

# 교무업무시스템에서의 개인정보보호를 위한 역할기반 접근 제어 확장

## (Extending Role-based Access Control for Privacy Preservation in Academic Affairs System)

김보선<sup>†</sup>      홍의경<sup>\*\*</sup>  
(Bo-Seon Kim)      (Eui-Kyeong Hong)

**요약** 사용자가 많은 대규모 기업 조직 시스템이나 전자정부시스템에서 사용자의 정보 객체에 대한 접근을 제한하는 효과적인 방법으로 역할기반 접근 제어(RBAC: Role based Access Control)를 들 수 있다. 이는 사용자에게 정보 객체의 접근권한을 직접 부여하는 것이 아니라 조직에서 정의된 역할을 부여함으로써 정보 객체에 접근한다는 개념이다. RBAC는 개인정보에 대한 접근 제어는 가능하나 법제도적으로 규정하고 있는 자기정보결정권 및 조직의 개인정보에 대한 관리감독 규제의 개념은 반영되어 있지 않다.

본 논문에서는 교무업무시스템에 저장되어 있는 학생자료에 대한 접근 제어 및 개인정보보호 수단으로 RBAC 확장모델을 제시하고자 한다. RBAC 시스템에 개인정보 접근권 및 참여권을 반영하기 위하여 자료권한과 자료권한 배정 구성요소를 추가하고, 이를 통해 개인정보의 흐름 및 관리 감독체제의 구축이 가능하도록 설계한다. 또한 RBAC 구성요소별 개인정보보호 개념을 추가하고, 확장된 모델을 바탕으로 시스템 구현 사례와 기존 RBAC와의 비교 평가를 통해 시스템의 중요성과 차별성을 제시한다.

**키워드** : 데이터베이스 보안, 역할기반 접근 제어, 개인정보보호, 통제권, 접근권, 전자정부시스템

**Abstract** RBAC(Role based Access Control) is effective way of managing user's access to information object in enterprise level and e-government system. The concept of RBAC is that the access right to object in a system is not directly assigned to users but assigned by being a member of a role which is defined in a organization. RBAC is utilized for controlling access range of privacy but it does not support the personal legal right of control over information and right of limited access to the self. Nor it contains the way of observation of privacy flow that is guided in a legal level.

In this paper, extended RBAC model for protecting privacy will be suggested and discussed. Two components of Data Right and Assigning Data Right are added to existed RBAC and the definition of each component is redefined in aspect of privacy preservation. Data Right in extended RBAC represents the access right to privacy data. This component provides the way of control over who can access which privacy and ensures limitation of access quantity of privacy. Based on this extended RBAC, implemented examples are presented and the evaluation is discussed by comparing existed RBAC with extended RBAC.

**Key words** : Database Security, RBAC(Role based Access Control), Privacy Preservation, Right of Control over Information, Right of Limited Access to the Self, E-government System

· 본 연구는 첨단정보기술 연구센터를 통하여 과학재단의 지원을 받았음

† 정 회 원 : 한국교육학술정보원 교육행정정보센터 선임연구원  
ysoonkim@keris.or.kr

\*\* 종신회원 : 서울시립대학교 컴퓨터과학교수  
ekhong@venus.uos.ac.kr

논문접수 : 2007년 10월 17일

심사완료 : 2007년 12월 7일

Copyright©2008 한국정보과학회 : 개인 목적이나 교육 목적인 경우, 이 저작물의 전체 또는 일부에 대한 복사본 혹은 디지털 사본의 제작을 허가합니다. 이 때, 사본은 상업적 수단으로 사용할 수 없으며 첫 페이지에 본 문구와 출처를 반드시 명시해야 합니다. 이 외의 목적으로 복제, 배포, 출판, 전송 등 모든 유형의 사용행위를 하는 경우에 대하여는 사전에 허가를 얻고 비용을 지불해야 합니다.

정보과학회논문지: 컴퓨터의 실제 및 레터 제14권 제2호(2008.4)

## 1. 서론

정보통신 기술을 바탕으로 국가 경쟁력 향상을 위한 주요 수단으로 등장한 전자정부사업에서는 국가행정업무 생산성 향상을 위하여 기밀수준의 정보를 다양한 형태로의 활용이 용이한 통합 데이터베이스를 구축하였다. 이 중 교육행정 업무를 처리하기 위한 교무업무시스템은 교사가 시스템에 접속하여 학생의 개인 신상정보, 학적, 성적, 보건 등 학생 지도 및 교육을 위한 사항을 기록하고 진출입 및 진학 시 학교 간 학생정보를 공유할 수 있도록 개발되었다. 그러나 컴퓨터와 정보처리기술의 발달에 따른 정보화 사회가 진전됨과 동시에 통합 데이터베이스에 저장된 학생정보 침해 가능성 및 유출에 대한 우려가 제시되었고 이것이 사회적으로 보호되어야 하는 가치로 급부상하게 되었다.

개인정보란 생존하는 자연인의 가치관, 종교와 같은 내면적 사실, 신체나 재산상의 특질, 사회적 지위나 속성에 관하여 식별되거나 또는 식별할 수 있는 정보의 총체를 일컫는 것이라 할 수 있다[1-3]. 정보화시대의 개인정보보호가 기존의 개인정보보호와 차별되는 이유는 첫째 정보 보호의 대상영역이 확대되는 점이다. 둘째 사적정보에 대해 개인에게 불가침의 영역을 보장하는 소극적 측면의 보호에서 적극적으로 자신에 관한 정보의 수집·처리·유통 및 제공에 있어서 통제권(Right of Control over Information)과 접근권(Right of Limited Access to the Self)을 부여한다는 점이다. 특히 정보화 시대에 데이터베이스에 저장된 개인정보는 정보통신기술에 의한 분류를 통해 개인에 대한 체계적인 평가를 가능하게 하고, 영구보존이 가능하며, 시간의 제한 없이 광범위하게 전달할 수 있게 되었다[4] 이러한 정보는 선전·광고 등의 상업적 목적 혹은 범법목적으로 악용되고 있는 실정이다.

