通信情報保護學會論文誌
第 11 券 第 1 號, 2001. 2

기업환경을 위한 과업-역할기반 접근제어 모델*

오 세 종**, 박 석***

Task-Role-Based Access Control Model For Enterprise Environment

Se-jong Oh**, Seog Park***

요 약

대형 기업들은 많은 수의 사용자와 정보객체들을 가지고 있으며 승인된 사용자만이 지정된 정보 객체를 접근할 수 있도록 접근을 제어하는 것이 중요한 과제로 대두되고 있다, 그러나 기존에 제시된 접근제어 모델들은 기업의 접근제어 요구사항을 충분히 만족시키지 못하고 있다. 본 논문은 기업환경에 적합한 접근제어 모델을 제안하는 것을 목표로 한다. 이를 위해 접근제어와 관련된 기업 환경의 특성에 대해 분석하였고 이를 바탕으로 과업-역할기반 접근제어(T-RBAC) 모델을 제안하였다. 이 모델은 과업 및 과업 분류에 기초하고 있으며, 과업이 속한 클래스의 특성에 따라 서로 다른 접근제어를 적용 할 수 있도록 하였다. 또한 권한관리를 용이하게 하기위하여 감독-역할계층을 지원할 수 있도록 하였다.

ABSTRACT

There are many information objects and users in a large company. It is important issue how to control user's access in order that only authorized user can access information objects. Traditional access control models do not properly reflect the characteristics of enterprise environment. This paper proposes an improved access control model for enterprise environment. The characteristics of access control in an enterprise environment are examined and a task role-based access control (T-RBAC) model founded on concept of classification of tasks is introduced. T-RBAC deals with each task differently according to its class, and supports task level access control and supervision role hierarchy.

keyword : *role-based access control, task, enterprise environment,*

Ⅰ. 서 론

1970년대에 들어서면서 컴퓨터 시스템이 다수의 사용자에게 다수의 응용(application)을 제공하는 특성을 갖게되면서 데이타 보안 문제에 대한 관심이 높아지게 되었다. 시스템 관리자와 소프트웨어 개발자들은 권한이 있는 사용자들에게만 특정 데이타 또는 자원들이 제공되는 것을 보장하기 위한 서로 다른 종류의 접근제어(access control)를 구현하기 위해 노력하였다. 접근(access)이란 컴퓨터 내의 자원에 대해 어떤 작업(예 : 사용, 변경, 조회)을 할 수 있는 능력을 말한다. 접근제어(access control)는 그러한 능력을 가능하게 하거나 제한할 수 있는 수단이다[1~12].

현대의 기업경영에서는 정보시스템에 의해 구축된 기업 정보가 경영자원의 하나로 인식되며 기업 경쟁력을 결정짓는 중요한 요소로 보고 있다. 따라서 기업 정보를 보호하는 일은 매우 중하다. 기업에서의

* 본연구는 정보통신연구진흥원 2000년 대학기초연구 지원비에 의한 결과임(과제번호: 정보 93)
** 서강대학교 컴퓨터학과 데이타베이스연구실 (sejong@dblb.sogang.ac.kr)
*** 서강대학교 컴퓨터학과 교수 (spark@dblb.sogang.ac.kr)

정보보호는 군사 환경과는 달리 정보를 '감추는'데 목적이 있지 않다. 기업 정보는 업무과정에서 발생하며 이를 필요로 하는 구성원들에게는 적극적으로 제공되어야 한다. 즉 정보의 '활용성' 또한 중요한 것이다. 여기에 기업 환경에서 접근제어의 어려움이 발생한다. 접근제어가 정보의 '기밀성'과 '활용성'을 동시에 지원할 수 있어야 하는 것이다. 기업 환경에서 접근제어의 어려운점을 좀더 살펴보면 다음과 같다.

