의무 분리를 위한 직무 기반 접근권한의 모델링

천 은 홍[†] · 김 동 규[††]

요 약

기존의 접근 제어 메커니즘인 강제적 접근 제어와 임의적 접근 제어는 무결성을 요구하는 상용 환경의 정보 보안에는 부족하여 이의 대안으로 직무 기반 접근 제어(RBAC:Role Based Access Control)가 주목 받고 있으며, 직무를 수행하는 사용자의 의무 분리(Separation of Duty)에 대한 연구가 최근 이루어지고 있다. RBAC에서 사용자는 직무에 배정된 접근권한(Privilege) 만을 수행하여야 하는데 상호 배타적(Mutual exclusive) 특성을 갖는 직무는 표현 및 접근권한의 직무 배정과 수행에 있어서 어려움이 있다. 본 논문에서는 RBAC의 기본 특성을 분석하여 직무에 접근권한을 부여하고 사용자를 직무에 배정하는데 따른 안전한 접근 제어를 위하여 반순서 관계를 갖는 직무의 승계 속성에 따라 직무의 계층 형태를 분류하고, 직무에 배정되는 접근권한의 표현과 관리를 용이하게 하기 위하여 객체에 부여된 객체 접근권한을 분석하여 방향성 그래프를 이용하여 기본 접근권한으로 모델링한다. 접근권한 그래프(Privilege Graph)로 표현된 기본 접근권한에 직무를 배정하면 상호 배타적 직무의 접근권한과 의무 분리의 표현 및 관리를 용이하게 할 수 있다. 이를 기반으로 의무 분리를 포함한 RBAC의 안정성 특성과 접근권한 그래프를 이용한 직무의 의무 분리를 위한 직무 관리 알고리즘을 제시한다.

A Modeling of Role Based Access Privileges for Separation of Duties

Eun-Hong Cheon[†] · Dong-Kyoo Kim[††]

ABSTRACT

The MAC(Mandatory Access Control) and DAC(Discretionary Access Control) policies which it was described for access control had been explored to prevent the unauthorized disclosure of classified information. A RBAC(Role Based Access Control) has been focused as an alternative to realize integrity for organization's information assets in commercial environment. A separation of duty for a authority and responsibility according to perform privileges has been researched today. With RBAC, when a user is assigned roles in a mutual exclusive sets, user must perform only privileges to ensure mutual exclusive property. There are some difficulties in representation and assignments of privileges for mutual exclusive roles.

In this paper, we examine the inheritance properties of roles with partial ordering relations, and classify a kind of forms for the role hierarchy. We examine the relationships between roles and privileges, and modeling object privileges to ordinary privileges using the property of direct acyclic graph. A Privilege Graph can provide flexibility in representations and assignments of mutually exclusive privileges. We define the separation of duty including mutual exclusive roles and propose safety properties, and show that the role management algorithms can enforce separation of duty.

1. 서 론

최근들어 컴퓨터와 정보통신 기술이 발달하여 컴퓨터의 자료 처리 능력이 향상되고 정보의 저장 용량이 대형화됨에 따라 사용자의 요구를 만족시키기 위한 정보의 공유 및 전송 등이 이루어지고 있다. 이와 같이 컴퓨터를 이용하여 취급되고 있는 정보들이 증가하면서

※ 이 논문은 1998년도 우석대학교 학술연구 조성비에 의하여 연구되었음.

† 정 회 원 : 우석대학교 정보통신 및 컴퓨터공학부
†† 정 회 원 : 아주대학교 정보 및 컴퓨터공학부 교수

논문접수 : 1998년 2월 16일, 심사완료 : 1998년 6월 23일

이들 정보에 대한 불법적인 사용자에 의한 정보의 누출이 발생하고 있다. 정보 자원에 대한 접근 제어에서 발생할 수 있는 위협은 정보나 망의 자원의 파괴, 정보의 변형이나 불법적인 수정, 정보나 다른 자원의 절도, 제거, 분실과 정보의 불법적인 승인되지 않은 노출 등으로 나타날 수 있다. 자동화 시스템 환경에서 개인이나 기관의 중요한 정보를 권한이 없는 불법 침입자로부터 보호하고, 불법 접근에 의한 정보의 노출 및 불법 내용 변경 등에 대한 보안 대책이 중요한 문제로 등장하게 되었다.

컴퓨터 망의 정보 보호를 위하여 ISO, ITU, NIST, NCSC 등의 표준 기관에서 보안 서비스와 메커니즘에 대한 많은 논의와 연구가 진행되고 있다. ISO/IEC JTC1/SC1에서는 보안을 위한 표준 참조모형으로 7498-2 보안구조(Security Architecture)를 통하여 보안 위협 요소와 개방형 시스템간에 사용될 수 있는 보안 서비스 및 기법에 대하여 기술하였고[7], 보안 서비스 중에서 접근 제어(Access Control) 서비스에 대한 주요 연구로 기밀성 제어를 위한 BLP(Bell LaPudula) 모델[2]과 Denning의 정보 흐름(Information flow) 모델[13] 등의 연구가 이루어졌다. 미국의 NCSC(National Computer Security Center)는 1983년에 컴퓨터 시스템의 보안 요구 사항과 평가 등급에 대한 보안 평가 지침서인 TCSEC(Trusted Computer Security Evaluation Criteria)[4]를 발표하여 이를 기준으로 보안 시스템들이 개발되고 있다.

TCSEC에 기술된 강제적 접근 제어(MAC:Mandatory Access control)와 임의적 접근 제어(DAC:Discretionary Access Control)는 등급화된 정보에 대한 비승인된 접근의 방지로 기밀성 제어에 초점이 맞추어져 있다. 강제적 접근 제어는 BLP 모델의 단순 특성(simple property)이나 스타 특성(*-property)과 같이 주체에 부여되는 보안 자격(clearance)과 객체에 부여되는 보안 등급(classification)으로 주어진 보안 레이블(label)에 따라 접근을 제어하는 보안 정책이고, 임의적 접근 제어는 사용자나 그룹의 식별자에 따라 객체에 대한 접근을 제한하는 수단으로 객체의 소유자는 시스템 관리자의 간섭없이 주체의 객체에 대한 접근권한을 임의로 지정하거나 다른 주체에게 간접적으로 위임할 수 있다.

기업이나 정부 조직 등의 상용환경에서의 접근 제어를 위한 연구가 진행되고 있는데 MAC은 등급화된 정보의 기밀성을 위한 보안에 초점이 맞춰져 있고, DAC은 접근제어 권한이 주체에 의해 임의로 주어질 수 있어서 기업이나 정부 조직과 같이 무결성을 요구하는 상업적 응용의 정보 보안에는 부적절하다. 이와 비교하여 직무 기반 접근 제어는 무결성 제어가 필요한 상업 응용에 적합하고 사용자가 배정될 직무의 접근권한을 시스템 관리자가 부여하는 비임의적 접근 제어(non-discretionary access control)로써 전통적인 접근 제어 기법인 MAC 및 DAC의 보완책으로 주목받고 있다[5, 15].

