survay of Privacy Policy Languages," Proceeding of the 3rd Symposium on Usable Privacy and Security, Jul. 2007.

[6] Anne. H. Anderson, "A Comparison of Two Privacy Languages : EPAL and XACML," Proceedings of the 3rd ACM Workshop on Secure Web Services, pp. 53-60, Nov. 2006.

[7] J.W. Byun, E. Bertino and N. Li, "Purpose Based Access Control of Complex Data for Privacy Protection," SACMAT'05, Jun. 2005.

[8] OASIS, "eXtensible Access Control Markup Language(XACML) ver2.0," Feb. 2005.

[9] W3C, "The Platform for Privacy Preferences (P3P1.1) Specification," Feb. 2004. http://www.w3.org/TR/200 4/WD-P3P11-20040210/

[10] Qingfeng He, "Privacy Enforcement with an Extended Role-Based Access Control Model," NCSU Computer Science Technical Report TR-2003-09, Feb. 2003.

[11] IBM, "The Enterprise Privacy Authorization Language(EPAL1.1)," Jun. 2003.

[12] Simone Fischer-Hübner, "IT-Security and Privicy:Design and Use of Privacy-Enhancing Security mechanisms," Lecture Notes in Computer Science 1958, 2001.

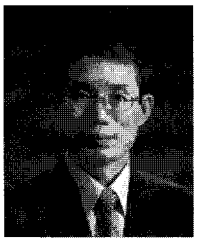
[13] R.S. Sandhu and E.J. Coyne, "Role-Based Access Control Models," IEEE Computer, pp. 38-47, Feb. 1996.

VI. 부 록

〈의료정보시스템의 IPP-RBAC 퍼미션 배정 정책 인스턴스 예〉

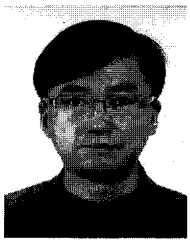
```
〈?xml version="1.0" encoding="euc-kr"?〉

〈privacyPermissionAssignmentSet xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://ssrc.jnu.ac.kr/ipp-rbac privacyPermissionAssignmentSet.xsd"
 xmlns="http://ssrc.jnu.ac.kr/ipp-rbac"〉

        〈roleSet〉  〈role roleID="r1" roleName="의사"/〉
           중간생략
                〈roleInherit〉 〈fromRole〉의사〈/fromRole〉 〈toRole〉수련의〈/toRole〉 〈/roleInherit〉 〈/roleSet〉
        〈objectSet〉
                〈object objectID="obj1" objectName="환자레코드"/〉
           중간생략
                〈objectInherit〉 〈fromObject〉환자레코드〈/fromObject〉 〈toObject〉인적〈/toObject〉 〈/objectInherit〉
           중간생략 〈/objectSet〉
        〈operationSet〉
                〈operation operationID="rd" operationName="read"/〉
           중간생략 〈/operationSet〉
        〈permissionSet〉
                〈permission permissionID="perm1"〉
                        〈object〉obj1〈/object〉
                        〈operation〉rd〈/operation〉
                〈/permission〉
        〈/permissionSet〉
        〈purposeSet〉 〈purpose purposeID="purp1" purposeName="일반"/〉
           중간생략
                〈purposeInherit〉 〈fromPurpose〉일반〈/fromPurpose〉 〈toPurpose〉진료〈/toPurpose〉
                〈/purposeInherit〉        중간생략  〈/purposeSet〉
        〈conditionSet〉 〈condition CondID="cond1"〉
                〈Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-less-or-equal"〉
                 〈attributeDesignator attributeId="http:///ssrc.jnu.ac.kr/ipp-rbac/environment/current-date"/〉
                 〈Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-add-yearMonthDuration"〉
                   〈attributeSelector xpath="md://환자레코드/md:인적/md:식별/md:생일/text()"/〉
                   〈attributeValue〉P13Y〈/attributeValue〉 〈/Apply〉 〈/Apply〉 〈/condition〉
           중간생략  〈/conditionSet〉
        〈obligationSet〉
                〈obligation obligationID="obli1"〉Log〈/obligation〉
           중간생략  〈/obligationSet〉
        〈permittedPurposeBindingSet〉 〈permittedPurposeBinding ppubid="ppub1"〉
                〈permission〉perm1〈/permission〉  〈purpose〉purp1〈/purpose〉 〈/permittedPurposeBinding〉
           중간생략  〈/permittedPurposeBindingSet〉
        〈conditionBindingSet〉  〈conditionBinding conbid="cb1"〉
                        〈permission〉perm1〈/permission〉  〈condition〉cond1〈/condition〉
                〈/conditionBinding〉 〈/conditionBindingSet〉
        〈obligationBindingSet〉 〈obligationBinding oblibid="oblib1"〉
                        〈permission〉perm1〈/permission〉  〈obligation〉obli1〈/obligation〉
                〈/obligationBinding〉 〈/obligationBindingSet〉
        〈attribConditionSet〉 〈attribCondition attriConID="atcond1"〉
                〈Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal"〉
                                〈roleAttributesDesignator attributeId="clinic_type"/〉
                                〈attributeValue〉자문〈/attributeValue〉
                        〈/Apply〉 〈/attribCondition〉
          중간생략 〈/attribConditionSet〉
        〈conditionRoleSet〉 〈conditionRole condRoleID="cr1" condRoleName="CanConsult"〉
                〈roleName〉수련의〈/roleName〉 〈attribCondition〉atcond2〈/attribCondition〉 〈/conditionRole〉
          중간생략 〈/conditionRoleSet〉
        〈privacyPermissionAssignment ppaid="p-pa1"〉
                〈role〉r2〈/role〉
                〈permission〉perm1〈/permission〉
                〈purpose〉purp3〈/purpose〉
                〈condition〉cond1〈/condition〉
                〈obligation〉obli2〈/obligation〉
        〈/privacyPermissionAssignment〉
        〈privacyPermissionAssignment ppaid="p-pa2"〉
                〈conditionRole〉cr1〈/conditionRole〉
                〈permission〉perm1〈/permission〉
                〈purpose〉purp4〈/purpose〉
                〈condition〉cond1〈/condition〉
                〈obligation〉obli1〈/obligation〉
        〈/privacyPermissionAssignment〉

〈/privacyPermissionAssignmentSet〉
```

