RBAC 기반 워크플로우 보안 기술

원 재 강* 김 광 훈** 정 관 희***

목 차

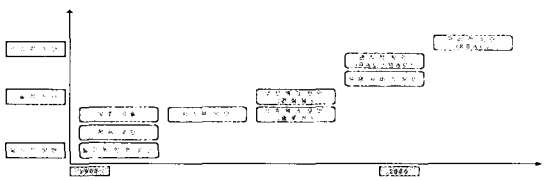
1. 서 론
2. 디지털 보안
3. 디지털 보안 기술 요소
4. 디지털 보안 기술
5. 최근 기술 동향
6. 결 론

1. 서 론

최근의 워크플로우(Workflow) 기술과 역할기반 접근제어(RBAC : Role Based Access Control) 기술은 국내외적인 기술개발 및 그의 채택현황에 있어 급속히 발전하고 있는 분야임에 틀림없다. 그러나 선진 외국에서의 역할기반 접근제어(RBAC) 및 워크플로우 기술 개발은 대중적 인지도에서 최고의 단계이며, 그의 적용 사례들도 초기 적용 단계를 지나 급속한 신장을 보이고 있는 것이 사실이다. 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 예상 되어지고 있다. 이에 반해 국내의 워크플로우 기술과 역할기반 접근제어(RBAC) 기술은 새로운 기술의 첫 단계인 연구 및 광고 단계에 있어 워크플로우 기술의 대중적 인지도 측면뿐만 아니라, 그에 접목되어진 역할기반 접근제어 기술 역시 매우 초보적인 상황이라 할 수 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.

보안 분야의 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.



(그림 1) 정보보안분야의 발전 추세

* 경기대학교 전자계산공학과 박사과정
** 경기대학교 정보과학부 조교수
*** 경기대학교 정보과학부 정교수

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.

정보보안분야의 발전 추세를 살펴보면 그림 1과 같다.

이러한 정보보안분야의 발전 추세를 바탕으로 차세대 기술로 제시되고 있는 워크플로우 기술과역할기반 접근제어(RBAC) 기술을 접목한 RBAC 기반 워크플로우 보안 기술을 제안함으로서 국내의 워크플로우 기술 자립을 도모하고 역할기반 접근제어(RBAC) 기술의 기반기술을 확보하고자 한다.

본 논문에서는 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.

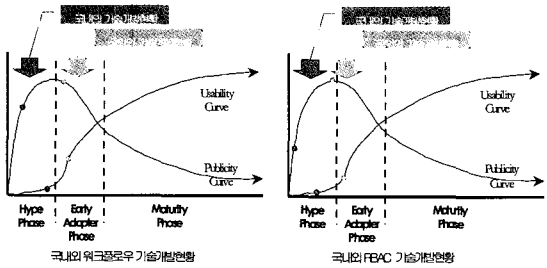
2. 역할기반접근제어(RBAC)

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 부여 받거나 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 접목 되어진 워크플로우 시스템의 개발은 국내에서는 아직 초기 단계이며, 상용화된 제품 사례 역시 보고되어지고 있지 않다.

이에 따른 국내외의 워크플로우 기술개발현황과 RBAC 기술개발현황을 살펴보면 그림 2와 같다..

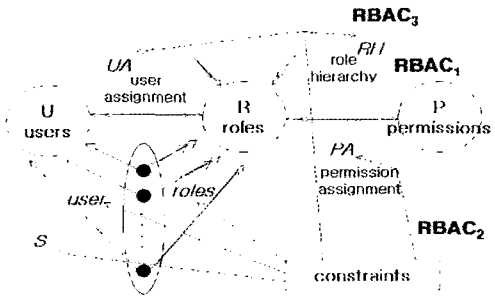
역할기반 접근제어의 중심적인 개념은 사용자가 기업이나 조직의 정보자원을 임의로 접근할 수 없도록 하는 것이다. 대신에 접근 권한이 역할에 부여되고 사용자는 적절한 역할에 소속됨으로써 역할의 수행에 필요한 최소 자원만을 접근할 수 있도록 하는 것이다.