- 기업정보는 공유적 특성을 갖는다. 즉 하나의 정보 객체에 관련된 사용자가 다수인 경우가 많다. 그 이유는 기업의 업무는 서로 관련되어 있고 정보 객체를 매개로 하여 업무가 연결되기 때문이다.
- 기업에는 많은 수의 사용자와 매우 많은 수의 정보 객체가 존재한다. 따라서 개별 사용자의 접근제어 권한 정보를 생성하고 유지하는 일이 매우 어렵다.
- 어떤 사용자가 접근 권한이 있는 경우라도 여러 가지 제약 요소가 존재할 수 있다. 예를 들면 특정 고객주문 정보의 갱신은 그 주문 물품이 납품되기 이전에만 가능하다. 기업에는 이와 같은 '업무규칙(business rule)'이 존재한다.
- 기업 환경에서는 합법적 사용자가 정보를 불법적으로 사용하거나 사용자들이 공모하여 사기행위를 할 수 없도록 방지하는 것이 중요하다. 이와 관련된 원칙이 '임무분리(separation of duty)'이다.[10] 즉 한 사람의 사용자가 할 경우 불법 행동이 가능한 업무를 여럿으로 분리하고 이를 서로 다른 사람이 수행하면서 상호 견제하도록 하는 것이다. 이와 같은 정책들이 접근제어에도 영향을 미친다.

이상의 이유로 인해 기업 환경에 적합한 접근제어 모델을 설계하는 일은 매우 어렵다. 지금까지 여러 접근제어 모델에 제안되었지만 기업의 특성을 충분히 반영하는 모델은 없는 실정이다. 본 논문에서는 접근제어와 관련된 기업환경의 특성에 대해 밝히고, 기존의 역할기반 접근제어 모델을 기초로 하여 기업 환경의 특성을 충실히 반영하는 과업-역할기반 접근제어(T-RBAC:Task-Role-Based Access Control) 모델을 제안하였다. 제안된 모델은 기업에서 정보의 접근 권한이 과업을 중심으로 묶여지고 이 과업은 사용자가 조직내에서 맡고 있는 직위(job position)나 업무 역할(business role)에 따라 부여된다는 사실에 기초한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존에 제안된 접근제어 모델을 간략히 설명하고 기업환경에 적용할 때의 문제점을 설명한다. 3장에서는 접근제어와 관련된 기업 환경의 특성을 설명하고 과업분류(task classification)의 개념을 제시한다. 4장에서는 T-RBAC 모델의 요소들과 내용을 설명하고 이에 대한 예제를 제시한다. 또한 T-RBAC 모델의 특징 및 장점에 대해 평가한다. 5장에서는 결론 및 연구과제를 기술한다..

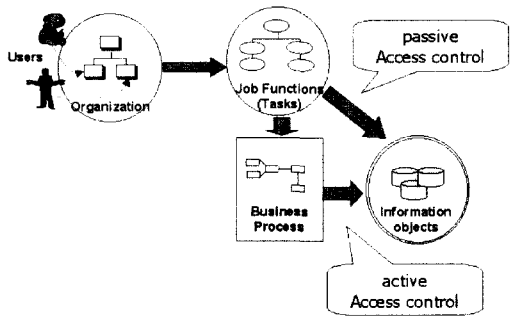
II. 기존의 연구 및 문제점

지금까지 연구된 대표적인 접근제어 기법으로는 강제적 접근제어(MAC: mandatory access control), 자율적 접근제어(DAC: discretionary access control), 역할기반 접근제어(RBAC: role-based access control), 행위기반 접근제어(ABAC: activity-based access control)가 있다.

강제적 접근제어(MAC)[5,11]는 각 정보에 결합된 비밀등급(classification level)과 사용자에게 부여된 인가등급(clearance level)을 사전에 규정된 규칙과 비교하여 그 규칙을 만족하는 사용자에게만 접근 권한을 부여하는 보안정책으로서, 군사적 환경과 같이 정보의 기밀성이 매우 중요시되는 환경에서 사용되고 있다. 그러나 기업환경에서는 기밀등급, 보안등급을 부여하는 것이 어렵고 정보의 활용을 촉진하기 어렵기 때문에 적합하지 않다.

자율적 접근제어(DAC)[5,11]는 정보객체의 소유자 혹은 관리자가 보안관리자의 개입 없이 자율적 판단에 때라 접근권한을 다른 사용자에게 부여하는 기법으로서, 정보보호 보다는 정보의 공동활용이 더 중요시되는 환경에 적합하다. 그러나 정보의 유출 가능성 등으로 인해 기업환경에는 적합하지 않다.

역할기반 접근제어(RBAC)[3,6,8,9]의 중심적인 개념은 사용자가 기업이나 조직의 정보 자원을 임의로 접근할 수 없도록 하는 것이다. 대신에 접근 권한이 역할(role)에 부여되고 사용자는 적절한 역할에 소속됨으로서 역할의 수행에 필요한 최소 자원만을 접근할 수 있도록 한다. 이러한 아이디어는 권한 관리를 매우 단순화 시켜주고 기업의 특정한 보안정책을 구현하는데 있어서 유연성을 제공하는 장점이 있다. 사용자는 그들의 업무적 권한과 책임에 따라 특정 역할의 구성원이 되며 접근 구조의 변경이 없이도



〔그림 1〕 기업환경에서의 접근제어

역할의 변경을 쉽게 할 수 있다.

