情報保護學會論文誌
第13券 第4號, 2003. 8

권한상속제한 역할계층을 이용한 역할기반 위임 모델*

박 종 순**, 이 영 록***, 이 형 효****, 노 봉 남***, 조 상 래*****

A Role-Based Delegation Model Using Role Hierarchy with Restricted Permission Inheritance

Jong-Soon Park**, Young-Lok Lee***, Hyung-Hyo Lee****, Bong-Nam Noh***, Sang-Rae Cho*****

요 약

역할기반 접근통제모델은 기업의 다양한 조직체계를 반영할 수 있는 보안모델로 주목받고 있다. 기존의 역할기반 접근통제는 역할계층에 따라 하위역할에 배정된 모든 권한이 상위역할로 무조건 상속되는 특성으로 인해 상위역할에 배정된 사용자에게 권한이 집중되는 현상이 발생되어 권한 남용의 위험성을 내포하고 있다. 기업환경에서는 실제로 하위역할에 배정된 모든 권한이 상위역할까지 상속될 필요가 없는 제한적 업무가 많으므로 기업환경에 적합한 역할기반 접근통제 연구가 필요하다. 본 논문에서는 하나의 역할을 업무특성과 권한상속 정도에 따라 여러 개의 부역할로 나누어 보안관리자가 권한상속을 쉽게 통제할 수 있도록 권한상속제한기능을 제공하는 역할계층 모델을 이용하여, 사용자간 위임과 역할간 위임이 이루어지는 역할기반 위임모델을 제안한다. 또한 제안된 모델과 기존의 모델을 비교 평가하여 타당성을 보인다.

ABSTRACT

Role-Based Access Control(RBAC) model is becoming a promising model for enterprise environments with various organization structures. In terms of role hierarchy, each senior role inherits all the permissions of its junior roles in the role hierarchy, and a user who is a member of senior role is authorized to carry out the inherited permissions as well as his/her own ones. But there is a possibility for senior role members to abuse permissions. Since senior role members need not have all the authority of junior roles in the real world, enterprise environments require a restricted inheritance rather than a unconditional or blocked inheritance. In this paper, we propose a new role-based delegation model using the role hierarchy model with restricted inheritance functionality, in which security administrator can easily control permission inheritance behavior using sub-roles. Also, we describe how role-based user-to-user, role-to-role delegations are accomplished in the model and the characteristics of the proposed role-based delegation model.

keyword : *Role-based Access Control, Delegation, Role Hierarchy*

* 본 연구는 한국전자통신연구원 연구과제(0701-203-0021) 지원으로 수행하였습니다.
** 전남대학교 정보보호협동과정(jspark@athena.jnu.ac.kr)
*** 전남대학교 전산학과({yrlee, bongnam}@athena.jnu.ac.kr)
**** 원광대학교 정보·전자상거래학부(hlee@wonkwang.ac.kr)
***** 한국전자통신연구원(ETRI) 정보보호연구본부 인증기반연구팀(sangrae@etri.re.kr)

Ⅰ. 서 론

역할기반 접근통제모델(Role Based Access Control : RBAC)의 특징은 데이터에 대한 접근권한(permissions)이 조직내의 책임과 자격에 따라 분류된 역할에 배정되고, 그 역할에 사용자가 할당된다는 것이다[1]. 권한의 관리를 사용자와 정보객체간의 관계로 인식하는 대신 기업환경에서의 역할과 객체간의 관계로 설정 관리함으로써 사용자와 정보객체의 수가 대단히 많은 실제의 기업환경에 매우 적합한 특성을 제공한다[2,11]. RBAC에서는 역할에 할당된 사용자만이 그 역할에 배정된 접근권한을 사용할 수 있다.

그러나 지금까지 RBAC 모델에서는 역할 계층상에서 상위 역할에 배정된 사용자는 하위 역할의 모든 접근권한을 상속받게 되는데, 이는 상위 역할에 배정된 사용자에게 권한이 집중되는 현상이 발생하여 불필요한 권한의 실행을 허가 받음으로써 최소권한 원칙을 위배할 수 있는 가능성이 커진다. 이런 문제점의 해결책으로 고유 역할(private role)을 통한 권한 상속 제한이 있는데[2], 고유 역할은 단지 각 역할간의 권한 상속을 방지하는 기능만을 제공할 뿐이다.

따라서 기존의 RBAC 연구는 기업의 조직구조와 역할 계층간의 불일치와 최소권한 원칙의 위배, 그리고 임무분리의 어려움 등으로 인해 기업의 특성을 충분히 반영하지 못하고 있다. 현실세계의 기업 환경에서는 실제로 하위역할에 배정된 모든 권한이 상위역할까지 상속될 필요가 없는 제한적 업무가 많으므로 기업환경에 적합한 연구가 필요하다.

이러한 문제점들을 해결하기 위하여 하나의 역할 계층을 권한 상속 정도에 따라 여러 개의 부역할(sub- role)로 세분화 한 새로운 모델[12]이 제시되었다. 조직공통과 부서공통에 대해서는 기존의 RBAC 모델의 역할계층과 같이 무조건적인 권한 상속을 허용하며, 제한상속 역할에 대해서는 부분적인 권한상속을 허용하고, 고유역할에 대해서는 권한상속 금지라는 특성을 부여한다. 보안관리자는 제안한 새로운 역할 계층 모델을 이용하여 권한상속 정도를 쉽게 통제할 수 있다. 본 논문은 권한상속제한 역할계층을 토대로 역할기반의 사용자 대 사용자(user-to-user) 위임과 역할 대 역할(role-to-role) 위임이 이루어질 수 있도록 새로운 역할기반 위임 모델을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 지금까지 이루어진 RBAC 위임모델에 대한 관련연구를 기술하고, 3장에서는 권한상속제한 역할계층 모델의 부역할과 구성요소들에 대한 설명과 이들 요소에 대한 정형화된 정의를 기술한다. 4장에서는 제안된 역할계층을 이용하여 이루어지는 사용자 대 사용자 위임, 역할 대 역할 위임에 대해 정의하고, 이들 정의에 따른 특성을 정형화하여 서술하며, 마지막으로 5장에서는 제안한 모델과 기존의 모델에 대해 비교 평가한다. 그리고 마지막 6장에서는 결론과 추후과제에 대해 기술한다.

