ebXML 기반 e-Logistics 시스템의 사용자 관리 시스템 설계

채정숙[O] 김영희 이용준
우정기술 연구센터 전자통신연구소
{chaejs[O], kimyh , yjl}@etri.re.kr

Design of User Management System for e-Logistics System Based on ebXML

Jeongsook Chae[O] Younghee Kim oungjun Lee
Information Technology Management Research Group,
Electronics and Telecommunications Research Institute

요 약

사용자 관리 시스템은 single sign on 개념의 통합인증시스템으로 처음 1회 인증으로 이미 정의된 업무 규칙에 따라 부여된 권한으로 시스템에 접근하게 하는 모듈로써, 시스템에 대한 사용자들의 시스템 접근을 편리하게 해 줄 뿐 아니라 정보를 보호하고 시스템의 안정성을 극대화 한다. 본 논문에서는 e-Logistics 통합 플랫폼의 서브 시스템(or 모듈)별로 접근권한체계를 DAC(Discretionary Access Control) 기반으로 통합 관리하는 사용자 관리 시스템을 제시함으로써 효율적인 시스템의 접근 권한을 관리하는 것을 목적으로 한다.

1. 서 론

최근 인터넷의 이용이 급증함에 따라 인터넷을 이용한 기업간 전자상거래가 대두되면서 수 많은 IT 업체들이 전자상거래를 위한 표준화 노력에 앞장서서 XML(eXtensible Markup Language) 기반의 여러 solution들을 개발하고 있다. 기존의 서로 다른 기업 또는 조직간의 표준화된 상거래 서식을 제공하여 서로 합의된 통신표준에 따라 컴퓨터간의 문서를 주고받던 EDI(Electronic Data Interchange)는 문서 교환 시 종이를 이용하지 않고, 비용을 절감하며 전자적인 형태로 정보를 교환하여 기업의 효율성을 증대하였으나 인터넷을 이용한 중소기업에서 대기업에 이르는 모든 규모의 회사들이 문서 교환에 필요한 특별한 합의 없이 e-Business를 수행할 수 있어야 하는 문제에 이르렀다. 이에 새롭게 등장한 것이 ebXML이다. ebXML(electronic business XML)은 국제 EDI 표준화 기구인 UN/CEFACT와 XML 표준화 기구인 OASIS가 주축이 되어 XML표준화 공동작업에 합의하여 만들어진 글로벌 전자상거래 표준이다. 새로운 전자상거래 표준으로 자리를 굳히고 있는 ebXML은 XML 문서 정의, 전송, 저장, 검색 등에 관한 표준을 제정함으로써 전 세계 전자 상거래의 자동화를 목표로 하고 있다[1].

이러한 ebXML에 기반을 둔" e-Logistics 통합 플랫폼" 은 물류 알선 및 물류 정보관리(물류정보관리시스템) 및 물류 비즈니스 프로세스를 자동화하여 물류에 관한 표준 문서를 작성하여(BP 관리 시스템) 메세징 서비스(메세징 시스템)를 통해 기업간의 거래를 수행하는 것으로 실시간으로 차량 및 운송화물을 추적(Track/Trace 시스템)하고 이를 알리는 서비스와 외부 시스템과의 연동이 가능한 통합 메세징 서비스를 하는 ebXML 기반의 B2Bi solution이다. " 본 논문에서는 ebXML 기반의 "e-Logistics 통합 플랫폼"에 접근하기 위한 사용자 관리 시스템(User Management System)을 설계한다. 사용자 관리 시스템은 최초 1회 인증으로 모든 서브 시스템들의 접근이 가능하며, 사용자 역할을 생성하여 사용자의 역할에 맞는 권한을 부여함으로써 효율적으로 시스템의 접근을 통제할 수 있다.

본 논문의 구성을 살펴보면 다음과 같다. 2장에서는 시스템의 접근 권한을 관리하기 위한 관련연구로서 DAC(Discretionary Access Control), MAC(Mandatory Access Control), RBAC(Role Based Access Control)에 대한 개념을 소개하고, 3장에서는 본 논문에서 설계한 사용자 관리 시스템의 구조에 대해 기술하고, 3장에서는 사용자 관리 시스템의 세부 시스템의 기능적 요구사항에 대해 설명한다. 4장에서는 사용자 관리 시스템의 사용자 권한을 부여하는 역할 관리 생성에 대해 논하고, 마지막으로 5장에서는 결론 및 향후 연구 방향을 고찰한다.