(그림 2) 국내외의 기술개발현황

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 특정한보안 정책을 구현하는데 있어서 유연성을 제공하며, 사용자는 그들의 업무적 권한과 책임에 따라 특정 역할의 구성원이 되어 접근 구조의 변경 없이도 역할의변경을 쉽게 할 수 있다는 장점을 가지고 있다.

역할기반 접근제어 기본 모델은 다음과 같다.



(그림 3) 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 특정접근모드(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.

2.1 역할기반접근제어표준

역할기반 접근제어 기술에 관한 표준화 작업은 NIST(National Institute Standards and Technology)에서 담당하고 있으며, 제정 되어있는 역할기반 접근제어 표준의 구성을 보면 역할기반 접근제어 참조 모델과 요구사항의 명세라는 두 부분으로 구성 되어있다. 외부 연구소와 ACM 공동 연구회를 통한 NIST에서의 표준 제정은 이러한 사항을 충족시키기 위해 역할기반 접근제어 표준을 네 가지의 기본 모델로 제시하고 있으며, 그에 대한 구분은 살펴보면 다음과 같다.

Core RBAC
Hierarchical RBAC
- Limited Hierarchies
- General Hierarchies

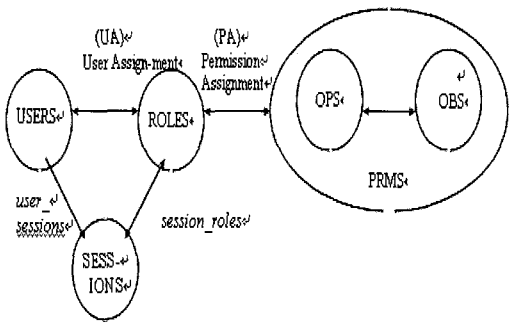
Static Separation of Duty Relations
- Without Hierarchies
- With Hierarchies

Dynamic Separation of Duty Relations

2.2CoreRBAC

Core RBAC 모델은 역할기반 접근제어 모델을 구성하기 위한 가장 기본이 되는 모델로서 역할기반 접근제어 모델을 구성하기 위한 필수적인 구성 요소들과 그들 간의 관계를 정의하고 있다.

기본적인 구성 요소들과 그에 따른 관계에 대해 간략히 요약하면 다음과 같다.



(그림 4) Core RBAC

• 사용자(user)와 역할(role) : 사용자는 컴퓨터 시스템을 통하여 시스템 내의 정보를 사용하는 객체로서 한 사용자는 한 명의 사람에 대응된다. 역할은 접근제어 정책을 구현하는 중요한 의미적 구조이다. RBAC 시스템에서는 시스템 관리자가 회사나 조직의 업무 기능에 따라 역할을 생성하고 역할에 권한을 부여한다. 역할 계층(RH : role hierarchy)은 관련성이 있는 역할들 간의 부분순서(partial order) 관계로서 정의되며 기업의 권한과 책임의 체계와 매우 유사하여 기업의 권한체계를 모델링 하는데 매우 적합하다.

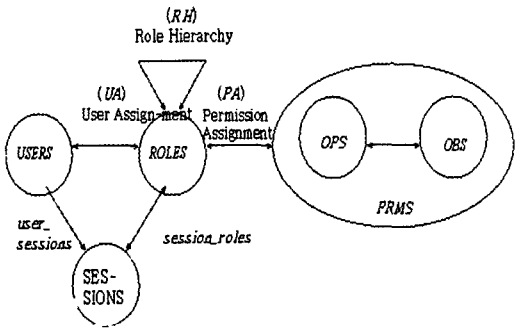
• 인가권한(permission) : 인가권한은 시스템의 하나 또는 그 이상의 객체에 대한 특정 접근 모드(예 : read, write, update)의 승인을 나타낸다. RBAC에서의 인가권한(permission)은 권한허가(authorization), 접근권리(access right), 권한(privilege)과 같은 의미를 갖는다. 여기서 객체는 기업 또는 조직 내의 정보시스템을 구성하고 있는 자료(data)나 시스템 자원(system resource)을 말한다. 인가권한은 네트워크 수준으로부터 특정 레코드의 특정 필드에 대한 접근 단위에 이르기까지 다양한 레벨, 다양한 범주로 주어질 수 있다.