행위기반 접근제어(ABAC)[7,13,14,15]는 워크플로우(workflow)와 같은 협력작업 환경을 위한 모델로서, 앞의 세 모델이 접근권한의 부여시점에서 권한이 활성화(activate) 되어 임의의 시점에서 사용가능한 반면 행위기반 접근제어 모델에서는 접근권한의 부여(assignment)와 권한의 활성화(activation)가 분리되어 있다. 어떤 사용자가 워크플로우 내의 과업(task)에 대한 실행 권한을 부여받았다 하더라도 그 권한의 사용은 워크 플로우의 진행 상태에 따라 제약을 받는다.

일반적으로 DAC과 MAC은 기업환경에 적합지 않은 것으로 평가된다. ABAC은 기업 환경에 이용될 수 있으나 사용 분야가 다소 제한적이다. RABC은 네가지 모델중 기업환경에 가장 적합한 모델로 알려져 있다. 그러나 RBAC 은 다음과 같은 점에서 문제를 가지고 있다.

- RBAC 은 행위기반 접근제어의 특성을 갖고 있지 않기 때문에 기업내에 존재하는 워크플로우에 대한 적절한 접근제어를 제공하지 못한다.
- RBAC의 역할 계층(role hierarchy)은 기업의 조직구조를 모델링 한 것이나 조직구조의 특성을 잘 반영하지 못한다.[2] 그 예로 임무분리 관계에 있는 두 역할은 같은 상위 역할을 갖을 수 없다.
- 현실세계에서 접근 권한을 부여하는 실제적인 단위는 '역할(role)'이 아니라 '과업(task)'이다. 따라서 하나의 역할에는 하나 이상의 과업이 포함되어 있는데 과업 단위로 접근 권한 관리를 하는 것이 불가능하다. 또한 현실세계에는 여러 특성을 갖는 과업들이 존재하고 그 특성에 따라 서로 다른 접근제어를 필요로 하는데 RBAC은 이를 지원하지 못한다.

본 연구에서는 이러한 RBAC의 문제를 해결할 수 있는 개선된 접근제어 모델을 제안한다.

Ⅲ. 기업 환경에서의 접근제어 특성 분석

기업 환경에 적합한 접근제어 모델을 개발하기 위해서는 모델에 반영해야할 기업환경의 특성이 무엇인지를 알아내는 것이 중요하다. 〔그림 1〕은 기업환경에서의 접근제어를 보여준다. 먼저 사용자는 회사 조직의 어떤 부서에 소속되어 있다. 그리고 조직내에서 적절한 직위(job position)와 업무역할(business role)을 부여받는다. 이러한 직위와 업무역할은 접근 권한의 범위를 정하는 기준이 된다. 사용자들은 자신에게 부여된 직위와 역할에 따라 여러 과업(task)을 수행하는데, 정보객체에 대한 접근은 바로 과업을 수행하기 위해 필요하다. 결국 최종적으로는 사용자가 어떤 과업을 수행할 책임이 있는가에 따라 접근할 수 있는 정보객체의 범위가 결정된다. 기업환경에 대한 관찰을 통해서 분석된 내용은 다음과 같다.

- 최소권한 원칙(least privilege principle)은 기업환경에서 접근제어의 기본 원칙이다. 즉 사용자들에게 자신의 과업의 수행에 필요한 최소한의 권한만을 할당함으로서 정보의 유출이나 불법적 사용을 제한하는 것이다. 이 원칙은 'need- to-know' 와 'need-to-do' 원칙으로도 표현된다.
- 기업의 조직구조(일반적으로 계층적 구조)는 기업의 권한 및 감독 체계를 반영한다.
- 과업(task)은 기업의 구성원들이 수행하는 업무기능(job function) 또는 업무행위(business activity)의 기본적인 단위를 말한다. 사용자들이 수행하는 과업은 접근권한 할당의 기본적인 근거가 된다.
- 사용자는 과업의 특성에 따라 2가지 통로로 정보객체에 접근한다. 첫 번째는 수동적 접근제어(passive access control)로서 '판매실적 조회'와 같은 과업을 할당받은 사용자는 임의의 시점에서 그 과업과 관련된 정보객체에 접근 할 수있다. 둘째는 능동적 접근제어(active access control)로서 '주문서 발행'과 같이 비즈니스 프로세스 혹은 워크플로우상에서 다른 과업들과 연결된 과업은 비