2. 관련연구

사용자 관리 시스템(user management system)은 "e-Logistics 통합 플랫폼" 내에서 공통으로 사용될 사용자 정보와 접근권한을 관리하는 모듈이다. 또한 사용자 계정과 역할(Role)을 관리하고, 통합인증시스템과 연계되어 포탈 내의 단위 시스템 별 사용자 접근을 제어한다.

시스템과 데이터베이스에의 데이터 베이스의 일부를 악의적으로 변경하는 것을 제어하는 것을 접근제어(access control)이라고 하며, 접근 권한이 없는 사용자들이 시스템에 접근하여 정보를 얻기 위한 접근 제어 방식은 크게 다음의 세가지로 나눌 수 있다.

2.1 DAC(Discretionary Access Control)

임의적 접근 제어는 사용자 또는 그룹의 식별자에 따라 객체에 대한 접근을 제한하는 수단으로 객체의 소유자는 시스템 관리자의 간섭 없이 주체의 객체에 대한 접근권한을 임의로 지정하거나 다른 주체에게 간접적으로 위임할 수 있다. 접근통제 정책의 하나로 시스템 객체에 대한 접근을 사용자 개인 또는 그룹의 식별자를 기반으로 제한하는 방식으로 임의적이라는 말은 어떤 종류의 접근 권한을 갖는 사용자는 다른 사용자에게 자신의 판단에 의해서 권한을 줄 수 있다는 것이다. 주체 및 객체의 신분 및 임의적 접근통제 규칙에 기초하여 객체에 대한 주체의 접근을 통제하는 방법이다[2][4].

2.2 MAC(Mandatory Access Control)

MAC 방법은 BLP 모델의 단순 특성이나 스타 특성(*-property)와 같은 주체에 부여되는 보안 자격과 객체에 부여되는 보안 등급으로 주어진 보안 레이블에 따라 접근을 제어하는 보안 정책이다. 즉, 객체에 포함된 정보의 비밀성과 이러한 비밀성의 접근 정보에 대하여 주체가 갖는 권한에 근거하여 객체에 대한 접근을 제어한다. MAC는 등급화된 정보의 기밀성을 위한 보안에 초점이 맞춰져 있다. 최근에는 MAC는 DAC 방법과는 달리 정보 흐름의 통제를 보다 강화하여 안정성을 제공하며 중앙집중적인 보안 관리를 가능하게 한다[2][4].

2.3 RBAC(Role Based Access Control)

RBAC는 사용자가 수행할 업무 능력에 따라 직무를 생성하고, 접근 권한을 부여하며 사용자를 책임과 자격에 따라 직무에 배정하는 모델이다. 직무는 조직의 규모나 체제에 따라 여러 작업으로 표현되며, 필요에 따라 쉽게 새로운 접근 권한이 부여되고 삭제 될 수 있는 장점이 있다. 즉 접근 권한이 역할에 부여되므로 시스템이 변경될 때 필요에 따라 쉽게 새로운 접근 권한을 역할에 부여하거나 삭제할 수 있고, 조직의 요구에 따른 접근 제어 정책의 관리가 용이하게 한다[2][3].

3. 사용자 관리 시스템

3.1 사용자 관리 시스템 정의

사용자는 회원(화주, 운송업체)과 비회원(guest, 일반사용자) 그리고 관리자(administrator)로 구분되며, 시스템 관리자로부터 이미 정의된 사용자 역할에 의한 회원은 최초 가입/인증과정을 거쳐 시스템에 로그인하여 권한을 부여 받아 회원 별로 서비스를 이용하는 일부 제한된 기능의 서비스를 수행하게 된다. 사용자는 e-Logistics 통합 플랫폼의 각 서브 시스템(, BP 관리 시스템, RR 관리 시스템, 문서 변환 시스템, Track&Trace, Alert 시스템, 모바일 서비스)의 사용 접근을 위해 사용자의 서브시스템에 대한 권한을 가지고 있는지를 체크하게된다. 임의의 주체에 대한 특정 객체의 접근 허용 여부를 결정하는 방식으로 임의적 접근제어 DAC 방식의 ACL 메커니즘을 사용한다. 본 논문에서는 "e-Logistics 통합 플랫폼"의 각 서브시스템의 사용자 접근 제어는 사용자(개인, 그룹, 직무)의 구분이 필요로 하게 된다. 따라서 이에 적합한 DAC의 ACL(Access Control List)에 따라 시스템에 대한 역할 권한을 생성한다. ACL 은 타켓의 소유자 또는 관리자가 앞서서 부여된 허가를 사용하기 쉽게 하는 장점이 있다.