우리나라 경우에는 전자정부법, 공공기관의개인정보보호에관한법률을 바탕으로 공공기관을 중심으로 개인정보보호원칙을 따르고 있다. 교육 분야에서는 교육기본법, 초·중등교육법, 학교보건법에 학생개인정보의 집적 및 이용에 대한 조항을 추가하여 정보시스템에서의 학생개인정보 파일의 취급절차 요건에 대한 법적 근거를 제공하였다. 개인정보를 위한 구체적 관리방안으로 법규정의 제정 내용을 실현할 수 있는 개인자료의 접근 및 통제시스템의 구현을 통해 개인정보심의위원회와 같은 감독기구에서 전산망의 연결을 통한 시스템의 개인정보 접근 현황을 감독해야 한다는 논의가 진행되고 있다 [5,6].

이에 본 연구에서는 이러한 사회적 배경을 바탕으로 교무업무시스템에 저장되어있는 학생 개인정보보호를

위한 접근 제어 방안을 제시하고자 한다. 현재 가장 널리 사용되고 있는 접근 제어 방식은 역할기반의 접근 제어이다. 이는 사용자가 조직에서 책임 및 권한 등의 업무를 바탕으로 정의한 역할을 부여받아 정보 객체에 접근하는 방식이다. 1990년대 말 미국에서는 의료정보시스템에 RBAC를 적용하여 환자의 의료정보에 대한 접근 제한을 통해 개인정보보호를 구현하도록 의료보호법에서 규정하였고, 우리나라에서도 의료정보시스템에 RBAC를 적용하기 위한 사례연구가 빈번히 발생하고 있다[7,8].

RBAC는 교무업무시스템에 적용하여 사용자 역할에 따라 학생정보의 접근 범위를 제한 할 수 있으나, 법제도상의 개인정보보호에 관한 접근권 및 통제권과 개인정보 사용에 대한 조직의 관리 감독 기능 등 자율적 법규제는 충족시키지 못한다. 따라서 본 연구에서는 개인정보 보호에 대한 법적 개념을 시스템으로 통제할 수 있는 접근 제어 방법을 구현하여 조직에서의 개인정보 접근 및 흐름에 대한 시스템을 통한 관리감독 체제 시스템을 제공하는 것을 목표로 한다.

2장에서는 사용자 접근 제어와 관련된 기존 사례 연구로서 Sandhu와 미국표준기술원(NIST: National Institute Standards and Technology)이 제시한 역할기반 접근 제어 방식에 대해 살펴본다. 3장에서는 교무업무시스템에 저장된 학생개인정보의 접근 통제 및 관리 감독을 위한 RBAC 확장 모델을 제시한다. 4장에서는 설계 시스템의 장점 및 평가내용을 기술한다. 끝으로 5장에서 본 논문의 의의 및 향후 추진 연구에 대해 언급한다.

## 2. 관련 연구

역할기반 접근 제어 모델의 가장 큰 특징은 정보 객체에 대한 연산을 수행할 수 있는 권한을 사용자에게 직접 할당하지 않고, 조직 내에서 정의한 역할을 통해 정보 객체에 접근한다는 점이다. 따라서 사용자가 정보 객체에 접근하고자 할 때는 먼저 해당 정보 객체에 대한 연산을 실행할 수 있는 권한을 가진 역할의 소속원이 되어야 한다.

최근 소프트웨어 개발자들은 데이터베이스 관리나 보안관리, 운영체제 등의 제품에 RBAC 특징을 구현하기 위한 노력을 기울여 왔다. 그러나 현재까지는 표준화되지 않은 많은 RBAC 모델이 대학이나 연구소 등에서 제안되고 있으며 기존의 RBAC 구현 제품 또한 이들 모델들의 일부 특징들만을 구현한 예에 불과한 경우가 많다.

1990년에 Ravi Sandhu가 RBAC 모델을 제시하면서 역할, 사용자, 권한, 역할계층 등의 용어를 정립하였다 [9]. 이 후 다양한 RBAC 확장 모델이 발표되었고, NIST

의 표준화 노력을 통해 96년 표준 RBAC 참조모델이 등장하였다[10-14].

**2.1 Sandhu의 RBAC 모델**

그림 1은 Sandhu의 RBAC 모델을 나타낸 것이다. 이 모델의 주요 요소는 사용자, 역할, 권한이다. 사용자는 컴퓨터 시스템을 통하여 시스템 내의 정보를 사용하는 객체이며, 역할은 주어진 기업 환경에서 정의된 업무라 할 수 있다. 권한은 정보 객체에 대해 수행 가능한 접근모드 집합이다. 역할 계층은 기업의 권한과 책임 체계와 유사하여 기업의 권한체계를 모델링 하는데 유용하다. 권한은 허가정보, 접근권한, 특권 등의 의미로 사용되며, 은행에서의 입금, 출금 등 트랜잭션 수준의 보다 의미 있고 추상적인 개념을 통해 표현된다. 세션은 한 사용자와 여러 개의 역할들로 구성된 집합으로 표현될 수 있으며, 사용자는 세션을 통하여 자신에게 배정된 역할들 중의 일부 또는 전체를 수행할 수 있다. 사용자 배정은 사용자를 해당 역할의 구성원으로 하는 것이고 권한 배정은 정보 객체들에 대해서 실행할 수 있는 연산들을 업무 수행에 필요한 역할에 부여하는 것이다. 이러한 방법은 사용자와 정보 객체의 수가 많은 일반 기업 환경에서 권한의 관리를 용이하게 수행할 수 있는 장점을 제공한다.

그림 1에서 요소와 요소간의 관계를 나타내는 화살표가 하나인 것은 단일한 관계를 나타내고 이중 화살표는 다대다 관계를 나타낸다. 따라서 역할과 사용자 사이에 이중 화살표가 표시되어 있는 것은 한 사용자가 동시에 여러 개의 역할을 할 수 있음을 의미한다.

