DOI: 10.3745/KIPSTC.2009.16-C.3.307

국제 물류 서비스를 위한 RBAC 기반 보안 모델

황 정 희[†] · 신 문 선[††] · 이 종 연[†††] · 황 익 수[††††]

요 약

RFID 기술은 유비쿼터스 환경을 구현하기 위한 핵심기술 중 하나로 물리적인 접촉 없이 인식 가능한 기술로써 기업과 학술적 분야에서 많은 관심을 받고 있다. 특히 물류 환경에서 RFID 기술 기반의 물류 환경 관리는 비용 및 납기의 개선 등에 큰 효율성을 가져올 수 있다. 이 논문에서는 국제 물류 프로세스에 대한 보안 요구사항을 분석하고 RBAC 기반의 접근 제어 모델을 제안한다. 그리고 접근제어의 제약조건을 UML로 표현한다.

키워드 : RFID, 보안, 보안 정책, 물류 서비스

RBAC Based Security Model for International Logistic Service

Jeong Hee Hwang[†] · Moon Sun Shin[††] · Jong Yun Lee[†††] · Ik Soo Hwang[††††]

ABSTRACT

RFID technique which is recognizable without the physical contact between the reader and the tag is the core to archive ubiquitous environment, and has been attracting a lot of interest from both industry and academic institutes. Especially, RFID based logistic service management can get the low priced cost and the advancement of the appointed date of delivery. In this paper, we first analyze security requirements of international logistics process, and then propose a RBAC based security model and represent access control constraints using UML.

Keywords : Radio Frequency Identification, Security, Security Policy, Logistics Service

1. 서 론

RFID(Radio Frequency IDentification) 시스템은 무선 통신 기술을 이용하여 직접 접촉하지 않고 RFID 태그 정보를 식별할 수 있기 때문에 기존의 바코드 시스템보다 많은 장점을 갖는다. 즉, 주파수를 사용하여 태그에 직접 접촉하지 않고도 한 번에 다수의 태그를 읽을 수 있다. 이러한 RFID의 장점 때문에 기존의 표준화된 제품을 대량 생산하는 방식에서 탈피하여 RFID 시스템을 기반으로 하는 고객의 다양한 요구에 맞추어 제조, 납품하는 대량 맞춤 서비스가 보편화되고 있으며 SCM(Supply Chain Management)을 위한 비즈니스 솔루션이 등장하게 되었다[1, 2]. RFID를 이용한 제품의 제조 및 유통과정에서 제품의 흐름에 대한 가시성을 확보할 수 있어 업무 효율성이 향상되고 전체적인 물류 유통흐름에서 보다 효과적인 재고 관리 및 제품 추적이 가능하며, 제품 무결성이 향상되고 제품 손실률을 줄일 수 있는 장점이 있다[2-4]. 그러나 RFID기반의 국제 물류 서비스 플랫폼에서의 효율적인 물류처리 서비스에서는 우선적으로 물류 정보의 보안 문제를 해결해야 한다. 제품 정보에 대한 보안뿐만 아니라 도용, 위치 추적, 물리적 공격 등 RFID 기반 물류 환경의 특성상 나타나게 되는 여러 가지 위협에 대한 보안정책과 프라이버시 문제가 드러나고 있으며 이는 RFID기술 기반 물류 환경 관리의 기술발전과 보급을 저해하는 요인이 되고 있다.

EPCglobal Network[5-7]는 RFID 태그 정보의 구조, 의미, 전달방법에 대한 표준을 제공하며, 개별기업은 EPCglobal Network 상에서 발생하는 정보를 각 기업과 기관의 방화벽 안에서 개별적으로 관리하고, 이 정보는 ONS(Object Naming Service)와 Discovery Service를 통해 공유하는 방식으로 운영된다. 이렇게 EPCglobal Network는 거대한 물류환경에서 EPC(Electroic Product Code) 정보의 분산관리와 전달 효율성을 높일 수 있으나 각 기업과 기관의 방화벽과 같은 보안계층으로만 위협요소를 모두 제거할 수 없으며 국제물류 서비스 플로우상에서 나타나는 위협에 대한 보안 요구사항의 분석 및 보안 모델은 현재 미비한 단계이다.

이 논문에서는 RFID기반의 국제 물류 서비스 플랫폼에서

※ 이 연구는 지식경제부 uGLP성장동력기술개발사업(한국무역정보통신)의 지원에 의하여 연구되었음
† 종신회원 : 남서울대학교 컴퓨터학과 전임강사
†† 종신회원 : 건국대학교 컴퓨터시스템학과 강의교수(교신저자)
††† 종신회원 : 충북대학교 컴퓨터교육과 부교수
†††† 정 회 원 : 한국무역정보통신
논문접수 : 2008년 11월 13일
수 정 일 : 1차 2009년 1월 5일, 2차 2009년 1월 15일
심사완료 : 2009년 2월 2일

의 신뢰성과 제품 무결성의 보장 및 EPC Network 상에서 물류 정보와 사용자 정보를 보호하기 위해 EPCglobal의 보안 가이드라인을 기반으로 하는 국제 물류 서비스에서의 보안 요구사항 및 보안 정책방안을 기술하고 역할기반 접근제어 모델인 RBAC(Role Based Access Control Model)을 적용한 정보보호 모델을 제한한다. 그리고 접근 제어의 제약조건을 UML로 표현한다.

이 논문의 구성은 다음과 같다. 2장에서는 먼저 NIST (National Institute of Standards and Technology)의 RFID 시스템의 보안 가이드라인의 내용을 기술하고 3장에서는 RFID 기반 EPC 네트워크 응용 서비스에서의 보안 요구사항을 설명한다. 4장에서는 국제 물류 프로세스 상에서 고려해야 할 보안 위협 및 프로세스 각 단계에 대한 보안 요구사항을 기술한다. 5장에서는 국제 물류 프로세스에 대한 RBAC 기반의 보안 모델을 제시하고 접근 제어의 제약조건을 UML로 표현한다. 6장에서는 결론과 향후 연구 계획을 기술한다.

2. 관련연구

EPCglobal 아키텍처 프레임워크는 EPC를 사용하여 공급/유통망 강화라는 공동 목표를 위해 서비스하는 것이다. 즉, EPCglobal과 위임기관이 운용하는 코어서비스(EPCglobal Core Service)와 데이터 인터페이스, 소프트웨어, 하드웨어 관련 표준(EPCglobal Standard)의 종합이다[5].