RBAC과 상용환경에서의 무결성 접근 제어와 관련된 연구를 살펴보면, Clark와 Wilson[3]이 군용 환경에 적합한 기존의 접근 제어 모델과 비교하여 상용 환경에서의 데이터 무결성 제어를 위해 잘 정의된 트랜잭션(Well-Formed Transaction)과 의무 분리의 필요성을 제안한 이래, 상용 환경에서의 의무 분리[10,12] 및 무결성 제어에 관한 연구[8,9]가 계속되어 왔고, 최근에는 직무 환경에서 의무 분리에 대한 연구[11,16]가 이루어지고 있다. Baldwin[1]은 데이터 베이스에서의 접근제어를 위하여 보안 영역(NPD:Named Protection Domain)를 이용하여 직무와 유사한 개념을 제시하고 그래프를 이용하여 보안 영역을 표현하였다.

NIST의 Ferraiolo와 Kuhn[5,6]은 상용 환경에서의 효과적인 접근 제어를 위해 사용자가 임의로 접근권한을 줄 수 있는 임의적 메커니즘 특성을 갖는 그룹과 비교하여 RBAC을 시스템 관리자가 접근권한을 부여하는 비임의적 메커니즘으로 기술하고, 접근권한의 성질을 화일의 접근 모드가 아닌 접근 권한과 데이터의 집합으로 표현하는 트랜잭션을 이용한 응용 레벨에서의 접근 개념을 도입하여 RBAC의 기본 특성을 기술하였다. Sandhu[14,15]는 RBAC의 정형화된 통합 모델을 위해 의무 분리를 포함한 다차원 모델을 개발하고 분류하여 RBAC 기본 모델을 정의하고, RBAC에서의 제한 사항(Constraints)을 기술하였다.

본 논문에서는 2장에서 RBAC의 개념과 기본 모델에 따라 특성을 분석하고, 3장에서 직무의 접근권한 배정 및 수행을 용이하도록 하기 위하여 반순서 관계에 갖는 직무의 승계 속성에 따라 직무의 계층을 분류하고, 접근권한 그래프를 이용하여 상호 배타적 성질을 갖는 객체 접근권한과 직무에 배정되는 접근권한인 기

본 접근권한의 관계를 모델링한다. 이를 기반으로, 4장에서 사용자가 직무를 수행하는데 있어서 의무 분리를 준수하기 위한 안정성 특성과 접근권한 그래프를 이용하여 표현된 직무의 의무 분리를 위한 직무 수행 특성 알고리즘을 제안하고, 5장에서 결론과 향후 연구 방향을 제시한다.

2. RBAC의 개념

RBAC의 기본 개념을 살펴보고, 최근 연구되고 있는 RBAC의 기본 모델의 정의에 따른 성분들을 분석한다.

2.1 RBAC의 개념

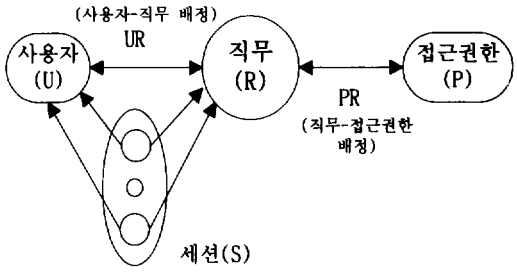
직무는 자원에 대한 접근이 허가된 개인이나 그룹으로 정의할 수 있다. 직무는 그룹과 비슷한 개념으로 그룹은 사용자의 모음으로 화일에 대한 읽기, 쓰기와 실행 등의 접근권한이 임의로 부여되는데, 직무는 사용자 및 접근권한의 모음으로 트랜잭션 형태의 접근권한이 시스템 관리자에 의해 부여된다.

RBAC에서 시스템 관리자는 기업이나 조직에서 수행할 업무 기능에 따라 직무를 생성하여 직무에 접근권한을 부여하고, 사용자를 책임과 자격에 따라 직무에 배정한다. 직무는 조직 체제에 따라 여러 작업 기능으로 표현되고, 직무에는 필요에 따라 쉽게 새로운 접근권한이 부여되고 삭제될 수 있다. 이와 같이, RBAC에서는 접근권한이 직무에 부여되므로 시스템이 변경될 때 필요에 따라 쉽게 새로운 접근권한을 직무에 부여하거나 삭제할 수 있고, 조직의 요구에 따른 접근 제어 정책의 관리를 용이하게 한다.

RBAC의 접근 제어는 직무-접근권한(role-privilege), 직무-사용자(role-user)와 직무-직무(role-role)의 성분으로 이루어지고, 시스템 관리자에 의해 직접적으로 혹은 시스템 관리자에 의해 위임된 적절한 직무에 의해 간접적으로 구성된다. 직무-직무 관계는 상호 배타적으로 설정되거나 권한의 승계가 이루어질 수 있고, 직무 간의 관계에 따라 직무-사용자를 배정하여 의무 분리와 권한의 위임을 포함하는 보안 정책을 준수할 수 있다. 직무-접근권한 관계는 직무에 대해 접근권한이 미리 정의되므로 시스템 관리자가 사용자에게 접근권한을 부여하는 것보다 직무-접근권한 배정의 변화 없이 직무에 사용권을 부여하거나 삭제할 수 있어서 접근권한의 관리가 용이하다[15].

2.2 RBAC 기본 모델

RBAC에서 접근권한이 직무에 부여되고 사용자는 직무의 일원이 되어 접근권한을 배정받는다. RBAC 모델은 (그림 1)과 같이 사용자(U), 직무(R), 접근권한(P), 세션(S)의 개체로 구성된다.



(그림 40) RBAC 모델
(Fig. 1) RBAC Model

【정의 2.1】 RBAC은 직무-사용자(UR), 직무-접근권한(PR)의 성분을 갖고, 다음과 같은 특성을 갖는다.

- 사용자-직무(UR) 관계는 $U_r: R \rightarrow 2^u$
- 접근권한-직무(PR) 관계는 $P: R \rightarrow 2^{pv}$

사용자 $U=\{id_1, id_2, \ldots, id_i\}$는 객체에 대해 접근 동작을 하려는 일반 사용자이고, 직무 $R=\{r_1, r_2, \ldots r_i\}$는 사용자에게 주어지는 권한과 책임을 가진 조직 내의 작업 기능이다. 접근권한 $P=\{pv_1, pv_2, \ldots pv_i\}$은 접근 권리나 특권 등으로 표현할 수 있는 시스템에서 하나 이상의 객체에 대한 특별한 접근 모드의 승인으로 접근권한은 그들의 소유자에게 시스템에서 행동을 수행할 수 있도록 하고, 사용자는 세션 $S=\{s_1, s_2, \ldots, s_i\}$에 의해 직무를 수행한다.

