기업환경의 접근제어를 위한 확장된 GTRBAC 위임 모델☆

Extended GTRBAC Delegation Model for Access Control Enforcement in Enterprise Environments

황 유 동*　　박 동 규**
Hwang Yu-Dong　　Park Dong-Gue

요 약

인터넷과 웹이 활성화됨으로써 사용자는 문서, 디렉토리, 데이터베이스, 웹 페이지 등과 같은 자원들을 액세스하는 것이 훨씬 더 쉬워졌다. 그러나 이로 인하여 네트워크의 인증, 자원들을 액세스하기 위한 권한의 허가, 데이터의 정책과 보안 그리고 보안 시스템의 무결성과 같은 중대한 보안 문제들이 생기게 되었다.

본 논문에서는 기업 환경의 접근제어를 위하여 시간(기간과 주기)에 따른 제약으로 자원의 사용을 제한할 수 있는 GTRBAC(Generalized Temporal Role Based Access Control) 모델에 부역할(sub-role) 개념과 PBDM(Permission Based Delegation Model) 개념을 적용한 확장된 GTRBAC 위임(Ex-GTRBAC Delegation)모델을 제안한다.

제안 모델은 부역할을 사용하여 하위 역할에 할당된 권한을 상위 역할에 할당된 사용자가 모두 상속하여 실행할 수 없도록 하여 권한의 남용을 방지하여 최소권한의 원칙을 지킬 수 있도록 하고, 기업 환경에서 빈번히 발생하는 권한의 위임에 대해서 사용자 대 사용자 위임, 역할 대 역할 위임, 다단계 위임, 다중 위임과 같은 기능을 제공하여 기업 환경의 특성에 따라 다양하고 정교한 접근제어 정책을 적용할 수 있도록 한다.

Abstract

With the wide acceptance of the Internet and the Web, volumes of information and related users have increased and companies have become to need security mechanisms to effectively protect important information for business activities and security problems have become increasingly difficult.

This paper proposes a improved access control model for access control enforcement in enterprise environments through the integration of the temporal constraint character of the GT-RBAC model, sub-role hierarchies concept and PBDM(Permission Based Delegation Model).

The proposed model, called Extended GT-RBAC(Extended Generalized Temporal Role Based Access Control) delegation Model, supports characteristics of GTRBAC model such as of temporal constraint, various time-constrained cardinality, control flow dependency and separation of duty constraints (SoDs). Also it supports conditional inheritance based on the degree of inheritance and business characteristics by using sub-roles hierarchies and supports permission based delegation, user to user delegation, role to role delegation, multi-step delegation and temporal delegation by using PBDM.

☞ Keyword : Access control, RBAC, temporal constraint, sub-role, GTRBAC

1. 서 론

인터넷과 웹이 활성화됨으로써 사용자는 문서, 디렉토리, 데이터베이스, 웹 페이지 등과 같은 자원들을 액세스하는 것이 훨씬 더 쉬워졌다. 그러나 이로 인하여 네트워크의 인증, 자원들을 액세스하기 위한 권한의 허가, 데이터의 정책과 보안 그리고 보안 시스템의 무결성과 같은 중대한 보안 문제들이 생기게 되었다.

정보 보안은 시스템들이 인증(authentication), 접근제어(access control), 무결성(integrity), 기밀성(confidentiality), 그리고 부인봉쇄(non-repudiation)와 같은 5가지의 중요한 서비스를 제공하도록 요구

* 정 회 원 : 순천향대학교 대학원 전기전자공학과 수료(박사)
coppermilk@sch.ac.kr(제1저자)
** 정 회 원 : 순천향대학교 정보기술학부 교수
dgpark@sch.ac.kr
[2005/05/04 투고 - 2005/05/25 심사 - 2005/08/23 심사완료]
☆ 본 논문은 정보통신부와 정보통신연구진흥원에서 지원하는 기초기술연구지원사업을 통해서 연구된 과제임

한다. 이 중 접근제어는 컴퓨터내의 자원, 통신 자원 및 정보 자원 등에 대하여 사용, 변경, 조회 등의 작업을 할 수 있는 능력을 가능하게 하거나 제한할 수 있는 수단으로 식별 및 인증된 사용자만이 허가된 범위 내에서 시스템 내부의 정보에 대한 접근을 허용하는 기술적 방법이다.

접근제어를 위해 개발된 보안 정책으로는 임의적 접근 통제(DAC : Discretionary Access Control)[1], 강제적 접근 통제(MAC : Mandatory Access Control), 역할 기반 접근 통제(RBAC : Role Based Access Control)[2,3] 및 행위 기반 접근 통제(ABAC : Activity Based Access Control)[4,5] 모델과 기업 환경에 적합한 과업-역할 기반 접근 통제 모델(T-RBAC : Task-Role Based Access Control)[6] 모델 등이 있다.

그러나 이들 모델들은 모두 기업 환경에 대한 애플리케이션에서 시간 제약에 따른 자원의 사용제한을 하지 못한다는 제약이 있고, 역할 계층상에서 상위 역할에 배정된 사용자가 하위 역할의 모든 접근 권한을 상속받게 되어 불필요한 권한의 실행을 허가하게 되어 최소 권한 원칙을 위배하게 되는 제약이 있다. 이러한 문제점들을 해결하기 위하여 시간(기간과 주기)에 따른 제약으로 자원의 사용을 제한할 수 있는 GTRBAC (Generalized Temporal Role Based Access Control)[10-12] 모델에 권한의 상속을 제한할 수 있는 부역할(sub role)[7,8] 개념을 적용하여 권한의 남용을 방지하고, 최소권한의 원칙을 지킬 수 있는 확장된 GTRBAC (Extended GTRBAC) 모델[13]이 제시되었다.

또한 위 모델들은 기업 환경에서 빈번히 일어나는 위임을 고려하지 않고, 위임을 고려하는 모델도 사용자 대 사용자 위임, 역할 대 역할 위임, 다단계 위임, 다중 위임과 같은 다양한 위임 정책을 고려하지 않는다는 단점이 있다.

본 논문에서는 보안 관리자가 상위 역할로의 권한 상속을 쉽게 통제할 수 있는 확장된 GTRBAC 모델[13]에 PBDM(Permission Based Delegation Model)[14] 개념을 적용하여 역할계층을 이용한 권한의 상속에서 최소권한의 원칙을 지킬 수 있고, 기업 환경에서 빈번히 발생하는 다양한 위임 정책을 적용할 수 있는 새로운 위임 모델을 제시한다.

본 논문에서는 2장에서 기존에 연구되어왔던 접근제어 모델들을 분석한다. 3장에서는 제안 모델의 특징을 서술하고 4장에서는 제안 모델과 기존 모델을 비교 분석하며, 5장에서 결론을 유도한다.

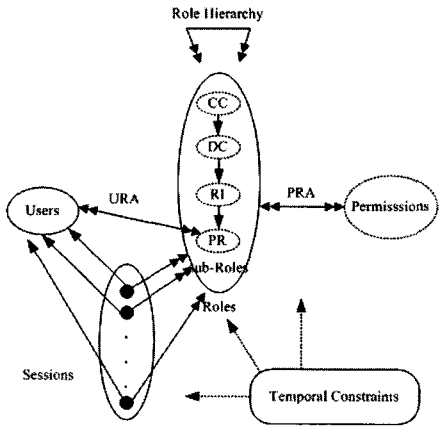
2. 기존 접근제어 모델의 분석

이 장에서는 접근제어와 관련이 있는 기존 연구들을 재검토하고 그들이 기업 환경에 적용될 때 제한 사항들을 분석한다.