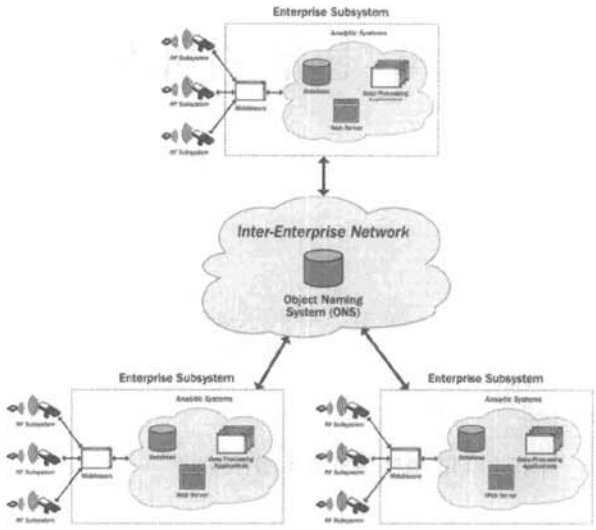
2.1 EPCglobal 네트워크

EPCglobal 네트워크란 EPC 코드와 RFID 기술을 바탕으로 제품에 식별번호를 부여하고 정보를 저장할 수 있는 공간을 네트워크로 연동하여 공급자, 수요자, 그리고 소비자가 제품에 관련된 정보를 알 수 있게 해주는 시스템이다. 즉, RFID 리더와 같은 여러 데이터 자원에서 하나 이상의 EPC 데이터를 수집하고, 사용자의 요구에 맞게 필터링 및 그룹화하여 다양한 형태로 보고하거나 EPC IS(Information Services)에 처리된 데이터를 저장할 수 있는 표준이며, 애플리케이션 비즈니스 로직과 인프라스트럭처 컴포넌트 사이에 독립성을 제공한다.

EPCglobal 네트워크기반의 RFID 응용 시스템은 다양한 응용분야에서 기본적으로 (그림 1)과 같은 Inter-Enterprise Architecture 프레임 기반으로 적용 가능하다. 오픈 네트워크 형태이든지 혹은 클로즈드 네트워크을 기반으로 하든지 기본 구조는 (그림 1)과 같은 형태의 엔터프라이즈 서브시스템의 연동을 통해서 응용서비스를 수행하게 된다[8, 9].

2.2 EPCglobal의 보안 가이드라인

RFID 시스템과 연관된 비즈니스 리스크를 줄이기 위한 EPCglobal의 보안 가이드라인의 보안 정책(security control)[10]에 대해 기술한다. 보안 정책에 있어 시스템의 관리에 대한 제어는 RFID 시스템의 관리 및 보안 유지를 위해 필



(그림 1) Inter-Enterprise Architecture

요한 정책을 의미하며, 이는 위험평가, 시스템 설계 그리고 시스템 인증 등과 연관 있다. 즉, 개인정보와 같은 중요한 데이터는 태그에 직접 저장하는 대신 엔터프라이즈 서브시스템에 저장하고, 태그의 아이디를 이용하여 검색할 수 있게 해야 한다. 이것은 정당한 접근자만 접근 가능하게 한다. 그러므로 데이터 암호화와 접근 제어는 RF 서브시스템보다 엔터프라이즈 서브시스템에서 수행하는 것이 비용면에서 더 효율적이다. 그러나 노출되어 있는 EPC 포맷의 식별자를 사용할 경우 공격자가 중요한 정보를 가로챌 수 있고, 엔터프라이즈 서브시스템에 있는 데이터도 네트워크를 통해 데이터 공격에 여전히 노출될 가능성이 있다.

RFID 시스템 작업에 배정된 개인과 조직의 역할에서 인증된 사용만을 허용하도록 하는 사용 인증 및 RFID와 연관된 IT 보안 정책을 고려하여 RFID 서브시스템, 네트워크, 데이터베이스 등에 대한 보안정책도 시스템 관리를 통한 보안 정책의 한 방법이다. RFID에 대한 접근제어, 포트와 프로토콜들을 포함하는 주변기기 및 서브시스템에 대한 보호, 패스워드 관리, RFID 보안 교육, 암호시스템의 관리 등의 이와 관련된다. 따라서 이 정책은 엔터프라이즈 서브시스템과 관련된 RFID 시스템 구현에 적용가능하다. 이러한 점에서 RFID 시스템의 개별적 관리, 구현 및 디자인을 위한 가이드를 제공할 수 있다는 장점이 있다. 한편 정책 수행을 위해 효율성을 고려하는 적당한 기술적 제어의 수행이 필요하다.

시스템의 기술적 제어는 시스템 동작에 대한 제한과 시스템의 가동상황을 모니터하기 위한 기술적 정책과 관련된다. RFID 시스템의 서브시스템을 위한 가장 일반적인 기술은 패스워드, 키-해쉬 메시지 인증 방식 그리고 디지털 서명이다. 키-해쉬 메시지 인증 방식은 알고리즘의 조합에 의해 공통된 비밀키를 공유하여 보안을 유지하는 정책이다. 디지털 서명 방식은 태그 트랜잭션 처리와 관련된 이벤트 데이터, 타임 스탬프(time stamp), 태그 식별자 등을 디지털로 서명하는 암호화방식이다. 그리고 이들 방법의 주된 목적은 태그에 대해 인증되지 않는 사용자의 읽기를 방지하는 것이다.

암호화기반의 인증 기술은 인증 트랜잭션의 데이터에 대한 무결성 서비스를 제공한다.

그리고 태그는 정확한 패스워드가 아니고는 password-protected command(태그의 읽기, 쓰기)를 허용하지 않는다. 이 정책을 사용하면 패스워드 관리 시스템을 향상시킬 수 있다. 패스워드는 도청을 막기 위해 주변 환경을 물리적으로 보호하는 차원에서 각각의 태그에 지정해야 한다. 즉, 태그간의 패스워드를 공유하지 말아야 한다.