Ⅱ. 관련연구

역할기반 접근통제는 큰 규모의 기업환경 시스템에 보안을 관리하기 위해 널리 이용되는 기술로 가장 일반적인 모델은 RBAC96[1,2]이다. RBAC96의 주된 개념은 권한이 역할에 배정되고 사용자는 그 역할에 적절히 배정된다. 사용자는 하나의 역할에서 다른 역할로 쉽게 배정될 수 있으며 역할은 새로운 권한을 부여 받을 수 있고 권한은 필요에 따라 역할로부터 쉽게 철회될 수 있어 보안관리자는 권한의 관리를 매우 쉽고 단순하게 할 수 있다.

ARBAC97[5]에서 Sandhu 등은 보안 관리자에 의해 수행되는 사용자 역할 배정을 위한 URA97을 제시하였다. ARBAC97의 기본개념은 RBAC을 관리하기위해 RBAC을 이용할 수 있다는 것인데 이것은 관리적인 편의성과 확장성을 제공한다. 하지만 보안관리자의 지속적인 개입으로 인하여 분산 환경에서는 관리 노력이 증대된다.

역할기반 위임의 핵심은 시스템내의 활성개체(active entity)가 또 다른 활성개체에게 자신을 대신하여 어떤 기능을 수행할 권한을 부여하는 것이다. 컴퓨터에서의 위임은 위임방식에 따라 사용자 대 사용자, 사용자 대 기계, 기계 대 사용자, 기계 대 기계로 구분한다. 지금까지 대부분의 위임모델은 사용자 대 사용자와 기계 대 기계 위임[6,7,8,9]을 다루고 있다.

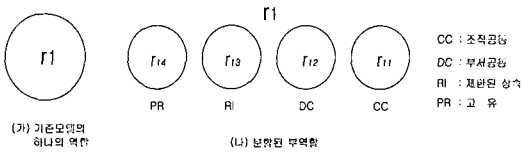
Barka와 Sandhu는 단순한 역할기반 위임모델인 RBDM0[3,4]를 제안했는데, 역할계층과 관련된 권한의 위임과 철회, 부분위임과 다단계 위임을 포함한 몇 가지 쟁점사항을 논의하였으며 전체위임과 역할들의 위임모델을 정형화 하였다. 그러나 RBDM0의 단점으로는 위임모델의 중요개념인 위임 구성요소간의 관련성을 설명하지 못하고 있다. RDM2000[10] 모델은 RBDM0의 확장으로 역할계층과 다단계 위임을 지원하며, 규칙기반 언어를 도입하여 제안된 모델에 대한 정책을 명세하고 있다.

Ⅲ. 권한 상속기능을 제공하는 역할계층

3.1 역할과 부역할

역할은 조직에서의 권한과 책임을 기술한 작업기능이라고 정의할 수 있으며 이 역할에 사용자가 배정된다. 관리자는 조직내에서 수행되는 작업기능에 따라 역할을 만들 수 있다[2]. 이 절에서는 기업 환경에서 상속에 관한 문제를 해결하기 위하여 적용할 수 있는 유연한 역할계층에 대해 논의한다. [그림 1]은 기존의 역할과 제안된 부역할의 개념을 나타낸다.

[그림 1]은 기존모델에서의 하나의 역할을 기업환경에 맞도록 업무특성 및 상속정도의 특성에 따라 부역할로 나눈 것을 보인 것이다. 역할은 조직의 기능과 상속정도에 따라 조직공통(Corporate Common : CC), 부서공통(Department Common : DC) , 상속제한(Restricted Inheritance : RI), 고유(PRivate) 역할 네 가지 부역할로 분류된다. 분류 기준에 따른 부역할의 특징은 [표 1]과 같다.



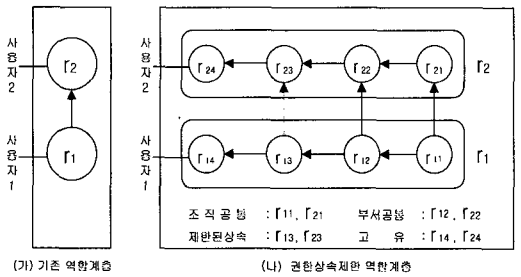
〔그림 1〕 기업환경을 위한 제안된 부역할

표 1. 부역할의 종류와 그 특성

부역할 종류	상속 정도	부역할에 배정된 권한 특징
조직공통 (CC)	전체 상속	· 조직내의 모든 구성원들에게 허용되어 있는 권한 · 상위 부역할은 하위 부역할에 배정된 모든 권한을 포함
부서공통 (DC)	전체 상속	· 특정 부서에 소속된 구성원들에게 허용된 권한 · 상위 부역할은 하위 부역할에 배정된 모든 권한을 포함
상속제한 (RI)	제한적 상속	· 상속제한 부역할 계층내의 상위 부역할에 상속허용 정도에 따라 상속될 수도 있고 상속되지 못할 수도 있는 권한 · 보안 관리자는 제한적으로 상속되는 권한을 명세
고유역할 (PR)	상속 없음	· 직접적으로 배정된 사용자들에게만 허용되는 권한 · 상위 부역할에 상속 불가

3.2 사용자 배정

[그림 2]는 제안된 역할계층의 사용자 역할 배정을 보여 주고 있다. 기존의 역할계층구조는 [그림 2(가)]와 같고 권한상속제한 역할계층 모델의 역할계층구조는 [그림 2(나)]와 같다. 우선 $r_{11} \rightarrow r_{21}$ 와 $r_{12} \rightarrow r_{22}$ 는 각각 조직공통과 부서공통의 역할계층으로서 하위역할에 배정된 모든 권한이 상위역할에 상속된다. 다음으로 $r_{13} \cdots \rightarrow r_{23}$(점선)은 상속제한 역할계층으로 제한적인 권한상속이 일어나게 된다. 이때 상속의 정도를 명세하여 상위 어느 역할까지 상속되는지 표시할 수 있다. 마지막으로 r_{14}와 r_{24}는 고유역할로서 상위역할에 대한 상속관계가 없는 고유의 역할이다. 사용자 배정을 위해서는 사용자를 고유역할에 배정하였으나 사용자 대 사용자 위임에서는 사용자를 위임되는 역할에 배정하는 것을 허용한다.

