

역할 기반 워크플로우 조직 관리 시스템 설계

김태욱[○] 박민재 원재강 김광훈
 경기대학교 전자계산학과

twkim@kyonggi.ac.kr, mjpark@kyonggi.ac.kr, wonjk@kyonggi.ac.kr, kwang@kyonggi.ac.kr

Role based Workflow Organization Management System Architecture

Taewook Kim[○] Minjae Park Jaekang Won Kwanghoon Kim
 Computer Science, Kyonggi University

요 약

본 논문에서는 기업과 정부의 다양한 조직체계를 반영하고 워크플로우의 현실적/효율적 운영관리 및 여러 복잡한 직책에 의해 발생하는 복잡성 해결을 위해 적합한 접근제어 모델인 역할기반 접근제어(RBAC : Role Based Access Control)를 이용한 워크플로우 조직 관리 시스템에 관하여 기술하고 설계한다. 역할 기반 워크플로우 조직 관리 시스템은 앞으로 매우 성장 가능성이 높은 시장을 형성할 것으로 예상되며 다양한 조직체계를 반영하는 데 적합한 접근제어 모델이다. 현재 기업, 정부, 공공기관 등의 서로 다른 조직체계에 워크플로우를 적용하게 되는 경우 조직관리 시스템은 워크플로우 시스템에 있어서 필수 컴포넌트로 자리 잡고 있지만 기존 조직관리 시스템들은 보안문제나 동적인 조직의 관리에 문제점을 갖고 있는 것이 사실이다 따라서 본 논문에서는 “역할 기반 접근 제어”라고 하는 RBAC(Role-Based Access Control)의 기본 개념과 워크플로우 엔진과 역할기반의 워크플로우 조직관리 시스템간의 관계에 따른 역할기반 워크플로우 조직 관리 시스템을 제안, 설계한다.

1. 서 론

역할기반 접근제어(RBAC : Role Based Access Control) 및 워크플로우 기술 개발은 대중적 인지도에서 최고의 단계이고 그 외 적용사례들도 초기 적용단계를 지나 급속한 성장을 보이고 있다. 이에 대한 근거로 현재 선진 외국의 개발 중 또는 상용화된 워크플로우 관리 시스템은 300여 개에 달한다고 알려져 있다. 이런 워크플로우 관리 시스템은 전 세계적으로도 성장 가능성이 매우 높은 시장을 형성할 것으로 예상되며, 선진 외국의 경우 상용화 제품들이 출시되고 있는 실정이다. 또한 개발 중 또는 상용화된 워크플로우 관리 시스템에 접목할 수 있는 역할기반 접근제어 기술 역시 앞으로 매우 성장 가능성이 높은 시장을 형성할 것으로 예상되고 있다.

2. RBAC(Role Based Access Control)

국외에서의 역할기반 접근제어(RBAC)는 대단위 네트워크의 복잡성과 보안관리 비용을 줄이는 대안으로 매우 주목받고 있다. 역할기반 접근제어에서는 조직의 구조와 연동하여 직책에 따라 보안등급을 부여하며, 개별사용자가 특정 직책을 부여받으면 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 관리가 쉬워지게 된다. 이와 같은 이유로 국외에서는 역할기반 접근제어 기술이 다양한 분야에서 활용되고 있으

며, 상용화된 제품 역시 상당수가 출시되었다. 그러나, 역할기반 접근제어 기술과 접목된 워크플로우 시스템의 개발은 국내에서는 아직 초기 단계이며, 상용화된 제품 사례 역시 보고되고 있지 않다.