또한 보안 유지를 위해 시스템 관리자와 사용자가 수행해야 하는 행동(action)과 관련된 보안 정책은 중요하다. 일반적으로 물리적 접근 제어는 fence, gate, wall, locked door와 같은 접근 제어 장치를 이용하여 사용자에 대한 시스템 및 데이터 접근을 제한한다.

공격의 위험 요소에는 태그에 대한 인증되지 않은 읽기, 쓰기, 태그 복제, 사용자 스푸핑(spoofing), RFID의 물리적 파괴, 인증되지 않은 커맨드(command)를 서비스하는 부정 행위 등이 있다. 이를 방지하기 위한 물리적 접근제어의 정책의 장점은 RFID 시스템 컴포넌트에 접근하는 공격 가능성을 제한할 수 있다는 점이다. 그러나 내부에서의 공격을 막을 수 없고, 주파수 방해와 같은 공격에 대한 실질적인 보안 정책은 될 수 없다는 단점이 있다.

또한 태그와 리더를 적당한 위치에 설치하는 것은 전자적 방출에 대한 위험과 방해를 피할 수 있다. 이를 위해 불필요한 전자적 방출(electromagnetic radiation)을 최소화 시킬 수 있는 곳에 RFID 시스템 장비를 두어야 한다. 이러한 정책의 장점은 도청 및 권한 없는 자의 접근 등을 방지할 수 있다는 것이고 한편으로는 모바일에 적용할 때와 같이 태그의 위치를 항상 제어할 수 없을 경우에는 효율성이 떨어지게 된다.

더 이상 유용하지 않은 태그는 물리적 또는 전자적 폐기 및 보안 정책을 위한 적합한 가이드라인과 정책을 따르도록 시스템 사용자를 교육하는 것도 중요하다. 보안에 대한 지식과 기술을 익히도록 하고, 인증되지 않은 사용 및 식별 방법, 위반을 발견했을 때 누구에게 보고할 것인지 등을 교육해야 한다.

3. RFID 시스템의 보안 요구사항

RFID 시스템은 태그, 리더, 서버(미들웨어 및 응용 서비스 플랫폼)로 구성되고 유무선 통신망과 연동되어 사용된다. 태그는 객체를 인식할 수 있는 정보를 가지고 네트워크 상에 위치하며, 리더는 객체의 정보를 수집하고 이를 처리하며 송신, 수신하는 기능을 가진다. 서버는 객체의 정보를 활용하여 응용처리를 수행한다. 이 장에서는 RFID 시스템의 주요 구성요소인 태그, 리더기, 안테나에 대한 보안 위험 및 이를 고려하는 보안 요구사항을 기술한다.

3.1 태그(tag) 보안

기본적인 물품 코드 정보를 포함하고 있는 태그에 대한 보안 정책 방안으로 태그에 패스워드를 부여하여 인증하는 방식을 사용한다. 패스워드는 도청을 막기 위해 주변 환경을 물리적으로 보호하는 차원에서 사용될 수 있으므로 각각의 태그에 지정해야 한다. 그리고 태그 간에 서로 다른 패스워드를 지정하여 공유할 수 없도록 해야 한다. 이러한 태그의 패스워드 부여와 더불어 안전한 보안을 위해 태그에 데이터를 저장하기 전에 데이터에 대한 암호화를 하는 것이 필요하다. 패스워드가 누출되어 태그에 접근했을 때에도 데이터에 대한 암호화로 인해 실제 데이터를 읽을 수 없도록 하는 방법이 필요하다.

RF 인터페이스에서 리더기와 태그간의 교류가 자주 발생하지 않는 태그에 대해 일시적으로 정지(turn off)가 가능하도록 한다. 이것은 공격자로부터의 도청이나 공격을 줄일수 있는 방법이 될 수도 있다. 그러나 이와 같은 일시적 정비 방법은 태그와 리더기간의 교류 횟수에 대한 예측을 할 수 있는 경우에 적용할 수 있다. 이와 같은 방법의 하나로 태그를 비활성화(deactivate)상태에 두고 있다가 스위치가 켜지면 다시 RF와 태그가 교류할 수 있도록 활성화하는 방법도 가능하다. 리더기는 주기적으로 태그의 지속적인 존재와 동작 상태를 확인할 수 있는 모니터링을 수행하여 태그에 인증받지 않은 접근자의 탐지 및 예기치 않은 데이터 교환 등을 즉시 식별할 수 있도록 해야 한다.

이와 같은 태그 보안 정책과 더불어 태그와 관련하여 신호를 전송하고 받는 radio frequency는 태그의 수행에 있어 태그의 동작 범위, 속도, 데이터 전송률과도 연관된다. 그러므로 태그가 반응할 수 있는 범위, 주파수의 충돌 가능성, 주파수 변화에 따른 태그의 이동성 등을 고려해야 한다.

3.2 리더기(reader) 보안

리더기와 태그 간의 커뮤니케이션을 위해서는 표준을 따라야 한다. 이를 위해 일반적으로 같은 벤더의 태그와 리더기가 사용된다. 리더의 형태에는 유선 리더와 무선 리더가 있다. 유선 리더는 고정된 위치에 있으면서 리더에 접근하여 태그를 읽는 형태가 있다. 이러한 예로써 신호 위반 카메라가 이에 속한다. 그리고 무선 리더는 이동 가능한 리더를 의미한다. 모든 리더기는 태그와 소통할 수 있는 RF 서브시스템이 있다. 그리고 엔터프라이즈 서브시스템과 소통할 수 있는 인터페이스가 있다. 엔터프라이즈 서브시스템 인터페이스는 분석 및 처리를 위해 리더로부터 엔터프라이즈 서브시스템의 컴퓨터까지 RFID 데이터의 전송을 지원한다.

각 리더기에는 허용되는 power output 과 duty cycle이 있다. duty cycle는 장치가 일정기간동안 에너지를 방출하는 시간의 퍼센트(1분에 30초 소통시-50%)를 의미한다. 수동태그와 통신하는 리더는 능동 태그와 통신하는 것보다 더 큰 power output를 필요로 한다. 강력한 전력의 duty cycle를 가진 리더는 더 먼 거리로부터 또는 정확하게 태그를 읽는다. 그러나 너무 강력한 전력은 도청 위험을 증가시킬 수 있으므로 이를 고려해야 한다.