역할계층은 역할에 배정된 권한들 사이에 포함관계가 있는 역할들 간의 부분 순서 관계로서 기업의 권한과 책임 체계와 유사하여 기업의 권한체계를 모델링 하는데 유용하다. 그림 2는 역할계층의 개념과 역할 계층에서의 관리 범위를 나타낸 것이다. CSO의 역할은 S의

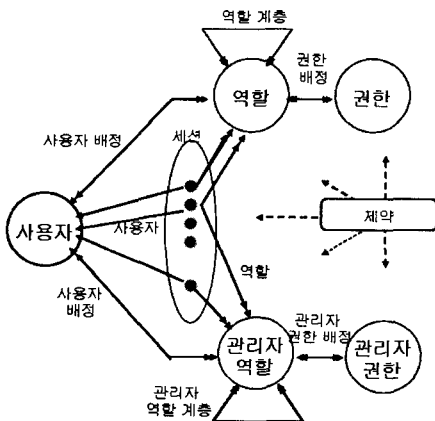


그림 1 Sandhu의 RBAC 모델

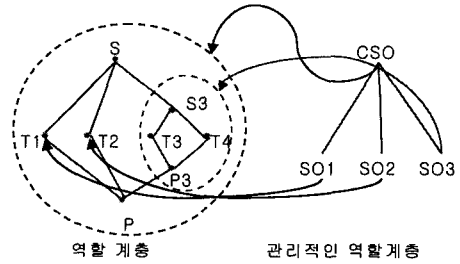


그림 2 역할계층에서의 관리 범위

모든 역할을 관리할 수 있고, SO1이 작업 T1을 관리할 수 있다고 할 때 P의 하위 역할을 관리할 수 있도록 해서는 안 된다. 따라서 SO2는 T2의 작업만을 관리하고, SO3의 경우는 S3의 모든 관리를 할 수 있으나 이 역시 하위 작업인 P를 관리할 수는 없다.

제약 조건은 위에서 정의된 구성 요소들에 대하여 적용되며 각 구성요소가 가지는 특성을 제한사항이나 조건 등으로 기술한다.

Sandhu는 RBAC 구성 요소에 관리자 기능을 강조한 관리자적 RBAC 모델을 추가로 제시하였다. 그림 1에 관리자적 구성 요소를 설정하고 배정 업무를 처리하기 위한 관리자 역할과 관리자 권한, 관리자 역할 계층을 함께 명시하여 제안하였다.

**2.2 NIST의 표준 RBAC 참조모델**

NIST의 표준 RBAC 참조모델(Reference Model)은 Sandhu의 RBAC 모델과 유사하나 그림 3에서 보는 바와 같이 Sandhu의 권한을 연산과 정보 객체로 분리하였다.

표준 RBAC 참조모델의 구성 요소는 사용자, 역할, 연산, 객체, 세션으로 구성된다. 사용자는 조직에 속한 개별 이용자 혹은 시스템에서의 에이전트 등을 의미하고 역할은 조직에서의 위치 및 담당 업무 등을 나타낸다. 연산은 사용자에게 의해서 실행되어지는 응용프로그램이라 할 수 있으며 데이터베이스에서는 데이터의 추가, 입력, 삭제 등을 예로 들 수 있다. 객체는 정보를 보유하는 정보 객체를 의미한다. 파일시스템에서는 파일이나 디렉터리를 의미하고, 데이터베이스에서는 컬럼, 테이블, 뷰 등이 해당한다.

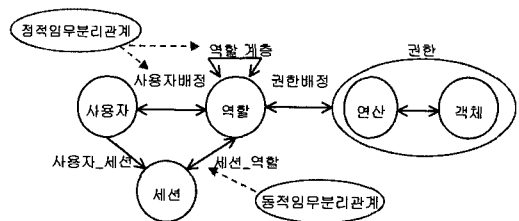


그림 3 NIST의 표준 RBAC 참조모델

사용자 배정은 사용자를 역할에 배치하는 것을 의미하고, 사용자는 하나 이상의 역할에 배치될 수 있다. 권한 부여는 정보 객체를 대상으로 수행할 수 있는 연산 집합을 역할에 지정하는 것이다. 역할계층에서는 사용자 포함관계의 관점에서 상속 개념을 지원한다.

제약조건으로는 동적임무분리(SSD: Static Separation of Duty)와 정적임무분리(DSD: Dynamic Separation of Duty)를 제시하였다. 정적임무분리란 사용자에게 역할을 배정을 할 때 은행에서 지불을 신청하는 담당자와 지불을 허가하는 담당자와 같이 배타적 관계에 있는 역할에 한 사용자를 배정하지 않도록 하는 것이다. 그러나 상호배제 관계에 있는 역할은 사용자가 역할에 배정되는 시점부터 원칙적으로 한 사용자에게 배정할 수 없으므로 사용자에게 배정할 수 있는 잠재적인 역할의 수를 감소시키는 결과를 초래한다. 따라서 상호배제 관계에 있는 역할에 배정된 권한들을 한 사용자에게 부여하는 것은 허용되되 동시에 세션이 활성화되는 것은 제한을 가하는 것이 동적임무분리 제약조건이다.

NIST의 표준 RBAC 참조모델에는 나타나 있지 않으나 Sandhu의 RBAC 모델에서 표현된 관리자 역할 및 관리자 권한을 내재하여 포함하고 있다.

### 3. 개인정보보호를 위한 RBAC 확장

#### 3.1 개인정보보호를 위한 RBAC 확장

교무업무시스템은 교직원인 학생정보 관리 및 학교행정을 처리하기위해 사용하는 시스템으로 그림 4는 교직원

의 역할에 따른 자료접근 영역의 예시를 나타낸 것이다.

학생 개인정보는 학적정보 및 보건정보 등이 해당하고 비개인정보로는 학교 운영을 위한 교육과정, 연월간 학사일정, 학교 주변 보건위생 관리정보 등이다. 학생정보를 접근하는 역할은 반담임, 과목 담임, 개발활동 담임, 성적계, 학적계, 입학, 보건 업무를 담당하는 사용자이다. 반 담임은 학생의 모든 정보를 접근하고, 과목 담임은 자신의 과목을 수강하는 학생의 해당 과목 성적에만 접근하고, 성적계는 전체 석차 처리를 위한 학생의 학기말 최종 성적만을 접근할 수 있어야 한다. 학적계는 학적변동을 맡은 반 학생의 모든 데이터를, 보건교사는 학생의 신체발달 상황만을 접근한다. 비개인정보를 접근하는 역할로는 교무부장, 정보부장이 있다. 그림에서와 같이 교사의 역할별 접근하는 데이터가 구별되고, 학생 데이터에 대한 접근 범위도 제한되어 있음을 알 수 있다.