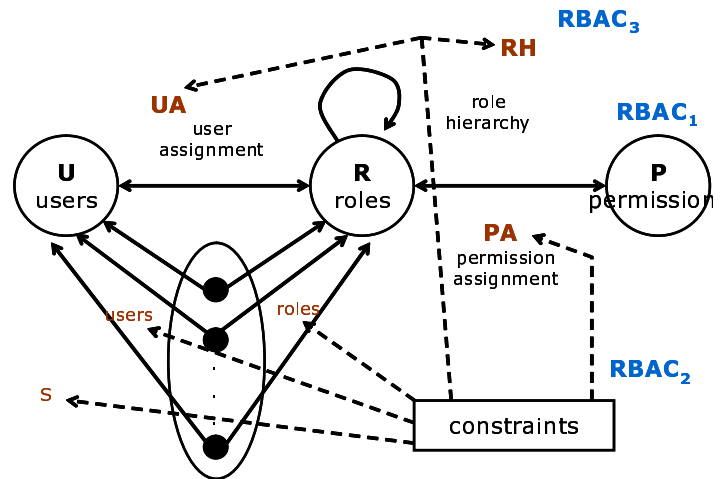


그림 1. RBAC 기본모델

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 구성되어 질 수 있다.[1, 2] 역할기반 접근제어의 중심적인 개념은 사용자가 기업이나 조직의 정

보자원을 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 차원에서 관리 형태를 탈피하여 정보 보안에 있어 새로운 대안으로 주목 받고 있다. 또한 기업 및 부서 차원의 권한 관리를 매우 단순화 시켜주고 기업의 특정한 보안정책을 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

최근 IT기술의 발전에 따라 기존 그룹웨어, 전자결재, 문서관리시스템 등과 같은 데이터 처리중심의 시스템이 업무 프로세스를 지원하는 워크플로우 시스템으로 변해가고 있다. 워크플로우 시스템은 그룹웨어에서부터 급격한 변화를 거치며 성장해 왔으나, 이에 따른 새로운 문제점인 정보 보안이 부각되어진 사실도 간과되어질 수 없는 부분일 것이다. 역할기반 접근제어 기술을 이용한 워크플로우 보안기술은 미래 지향적인 새로운 기술로서 위치를 선점하게 될 것이다. 이러한 역할기반 접근제어 및 워크플로우의 발전방향을 살펴보면 다음과 같다.

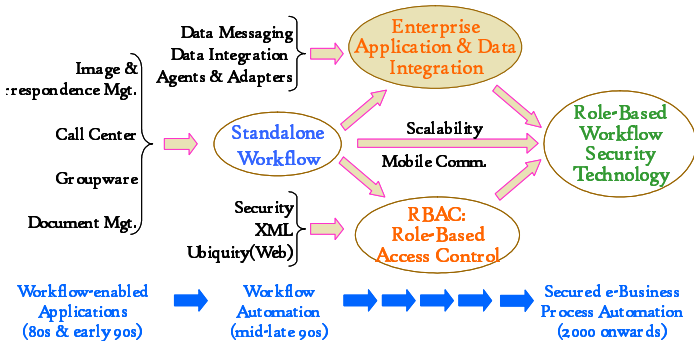


그림 2. 워크플로우의 발전 추세

기존의 워크플로우 시스템은 기업의 사무업무 프로세스들을 모델링하며, 이의 구문적 또는 의미적 오류를 처리하고 분석하는 워크플로우 정의 도구를 설계 및 구현함으로써 기업의 업무 효율을 증대시키는 부분에만 편중되어 있는 것이 사실이다. 그러나, 현실은 업무의 효율적 운영 관리뿐만 아니라 정보 보안이라는 부분이 강조되고 있다. 또한 사회가 분화, 전문화되면서 사회 조직이 증가하여 대규모 조직을 합리적으로 관리해야 할 필요성이 대두되고 있다. 이에 기존의 관리자/일반 사용자 시스템으로는 회사 조직의 정보 제한 및 효율적 조직 관리를 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 워크

