유비쿼터스 업무공간의 협업 RBAC모델 설계

이수정°
고려대학교 컴퓨터정보통신대학원
ngenius@korea.ac.kr°

A Collaboration RBAC Model in Ubiquitous Workspace

SooJeong Lee°
Graduate School of Computer Information and Technology, Korea University

요 약

유비쿼터스 인프라의 발달로 인한 업무 환경의 활발한 변화는, 다양한 (이동성) 단말과 끊김 없는 네트워크를 통하여, 기업 내외부의 응용을 활용하며, 효율적인 상황인식에 따른, 실시간적 업무공간을 지원 받을 것이다. 이는 인증과 인가의 분리 구조로서, 기업 내부의 접근제어 미들웨어와 기업 외부의 서비스 프로바이더 간의 분산 환경을 의미한다. 그러나 이러한 처리는 도메인 상호간 안전한 상호운용성이 선결되어야 한다. 즉 유비쿼터스 업무공간의 협업 서비스를 위한 접근제어모델은, 상황인식과 실시간 정책변경의 처리가 다중도메인간의 안전한 연동과 함께 요구된다. 본 논문은 메타정책(Metapolicies) 기반으로 도메인 내부와 외부도메인의 접근제어를 구분하여 보호한, 다중도메인 관계의 동적 협업 RBAC모델을 제안한다.

1. 서 론

유비쿼터스[1] 인프라의 발달에 따라 업무 환경에도 활발한 변화를 지원받게 될 것이다.[10] 정보 근로자는 다양한 이동성/비이동성 단말로써, 유무선의 끊김 없는 네트워크를 통하여, 전문화 세분화로 분리된 기업 외부의 서비스 프로바이더(SP)가 제공하는 응용서비스들을 마치 내부서비스처럼 활용하며, 시간, 위치, 단말UI, 네트워크 QoS, SP제공상태 등의 효율적인 상황인식에 따른, 실시간적 업무공간을 지원받을 것이다.

다양한 업무 중에서 협업 유형은, 관계자와 의사소통 및 정보공유를 용이하게 지원하는 업무이며, 조직과 직책에 독립적인 직무구조를 갖는다.[2] 이러한 협업서비스의 접근제어모델은 효율적인 상황인식, 실시간 정책변경 등에 앞서 서로 다른 플랫폼으로 요청/시행이 분산된 수준의 처리가 요구된다[3]. 이 때 외부서버에 대한 원격접속 형태가 아닌, '인증'과 '인가'의 도메인이 분리된 환경에서는, '권한'의 논리적 의미를 정확하고 안전하게 인터페이스할 상호운용성이 선결되어야 한다.

RBAC모델[4]의 향후 과제로서, B2B, B2C를 위한, 교차-조직 체계에서, 사용자할당(UA)과 권한할당(PA)이 분리된 광범위한 응답처리 기술을 예측한 바 있으며,[5] 서로 다른 도메인은 접근제어모델, 시맨틱, 스키마, 자료명, 정책 제약조건 등의 차이에서 여러 유형의 충돌이 일어날 수 있기 때문이다.[6]

그러나 기존의 다중도메인 상황인식 접근제어에 관한 연구는 외부도메인의 '인가'를 위하여 프로바이더 자신의 '역할'을 직접 사용한 접근을 처리하고 있다. RBAC 체계 내에서 '권한'을 사상하는 '역할'의 노출은 곧 <표 2>와 같은 크로스도메인 공격에 대한 보안상의 치명적 결함이 될 수 있다.

이에 본 논문은 메타정책(Metapolicies) 기반으로 내부 접근제어와 외부도메인의 접근제어를 명확히 구분함으로써 보안성을 개선하여 안전한 다중도메인간의 상호운용성을 보장하는, 유비쿼터스 업무공간의 상황인식 협업 RBAC모델을 제안한다.