〔표 2〕 과업의 분류

클래스	계승성	필요 접근제어	과업의 특성
S	Yes	수동적 접근제어	감독, 위임 관련
W	No	능동적 접근제어	워크플로우 참여
P	No	수동적 접근제어	사적(private)

록 사용자가 그 과업을 할당 받았다 할지라도 워크플로우의 진행 상태에 따라 접근 권한이 제한된다. 기업 환경이 능동적 접근제어와 수동적 접근제어 모두를 필요로 한다는 사실은 매우 중요하다.

- 앞에서 본 바와 같이 기업에서의 과업은 서로 다른 특성을 가지고 있다. 이를 계승(inheritance)과 워크플로우 참여 여부를 기준으로 분류하면 〔표 1〕과 같이 3가지 클래스로 분류될 수 있다.
  - 클래스 S : 이 클래스에 속한 과업들은 계승(inheritance)성질이 있다. 즉 'User A'가 클래스 S에 속한 과업 T1을 할당 받았다면 T1은 기업 조직 라인상에서 'User A'보다 상위에 있는 사용자들에게도 자연적으로 할당된다. 주로 감독(supervision), 위임(delegation)에 관련된 과업들이 이에 해당한다.
  - 클래스 W : 〔그림 1〕에서 비즈니스 프로세스에 참여하는 과업들은 클래스 W로 분류된다. 이 클래스에 속한 과업들은 행위기반 접근제어를 필요로 한다.
  - 클래스 P : 이 클래스에 속한 과업들은 비즈니스 프로세스에 속하지도 않고 계승성질도 갖지 않는다. 분석작업, 의사결정 등에 관련된 과업이 이에 속한다.
- 각각의 과업은 자신이 속한 클래스의 특성에 따라 서로 다른 접근제어가 적용되어야 한다 (〔표 1〕 참조).

이상에서 기업환경에서의 접근제어 특성에 대해 살펴 보았다. 다음 장에서는 이와 같은 특성을 잘 반영할 수 있는 과업-역할기반 접근제어 모델을 제안한다.

Ⅳ. 과업-역할기반 접근제어(T-RBAC) 모델

4.1 T-RBAC 개요

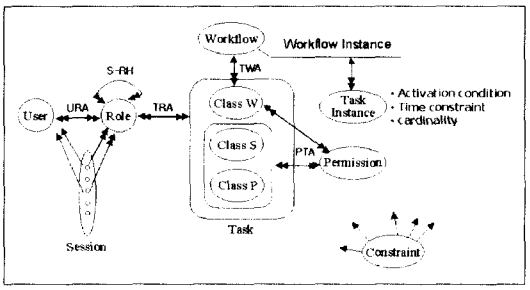
T-RBAC 모델에서는 정보객체에 대한 접근권한(permission)이 이를 필요로 하는 과업(task)들에 할당이 되고 이러한 과업들은 적절한 역할(role)에 할당된다. 사용자는 자신의 직위 또는 업무역할에 따라 필요한 역할(role)들에 할당된다. 과업들은 3장에서 살펴본 바와 같이 3개의 클래스로 구분되며, 클래스에 따라 서로 다른 접근제어가 적용된다.

특별히 클래스 W에 속하는 과업들은 워크플로우 템플릿을 구성하며, 그 과업에 할당된 인가권한들은 평상시에는 비활성화 상태에 있다가 워크플로우 템플릿에 의해 워크플로우 인스턴스가 생성되고 그 인스턴스에 포함된 대응되는 과업 인스턴스가 활성화될 때 인가권한도 함께 활성화(activate) 된다. 대응되는 과업 인스턴스가 비활성화(deactivate)되면 인가권한도 다시 비활성화 된다. 클래스 W의 과업들은 행위기반 접근제어를 가능하게 하기 위해 과업의 활성화 조건(activation condition), 활성화 된뒤의 유효시간(time constraint), 동시에 활성화 할수 있는 과업 인스턴스의 수(cardinality)를 속성값으로 갖는다.