대학 입학 전형 시 대학에 제출되는 학생 자료는 대학의 요정과 담당교사의 승인 후 온라인으로 제공하게 되어있다. 그러나 학생이 원하지 않는 경우 학생의 자료가 온라인으로 대학에 송부되지 않도록 통제하는 기능이 지원되어야 한다.

본 논문에서 제안하는 개인정보보호를 위한 역할기반의 접근 제어 시스템을 설계한 배경 및 해결 과제는 다음과 같다. 첫째, 시스템은 다수의 사용자와 대량의 데이터를 다루며 사용자와 데이터는 계속 증가한다. 이는 시간의 흐름에 따라 데이터의 접근 범위, 보안 규칙이 달라짐을 의미한다. 둘째, 새로운 업무가 추가 발생되고,

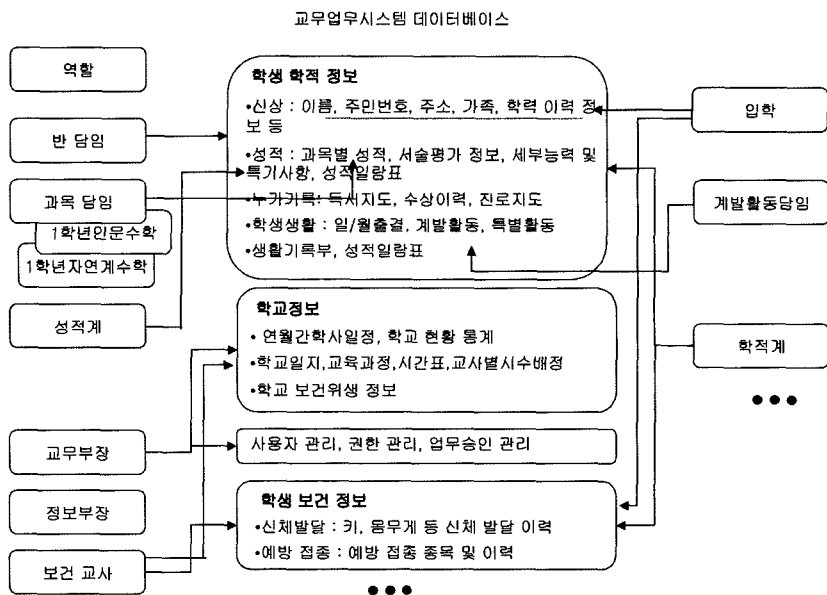


그림 4 교무업무 역할별 데이터 접근 범위

사용자의 인사이동 및 업무 변경이 빈번하다. 사용자는 세분화된 업무 체계에서 해당하는 업무만을 수행하고, 보안정책은 주기적으로, 혹은 수시로 변경된다. 셋째, 개인신상정보의 접근과 사용은 규칙 및 규정에 근거하여 운영된다. 학생 개인 정보는 업무 담당자만이 접근 할 수 있어야 하고, 정보 주체인 학생이 원하는 경우 학생 자료의 접근 및 제 3기관에 학생자료를 전송하여 공유하는 것을 통제할 수 있어야 한다. 나아가 학생 개인정보의 접근 및 활용에 대해 조직의 개인정보보호담당자에 의해 자료의 통제 및 흐름에 대한 관리감독이 가능해야 한다.

위의 첫 번째와 두 번째 문제는 역할기반 접근 제어 규칙에서 역할과 권한의 개념이 소개되면서 문제를 단순화 시켰다. 이는 또한 엔터프라이즈 수준의 응용시스템에서 보안 정책에 대한 기술을 단순화시킴으로 접근 제어 시스템에 상당한 영향을 미쳤다[11,15-17]. RBAC의 장점은 복잡한 접근관리 정책을 추상적 모델로 단순화 시킨 것과 접근 제어 관리업무에 대해 오류 발생과 관리 비용을 감소한 것이라 할 수 있다.

위의 세 번째 해결 과제인 개인정보보호와 관련된 사항은 우리나라에서는 현재까지는 법·제도에 기초하여 조직에서 대응하는 소극적인 자율 규제로서 법적행의 현실적인 한계를 가지고 있다. 개인정보보호에 대한 법규제가 엄격하게 이루어지기 위해서는 법 준수 여부에 대한 감시 장치 및 이를 관리하기 위한 행정적 비용과 노력을 필요로 한다. 또한 개인정보 침해에 대한 분쟁 발생 시 해결을 위하여 어느 사용자가 개인정보보호 규정을 위반하였는지 문제 발생 시점에 대한 정확한 근거 자료 및 로그 자료를 산출할 수 있어야 한다.

따라서 위 세 번째 문제를 해결하기 위하여 학생개인정보에 대한 정보 객체 접근은 기관관리자에 의해서 명시적으로 부여받는 형태의 RBAC 확장 모델을 제시한다. 이를 위한 NIST의 RBAC 모델의 확장은 다음 그림 5와 같다.

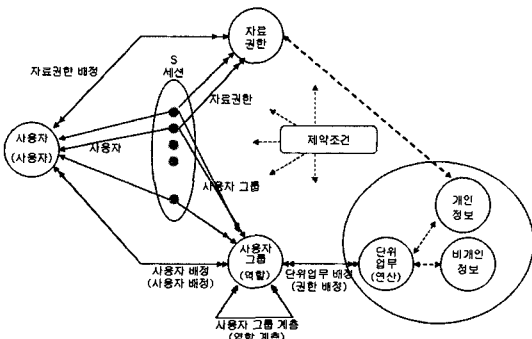


그림 5 개인정보보호를 위한 NIST의 RBAC 확장 모델

그림 5에서 객체를 보안 및 통제의 대상이 되는 개인 정보 객체와 그 외의 정보로 구분하고, 개인정보에 대한 접근을 필요로 하는 연산에 대해서는 해당 사용자가 개인 정보 객체의 접근 권한이 있는지 연산 수행 시점에 확인하는 접근통제 수단을 추가하였다. 이로써 법에서 보장하는 개인정보에 대한 접근권 및 통제권을 시스템에 반영한 것이다. 또한 관리자는 사용자별로 어떤 개인 정보에 접근하고 활용하는지, 정보의 유출 및 관리에 대한 책임을 분할하여 위임하며, 자료권한 배정 내용을 근거로 개인정보 이용에 대한 관리, 감독체제를 운영할 수 있다. 그림 5의 NIST의 RBAC 확장 모델을 교무업무 시스템에 적용하기 위한 구성도는 그림 6과 같다.