RBAC은 직무-접근권한(PR), 직무-사용자(UR)와 직무-직무(RR)의 성분으로 이루어진다. 직무-접근권한은 직무에는 다수의 접근 권한이 부여될 수 있고 동일 접근권한에 여러 직무가 배정될 수 있는 관계로 $P(r_i)=\{pv_1, pv_2, \ldots, pv_i\}$로 표현할 수 있다. 사용자-직무는 사용자는 여러 직무를 갖을 수 있고 동일

직무에 다수의 사용자가 배정될 수 있는 관계로 $U(r_i)=\{id_1, id_2, \ldots, id_i\}$로 표현할 수 있다.

【정의 2.2】 사용자는 세션 (s_i)에 의해 직무를 수행하고, 세션은 다음과 같은 특성을 갖는다.

- 사용자와 세션의 관계는 $U : S \rightarrow U$,
- 사용자 세션의 직무는 $R : S \rightarrow 2^R$이고 $R(s_i) \subseteq \{r | (U(s_i), r) \in U_r\}$,
- 사용자 세션 (s_i)의 접근권한은 $\bigcup_{r_i \in R(s_i)} P(r_i)$.

사용자는 세션에 의해 그들에게 배정된 직무를 수행한다. 각 세션은 한 사용자에 관계하고, 한 사용자에게 배정된 여러 직무의 수행을 가능하게 한다. 사용자가 활성화한 세션의 직무는 사용자에 배정된 직무의 부분집합이다. 사용자는 다중 세션을 열 수 있고, 각 세션은 다른 활성화된 직무를 조합한다. 사용자의 세션이 갖는 접근권한은 활성화한 세션의 직무에 허가된 접근권한의 합집합이다.

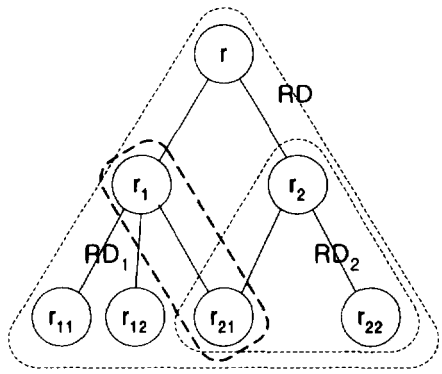
3. 직무와 접근권한

RBAC은 직무에 접근권한을 부여하고, 사용자를 직무에 배정하므로 RBAC의 성분인 직무-접근권한, 직무-사용자, 직무-직무 관계의 세밀한 분석이 필요하다. 직무의 접근권한 배정 및 수행을 용이하도록 하기 위하여 반순서 관계에 갖는 직무의 승계(inheritance) 속성에 따라 직무의 계층(role hierarchy)을 분류하고, 방향성 그래프를 이용하여 접근권한 관계를 모델링하여 직무를 배정함으로써 의무 분리의 준수를 용이하게 할 수 있다.

3.1 직무 계층

직무 계층은 조직 체제에서 직무의 권한과 책임을 반영하여 직무를 구성하는 기본 수단으로 직무 계층은 직무 영역(RD:Role Domain)의 집합으로 표현될 수 있다. 직무 영역은 조직에서 한 기능을 수행하는 직무의 집합으로 시스템내에서 사용자의 행동을 제어하는 접근권한의 집합으로 기술되며 주어진 직무를 갖는 사용자는 해당 직무 영역내의 접근권한을 수행할 수 있다. 어떤 조직에서 한 부서의 업무는 확실하게 구분되어 있으며 부서에서 수행해야 하는 업무를 직무 영역으로 정의할 수 있다.

본 논문에서는 직무 계층에서 직무간의 관계를 표현하기 위하여 (그림 2)와 같은 그래프로 구성한다. 직무 계층은 직무 영역(r, r_1, r_2), (r_1, r_{11}, r_{12}), (r_2, r_{21}, r_{22})의 집합(RD, RD_1, RD_2)으로 구성될 수 있고, 부서간의 직무의 관련성에 따라 일부 직무는 다른 부서의 직무에 연결(r_1, r_{21})되어 정보의 흐름이 발생될 수 있다.



(그림 41) 직무 계층과 직무 영역
(Fig. 2) Role Hierarchy and Domain

3.2 직무의 승계

직무 계층에서 직무는 위치에 따라 상위 직무(r_s:senior role)와 하위 직무(r_j:junior role)로 구성될 수 있다. 상·하위 직무에 있어서 두 직무간의 정보의 흐름을 (→) 으로 표현할 때, 임의의 직무 집합이 $(r_i \rightarrow r_i)$인 반사, $(r_i \rightarrow r_j)$ 이고 $(r_j \rightarrow r_i)$ 이면 $r_i = r_j$ 인 반대칭, $(r_i \rightarrow r_j)$ 이고 $(r_j \rightarrow r_k)$ 이면 $r_i \rightarrow r_k$ 인 천이 관계를 갖으면 반순서 관계(partial ordering relation : $\geq$)라 하고, 그 관계를 갖는 집합을 반순서 집합(partial ordered set)이라 한다. 직무 계층에서 접근권한은 상·하위 직무간의 반순서 관계에 따라 승계될 수 있고, 반순서 관계를 만족하는 다중 승계가 이루어질 수 있다.

【정의 3.1】 임의의 직무 (r_j) 가 다른 직무 (r_i) 로 승계 ($r_j \leq r_i$)될 때, 직무 (r_i) 의 세션 (s_i)은 다음과

같은 특성을 갖는다.

- 사용자 세션 (s_i)의 직무는

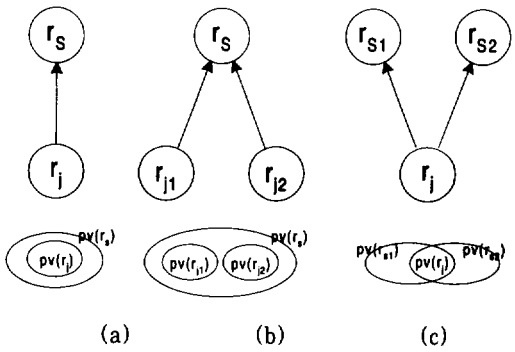
$$R(s_i) \subseteq \{r \mid (\exists r_i \geq r)(U(s_i), r_i) \in U_r\}.$$

- 사용자 세션 (s_i)의 접근권한은

$$\bigcup_{r_i \in R(s_i) \mid \exists r_j \leq r_i} P(r_j)$$

직무 (r_j) 가 승계 $(r_j \leq r_i)$ 될 때 사용자가 활성화한 세션의 직무는 사용자의 직무와 직무를 승계한 하위 직무가 활성화한 세션 (s_i)이 속한 직무의 부분집합이고, 사용자의 세션 (s_i)이 갖는 접근권한은 세션에서 활성화된 모든 직무에 허가된 접근권한과 승계된 하위 직무에 배정된 접근권한의 합집합이다.

