동적 조직을 위한 접근제어 모델

심완보*
*충청대학 디지털전자통신과
e-mail : cool96@ok.ac.kr

An Access Control Model for the Dynamic Organization

Won-Bo Shim*
*Dept. of Digital Electronic Communications, Chung-Cheong University

요 약

본 논문에서는 기존의 관료제 조직과 다른 동적조직의 특성을 살펴보고 이러한 특성으로 인해 기존의 접근제어 모델들을 동적조직의 접근제어 모델로 사용할 때 문제가 되는 점들을 살펴본다. 이를 바탕으로 동적조직을 위한 개선된 역할기반 접근제어 모델을 제안한다. 제안된 모델은 기존 접근제어 모델들의 문제점을 해결하기 위한 방법들을 제시한다.

1. 서론

동적조직의 정의는 다양한 전문 기술을 가진 비교적 이질적인 전문가들이 프로젝트를 중심으로 집단을 구성해 문제를 해결하는 변화가 빠르고 적응적이며 일시적인 체제 라고 할 수 있다. 지금까지의 역할기반 접근제어 모델을 포함한 접근제어 모델들은 업무가 표준화되어 있고 변화가 없는 안정적인 구조의 상하관계가 명백한 관료제의 조직구조를 지원하는 모델들이었다.

R. Sandhu 의 역할기반 접근제어 모델은 상하관계가 분명하고 업무처리가 표준화 되어있는 관료제조직을 대상으로 하기 때문에 동적조직의 특성을 반영하기는 어려운 모델이다.[2] R.K. Thomas 가 제안한 C-TMAC 모델은 팀원간의 협업을 지원하는 모델이긴 하나 팀을 임시적인 조직이라기 보다는 어느 정도 영구성을 갖는 팀 조직을 대상으로 한 모델이다.[3] 또한 C-TMAC 모델에서는 사용자가 복합적인 권한을 부여받음으로 해서 발생할 수 있는 권한충돌에 대한 고려가 없으며 팀 자체적인 권한관리가 어려워 이로 인해 표준화되지 않은 업무를 처리해야 하는 동적조직의 특성을 반영하긴 어렵다. 이와 같이 일부 팀 기반 접근제어 모델(Team-Based Access Control Model)과 같은 팀 개념을 지원하는 접근제어 모델이 제안되긴 하였지만 기업의 태스크포스팀과 같이 유기적이며 임시적이고 업무가 표준화되어 있지 않고 환경변화가 많고 상하관계가 분명치 않은 동적조직의 특성을 충분히 반영하지는 못했다.

본 논문에서 접근제어 연구의 대상으로 삼고 있는 동적조직에 대하여 살펴 보고 동적조직에 대한 특징들을 살펴봄으로 해서 동적조직의 특성을 반영하는 접근제어 모델을 만들기 위해 어떠한 사항들이 고려되어야 하는 가를 살펴보고자 한다.

2. 동적조직을 위한 접근제어관점에서의 분석

문제점을 동적조직의 자치적 기능으로 인해 발생되는 문제점과 동적조직의 특성으로 인해 발생하는 문제점으로 나누어 생각해 본다.

먼저 동적조직의 자치적 기능으로 인해 발생되는 문제점을 살펴 보면 다음과 같은 3가지이다.

[문제1] 수행하는 업무의 비표준화로 인한 업무수행상 접근해야 할 자원범위 예측의 어려움이 있다.

[문제2] 팀 내의 자치적인 권한 관리가 필요하다.

[문제3] 사용자 자원에 대한 임의적 접근제어의 허용

다음은 동적 권한제어 기능제공으로 인해 발생되는 문제점 3가지이다.

[문제4] 개인의 능력과 주어진 업무의 중요도에 따른 권한의 할당

[문제5] 상충되는 권한충돌의 문제 해결

[문제6] 업무에 따른 역할에 할당된 자원접근 권한의 제한

이상과 같이 동적조직의 특성으로 인해 접근제어 관점에서 해결되어야 할 많은 다양한 기술적 문제들이 존재함을 보았다. 다음은 동적조직을 위한 접근제어의 요구사항에 대해 살펴본다.