플로우 시스템은 역할기반 접근제어 서버 및 클라이언트를 바탕으로 정보 보안 및 멀티 인증 처리, 클라이언트 자료의 암호화 등으로 정보의 유출을 사전에 차단할 수 있으며, 권한관리를 단순화 시켜준다. 또한 사용자의 작업 시간을 실시간으로 검사하여 그 권한을 박탈하거나 강제 퇴장시킬 수 있는 접근 및 작업시간 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. 사용자들은 클라이언트를 통해 엔진에 접근하기 전에 RBAC엔진에 접근하여 역할에 따른 행동 권한을 할당받게 되며 그 권한에 따라 업무를 수행하게 된다. 역할기반 접근제어기술을 이용한 워크플로우 보안기술에 관한 기본구조는 다음과 같다.[3]

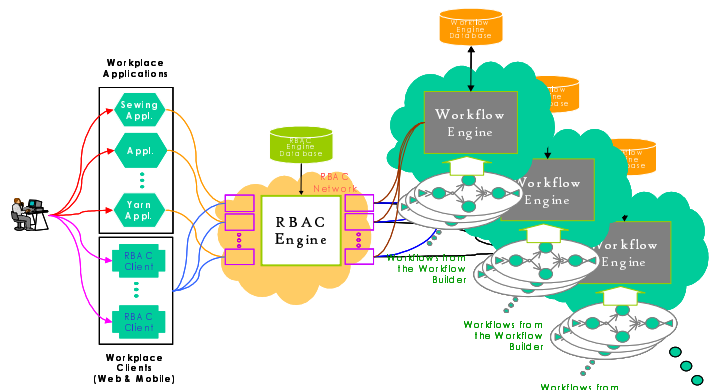


그림 3. RBAC 기반 워크플로우 보안 기술

4. 역할기반 워크플로우 조직 관리 시스템

4.1 역할기반 워크플로우 조직 관리 시스템 개요

역할기반 워크플로우 조직 관리 시스템은 동적으로 워크플로우 시스템 및 서브시스템으로 접근하는 역할기반 보안 메커니즘을 적용하여 워크플로우 통합 환경의 사용자 및 시스템을 관리한다. 사용을 희망하는 워크플로우 시스템 관리자와 워크플로우 시스템 사용자를 구분하여 등록 한 후 워크플로우 조직 관리 시스템의 사용 접근 권한을 부여하고, 사용자 정보를 등록 관리한다. 조직 관리 시스템의 모듈은 크게 관리자 모듈과 사용자 웹서비스로 분류한다. 플랫폼의 시스템관리자는 역할기반 워크플로우 조직 관리 시스템 서버의 관리자 모듈에서 사용자 역할에 맞게 권한이 부여된 역할과 권한 및 이용할 수 있는 메뉴를 등록, 수정, 삭제를 할 수 있는 시스템 관리 기능을 담당한다. 워크플로우 조직 관리 시스템 통합 플랫폼의 계정관리자는 워크플로우 시스템 관리자의 계정의 발급을 승인하고 역할을 부여하며, 조직의 정보를 추가, 수정 및 삭제하는 일을 담당한다. 워크플로우 조직 관리 시스템 관리자는 자신의 시스템을 사용하고자 하는 사용자를 관리하고 권한을 부여한다. 웹서비스 모듈은 새로운 사용자의 등록 모듈과 기타 확장 가능한 서브 시스템에 접근할 수 있는 메뉴를 제공하여 워크플로우 엔진에 전반적인 서비스를 제공한다.

4.2 RBAC기반 인증 시스템 기능

RBAC기반 인증 시스템은 기본적으로 SOAP(Simple Object Access Protocol)을 통신 프로토콜로 이용한다. SOAP은 전자적 커뮤니케이션의 기본 프로토콜로서 XML로 작성된 간단한 요청과 응답 메시지들을 위한 모델이다. SOAP은 어떠한 전송 프로토콜과도 함께 사용될 수 있으며, SOAP 메시지는 플랫폼-중립적인 리모트 프로시저 호출 메커니즘으로 모델링되기도 하며, 어떤 형태의 XML정보를 교환하는데도 사용될 수 있다. SOAP은 어떻게 XML 데이터가 모든 플랫폼 상의 미들웨어와 하드웨어에 의해, 그리고 모든 프로그래밍 랭귀지로, 모든 네트워크 프로토콜을 통해, 모든 오브젝트 모델을 기반으로 지원될 수 있는 표준 메커니즘을 이용하여 교환될 수 있는지 알려준다. 또한, SOAP은 어떠한 프로토콜과도 사용이 가능하여, 모든 형태의 시스템에서의 통합을 이룰 수 있도록 한다. 따라서, 클라이언트와 사용자, 역할, 권한 관리를 하여 RBAC기반 인증 시스템을 통해 인증을 받은 후, 워크플로우 시스템과 통신을 하여 작업을 처리한다. 이때 RBAC기반 인증 시스템은 다음 몇 가지 보안 서비스를 제공한다.