리더기는 일반적으로 다양한 안테나 타입을 사용하여 태

그와 소통할 수 있다. 특히, 분리된 안테나(detachable antenna)는 리더의 요구사항에 맞게 선택적으로 적용될 경우에 적합하다. 그러므로 안테나의 특징들을 기반으로 하여 태그와 안테나의 커뮤니케이션 방법을 이해하고 이를 고려해야 한다. 또한 여러 개의 태그가 근접해 있을 때 리더기가 특정 태그를 식별하고 처리할 수 있는 개별화(Singulation)할 수 있어야 한다. 리더기가 특정 태그에게 질의를 보낼 때 리더기는 여러 개의 태그로부터 동시에 응답을 하지 말아야 한다. 즉, 태그는 랜덤하게 주어지는 번호에 일치할 때 응답하고, 리더기는 충돌되는 태그가 없다는 것을 확인하고 태그와 정보를 커뮤니케이션해야 한다.

3.3 안테나(antenna) 보안

태그에서 보내온 신호를 수신하는 안테나를 위한 보안 정책 방안으로 가장 일반적인 방법은 부서지기 쉬운 안테나를 사용하는 것이다. 이것은 RFID 태그는 공격자가 태그를 수정 및 변경하거나 태그를 제거하는 것을 방지하기 위해 위조가 불가능하도록 공격자의 접근했을 때 안테나가 오작동을 일으켜 태그에 접근할 수 없도록 하는 방법이다.

그리고 안테나의 사용에 있어 비즈니스 응용에 따라 적당한 무선 주파수(Radio frequency)를 선택해야 한다. 주파수 사용에 있어서 고정된 주파수(fixed frequency)를 사용하는 것은 무선 신호에 대한 방해 및 충돌을 효과적으로 줄일 수 있기 때문이다.

RF 시스템의 운영자(operator)는 리더기 또는 능동 태그로부터 전송된 RF 에너지 레벨을 조정하여 보안에 대비할 수 있다. 즉, 안테나의 일부 타입은 전송된 RF 에너지의 방향을 조정할 수 있도록 되어 있기 때문에 이러한 안테나의 조정을 통해 보안에 대비할 수 있다. 또한 안테나와 관련된 전파 범위에 전자기의 보호(electromagnetic shielding) 장치 및 제한할 수 있는 방법을 마련하는 것이다. 이것은 RF 신호를 보호구역 외로 전파되는 것을 방지할 수 있도록 하여 외부로 부터의 안테나와 관련된 동작 자체를 차단시키는 것이 중요하기 때문이다.

이러한 안테나의 보안 요소를 고려하여, 태그와 소통할 수 있는 충분한 범위 그리고 리더기의 요구사항에 맞는 안테나를 선택하여 적용해야 다른 주파수의 방해를 최소화 하고 도청 가능성을 줄일 수 있다.

3.4 네트워크(Network) 보안 요구사항

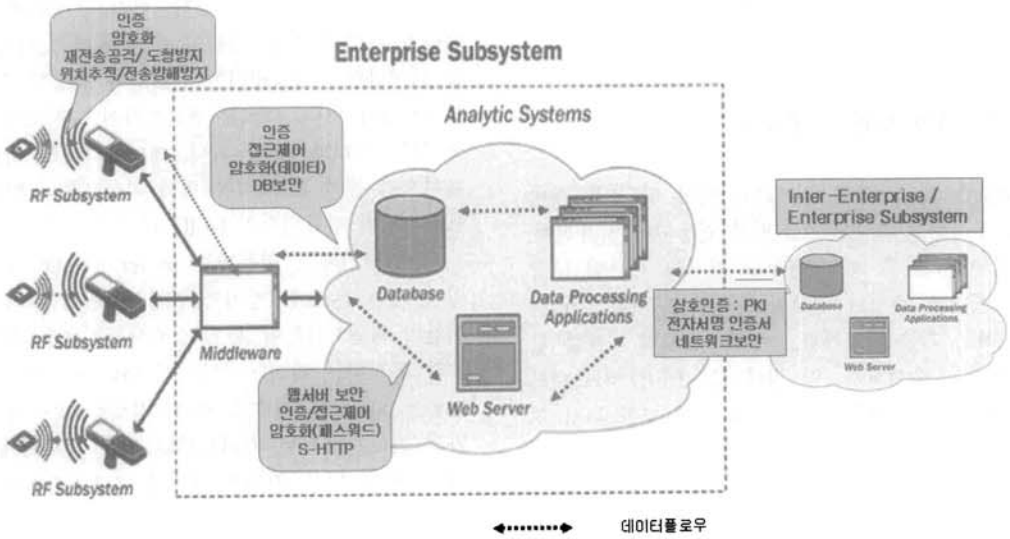
EPCGlobal 네트워크를 구성하는 RFID 엔터프라이즈 서브시스템과 엔터프라이즈 시스템간에는 이러한 보안 위협에 대응할 수 있는 보안 요구사항을 고려하여 안전하고 신뢰성 있는 국제물류 서비스 플랫폼을 제공할 수 있어야 한다.

RFID 시스템은 기본적으로 네트워크 보안과 프라이버시 보호를 충족시켜야 한다. 기밀성, 무결성, 가용성, 부인봉쇄, 인증을 보장하는 보안 메커니즘이 요구되며 정보흐름에 따른 각 세션에서의 보안메커니즘의 구현이 필수적이다. (그림 2)는 RFID Enterprise Subsystem의 데이터 플로우를 도식화하고 그에 따른 보안 요구사항들을 나타낸 것이다.

도청 방지, 위조태그 방지, 불법복제 태그방지, 위장 리더 방지 등을 포함하는 프라이버시 보호와 서비스거부공격에 대한 방어, 해킹으로 인한 정보유출시 유출된 정보의 기밀성 보장 등을 포함하는 네트워크 보안을 위해서는 RFID 태그와 리더 사이의 인증기술 및 태그와 리더 사이의 안전한 데이터 송수신을 위한 대칭키 또는 공개키 방식의 키 관리 등과 같은 보안 기술이 요구된다. 이것은 RFID 시스템의 태그 자체의 보안 문제, 태그와 리더 구간에서의 보안문제, 리더와 로컬 서버사이의 보안문제, 서버 자체 보안 문제 등이 존재하기 때문이다.