먼저 일반적인 접근제어 모델로서의 요구사항들이다. 일반적인 요구사항은 사용자의 자원에 대한 접근 권한관리를 쉽게 할 수 있고 다양한 조직의 보안 요구사항을 만족시키는데 있다.

[요구사항1.1] 역할(role)개념의 사용으로 권한관리가 쉬워야 한다.

[요구사항1.2] 의무분리와 같은 제약사항을 기술할 수 있어야 한다.

[요구사항1.3] 접근제어 모델은 조직구조를 반영할 수 있어야 한다.

[요구사항1.4] 권한의 상속은 전체적인 상속과

부분적인 상속 모두가 지원되어야 한다.
[요구사항1.5] 정책 중립적이어야 한다.
이러한 일반적인 요구사항들은 역할기반접근제어의 특징과 많은 부분에서 일치하고, 역할기반접근제어 모델이 이러한 일반적인 요구사항들을 만족시켜 줄 수 있기 때문에 본 논문에서 제안하는 접근제어 모델은 역할기반접근제어 모델을 기반으로 한다.
다음은 동적조직의 특성으로 인한 접근제어 관점에서의 요구사항들이다.
[요구사항2.1] 표준화되지 않은 업무를 수행해야 한다.
[요구사항2.2] 팀 내의 자치적인 권한관리를 허용해 주어야 한다.
[요구사항2.3] 복합적인 권한에 대한 충돌문제를 해결해야 한다.
[요구사항2.4] 팀원들간의 수평적 관계를 반영해야 한다.
[요구사항2.5] 수행하는 업무에 따른 자원 접근 범위의 조정이 필요하다.
[요구사항2.6] 동적조직내의 융통성 있는 권한 관리가 필요하다.

표1. 동적특징과 연관된 요구사항 및 문제

분류	동적조직특징	동적특징 관련 요구사항	연관된 문제
자치적 기능	상호조정	요구사항 2.1, 2.2, 2.6	문제 1, 3
	행동의 낮은 공식화	요구사항 2.1, 2.2, 2.5, 2.6	문제 1, 2, 3
	횡적연결장치가 조직전반에 걸쳐 많음	요구사항 2.1, 2.2	문제 1, 2
	갈등해결이 상호작용에 의해 조정	요구사항 2.1, 2.2, 2.6	문제 1, 3
	의사전달이 충고와 상담에 의해 이루어짐	요구사항 2.1, 2.2, 2.6	문제 1, 2, 3
	규칙이 적음	요구사항 2.1, 2.2	문제 1, 2
동적권한제어기능	권력의 초점이 기술과 능력에 따라 어느 곳에서도 존재	요구사항 2.6	문제 4
	높은 수평적 분업화	요구사항 2.4, 2.5, 2.6	문제 4, 6
	매우 복잡한 기술시스템	요구사항 2.3, 2.4, 2.5	문제 5, 6
	복잡하고 동태적인 환경	요구사항 2.3, 2.4, 2.5, 2.6	문제 4, 5, 6
	권한이 개인 능력에 좌우됨	요구사항 2.6	문제 4