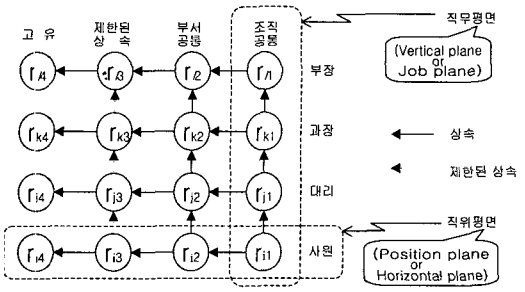


〔그림 2〕 사용자 배정 예

3.3 부역할간 역할계층

권한상속제한 역할계층 모델에서 하나의 역할은 여러 개의 부역할로 세분화되며 부역할들은 기존의 역할과 같이 역할계층을 갖는다. 조직공통과 부서공통 역할계층에서는 하위 역할의 모든 권한이 자신의 상위역할에 상속된다. 상속제한 계층구조는 제한적으로 권한 상속이 일어나는 역할에 상속의 정도를 기술하여 그 역할이 어느 역할까지 상속되는지를 기술한다. 상속제한 계층은 상속을 제한시켜 하위역할에 배정된 권한이 모든 상위역할에 상속되지 않는다.

[그림 3]에서 실선은 하위 부역할들의 권한이 상위 부역할에 무조건적으로 상속되는 것을 나타내고, 점선은 제한된 상속을 나타낸다. 실선은 부서공통 및 조직공통의 직무(job)평면상과 직위(position)평면상의 관계에서 나타나고, 점선은 제한상속 직무평면상에서 나타남을 보여주고 있다. [그림 3]의 예제에서 실선



〔그림 3〕 권한상속제한 역할계층 모델의 역할계층 예

의 방향성 그래프가 나올 수 있는 경우를 기술하면 다음과 같다.

- ***경우1*** : $r_{i1} \rightarrow r_{i2}$

역할계층 구조내에서 $r_{i1} \rightarrow r_{i2}$의 관계가 있다면 한 직위평면내에 존재하는 부역할들간에 계층이 있음을 나타내는 것으로 하위 계층에 배정된 부역할 r_{i1}의 모든 권한이 상위 계층의 r_{i2}에 상속된다.

- ***경우2*** : $r_{j2} \rightarrow r_{k3}$

r_{j2}과 r_{k2}는 DC 계층의 평면상에서의 하위 부역할 r_{j2}와 상위 부역할 r_{k2}간의 역할계층이 있음을 나타내고, r_{k2}와 r_{k3}는 동일한 직위평면상의 하위 부역할 r_{k2}와 상위 부역할 r_{k3}간의 역할계층이 있음을 알 수 있다. 따라서 서로 다른 평면상의 하위 부역할 r_{j2}와 r_{k3}는 $r_{j2} \rightarrow r_{k3}$의 역할계층이 존재함을 나타내고, 결국 부역할 r_{k3}는 부역할 r_{j2}의 모든 권한을 상속함을 알 수 있다.

3.4 권한상속제한기능을 지닌 역할계층모델의 정형화

[그림 4]는 권한상속제한기능을 지닌 모델을 구성하는 기본적인 요소와 용어들을 정의한 것이다. 기존 RBAC의 역할이 부역할로 나뉘어 지므로 본 절에서 특별한 언급이 없는 한 역할은 부역할을 의미한다.

R은 부역할들의 집합이다. R은 업무의 특성에 따라 조직공통 업무인 R_{CC}와 부서공통인 R_{DC}, 제한상속인 R_{RI}, 그리고 고유업무인 R_{PR}로 나눌 수 있다.

R_{Pi}는 대리, 과장, 부장 등과 같이 직위와 연관된 부역할들의 집합으로 수평평면(horizontal plane)을 나타낸다. 이와같은 직위들과 연관된 부역할들의 합집합은 R_{POS}로 표기한다. 이와는 달리 업무의 특성으로 분류된 R_{CC}와 R_{DC}, R_{RI}, 그리고 R_{PR}로 이루어진 부역할들의 합집합이 R_{JOB}이라 할 때 R_{CC}, R_{DC} 등은 수직

【정의 1】 권한상속제한 역할계층 모델을 위한 구성요소

- R : 부역할들의 집합($r_{11}, r_{12}, r_{13}, r_{14}, r_{21}, r_{22}, ..., r_{n1}, r_{n2}, r_{n3}, r_{n4} \in R$)
- R_{CC} : 조직 공통 부역할(Corporate Common sub role)들의 집합
- R_{DC} : 부서 공통 부역할(Department Common sub role)들의 집합
- R_{RI} : 제한상속이 이루어지는 부역할(Restricted Inheritance sub role)들의 집합
- R_{PR} : 고유 부역할(PRivate sub role)들의 집합
- R_{Pi} : 각 직위와 연관된 부역할들의 집합 (R_{Pi}, where $1 \le i \le n$)
- R_{POS} : 모든 직위와 관련된 부역할들의 합집합(i.e. 수평평면)
$$R_{POS} = \bigcup_{i=1}^{n} R_{Pi}$$
- R_{JOB} : 모든 업무와 관련된 부역할들의 합집합(i.e. 수직평면)
$R_{JOB} = R_{CC} \cup R_{DC} \cup R_{RI} \cup R_{PR}$
- $R = R_{JOB} = R_{POS}$