• 세션(session) : 사용자는 시스템에 로그인 등을 통해 그들이 가진 역할의 부분집합을 활성화할 때 세션을 형성한다. 각 세션은 하나의 사용자와 여러 개의 권한을 매핑한다. 이중 화살표는 다중 역할이 동시에 활성화한다는 것을 말한다.

• 사용자 배정(user assignment)과 인가권한 배정(permission assignment) : 사용자 배정과 인가권한 배정은 다대다 관계이며 RBAC 모델에서 매우 중요한 구성요소이다. RBAC의 특징 중의 하나는 사용자가 정보 객체들에 대해서 실행할 수 있는 연산들을 직접 사용자에게 부여하는 대신 조직의 업무 수행에 필요한 역할에 배정하고(인가권한 배정), 사용자는 해당 역할의 구성원이 됨으로써(사용자 배정) 정보 객체에 대해 지원하는 연산을 수행하도록 하는 것이다. 이러한 방법은 사용자와 정보 객체수가 많은 일반 기업 환경에서 권한의 관리를 매우 용이하게 수행할 수 있는 장점을 제공한다.

2.3HierarchicalRBAC

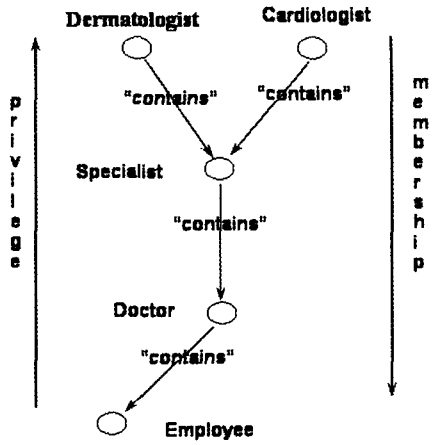
Hierarchical RBAC 모델은 역할기반 접근제어 모델 내에서의 역할에 관한 상속 관계에 초점을 맞추고 있다. 이러한Hierarchical RBAC 모델은 조직은 구조와 기능적 구조를 반영하는데 적합한 모델이며, 일반적으로 Limited Hierarchies 모델과 General Hierarchies 모델과 구분할 수 있다.



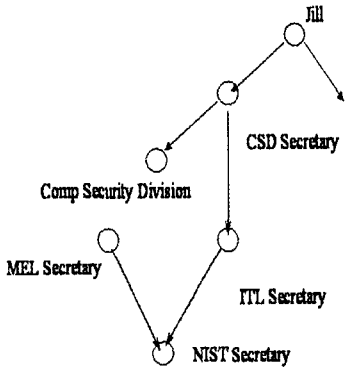
(그림 5) Hierarchical RBAC

Limited Hierarchies 모델의 구성과 General Hierarchies 모델의 구성은 다음과같이 표현되어질 수 있다.

이러한 Limited Hierarchies 모델과General Hierarchies 모델을 구성함으로써 사용자들을 다양하게 표현할 수 있으며, 또한 사용자들은 둘 또는 그 이상의 종속 되어진 역할을 부여 받을 수 있는 장점을 가지고 있다.



(그림 6) Limited Hierarchies



(그림 7) General Hierarchies

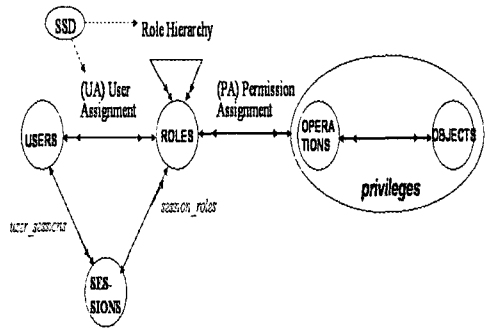
2.4StaticSeparationofDutyRelations

Hierarchies RBAC 모델의 부분집합이라 정의할 수 있는 Static Separation of Duty Relations 모델은 조직을구성하는 구성원들 간의 적절한 권한 부여 및 구성원 사이의 역할 할당에 관한 정책을 제시하기 위한 모델이다.