동적조직은 계속적인 상황변화를 겪게 된다. 팀원의 구성도 계속해서 바뀔 수 있고 팀원이 수행하는 업무도 바뀔 수 있다. 또한 팀원들의 업무변화에 따라 자원에 대한 접근권한이 수시로 바뀔 수 있다. 즉 팀내의 접근제어의 구성 요소들인 역할, 사용자, 접근권한, 업무 등이 수시로 바뀔 수 있다는 것이다. 이러한 상황에서 팀원의 자원에 대한 접근권한의 관리가 이러한 변화를 따라주지 못한다면 팀원의 업무수행에 많은 장애를 줄 것이다. 이를 위해 팀내의 자원에 대한 접근관리의 자율성이나 다른 동료로부터 자원에 대한 접근권한을 일시적으로 허락받는 시스템적인 지원이 필요하게 된다.이상으로 동적조직을 위한 접근제어에 있어 일반적인 접근제어 모델로서의 요구 사항들과 동적조직의 특성으로 인한 접근제어 모델로서의 요구사항들을 살펴 보았다. 표1에서는 접근제어의 관점에서의 특징들과 동적조직의 특성으로 인한 접근제어 관점에서의 요구사항 및 문제점들이 어떠한 연관관계를 가지고 있는지를 자치적 기능과 동적 권한제어 기능으로 분류해 도표로 정리하였다. 일반적인 요구사항은 역할기반 접근제어 모델을 사용하여 해결할 수 있는 문제이므로 여기서는 생략하였다.
표 1 에서 보는 바와 같이 동적조직의 특징에 따라 다양한 요구사항과 문제점들이 서로 연관되어 있으며 이러한 요구사항을 만족하고 문제점을 해결함으로써 동적조직의 특징들을 충분히 반영한 접근제어 모델과 문제 해결 방법을 찾을 수 있음을 알 수 있다. 다음은 지금까지 연구된 다른 접근제어 모델들을 살펴보고, 이 접근제어 모델들이 앞에서 살펴본 동적조직을 위한 접근제어에서의 문제점들을 충분히 해결할 수 있는지를 분석해 본다.

표 2. 기존모델의 요구사항 만족도 분석

구분	요구사항	RBAC [2]	T-RBAC [5]	TMAC [1]	C-TMAC [3]
일반사항	요구사항 1.1	O	O	O	O
	요구사항 1.2	O	O	O	O
	요구사항 1.3	O	O	O	O
	요구사항 1.4	O	O	O	O
	요구사항 1.5	O	O	O	O
동적조직특징사항	요구사항 2.1:	X	X	X	X
	요구사항 2.2	X	X	X	X
	요구사항 2.3	N/C	N/C	N/C	N/C
	요구사항 2.4	X	X	△	△
	요구사항 2.5	X	X	O	O
	요구사항 2.6	X	X	X	X

N/C : No Comment

표 2 에 동적조직을 위한 요구사항에서는 RBAC, T-RBAC, TMAC, C-TMAC 모델들은 각 요구 사항들을 만족시키기에는 적합하지 못함을 알 수 있다. 다음에는 이러한 문제점 분석과 요구사항 분석을 바탕으로 동적조직의 특성을 반영한 개선된 RBAC 모델을 제시하고 문제점들을 해결하는 방법들을 제시한다.

3. 제안하는 모델

제안하는 모델에서는 기존의 관료제 조직과 동적조직의 특성을 통합하여 반영한 접근제어 모델을 만들기 위해 다음과 같은 이중의 역할 구조를 사용했다.

표 3. 모델 표기법

표기	설명
U	사용자
U_i	내부역할 구조내의 사용자
R	역할
R_i	내부역할
R_e	외부역할
P	퍼미션
P_i	내부역할의 퍼미션
P_e	외부역할의 퍼미션
W_i	내부역할 구조내의 워크
SW_i	내부역할 구조내의 서브워크
S	세션
C	컨텍스트
I-RH	내부역할 구조
E-RH	외부역할 구조
V_i	내부역할 구조내의 뷰
$R_i < R_j$	R_j는 R_i의 직접 상위역할이다.
$R_i <^* R_j$	R_j는 R_i의 직접 또는 간접 상위역할이다