T-RBAC 모델에서는 RBAC에서의 일반적인 역할계층(role hierarchy) 대신에 감독-역할계층(S-RH; supervision role hierarchy)을 사용한다. 일반 역할 계층에서는 하위역할의 모든 인가 권한이 상위 역할로 계승되지만 감독-역할계층(S-RH)에서는 하위 역할의 인가권한 중 클래스 S에 해당하는 과업의 인가권한만 상위로 계승된다.

T-RBAC 모델의 구성 요소는 다음과 같다(〔그림 2〕 참조).

- 사용자(User)
- 역할(Role)
- 과업(Task) 및 과업의 클래스
- 인가권한(Permissiom) : 정보객체+접근유형
- 감독-역할계층 (S-RH; Supervision role hierarchy)
- 사용자-역할 부여(URA; User-Role Assignment)
- 과업-역할 부여(TRA; Task-Role Assignment)
- 인가권한-과업 부여(PTA; Permission-Task Assignment)
- 과업-워크플로우 부여(TWA; Task-Wrokflow Assignment)
- 제약조건(Constraints) : 접근제어의 수행시 필요한 제약조건으로 여기서는 임무분리 (separation of duty)만을 고려하였다.

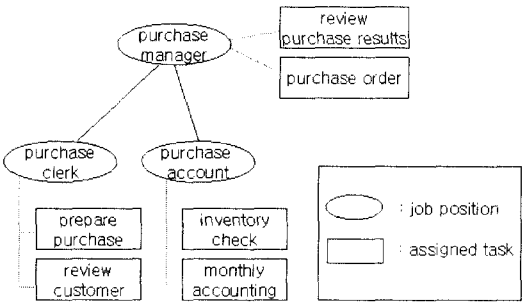


〔그림 2〕 T-RBAC 모델

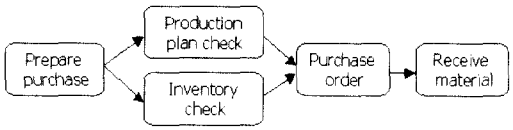
4.2 T-RBAC 모델 예제

어떤 기업의 구매 부서의 조직과 과업이 〔그림 3〕과 같다고 할 때 T-RBAC 모델이 어떻게 적용될수 있는지를 보도록 하자.

접근제어를 위해서는 우선 접근제어 정보가 사전에 구축되어야 한다. 〔그림 3〕의 상황으로부터 T-RBAC 스키마 정보가 다음과 같이 구축될 수 있다.



(a) 조직구조와 과업 부여



(b) 구매 워크플로우

〔그림 3〕 기업환경의 예

T-RABC의 스키마 정보가 〈그림 4〉와 같을 때 T- RBAC의 특성은 다음과 같은 질문들을 통해 설명될 수 있다.

Q1. 사용자 S001에게 부여된 접근권한은 무엇인가

(Ans.) S001의 역할은 p_manager이고 이 역할에는 과업 T1,T2 가 할당되어 있으므로 S1에 부

User

user_id	name
S001	John
S002	Tom
S003	Kate
S004	Adam

Role

role_name
p_manager
p_clerk
p_account

Task

task_id	task_name	class
T1	review purchase result	S
T2	purchase order	W
T3	prepare purchase	W
T4	review customer	S
T5	inventory check	W
T6	monthly accounting	P

S-RH (supervision role hierarchy)

parent_role	child_role
p_manager	p_clerk
p_manager	p_account

URA (user-role assignment)

user_id	granted_role
S001	p_manager
S002	p_clerk
S003	p_clerk
S004	p_account

TRA (task-role assignment)

role	task
p_manager	T1
p_manager	T2
p_clerk	T3
p_clerk	T4
p_account	T5
p_account	T6

PTA (permission-task assignment)

task	info_object	access_type
T1	file1	r,w
T2	file1	r
T2	file2	w
T3	file3	r,w
T4	file4	r
T5	file5	r,w
T6	file1	r
T6	file6	r,w

Task_class_W

task	activation_condition	duration time	cardinality
T2	-	72 h	10
T3	-	24 h	5
T5	not exceed 24hours after prior task is completed	48 h	5

SOD (separation of duty)

task_A	task_B
T3	T2

〔그림 4〕 T-RBAC 스키마 정보

여된 접근권한은 file1{r,w}, file2{w} 이다. 그런데 S- RH 상에서 p_manager의 하위 역할인 p_clerk의 과업 T4 가 클래스 S에 속하므로 상위 역할로 그 권한이 계승된다. 따라서 file4{r} 도 S001의 접근권한이다.