3.2 기능적 세부 구조

e-Logistics 통합 플랫폼의 기능적 세부구조를 살펴보면 다음 그림 1과 같이 J2EE기반의 서비스 인터페이스와 메시지 지향 미들웨어, e-Logistics 서버, 애플리케이션/데이터 통합 인터페이스로 구성된다.

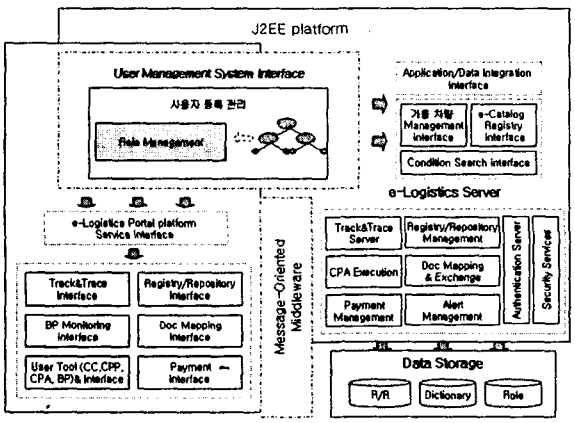

그림 1 e-Logistics 통합 플랫폼

사용자 관리 시스템은 크게 "e-Logistics 통합 플랫폼"의 상위 layer에서 end-user에게 시스템의 접근 권한을 부여하기 위하여 사용자 등록 관리와 사용자 역할 관리로 나눌 수 있다.

사용자 등록 관리는 e-Logistics 서버의 사용자 인증모듈과 연동하여 사용자 계정(account)을 발급하여 인적 사항 및 id, password, 사용자 등록 정보를 관리한다.

사용자 역할 관리는 "e-Logistics 통합 플랫폼"의 서브 시스템의 직무를 분리하여 사용자의 직무를 구분하고, 사용자 직무를 그룹화하여 계층구조인 트리 형태로 구성한다. 이를 기반으로 사용자 권한을 생성하고 이를 부여하여 권한을 관리하게 된다. 사용자는 guest, 화주, 운송업체, 관리자로 구성되며, 이들은 사용자 등록과 함께 생성되어진 역할 규칙에 의해 자신의 직무에 맞는 역할이 부여 되어 시스템의 접근을 통제 받게 된다.

그림 2는 사용자 관리 시스템의 구조도를 나타내며, 그림 3은 사용자 관리 시스템의 액터와 액티비티간의 유스케이스 다이어그램을 나타낸다.