접근제어를 위한 보안 정책으로는 역할기반 접근제어(Role Based Access Control : RBAC) 및 역할의 상속 제한과 시간(기간과 주기)에 따른 제약으로 자원의 사용을 제한할 수 있는 확장된 GTRBAC (Extended Generalized Temporal Role Based Access Control) 모델, 기업 환경에서 빈번히 일어나는 다양한 위임 정책을 반영하는 PBDM (Permission Based Delegation Model)이 있다.

역할기반 접근제어(RBAC)[2,3]는 사용자와 자원 관리를 경감시키기 위해 사용된다. 역할기반 접근제어에서 접근 권한은 역할과 관련이 있으며 그리고 사용자는 적절한 역할에 할당된다. 역할기반 접근제어는 접근제어 요구 사항을 지정하는 첫 번째 수단으로서 역할 추상화를 사용한다. 역할을 관리하는 동안에, 허가들은 역할들에 할당되고, 사용자들은 역할에 할당된다. 허가는 정보에 특정한 오퍼레이션을 수행할 능력을 승인하는 것이다. 현실 세계에서, 하나의 역할은 조직 내에서 하나의 직무 기능으로 정의할 수 있으며, 그 역할에 할당된 사용자에 부여된 권한과 책임을 의미한다. 하나의 역할 계층(role hierarchy)은 일반적으로 조직의 관리 구조에 따라서 역할사이의 권한 상속관계를 나타낸다. 역할 계층은 허가 권한 시스템과 유사하기 때문에 기업 조직 구조의 모델링에 적합하다. 그러나 역할기반 접근제어는 접근 권한의 동적 활성화와 응용 레벨 제약의 명세를 필요로 하는 워크플로우(workflow)를 고려하지 않고 있다.

확장된 GTRBAC(Extended GTRBAC) 모델은 다음 그림 1과 같이 표현 할 수 있다. GTRBAC



〈그림 1〉 확장된 GTRBAC 모델

모델의 특징인 시간제약과 역할 활성화, 이벤트, 트리거 등의 제약은 그림 1의 "Temporal Constraint"로 표현하고, 하위 역할에 할당된 권한의 상속을 제한하고 하위 역할을 활성화하여 활성화되는 역할에 할당되는 권한의 제한을 위하여 하나의 역할을 여러 개의 부역할로 나누었음을 알 수 있다.

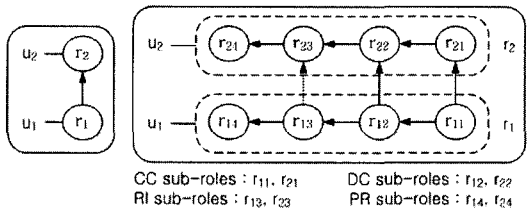
확장된 GTRBAC 모델에서 역할은 할당되는 권한에 따라 조직 공통 역할(CC : Corporate Common), 부서 공통 역할(DC : Department Common), 상속 제한 역할(RI : Restricted Inheritance), 고유 역할(PR : Private Role)로 나누어진다.

조직 공통 역할과 부서 공통 역할은 역할 계층에서 하위의 역할에 할당된 권한이 제한 없이 상위의 역할로 상속되고, 상속 제한 역할은 지정된 상위 역할까지만 권한이 상속되며, 고유 역할은 상위 역할로 상속되지 않는 권한이 할당된 역할이다.

각 부역할은 다음 표 1과 같은 특징을 가진다.

확장된 GTRBAC 모델에서 역할 계층은 GTRBAC 모델의 역할 계층과 동일하게 표현 할 수 있고, 각 역할에는 부역할 계층이 존재한다. 부역할 계층은 네 개의 부역할 사이의 권한 상속 관계를 나타내는 것으로 사용자에게 할당되어야 할 모든 권한이 상속되는 것으로 제한을 할 필요가 없다.

다음 그림 2는 기존 모델의 URA와 제안하는 모델의 URA를 비교하고, 부역할 사이의 역할 계층을 나타낸다.



〈그림 2〉 URA와 부역할의 권한 상속 관계

그림 2의 좌측 부분에서 u1, u2는 사용자를 의미하며, r1, r2는 역할을 의미한다. 이때 역할 r2는 역할 r1보다 역할 계층에서 상위에 있는 역할이다. 역할 r1에서 역할 r2로의 실선 화살표는 역할 r1에 할당된 모든 권한이 역할 r2로 상속됨을 의미한다. 또한 그림에서 보이는 것처럼 기존 모델들에서는 역할을 사용자에게 할당한다.

그림 2의 우측 부분은 제안모델의 URA와 역할 계층에서 상속 관계를 간단히 표현 하였다.

먼저 기존의 역할을 조직공통(CC : r11, r21)역할, 부서공통(DC : r12, r22)역할, 상속제한(RI : r13, r23)역할, 고유(PR : r14, r24)역할과 같은 네 개의

〈표 1〉 부역할 분류 기준

부 역할	상속의 정도	부 역할에 배정된 권한 특징
조직공통 (CC)	제한이 없다.	-. 조직 내 모든 사용자에게 허가된 권한 -. 상위 역할은 하위 역할의 모든 권한을 상속
부서 공통 (DC)	제한이 없다.	-. 부서에 속한 사용자들에게만 허가된 권한 -. 상위 역할은 하위 역할의 모든 권한을 상속
상속제한 (RI)	제한(지정된 단계만큼)적이다.	-. 역할 분석과 설계 과정에서 상속이 제한되는 권한에 대한 조사 필요 -. 하위 역할의 권한이 지정된 상위 역할까지만 상위로 상속 -. 역할 간에 제한적 상속이 가능함
고유역할 (PR)	상속될 수 없다.	-. 상위 역할로 상속이 이루어지지 않는 권한을 할당

부역할로 나누고 사용자에게는 상위역할로 상속되지 않는 권한을 할당하는 고유역할을 할당한다.

그림 2에서 네 개의 부역할 사이의 실선 화살표는 각 부역할 사이의 권한 상속 관계를 나타낸다. 즉, 부역할 사이의 역할 계층은 고유역할이 최상위에 존재하고, 상속제한 역할, 부서공통 역할, 조직공통 역할의 순서가 존재함을 알 수 있다. 이러한 부역할 사이의 상속관계로 인하여 사용자에게는 고유 역할만을 할당해도 모든 권한을 할당 받게 된다. 그림 2에서 상속제한 역할 r13에서 r23으로의 점선 화살표는 하위 역할에 할당된 권한이 상위 역할로 상속이 제한된다는 의미이다. 이때 하위 역할에 할당된 권한은 역할 계층에서 미리 지정된 상위 역할까지만 상속된다.

위와 같이 확장된 GTRBAC 모델은 GTRBAC 모델에 부역할(sub role) 개념을 적용하여 하위 역할에 배정된 권한을 상위 역할에 배정된 사용자가 모두 상속하여 실행할 수 없도록 하여 권한의 남용을 방지하고, 최소권한의 원칙을 지킬 수 있는 장점을 가지게 되었으나, 기업 환경에서 빈번히 발생하는 위임정책을 반영하지 않는 단점이 있다.