〔그림 4〕 권한상속제한 역할계층 모델을 위한 구성요소와 용어 정의

【정의 2】 권한상속제한 역할계층 모델을 위한 부역할들간의 계층관계

- $\geq$: 동일한 평면상의 부역할들간의 부분순서 관계(만일 $r_2 \geq r_1$ 이면 r_2는 r_1의 상위역할(senior role)
- RH : 역할 계층, $RH \subset R \times R$, 부분순서
- RH_{CC} : 조직 공통 역할간의 부역할 계층
$RH_{CC} \subset R_{CC} \times R_{CC}$, 부분 순서
- RH_{DC} : 부서 공통 역할간의 부역할 계층
$RH_{DC} \subset R_{DC} \times R_{DC}$, 부분 순서
- RH_{RI} : 제한된 상속을 수행하는 부역할간의 역할 계층
$RH_{RI} \subset R_{RI} \times R_{RI}$, 부분 순서
- RH_{Pi} : 특정 직위와 관련된 부 역할들의 역할 계층
$RH_{Pi} \subset R_{Pi} \times R_{Pi}$, where $1 \le i \le n$, 부분 순서
- RH_{POS}: 모든 직위들과 관련된 부역할 계층들의 합집합
$RH_{POS} = RH_{P1} \cup RH_{P2} \cup RH_{P3} \cup ... \cup RH_{Pn}$
- RH_{JOB}: 모든 직무와 연관된 부역할 계층들의 합집합
$RH_{JOB} = RH_{CC} \cup RH_{DC} \cup RH_{RI}$
- RH_{PL} : 수평평면(horizontal planes) 부역할계층과 수직평면상(vertical planes)의 부역할계층의 합집합
$RH_{PL} = RH_{POS} \cup RH_{JOB} \subset RH$
$\forall (r_i, r_j) \in RH_{PL} \Rightarrow (r_i, r_j) \in RH_{POS} \vee (r_i, r_j) \in RH_{JOB}$

〔그림 5〕 부역할간 계층관계

평면(vertical plane)을 이룬다. 부역할의 전체집합인 R은 $R = R_{JOB} = R_{POS}$ 으로 동일함을 알 수 있다.

[그림 5]는 부역할들간의 계층관계를 나타낸 것이다. 업무별 부역할들간의 계층관계는 RH_{CC}와 RH_{DC} 그리고 RH_{RI}이 있으며 이들의 합집합을 RH_{JOB}으로 표기한다. RH_{Pi}는 각 직위와 연관된 역할들간의 계층을 나타낸 것으로 이들 각각을 합집합한 것이 RH_{POS}이다. 그리고 RH_{POS}와 RH_{JOB}을 합집합한 것이 RH_{PL}이다.

Ⅳ. 권한상속제한 역할계층을 이용한 위임

3장에서 지시한 제한상속 기능을 제공하는 역할계

층을 이용한 모델에서의 위임은 사용자 대 사용자(user-to-user), 역할 대 역할(role-to-role)간의 위임을 제공한다. 사용자 대 사용자간의 위임은 전체위임(total delegation)과 부분위임(partial delegation)을 지원하며, 역할 대 역할 위임은 전체위임, 부분위임, 상속가능한(with inheritance) 위임, 상속 불가능한(without inheritance) 위임을 제공한다. 기존의 역할계층을 이용한 위임은 위임되는 역할의 모든 권한이 상위 계층의 역할로 상속되기 때문에 상속되는 위임에 제약을 가하기가 어렵다. 그러나 권한상속제한 역할계층 모델에서의 위임은 부역할간 계층구조를 이용하여 부분상속이나 전체상속이 가능하다. 이 장에서는 권한상속제한 역할계층 모델에서 제공하는 다양한 위임과 그 특징에 대해서 기술한다. 본 논문에서는 집합을 명세하기 위해 집합론의 set comprehension 표기방법을 이용하였으며, 이에 대한 설명은 다음과 같다[13].

{선언부(declaration list) | 선언변수가 포함된 명제(predicate or constraint) • 집합 표현(expression or term)}

| 기호 앞부분은 제약사항인 명제에 쓰이는 변수들에 대한 정의이고, | 다음은 실제로 명제가 참(true)이기 위한 제약사항들이 기술되며, • 뒤에 있는 집합 표현은 제약조건을 만족하여 얻어질 수 있는 집합원소들에 대한 표현을 나타낸다.

4.1 권한상속제한 역할계층 모델의 위임 구성 요소 정형화

권한상속제한 역할계층 모델에서의 위임은 격자평면의 계층구조에서 이루어지게 되는데, 수평평면 부역할계층과 수직평면 부역할계층의 합집합(RH_{PL})에서 상위계층의 부역할과 하위계층의 부역할을 구별하기 위해 연산자 ≥ 를 정의한다. 또한 고유업무에 해당하는 역할은 계층을 이루지 않으므로 고유업무를 위임할 필요가 있을 때에 직위의 상하 관계를 알아내기 위해 함수 role_position을 정의하여 이용한다. 그리고 위임되는 역할에 대한 상속을 제한하기 위해 위임받는 대상의 업무를 선정하는데 필요한 함수인 role_job를 정의하여 이용한다. 이들에 대한 정형화된 표현은 [그림 6]과 같다.