Hierarchies RBAC 모델 내에서의 SSD(Static Separation of Duty Relations 모델은 다음과 같다.

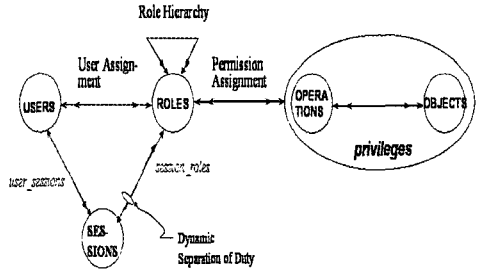
2.5DynamicSeparationofDutyRelations

Dynamic Separation of Duty Relations 모델은 Static Separation of Duty Relations 모델과 비슷한 구조를 가지고 있다. 즉, 사용자들이 가질



(그림 8) Hierarchies RBAC 모델에서의 SSD

수 있는 허가 권한을 제한하는 측면에서는 서로 비슷하다고 할 수 있다. 그러나, 기본적으로 DSD(Dynamic Separation of Duty Relations)는 권한의 제한이 전후 상황이나 배경에 따라 강요되어진다는 차이점을 가진다.



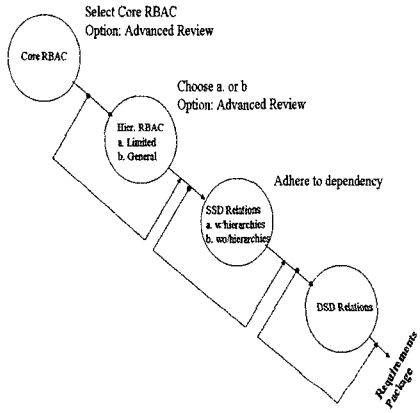
(그림 9) Hierarchies RBAC 모델에서의 DSD

2.6RequirementPackages

역할기반 접근제어(RBAC) 기술은 접근제어를 관리하기 위해 다양한 특성들을 제공하는 기술이라 할 수 있다. 이러한 역할기반 접근제어 기술은 Core RBAC, Hierarchical RBAC, Static Separation of Duty Relations, 그리고Dynamic Separation of Duty Relations 등과 같은 구성요소들에 의하여 정의 할 수 있으며, 각각의 구성요소들은 다음과 같은 기본적인 분야들로 구성되어있다.

- 역할기반 접근제어를 구성하고 있는 여러 요소들과 그에 따른 관계를 생성하고 관리하기 위한 관리적 분야
- 관리적 측면에서의 재검토를 위한 기능
- 접근제어를 결정하고 사용자들에게 역할을 부여하는 시스템 단계에서의 기능

다음은 역할기반 접근제어의 기본적 구성요소와 기능들을 바탕으로 서로 다른 여러 환경에서의 역할기반 접근제어 기술을 이용하기 위한 방법론에 관하여 도식화 하였다.

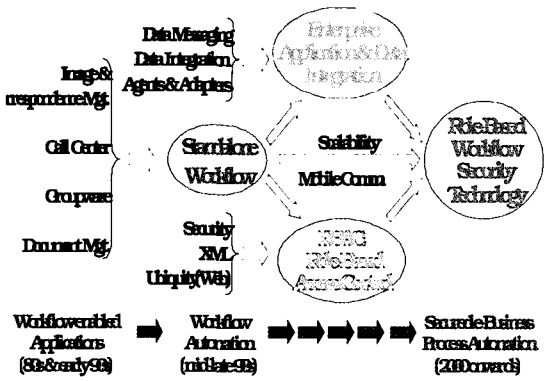


(그림 10) 역할기반 접근제어 방법론

3.RBAC기반워크플로우보안기술

컴퓨터 기술과 전자통신 기술의 급진적인 발전 및 인터넷의 보급, 확산은 기업과 조직체 내에서의 효율적인 상호 작용 지원 수단 및 방법을 탄생시켰다. 이러한 발전은그룹웨어를 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.