4. 국제물류 프로세스에서의 보안 정책

EPCglobal 산하 TLS(Transport and Logistics Services)



(그림 2) RFID Enterprise Subsystem

비즈니스 액션 그룹 주관 하에 2006년 10월에 시작되어 2007년 2월에 마무리 된 홍콩과 일본 간의 수출입 물류 프로세스를 토대로 국제 물류 프로세스 상의 위험요소를 분석한다. 이 사업은 EPC/RFID를 이용하여 홍콩에서 일본까지 수출입물류가 어떻게 운용되는지에 대한 가시성 확보 및 RFID기술을 기반으로 수출입에 사용된 선적 정보 등을 조사하는데 목적을 두고 실시되었다[11].

홍콩-일본 간 수출입 비즈니스 프로세스를 살펴보면 먼저 운송업자 발생 기점에서 생산된 제품을 패킹하고 상자를 트럭에 신고 통합창고로 이동한다. 여기서 먼저 태그를 프린팅하여 적용하고, 상자 단위의 태깅을 한다. 그리고 태깅 정보를 홍콩 EPCIS에 보낸다. 상자를 팔레트 위에 쌓고 트럭에 적재하여 통합창고 게이트를 통과한다. 팔레트 단위의 제품을 컨테이너에 적재하고 컨테이너 문을 닫고 문에 e-Seal을 적용한다. 이 때 상자의 데이터는 홍콩 EPCIS에 보낸다.

상자의 태그 정보와 e-Seal정보, 그리고 적재정보를 조합하여 홍콩 EPCIS에 보낸다. 컨테이너 차량은 통합창고의 게이트를 통과하여 항구 터미널에 도착하게 되고 운송할 선박에 컨테이너를 적재하게 된다. 배는 홍콩을 떠나 일본으로 운항하게 된다. 항구터미널에 도착한 배로부터 컨테이너를 하역하게 되고 이때 컨테이너의 e-Seal정보를 EPCIS에 캡처링하게 된다.

차량에 실린 컨테이너 e-Seal를 컨테이너 야드 게이트에서 읽어 EPCIS에 캡처링한다. 포워더를 통해 컨테이너 차량은 이동되고 저장창고 게이트 입구와 저장창고 문에서 e-Seal를 읽는다. 이 모든 정보는 일본 EPCIS에 저장된다.

저장창고에서 컨테이너에 실린 화물을 하역 운반하고, 상자와 팔레트의 태그를 읽어 선적통지서와 실제 화물을 확인/확정한다. 상자나 팔레트를 일본 내로 운송할 차량에 적재한다. 차량 문에 e-Seal을 적용한다. 창고 문에서 창고를 나가는 차량을 e-Seal을 통해 확인한다. 화물 인수자의 게이트에서 e-Seal이 읽혀지고, 수송차량이 창고 문에 도착하면 e-Seal통해 확인한다. 차량 문의 e-Seal을 통해 파손여부를 확인한다.

(그림 3)은 국제 물류 수출 프로세스 플로우 상에서 발생할 수 있는 EPCglobal Network 침해 유형을 연관 지어 도식화한 것이다.

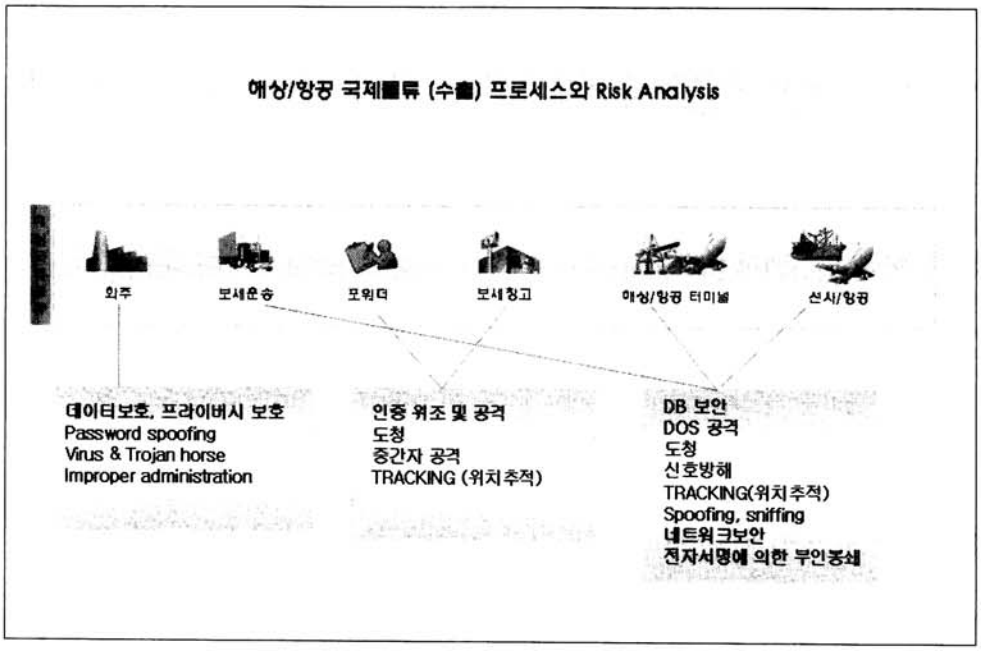
각 프로세스 단계에서 발생할 수 있는 위험요소 및 이에 대한 보안 정책을 기술하면 다음과 같다.

■ 상자 및 팔레트 : 태그 프린팅

태그에 저장된 데이터를 보호하기 위하여 태그에 개인 정보와 같은 프라이버시 침해를 유발할 수 있는 정보를 저장하지 않거나 최소화하여 정보가 유출되었을 때에도 쉽게 식별할 수 없도록 해야 한다. 그리고 태그에 사용되는 식별자 형식을 노출되지 않도록 고유의 방법을 선택해야 공격자가 식별자에 대한 예측을 불가능하게 할 수 있다. 태그에 데이터를 저장하기 전에 패스워드 방식 및 암호화하여 정보의 직접적 접근을 방지해야 한다. 또한 데이터 손실이 발생했을 지라도 데이터를 다시 복구할 수 있도록 백업 시스템을 준비해야 한다. 태그 데이터를 보호하기 위한 방법으로 태그 명령어(command)의 사용을 제한하거나 더 이상 사용하지 않는 태그에 대한 kill feature를 적용하여 정보가 유출될 가능성을 줄이는 것도 보안 위험요소를 방지할 수 있다.

