RBAC 기반 워크플로우 보안 기술

원재강° 이선현 정관희 김광훈
경기대학교 일반대학원 전자계산학과
06240604@hanmail.net°, {twinfafa, khchung, kwang}@kyonggi.ac.kr

RBAC-Based Workflow Security Technology

Jae-Kang Won°, Sun-Hyun Lee, Kwan-Hee Chung, Kwang-Hoon Kim
Dept. of Computer Science, Kyonggi University

요 약

본 논문에서는 워크플로우 기술과 기업과 정부의 다양한 조직 체계를 반영하고 워크플로우의 현실적/효율적 운영관리 및 정보 보안을 위해 적합한 접근제어 모델인 역할기반 접근제어(RBAC : Role Based Access Control)를 이용한 워크플로우 보안 기술에 관하여 제안하였다. RBAC 기반 워크플로우 보안 기술은 워크플로우 시스템에 다양한 접근제어 서비스를 제공하기 위하여 서버/클라이언트 모델을 기반으로 하고 있으며, 이러한 워크플로우와 역할기반 접근제어 기술을 접목한 워크플로우 보안 기술은 기업 업무의 효율성을 증대시키고, 정보 보안 분야에 있어 정보 보안성 증대 및 정보보안정책을 구현하는데 유연성을 제공하는 새로운 기술로서의 역할을 수행한다.

1. 서 론

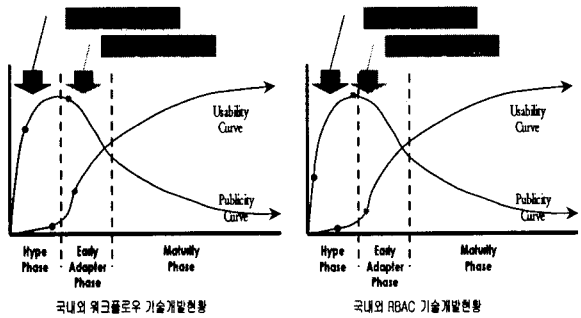
선진 외국에서의 역할기반 접근제어(RBAC : Role Based Access Control) 및 워크플로우 기술 개발은 대중적 인지도에서 최고의 단계이고 그의 적용 사례들도 초기 적용 단계를 지나 급속한 신장을 보이고 있다. 이에 대한 근거로 현재 선진 외국의 개발 중 또는 상용화된 워크플로우 관리 시스템은 300여 개에 달한다고 알려져 있다. 이러한 워크플로우는 전세계적으로도 성장 가능성이 매우 높은 시장을 형성할 것으로 예상되어지며, 선진 외국의 경우 상용화 제품들이 출시되어지고 있는 실정이다. 또한 개발 중 또는 상용화된 워크플로우에 접목할 수 있는 역할기반 접근제어 기술 역시 앞으로 매우 성장 가능성이 높은 시장을 형성할 것으로 예상되어지고 있다.

이에 본 논문에서는 워크플로우 기술과 기업과 정부의 다양한 조직 체계를 반영하는데 적합한 접근제어 모델인 역할기반 접근제어 기술을 접목한 RBAC 기반 워크플로우 보안 기술에 관하여 제안하고자 한다.

보안분야의 초기단계에서는 물리적 보안과 기술적 보안 기술이 연구 개발되었고, 관리적 보안 기술의 개발은 그 이후에 시작되었다. 관리적 차원의 보안 개념이 필요했던 이유는 1970년대에 들어서면서 컴퓨터 시스템이 다수의 사용자에게 다수의 응용(Application)을 제공하는 특성을 갖게 되면서 데이터 보안 문제에 대한 관심이 높아지고, 시스템 관리자와 소프트웨어 개발자들은 권한이 있는 사용자들에게만 특정 데이터 또는 자원들이 제공되는 것을 보장하기 위한 서로 다른 종류의 접근제어(Access Control)를 구현하기 위해 노력했다. 그에 따른 접근제어 기법들 중 하나가 바로 역할기반 접근제어(RBAC)라 할 수 있다.