반순서 관계 있는 직무는 접근권한의 승계 속성에 따라 단순 접근권한 승계(SI:Simple Inheritance), 공통 상위 접근권한 승계(CS:Common Senior inher-itance)와 공통 하위 접근권한 승계(CJ:Common Junior inheritance)의 세가지 유형으로 구분된다.



(그림 42) 직무의 기본 구성
(Fig. 3) Role Basic Organization

【정의 3.2】 하위 직무 (r_j)의 접근권한이 반순서 관계에 있는 상위 직무 (r_s)로 승계되면 단순 접근권한 승계 $(r_j, r_s) \in SI$라 하고, 접근권한은 $P(r_j) \subseteq P(r_s)$의 특성을 갖는다

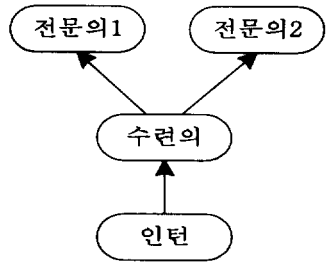
단순 접근권한 승계는 (그림 3)의 (a)와 같이 하위 직무 (r_j) 의 접근권한이 반순서 관계에 있는 상위 직무 (r_s)로 승계되어 하위 직무의 접근권한을 수행할 수 있도록 한다.

【정의 3.3】 두 개이상의 하위 직무가 반순서 관계에 있는 하나의 상위 직무로 접근권한이 승계되면 공통 상위 접근권한 승계 $((r_{j_1}, r_{j_2}), r_s) \in CS$라 하고, 접근권한은 $P(r_{j_1}) \cup P(r_{j_2}) \subseteq P(r_s)$의 특성을 갖는다.

공통 상위 접근권한 승계는 (그림 3)의 (b)와 같이 두 개이상의 하위 직무 (r_{j_1}, r_{j_2})의 접근권한이 반순서 관계에 있는 상위 직무 (r_s) 로 승계되는 관계로 하위 직무의 모든 접근권한을 상위 직무에서 수행할 수 있다.

【정의 3.4】 하위 직무의 접근권한이 반순서 관계에 있는 두 개이상의 상위 직무로 승계되면 공통 하위 접근권한 승계 $((r_j, (r_{s_1}, r_{s_2})) \in CJ$라 하고, 접근권한은 $P(r_j) \subseteq P(r_{s_1}) \cap P(r_{s_2})$의 특성을 갖는다.

공통 하위 접근권한 승계는 (그림 3)의 (c)와 같이 하위 직무 (r_j) 의 접근권한이 두 개이상의 상위 직무 (r_{s_1}, r_{s_2})로 승계되어 하위 직무의 접근권한을 부분적으로 상위 직무에서 수행할 수 있다. 예를 들어, 병원 업무에서 (그림 4)와 같이 인턴의 환자에 대한 진료기록의 접근권한이 수련의에게 승계되고, 환자의 상태에 따라 접근권한이 여러 전문의에게 다중 승계될 수 있다.



(그림 43) 직무의 승계
(Fig. 4) Role Inheritance

3.3 직무와 접근권한

직무에 접근권한을 부여하는데 있어서 직무의 실제

특성을 완전히 수용하지 못하기 때문에 접근권한의 수행에 어려움이 있고, 어떤 경우에는 직무에 허가된 행동의 집합에 대하여 동시 수행을 제한해야 하기 때문에 실제 직무가 허가된 행동의 집합으로 고려될 수 없다. 이에 따라 직무에 접근권한을 부여하는데 따른 접근권한의 세밀한 분석이 필요하다.

본 논문에서는 접근권한의 분리 및 효과적인 유지와 관리를 위하여 유방향 비사이클 그래프(direct acyclic graph)를 이용하여 접근권한을 표현한다. 접근권한 그래프(PG:Privilege Graph)는 접근권한을 객체에 대한 접근권한을 표현하는 객체 접근권한(Object Privil-ege)과 이를 체계화하여 직무에 부여하는 기본 접근권한(Ordinary Privilege)으로 구성된다. 객체 접근권한을 직무에 부여하는데 있어 고려해야 할 요구사항에 따라 크게 4가지 형태로 구분하고, 이를 그래프를 사용하여 (그림 5)와 같이 기본 접근권한과의 관계로 표현한다. 기본 접근권한을 직무에 배정하면 객체 접근권한을 직접 직무에 배정하는 것보다 RBAC에서 준수해야 하는 보안원칙인 최소권한 원칙과 의무 분리 등의 보안원칙을 준수하기가 용이하고 직무 관리의 유연성을 제공한다. 직무에 의해 수행되어야 하는 객체 접근권한을 접근권한의 특성에 따라 분류하여 직무에 부여되는 기본 접근권한을 사용하여 표현하므로 직무와 접근권한의 관계를 정확히 표현할 수 있다.

기본 접근권한은 객체 접근권한과의 관계에 따라 공통 접근권한(PV_c:Common Privilege), 상호 배타적 접근권한(PV_m:Mutual exclusive Privilege), 합 접근권한(PV_a:And Privilege)과 순서기반 접근권한(PV_o:Ordered Privilege)으로 구분된다.

【정의 3.5】 접근권한 그래프(PG)는 유방향 비사이클 그래프의 특성을 갖는다.

【정의 3.6】 기본 접근권한에 연결된 객체 접근권한 (pv_i, pv_j)을 모두 수행할 수 있는 접근권한을 공통 접근권한 $(pv_i, pv_j) \in PV_c$이라 한다.

공통 접근권한(PV_c)을 갖는 직무(r_i, r_j)는 기본 접근권한에 연결된 영역내에 있는 객체 접근권한(pv_i, pv_j)을 모두 수행할 수 있으며 (그림 5)의 (a)와 같은 그래프로 표현할 수 있다. 예를 들어, 한 부서내의 모든 사원에게 그 부서의 공통 직무를 모두 수행할 수 있도록 공통 접근권한으로 분류하여 접근권한을 허가한다.

【정의 3.7】 기본 접근권한에 연결된 객체 접근권한 (pv_i, pv_j)을 동시에 수행할 수 없는 접근권한을 상호 배타적 접근권한 $(pv_i, pv_j) \in PV_m$이라 한다.