- 인증(Authentication) 서비스 : 인증은 상대방의 신분과 자격 여부를 확인하는 것으로, 상대방 혹은 상대방의 컴퓨터와 최초 연결이 이루어질 때 필요한 서비스
- 접속제어(Access Control) 서비스 : 접속제어는 시스템에 들어온 사용자가 정보를 취득하고자 할 때 사용할 수 있는 권한이 있는지 여부를 판단할 때 필요한 서비스
- 부인방지(Non-Repudiation) 서비스 : 자료를 송수신하는데 있어서 사용자가 자신의 행위 사실을 부인할 수 없도록 해야 할 때 필요한 서비스

또한, RBAC 기반 인증서비스는 다음과 같은 접근제어 모델을 설계할 수 있도록 한다. 역할기반 접근제어 인증 시스템은 user, role, permission 객체로 구성되며, 한명의 user에 여러 role이 할당되고, 하나의 role에 여러 permission이 할당된다. 서비스 정보는 서비스 관리자에게 서비스 내의 모든 객체들의 존재시간을 관리 할 수 있는 권한을 부여할 수 있다. 사용자에게는 자신의 업무에 해당하는 역할이 할당되고 역할에 접근권한이 할당된 경우에만 사용자가 특정한 모드로 서비스에 접근할 수 있다. 접근권한이 역할에 부여되므로 시스템이 변경될 때 필요에 따라 쉽게 새로운 접근 권한을 역할에 부여하거나 삭제할 수 있고 서비스 조직의 요구에 따른 접근제어 정책의 관리가 용이하다. 역할기반 접근 통제 정책은 자율적이 아니며, 역할 기반 접근 통제 정책은 사용자-역할, 역할-허가에 대한 관계로 설정된다. 역할기반 접근 인증 시스템은 다음의 RBAC특징이 모두 만족되도록 설계되어야 한다.

- Authorization management : 사용자의 권한 지정을 두 부분으로 나누기 때문에(사용자-역할부여, 역할-권한 허가) 논리적으로 독립적이어서 보완 관리가 용이하다.
- Hierarchical roles : 역할에 대한 계층을 주어 권한 상

속이 가능하다.

- Least Privilege : 사용자에게 최소한의 권한만을 허용함으로써 권한의 남용을 방지한다.
- Separation of Duty : 시스템 상에서 필요 이상의 특권이 사용된 사용자를 배제할 수 있다.
- Object class : 수행하는 활동에 따라 사용자를 분류하는 것이 가능하다.

4.3 역할기반 워크플로우 조직관리 시스템 설계

다음은 본 시스템이 제공하는 주요 서비스 중 하나인 접근제어 유즈케이스이다. 기본적인 행위인 접근제어 행위로서 사용자의 관련된 역할과 권한을 관리하며, 그에 따라 이용 가능한 서비스를 제어한다.