기존의 워크플로우 시스템은 B2C와 B2B로 구성되는 기업의 사무업무 프로세스들을 모델링하며, 이의 구문적 또는 의미적 오류를 처리하고 분석하는 워크플로우 정의 도구를 설계 및 구현

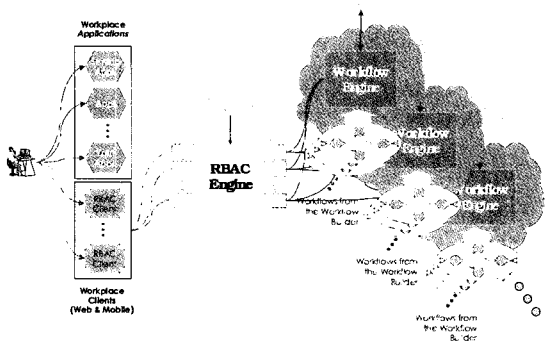


(그림 11) RBAC 및 워크플로우 발전 방향

함으로써 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 사용자의작업 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 12) BRAC 기반 워크플로우 보안 기술

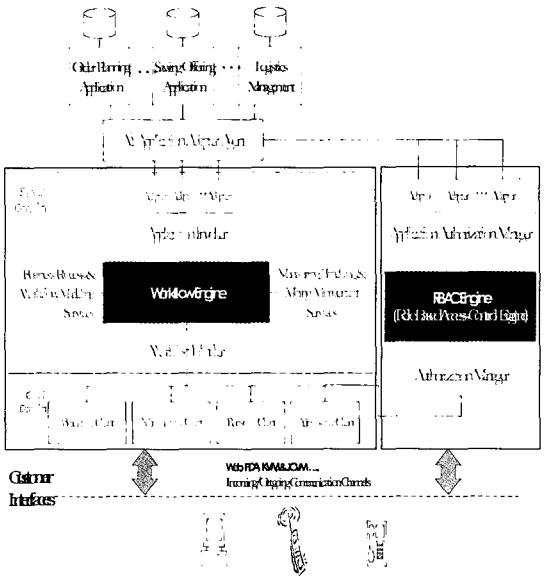
역할기반 접근제어 기술을 이용한 워크플로우 보안 기술은 역할기반 접근제어 서버/클라이언트 모델을 기반으로 워크플로우 시스템 차원에서의 관리를 탈피하여 다양한 접근제어 서비스를 제공할 수 있으며, 웹 기반의 클라이언트를 통해 사용자 인터페이스의 접근을 용이하게 할 수 있다. 즉, RBAC(Role-based Access Control)의 중심적인 개념은 사용자가 기업이나 조직의 정보자원을 임의로 접근할 수 없도록 하는 것이다. 대신에 접근 권한이 역할(role)에 부여되고 사용자는 적절한 역할에 소속됨으로써 역할의 수행에 필요한 최소 자원만을 접근할 수 있도록 한다. 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 권한관리를 매우 단순화 시켜주고 기업의 특정한 보안정책을 구현하는데 있어서 유연성을 제공하며, 사용자는 그들의 업무적 권한과 책임에 따라 특정 역할의 구성원이 되어 접근구조의 변경 없이도 역할의 변경을 쉽게 할 수 있다는 장점을 가지고 있다.

이에 따른 역할기반 접근제어 시스템의 구조는 다음 그림 13과 같다.

역할기반 접근제어 기술을 이용한 워크플로우 보안 기술의 기능은 다음과 같다.