본 논문의 구성은, 2장은 기존의 협업, 상황인식, 상호운용성 관련 모델 연구를, 3장은 제안 모델의 설계를, 4장은 유비쿼터스 업무공간의 협업의 모델링을 통하여 제안 모델을 검증한다.

2. 관련 연구

협업시스템이 갖추어야할 요구사항을 점검하고, 이에 추가적으로 상호운용성 지원 모델과 상황인식 처리 모델을 연구하고, 그 문제점과 보완사항을 위하여 관련 모델을 분석한다.

2.1 협업시스템을 위한 접근제어모델의 요구사항[3]

접근제어모델의 설계시 요구사항을 아래와 같이 정의하였다.

① 분산된(distributed) 플랫폼 수준에서 요청/시행 될 것.
② Role, Context 등 변동적(varied) 정보로 효율적 권한 정의.
③ 단일사용자 모델보다 기능공유로 인한 확장성 지원.
④ 정보와 자원에 대해서도 방어 가능.
⑤ 협업에 제약을 주지 않는 간편 투명한 접근과 통제.
⑥ 관리 효율을 향상시킬 높은 수준의 접근권한 정의.
⑦ 실행 도중에도 정책 정의와 변경 가능.

<표 1> 접근제어모델의 비교[3]

구분	Matrix (ACL)	RBAC	TBAC	TMAC	C-TMAC	SAC	Context-AW
복잡도	Low	M	M	M	M	L	High
이해도	Simple	S	S	S	S	S	S
편리성	Medium	H	M	H	H	L	H
실용성	M	H	M	M	H	L	H
협업지원		L	Y	Y	Y	Y	Y	Yes
그룹지정		L	Y	L	Y	Y	Y	Y
정책정의		L	Y	L	Y	Y	L	Y
정책적용		No	L	L	Y	Y	N	Y
임의권한		Passive	P	A	A	A	A	Active
활성화		N	L	M	M	M*	M	Medium*
상황인식								

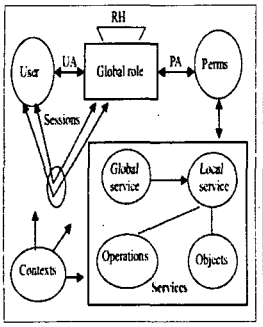
2.2 다중도메인의 상호운용성을 위한 모델 분석

2.1.1 CGRBAC과 CWS-RBAC 모델

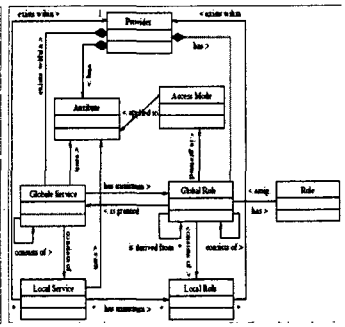
[그림1,2]는 외부향 다중도메인 상호운용성 모델로서, 웹서비스에서, 외부 연동 서비스(Composite Service, Global Service)에 대한 상호운용성을 정의하였다. SOAP을 통한 외부서비스 호출시, 외부접근용 역할(Global Role)과 각 프로바이더의 자체 역할(Local Role)에 대한 매핑이 미리 정의되어 있어, 실제접근은 각 프로바이더의 '역할'로 해석되어 요청된다.[7][8]

이 때 내부는 동일 역할(서비스)에 대해서도 프로바이더 마

다 서로 다른 역할-매핑을 내부 집중형으로 전담하는 구조이다. 또한 외부 수용을 위한 프로바이더측은 역할계층이 노출된 보안상 취약성을 보인다.