PBDM(Permission Based Delegation Model) [14]은 PBDM0, PBDM1, PBDM2 모델로 구성되어있으며 다음과 같은 특징으로 정교한 위임 기능을 제공하는 장점이 있다.

- 역할을 권한의 위임이 불가능한 일반 역할과 위임 가능한 역할로 구분한다.
- 하나 또는 여러 개의 위임 역할을 만들고 만든 역할에 권한을 할당하여 권한을 위임한다.
- 사용자 대 사용자 권한 위임 기능 제공
- 역할 대 역할 권한 위임 기능 제공
- 역할 계층상에서 하위 단계의 사용자에게 상위 단계 사용자의 권한을 위임 할 수 있다.
- 다단계 위임 기능 제공
- 다중 위임 기능 제공

위의 특징에서 알 수 있듯이 PBDM은 정교한 위임 정책을 제공하지만 역할의 제한적 상속 기능을 제공하지 않고, 접근 권한의 동적 활성화와 응용 레벨 제약의 명세를 필요로 하는 워크플로우(workflow)를 고려하지 않고 있다.

위 내용으로 각 접근제어 모델들이 장점을 가지고 있지만 기업 환경에 적용하기에는 여러 가지 제한 사항들이 있음을 알 수 있다.

본 논문에서는 시간(기간과 주기)에 따른 제약으로 자원의 사용을 제한할 수 있고, 역할 활성화와 이벤트, 트리거를 이용하여 사용자 수를 제한하고 워크플로우에 해당하는 작업을 다룰 수 있는 장점을 가지는 GTRBAC(Generalized Temporal Role Based Access Control)모델에 부역할(sub role) 개념을 적용하여 하위 역할에 배정된 권한을 상위 역할에 배정된 사용자가 모두 상속하여 실행할 수 없도록 하여 권한의 남용을 방지하고 최소권한 원칙을 이행할 수 있도록 하고 PBDM(Permission Based Delegation Model)[14]을 적용하여 사용자 대 사용자, 역할 대 역할, 다단계, 다중 위임이 가능한 확장된 GTRBAC (Extended GTRBAC) 위임 모델을 제안한다.

3. 확장된 GTRBAC 위임 모델

확장된 GTRBAC 위임 모델(Extended GTRBAC Delegation Model)은 다음 그림 3과 같이 표현된다.

확장된 GTRBAC 위임 모델은 다음 그림 3에서와 같이 사용자 - 역할 할당 관계에 의해서 사용자에게 부역할들 중 고유역할만 할당하고 다른 부역할 들

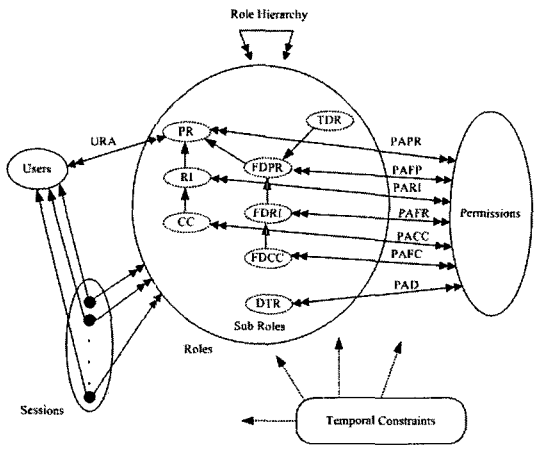


그림 3 Ex-GTRBAC 위임 모델

에 할당된 권한은 부역할 계층에 의해서 사용자가 고유역할을 활성화 했을 때 사용자에게 할당된다.

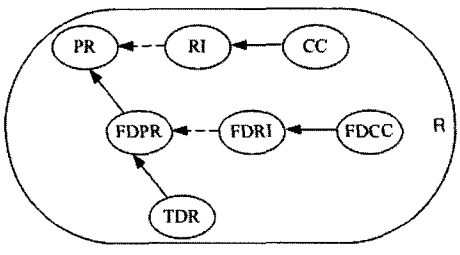
3.1 역할과 부역할 계층

확장된 GTRBAC 위임 모델에서는 다양한 위임 기능을 제공하기 위하여 확장된 GTRBAC 모델에 새로운 부역할을 추가해야할 필요가 있다.

확장된 GTRBAC 모델의 부역할을 상속정도에 따라 세종류(PR : Private Role, RI : Restricted Inheritance, CC : Corporate Common)의 부역할로 구분하고 각 부역할은 다른 사용자 또는 역할에 위임 가능한 권한이 할당되는 부역할(PR, RI, CC)과 위임 불가능한 권한이 할당되는 부역할(FDPR : Fixed Delegatable Private Roles, FDRI : Fixed Delegatable Restricted Inheritance, FDCC : Fixed Delegatable Corporate Common)로 구분 된다. 또한 확장된 GTRBAC 모델의 부역할 중 DC(부서 공통 역할)와 CC(조직 공통 역할)역할은 하나의 역할(CC)로 재설정하였다.

확장된 GTRBAC 위임 모델에서 부역할의 종류와 부역할 사이의 권한 상속 관계인 부역할 계층은 위 그림 4와 같다. 위 그림 4의 부역할 중 최상위에 있는 PR은 사용자 - 역할 할당 관계에 의해 사용자에게 할당되는 역할로 모든 부역할의 권한이 이 역할로 상속된다.

확장된 GTRBAC 위임 모델에서 새로 추가된 부역할은 FDPR, FDRI, FDCC, TDR(Temporal Delegatable Roles), DTR(Delegation Roles)이고 각 부역할의 특징과 부역할에 할당되는 권한의 특징은 다음과 같다.



〈그림 4〉 Ex-GTRBAC 위임 모델의 부역할 계층

· FDPR(Fixed Delegatable - PR)

역할 계층에서 상위 역할로 상속할 수 없는 권한이 할당되는 고유역할(PR)을 권한의 위임 가능성에 따라 위임 불가능한 권한이 할당되는 역할 PR과 위임 가능한 권한이 할당되는 역할 FDPR로 구분

역할 계층에서 상위 역할로 상속 불가능한 권한 중 다른 역할 또는 사용자에게 위임 가능한 권한이 할당.

· FDRI(Fixed Delegatable - RI)

역할 계층에서 상위 역할로 상속을 제한할 수 있는 상속 제한 역할(RI)을 권한의 위임 가능성에 따라 위임 불가능한 권한이 할당되는 역할 RI와 위임 가능한 권한이 할당되는 역할 FDRI로 구분

역할계층에서 정해진 역할까지 상위 역할로 상속이 가능한(제한된 상속) 권한 중 다른 역할 또는 사용자에게 위임이 가능한 권한이 할당.

· FDCC(Fixed Delegatable - CC)

역할 계층에서 상위 역할로 무조건 상속되는 권한이 할당되는 조직공통 역할(CC)을 권한의 위임 가능성에 따라 위임 불가능한 권한이 할당되는 역할 CC와 위임 가능한 권한이 할당되는 역할 FDCC로 구분.

역할 계층에서 상위 역할로 무조건 상속이 가능한 역할의 권한 중 다른 역할 또는 사용자에게 위임이 가능한 권한이 할당.