■ 컨테이너(트럭차량): e-Seal

물류는 운송중일 때 보안에 가장 취약한 점이 있기 때문에 더욱 주의해야 한다. DOS 공격이나 인증되지 않는 사용



(그림 3) 수출 프로세스 플로우 상에서의 보안 위협 요소

자의 접근 및 위치 추적 등과 같은 보안 위협요소들을 방지할 수 있는 보안 정책이 필요하다. 이를 위해 공격 가능한 거리를 예측하여 추가적인 장비 보안 및 위치 추적이 가능하지 않도록 주기적으로 태그의 지속적인 존재와 동작 상태를 모니터링 하는 방법들이 필요하다.

■ 포워더

물류의 수출과 수입에 있어 제 3자에 해당하는 포워더에 관한 보안 정책으로는 정보의 접근 범위 및 운송 정책에 대한 기밀 보안 사항을 유지할 수 있도록 MOA(Memorandum Of Agreement) 또는 MOU(Memorandum Of Understanding)에 대한 약정의 협약이 필요하다. 그리고 제 3자 기업체의 직원들의 보안 정책들을 잘 숙지하고 있는지 점검을 수시로 해야 정보 유출을 예방할 수 있다.

■ 통합창고 : 게이트

물품을 보관하는 통합창고에서는 물리적인 접근 제어를 최소화 하기 위해 전파 범위에 전자기의 보호(electromagnetic shielding) 장치 및 접근을 제한할 수 있는 방법을 마련하는 것이 필요하다. 즉, RF 신호를 보호구역 외로 전파되는 것을 방지할 수 있도록 하여 외부로부터 태그와 관련된 동작 자체를 차단시킬 수 있는 electronic shielding과 같은 방법들의 적용 가능성을 고려하는 정책이 필요하다. 그리고 추가적인 보안 방법으로 태그를 비활성화 하여 태그와의 전자적 통신을 통해 물품 정보가 공격받지 않도록 미리 예방하는 정책이 필요하다.

■ 항구터미널 및 선박 : 컨테이너 적재

항구 터미널에서는 선박에 물품을 적재하는 물품 이동 과정을 수반하므로 접근이 허용된 사용자에 한해서만 물품의 운반 과정에 참여해야 하고, 보안 정책에 준하는 행동이 잘 지켜지고 있는지 모니터링 해야 한다. 또한 보안 정책에 위반하는 행동 및 물품의 적재 방법이 발견되었을 때 즉시 위반 사항을 보고하고 이를 통제 및 확인하는 절차가 빠르게 이루어질 수 있도록 사전에 시스템 및 물품 수송과 관련된 직원들의 임무를 분담하고 직원간에 상호감시를 하도록 하는 철저한 교육이 필요하다.

국제 물류의 프로세스 플로우상에서 발생할 수 있는 위험요소 및 보안 위협에 대비하기 위해서는 각 단계별에서의 태그 타입과 사용 주파수 그리고 네트워크상에서 이루어지는 시스템 인증 및 사용자 인증에 대한 보안 요구사항을 시스템 분석과 네트워크를 동시에 고려하는 다양한 측면에서의 철저한 준비가 요구된다.

5. 국제 물류 서비스를 위한 보안 모델

역할 기반 접근 제어의 기본 개념은 사용자(U), 역할(R), 권한(P)으로 구성된다[12-14]. 이 장에서는 국제 물류 서비스를 위한 RBAC 기반의 보안 모델과 접근제어의 제약조건을 UML로 표현한다.

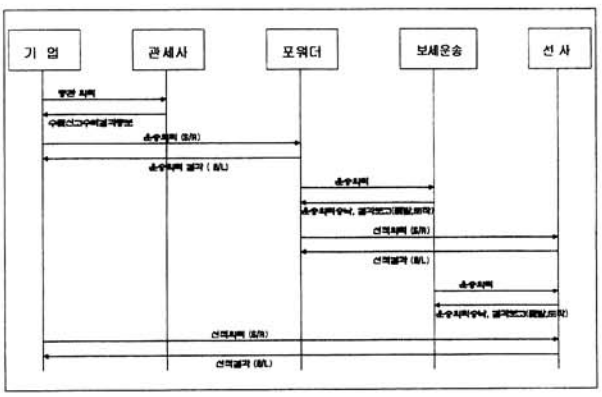
5.1 RBAC 기반 보안 모델

RFID 기반의 국제 물류 프로세스 시퀀스 다이어그램은 다음의 (그림 4)와 같은 흐름을 갖는다. 그리고 EPCglobal Network 상에서의 물류 정보 보안을 위한 흐름은 (그림 5)와 같이 각 기관별 EPC IS를 통해 전달되어온 정보를 사용자 인증 및 역할 권한에 따른 인증을 통해 연동으로 처리되는 형태이다. 이와 같은 인증 관계를 토대로 각 단계별 사용자 및 역할에 대한 인증 및 제약 조건을 모델링해야 한다.

RBAC을 적용한 보안관리는 방대한 네트워크 환경에서 복잡한 권한 부여를 단순화함으로써 보안 관리에 드는 비용과 시간을 감소시켜준다. RBAC을 EPCGlobal Network 에 적용하기 위해서는 다양한 상업적, 이질적 환경에서의 역할(Role)과 타스크(Task)에 관한 설계 및 다양한 조직의 보안 정책을 반영할 수 있도록 하는 유연성이 필요하다.

다음 <표 1>은 제안한 모델의 구성요소에 대한 정의이다.