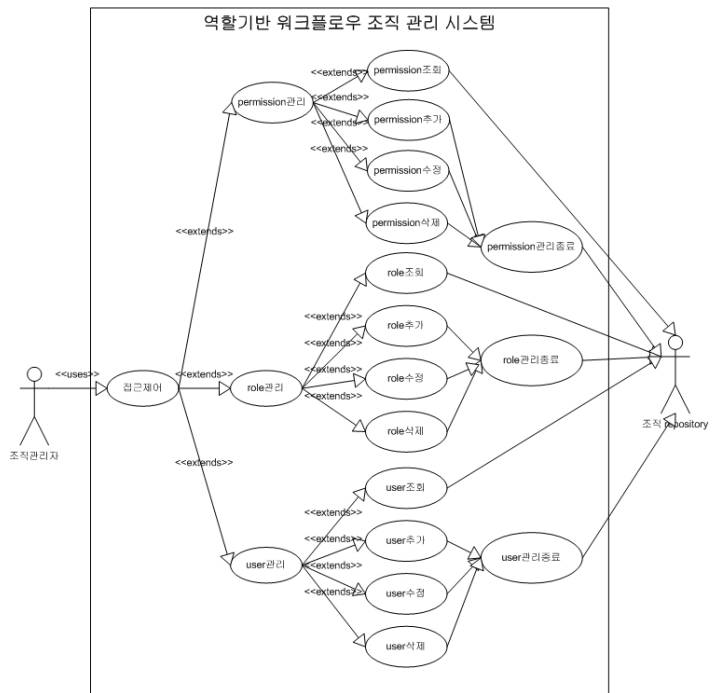


그림 4. 접근제어 유즈케이스

그림 5는 경기대학교 워크플로우 연구실에서 개발한 워크플로우 엔진의 구조이다. 기존 워크플로우 엔진에서는 조직 구조와 엔진의 의존성이 높아 조직이 변경되는 경우 조직 구조는 물론이고 엔진까지 조직 구조에 맞추어 변경하는 경우가 생기는 등 의존성 문제가 심각하게 대두되고 있는 상태이다.

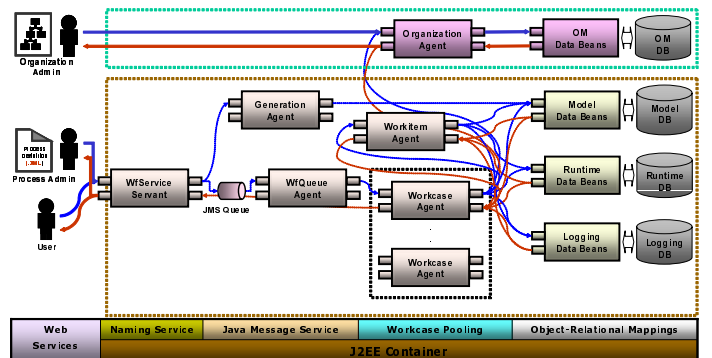


그림 5. 기존의 워크플로우 엔진 구조

다음은 본 시스템을 구성하고 있는 주요 구성요소와 XPDL2.0기반의 워크플로우 엔진과의 상호 작용을 나타내는 역할기반 워크플로우 조직관리 시스템의 설계 그림이다. 이 경우 조직 구조와 엔진의 의존성을 낮춰 조직 구조에서 제공하는 서비스만 일치를 시킨다면 조직 구조의 변경에 영향을 받지 않고 사용자 또한 조직 구조와는 상관없이 런타임 클라이언트를 통해 자신의 권한에 따른 업무만을 처리 하게 되므로 훨씬 더 효율적인 조직 관리 구조를 갖게 되는 것이다. 또한 역할기반의 워크플로우 조직 관리 시스템은 경량의 Spring Framework와 Hibernate를 사용하는 구조를 선택하여 설계하였다.

본 개념과 워크플로우 엔진과 역할기반의 워크플로우 조직관리 시스템간의 관계에 대해 알아보고 시스템을 제안, 설계하였다. 이러한 역할기반 워크플로우 조직관리 시스템은 기존의 워크플로우 시스템뿐만 아니라 기업의 업무 처리에 대한 효율적 관리 및 처리, 제어에 필요한 관리적 워크플로우 시스템, 그리고 문서 중심의 간단한 작업이나 결재 처리, 자동문서 전달 및 분배와 같은 비정형 워크플로우 시스템 등에 활용 되어질 것이라 기대되며, 현재는 기업 및 부서단위의 비즈니스 프로세스에 주로 적용 되어지는 워크플로우 조직 관리 시스템에서 탈피하여, 기업 또는 부서 간의 상호 협조 및 협업 작업을 필요로 하는 워크플로우 시스템으로 그 적용이 확대 되어질 것이라 예상된다.