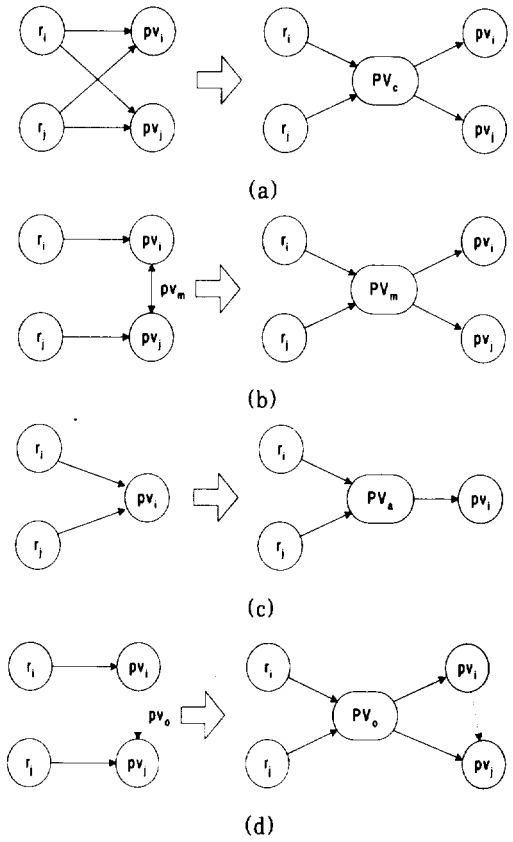
상호 배타적 접근권한(PV_m)을 갖는 직무(r_i, r_j)는 기본 접근권한에 연결된 영역에 있는 객체 접근권한(pv_i, pv_j)을 동시에 수행할 수 없고, 상호 배타적으로 수행하여야 하며 (그림 5)의 (b)와 같은 그래프로 표현할 수 있다. 예를 들어, 어떤 부서에서 상호 배타적 직무인 수입과 지출 업무를 상호 배타적 접근권한으로 분리하여 한번 수행한 업무에 대한 수행을 방지한다.

【정의 3.8】 기본 접근권한에 연결된 객체 접근권한 (pv_i, pv_j)을 모든 권한의 승인이 있어야 수행할 수 있는 접근권한을 합 접근권한 $(pv_i, pv_j) \in PV_a$이라 한다.

합 접근권한(PV_a)을 갖는 직무(r_i, r_j)는 기본 접근권한에 연결된 영역내에 있는 객체 접근권한(pv_i, pv_j)을 모두 수행할 수 있으며 (그림 5)의 (c)와 같은 그래프로 표현할 수 있다. 예를 들어, 어떤 조직에서 예산집행과 같은 직무를 수행할 때, 다른 직무의 승인이 필요한 업무가 있을 수 있다.

【정의 3.9】 기본 접근권한에 연결된 객체 접근권한을 정해진 순서에 따라 수행하여야 하는 접근권한을 순서기반 접근권한 $(pv_i, pv_j) \in PV_o$이라 한다.

순서기반 접근권한을 갖는 직무(r_i, r_j)는 기본 접근권한에 연결된 영역에 있는 객체 접근권한(pv_i, pv_j)을 순서에 따라 수행하여야 하는데 방향성 비사이클 그래프의 특성에 따라 (그림 5)의 (d)와 같이 접근권한을 부여하면 순서를 준수하면서 접근권한을 수행하도록 할 수 있다. (그림 5)의 (d)의 점선은 순서에 따라 접근권한이 수행되어야 함을 의미하고, 순서기반 접근권한은 일반적으로 상호 배타적 특성을 갖는다. 예를 들어, 어떤 조직의 물품 구매 업무에 있어서 구매 의뢰서의 승인, 물품 입고, 지불 등의 업무가 순서에 따라 이루어



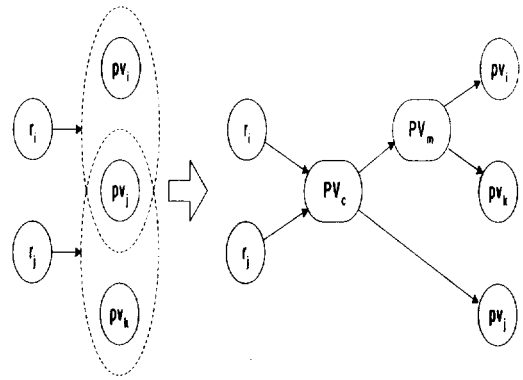
(그림 5) 직무와 접근권한의 관계
(Fig. 5) Relationships of Role and Privilege

져야 한다. 이와 같이 직무의 접근권한이 순서적으로 수행되어야 하는 경우에는 순서기반 접근권한으로 구성하여 직무에 배정하면 순서를 준수하면서 수행하도록 할 수 있다.

직무 (r_i, r_j)가 공통 접근권한($PV_c \rightarrow pv_j$)과 상호 배타적 접근권한($PV_m \rightarrow (pv_i, pv_k)$)을 동시에 갖는 직무는 이를 조합하여 (그림 6)과 같은 접근권한으로 분리하여 표현할 수 있다.

4. 의무 분리

RBAC에서 동일 사용자가 동시에 수행하지 말아야 하는 임의의 직무에 대하여 사용자가 이를 준수하면서 직무의 접근권한을 수행하는 것을 의무 분리라 한다.



(그림 6) 접근권한의 조합
(Fig. 6) Combination of Privilege

의무 분리는 어떤 업무에 부여된 동작을 여러 접근권한으로 나누고, 각 접근권한을 다른 사람에 의해 수행함으로써 확실하게 할 수 있다. 의무분리는 정적(Static) 의무 분리와 동적(Dynamic) 의무 분리가 있는데, 앞에서 표현한 기본 접근권한을 사용하여 직무를 배정하면 의무 분리의 표현 및 관리를 용이하게 할 수 있다.

4.1 상호 배타적 직무

상호 배타적 직무(R_m :Mutual exclusive Role)는 상호 배타적 접근권한 (PV_m)을 갖는 직무에 배정된 접근권한을 사용자가 동시에 수행하는 것을 방지해야 하는 직무로써, 상호 배타적 직무는 하나의 직무에 두 개이상의 상호 배타적 접근권한이 주어지는 경우와 두 개이상의 직무에 상호 배타적 접근권한이 주어져서 수행되어야 하는 경우가 있다. 예를 들어, 어떤 조직에 구매부서와 경리부서가 있을 때, 구매부서의 거래 명세서 발급 업무와 경리부서의 비용 지불 업무를 상호 배타적 직무라 한다. 이 직무는 분리되어 수행되어야 하므로, 각 사원이 양쪽의 권한을 동시에 수행할 수 없도록 직무를 분리하여 배정하여야 한다. 그렇지 않으면, 두 권한을 남용하여 실제 구매는 이루어지지 않고 비용만 지불될 수 있다.

【정의 4.1】 상호 배타적 접근권한 (PV_m)을 갖는 직무 (r_i, r_j)를 상호 배타적 직무 $(r_i, r_j) \in R_m$라 하고, 임의의 접근권한 (pv_k)에 대하여 $pv_k \in P(r_i)$일 때 $pv_k \notin P(r_j)$인 특성을 갖는다.

【정리 4.1】 공통 상위 접근권한 승계 $((r_i, r_j), r_s) \in CS$ 관계인 상호 배타적 직무 $(r_i, r_j) \in R_m$의 접근권한은 승계될 수 없다.