- 정보 보안
- 인증 데이터의 암호화

- 멀티 인증 처리
- 접근 및 작업 시간 제어 기능
- 역할기반 접근제어 서버를 기반으로 하는 중앙관리시스템
- 자체 데이터베이스 시스템으로 추가적 소프트웨어 설치 불필요
- 자체 웹 서버로 추가적인 소프트웨어 설치 불필요



(그림 13) 역할기반 접근제어 시스템 구조

4. 결론

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 결재처리, 자동 문서 전달 및 분배와 같은 비정형 워크플로우 시스템 등에 활용 되어질 것이라 기대 되어진다. 또한, 현재는 기업 및 부서 단위의 비즈니스 프로세스에 주로 적용 되어지는 워크플로우 시스템에서 탈피하여, 기업 또는 부서 간의 상호 협조 및 협업 작업을 필요로 하는 워크플로우 시스템으로 그 적용이 확대되어질 것이라 예상된다.

참고문헌

[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 & 21stCentury Commerce, Global Business Solutions for the New Millennium, 1998.

[6] [AS00] Gail Ahn, Ravi Sandhu, "Role-Based Authorization Constraints Specification." ACM Transactions on Information and System Security, Volume 3, Number 4, November 2000.

[7] [BBF00] E. Bertino, P. Bonatti, and E. Ferrari. TRBAC: a temporal role-based access control model. In Proc. of fifth ACM Workshop on Role based access control, pp. 21-30, 2000.

[8] [CR98] R. Chandramouli and R. Sandhu. Role-based access control features in commercial database management systems. In Proc. of the NIST-NSA

Nat. (USA) Comp. Security Conf., pp 503-511, 1998.
[9] [SCFY96] R Sandhu, E. Coyne, H. Feinstein, and C. Youman. Role-based access control models. IEEE Computer, 29(2), February 1996.
[10] [San98] Ravi Sandhu, "Role Activation Hierarchies." Proc. Third ACM Workshop on Role-Based Access Control, Fairfax, Virginia, October 22-23, 1998, pages 33-40.
[11] [San98b] Ravi Sandhu, "Role-Based Access Control." Advances in Computers, Volume 46, (M. Zelkowitz editor), Academic Press, pages 237-286, 1998.
[12] [SBM97] Ravi Sandhu, Venkata Bhamidipati and Qamar Munawer. "The ARBAC97 Model for Role - Based Administration of Roles." ACM Transactions on Information and System Security, Volume 2, Number 1, February 1999, pages 105-135.
[13] [SFK00] R. Sandhu, D. Ferraiolo, R. Kuhn. The nist model for role-based access control: Towards a unified standard. In proceedings of 5th ACM Workshop on Role-Based Access Control, pages 47-63. (Berlin, Germany, July 2000). ACM.
[14] [SCYG96] C. Smith, E. Coyne, C. Youman and S. Ganta. Market analysis report: NIST small business innovative research (SBIR) grant: role based access control: phase 2. A marketing survey of civil federal government organizations to determine the need for role-based access control security product, SETA Corp., July 1996.
[15] [TDH92] T. C. Ting, S. A. Demurjian, and M. Y. Hu. Requirements capabilities and Functionalities of User-Role Based Security for an Object-Oriented Design Model. In S. Jajodia and C. E. Landwehr, editors, Database Security, IV: Status and Prospects, pages 275-296. North-Holland, 1992.

◐ 저 자 소 개 ◑

원재강

1999년 강릉대학교 생물학과 학사
2002년 경기대학교 대학원 전자계산학과 석사
2002년~현재 : 경기대학교 대학원 전자계산학과 박사과정

김광훈

1984년 경기대학교 전자계산학과 학사
1986년 중앙대학교 대학원 전자계산학과 석사
1994년 콜로라도대학교 대학원 컴퓨터과학과 석사
1998년 콜로라도대학교 대학원 컴퓨터과학과 박사
1998년~현재 : 경기대학교 정보과학부 조교수

정관희

1972년 동국대학교 통계학과 학사
1975년 동국대학교 대학원 응용통계학과 석사
1992년 동국대학교 대학원 전자통계학과 박사
1980년~현재 : 경기대학교 정보과학부 정교수