· TDR(Temporal Delegatable Role)

다른 역할 또는 사용자에게서 위임 받은 권한이 할당된 위임역할(DTR : Delegation Roles)을 역할 - 역할 할당에 의해 할당 받는 역할.

역할 계층에서 상위의 역할로 상속되지 않는다.

역할 - 역할 할당 관계에 의해 DTR에 할당된 권한을 수행할 수 있게 되므로 권한과의 할당 관계는 존재 하지 않는다.

이 역할을 사용함으로써 역할 대 역할 위임을 수행하였을 때 역할 계층에 의한 권한의 상속에 따른 문제가 발생하지 않는다.

· DTR(Delegation Roles)

역할 - 역할 할당 관계에 의해 TDR에 할당된 다음 사용자가 권한을 수행 할 수 있게 되므로 사용자와의 할당 관계는 존재하지 않는다.

보안 관리자에 의해 권한 또는 역할을 위임 하고자 할 때 생성 되고, 위임을 취소하고자 할 때 삭제된다.

위임 가능한 역할이나 권한이 할당된다.

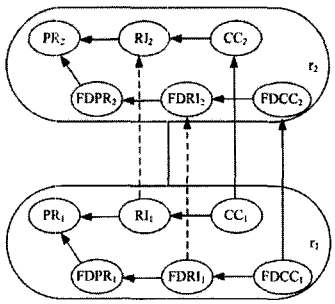
*TDR*에 할당된 권한 또는 역할(다른 사용자 또는 역할에게서 위임 받은 권한 또는 역할)을 할당 받으면 다단계 위임과 다중 위임이 이루어진다.

확장된 GTRBAC 위임 모델에서 부역할은 부역할에 할당된 권한들의 상속정도와 위임 가능성에 따라 다음 표 2와 같이 분류할 수 있다.

3.2 역할 계층

확장된 GTRBAC 위임 모델에서 역할 계층은 다층 형태로 존재하며 역할 계층상에서 상위 역할로의 상속 관계는 확장된 GTRBAC 모델의 상속 관계와 동일하다.

다음 그림 5는 확장된 GTRBAC 위임 모델의 역할계층에서 하위 역할에서 상위 역할로 권한 상속의 예이다. 그림 5에서 하위 역할에서 상위 역할로 연결된 실선은 공통 역할과 위임 가능한 공통 역할에 할당된 권한의 제한 없는 상속을 의미하고 점선은 상속 제한 역할과 위임 가능한 상속 제한



〈그림 5〉 확장된 GTRBAC 위임 모델의 역할 계층 예

역할에 할당된 권한이 제한적으로 상속됨을 의미한다. 또한 고유역할과 위임 가능한 고유역할의 권한은 상위 역할로의 연결선이 존재하지 않아 권한이 상위 역할로 상속되지 않음을 보여준다. 또한 다음 그림 5에서 확장된 GTRBAC 위임 모델에서 하위 역할에 할당된 권한이 상위 역할로 상속될 때 부역할 들은 상속 정도에 따라 공통 역할과 위임 가능한 공통 역할을 그룹으로 묶을 수 있으며, 상속 제한 역할과 위임 가능한 상속 제한 역할을 그룹으로, 마찬가지로 고유역할과 위임 가능한 고유역할을 그룹으로 구분할 수 있음을 알 수 있다.

다른 역할이나 사용자에게서 위임받은 권한 또는 역할이 할당되는 임시 위임 역할(TDR)과 위임 역할(DTR)은 역할 계층에 존재하지 않으므로 위임

〈표 2〉 확장된 GTRBAC 위임모델의 부역할 특징

부 역할	상속의 정도	위임의 정도	부 역할에 할당된 권한의 특징
공통역할 (CC)	무제한 상속	위임 불가능	-. 조직 내 모든 사용자에게 허가된 권한 -. 부서에 속한 사용자들에게만 허가된 권한 -. 상위 역할은 하위 역할의 모든 권한을 상속
위임 가능한 공통역할 (FDCC)		위임 가능	-. 조직공통역할(CC)의 특징 포함 -. 다른 역할 또는 사용자에게 위임 될 수 있다.
상속 제한 역할 (RI)	제한적 상속 (지정된 단계 만큼)	위임 불가능	-. 역할 분석과 설계 과정에서 상속이 제한되는 권한에 대한 조사 필요 -. 하위 역할의 권한이 지정된 상위 역할까지만 상위로 상속 -. 역할 간에 제한적 상속이 가능함
위임 가능한 상속 제한 역할 (FDRI)		위임 가능	-. 상속 제한 역할(RI)의 특징 포함 -. 다른 역할 또는 사용자에게 위임 될 수 있다.
고유역할 (PR)	상속 불가능	위임 불가능	-. 상위 역할로 상속이 이루어지지 않는 권한을 할당
위임 가능한 고유역할 (FDPR)		위임 가능	-. 고유역할(PR)의 특징 포함 -. 다른 역할 또는 사용자에게 위임 될 수 있다.
임시 위임 역할 (TDR)	상속 불가능	위임 가능	-. 위임자로부터 역할 대 역할 할당 관계에 의해 권한을 할당 -. 이 역할에 할당된 권한들은 다단계 위임 될 수 있다.

받은 권한 또는 역할은 상속되지 않음을 알 수 있다.

따라서 확장된 GTRBAC 위임 모델은 확장된 GTRBAC 모델과 동일한 역할계층을 가진다고 할 수 있다.

3.3 위임

확장된 GTRBAC 위임 모델은 기업 환경에서 반드시 필요하고 빈번히 발생할 수 있는 다양하고 정교한 위임 정책을 제공하며, 각 위임 기능은 다음과 같이 구현된다.

· 사용자 대 사용자 위임

사용자에게 할당된 위임 가능한 역할과 위임 가능한 역할에 할당된 권한을 위임 역할에 할당하여 다른 사용자에게 할당된 임시 위임 역할에 할당.

· 역할 대 역할 위임

사용자에게 할당된 위임 가능한 역할과 임시 위임 역할을 다른 임시 위임 역할에 할당.

· 다단계 위임

임시 위임 역할에 할당되어 위임된 권한을 다른 사용자에게 할당하고 이 사용자는 자신의 권한을 포함하거나 포함하지 않고, 또 다른 사용자들에게 할당.

· 다중 위임

사용자에게 할당된 위임 가능한 역할과 위임 가능한 역할에 할당된 권한을 여러 사용자에게 할당.

확장된 GTRBAC 위임 모델에서 권한을 위임하고 위임된 권한을 취소하는 과정은 다음과 같다.

· 권한의 위임

위임 역할(DTR) D를 생성

생성된 위임 역할 D에 위임 가능한 공통역할(FDCC), 위임 가능한 상속 제한 역할 (FDRI), 위임 가능한 고유역할(FDPR)에 할당된 권한 중 위임하고자 하는 권한을 할당한다.

위임 역할 D에 위임 가능한 공통역할(FDCC), 위임 가능한 상속 제한 역할 (FDRI), 위임 가능한 고유역할(FDPR) 중 위임 하고자 하는 역할을 할당 한다.

권한을 위임 받는 사용자에게 할당된 임시 위임 역할(TDR)에 위임 역할 D를 역할 대 역할 할당 관계에 의해 한다.