이러한 워크플로우 기술과 역할기반 접근제어 기술의 접목은 기존의 임의적 접근제어(DAC)나 강제적 접근제어(MAC)보다 기업과 정부의 다양한 조직 체계를 반영하는데 보다 효율적인 방법일 뿐만 아니라, 정보 보안성 증대에도 효과적이라 할 수 있다.[1]

이에 따른 역할기반 접근제어(RBAC) 및 워크플로우 기술에 관한 국내• 외의 기술개발현황을 정리하면 다음과 같다.



<그림 1 국내• 외 워크플로우 및 RBAC 기술개발현황>

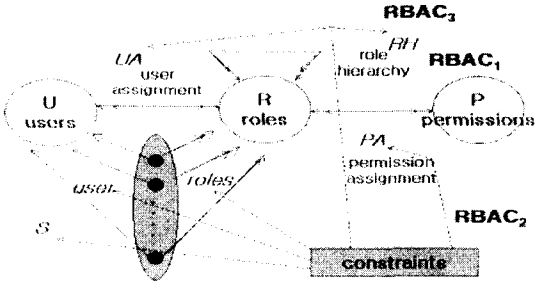
본 논문의 구성은 제 2절에서 RBAC의 기본 개념을 소개하며, 제 3절에서는 RBAC 기반 워크플로우 보안 기술에 관하여 설명한다. 마지막으로 제 4절에서는 결론 및 향후 발전 방향에 관하여 기술한다.

2. RBAC(Role based Access Control)

국외에서의 역할기반 접근제어(RBAC)는 대단위 네트워크의 복잡성과 보안 관리 비용을 줄이는 대안으로 매우 주목 받고 있다.

역할기반 접근제어에서는 조직의 구조와 연동하여 직책에 따라 보안 등급을 부여하며, 개별 사용자가 특정 직책을 부여 받으면 그에 상응하는 권한을 획득한다. 그러므로 역할기반 접근제어 시스템에서의 보안관리는 각 직책에 해당하는 권한을 결정하여 두고, 각 사용자에게는 직책만을 배정하면 된다. 즉, 한 사용자가 여러 직책을 부여받거나 직책간의 계층구조 등으로 발생하는 복잡성은 역할기반 접근제어 시스템에서 관리하므로 보안관리가 쉬워지게 된다. 이와 같은 이유로 국외에서는 역할기반 접근제어 기술이 다양한 분야에서 활용되어지고 있으며, 상용화된 제품 역시 상당 수가 출시되어졌다. 그러나, 역할기반 접근제어 기술과 접목되어진 워크플로우 시스템의 개발은 국내에서는 아직 초기 단계이며, 상용화된 제품 사례 역시 보고되어지고 있지 않다.

역할기반 접근제어 기본 모델은 다음과 같다.



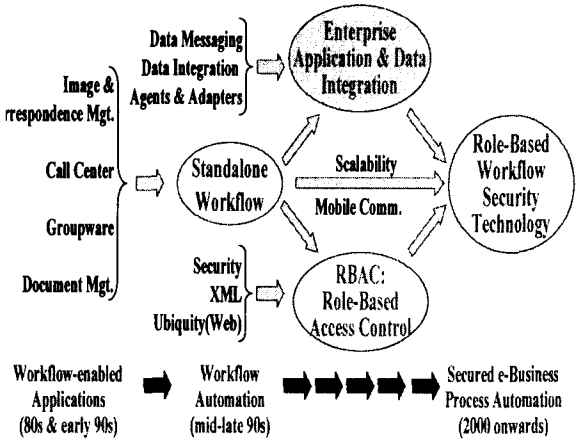
<그림 2 RBAC 기본 모델>

역할기반 접근제어 기본 모델은 컴퓨터 시스템을 통하여 시스템 내의 정보를 사용하는 객체로서의 사용자(U : User)와 시스템의 하나 또는 그 이상의 객체에 대한 특정 접근모드(예 : read, write, update)의 승인을 나타내는 역할(R : Role) 그리고, 사용자 배정(UA : User Assignment)과 인가 권한(P : Permission), 세션(S : Session)으로 구성되어질 수 있다.[1, 2, 3]

역할기반 접근제어의 중심적인 개념은 사용자가 기업이나 조직의 정보자원을 임의로 접근할 수 없도록 하는 것이다. 대신에 접근 권한이 역할에 부여되고 사용자는 적절한 역할에 소속됨으로써 역할의 수행에 필요한 최소 자원만을 접근할 수 있도록 하는 것이다. 이러한 역할기반 접근제어에 관한 기술은 기존의 워크플로우 시스템 차원에서의 관리 형태를 탈피하여 정보 보안에 있어 새로운 대안으로 주목 받고 있다. 또한, 기업 및 부서 차원의 권한 관리를 매우 단순화 시켜주고 기업의 특정한 보안 정책을 구현하는데 있어서 유연성을 제공하며, 사용자는 그들의 업무적 권한과 책임에 따라 특정 역할의 구성원이 되어 접근 구조의 변경 없이도 역할의 변경을 쉽게 할 수 있다는 장점을 가지고 있다.