【증명】 상호 배타적 직무 (r_i, r_j)의 접근권한이 r_s에 승계될 수 있다고 가정하자. 반순서 관계에 있는 직무가 승계 $(r_i \leq r_s)$되면 접근권한은 $P(r_i) \subseteq P(r_s)$ 이므로 $pv_m \in P(r_i)$인 상호 배타적 접근권한 pv_m 이 있으면 $pv_m \in P(r_s)$이고, 마찬가지로 직무가 승계 $(r_j \leq r_s)$되면 접근권한은 $P(r_j) \subseteq P(r_s)$ 이므로 $pv_n \in P(r_j)$인 상호 배타적 접근권한 pv_n이 있으면 $pv_n \in P(r_s)$이다. 그러므로 $(pv_m, pv_n) \in (r_s)$ 이다.

그러나, 상호 배타적 직무의 [정의 4.1]에서 상호 배타적 직무의 접근권한은 $pv_m \in P(r_s)$이면 $pv_n \notin P(r_s)$이어야 하므로 가정은 모순이어서 CS 관계인 상호 배타적 직무의 접근권한은 승계될 수 없다. □

상호 배타적 직무의 접근권한은 일반적으로 승계될 수 없고, 각 직무에 배정된 고유 접근권한의 형태로 표현된다.

4.2 정적 의무 분리

직무의 접근권한이 분리되어 있는 상호 배타적 직무에 대하여 사용자를 직무에 접근권한에 분리 배정하여 정적 의무 분리를 이룰 수 있다. 예를 들어, 회사 업무에서 사원을 상호 배타적 직무에 구매 업무와 경리 업무에 분리 배정하면 정적 의무 분리를 준수할 수 있다.

【정의 4.2】 상호 배타적 직무 집합 $(r_i, r_j) \in R_m$에서 임의의 사용자 (id_k)에 대하여 $id_k \in U(r_i)$일때 $id_k \notin U(r_j)$ 이면 정적 의무 분리이다.

【정리 4.2】 단일 접근권한 (pv_k) 을 갖는 상호 배타적 접근권한 (PV_m)에 단일 직무가 연결되면 정적 의무 분리를 준수한다.

【증명】 상호 배타적 접근권한(PV_m)에 두 개이상의 상호 배타적 객체 접근권한 (pv_x, pv_y)이 배정되었다고 가정하자. PV_m에 대하여 두개이상의 접근권한 (pv_x, pv_y)이 배정되면, PV_m에 연결된 임의의 직무 (r_i) 는 $pv_x \vee pv_y \in P(r_i)$의 접근권한을 갖는다. 이는 상호 배타적 직무의 [정의 4.1]에서 $pv_x \in P(r_i)$일때 $pv_y \notin P(r_i)$에 모순이 된다.

또한, PV_m에 두 개이상의 직무 (r_i, r_j)가 배정되었다고 가정하자. 상호 배타적 접근권한 (PV_m)에 대하여 두개이상의 직무 (r_i, r_j)가 배정되면 임의의 상호 배타적 접근권한 (pv_k)에 대하여 $pv_k \in P(r_i)$일때 $pv_k \in P(r_j)$이 된다. 이는 상호 배타적 직무의 [정의 4.1]에서 $pv_k \in P(r_i)$일때 $pv_k \notin P(r_j)$에 모순이 되므로 정적 의무 분리를 위하여 단일 접근권한을 갖는 PV_m에 단일 직무가 배정되어야 한다. □

4.3 동적 의무 분리

사용자가 상호 배타적 직무에 부여된 접근권한을 수행할 때 상호 배타적 직무의 접근권한을 동시에 수행하지 못하도록 하는 것을 동적 의무 분리라 하는데, 두 개이상의 직무가 상호 배타적 접근권한 (PV_m)에 배정될 때 동적 의무 분리를 준수할 수 있도록 하여야 한다. 동적 의무 분리를 만족하기 위하여 사용자의 직무에 배정된 상호 배타적 접근권한의 수행여부를 감사(audit trail)하여 상호 배타적 직무를 동시에 수행하지 못하도록 하여야 한다.

동적 의무 분리는 동일 사용자가 동시에 상호 배타적 직무를 수행할 수 없도록 하는 단순 동적 의무 분리, 두 사용자가 동일 직무를 갖지만 한 사용자가 앞서 수행한 객체에 대한 접근권한을 주지 않는 객체 기반 의무 분리와 상호 배타적 접근권한을 순서에 따라 수행하도록 해야 하는 순서기반 의무 분리 등으로 구분할 수 있다.

【정의 4.3】 상호 배타적 직무 집합 $(r_i, r_j) \in R_m$에서 $id_k \in U(r_i)$이고 $id_k \in U(r_j)$인 임의의 사용자 (id_k)가 활성화한 세션 (s_i)이 $r_i \in R(s_i)$일때 $r_j \notin R(s_i)$이면 단순 동적 의무 분리이다.

【정의 4.4】 상호 배타적 직무 집합 $(r_i, r_j) \in R_m$에서 임의의 사용자 (id_k)가 활성화한 세션 (s_i) 이 상호

배타적 접근권한(pv_k)에 대하여 $r_i \in R(s_i)$이고 $pv_k \in P(r_i)$일 때, $r_j \in R(s_i)$에 대하여 $pv_k \notin P(r_j)$이면 객체 기반 의무 분리이다.

【정의 4.5】 순서기반 접근권한 $(pv_x, pv_y) \in PV_o$을 갖는 상호 배타적 직무 $(r_i, r_j) \in R_m$에서 임의의 사용자(id_k)가 활성화한 세션(s_i)이 상호 배타적 접근권한 (pv_x, pv_y)에 대하여 $r_i \in R(s_i)$이고 $pv_x \in P(r_i)$일 때, $r_j \in R(s_i)$에 대하여 $pv_x \notin P(r_j)$이고 $pv_y \in P(r_j)$이면 순서기반 의무 분리이다.

의무 분리 규칙의 목적은 공모나 사기를 방지하기 위하여 두 사람 이상에 의하여 수행하여 할 업무의 모든 부분을 한 사람이 수행하지 못하도록 하는데 있다. 예를 들어, 조직에서 비용의 지불 및 승인 업무는 두 사람 이상에 의하여 수행될 것을 요구한다. 만약 그러한 작업에 단지 두 접근권한 만이 있으면, 각 접근권한은 직무에 분리하여 배정하여야 하고, 직무는 상호 배타적이어야 한다.

의무 분리를 준수하기 위하여 보장해야 하는 업무의 안정성 조건은 다음과 같이 표현할 수 있다.

【정의 4.6】 업무의 안정성 조건 $C(t)$ 은 다음과 같은 특성을 갖는다.

- 직무의 안정성 함수 $C(t): T \rightarrow 2^{pv}$
- 접근권한 $P[t] \subseteq \bigcup_{r_i \in R \mid id_k \in U(r_i)} P(r_i)$

한 사람이 업무를 모두 수행할 수 없도록 하기 위하여 사용자는 C(t)에 있는 모든 접근권한을 갖지 않아야 한다. RBAC 시스템에서 상호 배타적 직무에 대하여 의무 분리를 위하여 다음과 같은 안정성 특성을 갖는다.

