通信情報保護學會誌
第 10 券 第 2 號, 2000. 6

RBAC 표준 참조 모델 연구동향

김 학 범*, 김 동 규**

요 약

역할기반 접근통제(RBAC)는 사용자의 역할에 기반을 둔 접근통제 방법으로 Ravi S. Sandhu가 제안한 기본 모델 이후로 다양한 모델들이 제안되어졌다. 그러나 이러한 모델들은 RBAC을 구성하는 특성들에 대한 일반적인 합의 없이 이루어지고 있으며 표준 참조 모델의 부재는 RBAC의 사용과 의미에 대해 혼란을 가져오고 있다. NIST(National Institute of Standards and Technology)에서는 이러한 문제점을 해결하기 위하여 현재까지 제안된 RBAC 모델과 상용 제품 등을 통합하여 단일화된 RBAC 모델을 제안하였고 앞으로 표준 제정을 위한 기초로서 활용할 예정이다. 본 논문에서는 NIST가 제안한 RBAC 표준 참조 모델을 소개한다.

Ⅰ. 서 론

전통적인 접근통제 방법은 객체에 접근을 하고자 하는 주체의 접근 권한에 따라 접근을 통제하는 임의적 접근통제 방법과 주체의 레이블과 주체가 접근하고자 하는 객체의 보안레이블을 비교하여 보안정책에 합당한 접근통제 규칙에 의하여 접근을 통제하는 강제적 접근통제 방법이다.

역할기반 접근통제(RBAC:Role Based Access Control)는 사용자의 역할에 기반한 접근통제 방식으로 임의적 접근통제와 강제적 접근통제에 비하여 정교함과 유연성을 제공한다[1]. RBAC은 수행이 어려운 보안관리 과정을 관리자가 효과적으로 처리할 수 있도록 해주며 조직에 적합한 보안정책을 정확히 표현하고 적용할 수 있도록 한다[2][3].

RBAC은 조직 수준에서 보안 관리를 증진시키기 위해서 사용자 식별자 수준(user identity level)이 아닌 추상화 수준(abstraction level)을 제공하므로, 업무를 수행하는 실제 환경에 자연스럽게 접목될 수 있다. 조직 내에서의 기능 역할에 기반한 허가(permission)를 확립하고 사용자들은 역할 또는 역할의 집합에 적절히 할당한다. RBAC에서 접근결정(access decision)은 조직내에서 사용자가 가지는 역할에 기반하여 이루어진다. 역할은 조직과 관련된 직무, 책임, 자격 등을 나타낸다. 조직내에서의 역할은 사용자 교체, 업무(task)의 재할당에 비해 상대적으로 변화가 적기 때문에, RBAC은 조직내의 사용자 허가 할당에 있어서 복잡성과 비용, 잠재적인 실수를 줄이기 위한 강력한 메커니즘을 제공한다.

RBAC의 이러한 장점 때문에 RBAC 제품에 대해 커다란 수요가 발생하였고, 벤더들은 데이터베이스, 시스템 관리, 운영체제 제품에 RBAC 특성들을 통합시켜왔으며 다양한 RBAC 모델들이 제안되고 구현되고 있다[4-8].

1993년 NIST는 정부와 산업체의 협동작업으로 상용, 정부 및 국방 분야의 정보보호의 필요성에 대한 연구를 진행하여 다양한 응용 환경에 적용할 수 있는 새로운 접근통제 정책의 필요성을 인식하였다. 이러한 연구를 기반으로 현재까지 NIST를 중심으로 역할기반 접근통제 분야에 있어 독립적으로 3가지가 개발되어 진행중이다. 그 첫째가 조지메이슨 대학 및 Seta Corporation의 Ravi S. Sandhu 박사가 주축이 되어 진행되고 있는 역할기반 접근통제 정의 및 실현가능성에 대한 연구이다. 두 번째가 NIST의 John Barkley를 중심으로 의료(health care) 시스템에 역할기반 접근통제를 적용하는 시도이며, 세번째가 메릴랜드 대학의 Virgil Gligor

* 한국정보보호센터(hbkim@kisa.or.kr)
** 아주대학교 컴퓨터공학과(dkkim@madang.ajou.ac.kr)

박사를 중심으로 접근통제에 안전하고, 효과적이며 일관적인 메커니즘을 적용하기 위한 역할기반 접근통제에 대한 정형적 참조모델(Formal Reference Model) 개발이다. 이를 위하여 NSA(National Security Agency)와 공동 연구개발을 통하여 개발된 역할기반 접근통제에 대한 정형적 참조 모델을 Mach 운영체제에 기반한 NSA의 Synergy 플랫폼 상에 구현 중에 있다[9]. 이러한 노력의 결실로 역할기반 접근통제는 SESAME(Secure European System for Applications in a Multi-vendor Environment) 분산 시스템과 OMG(Object Management Group)의 CORBA(Common Object Request Broker Architecture) 보안명세서[10]에서도 분산 객체 기술로 사용할 수 있는 접근통제 메커니즘의 하나로서 역할기반 접근통제를 사용토록 하고 있다. 역할기반 접근통제 관련 기술을 구현하고 있는 제품도 Oracle, Sybase, Lotus Notes, Microsoft Transaction Server 등 점차적으로 증가하고 있는 추세에 있다[11]. 이와 함께 '98년 5월 버전 2.0이 발표되어, '99년 6월 ISO/IEC 15408 국제표준으로 제정된 국제공통평가기준(CC : Common Criteria)[12]에 역할기반 접근통제 내용이 포함되었으며, 이를 기반으로 접근통제 기능을 평가하기 위한 역할기반 접근통제 보호프로파일(PP : Protection Profile)[13]이 발표되었다. 또한 ISO/IEC 9075인 SQL 표준에도 RBAC이 포함되어 있다[14].