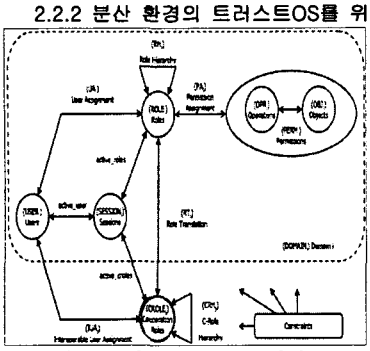


[그림 1] CGRBAC모델[7]

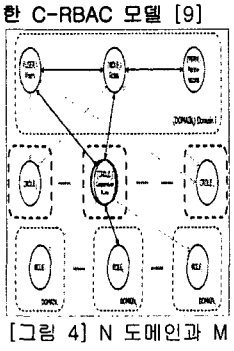


[그림 2] CWS-RBAC 모델[8]

2.2.2 분산 환경의 트러스트OS를 위한 C-RBAC 모델 [9]



[그림 3] C-RBACモデル[9]



[그림 4] N 도메인과 M 협력도메인[9]

[그림 3]은 내부향 다중도메인 상호운용성 모델로서, 분산 환경의 운영체제에서 외부도메인의 접근에 대하여 '메타역할'로써 '시큐리티-도메인'을 보장한 RBAC 모델이다.<표 2>의 보안사항을 고려하고 '메타정책(MetaPolicies)'을 수용하여 도메인에 독립적인 '메타역할'(;협력역할, CROLE, Cooperation-ROLE, Meta ROLE)과 내부 정규역할간의 해석관계(*RT*), 사용자 할당(IUA) 등을 정의하여, 내부역할이 노출되지 않는 간접적 해석 구조를 제시하였다. [그림4]는 협력역할을 중앙으로 여러 도메인과 연동하는 상호운용성을 예시하고 있다. 아래는 주요 정의이다.

■ **C-RBAC model**
- $DOMAIN_i$: 독립 역할 계층 영역. $(1 \le i \le n)$
- $CROLE_j$: 협력역할 (;메타역할). $(1 \le j \le m)$
- $USER_i$, $ROLE_i$, OPR_i, OBJ_i, $PERM_i$, $SESSION_i$
- $IUA_i \subseteq USER_i \times CROLE_j$: 협력 역할 사용자 할당 정의
- $RT_i \subseteq ROLE_i \times CROLE_j$: 정규역할과 협업역할의 관계정의
- $CRH_j \subseteq CROLE_j \times CROLE_j$, $CROLE_j$의 partial ordering

■ **Access Dicision**
- $access\_to\_local(u{:}USER_i,\ p{:}PERM_i) \rightarrow \{true,\ false\}$
- $access\_to\_foreign(u{:}USER_i,\ p{:}\bigcup_{k=1}^{n} PERM_k) \rightarrow \{true,\ false\}$

<표 2> 다중도메인 관계 RBAC에서 가능한 충돌[9]

Conflict	Configurative condition	Possible threats
Domain conflict	Cross-domain UA Cross-domain PA Cross-domain UA and PA	Conflict of interest Conflict from multiple managers Conflict of duties
Rule conflict	Cross-domain role-to-role translation	Covert promotion
Policy freeness	Cross-domain role-to-role translation	Infiltration

2.3 Environment RBAC 모델[10]

본 모델은 <표1>에서 'Context-AW'로 분석되었던, 'GRBAC'으로 알려진 상황인식 접근제어 모델이다. 상황정보를 환경역할계층(ER)으로 정의하고, 이는 권한 요청시 환경조건(EC)에 따라 동작되어, 정규역할의 활성화를 판단하여 준다.

Tuple : <srole, object, erole-set, op>

위와 같은 구조로서, 시간, CPU/네트워크부하 등의 상황(환경조건)에 따라 동작된 환경역할(***erole-set***) 판단을 통하여 정규역할(***srole***)의 활성화와 기능(***object***)의 권한(***op***)을 결정한다.

3. 다중도메인 상호운용성 관계의 동적 협업 RBAC모델 설계

'2.1'절에 대한 상세 정의로서 아래 사항을 고려한다.

⑧ 외부 도메인의 기능 사용이 가능한 접근제어.

⑧' 외부 도메인의 역할계층의 안전한 참조 및 해석 가능.