【정리 4.3】 상호 배타적 직무 집합 $(r_i, r_j) \in R_m$에서 정적 의무 분리가 준수되면 RBAC 시스템은 안정하다.

【증명】 정적 의무 분리가 준수되어도 시스템이 안정하지 않다고 가정하자.

임의의 업무 (t) 의 모든 접근권한 (pv) 에 승인된 사용자 (id_k) 가 있다 하고, $P[t]$ 가 작업을 처리하는데 필요한 pv 의 집합을 나타내면 업무의 안정성 조건은 $P[t] \subseteq \bigcup_{id_k \in U(r)} P(r)$이고, 정적 의무 분리를 위하여 $P[t]$ 는 적어도 둘 이상의 상호 배타적 직무 (r_i, r_j)로 나누어져야 하므로 $P[t] = P(r_i) \cup P(r_j)$이다. $R(id_k)$ 가 사용자 (id_k) 에 승인된 모든 직무의 집합을 나타낸다고 하면 $P(r_i) \cup P(r_j) \subseteq \bigcup_{r \in R(id_k)} P(r)$이고, r_i와 r_j에 있는 모든 상호 배타적 직무의 pv 는 사용자 (id_k) 의 모든 pv 의 집합인 $\bigcup_{r \in R(id_k)} P(r)$내에 있어야 한다.

상호 배타적 직무로 지정된 어떤 직무에 있는 pv 는 단지 하나의 직무에 배정될 것을 보장하므로 pv 는 $P(r_i)$나 $P(r_j)$중에 있어야 하고, $P(r_i)$와 $P(r_j)$의 pv 를 사용자가 수행할 수 있도록 하기 위해서 직무 r_i 와 r_j 는 사용자의 승인된 직무의 집합에 있어야 하는데, 정적 의무 분리의 [정의 4.2]에서 상호 배타적 직무 $(r_i, r_j) \in R_m$에 대하여 사용자 (id_k)가 $id_k \in U(r_i)$이면 $id_k \notin U(r_j)$에 모순이 된다. 그러므로, 정적 의무 분리가 준수되면 RBAC 시스템은 안정하다. □

4.4 의무 분리 알고리즘

접근권한 그래프로 표현된 상호 배타적 접근권한을 갖는 직무에 배정된 사용자에 대하여 정적·동적 의무 분리를 준수하는 직무 배정 및 직무 수행 알고리즘을 제안한다.

직무의 구성에 대하여 직무 영역에 주어진 접근권한 그래프에 따른 객체 접근권한(pv)과 기본 접근권한(PV)의 관계를 표현한 접근권한 표가 〈표 1〉과 같이 구성되어 있을 때, 직무(Role) 사용자(id), 접근권한(Privilege)의 관계를 나타내는 직무 접근 제어 표(R_{ACL}:Role Access Control List)는 〈표 2〉와 같이 구성될 수 있다.

공통 접근권한 PV_c를 갖는 직무는 PV_c에 주어진 모든 접근권한 (pv_7, pv_8)을 수행할 수 있다. 상호 배타적 접근권한 PV_m을 갖는 직무는 정적 의무 분리나 동

〈표 1〉 접근권한 표
〈Table 1〉 Privilege table

PV	pv
PV_{m1}	pv_1
PV_{m2}	pv_2
PV_{m3}	pv_3, pv_4
PV_{o1}	pv_5, pv_6
PV_{c1}	pv_7, pv_8
PV_{c2}	pv_9
...	...

〈표 34〉 직무 접근 제어 표
〈Table 2〉 Role Access Control List

Role	id	Privilege
r_1	id_1	PV_{m1} , PV_{c1}
r_2	id_2	PV_{m2} , PV_{c1}
r_3	id_3	PV_{m3} , PV_{c1}
r_4	id_4	PV_{m3} , PV_{c1}
r_5	id_5	PV_{o1} , PV_{c2}
r_6	id_6	PV_{o1} , PV_{c2}
...	...	...

적 의무 분리를 준수하도록 사용자를 배정하거나 수행을 허가하여야 하는데 직무 배정 및 수행 알고리즘은 다음과 같이 동작한다.

PV_{m1}과 PV_{m2}을 갖는 직무인 r_1과 r_2는 (그림 7)의 직무 배정 알고리즘과 같이 PV_m을 갖는 직무를 검사하여 이미 사용자가 배정되어 있으면 정적으로 표시(s_flag)하고, 그렇지 않으면 동적으로 표시(d_flag)하여 사용자 id_1과 id_2를 분리 배정하면 정적 의무 분리를 준수할 수 있다.

PV_{m3}을 갖는 직무인 (r_3, r_4)에 사용자 (id_3, id_4)가 배정되어 있을 때, PV_{m3}이 두개의 접근권한을 갖으므로 (그림 8)의 직무 수행 알고리즘과 같이 동적 의무 분리를 준수하면서 수행하도록 허가하여야 한다. r_3에 배정된 사용자 id_3가 pv_3를 수행하면 로그(log)에 표시(e_flag)하여, id_3는 pv_4를 수행하지 못하도록 하고, r_4에 배정된 사용자 id_4만이 pv_4를 수행하도록 허가하여야 한다. PV_{o1}을 갖는 직무 (r_5, r_6)에 사용자 (id_5, id_6)가 배정되어 있을 때, r_5에 배정된 사용자 id_5가 pv_5의 수행하면 이를 로그하고 미리 pv_5가 수행되었음을 확인하여 r_6에 배정된 사용자 id_6 만이 pv_6를 수행하도록 허가하여야 한다.

Algorithm Assign_User_to_Role(id, r)
Input : user id(id) and role(r) to be assigned.
Output : check mutual exclusive privilege(PV_m) for role(r), and assign id to role ACL.{R_{ACL}} with s_flag(static) and d_flag(dynamic).
Procedure :
begin
 for all {R_{ACL}} do
  if($PV_m \in P(r)$) then
  /* Mutual exclusive role */
   for all {R_{ACL}} do
    if($id \in \{U(r)\}$) then
    /* Dynamic Separation of Duty */
     Assign (r, id) to {R_{ACL}} with d_flag;
    else
     Assign (r, id) to {R_{ACL}} with s_flag;
  else
   Assign (r, id) to {R_{ACL}};
end

(그림 7) 직무 배정 알고리즘
(Fig. 7) Role Assignment Algorithm

Algorithm Perm_Role_for_User(id, pv)
Input : user id(id) and privilege(pv) for current session to be executed.
Output : check privilege in role ACL.{R_{ACL}} and permit pv for id.
Procedure :
begin
 for all {R_{ACL}} do
  if($pv \in (PV_m \vee PV_o)$) then
   /* Mutual exclusive role */
    if(s_flag) then
    /* Static role */
    Permit pv for id;
   else if(e_flag) then

```
            Log(id, pv);
            Permit pv for id;
        else
            Alarm violation;
    else
        Permit pv for id;
end

Procedure Log(id, pv)
/* Check pv for id, clear or set e_flag(executed) */
begin
    if(e_flag) then
        Clear e_flag for (id, pv);
    else
        Set e_flag for (id, pv);
end
```

(그림 8) 직무 수행 알고리즘
(Fig. 8) Role Execution Algorithm

5. 결 론

기존의 접근 제어 모델인 MAC이나 DAC이 기밀성 제어를 위주로 하는 접근 제어 모델인데 비해 RBAC은 상용 환경의 응용에서 데이터 무결성 제어에 사용하기가 유리한 접근 제어 모델로써 접근권한을 직무에 부여하고 사용자를 직무에 배정하므로 접근 제어의 관리를 용이하게 할 수 있는 잇점을 가지고 있다.