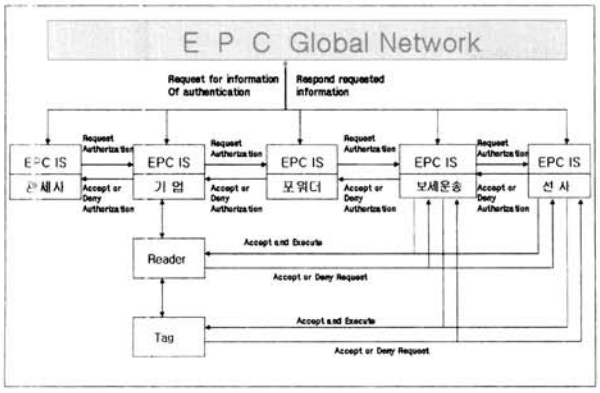
국제 물류 서비스 플랫폼에서 적용하기 위해서는 비즈니스 파트너를 안전하게 수용할 수 있는 역할과 권한 관리 및 사용자 관리가 강화된 RBAC 모델을 설계하였다. 기존의 관



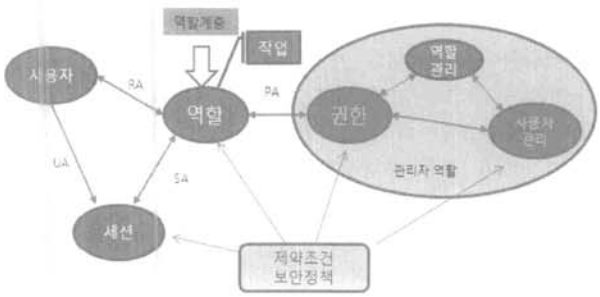
(그림 4) 국제 물류 프로세스 시퀀스 다이어그램

〈표 1〉 제안모델의 구성요소 정의

U(User) : 사용자 집합
R(Role) : 역할 집합
T(Task) : 작업집합 단, 역할은 작업으로 구성가능
P(Permission) : 권한 집합(read, write, execute, append, delete, update)
S(Session) : 세션 집합
C(Constraints) : 제약조건 집합
SP(Security Policy) : 보안정책 집합
MR(Manager Role) : 관리자 역할
RH(Role Hierarchy) : 역할 계층
UA : 사용자 할당
PA : 권한 할당
SA : 세션할당
RA : 역할 할당
TA : 작업할당



(그림 5) EPCglobal Network 상에서의 상호인증 관계



(그림 6) RBAC에 기반한 강화된 보안 모델 설계

리자 역할에서의 보안 관리를 수행한 것과 유사하게 권한 생성 및 역할 생성 사용자 생성 및 역할 관리 등 보안관리 기능을 세분화하였다.

(그림 6)은 Role Engineering을 기반으로 한 국제물류서비스 플랫폼을 위한 확장된 RBAC 모델이다. 이 모델은 강화된 관리자역할과 함께 제약조건과 보안정책을 모든 구성요소에 적용할 수 있도록 정책 반영 기능을 한층 강화하여 물류 환경에서의 상황변화에 따른 유연성과 적응성을 유도하였다. 특히 물류 환경은 이해관계에 따라 비즈니스 파트너의 접근제어가 허용되거나 금지될 수 있어 이러한 상황변화에 따른 보안정책 변경을 보안모델에 신속하게 반영하기 위해서이다.

관리 사용자지정, 관리 역할, 관리 권한지정, 관리권한 등은 보안 관리를 위한 관리목적의 구성요소들이다. 제안 모델은 EPC IS 역할을 수행하는 엔터프라이즈 서브시스템에서 접근제어를 위해 구현되어 물류환경에서의 조직의 물류정보와 사용자정보 보호를 위해 활용되어질 수 있다. 또한 다양한 보안정책을 기술하고 이를 수행시키기 위한 보안모델의 일반화된 기술사항이다.

기술된 보안정책은 시스템 관리자 절차를 통해서 구현가능하며, 수립된 보안정책들은 정보처리시스템(IT시스템)의 적절한 부분으로 각각 구현될 수 있어야 한다. 보안도구에 의해서 적절히 권한을 가지고 실행될 수 있어야 하며 변화에 따른 정책의 갱신 메커니즘과 특정 하드웨어 소프트웨어 독립적 수립이 보장되어야한다. 또한 정보처리시스템에 구현된 보안정책 외에 외부 환경적 요소에서의 수행과 실행 등의 올바른 보안정책이행과정이 있어야 보안의 확실성을 보증할 수 있다.

5.2 RBAC 기반 접근제어 제약의 UML 표현

RBAC 정책을 명세하기 쉽고 편리한 모델링 언어인 UML을 이용하면 응용프로그램 설계 모델에서 조직화되고 체계화된 방법으로 RBAC 정책을 표현할 수 있어 유용하다 [17, 18].

(그림 7)은 RBAC 모델 기반의 보안 정책에 대한 오브젝트 다이어그램으로 사용자, 역할, 권한, 세션, 역할계층 등의 기본 구성요소와 제약조건인 정적의무분리정책, SSD(Static Separation of Duty)와 동적 의무분리정책, DSD(Dynamic Separation of Duty)를 나타내고 있다. 국제 물류 프로세스 상에서 기업에서 의뢰해야 할 통관, 운송, 선적에 대한 역할 관계를 나타낸다. UML다이어그램은 유즈케이스, 클래스 다이어그램, 시퀀스 다이어그램, 오브젝트 다이어그램 등으로 표현되며 이들 다이어그램에 역할 기반 접근 제어 요구사항 및 제약조건, 보안정책을 유도할 수도 있다.

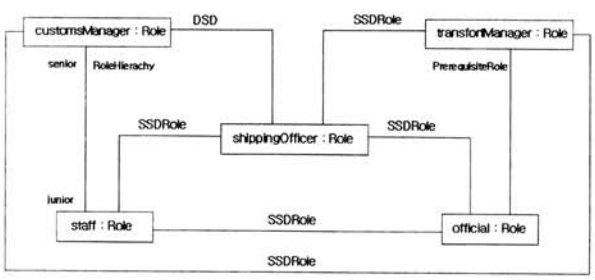
역할기반 접근제어모델인 RBAC 의 효용성을 극대화하기 위해서는 역할 계층, 퍼미션, 역할 퍼미션 할당, 제약조건 등 RBAC 구성요소들을 개발하기 위한 역할 엔지니어링 분야가 요구되어진다.RBAC 시스템에서 역할, 역할 계층, 퍼미션, 제약조건 등의 구성요소들을 모델링 언어로 표현할 수 있다. 역할 엔지니어링이란 RBAC 모델의 구성요소들을 설계하는 것이며 특정 조직의 정책을 바르게 표현할 수 있도록 구성하는 것이다.