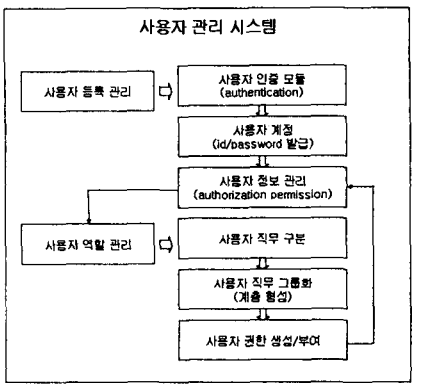

그림 2 사용자 관리 시스템의 구조

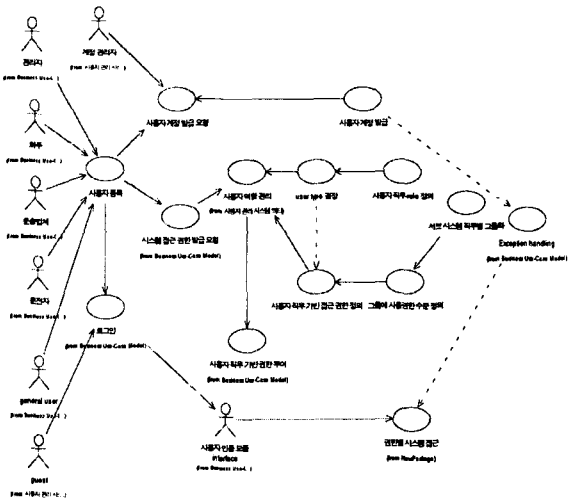

그림 3 사용자 관리 시스템의 유스케이스 다이어그램

4. 사용자 관리 시스템의 역할 생성

" e-Logistics 통합 플랫폼" 에서 제공하는 사용자 관리 시스템은 ' e-Logistics 통합 플랫폼 내에서 공통으로 사용될 사용자 정보와 접근권한을 관리하는 모듈이다. 사용자 관리 시스템에서 관리하는 사용자 계정과 역할은 통합 인증시스템과 연계되어 포탈내의 단위 시스템 별로 사용자 접근을 제어한다. e-Logistics 통합 플랫폼은 9개의 서브 모듈로 이루어진다. 따라서 각기 서브 시스템에 정보 관리 및 사용자 프로파일을 관리하기 위해 사용자의 접근 권한 역할이 필요하다. 즉, 데이터베이스 측면에서 고려해 볼 때, 다양한 등급을 갖는 다수의 사용자가 접근하게 되면 보안의 유출 및 자료의 생성 및 소멸이 일어나지 않도록 시스템을 관리하기 위한 역할 관리가 필요하게 된다. 서브 시스템에 접근하기 위한 권한을 부여하기 위해서는 역할 관리가 필요하게 된다. 역할 관리는 다음의 두 가지로 분류할 수 있다. 첫 번째로 다중 권한 체계를 기반으로 한 사용자 역할 관리와 개별 사용자 인적 사항 및 역할 관리가 있으며, 본 논문에서 제안하는 방법은 후자로 DAC의 타켓 기반 ACL 메커니즘을 사용하여 "e-Logistics 통합 플랫폼"의 각 서브 시스템의 각 액터들을 분류하고 이들의 직무를 명확히 구분하여 이들을 그룹으로 나눈다. 이러한 그룹을 트리 형태로 표현이 가능하며 각 그룹은 계층을 형성하게 된다. 하위 계층의 접근 허가를 부여 받은 권한은 상위 계층의 시스템에 권한 허가가 상속된다. 이렇게 사용자 권한을 생성하게 되면 나중에 직무가 추가된다 하더라도 역할을 부여하기가 쉬우며, 시스템의 사용 접근 권한의 변경 또한 용이하게 된다. 그림 4는 접근 통제를 위한 개념도를 나타낸다.

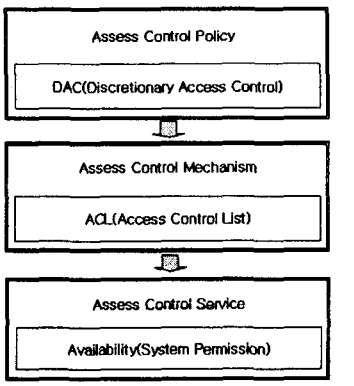

그림 4 접근 통제 개념

5. 결론 및 향후 연구방향

본 논문에서는 " e-Logistics 통합 플랫폼" 에 적용되는 사용자 관리 시스템의 아키텍처와 사용자 관리 시스템의 세부 구조, 사용자 관리 시스템의 역할 생성 규칙에 대해 기술하였다. 사용자 관리 시스템은 크게 사용자 등록 관리와 역할관리로 구분하여 설계하였으나, 현재 통합 인증 모듈과 연동과 보안에 대해서는 고려하지 않았다. 이는 차후에 연구할 내용으로 시스템의 안정성을 위해 반드시 고려되어야 한다.

[참고문헌]

[1]UN Technical Architecture Team, "*Technical Architecture Specification v1.0.4*", 16 February 2001.

[2] http://www.kisa.or.kr/technology/sub3/AC_9901.html

[3]D.F. Ferraiolo, J. Barkley, D.R. Kuhn, "A Role Based Access Control Model and Reference Implementation within a Corporate Intranet", *ACM Transactions on Information Systems Security,* Volume 1, Number 2, February 1999.

[4]Ravi Sandhu and Qamar Munawer,"How to do discretionary access control using roles" In *Proceedings of the Third ACM Workshop on Role-Based Access Control* (RBAC '98, Fairfax,VA, Oct. 22-23). 1998.