Q2. 사용자 S004는 file2를 읽을 수 있는 권한이 있는가?

(Ans.) 없음. S002의 역할은 p_account 이고 부여된 과업은 T5,T6인데 이들 과업은 file2{r} 권한을 포함하지 않는다.

Q3. 사용자 S001 은 p_clerk 역할을 할당 받을수 있는가?

(Ans.) 없음. S002 가 수행할수 있는 과업중 T2 와 p_clerk 이 수행할 수 있는 과업 T3 가 임무분리 관계에 있기 때문에 T2, T3를 동일 사용자에게 할당하는 것은 T-RBAC 시스템에 의해 금지된다.

Q4. 사용자 S001 의 역할 p_manager는 p_ clerk 의 상위 역할이기 때문에 p_clerk의 과업 T2를 S001 도 수행할 수 있지 않은가?

(Ans.) 없음. 과업 T2는 클래스 W에 속하기 때문에 상위 역할로 그 권한이 상속되지 않는다. 참고로 RBAC 모델에서는 모든 권한이 상위 역할로 상속되어 임무분리 원칙이 깨어진다.

※ 행위기반 접근제어의 특성을 보이기 위해 구매 워크플로우의 현재 상태가 {표 2}와 같다고 가정해 보자.

Q5. 현재 시점에서 사용자 S001은 워크플로우 인스턴스 W015의 과업 T2를 실행(활성화) 시킬 수 있는가?

(Ans.) 없음. T2를 실행할수 있기 위해서는 이전 과업인 T5와 prod_plan_check가 모두 완료되어야 하는데 prod_plan_check가 아직 완료되지 않았다.

Q6. 사용자 S016이 prod_plan_check를 수행할 권한이 있다고 가정할 때 현재 시점에서 S016은 워크플로우 인스턴스 W016에서 prod_plan_check를 실행(활성화) 할수 있는가?

(Ans.) 없음. 현재 시각이 이전 과업 T3이 완료된뒤 25시간이 경과 했기 때문에 prod_plan_check의 활성화 요구조건을 위배한다. 워크플로우 W016은 이제 더 이상 진행될 수 없고 작업이 곧 취소될 것이다.

{표 2} 구매 워크플로우의 현재 진행 상태

workflow instance id	task	status	activated/ completed time
W015	T3	completed	10/4 10:10
W015	T5	completed	10:4 14:30
W015	prod_plan_ Check	activated	10/5 11:50
W015	T2	-	-
W015	receive_ material	-	-
W016	T3	completed	10/4 15:20
W016	T5	activated	10/5 10:10
W016	prod_plan_ Check	-	-
W016	T2	-	-
W016	receive_ material	-	-

(현재 시각 : 10/5 16:30)

4.3 과업-역할기반 접근제어(T-RBAC) 모델의 평가

접근제어 모델에 대한 평가는 그 특성상 성능평가나 정량적인 평가가 어렵다. 따라서 본 연구에서는 T-RBAC 모델이 대상 현실세계를 얼마나 잘 반영하고 있는가를 다른 접근제어 모델과 비교평가하고, 어느 정도의 유용성을 가지고 있는가에 대해 기술하기로 한다. 먼저 RBAC, T-RBAC, ABAC 모델을 비교해 보면 {표 3}과 같다. *(ABAC은 Workflow Management Coalition (WfMC) 의 워크플로우 관리 시스템 표준에서 제공하는 접근제어 사양[18]을 기준으로 하였다. 강제적 접근제어 모델이나 자율적 접근제어 모델은 기업 환경에 적합하지 않기 때문에 비교평가에서 제외하였다.)*

T-RBAC 모델은 RBAC 모델을 기초로 하여 ABAC 모델을 통합한 모델이다. 두 모델의 장점을 취하면서 기업환경의 접근제어 특성을 충분히 반영하도록 개선한 것이 T-RBAC이다. T-RBAC 모델의의 장점을 요약하면 다음과 같다.