그러나 이러한 노력들은 역할기반 접근통제를 구성하는 특성들에 대한 일반적인 합의 없이 계속되었다. RBAC 기술에 대한 표준 참조 모델의 부재로 인해 RBAC 용어 자체도 일반적으로 받아들여지는 의미를 갖지 않으며, 사용자들과 개발자들 사이에서 다양한 방식으로 사용되어지고 있으며 RBAC의 가장 중요한 특성인 역할에 대해서도 제품별로 다양한 방식의 구현이 이루어지고 있다.

이러한 모든 점들이 RBAC 기술의 발전을 느리게 하고 있다. 따라서 RBAC을 구현하고 제품을 선택하는 기준이 될 수 있는 RBAC의 표준 제정이 시급한 실정이다.

이러한 문제점을 해결하고 역할기반 접근통제 기술의 발전과 효율적인 사용을 위해 NIST는 역할기반 접근통제에 대한 표준 참조 모델을 제안하였다[15].

본 논문에서는 NIST의 역할기반 접근통제 표준 참조 모델을 소개한다.

II. 기존의 RBAC 모델

RBAC 모델에 관한 연구는 다양하게 진행되어 왔으나 가장 대표적인 연구로써 Ravi S. Sandhu의 RBAC에 관한 연구와 NIST의 연구를 들 수 있다.

1. Ravi S. Sandhu의 RBAC 모델

Ravi S. Sandhu는 4가지 형태의 개념적인 RBAC 모델로서 $RBAC_0$, $RBAC_1$, $RBAC_2$, $RBAC_3$을 제안하였다[4]. $RBAC_0$ 모델은 RBAC을 다양한 시스템에 적용할 수 있도록 개발된 기본 모델이다. $RBAC_1$과 $RBAC_2$는 $RBAC_0$을 포함하지만 각각 고유한 특성을 가지고 있다. $RBAC_1$은 다른 역할로부터 허가를 상속받을 수 있다는 역할 계층의 특성을 추가하였으며, $RBAC_2$는 RBAC의 설정에 제한조건을 설정할 수 있는 제약을 가하는 특성을 부가하였다. $RBAC_1$과 $RBAC_2$는 서로가 비교할 수 없는 모델이다. $RBAC_3$은 $RBAC_1$과 $RBAC_2$를 통합한 모델이다. Ravi S. Sandhu가 제안한 RBAC 모델은 그림 1과 같다.

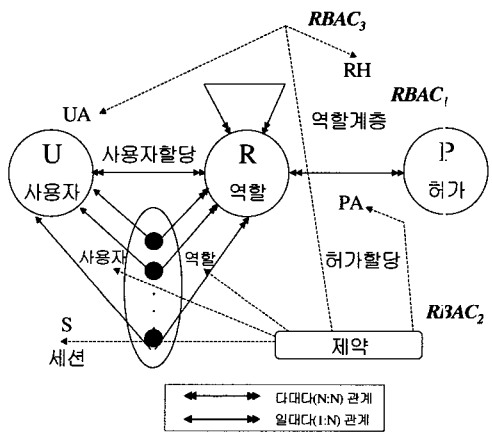

그림 1. Ravi S. Sandhu의 RBAC 모델

2. NIST의 강화된 RBAC 모델

NIST에서도 RBAC 모델에 대한 계속적인 연구를 수행하였고 health care 시스템에 RBAC을 적용하려는 노력이 있었다. 1999년 NIST에서는 그동안의 연구결과를 종합한 강화된 RBAC 모델을

정형적으로 제시하였다[6].

RBAC의 강화된 모델은 RBAC 권한 데이터베이스 모델인 MC_0과 RBAC 활성화 모델인 MC_1의 두 개의 구성요소를 가진다. MC_0은 역할, 허가, 사용자에 대한 사상(mapping)을 정형화하고 RBAC의 정적 특성을 정의한다. 역할 계층, 상속, cardinality, 정적의무분리 등이 포함된다. 반면에 MC_1은 정적 특성을 보완하는 동적 특성을 정의하고 있다. 주체 또는 주체로부터 다른 기본 요소들로의 사상을 포함하며 역할 활성화, 동적 의무분리, 오퍼레이션 권한, 객체 접근 권한 등이 포함된다.

Ⅲ. NIST의 표준 참조 모델

1. 개 요

Ravi S. Sandhu와 NIST가 제안한 RBAC 표준 참조 모델은 다음의 4단계의 순서로 구성된다.

- Flat RBAC
- Hierarchical RBAC
- Constrained RBAC
- Symmetric RBAC

가장 아래 단계의 모델은 Flat RBAC이며 각 단계마다 한가지의 특성이 증가된다. 또한 각 단계는 아래 단계의 요구사항을 누적하여 포함한다.

● Flat RBAC

Flat RBAC은 RBAC의 가장 본질적인 측면을 나타내고 있다. RBAC의 가장 기본적인 개념은 사용자들이 역할에 할당되고, 역할에 허가가 할당되며 사용자들은 역할의 멤버가 됨으로써 허가를 얻는 것이다. NIST의 RBAC 모델은 사용자-역할, 허가-역할 할당이 다대다 관계를 가질 것을 요구한다. 따라서 한 사용자가 여러 개의 역할에 할당되고, 하나의 역할은 복수의 사용자를 가질 수 있다. 허가에 관해서도 마찬가지이다. 또한 Flat RBAC은 특정 역할에 할당되는 사용자 뿐 아니라 특정 사용자에게 할당되는 역할들이 결정될 수 있는 사용자-역할 리뷰(user-role review) 요구사항을 가진다. 마지막으로 Flat RBAC은 사용자들이 동시에 다양한 역할의 허가들을 수행할 수 있도록 요구한다.