【정의 3】 제한상속 계층을 이용한 위임에 필요한 요소와 함수

≥ $\forall r_x, r_y \in R \bullet r_x \geq r_y \Leftrightarrow r_z \in R \bullet (r_x, r_z) \in RH_{JOB} \wedge (r_y, r_z) \in RH_{POS} \wedge ((r_x \geq r_z) \wedge (r_y \geq r_z))$

서로 다른 평면에 있는 역할간의 부분 순서(partial order)

보안관리자는 아래와 같이 $r_x \geq r_y$을 만족할 때 부분역할 r_x를 부분역할 r_y에게 역할을 위임할 수 있다.

role_job : R → $R_{CC} \cup R_{DC} \cup R_{RI} \cup R_{PR}$

특정 부역할이 속해있는 업무가 R_{CC}, R_{DC}, R_{RI}, R_{PR} 중 어느 범주에 속하는지를 말해주는 함수.

role_position : R → (: 자연수)

특정 부역할이 속해있는 직위를 반환해주는 함수

UA ⊂ U × R 사용자를 역할에 배정 (U: 사용자들의 집합)

users(r) = {u | ∃u∈U • (u, r)∈UA }

특정한 부역할 r_x에 배정된 사용자들의 집합

$sup(r_j) = \{r_i, r_j \in R \mid r_i \geq r_j \wedge (role\_position(r_i) = role\_position(r_j)) \bullet (r_j, r_i)\}$

같은 직위상의 부역할들간의 역할 계층상에서의 한 부역할을 상위 부역할에 사상시키는 함수

PA ⊂ P × R 권한을 역할에 배정

(P: 권한(permissions) 집합)

permissions(r) = {p | ∃p∈P • (p, r)∈PA}

한 부역할에 배정된 권한들의 집합

- check_empty_perm(r) =

$\begin{cases} True \text{ if } \bigcup_{r' \in sup(r)} Permissions(r') \neq \emptyset \\ False \text{ if } \bigcup_{r' \in sup(r)} Permissions(r') = \emptyset \end{cases}$

동일 직위(position)의 상위 부역할(sub role) 권한(permission) 집합의 합집합이 공집합이 아니어야한다.

〔그림 6〕 위임에 필요한 요소와 함수

4.2 사용자 대 사용자 위임

역할기반 위임에 관한 최근의 연구는 사용자 대 사용자(user-to-user) 위임에 초점을 맞추고 있다[3,4]. 위임받는 사용자(delegated user)를 위임하는 역할(delegating role)에 배정함으로써 그 위임받는 사용자는 위임하는 역할에 배정된 권한 행사를 부여받는다. 그러나 지금까지의 연구에서는 사용자 대 사용자 위임이 전체위임(tatal delegation)만을 지원하고 있기 때문에 위임받는 사용자는 위임하는 역할의 모든 권한을 위임받게 된다.

그러나 제안된 모델에서 위임자는 자신이 지닌 역할 중 어떤 업무의 역할에 위임받는 사용자를 배정할 것인지를 결정함에 따라 전체위임이나 부분위임을 수행할 수 있다. 만일 사용자가 고유역할의 업무에 배정된다면, 위임하는 역할의 모든 권한이 사용자에게 위임된다. 그러나 고유역할의 업무 이외의 업무 역할에 사용자가 배정된다면 그 사용자는 위임하는 역할의 일부 권한을 부여받게 된다.

사용자 대 사용자의 위임은 위임하는 역할을 지닌 사용자가 일정조건을 만족하는 하위역할에 배정된 사용자 중 한사람만을 선택해서 위임해줄 수 있다는 장점이 있다. 본 논문에서는 보안관리자가 위임하는 역할의 사용자를 대신하여 위임하는 역할을 하위역할에 배정된 사용자에게 배정한다고 가정한다. 또한 위임을 위해 사용자를 위임되는 역할에 배정한다.

4.2.1 전체위임(Total Delegation)

권한상속제한 역할계층 모델에서는 사용자가 고유역할의 업무에 배정됨을 알 수 있다. 따라서 보안관리자는 위임하려는 상위 고유역할을 하위 고유역할에 배정된 사용자에게 배정함으로써 위임을 수행할 수 있는데, 이때 위임되는 권한은 상위 역할에 배정된 모든 권한이 위임되므로 전체위임이 이루어진다. 보안관리자는 r_x의 직위가 r_y의 직위보다 상위일 때 r_y에 배정된 사용자 중 특정 사용자를 위임하는 역할 r_x에 배정한다.

【정의 4】 사용자 대 사용자 전체위임

u2u_total_delegation

$==\{\forall r_x, r_y \in R_{PR} \mid role\_position(r_x) > role\_position(r_y) \bullet (users(r_y), r_x)\}$

4.2.2 부분위임(Partial Delegation)

사용자를 역할에 배정하는 사용자 배정은 고유역할에 배정하지만 위임과 관련해서는 위임받는 사용자는 어느 부역할에도 배정될 수 있다고 제약사항을 완화한다. 정의 3에서 정의된 연산자 $\geq$ 를 사용하여 $r_y \geq r_x$ 관계인 두 부역할이 있을 때 관리자는 r_x에 배정된 사용자 중 특정인을 위임하는 역할 $r_y \in (R_{CC} \cup R_{DC} \cup R_{RI})$에 배정함으로써 위임받는 사용자는 부분역할을 위임받게 된다.

【정의 5】 사용자 대 사용자 부분위임

u2u_partial_delegation

$==\{ \forall r_x \in R;\ r_y \in (R_{CC} \cup R_{DC} \cup R_{RI}) \mid r_y \geq r_x \bullet (users(r_x), r_y) \}$

4.3 역할 대 역할 위임

실세계의 기업환경에서 보안관리자가 하나의 역할을 특정역할에 배정되어 있는 특정 사용자가 아닌 모든 사용자에게 위임하고자 할 때는 사용자 대 사용자가 아닌 역할 대 역할 위임이 매우 효율적이다[10]. 이 절은 권한상속제한 역할계층 모델이 제공할 수 있는 역할 대 역할 위임에 대해서 기술한다.