그림 6에 소개된 용어를 정의하면 다음과 같다. 사용자는 조직에 속한 개별 사용자를 의미한다. 이는 개인정보 운영 및 관리의 1차 책임 주체이며 제 3기관과의 개인정보 공동 활용을 위하여 전송하는 경우 정보 주체를 대신한 정보 접근권 및 통제권을 행사한다. 사용자 그룹은 같은 업무 혹은 유사 업무를 담당하는 사용자들을 모아 놓은 그룹이다. NIST의 RBAC 모델에서의 역할에 해당한다. 단위업무는 사용자 그룹이 처리하는 세부적인 업무를 의미하며 NIST의 RBAC 모델에서의 연산에 해당한다. 단위업무는 단위업무 수행을 위한 여러 개의 페이지로 구성된다. 하나의 페이지는 하나의 웹 화면과 일대일 대응하고 연산 기능을 제공한다. 자료권한은 개인정보 접근권한이다. 교무업무시스템에서의 개인정보는 학생정보가 이에 해당한다. NIST의 RBAC 모델에서 세션은 사용자와 역할만 결정되면 세션이 활성화되었으나 개인정보보호를 위한 RBAC 확장에서는 개인정보를 접근하는 경우 자료권한이 추가로 필요하다. 따라서 그림 4의 교무부장이 교육과정 편성 업무를 수행하기 위해 교육과정 정보에 접근할 때는 자료권한이 없이도 세션이 형성되고, 반담임이 학생의 생활기록부 관리업무를 통해 학생개인정보에 접근하고자 할 때는 자료권한 정보가 있어야 세션 형성이 가능하다.

RBAC 확장 모델에서의 배정은 사용자 배정, 단위업

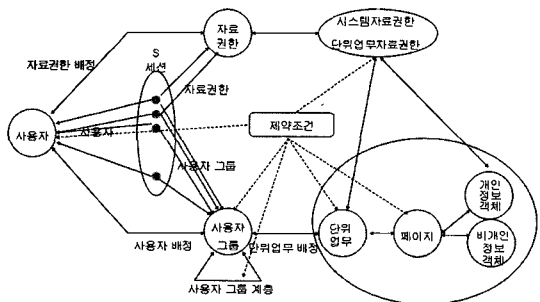


그림 6 교무업무시스템을 위한 RBAC 확장

무 배정, 자료권한 배정 등 세 가지로 구별된다. 사용자 배정은 사용자를 사용자가 속한 사용자 그룹의 구성원으로 등록하는 것이고, 단위업무 배정은 사용자 그룹이 수행하는 단위업무들을 사용자 그룹에 부여하는 것이다. 자료권한 배정은 관리자로부터 사용자의 개인정보 접근에 대한 권한을 부여받는 것으로 사용자 개인별 어느 정보 객체에 접근할 수 있는지를 정의하는 것이다. 자료권한 배정을 통해서 사용자별 개인정보 접근 리스트를 추출할 수 있고 어떤 정보를 접근하는지 개인정보 흐름을 파악할 수 있다.

관리자의 역할은 Sandhu와 NIST의 RBAC 모델보다 한층 더 강화되었다. 관리자는 RBAC의 구성요소를 생성하고 구성요소 간의 관계를 형성할 뿐만 아니라 시스템에 저장되어 있는 개인정보의 접근 제어 및 관리에 대한 총체적 책임을 보유한다. 이는 개인정보보호규칙에서 정의한 개인정보보호담당자로서 사용자별 자료권한 배정업무를 통해 개인정보 관리업무를 분할하여 책임을 위임하고 관리 감독 기능을 수행한다.

사용자 그룹계층은 조직에서의 업무상 직급 체계와 동일하다. 사용자 그룹은 상속의 단위이며, 상위 사용자 그룹은 하위 사용자 그룹에 자신이 가진 권한을 부여할 수 있다.

**3.2 시스템 자료권한과 단위업무 자료권한**

RBAC의 장점 중 하나는 사용자가 많은 대규모 기업 조직에서 사용자에게 일일이 어떤 정보 객체에 접근할 것인지를 부여하는 대신 사용자가 부여받은 역할의 소속원이 되도록 함으로써 접근하는 정보 객체를 제어한다는 것이다. 따라서 이는 대규모 수준의 조직에서 사용자 관리업무의 편리성과 경제적 효과를 이루었다[7]. 그러나 본 논문에서 제시한 자료권한 배정은 개별 사용자에게 어떤 개인정보의 접근권한을 부여할 것인지에 관한 규칙을 정의하는 것으로 사용자와 시스템에 저장되어 있는 개인정보가 증가할수록 관리자의 업무는 증폭된다. 따라서 이를 단순화할 수 있도록 교무업무시스템의 특성을 반영하여 그림 7과 같이 시스템 자료권한과 단위업무 자료권한 두 가지로 구성하여 제시한다.

시스템 자료권한은 학생을 직접 가르치는 사용자들을 대상으로 부여하는 권한으로 사용자 그룹을 대상으로 부여한다. 이는 반담임 권한, 교과담임 권한, 개발활동담임 권한으로 구성되어 있다. 반담임 권한은 담임의 역할을 하는 사용자에게 해당 반 학생의 학적, 성적 등의

정보를 조회, 수정 할 수 있음을 의미한다. 교과담임 권한은 가르치는 과목의 성적만을 조회, 수정할 수 있는 권한을 의미하고, 개발활동 담임 권한은 개발활동 담임이 가르치는 학생의 개발활동에 대한 누가 기록 및 학기, 학년말 기록을 조회, 수정할 수 있는 권한을 의미한다. 예를 들어 1학년 1반 반담임을 대상으로 소속반의 모든 학생에 대해 일일이 자료권한을 부여하는 것이 아니라 1학년 1반 담임이라는 시스템 자료권한을 부여함으로써 일회성 업무로 단순화된다.