● Hierarchial RBAC

Hierarchical RBAC은 Flat RBAC에 역할 계층의 요구사항을 추가한 것이다. NIST의 RBAC 모델은 Hierarchical RBAC에서 다음의 두 가지 서브레벨을 인정한다.

- 일반 계층 RBAC
  (General Hierarchical RBAC)
- 제한 계층 RBAC
  (Limited Hierarchical RBAC)

일반 계층 RBAC은 임의의 계층에 대한 지원을 요구하고, 제한 계층 RBAC은 역할 계층에 제한(restriction)을 가한다.

역할 계층은 상속 계층(inheritance hierarchy), 활성화 계층(activation hierarchy) 또는 양 쪽 모두가 될 수 있다. 상속 계층에서는 하나의 역할이 활성화되면 모든 하위 역할들(junior role)이 활성화되며, 활성화 계층에서는 하나의 역할이 활성화되는 경우에 이 역할의 하위 역할들이 활성화되지는 않는다.

● Constrained RBAC

Constrained RBAC은 Hierarchical RBAC에 의무분리(SOD : Separation of Duties) 요구사항을 추가한 것이다. 의무분리는 조직내의 작업이나 행동에 대한 권한과 책임을 다양한 사용자에게 분산시킴으로써 사용자들이 공모하여 부정한 행위를 할 수 있는 위험을 감소시키는 방법으로 정적의무분리와 동적의무분리로 나뉘어진다.

● Symmetric RBAC

Symmetric RBAC은 Constrained RBAC에 Flat RBAC에서의 사용자-역할 리뷰와 비슷한 허가-역할 리뷰에 대한 요구사항을 추가한 것이다. 따라서 특정한 역할에 할당되어지는 허가들 뿐 아니라 특정한 허가에 할당되어지는 역할들도 결정되어질 수 있다.

Ravi S. Sandhu와 NIST의 강화 모델, NIST의 표준 참조 모델을 비교하면 표 1과 같다.

표 2. RBAC 모델 비교

모델	계층	특성
Ravi S. Sandhu 모델	$RBAC_0$	· 기본모델
	$RBAC_1$ $RBAC_2$	· $RBAC_0$+역할계층 · $RBAC_0$+제약 · $RBAC_1$과 $RBAC_2$는 대등관계
	$RBAC_3$	· $RBAC_1$+ $RBAC_2$
NIST의 강화 모델	MC_0	· 정적 특성
	MC_1	· MC_0 + 동적 특성
NIST의 표준참조 모델	Flat RBAC	· 기본 모델
	Hierarchical RBAC	· Flat RBAC + 역할 계층
	Constrained RBAC	· Hierarchical RBAC + 제약(의무분리)
	Symmetric RBAC	· Constrained RBAC + 허가-역할 리뷰

2. FLAT RBAC

Flat RBAC에서 요구되는 특성들은 모든 형태의 RBAC에서 필수적인 것으로서 다대다 사용자 할당 관계와 사용자가 역할을 통해 허가를 얻는다는 점이다.

그림 2. Flat RBAC

그림 2는 Flat RBAC을 나타낸다. RBAC에는 사용자(U)와 역할(R), 허가(P)라는 세가지 실체가 있다. 사용자는 사람 또는 프로세스, 컴퓨터와 같은 에이전트이다. 역할은 역할의 멤버에게 수여된 조직 책임과 권한에 관련된 의미를 가진 조직내의 직무 기능이나 직무 이름이다. 허가는 시스템의 객체에 대해 특정한 접근 모드로의 승인이다. 허가는 허가의 소유자에게 시스템에서 특정한 행동을 수행할 수 있는 능력을 부여한다. 이러한 허가는 시스템의 구현방식에 크게 의존하므로 접근통제의 일반 모델은 허가를 어느 정도까지는 해석되지 않은 심볼로 다룬다.

Flat RBAC은 사용자-역할 할당(UA)과 허가-역할 할당(PA)이 다대다 관계일 것을 요구한다. 즉 사용자는 여러 역할에 할당될 수 있고 역할은 여러 사용자들을 가질 수 있다. 또한 역할은 많은 허가를 가질 수 있고 허가도 여러 역할에 할당되어질 수 있다.

또한 Flat RBAC은 특정한 사용자가 어떠한 역할들에 속하게 되고 특정 역할이 어떠한 사용자들에게 할당되어지는 가를 효율적으로 결정될 수 있도록 하는 사용자-역할 리뷰 요구사항을 가진다.

3. Hierarchical RBAC

그림 3은 Hierarchical RBAC을 나타낸다. Flat RBAC 모델에 역할 계층 관계(RH)가 추가되어졌다.

역할 계층은 조직내에서 권한과 책임의 순서를 반영하기 위해 역할을 구조화하는 방법이다. 역할 계층의 예는 그림 4에 나와 있다. 일반적으로 상위의 역할이 역할 계층 다이어그램의 위 부분에 위치하고 하위의 역할들이 아래 부분에 위치한다. NIST의 RBAC 모델은 Hierarchical RBAC에서 일반 계층 RBAC과 제한 계층 RBAC이라는 두 가지 서브레벨을 인정한다. 일반 계층 RBAC은 임의의 계층을 지원하고 제한 계층 RBAC은 트리나 역트리 같은 구조로 제한된다.