6. 참고문헌

1. 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.
2. 박석, 오세종 "Web 환경에서의 역할기반 접근제어 (RBAC)의 적용에 관한 연구", 데이터베이스 연구회지 제16권 제1호, 8. 2000
3. 원재강, 이선현, 정관희, 김광훈, "RBAC 기반 워크플로우 보안 기술", 한국정보과학회 춘계학술발표논문집(A), 30권 1호 4. 2003
4. Craig Walls, Ryan Breidenbach, "Spring In Action", Independent Pub Group, 2004.
5. Christian Bauer, "Hibernate In Action", MANNING, 2004.

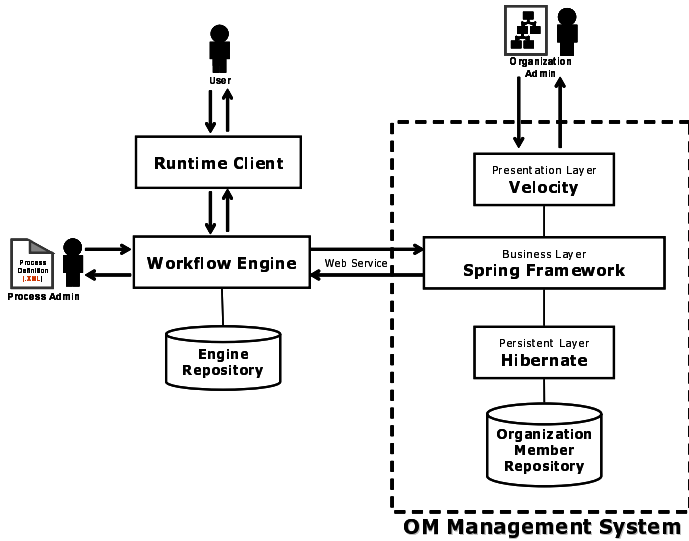


그림 6. XPDL 2.0엔진과 조직관리 시스템의 상호작용

SpringFramework와 Hibernate를 사용함으로써 어떠한 데이터 접근방식과 트랜잭션 기술을 사용한 방식에서도 명확한 어플리케이션 계층화와 어플리케이션 객체들 간의 약한 결합을 가능하게 한다. 이는 더 이상 비즈니스 객체는 데이터 접근 혹은 트랜잭션 방식에 의존적이지 않을 것이고, 하드 코딩된 리소스 검색이 없으며, 싱글톤 클래스를 재설정하는 어려움과 임의의 서비스 등록이 없게 되는 것을 말하며 이는 변화하는 조직 구조에 대해 조금 더 빠르고 신속하게 대응할 수 있다는 장점을 가지고 있다. 또한 어플리케이션 객체들을 묶고 그것들을 재사용가능하고 가능한 한 컨테이너 의존성으로부터 자유롭게 유지해주는 단 하나의 간단하고 일관된 접근방식을 제공해준다[4, 5]

5. 결론

워크플로우 시스템이 점차 발전해 나감에 따라 대단위의 워크플로우 시스템의 사용자가 발생하였고 워크플로우 시스템 사용자의 현실적, 효율적 운영관리 및 정보보안을 위하여 역할기반 접근제어를 이용하게 되었다. 기업, 정부, 공공기관 등의 서로 다른 조직체계에 워크플로우를 적용하게 되는 경우 조직관리 시스템은 워크플로우 시스템에 없어서는 안 될 필수 컴포넌트로 자리 잡았다. 하지만 기존 조직관리 시스템들의 보안문제나 동적인 조직의 관리를 위해서 본 논문에서는 "역할 기반 접근 제어"라고 하는 RBAC(Role-Based Access Control)의 기