- 역할과 인가권한 사이에 과업(task)을 둠으로서 좀더 세밀한 단위의 접근제어가 가능해졌다. 예를 들면 역할단위의 임무분리 뿐만 아니라 과업단위의 임무분리도 실현 가능하다. 과업은 현실세계에서 권한 할당을 위한 기본적인 단위로서,

〔표 3〕 접근제어 모델간의 비교

	RBAC	ABAC	T-RBAC
역할 개념 지원	○	○	○
역할단위의 접근제어	○	○	○
과업 단위의 접근제어	×	○	○
과업의 특성에 따른 접근제어	×	×	○
역할계층 지원	○	×	○
상위 역할이 하위 역할의 모든 권한을 계승	○	×	○
상위 역할이 하위 역할의 권한을 부분적으로 계승	×	×	○
수동적 접근제어 지원 (권한의 부여=권한의 활성화)	○	×	○
능동적 접근제어 지원 (권한의 부여⇒정해진 시간, 조건에서만 활성화)	×	○	○
임무분리 지원	○	○	○
제약조건(constraints)의 구현 방법 제시	×	○	×

역할에 전체 권한을 부여하는 것보다 과업에 권한을 할당한 뒤 이를 다시 역할에 할당하는 것이 현실을 더 잘 반영한다.

- 과업의 클래스 분류에 기초하여 클래스에 따라 각각의 과업들에게 서로 다른 접근제어의 적용이 가능하다. 클래스 S의 과업을 통하여 하위 역할의 권한은 상위의 역할에게 자동적으로 계승 시킬 수 있다. 또한 클래스 P나 클래스 W를 통해 상위 역할에 의해 영향 받지 않는 고유 업무를 수행할 수 있다. 클래스 W의 과업들은 워크플로우에 참여하며 행위기반 접근제어가 적용된다. 각 과업에 부여된 클래스는 보안관리자에 의해 변경 가능하며, 클래스의 변경에 따라 접근제어 유형도 자동적으로 달라진다.
- RBAC에서 역할 계층의 문제를 해결 하였다. 감독-역할 계층은 기업의 조직구조를 그대로 반영할 뿐만 아니라 하위 역할의 접근권한이 모두 상위로 계승되는 것을 제한함으로써 기업의 조직구조가 갖는 권한 및 책임구조를 충실히 반영할 수 있게 되었다.
- 단일 모델로서 일반 정보시스템에서 필요로하는 접근제어(수동적 접근제어)와 워크플로우 시스템에서 필요로 하는 접근제어(능동적 접근제어)를 모두 지원할 수 있다.

T-RBAC 모델의 유용성은 구현을 통하여 실제 상황에서 앞에서 제시한 모델의 장점들이 잘 드러남을 보임으로써 입증할 수 있다. 저자가 속한 연구실에서는 웹 환경에서 기존의 웹서버나 웹문서의 아무런 변경 없이도 인터페이스를 통해 역할기반 접근제어를 가능하게하는 미들웨어 시스템을 구현한 바 있다. 이 시스템을 통해 서버의 성능을 떨어뜨리지 않으면서 기존 시스템에 독립적으로 접근제어가 가능함을 입증하였다. 이에 대한 연구 결과가[19,20]에 소개되어 있다.

V. 결 론

본 논문에서는 기업환경에 적합한 과업-역할기반 접근제어(T-RBAC) 모델을 제안하였다. T-RBAC 모델은 3장에서 분석한 기업환경에서의 접근제어 특성을 충실히 반영하기 위하여 RBAC을 개선시킨 모델이다. T-RBAC의 특징은 RBAC과 달리 접근권한을 직접 역할에 부여하지 않고 그 역할이 수행하는 과업을 통해 부여한다는 점이다. 또한 과업의 특성에 따라 서로 다른 접근제어가 가능하도록 하였다. 특별히 ABAC 모델을 RBAC에 통합함으로써 하나의 모델에서 수동적 접근제어와 능동적 접근제어(행위기반 접근제어) 모두를 가능하게 하였다. 따라서 T-RBAC 모델은 기존에 제안된 모델들에 비해 기업환경에 더 적합한 모델이라 할 수 있다.[16,17]

본 논문과 관련하여 현재 연구중인 과제로는 현실세계로부터 T-RBAC 정보, 즉 사용자, 과업, 역할, 사용자-역할 부여 등의 정보를 효과적으로 추출하는 분야와 T-RBAC에서 권한의 위임(delegation)을 구현하는 분야가 있다. 또한 Web 환경에서 T-RBAC을 적용한 접근제어 미들웨어도 구현중에 있다.

참 고 문 헌

〔1〕 오세종, 박석, "Web 환경을 중심을 한 RBAC의 연구동향", 통신정보보호학회회지, 1999.6.

〔2〕 오세종, 박석, "역할기반 접근제어에서 기업 환경에 적합한 역할계층의 구성에 관한 연구", 한국통신정보보호학회 종합학술발표회 논문집, Vol 9. No1, 1999.11.