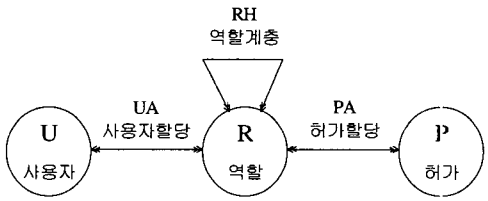

그림 3. Hierarchical RBAC

3.1 제한 계층과 일반 계층

그림 4.a는 기술부(Engineering Department)에 존재할 수 있는 역트리 구조를 나타낸다. 이 다이어그램에는 부서의 모든 고용인들이 속하는 최하위의 역할인 ED가 존재한다. ED의 상위에 프로젝트별로 E 역할이 존재하고 그 상위에 PE와 QE역할이 존재한다. 이러한 역트리 구조는 자원의 공유를 용이하게 한다. 즉 ED 역할이 이용할 수 있는 자원

들은 ED의 상위 역할들도 이용 가능하다. 그러나 이러한 구조는 하나 이상의 역할들로부터의 자원의 통합은 이루어지지 않는 단점이 있다.

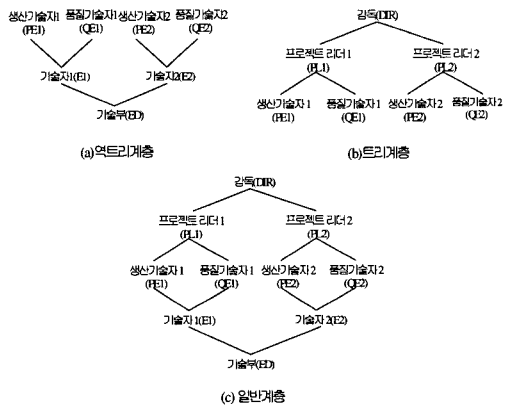

그림 4. 역할 계층의 예

그림 4.b는 하위 역할들의 허가를 상위 역할이 통합하는 트리 계층 구조를 나타낸다. 역할 PL1은 PE1과 QE1의 허가와 더불어 자신만의 추가적인 허가를 가진다. 이러한 구조는 자원의 통합에는 적합하지만 자원의 공유에는 적합하지 않다. 그림에서 보면 프로젝트1과 관련된 역할들과 프로젝트2와 관련된 역할들 사이에는 자원의 공유가 없다.

그림 4.c는 자원의 공유와 통합을 동시에 용이하게 하는 일반 계층을 보여주고 있다. 기술부에 최하위 역할인 ED가 있고 최상위 역할인 DIR이 있다. 이들 사이에 두 프로젝트에 대한 역할들이 위치한다. 각 프로젝트는 최상위에 PL 역할을 가지고 최하위에 engineer 역할을 가진다. 그리고 이 사이에 양립하는 PE와 QE 역할이 존재한다. 이러한 구조는 기술부의 더 많은 프로젝트로 확장될 수 있으며 각 프로젝트별로 다른 역할 구조를 가질 수도 있다.

또한 그림의 예는 다양한 부서로 확대될 수 있고, 이러한 부서는 각자에게 적용되는 다른 구조와 정책을 가질 수 있다. 실제의 많은 계층 구조는 그림과 같은 대칭형 구조보다는 비대칭형 구조를 가진다. NIST의 Hierarchical RBAC 모델은 그림 4와 같이 DIR과 같은 최상위 역할과 ED와 같은 최하위 역할이 반드시 존재할 것을 요구하지는 않는다. 적합한 계층의 설계는 조직의 정책에 관련된 문제로써 각기 다를 수가 있다. 본 모델에서의 요구사항은 일반 계층과 제한 구조를 지원하는 것이다.

3.2 제한 상속

그림 4.c에서의 DIR과 같은 상위 역할은 너무 큰 권한을 가지게 되므로 중대한 실수를 범할 수가 있다. 따라서 상위 계층에 상속을 제한할 필요성이 존재한다. 그림 5는 역할 계층에서 상속을 제한하는 예를 보여주고 있다.

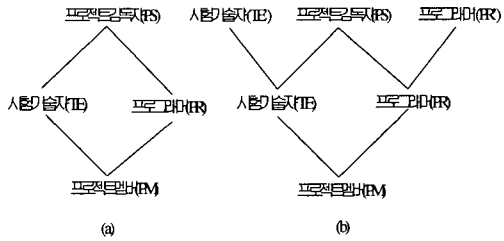

그림 5. 제한 상속의 예

그림 5.a에서 역할 PS는 프로젝트의 모든 허가를 상속한다. 반면에 그림 4.b에서는 TE가 PS에게 상속되지 않는 허가를 TE'에 가지도록 허락한다. 시험기술자들은 역할 TE'에 할당되며 TE는 단순히 TE'로 상속되어질 필요성이 있는 허가들을 가지는 장소이다. 이러한 TE'과 같은 역할을 사적 역할(private role)이라 한다. 예를 들어 시험기술자들이 자신들의 역할(TE)에 사적인 허가를 가지기를 원하여 역할 PS에게 상속을 제한하기를 원하는 허가가 있다고 하자. 예를 들어 아직 완성되지는 않았고 진행중인 업무사항에 대하여 시험기술자들은 프로젝트관리자가 이것을 보는 것을 원하지 않을 수도 있다. 시험기술자들을 역할 TE'에 할당하고 역할 TE로부터 허가를 상속한다. 이 허가들은 PS에게도 상속된다. 그러나 TE'의 허가는 역할 PS에 의하여 상속되지 않는다. 이러한 방식으로 특정한 허가들을 상위 역할이 상속하는 것을 막을 수 있다.