단위업무 자료권한은 사용자가 학생을 직접 가르치는 것은 아니나 학교행정 업무를 처리할 때 필요에 의해 학생자료 접근이 가능하도록 하는 것으로 단위업무별로 부여된다. 예를 들어 전입, 전출, 학적통계조회 등의 단위업무를 처리하는 학적계 사용자 그룹의 경우 학생개인자료를 접근하는 전입, 전출은 단위업무 자료권한을 부여하고, 학적통계조회와 같은 비개인정보를 조회하는 경우는 자료권한을 부여하지 않는다. 예를 들어 전출생이 발생한 경우 학적계 담당교사는 전출생의 성적, 출결, 보건 등의 모든 정보가 누락되지 않았음을 확인하고 학생자료를 전출 학교로 전송한다. 따라서 이러한 경우 학생의 개인자료에 접근하게 되므로 자료권한을 부여받아야 세션 형성이 가능하다.

그림 4의 학교에서의 사용자 그룹에 따른 자료 접근에 대하여 자료권한을 부여한 예시이다. 시스템 자료권한 배정이 필요한 역할은 학년반 담임, 교과담임, 개발활동 담임이고, 단위업무 자료권한이 필요한 사용자 그룹은 성적계, 학적계가 해당함을 알 수 있다.

**3.3 제약조건**

제약조건은 RBAC의 구성 요소인 사용자, 사용자 그룹, 사용자 그룹 계층, 단위업무, 페이지, 자료권한에 대한 제약조건이 있다.

사용자에는 사용기간, 사용여부에 대한 제약조건을 설정 할 수 있다. 사용기간은 사용자가 시스템을 접속할 수 있는 기간을 의미한다. 휴직 및 장기 출장 등의 경우 사용여부에 제약을 두어 일시적으로 시스템 접속을 차단할 수 있다.

사용자 그룹에는 부여가능, 사용가능, 적용일자 등에 대한 제약조건을 설정할 수 있다. 사용자 그룹은 사용자 그룹 계층에서 업무 상속을 하는 단위이다. 관리자는 사용자에게 배정한 사용자 그룹을 사용자가 다른 사용자에게 재 상속할 수 있는지 부여 여부를 설정 할 수 있다. 적용일자는 사용자 그룹을 시스템에서 사용 가능한 시작 일자를 의미한다. 조직의 업무 변경으로 사용자 그룹이 폐지된 경우 사용여부에 대한 제약조건을 부여할 수 있다.

사용자 그룹 계층에 대한 제약조건은 다음과 같다. 첫

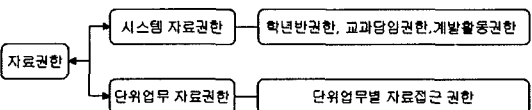


그림 7 자료권한 구분

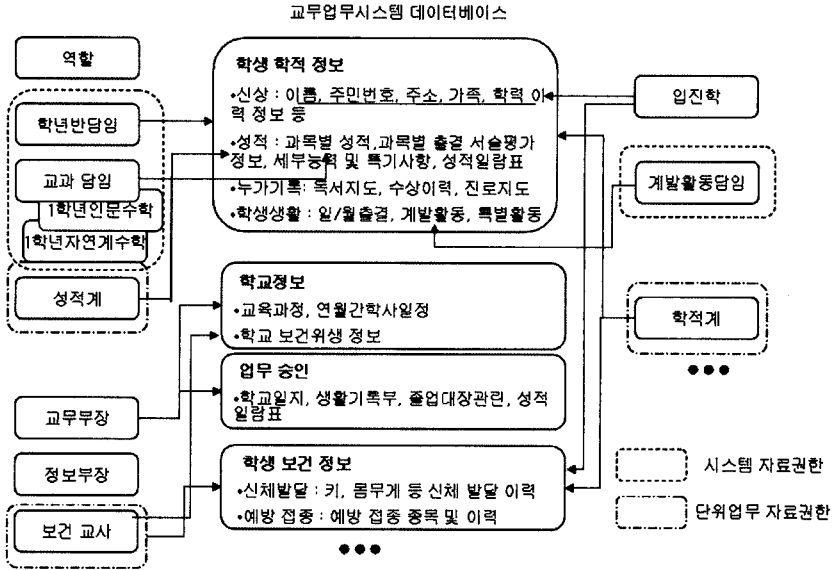


그림 8 시스템 및 단위업무 자료권한 예

제, 본인의 권한은 수정할 수 없다. 둘째, 본인이 관리하는 권한을 본인에게 부여할 수 없다. 이렇게 함으로써 관리자가 악의적인 의도로 자신에게 모든 권한을 배정하고 이용할 수 있는 절대적 통제권을 갖는 것을 제약하는 것이다. 이는 NIST의 정적임무분리관계와 동일하다. 만일 기관 관리자나 업무권한 담당자가 어떤 특정 업무를 배정받아야 하는 경우는 상위 조직으로부터 해당 업무 권한을 부여 받아야 한다.

단위업무에는 사용여부와 적용일자에 대한 제약조건을 설정할 수 있다. 사용여부 제약조건을 설정하여 단위 업무를 일시적으로 사용하지 못하도록 제한 할 수 있다. 적용일자 제약조건을 통해 단위업무가 적용되는 시점을 설정 할 수 있다. 페이지에는 사용여부에 대한 제약조건을 설정할 수 있다. 연산 기능을 더 이상 사용할 필요가 없는 경우 사용여부에 사용하지 않음을 적용할 수 있다. 자료권한에 eg 사용여부에 대한 제약조건을 설정 할 수 있다.