위의 네 단계에 의해서 사용자가 시스템에 로그인 했을 때 위임 받은 권한을 수행할 수 있게 된다.

위임된 권한의 취소는 권한의 위임과는 반대 과정을 통해 이루어진다.

· 위임된 권한의 취소

역할 대 역할 할당관계에 의해 임시 위임 역할(TDR)에 할당된 위임 역할 D의 할당 관계를 취소한다.

위임 역할 D에 위임된 역할과 권한을 취소한다.

위임 역할 D를 삭제한다.

확장된 GTRBAC 위임 모델은 위임 역할과 임시 위임 역할을 통하여 권한과 역할의 위임이 이루어지므로 기업 환경에서 반드시 필요하고 빈번히 발생할 수 있는 사용자 대 사용자, 역할 대 역할 위임과 다단계, 다중 위임 기능을 제공한다.

3.4 임시 역할 계층의 정형적 명세

제안 모델을 정형적으로 표현하면 다음의 정의[1~9]와 같고 정의에서 사용되는 기호들은 다음의 정리와 같다.

정리 : 모든 r, u, p, s는 시간 상수 $t \geq 0$ 일 때 다음과 같은 의미를 가진다. 이때 r(역할), u(사용자), p(권한), s(세션), rPR(고유 역할), rFDPR(위임 가능한 고유 역할), rRI(상속 제한 역할), rFDRI(위임 가능한 상속 제한 역할), rCC(조직 공통 역할), rFDCC(위임 가능한 조직 공통 역할), pPR(고유 역할에 할당된 권한), pFDPR(위임 가능한 고유 역할에 할당된 권한), pRI(상속 제한 역할에 할당된 권한), pFDRI(위임 가능한 상속 제한 역할에 할당된 권한), pCC(조직 공통 역할에 할당된 권한), pFDCC(위임 가능한 조직 공통 역할에 할당된 권한), rTDR(임시 위임 역할), pDTR(위임 역할에 할당된 권한)이다.

1. assigned(p, rPR, t) → can_be_acquired({pPR, pRI, pCC, pFDPR, pFDRI, pFDCC, pDTR},

{rPR, rRI, rCC , rFDPR, rFDRI, rFDCC, rTDR}, t)

2. assigned(u, rPR, t) → can_activate(u, rPR, t)
3. can_activate(u, rPR, t) ∧ can_be_acquired({pPR, pRI, pCC, pFDPR, pFDRI, pFDCC, pDTR}, {rPR, rRI, rCC, rFDPR, rFDRI, rFDCC, rTDR}, t) → can_acquire(u, {pPR, pRI, pCC, pFDPR, pFDRI, pFDCC, pDTR}, t)
4. active(u, rPR, s, t) ∧ can_be_acquired({pPR, pRI, pCC, pFDPR, pFDRI, pFDCC, pDTR}, {rPR, rRI, rCC, rFDPR, rFDRI, rFDCC, rTDR}, t) → acquires(u, {pPR, pRI, pCC, pFDPR, pFDRI, pFDCC, pDTR}, s, t)

각 함수의 의미는 다음과 같다.

· assigned() : 사용자 또는 권한에 역할의 할당
· can_be_acquired() : 권한의 획득 가능
· can_activate() : 역할 활성화 가능
· active() : 세션 상에서 역할의 활성화
· acquires() : 세션 상에서 권한의 획득

[정의 1] Unrestricted inheritance only hierarchy : 시간 t에 역할 x가 역할 y의 상위 역할 일 때(x ≥t y) I-역할 계층은 다음과 같은 의미를 가진다.

· yRI 의 권한 상속 범위가 역할 x 또는 x 보다 상위 역할로 지정되었을 경우 :

∀p, (x ≥t y) ∧ can_be_acquired({pRI, pCC, pFDRI, pFDCC}, {yPR, yRI, yCC, yFDPR, yFDRI, yFDCC}, t) → can_be_acquired(p, xPR, t)

· yRI 의 권한 상속 범위가 역할 x 보다 하위 역할로 지정되었을 경우 :

∀p, (x ≥t y) ∧ can_be_acquired({pCC, pFDCC,}, {yCC, yFDCC}, t) → can_be_acquired(p, xPR, t)

[정의 2] Activation hierarchy : 시간 t에 역할 x가 역할 y의 상위 역할 일 때(x ⩾t y) A-역할 계층은 다음과 같은 의미를 가진다.

∀u, (x ⩾t y) ∧ can_activate(u, xPR, t) → can_activate(u, yPR, t)

[정의 3] General inheritance hierarchy : 시간 t에 역할 x가 역할 y의 상위 역할 일 때(x ≥t y) IA-역할 계층은 다음과 같은 의미를 가진다.

(x ≥t y) ↔ (x ≥t y) ∧ (x ⩾t y)

[정의 4] Weakly restricted inheritance only hierarchy : 시간 t에 역할 x가 역할 y의 상위 역할 일 때(x ≥w,t y) I-역할 계층은 다음과 같은 의미를 가진다.

· yRI 의 권한 상속 범위가 역할 x 또는 x 보다 상위 역할로 지정되었을 경우 :

∀p, (x ≥w,t y) ∧ enabled(xPR, t) ∧ can_be_acquired({pRI, pCC, pFDRI, pFDCC}, {yRI, yCC, yFDRI, yFDCC}, t) → can_be_acquired(p, xPR, t)

· yRI 의 권한 상속 범위가 역할 x 보다 하위 역할로 지정되었을 경우 :

∀p, (x ≥w,t y) ∧ enabled(xPR, t) ∧ can_be_acquired({pCC, pFDCC}, {yCC, , yFDCC}, t) → can_be_acquired(p, xPR, t)

[정의 5] Weakly restricted activation hierarchy : 시간 t에 역할 x가 역할 y의 상위 역할 일 때(x ⩾t y) A-역할 계층은 다음과 같은 의미를 가진다.

∀u, (x ⩾w,t y) ∧ enabled(yPR, t) ∧ can_activate(u, xPR, t) → can_activate(u, yPR, t)

[정의 6] Weakly restricted general inheritance hierarchy : 시간 t에 역할 x가 역할 y의 상위 역할 일 때(x ≥w,t y) IA-역할 계층은 다음과 같은 의미를 가진다.

(x ≥w,t y) → (x ≥w,t y) ∧ (x ⩾w,t y)

[정의 7] Strongly restricted inheritance only hierarchy : 시간 t에 역할 x가 역할 y의 상위 역할 일 때(x ≥s,t y) I-역할 계층은 다음과 같은 의미를 가진다.

· yRI 의 권한 상속 범위가 역할 x 또는 x 보다 상위 역할로 지정되었을 경우 :

∀p, (x ≥s,t y) ∧ enabled(yPR, t) ∧ en-

abled(xPR, t) ∧ can_be_acquired({pRI, pCC, , pFDRI, , pFDCC}, {yRI, yCC, , yFDRI, yFDCC}, t) → can_be_acquired(p, xPR, t)

· yRI 의 권한 상속 범위가 역할 x 보다 하위 역할로 지정되었을 경우 :

∀p, (x ≥s,t y) ∧ enabled(yPR, t) ∧ enabled(xPR, t) ∧ can_be_acquired({pCC, pFDCC}, {yCC, yFDCC}, t) → can_be_acquired(p, xPR, t)

[정의 8] Strongly restricted activation hierarchy : 시간 t에 역할 x가 역할 y의 상위 역할 일 때(x ⩾s,t y) A-역할 계층은 다음과 같은 의미를 가진다.