〔3〕 T.Jaeger, F.Giraud, N.Islam, and J. Liedtke, "A Role-Based Access Control Model for Protection Domain Derivation and Management", Proc. 2nd ACM Workshop on Role-Based Access Control,

1997.

[4] H.Roeckle, G.Schimpf, and R. Weidinger, "Process-Oriented Approach for Role-Finding to Implement Role-Based Security Administration in a Large Industrial Organization", Proc. of 5th ACM Workshop on Role-Based Access Control, 2000.

[5] C.P.Pfleeger, *Security in Computing*, second edition, Prentice-Hall International Inc., 1997.

[6] E. Bertino, E.Ferrari, and V.Atluri, "A Flexible Model Supporting the Specification and Enforcement of Role-based Authorization in Workflow Management Systems", Proc. of 2nd ACM Workshop on Role-Based Access Control, 1997.

[7] Dagstull, G.Coulouris, and J.Dollimore, "A Security Model for Cooperative work : a model and its system implications", Position paper for ACM European SIGOPS Workshop, September 1994.

[8] R.S.Sandhu, E.J.Coyne, H.L.Feinstein, and C.E.Youman, "Role-Based Access Control Method", IEEE Computer, Vol. 29, Feb. 1996.

[9] D.Ferraio, J.Cugini, and R.Kuhn, "Role-based Access Control (RBAC): Features and motivations", Proc. of 11th Annual Computer Security Application Conference, 1995.12.

[10] Ravi Sandhu, "Separation of Duties In Computerized Information Systems", Proc. of the IFIP WG11.3 Workshop on Database Security, Halifax, U.K., September 18-21, 1990.

[11] E.G.Amoroso, *Fundamentals of Computer Security Technology*, PTR Prentice Hall, pp253-257, 1994.

[12] R.S.Sandhu, P.Samarati, "Access Control : Principles and Practice", IEEE Communication Magazine, pp 40-48, Sep. 1994.

[13] W.K.Huang, V.Atluri, "SecureFlow: A Secure Web-enabled Workflow Management System", Proc. of 4'th ACM Workshop on Role-Based Access Control, 1999.

[14] M.S.Oliver, R.P.Reit, E.Gudes, "Specifying Application-level Security in Workflow Systems", Proc. of 9'th International Workshop on Database and Expert Systems Applications, 1998

[15] R.K.Thomas, R.S.Sandhu, "Task- based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management", Proc. of the IFIP WG11. 3 Workshop on Database Security, 19 97.

[16] Sejong Oh and Seog Park, "Task-Role Based Access Control (T-RBAC): An Improved Access Control Method for Enterprise Environment", Lecture Note in Computer Science 1873, DEXA 2000.

[17] Sejong Oh and Seog Park, "An Integration Model of Role-Based Access Control and Activity-Based Access Control Using Task", Proc. of 14th Annual IFIP WG 11.3 Working Conference on Database Security, Aug. 2000.

[18] Workflow Management Coalition (WfMC), Workflow Reference Model, WF-TC-1003 V1.1, Jan. 1995.

[19] 박석, 인트라넷 환경에 적용 가능한 역할기반 접근제어 미들웨어 Prototype 개발, 연구과제완료보고서, 2001.1.

[20] Sejong Oh and Seog Park, "A Process of Abstracting T-RBAC Aspects from Enterprise Environment", 7th international Conference on Database Systems for Advanced Applications (DASFAA2001), April 2001, (Accepted).

〈著者紹介〉

오 세 종 (Se-Jong Oh) 학생회원
1989년 2월 : 서강대학교 컴퓨터학과 졸업
1991년 2월 : 서강대학교 컴퓨터학과 석사
1997년 9월~현재 : 서강대학교 컴퓨터학과 박사과정
〈관심분야〉 데이타베이스 보안, RBAC(Role-Based Access Control), ERP

박 석 (Seog Park) 정회원
1978년 2월 : 서울대학교 계산통계학 학사
1980년 2월 : 한국과학기술원 전산학 석사
1983년 8월 : 한국과학기술원 전산학 박사
1983년 9월~현재 : 서강대학교 컴퓨터학과 정교수
1997년 2월~현재 : 한국통신정보보호학회 이사
1999년 1월~현재 : 한국정보과학회 이사
2000년 4월~현재 : DASFAA Steering Committee member
〈관심분야〉 실시간 데이터베이스, 데이터베이스 보안, 웹과 데이터베이스