3.3 상속 계층과 활성화 계층

역할 계층에는 두 가지 다른 해석이 있다. 첫 번째는 역할 계층에서 상위 역할의 멤버들이 하위 역할로부터 허가를 상속받는 경우로, 허가-상속 해석이라 불리며 계층은 상속 계층이라 불린다. 그림 4.c에서 보면 역할 PL1이 활성화되면 역할 PL1과 PE1, QE1, E1, ED, 그리고 E에게 할당된 모든 허가들이 역할 PL1에 의해 사용되어질 수 있다.

두 번째 경우의 해석은 상위 역할을 활성화할지라

도 자동적으로 하위 역할들의 허가가 활성화되지는 않는 경우로서 활성화 해석이라 불리며 이러한 계층은 활성화 계층이라 불린다. 그림 4.c의 예에서 보면, 역할 PL1의 활성화가 상속 계층에서처럼 PE1, QE1, E1, ED, 그리고 E에게 할당된 허가들을 활성화하지는 않는다. 대신에 하위의 각 역할들이 허가를 사용하기 위해 활성화되어야 한다.

4. Constrained RBAC

그림 6과 그림 7에서 보듯이 Hierarchical RBAC 모델에 제약(constraints)을 추가한 것이 Constrained RBAC 모델이다.

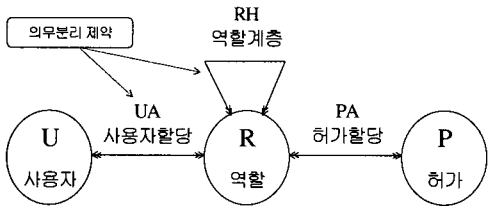

그림 6. Constrained RBAC-정적의무분리

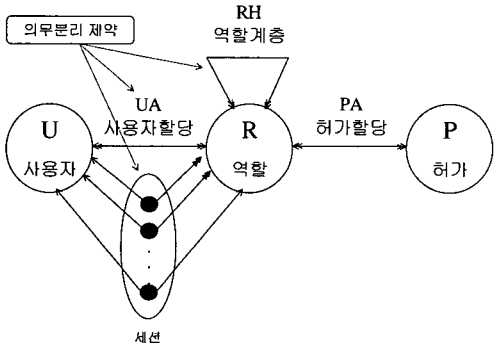

그림 7. Constrained RBAC-동적의무분리

제약은 사용자-역할 할당과 사용자 세션 내에서 역할들의 활성화와 관련된다. 분리(Separation)의 요구사항은 조직내의 사용자들이 그들의 직위에 적절한 권한 이상을 가지는 것을 방지하기 위하여 적용하는 이해의 상충(conflict of interest)에 대한 정책을 실행하기 위해 사용된다. 의무분리는 업무와 관련된 권한들을 다양한 역할들에 분배하는 것으로써 한 사용자가 너무 많은 권한을 획득하는 것을 막아준다. 따라서 중대한 부정행위는 많은 사용자들의 공모가 없이는 불가능하게 된다. RBAC 시스템에서는 분리의 개념이 최소 특권의 원리(principle of least privilege)에 의해 지원된다.

최소 특권은 사용자가 자신의 업무를 수행하기 위해 필요한 기능 이상의 특권을 가지지 않도록 사용자들에게 선택적으로 특권을 할당하는 관리 방법이다. 이렇게 함으로써 개인이 불필요하고 조직에 해가 될 수 있는 행동을 할 수 있는 능력을 갖지 못하도록 한다. 특권은 개인 또는 개인을 대신하여 활동하고 있는 주체에게 할당되는 권리로써 특권의 소유자는 이러한 권리의 범위 내에서 활동할 수 있다.

NIST의 RBAC 모델은 정적의무분리(SOD : Static Separation of Duty)와 동적의무분리(DOD : Dynamic Separation of Duty)를 지원한다.

4.1. 정적의무분리

역할에 기반한 시스템에서 이해의 상충은 사용자가 상충하는 역할들과 관련된 허가의 권한을 획득함으로써 발생한다. 이러한 이해의 상충을 방지하는 수단의 하나가 정적의무분리로써 사용자-역할 할당에 제약을 두는 것이다. 두 개의 상충하는 역할이 있다고 할 경우에 사용자가 한가지 역할에 할당되면 두 번째 역할에 할당되는 것은 금지된다.

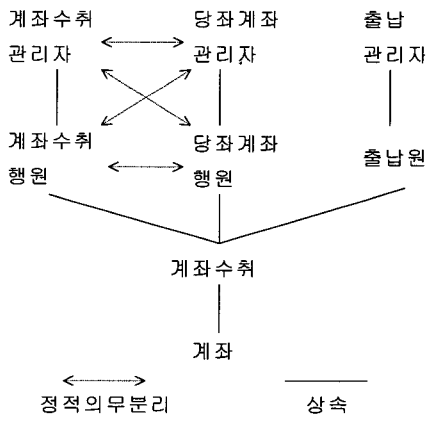

그림 8. Constrained RBAC-의무분리의 예

그림 8에서 보면, 당좌계좌 행원 역할에 할당된 사용자는 계좌수취 행원에는 할당될 수 없다.

제약은 역할 계층에서 상속된다. 예를 들어, 계좌수취 관리자 역할이 계좌수취 행원 역할을 상속하고, 계좌수취 행원 역할이 당좌계좌 행원 역할과 정

적의무분리 관계를 가진다면, 계좌수취 관리자 역할도 당좌계좌 행원 역할과 정적의무분리 관계를 가진다.