∀u, (x ⩾s,t y) ∧ enabled(xPR, t) ∧ enabled(yPR, t) ∧ can_activate(u, xPR, t) → can_activate(u, yPR, t)

[정의 9] Strongly restricted general inheritance hierarchy : 시간 t에 역할 x가 역할 y의 상위 역할 일 때(x ≥s,t y) IA-역할 계층은 다음과 같은 의미를 가진다.

(x ≥s,t y) → (x ≥s,t y) ∧ (x ⩾s,t y)

단, 위 [정의 1, 2, 3]은 시간 제약을 이용하여 권한의 상속과 역할의 활성화를 제한하지 않는 경우이다.

3.5 확장된 GTRBAC 위임 모델의 정형적 명세

제안 모델을 정형적으로 표현하면 다음과 같다.

DBR = FDPR ∪ FDRI ∪ FDCC ∪ TDR : delegatable roles

R = PR ∪ RI ∪ CC ∪ DBR ∪ DTR

(PR ∩ DBR) ∪ (RI ∩ DBR) ∪ (CC ∩ DBR) = Ø

(PR ∩ DTR) ∪ (RI ∩ DTR) ∪ (CC ∩ DTR) = Ø

DBR ∩ DTR = Ø

(FDPR ∩ TDR) ∪ (FDRI ∩ TDR) ∪ (FDCC ∩ TDR) = Ø

URA ⊆ U × PR

PAPR ⊆ P × PR

PAFP ⊆ P × FDPR

PARI ⊆ P × RI

PAFR ⊆ P × FDRI

PACC ⊆ P × CC

PAFC ⊆ P × FDCC

PAD ⊆ P × DTR

PRA = PAPR ∪ PAFP ∪ PARI ∪ PAFR ∪ PACC ∪ PAFC ∪ PAD

RAD = TDR × DTR

user_r(r) : PR → 2U : 고유 역할에 할당된 사용자 에게 고유 역할을 매핑하는 함수

own_ri(r) : RI → PR : 부역할 계층에 의해 상속 제한 역할을 고유역할에 매핑하는 함수

own_cc(r) : CC → RI : 부역할 계층에 의해 조직 공통 역할을 상속 제한 역할에 매핑하는 함수

own_fdpr(r) : FDPR → PR : 부역할 계층에 의해 위임 가능한 고유 역할을 고유역할에 매핑하는 함수

own_fdri(r) : FDRI → FDPR : 부역할 계층에 의해 위임 가능한 상속 제한 역할을 위임 가능한 고유역할에 매핑하는 함수

own_fdcc(r) : FDCC → FDRI : 부역할 계층에 의해 위임 가능한 조직 공통 역할을 위임 가능한 상속 제한 역할에 매핑하는 함수

own_td(r) : TDR → FDPR : 부역할 계층에 의해 임시 위임 역할을 위임 가능한 고유 역할에 매핑하는 함수

∀rr ∈ PR, ∃u : U, ri : RI, cc : CC, fdpr : FDPR, fdri : FDRI, fdcc : FDCC, tdr : TDR • (u, rr) ∈ URA ∧ rr =

own_dpr(r) : FDPR → 2DTR and ∄(fdpr1, fdpr2 ∈ FDPR, dtr ∈ DTR) • (fdpr1 ≠ fdpr2) ∧ (dtr ∈ own_fdpr(fdpr1) ∧dtr ∈ own_fdpr(fdpr2)) : 위임 가능한 고유 역할을 위임 역할에 매핑하는 함수

own_dri(r) : FDRI → 2DTR and ∄(fdri1, fdri2 ∈ FDRI, dtr ∈ DTR) • (fdri1 ≠ fdri2) ∧ (dtr ∈ own_fdri(fdri1) ∧dtr ∈ own_fdri(fdri2)) : 위임 가능한 상속 제한 역할을 위임 역할에 매핑하는 함수

own_dcc(r) : FDCC → 2DTR and ∄(fdcc1, fdcc2 ∈ FDCC, dtr ∈ DTR) • (fdcc1 ≠ fdcc2) ∧ (dtr ∈ own_fdcc(fdcc1) ∧dtr ∈ own_fdcc(fdcc2)) : 위임 가능한 조직 공통 역할을 위임 역할에 매핑하는 함수

rad(r) : TDR → 2DTR : 임시 위임 역할에 위임 역할을 매핑하는 함수

permissions_pr(r) : PR → 2P : 권한 집합을 고유 역할에 매핑하는 함수

permissions_ri(r) : RI → 2P : 권한 집합을 상속 제한 역할에 매핑하는 함수

permissions_cc(r) : CC → 2P : 권한 집합을 조직 공통 역할에 매핑하는 함수

permissions_fdpr(r) : FDPR → 2P : 권한 집합을 위임 가능한 고유 역할에 매핑하는 함수

permissions_fdri(r) : FDRI → 2P : 권한 집합을 위임 가능한 상속 제한 역할에 매핑하는 함수

permissions_fdcc(r) : FDCC → 2P : 권한 집합을 조직 공통 역할에 매핑하는 함수

permissions_d(r) : DTR → 2P : 권한 집합을 위임 역할에 매핑하는 함수

permissions_t(r) : TDR → 2P : RAD 관계로부터 상속된 권한 집합을 임시 위임 역할에 매핑하는 함수

permissions_f(r) : FDPR → 2P : RAD와 PAFP, PAFR, PAFC 관계로부터 위임된 권한 집합을 위임 가능한 고유역할에 매핑하는 함수

permissions_pr(r) = {p : P | ∃r' ≤ r • (r', p) ∈ PAPR}

permissions_ri(r) = {p : P | ∃r' ≤ r • (r', p) ∈ PARI}

permissions_cc(r) = {p : P | ∃r' ≤ r • (r', p) ∈ PACC}

permissions_fdpr(r) = {p : P | ∃r' ≤ r • (r', p) ∈ PAFP}

permissions_fdri(r) = {p : P | ∃r' ≤ r • (r', p) ∈ PAFR}

permissions_fdcc(r) = {p : P | ∃r' ≤ r • (r', p) ∈ PAFC}

permissions_d(r) = {p : P | ∃r' ≤ r • (r', p) ∈ PAD}

permissions_t(r) = {p : P | ∃r' ∈ DTR • (r', p) ∈ PAD ∧ r' ∈ rad(r')}

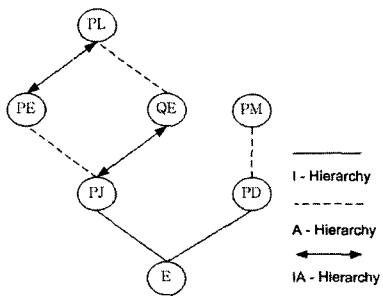
permissions_f(r) = {p : P | (r, p) ∈ PAFP} ∪ {p : P | ∃r' ∈ TDR • p ∈ permissions_t(r') ∧ r = own_td(r')} ∀dtr ∈ DTR, ∃ fdpr ∈ FDPR • ((dtr ∈ own_dpr(fdpr)) ∪ (dtr ∈ own_dri(fdri)) ∪ (dtr ∈ own_dcc(fdcc))) ∧ (permissions_d(dtr) ⊆ permission_f(fdpr)) : 생성된 위임 역할에 RAD와 PAFP, PAFR, PAFC에 의해 위임 가능한 역할들에 할당된 위임 가능한 권한. (다단계 위임에 필요)

can_delegate ⊆ FDPR × Pre_con × P_range × M : Pre_con 은 전제조건(prerequisite condition), P_range 는 위임 범위(delegation range), M 은 최대 위임 단계(maximum delegation depth) : 위임 범위, 전제조건, 최대 위임 단계에 따라 위임 가능한 역할의 매핑 관계 정의