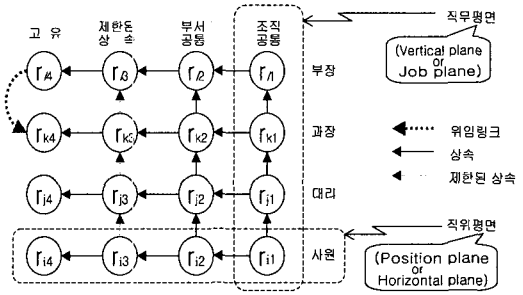
4.3.1 전체위임

권한상속제한 역할계층 모델에서 역할 대 역할 위임은 위임하는 역할로부터 위임받는 역할에 위임 링크(delegation link)를 삽입함으로써 이루어진다. [그림 7]에서 고유역할은 수평평면상에 있는 하위역할의 모든 권한과 하위의 조직공통과 부서공통 그리고 제한된 상속 업무 역할로부터 상속된 모든 권한을 상속받으므로, 위임하는 역할로부터 위임받는 역할인 수평적 하위 고유역할계층으로의 위임은 전체위임을 의미한다.

【정의 6】 역할 대 역할 전체위임

r2r_total_delegation

$==\{\forall r_x, r_y \in R_{PR} \mid role\_position(r_x) > role\_position(r_y) \bullet (r_x, r_y)\}$



〔그림 7〕 전체위임의 예

4.3.2 부분위임

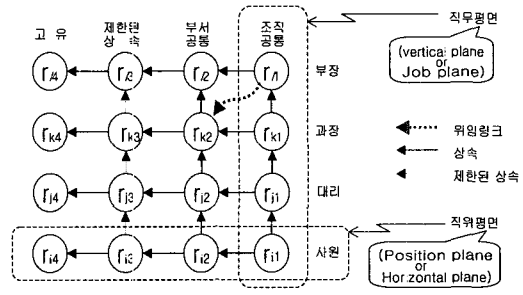
기존의 역할기반 위임모델은 부분위임을 제공하지 못하거나 극히 제한적으로 허용한 반면, 제안된 우리의 모델은 사용자 대 사용자 위임과 같이 상위의 조직공통, 부서공통, 제한상속역할에서 제약조건을 만족하는 하위역할로 위임하는 부분위임이 가능하다. [그림 8]은 위임하는 역할 $r_x(\in R_{CC} \cup R_{DC} \cup R_{RI})$로부터 위임받는 역할 $r_y(r_x \geq r_y)$에게 위임 링크를 보안관리자가 삽입함으로써 부분위임이 이루어지는 것을 보여주고 있다.

정의 7에서 나타낸 바와 같이 위임은 ↙ 방향으로만 효과가 있다. ↘방향으로의 위임은 위임이라는 한

【정의 7】 역할 대 역할 부분위임

r2r_partial_delegation

$== \{ \forall r_x \in (R_{CC} \cup R_{DC} \cup R_{RI});\ r_y \in R \mid r_x \geq r_y \wedge check\_empty\_perm(r_x) \bullet (r_x, r_y)\}$



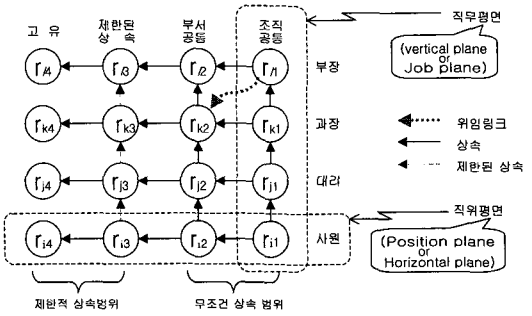
〔그림 8〕 부분위임의 예제

시적인 특징의 효과도 없을 뿐만 아니라 위임후 삽입된 위임링크로 인해 사이클이 형성되기 때문에 부분순서의 원칙에 위배된다. 따라서 역할 대 역할의 부분위임이 이루어지기 위한 제약조건은 연산자 ≥을 만족하는 두 역할간에만 위임이 이루어진다.

4.3.3 무조건 상속이 가능한 위임(Delegation with inheritance)

무조건 상속이 가능한 위임이란 위임하는 역할로부터 위임받는 역할에 위임된 모든 권한들이 위임받는 역할의 상위 역할에 상속되는 것을 의미한다. 무조건 상속이 가능한 위임은 [그림 9]에 나타낸 바와 같이 위임하는 역할로부터 조직공통이나 부서공통인 위임받는 역할로 보안관리자가 위임링크를 삽입함으로써 무조건 상속이 이루어진다.

【정의 8】 무조건 상속이 가능한 위임
r2r_delegation_with_inheritance
$== \{\forall r_x \in R\ ;\ r_y \in (R_{CC} \cup R_{DC}) \mid r_x \geq r_y \bullet (r_x, r_y)\}$



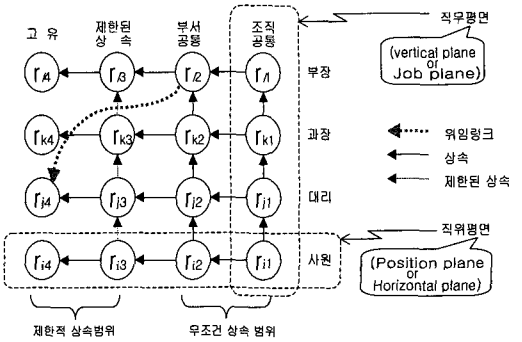
〔그림 9〕 무조건 상속이 가능한 위임 예

4.3.4 상속에 제약이 가해지는 위임(Delegation without Inheritance)

만일 보안 정책상 위임하는 역할을 위임받는 역할의 상위역할로 상속되지 못하게 하거나 상속정도에 따른 제약에 맞게 상속되도록 원한다면 보안관리자는 위임받는 역할을 조직공통이나 부서공통이 아닌 고유역할(R_{PR})이나 제약상속역할(R_{RI})로 한정하면 된다.

[그림 10]은 상속에 제약이 가해지는 위임을 설명한 것인데, 고유역할은 전혀 상속과 관련된 역할계층이 존재하지 않으므로 상속이 불가능하고, 제약상속역할의 계층상에 존재하는 링크의 유무에 따라 위임받는 역할의 권한이 상위역할로 상속될 수도 아니면 상속되지 못할 수도 있음을 나타내고 있다.