상속 계층에서 포함하고 있는 역할은 실제로 포함되는 역할의 인스턴스이므로 정적의무분리 관계가 성립하지 않는다. 그림에서 계좌수취 관리자 역할과 계좌수취 행원 역할과는 정적의무분리 관계를 가지지 않는다.

4.2. 동적의무분리

RBAC은 관리자에게 동적의무분리라는 조직에 특정한 정책을 실행할 수 있도록 한다. 정적의무분리는 사용자가 역할에 할당될 때 제약을 두지만 동적의무분리는 사용자가 독립적으로 행동할 때는 이해의 상충을 구성하지 않는 역할의 집합에 동시에 할당되는 것이 허용된다. 그러나 두 역할이 동시에 활성화될 때 문제가 발생할 수 있다. 예를 들어 한 사용자가 출납원 역할과 출납 관리자 역할에 할당되어져 있고 관리자는 출납원에게 열려진 현금 서랍을 닫도록 하는 행동이 허락되어져 있다고 하자. 출납원 역할로 행동하고 있는 사용자가 출납 관리자 역할로 변경하고자 한다면 RBAC은 사용자로 하여금 출납원 역할을 포기하도록 요구한다. 같은 사용자가 동시에 이 두가지 역할로 활성화되는 것을 허용하지 않는 한 이해의 상충 문제는 발생하지 않을 것이다. 이러한 효과는 사용자를 역할에 할당할 때 제약을 주는 정적의무분리에 의해서도 얻을 수 있지만, 동적의무분리는 조직에게 기능적인 유연성을 제공할 수 있다.

5. Symmetric RBAC

Symmetric RBAC은 그림 9와 그림 10에서 보듯이 Constrained RBAC에 허가-역할 리뷰에 대한 요구사항을 추가한 것이다.

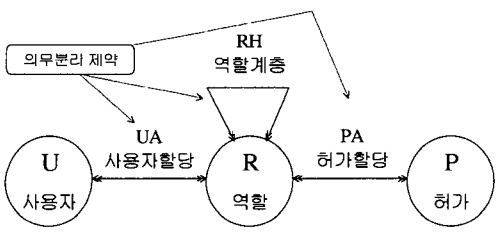

그림 9. Symmetric RBAC-정적의무분리

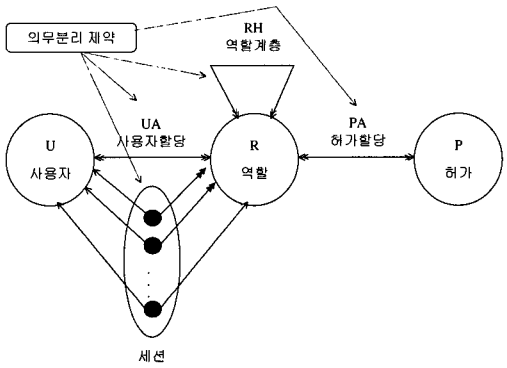

그림 10. Symmetric RBAC-동적의무분리

적절하고 정확한 허가-역할 할당을 유지하는 것은 권한 관리의 필수적인 요소이다. 과거의 허가-역할 할당은 조직의 상황이 변함에 따라 조직의 정책에 부적절해지는 경우가 있을 수 있다.

효과적으로 허가-역할 할당을 유지하기 위해, 조직은 허가-역할 할당에 대한 식별과 리뷰를 제공받아야 한다. 허가-역할 할당은 최소 특권의 원리가 지켜지도록 특별한 주의가 있어야 한다. 문제는 시스템 객체의 집합에서, 조직의 사용자에게 허가된 기능과 직무에 대응하는 적절한 허가 할당을 유지하는 방법이다.

허가 할당 리뷰의 필요성은 사용자가 조직을 떠나거나, 조직내에서 작업이 바뀌는 경우, 현재의 허가가 너무 오래된 경우 등의 다양한 관리적 상황에 기인하여 발생한다. 허가를 리뷰하고 조직의 운용을 위해 더 이상 필요가 없는 허가를 삭제하는 경우에는 주의를 기울여야 한다. 사용자가 조직을 떠나는 경우에는 사용자의 모든 허가는 효과적으로 취소되어야 한다. 하나의 방법은 조직내의 사용자의 모든 계정을 삭제하는 것이지만 시스템에 가비지를 남길 수 있고 잠재적인 위험요소가 될 수 있다. 사용자가 새로운 업무를 가지게 된 경우에 사용자의 새로운 책무에 필요한 허가를 지우는 것은 사용자가 효과적으로 자신의 업무를 수행하지 못하도록 할 것이며, 사용자의 업무를 수행하는 데 더 이상 필요 없는 허가를 삭제하지 않는 것은 최소 권한의 원리에 위반된다.

Flat RBAC 시스템은 사용자-역할과 허가-역할 할당에서 다대다 관계를 확립하고 유지할 것을 요구한다. 이러한 관계들 사이에서 Flat RBAC 시스템과 Hierarchical RBAC 시스템은 사용자-역할 할

당의 리뷰에 대한 인터페이스를 요구한다. Flat RBAC 요구사항은 사용자에게 직접적으로 할당되는 역할의 집합의 확립을 포함한다. Hierarchical RBAC은 사용자-역할 리뷰의 범위를 사용자에게 할당되는 역할들뿐만 아니라, 사용자에 할당된 역할들에 의해 상속되어지는 역할들까지 포함한다.