4. 확장된 GTRBAC 위임 모델의 적용 예

다음 그림 6의 역할 계층을 사용하여 실제 기업 환경에서 확장된 GTRBAC 위임 모델의 적용 예를 보여준다. 그림 6의 GTRBAC 모델을 적용한 역할 계층을 확장된 GTRBAC 위임 모델을 적용한 역할 계층으로 수정하면 그림 7과 같다. 또한 사용자-역할 할당 관계는 표 3과 같고 권한-역할 할당 관계는 표 4와 같다.

확장된 GTRBAC 위임 모델에서도 GTRBAC 모델에서와 같이 역할 계층은 I(permission - in-



〈그림 6〉 GTRBAC 모델의 역할 계층 예

〈표 3〉 GTRBAC 위임 모델의 사용자-역할 할당 관계 예

역할		할당관계	사용자
PL (Project Leader)	PL : Non Delegatable Role Set PL′ : Fixed Delegatable Role Set PL″ : TDR	URA (User - PR)	John
PE (Programming Engineer)	PE : Non Delegatable Role Set PE′ : Fixed Delegatable Role Set PE″ : TDR	URA (User - PR)	Tom
QE (Quality Engineer)	QE : Non Delegatable Role Set QE′ : Fixed Delegatable Role Set QE″ : TDR	URA (User - PR)	Smith
PJ (Project)	PJ : Non Delegatable Role Set PJ′ : Fixed Delegatable Role Set PJ″ : TDR	URA (User - PR)	Jenny
PM (Production Manager)	PM : Non Delegatable Role Set PM′ : Fixed Delegatable Role Set PM″ : TDR	URA (User - PR)	Scott

〈표 4〉 GTRBAC 위임 모델의 권한-역할 할당 관계 예

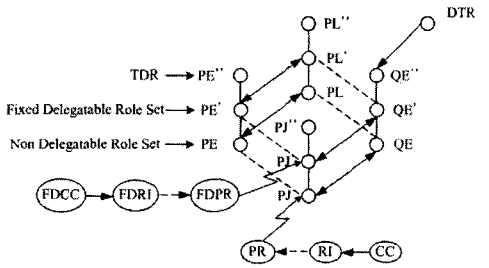
Non Delegatable Role Set		권한	Fixed Delegatable Role Set		권한	TDR	권한
PL	PR		PL′	FDPR	change_schedule	PL″	use_pj2_bbs
	RI	confirm_program		FDRI			
	CC			FDCC			
PE	PR		PE′	FDPR		PE″	
	RI			FDRI	req_program		
	CC			FDCC			
QE	PR	error_report	QE′	FDPR		QE″	
	RI			FDRI			
	CC			FDCC	review_program		
PJ	PR		PJ′	FDPR		PJ″	
	RI	use_pj1_bbs		FDRI			
	CC			FDCC			

heritance - only hierarchy), A(role - activation - only hierarchy), I-A(permission - inheritance - activation hierarchy) 역할 계층과 같은 부분 역할 계층이 존재하고 이들 역할 계층은 역할의 활성화/비활성화 제약과 시간 제약을 이용하여 제한된 상속 기능을 제공한다.

다음 그림 7은 위 그림 6의 역할 계층 일부를 확장된 GTRBAC 위임 모델의 역할 계층으로 표현한다.

그림 7의 역할 계층상에서 일반 역할과 위임 가능 역할에 할당된 권한은 상위 역할로 할당됨을 알 수 있고, 위임 받은 역할 또는 권한이 할당된 위임 역할이 역할-역할 관계에 의해 할당되는 임시 위임 가능 역할 계층에는 위임 받은 권한 만 할당 되어 있으므로 상위 역할로 상속되지 않음을 알 수 있다.

실제 기업 환경에서 다음 표 3, 4와 같은 할당 관계에 의해 사용자에게 역할이 할당되고, 권한에



〈그림 7〉 확장된 GTRBAC 위임 모델의 역할 계층 예

역할이 할당 되었을 때 위임 가능한 역할 집합 PL'에 할당된 권한 "change_schedule"과 위임 가능한 역할 집합 PE'에 할당된 권한 "req_program"을 사용자 "Smith"가 액세스 가능하도록 위임하는 과정은 다음과 같다.

· 권한 위임 과정

① 권한의 위임 과정을 수행하기 위하여 위임 역할 D(DTR)를 생성한다.

② 생성된 위임 역할 D에 PL'의 FDPR에 할당된 권한 "change_schedule"를 할당한다.

③ 생성된 위임 역할 D에 위임 가능한 역할 집합 PE'의 역할 FDRI를 할당한다.

④ 권한-역할 할당 관계인 PAD에 의해 할당된 권한 "change_schedule"와 "req_program"을 사용자 "Smith"가 액세스 가능하도록 임시 위임 가능 역할 QE''에 위임 역할 D를 할당한다.

위임된 권한의 위임취소는 보안 관리자에 의해 다음과 같은 방법으로 가능하다.

· 위임 역할 D에 PAD에 의해 할당된 권한의 할당관계 취소

· 위임 역할 D의 취소

· 위임 가능 역할에 할당된 권한을 일반 역할에 할당

5. 제안 모델과 기존 모델의 비교

시간(기간과 주기)에 따른 제약으로 자원의 사용을 제한할 수 있고, 역할 활성화와 이벤트, 트리거를 이용하여 사용자 수를 제한하고 워크플로우에 해당하는 작업을 다룰 수 있는 장점을 가지는 GTRBAC (Generalized Temporal Role Based Access Control)모델에 부역할(sub role) 개념을 적용하여 하위 역할에 배정된 권한을 상위 역할에 배정된 사용자가 모두 상속하여 실행할 수 없도록 하여 권한의 남용을 방지하고 최소권한 원칙을 이행할 수 있도록 하고 PBDM(Permission Based Delegation Model)을 적용하여 사용자 대 사용자, 역할 대 역할, 다단계, 다중 위임이 가능한 확장된 GTRBAC (Extended GTRBAC) 위임 모델과 기존 접근제어 모델의 특징을 비교하면 다음 표 5와 같다.