3. RBAC 기반 워크플로우 보안 기술

컴퓨터 기술과 전자통신 기술의 급진적인 발전 및 인터넷의 보급, 확산은 기업과 조직체 내에서의 효율적인 상호 작용 지원 수단 및 방법을 탄생시켰다. 이러한 발전은 그룹웨어를 거쳐 워크플로우에 이르기까지 급격한 변화를 거치며 성장해 왔으나, 이에 따른 새로운 문제점인 정보 보안이 부각되어진 사실도 간과되어질 수 없는 부분일 것이다. 이에 역할기반 접근제어 기술을 이용한 워크플로우 보안 기술은 미래지향적인 새로운 기술로서 위치를 선점하게 될 것이다. 이러한 역할기반 접근제어 및 워크플로우의 발전 방향을 살펴보면 다음과 같다.

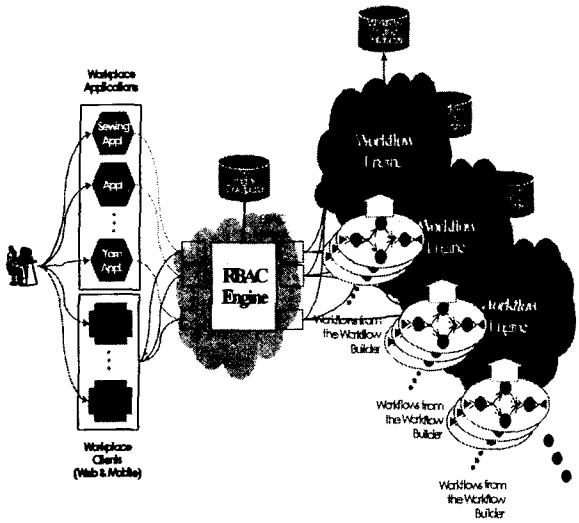


<그림 3 역할기반 접근제어 및 워크플로우 발전 방향>

기존의 워크플로우 시스템은 B2C와 B2B로 구성되는 기업의 사무업무 프로세스들을 모델링하며, 이의 구문적 또는 의미적 오류를 처리하고 분석하는 워크플로우 정의 도구를 설계 및 구현함으로써 기업의 업무 효율을 증대시키는 부분에만 편중 되어있는 것이 사실이다. 그러나, 현실은 업무의 효율적 운영 관리뿐만 아니라 정보 보안이라는 부분이 강조 되어지고 있다. 이에 기존의 관리자/일반 사용자 시스템으로는 회사 조직의 정보 제한을 기할 수 없게 되었다. 그래서 각 회사마다 별도의 인증 방법과 솔루션의 개발로 막대한 비용을 지불하고 있는 것이 현실이다. 이에 역할기반 접근제어 기술을 이용한 워크플로우 시스템을 기반으로 이러한 문제점을 해결하고자 한다.

역할기반 접근제어를 기반으로 하는 워크플로우 시스템은 역할기반 접근제어 서버 및 클라이언트를 바탕으로 정보 보안 및 멀티 인증 처리, 클라이언트 자료의 암호화 등으로 정보의 유출을 사전에 차단할 수 있으며, 권한 관리를 단순화 시켜준다. 또한 사용자의 작업 시간을 실시간으로 검사하여 그 권한을 박탈하거나 강제 퇴장 시킬 수 있는 접근 및 작업 시간 제어가 가능하며 중앙관리 시스템을 이용한 다른 웹 시스템에서의 접근이 가능하여 분산관리가 불필요하다. 이러한 중앙관리 시스템은 관리비 및 인건비를 감소시킬 것이며, 기술적인 문제점을 신속히 처리할 수 있다.