Symmetric RBAC은 이러한 요구사항들을 정의된 사용자와 역할에 대한 허가-역할 리뷰에 대한 인터페이스를 포함하도록 확대시킨다. 이러한 요구사항은 리뷰의 결과로써 관리자에게 리턴되는 데이터의 타입, 직접 또는 간접의 허가 할당을 선택하는 능력, 분산시스템에 대해서는 허가 리뷰가 적용될 목표 시스템을 선택하는 능력과 관련이 있다.

Symmetric RBAC은 허가-역할 리뷰 인터페이스가 특정 사용자와 역할에 할당된 허가와 관련된 객체의 집합 또는 오퍼레이션과 객체의 쌍의 두가지 타입의 결과 중 하나를 리턴하는 능력을 제공하도록 요구한다. 또한 이러한 질의의 옵션으로써 직접, 간접 허가 할당을 선택적으로 정의하는 능력을 요구한다. 직접 허가 할당은 사용자나 사용자에게 할당된 역할에 해당하는 허가의 집합이고 간접 허가 할당은 직접 허가 할당에 포함되어진 허가와 더불어 사용자에게 할당된 역할에 의하여 상속되어진 역할의 허가를 포함한다. 질의에 대한 또 하나의 옵션은 리뷰가 수행될 목표 시스템을 선택하는 것이다.

6. 기타 RBAC 특성

RBAC은 개방된 기술로써 표준화에 적합하지 않거나 아직까지 표준화에 대한 일치가 이루어지지 않는 특성들이 있다. NIST에서는 레벨 4의 RBAC 모델에 포함되지 않거나 부분적으로 포함된 RBAC의 아래와 같은 특성에 대해서 설명하고 있다.

● 확장성

확장성(Scalability)은 RBAC 제품의 선택에 있어서 매우 중요한 요소로써 확장성의 개념은 다양한 측면을 가진다. 즉 역할의 개수, 허가의 개수, 역할 계층의 크기, 사용자-역할 할당에 대한 제한 등이다.

NIST의 RBAC 모델에는 이러한 확장성을 통합시키지는 않았지만 제품 선택에 있어서 중요한 요소임에 틀림없다.

● 인 증

NIST RBAC 모델은 인증을 언급하지 않는다. 즉 개별 사용자들이 인증되는 방법과 사용자들이 속하는 역할에 관련되어지는 방법들을 언급하지 않고 있다. 이것은 RBAC을 위한 중요한 속성들로써 시스템 구조와 메커니즘의 고려 사항이다.

● 부정 허가

NIST RBAC 모델은 허가의 소유자에게 특정한 모드의 접근을 가능하게 하는 긍정 허가(Positive permissions)에 기반한다. 그러나 접근을 부정하는 부정 허가(Negative permissions)의 사용을 배제하고는 있지 않다. 그러나 이러한 부정 허가의 사용은 혼란을 가중시킬 가능성이 있다. 부정 허가를 채택한 경우와 같은 결과는 제약의 사용에 의해서 이루어질 수 있다.

● 허가의 속성

허가의 속성이 NIST RBAC 모델에서는 구체화되지 않는다. 허가는 개별적인 객체에서부터 전체 시스템에 이르기까지 적용될 수 있다.

허가는 읽기, 쓰기와 같은 원시 오퍼레이션의 관점에서 정의될 수도 있고 이것보다 더 큰 추상 오퍼레이션의 관점에서 정의될 수도 있다. 허가의 정확한 속성은 제품의 속성에 의해 결정된다. 운영체제, 데이터베이스 관리 시스템, 네트워크 관리 시스템 등은 모두 다른 종류의 허가를 지원할 것이다.

● 임의의 역할 활성화

NIST RBAC 모델은 사용자가 특정한 세션에 어떠한 역할들이 활성화되는지 선택하는 능력인 임의의 역할 활성화를 명시하지 않는다. 유일한 요구사항은 사용자에게 동시에 다양한 역할을 활성화하는 것을 허락하는 것이다.

● 역할 공학

NIST RBAC 모델은 역할을 설계하고 역할에 허가와 사용자를 할당하기 위한 지침을 제공하지는 않는다. 이러한 활동을 역할 공학이라 한다. 커다란 규모의 조직에서 RBAC의 효과적인 사용은 효과적인 역할 공학에 의존한다.

● 제 약

다양한 종류의 의무분리의 개념이 소개되고 있지만 NIST RBAC 모델은 제약으로써 정적의무분리와 동적의무분리만을 지원한다.

● RBAC 관리

NIST RBAC 모델은 역할에 사용자를 할당하고, 역할에 허가를 할당하고, 역할 계층을 구성하고 또한 이러한 할당을 취소시키는 관리적인 권한을 명기하지는 않는다.

● 역할 취소

NIST RBAC 모델은 역할 취소에 대해서 명기하지 않는다. 역할 취소에 관련된 주요한 이슈는 취소의 즉시성이다. 사용자가 역할로부터 취소되었을 때, 사용자가 그 역할로 활성화되어 있는 세션에서 사용자가 세션을 끝낸 후에야 취소되는가와 또는 즉시 비활성화 되는가의 문제이다.

Ⅳ. 결 론

RBAC이 나오게 된 동기는 보안 정책 관리를 단순화하기 위한 것이다. RBAC은 사용자의 역할에 기반을 둔 접근통제 방법으로 기존의 임의적 접근통제나 강제적 접근통제에 비하여 유연성과 적용성을 제공할 수 있다.