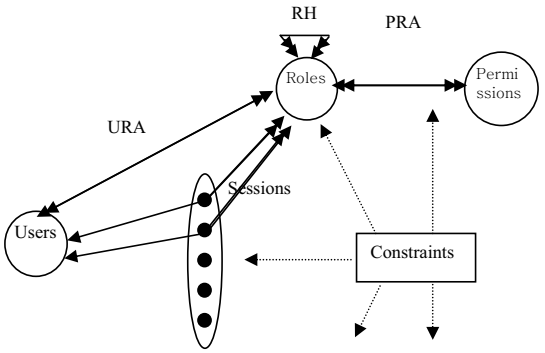

그림1. 외부 역할 모델

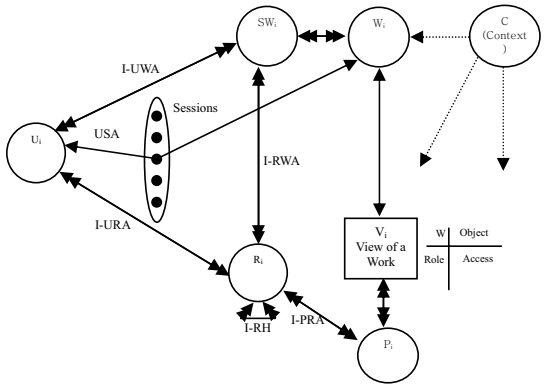

그림2. 내부 역할 모델

명제 1. 사용자는 자신에게 할당된 역할만을 활성화할 수 있다.

$\forall u : users, r : roles$

$r \in active - roles(u) \Rightarrow u \in role - members(r)$

명제 2. 사용자는 역할을 활성화해야만 역할에 할당된 Operation을 수행할 수 있다.

$\forall u : user, op : operation :$

$exec(u, op) \Rightarrow active - roles(u) \neq \varnothing$

명제 3. 사용자의 역할에 어떤 객체를 접근하기 위한 권한이 주어져 있고 그 역할이 사용자에 의해 활성화되어있을 때만 사용자가 그 객체에 접근하는 것이 가능하다.

$\forall u : user, o : object :$

$access(u, o) \Rightarrow \exists r : roles, op : operation :$

$r \in active - roles(u) \wedge op \in role - operations(r, o)$

명제 4. 역할에 대한 사용자 지정 수는 역할의 cardinality를 초과할 수 없다.

$\forall r : roles :$

$number - of - members(r) \leq membership - \lim it(r)$

명제 5. 어떤 사용자가 어느 한 역할에 할당을 받으면 그 사용자는 할당 받은 역할의 하위역할도 할당 받은 것으로 본다.

$\forall u : user, r_{i,j} : roles$

$r_j \in authorized - roles(u) \wedge r_j \succ r_i \Rightarrow$

$r_i \in authorized - roles(u)$

명제 6. 사용자는 자신에게 할당된 워크에 관계된 역할만을 활성화할 수 있다.

$\forall u : users, r : roles, w : works$

$r \in active - roles(u) \Rightarrow u \in work - members(w) \wedge$

$r \in authorized - work - roles(w) \wedge u \in role - members(r)$

4. 결론

제안하는 모델에서는 동적 접근제어 기능을 지원하는 데서 발생되는 문제를 해결하기 위해 다음의 세가지 문제를 해결했다.

첫째, 개인의 능력과 주어진 업무의 중요도에 따른 권한의 할당 문제에 있어서 TMAC과 C-TMAC 모델에서는 팀원이 팀에 소속됨으로써 팀에 부여된 역할을 사용할 수 있게 하는 방법이기 때문에 팀장을 제외한 모든 팀원은 같은 역할을 갖게 되므로 TMAC과 C-TMAC 모델을 이용해 이 문제를 해결하기는 어려움이 있고 Sandhu 모델과 TRBAC 모델에서는 직위에 따른 융통성 없는 권한 부여로 개인의 능력을 반영하기 어렵다. 제안하는 모델에서는 내부역할 구조에서 Sub Role을 이용하여 필요한 역할을 생성하여 중요한 일을 수행할 팀원에게 그의 상사보다 많은 권한을 주어 융통성 있게 할당함으로써 기존의 역할 구조상의 권한 관계를 뛰어 넘어 중요한 업무를 능력 있는 팀원에게 담당하게 할 수 있다.

둘째, 상충되는 권한충돌의 해결에 있어서는 다른 모델들은 이에 대한 언급이 없고 이를 고려하고 있지 않으나 우리가 제안하는 모델에서는 관료제 조직과 동적조직이 병존하는 상황에서 일어나는 충돌문제를 제안하여 해결 한다.