본 연구에서는 직무에 접근권한을 부여하고 사용자를 직무에 배정하는데 따른 안전한 접근 제어를 위하여 다음과 같은 연구를 수행하였다.

첫째, RBAC의 기본 특성을 분석하여 반순서 관계를 갖는 직무의 승계 속성에 따라 기본적인 직무의 계층 형태를 분류하고 둘째, 방향성 비사이클 그래프를 이용하여 원시 접근권한인 객체 접근권한을 접근권한의 특성에 따라 네가지 형태의 기본 접근권한으로 모델링하고, 기본 접근권한을 조합함에 따라 접근권한의 체계화가 가능하게 하였다. 특히 상호 배타적 특성을 갖는 직무를 방향성 그래프를 이용하여 표현함으로써 의무 분리에 어려움이 있는 직무의 접근권한 부여를 유연하게 할 수 있고, 사용자가 직무를 수행할 때 의무 분리의 준수를 용이하게 한다. 셋째, 정적·동적 의무 분리의 정의에 따라 RBAC의 안정성을 위한 특성을 제안하고, 직무의 기본 승계 속성과 접근권한 그래프를 근거로 의무 분리를 준수하는 직무 수행 알고리즘을 제시하였다.

향후에는 동적 의무 분리의 준수를 위한 세밀한 보안 특성의 연구가 이루어져야 하고, 직무 접근권한의 위임에 관한 연구가 필요하며, RBAC의 안전한 관리를 위한 직무 관리 프레임워크을 제시하여 이를 기반으로 직무 기반 접근 제어 시스템을 설계할 예정이다. RBAC은 데이터 무결성을 목적으로 하는 기업의 상업적 응용에 적합한 접근 제어 모델로써, 전자 상거래 등의 접근 제어에 사용될 수 있을 것으로 생각된다.

참 고 문 헌

[1] R. W. Baldwin, "Naming and grouping privileges to simplify security management in large database," Proc. of IEEE Computer Society Symposium on Security and Privacy, pp.61-70, Apr. 1990.

[2] D. E. Bell, L. J. Lapadula, Secure Computer Systems: Unified Exposition & Multics Interpretation. Technical Report MTR-2997, MITRE Co. Bedford, MA, 1976.

[3] D. D. Clark, D. R. Wilson, "A comparison of commercial and military computer security policies," Proc. of IEEE Computer Society Symposium on Security and Privacy, pp.184-194, May 1987.

[4] Department of Defence, Department of Defence Trusted Computer System Evaluation Criteria, DoD 5200-28-STD, Department of Defence, Dec. 1985.

[5] D. F. Ferraiolo, J. A. Cugini, D. R. Kuhn, "Role-Based Access Control (RBAC) : Feat-ures and Motivations," Proc. of 11th Annual Computer Security Application Conference, pp.241-248, Dec. 1995.

[6] D. F. Ferraiolo, D. R. Kuhn, "Role-based access controls," Proc. of 15th National Computer Security Conference, pp.554-563, Oct. 1992.

[7] ISO/IEC 7498-2 Information Processing Sys-tems-Open Systems Interconnection-Basic Reference Model-Part 2 : Security Architec-ture, 1991.

[8] P. A. Karger, "Implementing Commercial Data Integrity with Secure Capabilities," Proc. of IEEE Computer Society Symposium on Security and Privacy, pp.130-139, May. 1988.

[9] T. M. P. Lee, "Using mandatory integrity to enforce commercial security," Proc. of IEEE Computer Society Symposium on Security and Privacy, pp.140-146, May. 1988.

[10] M. J. Nash, K. R. Poland, "Some Conundrums Concerning Separation of Duty," Proc. of IEEE Computer Society Symposium on Security and Privacy, pp.201-207, Apr. 1990.

[11] M. Nyanchama and S. Osborn, "Role-based security, Object-oriented Databases and Separation of Duty," *SIGMOD Record*, Vol. 22, No. 4, pp.45-51, Dec. 1993.

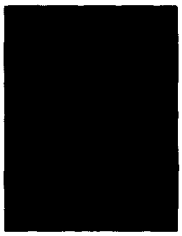
[12] R. S. Sandhu, "Separation of duties in computerized information systems," Proc. of Database Security, IV Status and Prospects, pp.179-189, 1991.

[13] R. S. Sandhu, "Lattice-based access control models," IEEE Computer, Vol.26, No.11, pp.9-19, Nov. 1993.

[14] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based Access Control : A Multi-Dimensional View," Proc. of 10th Annual Computer Security Applicat-ion Conference, pp.54-62, Dec. 1994.

[15] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," IEEE Computer, Vol.29, No.2, pp.38-47, Feb. 1996.

[16] R. T. Simon, M. E. Zurko, "Separation of Duty in Role-Based Environments," Proc. of 10th IEEE Computer Security Foundations Workshop, pp.183-194, Jun. 1997.



천 은 홍

1981년 광운대학교 응용전자공학과 졸업(공학사)

1985년 아주대학교 대학원 전자공학과 졸업(공학석사)

1998년 8월 아주대학교 대학원 컴퓨터공학과 박사 졸업 예정

1985년~87년 삼성전관 컴퓨터사업부 개발과 사원

1987년~88년 삼성종합기술원 정보시스템연구소 주임연구원

1988년 9월~현재 우석대학교 정보통신 및 컴퓨터공학부 부교수

관심분야 : 컴퓨터 네트워크, 정보보호, 정보통신 security 등

김 동 규

1973년 서울대학교 공과대학 졸업(학사)

1979년 서울대학교 자연과학대학원 졸업(석사)

1984년 미국 Kansas 주립대 대학원 졸업(전산학 박사)

1981년~1982년 미국 Kansas 주립대 전산학과 교수

한국통신정보보호학회 부회장 역임

1979년~현재 아주대학교 정보 및 컴퓨터공학부 교수

관심분야 : 컴퓨터 네트워크, 정보통신 프로토콜 엔지니어링, 정보통신 security, 분산처리 시스템 등