RBAC은 Ravi S. Sandhu가 제안한 기본 모델로부터 시작하여 최근의 강화된 NIST RBAC 모델까지 많은 발전을 거듭해왔다. 그러나 이러한 발전은 RBAC 특성의 구성에 대한 일반적인 합의 없이 이루어졌다. NIST에서는 이러한 문제점을 해결하기 위해 RBAC의 핵심 요소들을 정의하기 위한 노력을 기울여왔다. 본 논문에서는 NIST가 제안한 RBAC 표준 참조 모델을 소개하였다. RBAC은 계속 발전하고 있는 기술이지만 본 논문에 소개된 요소들은 RBAC의 핵심 요소들로써 안정되고 받아들여지는 것이다. RBAC의 핵심요소들에 대한 표준화는 RBAC 제품의 구현과 사용에 있어서 다양한 이점을 제공하리라 예상된다.

RBAC은 계속 발전하는 기술로써 새로운 RBAC의 특성이 제안되어 공감이 형성될 경우 NIST가 제안한 표준참조모델에 추가되어 모델의 강화가 있으리라 예상된다. NIST의 RBAC 연구 동향에 대한 계속적인 주시와 연구가 필요하리라 예상된다.

참 고 문 헌

[1] David F. Ferraiolo and D. Richard Kuhn, "Role-based access controls", *15th NIST-NCSC National Computer Security Conference,* pp 554-563, Baltimore, MD, October 13-16, 1992.

[2] David Ferraiolo, Dennis M. Gilbert, and Nickilyn Lynch, "An examination of federal and commercial access control policy needs", *16th NIST-NCSC National Computer Security Conference,* pp. 107-116, Baltimore, MD, September 20-23, 1993.

[3] David F. Ferraiolo, Janet A. Cugini and D. Richard Kuhn, "Role-Based Access Control(RBAC) : Features and Motivations", *Annual Computer Security Applications Conference,* pp 554-563, IEEE Computer Society, 1995.

[4] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein and Charles E. Youman, "Role-Based Access Control Models", *IEEE Computer,* pp. 38-47, Volume 29, Number 2, February, 1996.

[5] John F. Barkley, Anthony V. Cincotta, David F. Ferraiolo, Servan Gavrilla, and D. Richard Kuhn, "Role Based Access Control for the World Wide Web", *20th NISSC National Information Systems Security Conference,* pp 331-340, Oct. 7-10, Baltimore Convention Center, Baltimore, MD, April 8, 1997.

[6] David F. Ferraiolo, John F. Barkley, and D. Richard Kuhn, "A Role Based Access Control Model and Reference Implementation within a Corporate Intranet", *ACM Transaction on Information System Security,* pp 34-64, Volume 2, Number 1, Feb., 1999.

[7] W. A. Jansen, "Inheritance Properties of Role Hierarchies", *21th NCSC/NIST NISSC National Information Systems Security Conference,* pp. 476-485, Crystal City, VA, October 5-8, 1998.

[8] 김학범, 홍기웅, 김동규, "확장된 역할기반 접근통제 모델", 한국통신정보보호학회논문지, 제9권 제1호, Mar. 1999.

[9] Computer Systems Laboratory(CSL) Bulletin, "An Introduction to Role-Based Access Control", December, 1995.

[10] http://csrc.omg.org/corba/sectrans.htm #secl, "CORBAServices : Common Object Services Specification", 1998.

[11] Charles L. Smith, Edward J. Coyne, Charles E. Youman and Srinivas Ganta, "A Marketing Survey of Civil Federal Government Organizations to Determine the Need for a Role-Based Access Control(RBAC) Security Product", NIST&SETA, *Small Business Innovation Research(SBIR)*, July, 1996.

[12] ISO/IEC 15408-2, *Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 2 : Security functional require ments*, Aug, 1999.

[13] Jim Reynolds, Ramaswamy Chand-ramouli, *Role-Based Access Control Protection Profile*, Ver. 1.0, Cygnacom Solutions & NIST, July 30, 1998.

[14] ISO/IEC 9075-2, *Information Technology - Database Language SQL - Part 2, Foundation(SQL : 1999)*, Nov, 1999.

[15] Ravi S. Sandhu, David Ferraiolo, and D. Richard Kuhn, "The NIST Model for Role-Based Access Control : Towards A Unified Standard", RBAC 2000 Proceedings of the Fourth ACM workshop on Role-based access control(예정)

〈著者紹介〉

김 학 범 (Hakbeom Kim)
1990년 8월 : 중앙대학교 전자계산학과 졸업(석사)
1996년 3월 ~ 1999년 2월 : 아주대학교 컴퓨터공학과 박사과정 수료
1991년 10월 ~ 1996년 6월 : 한국전산원 주임연구원
1997년 4월 ~ 1998년 12월 : TTA/SC10/ SG3(시스템보안 연구위원회) 간사
2000년 1월 ~ 현재 TTA/TC10(정보보호 기술위원회) 간사, TTA/SC10/SG3 의장
1996년 7월 ~ 현재 한국정보보호센터 선임연구원, 표준과제책임자
※ 관심분야 : 컴퓨터·네트워크 보안, 접근통제, 정보보호 표준화

김 동 규 (Donggyu Kim)
서울대학교 공과대학 졸업(학사)
서울대학교 자연과학대학원 졸업(석사)
미국 Kansas 주립대 대학원 졸업(Ph. D, 전산학 박사, 정보통신 전공)
미국 Kansas 주립대 전산학과 교수
1979. 3 ~ 현재 아주대학교 컴퓨터공학과 교수
저서 : 데이터 통신시스템, 희중당, 1986년
저서 : 컴퓨터 통신 네트워크, 상조사, 1988년
한국통신학회 상임이사, 한국통신정보보호학회 부회장
※관심분야 : 컴퓨터 네트워크, 정보통신 프로토콜 엔지니어링, 정보통신 Security