〈著者紹介〉



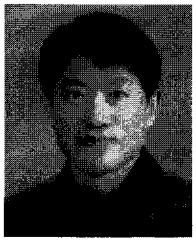
조 혁 현 (Hyug-hyun Cho) 정회원
1984년 2월: 홍익대학교 전자계산학과 학사
1989년 2월: 전남대학교 전산통계학과 석사
2010년 2월: 전남대학교 정보보호학과 박사
1989년~현재: 전남대학교 문화컨텐츠학부 교수
〈관심분야〉 데이터베이스 보안, 전자상거래 보안, 침입탐지, 보안정책

박 희 만 (Hee-man Park) 정회원
1996년 2월: 전남대학교 전기공학과 학사
2006년 2월: 전남대학교 정보보호학과 석사
2009년 2월: 전남대학교 정보보호학과 박사
2009년 3월~현재: 전남대학교 시스템연구센터 연구교수
〈관심분야〉 접근통제, 유비쿼터스 컴퓨팅 보안, 이벤트 시스템



이 영 록 (Young-lok Lee) 정회원
1986년 2월: 전남대학교 계산통계학과 학사
1990년 2월: 전남대학교 전산통계학과 석사
2003년 2월: 전남대학교 전산학과 박사
2003년 3월~현재 전남대학교 시스템연구센터 연구교수
〈관심분야〉 유비쿼터스 컴퓨팅 보안, 보안모델, 정보보호 시스템

이 형 효 (HyungHyo Lee) 종신회원
1987년 2월: 전남대학교 계산통계학과 학사
1989년 2월: 한국과학기술원 전산학과 석사
2000년 2월: 전남대학교 대학원 전산학과 박사
1990년~1997년: 삼보컴퓨터 기술연구소, 한국통신 연구개발원
2001년 3월~현재: 원광대학교 정보·전자상거래학부 부교수
〈관심분야〉 보안모델, 네트워크보안, 전자상거래보안



노 봉 남 (Bong-nam Noh) 종신회원
1978년 2월: 전남대학교 수학교육학과 학사
1982년 2월: KAIST 전산학과 석사
1994년 2월: 전북대학교 전산학과 박사
1983년~현재: 전남대학교 전자컴퓨터공학부 교수
2000년~현재: 전남대학교 시스템보안연구센터 소장
〈관심분야〉 컴퓨터와 네트워크 보안, 개인정보보호, 사이버사회와 윤리