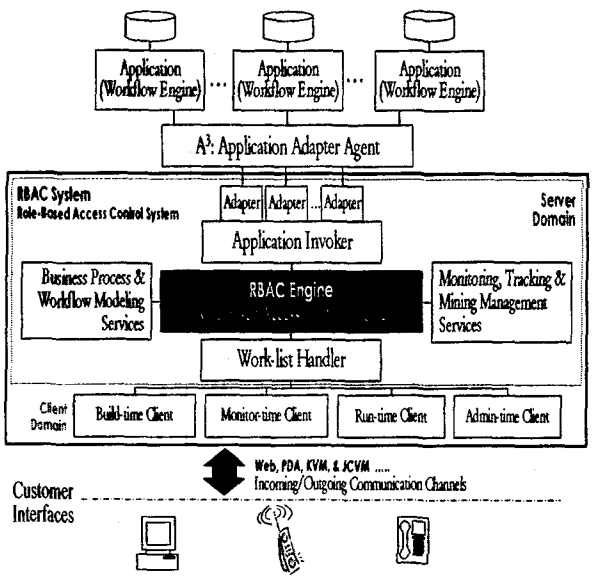
역할기반 접근제어 기술을 이용한 워크플로우 보안 기술에 관한 기본 구조는 다음과 같다.



<그림 4 BRAC 기반 워크플로우 보안 기술 기본 구조>

역할기반 접근제어 기술을 이용한 워크플로우 보안 기술은 역할기반 접근제어 서버/클라이언트 모델을 기반으로 워크플로우 시스템 차원에서의 관리를 탈피하여 다양한 접근제어 서비스를 제공할 수 있으며, 웹 기반의 클라이언트를 통해 사용자 인터페이스의 접근을 용이하게 할 수 있다.

이에 따른 역할기반 접근제어 시스템의 구조는 다음과 같다.



<그림 5 역할기반 접근제어 시스템 구조>

역할기반 접근제어 기술을 이용한 워크플로우 보안 기술의 기능은 다음과 같다.

- 정보 보안
- 인증 데이터의 암호화
- 멀티 인증 처리
- 접근 및 작업 시간 제어 기능
- 중앙관리 시스템
- 자체 DB 시스템으로 추가적 소프트웨어 설치 불필요
- 자체 웹 서버로 추가적인 소프트웨어 설치 불필요

4. 결 론

본 논문은 기존의 워크플로우 시스템에서의 업무 처리 효율성 및 정보 보안성을 향상시키기 위한 RBAC 기반 워크플로우 보안 기술에 관하여 기술하였다. 이러한 기술은 역할기반 접근제어 서버/클라이언트 모델을 기반으로 하고 있으며, 기존의 워크플로우 시스템뿐만 아니라 기업의 업무 처리 효율성 관리 및 처리, 제어에 필요한 관리적 워크플로우 시스템, 그리고 문서 중심의 간단한 작업이나 결재 처리, 자동 문서 전달 및 분배와 같은 비정형 워크플로우 시스템 등에 활용되어질 것이라 기대 되어진다. 또한, 현재는 기업 및 부서 단위의 비즈니스 프로세스에 주로 적용되어지는 워크플로우 시스템에서 탈피하여, 기업 또는 부서 간의 상호 협조 및 협업 작업을 필요로 하는 워크플로우 시스템으로 그 적용이 확대되어질 것이라 예상된다.

5. 참고 문헌

[1] 박석, 오세종, " Web 환경에서의 역할기반 접근제어(RBAC)의 적용에 대한 연구" , 데이터베이스 연구회지 제16권 제1호, 8. 2000

[2] David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, " A Proposed Standard for Role-Based Access Control" , D. Richard Kuhn and Ramaswamy Chandramouli National Institute of Standards and Technology, December 18. 2000

[3] K. Gutzman, " Role-based Access Control in the HTTP Environment with LDAP" , IEEE Internet Computing, May 1998

[4] Kwang-Hoon Kim, Clarence A. Ellis, " A Framework for Workflow Architectures" , University of Colorado/Department of Computer Science, Technical Reports, CU-CS-847-97, December 1997

[5] Barkley, Kuhn, Rosenthal, Skill, " Role-Based Access Control for the Web" , CALS Expo International & 21st Century Commerce, Global Business Solutions for the New Millennium, 1998