셋째, 업무에 따른 역할에 할당된 자원접근 권한의 제한에 있어서 TMAC이나 C-TMAC 모델에서 팀의 역할 개념을 이용하거나 시간, 장소 등의 정보를 이용한 컨텍스트 정보를 활용하고 있으나 이를 통해 업무에 따른 역할에 할당된 자원접근 권한의 제한문제를 충분히 해결하기 어렵다. 제안하는 모델에서는 Need-To-Know를 위한 워크 개념을 활용하여 사용자에게 할당된 역할들 중에 현재 수행중인 업무에 관계된 최소한의 필요한 역할권한만이 활성화될 수 있도록 역할 필터링 기능을 제공하여 해결하고 있다.

다음은 이상과 같은 제안된 모델의 미비점으로 인한 모델 사용상의 문제점들을 논의해 본다. 개런티 기능이나 위임역할, Sub Role 등의 사용으로 인해 보안관리의 보완을 위한 부담과 역할관리에 있어서 부담이 증가 하겠지만 이로 인해 동적조직을 위한 접근제어의 요구사항을 만족 시키는데 문제가 되는 것은 아니다. 그러나 충돌문제 해결에 있어서는 다소 시스템관리자에게 융통성을 부여하고 있으나 충분하지는 못할 수 있다. 워크플로우에 있어서는 실제 워크플로우 시스템이 조직 내에서 신속한 업무처리를 위해 일반적으로 쓰이고 있다고 볼 때 워크플로우 개념 지원을 하지 못함으로 인해 동적 조직에서 업무 처리자가 조직 외부의 개발자나 전문가의 도움 없이 프로세스를 정의하며 표준화되지 않은 업무를 자동화 하는데 대한 지원에 어려움이 있을 수 있다. 또한 워크플로우 시스템이 업무처리에 도입되면서 이로 인한 프로세스 단계별 권한제약이나 권한 충돌 문제도 새롭게 정의되고 해결되어야 할 것이다. 그러나 TRBAC을 제외한 다른 접근제어 모델에서도 워크플로우에 대한 것은 워크플로우 시스템에서 처리하여 사용하는 것으로 가정하고 별다른 고려를 하고 있지는 않다. 제안하는 모델도 워크플로우에 관련된 처리를 워크플로우 시스템 엔진에서 처리한다면 현재의 모델로도 워크플로우와 연동하여 사용되어질 수는 있을 것이다.

참고문헌

[1] Rosan K. Thomas, "Team-based Access Control (TMAC): A Primitive for Applying Role-based Access Controls in Collaborative Environments", ACM RBAC'97, 1997, pp. 13-19.

[2] R. Sandhu, E. Coyne, H. Feinstein, and C. Younman, "Role-Based Access Control Models", IEEE Computer Magazine Vol. 29, 1996, pp. 38-47.

[3] Christos K. Georgiadis, Ioannis Mavridis, G. Pangalos, Rosan K. Thomas, "Flexible Team-Based Access Control Using Contexts", Proc. of the 6th SACMAT, 2001, pp. 21-27.

[4] D.Ferraio, J.Cugini and R.Kuhn,"Role-based Access Control (RBAC): Features and motivations", Proc. of 11th Annual Computer Security Application Conference, 1995, pp. 241-248.

[5] Sejong Oh, Seog Park, "Task-Role Based Access Control (T-RBAC): An Improved Access Control Model for Enterprise Environment", DEXA, 2000, pp. 264-273.

[6] Rosan K. Thomas, Ravi Sandhu "Task-based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management". 11th IFIP Working Conference on Database Security, 1997, pp. 166-181.

[7] 심완보, 박석, "애드호크러시 조직의 특성을 고려한 역할기반 모델", 한국정보보호학회논문지 2002년 12권 4호, pp. 41-53.

[8] NIST SP 800-53, “Recommended Security Controls for Federal Information Systems”, Public Draft, Revision 1, 2006. 3

[9] NIST SP 800-53A, “Guide for Assessing the Security Controls in Federal Information Systems”, Second Public Draft, 2006. 4