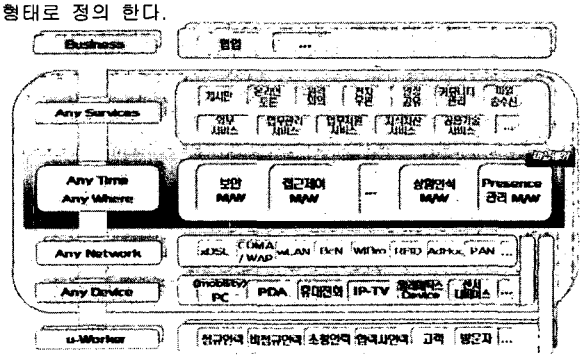
⑨ 실행 도중에도 상황인식에 의한 권한제어 가능.

⑨' 상황인식에 의한 동일 권한 내의 '기능' 변경제어 가능.

3.1 유비쿼터스 업무공간의 모델링

유비쿼터스 인프라의 5-ANY를 반영한 아키텍쳐를 설계하였다. 다양한 역할과 상황을 갖는 '*u-Worker*'에게 여러 서비스의 융합으로 이루어진 편리한 '비즈니스'를 제공하기 위하여, '단말', '네트워크', '미들웨어', '서비스'로 이루어진 유비쿼터스 인프라가 그 가운데에서 연동하며, 각 층은 확장성을 갖는다.

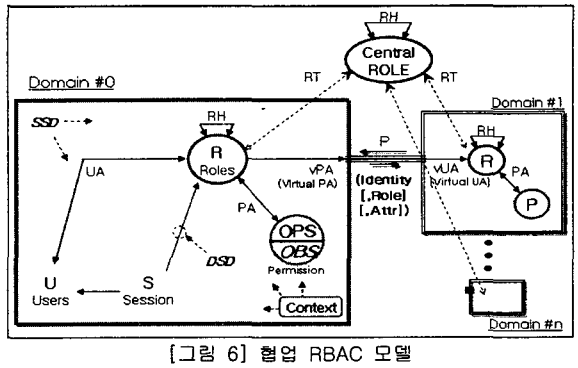
[그림 5]는 본 논문에서 다루고 있는 협업을 우선 배치하였다. 이 중 외부 SP, 상황인식 M/W 등과 인터페이스를 처리하는 '접근제어 시스템'은 '*AnyTime/AnyWhere*', 즉 '미들웨어'의 형태로 정의 한다.



[그림 5] 유비쿼터스 업무공간의 아키텍쳐

3.2 협업 RBAC 모델

[그림 6]은 본 논문이 제안하는 협업 RBAC 모델로서 중앙 협업역할의 참조를 통하여 외부 도메인과의 안전한 상호운용성을 확보하도록 개선되었다.



[그림 6] 협업 RBAC 모델

상황인식 등 세밀한 권한/정책제어는 기업 내부에서 수행되고, 제어된 권한은 SP에게 통보되며, 이 때 중앙역할계층의 참조를 통하여 SP의 오퍼레이션(OPR)이 변경되어, 실제 외부 SP 서비스의 기능(OBJ)에 대한 권한을 얻게 된다.

내부의 동일 역할, 동일 오퍼레이션에 대하여 기능만의 변경, 즉 SP 변경이 가능한 구조로서 정의한다.

■ 주요 정의

- $CentROLE_k$: 중앙 협업 역할. 메타역할. (Central Collaboration Role)
- $DOMAIN_i$: 독립 역할 영역. $(1 \le i \le n)$
- $USER_i$, $ROLE_i$, OPS_i, OBS_i, $PERM_i$, $SESSION_i$
- $UA_i \subseteq USER_i \times ROLE_i$: 정규 역할 사용자 할당 정의
- $PA_i \subseteq PERM_i \times ROLE_i$: 정규 역할 권한 할당 정의
- $PERM_i \subseteq OPS_i \times OBS_i$: 정규 역할 권한의 상세 정의
- $RT_i \subseteq ROLE_i \times CentROLE_k$: 정규역할과 중앙협업역할의 관계정의
- $vPA_i \subseteq PERM_i \times CentROLE_k$: 협업 역할 외부 권한 할당 정의
- $vUA_j \subseteq USER_j \times CentROLE_k$: 협업 역할 외부 사용자 할당 정의