【정의 9】 상속에 제약이 가해지는 위임
r2r_delegation_without_inheritance
$==\{\forall r_x \in R;\ r_y \in (R_{RI} \cup R_{PR}) \mid r_x \geq r_y \bullet (r_x, r_y)\}$



〔그림 10〕 상속에 제약이 가해지는 위임 예

V. 제안된 모델의 분석

RBAC 모델에서 역할기반 위임에 관한 연구는 미미하다. 최근의 역할기반 위임모델로는 RBDM0와 *RDM2000이* 있으며, *본 장에서는 몇 가지 위임특성*을 기준으로 RDM2000과 본 논문에서 제안한 위임모델을 비교분석한다. RBDM0는 RBAC96 모델에 기초로하여 만들어진 사용자 대 사용자 위임으로 RDM2000의 토대가 된 모델 이다. 위임모델 비교를 위한 기준으로는 위임방식, 영속성, 위임 후 역할 소유여부, 전체성, 상속제한, 위임주체, 그리고 위임단계 등이 있다[4]. [표 2]는 이 두 모델의 특징을 간단하게 기술한 것이다.

제안된 모델은 사용자 대 사용자와 역할 대 역할의 위임을 제공하는 반면에 RDM2000과 RBDM0 모델은 사용자 대 사용자의 위임만을 허용한다. 위임할 역할의 전체성에 대해서는 제안된 모델은 전체위임과 부분위임을 제공하는데 비해 RDM2000, RBDM0 모델은 전체위임만을 허용한다. 위임을 대행하는 개체에서 제안된 모델은 보안관리자가 수행하는 반면 RDM2000과 RBDM0 모델은 위임하는 역할에 배정된 사용자가 위임을 수행하는 특성을 지니고 있다. 본 논문에서 제시한 위임모델은 사용자 대 사용자와 역할 대 역할의 위임방식이 가능하고, 전체위임과 부분위임이 가능하며 위임된 역할의 상속여부를 제한할 수 있다. 또한 제안된 모델은 역할 대 역할의 위임이 이루어지므로 다중위임(multiple delegation)이 가능할 뿐만 아니라 사용자 대 사용자 위임으로 인한 단일위임(single delegation)이 가능하다는 장점이 있다.

[표 2] 제안된 모델과 기존 역할기반 위임 모델 비교

비교항목 \ 비교모델	제안된 모델	RDM2000	RBDM0
위임방식	사용자 대 사용자 역할 대 역할	사용자 대 사용자	사용자 대 사용자
영 속 성 (permanence)	일시적 (temporary)	일시적	영구적 (permanent) 일시적
위임 후 역할 보유 (monotonicity)	위임 후 위임된 역할 보유 (monotonic)	위임 후 위임된 역할 보유	위임 후 위임된 역할 보유
전 체 성 (totality)	전체(total) 위임 부분(partial) 위임	전체위임	전체위임
상속 제한 (restriction)	상속금지 조건적 (restricted) 상속	무조건 상속	무조건 상속
위임 주체 (administration)	대리인 (agent-acted)	위임하려는 역할에 배정된 사용자 (self-acted)	위임하려는 역할에 배정된 사용자
위임 단계 (levels of delegation)	일 단계 위임 (single-step delegation)	다 단계 위임 (multi-step)	일 단계 위임 이 단계 위임 (two-step delegation)
다중 위임 (multiple delegation)	다중(multiple) 위임 단일(single) 위임	단일위임	단일 위임

Ⅵ. 결 론

기존 역할기반접근통제 모델은 상위역할에 배정된 사용자가 하위역할의 모든 권한을 상속받아 권한 남용의 가능성이 항상 존재하므로 최소권한의 원칙을 위배하게된다. 이를 해결하기 위해 제시된 권한상속제한 역할계층모델은 일반적인 기업환경에 알맞다. 권한상속제한역할계층 모델은 하나의 역할계층을 업무특성과 권한상속 정도에 조직공통, 부서공통, 상속제한, 고유 부역할계층으로 나누어 보안관리자가 권한상속을 쉽게 통제할 수 있도록 하였다.

본 논문은 권한상속제한기능을 제공하는 역할계층 모델을 이용하여, 사용자간 위임과 역할간 위임이 이루어지는 역할기반 위임모델을 제안하였다. 제안된 모델에서 사용자 대 사용자 위임의 전체위임과 부분위임을, 역할 대 역할 위임에서 전체위임, 부분위임, 그리고 상속의 유무에 따른 위임을 기술하고 정형화하였다. 또한 제안된 위임모델과 기존의 모델을 비교평가하여 타당성을 보였다.

보안관리자는 제안된 위임모델을 이용하여 어떤 업무의 역할에 위임받는 사용자를 배정할 것인지를 결정함으로서 사용자 대 사용자의 전체위임이나 부분위임을 수행할 수 있다. 전체위임은 상위 고유역할에 조건을 만족하는 하위 고유역할의 사용자를 배정함으로써 위임하는 역할의 모든 권한이 사용자에게 위임되는 것이며, 부분위임은 고유역할의 업무 이외의 부역할에 조건을 만족하는 하위역할의 사용자를 배정함으로서 그 사용자는 위임하는 역할의 일부 권한을 부여받게 된다.

역할 대 역할의 전체위임은 상위 고유역할에서 하위의 고유역할로 위임하는 것이며 부분위임은 상위의 조직공통, 부서공통, 제한상속역할에서 제약조건을 만족하는 하위역할로 위임하는 것이다. 무조건 상속이 가능한 위임은 제약조건을 만족하는 상위 역할에서 조직공통, 부서공통의 하위역할로 위임하는 것이며 상속에 제약이 가해지는 위임은 제약조건을 만족하는 상위 역할에서 제한상속, 고유역할의 하위역할로 위임하는 것이다.