**3.4 RBAC 확장 모델 구현**

다음 그림 9는 권한 관리 부여를 위한 업무 처리 순서이다. 단위업무관리, 사용자 그룹 관리, 사용자 접근 제어 관리의 순으로 업무를 처리한다.

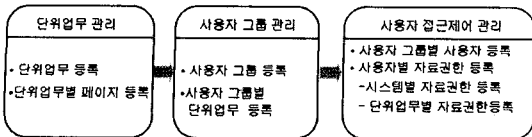


그림 9 사용자 접근 제어 관리 업무 흐름

* 사용자그룹목록									
등록조	사용자	사용자그룹명	단위	선택	사용자ID	사용자명	부여	사용	삭제
직	그룹ID		업무				가능	가능	가능
공통	30001	특_담임	[조회]	<input type="checkbox"/>	teacher	교사02	<input type="checkbox"/>	<input type="checkbox"/>	[2007.11.14]
공통	30018	특_봉사활동	[조회]	<input type="checkbox"/>	251805	교사05	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	[2006.04.06]
공통	30020	특_생활기록부	[조회]	<input type="checkbox"/>	251806	교사06	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	[2006.04.06]

그림 10 그룹별 사용자 등록 및 상속 조건부여

그림 10은 담임그룹이라는 사용자 그룹에 사용자를 배정한 화면의 예이다. 교사02는 담임그룹에 대해 사용만 가능하고 다른 사용자에게 재상속은 불가하나 교사05와 교사06은 담임업무에 대해 본인의 장기 출장 등으로 업무 대행자에게 담임업무의 상속이 가능하다.

그림 11은 학년반 담임 자료권한을 부여하는 예이다. 교사02는 2006학년도 고등부 1학년 1반의 학년반 권한을 배정받았음을 알 수 있다. 이로써 교사02는 해당 반의 모든 학생에 대한 모든 정보를 접근할 수 있다.

그림 12는 배정된 자료 권한 정보를 바탕으로 관리자가 사용자별 자료권한 목록을 출력하는 예시화면이다. 관리자는 본인이 직접 부여하지 않은 자료 권한이나 사

개인별권한 등록									
<input checked="" type="radio"/> 사용자명	<input type="radio"/> 사용자 ID	교사02	[조회]	자료권한목록등록					
ID :	teacher	성명 :	교사02	<input type="checkbox"/> 페이지권한	<input type="checkbox"/> 시스템자료권한	<input type="checkbox"/> 단위업무자료권한			
시스템	교무/학사	[조회]	학년반 권한    교과목권한    개발활동권한						
전체선택	전체해제	조회년도	[조회]	[등록]	[수정]	[삭제]	[목록]		
선택	시스템	학교과정구분	학년도	학년	반	사용여부			
<input type="checkbox"/>	교무/학사	고등학교(부)	2006	1	1	<input type="checkbox"/>			

그림 11 사용자에 대한 시스템자료권한 등록 화면

< 교과목 권한 >

사용자ID	사용자명	학교구분	학년도	학기	강의실명	학년	제출일
teacher	교사02	고등학교(중)	2006	1	.	1	2006.11.10
teacher	교사02	고등학교(중)	2006	1	.	1	2006.11.10
teacher	교사02	고등학교(중)	2006	1	.	1	2006.11.10
teacher	교사02	초등학교(중)	2006	1	.	1	2006.11.10

그림 12 사용자별 자료권한 목록 조회 화면

용자 그룹에 대해서 감시화면을 통해 조직의 접근체제 운영에 대한 임무를 수행할 수 있다.

### 4. 개인정보보호를 위한 RBAC 확장 평가

Sandhu와 NIST의 RBAC와 본 논문에서 제시한 RBAC 확장시스템의 비교 및 평가 내용은 다음 표 1과 같다.

표 1 RBAC 모델의 비교 및 평가

구 분	Sandhu의 RBAC	NIST의 RBAC	개인정보보호 RBAC
정보의 보안 등급 구별	×	×	○
개인정보 접근 제어	○	○	○
접근권 및 통제권 반영	×	×	○
개인정보 접근 목록(관리감독)	×	×	○

Sandhu와 NIST의 RBAC를 활용하여 개인정보에 대한 접근 제어가 가능하나, 개인정보보호 개념인 접근권 및 통제권, 관리감독을 위한 개인정보 접근 목록은 산출되지 못한다.

본 논문에서 제시하는 개인정보보호를 위한 RBAC 확장 모델의 특징을 기술하면 다음과 같다. 첫째, 법에서 명시하는 개인정보보호 원칙에 준한 시스템을 제공한다. 관리자가 자료권한을 통해 사용자가 접근하는 개인정보 접근을 통제함으로써 업무 담당자만이 개인정보에 접근할 수 있고, 개인정보 주체가 원하는 경우 개인정보의 접근을 통제할 수 있는 시스템을 제공한다. 둘째, 사용자가 개인정보 관리에 대한 1차 책임자로서 위임됨으로 개인정보에 대한 책임의 명확성이 증대하고 자료 유출 가능성이 줄며, 접근 현황이 추적, 감시되므로 보안성이 향상된다. 또한 관리자는 개인정보 접근 현황의 감시를 통해 개인정보 활용에 대한 관리 감독이 가능한 시스템 환경을 구축할 수 있다는 점이다. 셋째, 구성 요소별 사용기간, 사용여부 등의 제약조건을 설정할 수 있으며, 관리자 혹은 사용자 그룹 계층에서의 상속 시 발생할 수 있는 보안 위협에 대한 제약조건을 세분화함으로써 더욱 세밀한 개인정보보호 시스템을 운영할 수 있다.

본 시스템의 장점은 법에서 문헌상 제시하는 개인정보보호 개념을 시스템에 반영하여 보안성이 향상되었다는 점이다. 또한 조직에서 개인정보보호에 대한 자율적 규제를 통신망을 이용하여 명확하고 체계적으로 관리할 수 있다는 점이다.