■ 정책 Profile

- $\langle ROLE_i, OBS_i, OPS_i, [Context[,...]] \rangle$

4. 유비쿼터스 업무공간의 협업의 모델링

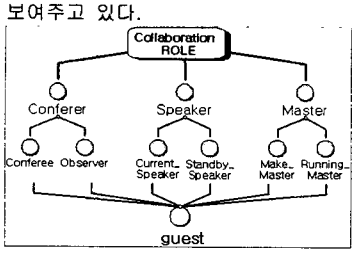
3장을 통하여 설계한 접근제어모델을 통하여, 아래와 같은 시나리오를 처리하도록 검증한다.

4.1 시나리오

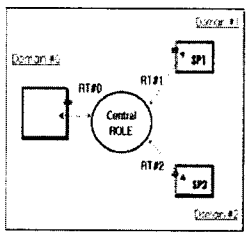
상황1 : (관리자 알림) 현재 PDA 영상회의 참여자중 일부가 QoS 기준 미달 상황으로 변화되고 있습니다. 해당 참여자를 전화회의 참여로 전환 하시겠습니까?

4.2 중앙 협업 역할의 정의와 연동

협업 역할의 정의는 조직과 직책에 독립적인 직무 성격을 반영하여 자체적인 직무분리가 필요하다. [그림 7]은 이 중 영상회의에 관계된 메타역할계층의 예이다. 이것으로 각 도메인의 메타역할을 통일하여, 중앙협업역할계층으로서 상호운용성을 위한 참조를 지원한다. [그림 8]은 이 중앙역할계층을 통하여 인가 처리를 위한 상호운용성이 지원되는 역할 연동의 구조를 보여주고 있다.



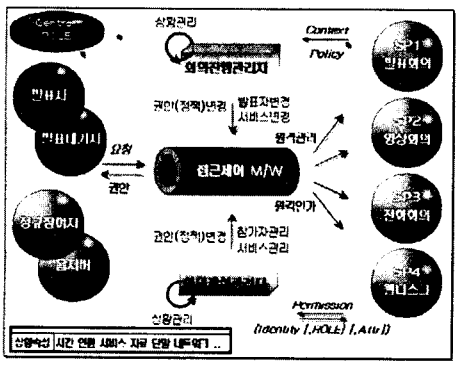
[그림 7] 협업 역할



[그림 8] 역할 연동

4.3 협업 비즈니스 프레임웍 설계

[그림 9]는 협업 비즈니스를 분석하여 도출한 프레임웍이다.



[그림 9] 협업 비즈니스 프레임웍

접근제어 미들웨어를 중심으로 참여자/발표자/관리자 등 해당 역할계층의 사용자와 서비스 프로바이더 등이 연동되는 구조이며. 이는 내부와 SP에 모두 중앙협업역할의 참조로서 접근제어의 상호운용성을 지원하게 된다.

4.4 접근제어 프로세스

3장과 4장의 구성요소들로써 '4.1'의 시나리오를 처리한다.

[그림 8]의 Domain0의 상황인식에 의하여 SP1에서 SP2로 실시간 변경에 대한 요구가 발생되었다. 각 도메인은 중앙역할에 대하여, 각각 RT#0, RT#1, RT#2의 관계정의가 이루어져 있다. Domain0는 정의1을 통하여, 새로운 기능에 대한 권한을 부여하고, 이는 정의 2를 통하여 외부도메인의 권한 승인과정을 거치게 된다. 이 때 동일 역할, 동일 오퍼레이션에 대하여 기능의 변경 및 권한관리를 위하여 세밀한 접근제어가 필요하므로, 아래와 같은 정의를 통하여 처리하였다.