본 논문은 보안관리자가 위임을 수행하는 개체로 가정을 하였고, 일 단계(single- step)의 위임만을 허용하였으나 향후에는 관리적 측면에서 권한위임의 개체를 사용자로 확장하고, 위임단계 측면에서는 다 단계(multi-step) 위임으로 확장하기 위한 위임경로, 연속적인 권한철회, 위임이 이루어지는 선행조건(prerequisite condition), 그리고 제약사항(constraint)에 대한 명세 및 검증방법 등에 대한 연구로 확장할 예정이다.

참 고 문 헌

[1] Ravi S. Sandhu, "Rational for the RBAC96 Family of Access Control Models," *In Proceedings of 1st ACM Workshop on Role-based Access control, ACM*, Article No. 9, 1996.

[2] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein and Charls E. Youman, "Role-based access control model," *IEEE Computer*, Volume 29, February 1996, pp.38~47.

[3] Ezedin Barka and Ravi Sandhu, "A Role-based

Delegation Model and Some Extensions," *Proceedings of 16th Anual Computer Security Application Conference*, Sheraton New Orleans, Dec. 11~15, 2000.

[4] Ezedin Barka and Ravi Sandhu, "Framework for Role-Based Delegation Models," *Proceedings of 23rd National Information Systems Security Conference*, Baltimore, Oct. 16~19, 2000, pp.101~114.

[5] Ravi S. Sandhu, Venkata Bhamidipati, Qamar Munawer, "The ARBAC97 model for role-based administration of roles," *ACM Transactions on Information and System Security, Volume 2, Issue 1*, 1999, pp.105~135.

[6] Henry M. Gladny, "Access Control for Large Collections," *ACM Transactions on Information Systems, Volume 15. Issue 2*, April 1997, pp.154~194.

[7] Martin Abadi, Michael Burrows, Butler Lampson and Gordon Plotkin, "A Calculus for Access Control in Distributed Systems," *ACM Transactions on Programming Languages and Systems, Volumn 15, Issue 4*, September 1993, pp.706~734.

[8] Morrie Gasser, and Ellen McDermott, "An Architecture for practical Delegation in a Distributed System," *1990 IEEE Computer Society Symposium on Research in Secutiry and Privacy*, Oakland, CA. May 7~9, 1990.

[9] Vijay Varadharajan, Philip Allen, and Stewart Black, "An Analysis of the Proxy Problem in Distributed systems," *IEEE Symposium on Research in Security and Privacy*, Oakland, CA 1991.

[10] Longhua Zhang, Gail-Joon Ahn, Bei-Tseng Chu, "A Rule-Based Framework for Role-Based Delegation," *ACM Workshop on Role Based Access Control, Proceedings of the Sixth ACM Symposium on Access control models and technologies, Chantilly*, Virginia, United States, May 3~4, 2001, pp. 153~162.

[11] R.W.Baldwin, "Naming and Grouping Priviledges to Simplify Security Management in Large Databases," *IEEE symposium on Computer Security and Privacy*, 1990.

[12] YongHoon Yi, Myongjae Kim, YoungLok Lee, HyungHyo Lee, BongNam Noh, "Applying RBAC Providing Restricted Permission Inheritance to a Corporate Web Environment," *APWeb Conference*, Sep. 2003, accepted and to be appeared.

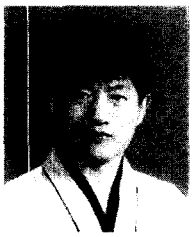
[13] Deri Sheppard, a*n Introduction to Formal Specification With Z and Vdm*, Mcgraw-Hill Book Company, 1995.

〈著者紹介〉

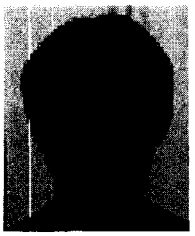
박 종 순 (Jong-Soon Park) 정회원
1986년 : 전남대학교 계산통계학과 졸업(학사)
1989년 : 한국외국어대학교 대학원 전자계산학과 졸업(석사)
2001년 : 전남대학교 대학원 정보보호협동과정 박사과정
1989년~현재 : 한국토지공사
<관심분야> 보안모델, 정보보호시스템, Data Mining, GIS

이 영 록 (Young-Lok Lee) 정회원
1986년 2월 : 전남대학교 계산통계학과 졸업(학사)
1990년 2월 : 전남대학교 대학원 전산통계학과 졸업(석사)
2003년 2월 : 전남대학교 대학원 전산학과 졸업(박사)
<관심분야> 전자상거래 보안, 보안모델, 네트워크 보안, 정보보호 시스템

이 형 효 (Hyung-Hyo Lee) 정회원
1987년 2월 : 전남대학교 계산통계학과 졸업(학사)
1989년 2월 : 한국과학기술원 전산학과 졸업(석사)
2000년 2월 : 전남대학교 대학원 전산학과 졸업(박사)
1990년~1997년 : 삼보컴퓨터 기술연구소, 한국통신 연구개발원
2001년 3월~현재 : 원광대학교 정보·전자상거래학부 조교수
<관심분야> 보안모델, 통신망 보안관리, 전자상거래보안, 침입탐지시스템



노 봉 남 (Bong-Nam Noh) 정회원
1978년 : 전남대학교 수학교육과 졸업(학사)
1982년 : KAIST 대학원 전산학과 졸업(석사)
1994년 : 전북대학교 대학원 전산과 졸업(박사)
1983년~현재 : 전남대학교 컴퓨터정보학부 교수
2000년 : 리눅스 보안 연구센터 소장
<관심분야> 컴퓨터와 네트워크 보안, 정보보호시스템, 전자상거래 보안, 사이버사회와 윤리



조 상 래 (Sang-Rae Cho) 정회원
1996년 : Imperial College of Science, Technology and Medicine, 전산과(학사)
1997년 : Royal Holloway, University of London, 정보보호(석사)
1997년~1999년 LG 종합기술원 연구원
1999년~한국전자통신연구원 연구원
< 관심분야> 정보보호(PKI, 인증/인가 기술, 프라이버시보호기술), 컴퓨터/네트워크 보안