기존 RBAC 시스템과 비교해보면 RBAC 확장시스템에서는 자료권한이라는 구성요소를 추가하여 정보 주체의 입장에서 정보 흐름 및 통제를 실현할 수 있는 시스템으로 설계하였다. 이는 다른 전자정부 행정시스템에 적용되어 개인의 신상정보 뿐만 아니라 엄격한 보안이 요구되는 자료의 접근을 직접적으로 통제하는 수단으로 폭넓게 활용될 수 있다.

### 5. 결론 및 향후 연구 과제

그동안 개인정보의 누출사고를 예방하기 위해 여러 단계의 보안시스템을 운영할 뿐 만 아니라 개인정보보호 인식제고 및 개인정보보호정책의 실현 등 정부수준의 다양한 노력이 전개되어왔다. 그러나 보안사고의 발생 중 80%가 내부 사용자에 의한 것이고, 전체 중 60%가 탐지하지 못했다는 해외 사례 통계를 볼 때 현실적으로 이를 제어할 수 있는 시스템의 제공은 필수적이라 할 수 있다.

그동안 개인정보 유출 사고가 없도록 사용자를 대상으로 개인정보보호에 대한 인식 증대를 위한 소극적인 활동에 의존해 온 실정으로 개인정보에 대한 접근권과 통제권에 대해 구현되어 있는 시스템은 아직 미비한 수준이다. 정보접근 및 유통을 관리한다는 의미는 사용자가 불필요한 정보에 접근할 경로를 사전에 차단한다는 의미이며, 데이터의 양적 범위가 제한됨으로 정보 유출의 범위가 줄고, 또한 정보유출 사고 시 책임 소재가 명확히 정의될 수 있다. 이러한 시스템에 의한 개인정보보호 체제는 종전의 조직 구성원의 의식에 의존하는 개인정보보호 체제에 비해 보안성을 월등히 향상한 것이라 할 수 있으며, 법제도적으로 정의하고 있는 개인정보보호정책을 구현한 사례라 할 수 있다.

향후 개인정보보호담당자의 관리업무를 위해 정보 객체의 관점에서 개인정보 접근 흐름 및 어떤 업무에서 누가 정보를 활용하였는지 등의 감시 방법을 더욱 세분화 하여 개인정보 흐름을 정교하게 제어할 수 있는 시스템 기능에 대한 지속적 연구가 필요하다.

### 참 고 문 헌

[1] 정영화, "인터넷상 개인정보보호 및 분쟁해결에 관한 연구", 인터넷법연구 제1호, 한국인터넷법학회. p.22, 2002.  
 [2] 정재훈, "민간부문에서의 정보프라이버시보호", 정보법



학회 세미나발표, 1997.

- [3] 정찬모, "개인정보 오·남용 실태와 법제도적 대응방향", 정보역기능방지대회 공청회, 1999. 9.
- [4] 소우영, "주요국가의 개인정보보호기관 운영상황 연구", 한국정보보호센터, 1998. 12.
- [5] 개인정보보호 정책 Forum, 정부혁신지방분권위원회, 2004. 6.
- [6] 개인정보보호 정책 Forum, 정부혁신지방분권위원회, 2004. 6.
- [7] Economic Impact of Role Based Access Control. Research Triangle Institute. NIST Planning Report 02-01. 2002.
- [8] 이동희, 의료정보의 프라이버시 보호를 위한 확장 RBAC 설계, 박사학위논문, 충북대학교, 2006. 2.
- [9] R. S. Sandhu, P. Samarati, "Access Control Principles and Practice," IEEE Communications Magazine, pp. 42-48, Sept. 1994.
- [10] NIST, "American National Standard for Information Technology - Role Based Access Control (Draft 4/4/2003)," American National Standard Institute Inc. 2003.
- [11] R. S. Sandhu, E. J. Coyne, Hall. Feinstein, and Charles E. Youman, "Role Based Access Control Models," IEEE Computer Vol.29, No.2, pp. 38-47, Feb. 1996.
- [12] Barkley John F. and Anthony V. Cincotta, "Managing Role/Permission Relationships Using Object Access Types," Proceedings of the 3rd ACM Workshop on Role-based Access Control, ACM, pp. 73-80, Oct. 1998.
- [13] D. F. Ferraiolo, R. S. Sandhu, S. Gavrila, D. R. Kuhn, Ramaswamy Chandramouli, "Proposed NIST Standard for Role-based Access Control," ACM Transactions on Information and System Security (TISSEC), Vol.4, Issue.3, pp. 224-274, Aug. 2001.
- [14] R. Chandramouli and R. S. Sandhu, "Role Based Access Control Features in Commercial Database Management Systems," 21st National Information Systems Security Conference, Crystal City, Virginia, Oct. 1998.
- [15] R. S. Sandhu, D. F. Ferraiolo, and R. Kuhn, "The NIST Model for Role-based Access Control: Towards a Unified Standard," 5th ACM Workshop on Role-based Access Control, 2000.
- [16] D. F. Ferraiolo, J. F. Barkley, and R. Kuhn, "A Role-based Access Control Model and Reference Implementation Within a Corporate Intranet," ACM Transactions on Information and System Security, Vol.2, No.1, pp. 34-68, Feb. 1999.
- [17] R. S. Sandhu, "Role Hierarchies and Constraints for Lattice-based Access Control," Proceedings of 4th European Symposium on Research in Computer Security (ESORICS), pp. 65-79, 1998.



김 보 선

1996년 덕성여자대학교 전산학과 졸업(B.S.). 1998년 서울시립대학교 컴퓨터통계학과 졸업(M.S.). 1998년~1999년 한국학술진흥재단부속 첨단학술정보센터 연구원. 2000년 일본 NIME 연구소 연구원. 1999년~현재 한국교육학술정보원 선임연구원. 관심분야는 데이터베이스 암호화, 사용자 접근제어



홍 의 경

1981년 서울대학교 사범대학 수학교육과 졸업(B.S.). 1983년 한국과학기술원 전산학과 졸업(M.S.). 1991년 한국과학기술원 전산학과 졸업(Ph.D.). 1984년~현재 서울시립대학교 컴퓨터과학부 교수. 2006년 9월 1일~현재 한국정보과학회 총무 부회장. 관심분야는 데이터베이스, XML, 데이터 마이닝, 분산데이터베이스