위 표5에서 기존 모델과 제안 모델과의 비교 항목은 접근제어 모델을 실제 기업 환경에 적용하기 위하여 반드시 고려되어야하는 항목이다. 기업 구

〈표 5〉 제안 모델과 기존 모델의 특징 비교

		RBAC	ABAC	TRBAC	GTRBAC	sub-role	PBDM	제안모델
워크플로우 고려		×	○	클래스W 과업 이용	이벤트와 트리거 이용	×	×	이벤트와 트리거 이용
일반 역할 및 권한 고려		○	×	○	○	○	○	○
역할 활성화 유효시간과 유효 기간 제약		×	×	×	○	×	×	○
사용자의 위치 정보에 따른 역할 활성화 제약		×	×	×	×	×	×	×
사용자의 위치 정보에 따른 역할의 제한적 상속		×	×	×	×	×	×	×
역할의 제한적 상속	역할의 활성화 제약과 유효 시간 제약	×	×	×	○	×	×	○
	부역할 이용	×	×	×	×	○	×	○
역할 활성화 유효 시간 및 기간 적용		×	×	×	○	×	×	○
위임	사용자 대 사용자	×	×	×	×	○	○	○
	역할 대 역할	×	×	×	×	○	○	○
	다단계	×	×	×	×	×	○	○
	다중	×	×	×	×	×	○	○
	위임된 권한이 할당된 역할의 유효 시간 및 기간에 따른 제약	×	×	×	×	×	×	○

성원간의 연속적인 업무환경을 고려하기 위하여 워크플로우가 고려되어야 하고, 시간과 기간에 따른 권한을 제어할 수 있어야 하며, 역할의 상속을 제한하여 최소 권한 만으로 업무 수행이 가능하여야 하며, 사용자에게 할당된 권한을 위임 할 수가 있어야 한다.

부역할(sub-role) 계층 모델[7,8]은 제안 모델의 중요한 특징 중 하나인 역할 계층에서 상위 역할로 상속되는 권한을 제한하는 기능을 제공하지만 권한의 위임 기능을 제공하지 않고, PBDM 모델[14]은 정교한 위임 정책을 제공하지만 권한의 상속을 제한하는 기능이 부족하다.

기존의 RBAC(Role Based Access Control)[2,3], ABAC(Activity Based Access Control)[4,5], TRBAC (Task-Role Based Access Control)[6], GTRBAC (Generalized Temporal Role Based Access Control)[10-12] 모델은 권한의 상속 제한 기능, 권한의 위임 기능 두 가지 모두를 고려하지 않고 있으며, 워크플로우를 고려하지 않는 경우도 있어 기업환경에 적용하기에는 무리가 따르며, 제안 모델 또한, 사용자의 위치 정보에 따른 역할의 활성화 제한과 역할의 제한적 상속 기능을 제공하지 않아 모바일 기업 환경의 접근제어에 적용할 수 없는 단점이 있다.

6. 결 론

본 논문에서는 시간(기간과 주기)에 따른 제약으로 자원의 사용을 제한할 수 있는 GTRBAC (Generalized Temporal Role Based Access Control)[10-12] 모델에 부역할(sub role)[7,8] 개념을 적용하여 하위 역할에 배정된 권한을 상위 역할에 배정된 사용자가 모두 상속하여 실행할 수 없도록 권한의 남용을 방지하고, PBDM 개념을 적용하여 기업 환경에서 반드시 필요하고 빈번히 발생할 수 있는 사용자 대 사용자(user to user) 권한 위임과 역할 대 역할(role to role) 권한 위임, 다단계 위임 및 다중 위임이 이루어질 수 있는 새로운 위임 모델을 제시한다.

제안 모델은 보안 관리자에 의해 위임 역할을 생성하여 위임될 권한과 역할을 할당한 후 위임 역할을 위임 받을 사용자에게 할당된 임시 위임 역할에 역할 대 역할 할당관계에 의해 할당함으로써 권한이 위임되고 반대의 과정으로 위임된 권한이 취소된다.

향후에는 실제 기업 환경에서 발생할 수 있는 다양한 권한의 상속과 위임 같은 문제를 해결하기 위하여 접근제어 시스템에 다양하고 복잡한 제약을 적용하였을 때 보안 관리자가 정책을 보다 간편하고 효율적으로 관리할 수 있는 형식 언어와 관리 모델 및 시스템에 대한 연구가 필요할 것으로 사료된다.

참 고 문 헌

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

[2] R.S.Sandhu and E.J.Coyne and H.L.Feinstein and C.E.Youman "Role-Based Access control Method", IEEE Computer, vol. 29, 1996

[3] D.Ferraiom and J.Cugini and R.Kuhm "Role-based Access Control(RBAC) : Features and motivations", Proc. of 11th Annual Computer Security Application Conference, 1995

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

[5] R.K.Thomas and R.S.Sandhu "Task-based Authorization Controls(TBAC) : A Family of Models for Active and Enterprise-oriented Authorization Management" Proc. of the IFIP WF11.3 Workshop on Database Security, 1997

[6] S. Oh and S. Park "Task-Role Based Access Control (T-RBAC): An Improved Access Control Model for Enterprise Environment", Proceedings of the 11th International Conference on Database and Expert Systems Applications, pp. 264-273, 2000

[7] HyungHyo Lee and YoungRok Lee and BongNam Noh "A New Role-Based Delegation Model Using Sub-Role Hierarchies" Proceedings of the 18 th Computer and Information Sciences - ISCIS2003, 2003

[8] YongHoon Yi and MyongJae Kim and YoungLok Leem and HyungHyo Lee and BongNam Noh "Applying RBAC Providing Restricted Permission Inheritance to a Corporate Web Environment", Proceedings of the 5 th Asia-Pacific Web Conference, 2003

[9] E. Bertino and P. A. Bonatti and E. Ferrari "TRBAC: A Temporal Role-based Access Control Model", Proceedings of the fifth ACM workshop on Role-based access control, pp.21-30, 2000

[10] J. B. D. Joshi and E. Bertino and A. Ghafoor "Temporal Hierarchies and Inheritance Semantics for GTRBAC", Seventh ACM Symposium on Access Control Models and Technologies, pp. 74-83, 2002

[11] J. B. D. Joshi and E. Bertino and A. Ghafoor "Hybrid Role Hierarchy for Generalized Temporal Role Based Access Control Model", Proceedings of the 26 th Annual International Computer Software and Applications Conference, 2002

[12] J. B. D. Joshi and E. Bertino and A. Ghafoor "Temporal Role Hierarchies in GTRBAC", CERIAS, 2002

[13] 황유동, 박동규, "기업환경의 접근제어를 위한 확장된 GTRBAC 모델", 한국멀티미디어학회, 2005.02, 8권 2호

[14] Xinwen Zhang, Sejong Oh, Ravi Sandhu "PBDM : A Flexible Delegation Model in RBAC", SACMAT, 2003

◐ 저 자 소 개 ◑

황 유 동(Hwang Yu-Dong)
1998년 순천향대학교 제어계측공학과 졸업(학사)
2000년 순천향대학교 대학원 전기전자공학과 졸업(석사)
2003년 순천향대학교 대학원 전기전자공학과 수료(박사)
관심분야 : 시스템 보안, 네트워크 보안
E-mail : coppermilk@sch.ac.kr

박 동 규 (Park Dong-Gue)
1985년 한양대학교 전자공학과 졸업(학사)
1988년 한양대학교 대학원 전자공학과 졸업(석사)
1992년 한양대학교 대학원 전자공학과 졸업(박사)
1992년~현재 순천향대학교 정보기술학부 교수
관심분야 : 시스템 보안, 네트워크 보안
E-mail : dgpark@sch.ac.kr