■ 정의 1: 내부도메인 접근 정의

- $[\exists r_i] [(u_i, r_i) \in UA_i \wedge (ops_i, r_i) \in PA_i \wedge (obs_i, r_i) \in PA_i]$

■ 정의 2: 외부도메인 접근 정의

- $[\exists r_i, cr_k, r_j] [(u_i, r_i) \in UA_i \wedge (ops_i, r_i) \in vPA_i \wedge (obs_i, r_i) \in vPA_i \wedge (r_i, cr_k) \in RT_i \wedge (r_j, cr_k) \in RT_j \wedge (u_j, r_j) \in vUA_j \wedge (ops_j, r_j) \in PA_j \wedge (obs_j, r_j) \in PA_j]$

5. 결론 및 향후 과제

본 논문에서는 유비쿼터스 인프라를 통하여 변화하는 업무공간에서의 확장된 서비스 형태를 위하여, 기업 내부의 접근제어 시스템과 외부도메인의 서비스 프로바이더간에 안전한 상호운용성을 갖는 접근제어모델에 관하여 개선하였다. 이는 중앙역할계층을 참조하여 권한의 논리적 의미를 인터페이스 하며, 이로써 기업의 접근제어정책이 외부 SP의 권한제어로 전달되는 상호운용성이 확보 되었고, 아울러 원격협업을 위한 서비스의 안전한 외부 확장을 가능하게 하였다. 이로써 기업의 내부 서비스 사용과 구분 없는 SP의 전문화된 서비스를 제공 받을 수 있는 환경을 갖추는 데에 활용될 수 있을 것이다.

향후 세밀한 접근제어를 위하여 중앙역할계층의 확장을 추가적으로 연구하며, 다양한 상황을 적용할 수 있도록 보완되어야 할 것이다.

6. 참고문헌

[1] Mark Weiser, "The Computer for the 21st Century", Scientific American, Vol.265, No.3, pp.94-104, Sep. 1991.

[2] 한국전산원, "범정부 서비스컴포넌트 참조모델 1.0", 정보통신부, 범정부 정보기술 아키텍처, 2005, 10.

[3] William Tolong, Gail-Joon Ahn, Tanusree Pai, Seng-Phil Hong, "Access Control in Collaboration Systems", ACM Computing Surveys, Vol.37, No.1, pp.29-41, Mar. 2005.

[4] D.F. Ferraiolo, R. Sandhu, S. Gavrila, D.R. Kuhn, and R. Chandramouli, "Proposed NIST standard for role-based access control model", ACM Trans. Information and Systems Security, Vol.4, No.3, pp.224-274, Aug. 2001.

[5] R. Sandhu, "Future Direction of Role-Based Access Control Model", Springer LNCS 2052, pp22-26, Aug. 2001.

[6] Basit Shafiq, James B.D. Joshi, Elisa Bertino, Arif Ghafoor, "Secure Interoperation in a MultiDomain Environment Employing RBAC Policies", IEEE Transaction on Knowledge and Data Engineering, Vol.17, No.11, Nov. 2005.

[7] SHEN Haibo, HONG Fan, "A Context-Aware Role-Based Assess Control Model for Web Services", Proc. of IEEE International Conference on ICEBE'05, Mar. 2005.

[8] Roosdiana Wonohoesodo, Zahir Tari, "A Role-Based Access Control Model for Web Services", Proc. of IEEE International Conference on SCC'04, Apr. 2004.

[9] Hyung-Chan KIM, R.S. Rama Krishna, *and* Kouichi Sakurai, "A Collaborative Role-Based Access Control for Trusted Operating Systems in Distributed Environment", IEICE Transaction on Fundamentals, Vol.E88-A, No.1, Jan. 2005.

[10] Covinton, "Securing Context-Aware Applications Using Environment Roles", ACM SACMAT'01, May. 3-4, 2001.