의무분리 제약은 정책의 충돌을 예방하기 위해 사용된다. 정적 의무분리(SSD) 제약은 사용자가 충돌되는 역할과 관계된 퍼미션을 획득할 때 발생하는 충돌의 예방을 목적으로 한다. SSD-Role 제약은 OCL(Object Constraint Language)를 사용하여 다음과 같이 표현된다.

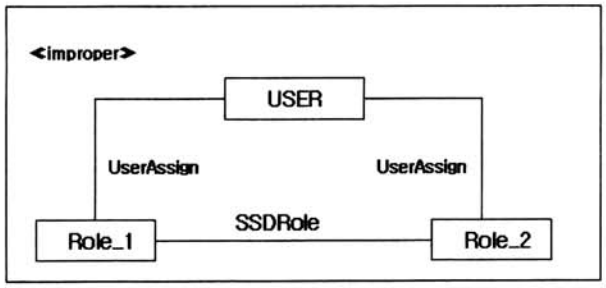
● SSD-Role 제약 : 충돌되는 역할을 같은 사용자에게 할당할 수 없다.

```
context SSDRole:
        Role_1.User → excludesAll(Role_2.User)
```

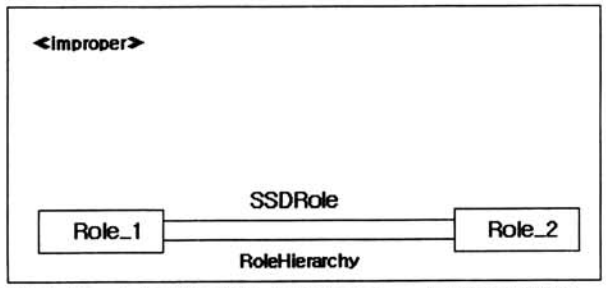
이러한 SSD-Role 제약 조건에 대한 위반을 (그림 8)과 같이 오브젝트 다이어그램을 사용하여 나타낸다.



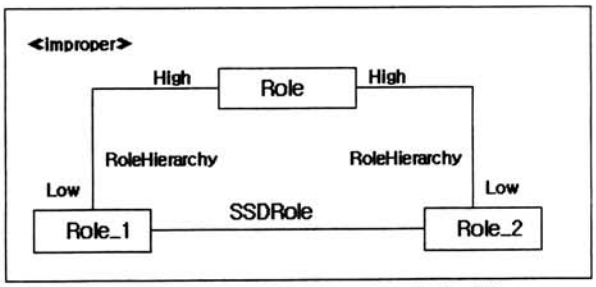
(그림 7) RBAC 모델 기반 보안 정책의 Object Diagram



(a) SSD-Role constraint의 role에 사용자를 할당하는 위반



(b) Role Hierarchy에 의한 두 개의 role이 SSD-Role constraint와 연관된 위반



(c) SSD constraint의 두 개 role이 같은 상위 role을 갖는 위반

(그림 8) SSD Role 제약 위반에 대한 Object Diagram

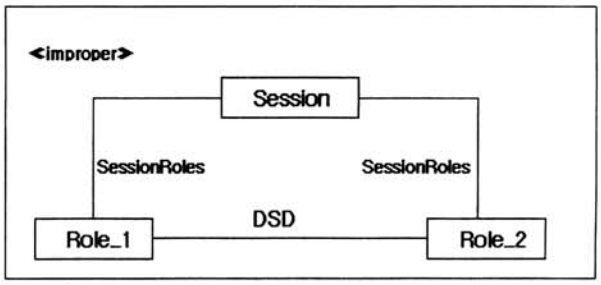
동적 의무분리(DSD) 제약은 같은 사용자 세션에서 활성화될 수 있는 역할에 제약을 두는 것이다. 즉, DSD constraint의 일부에 있는 역할이 활성화되면 사용자는 같은 세션에서 충돌되는 다른 역할을 활성화시킬 수 없게 한다. DSD 제약은 OCL를 사용하여 다음과 같이 표현된다.

● DSD constraint : 충돌되는 역할을 같은 세션에서 활성화될 수 없다.

context DSD:
Role_1.Session → excludesAll(Role_2.Session)

(그림 9)는 DSD 제약조건 위반의 예를 오브젝트 다이어그램으로 보여준다.

UML로 RBAC 모델을 명백하게 표현하는 것이 가능하지만 취약점도 존재한다. 먼저 용어에 있어서 명확한 구분이 필요하며 UML에서는 추상 클래스가 존재할 수 있으나 추상 패키지는 없으며 UML에서의 일반화를 위한 화살표와 응용 키 계층(Application Key Hierarchy)에 사용된 화살표는 의미하는 바가 서로 다르다. 또한 제약조건의 기술이 미약하므로 추가적인 확장이 필요하다.



(그림 9) DSD constraint 위반에 대한 Object Diagram

6. 결 론

최근 RFID기반 물류 환경은 비즈니스 효율성을 대폭 개선할 수 있을 뿐만 아니라 제품의 제조 유통과정에서 제품과 제품의 정보에 대한 가시성과 제품의 무결성을 확보할 수 있게 한다. 그리고 업무의 효율성이 향상되며, 물류 통합 서비스 플랫폼에서의 효과적인 재고관리는 물론 제품 추적이 가능하여 제품 무결성과 과잉재고방지, 제품 손실율을 줄일 수 있게 되었다. 그러나 RFID기반의 국제 물류 서비스 플랫폼에서의 효율적인 물류처리 서비스에서는 물류 정보의 보안 문제를 해결하기 위해 보안 위험 요소를 분석하고 이에 대한 보안 모델이 필요하다. 따라서 이 논문에서는 RFID 기반의 국제 물류 서비스를 위한 기반 연구로써 보안 요구사항을 분석하여 기술하였고, 물류 프로세스 플로우 상에서 발생할 수 있는 단계별 보안 위협 사항에 대한 보안 요구사항 및 국제 물류 프로세스 상에서의 보안 요구사항을 반영할 수 있는 RBAC 기반의 보안 모델을 제시하였다. 그리고 접근 제어의 제약조건을 UML로 표현하였다. 향후 연구에서는 제안한 역할기반의 보안모델을 구현할 수 있는 상세한 모델 설계 및 효율성을 검증하기 위한 연구가 지속적으로 수행될 것이다.

참 고 문 헌

[1] 대한상공회의소, "http://scm.korcham.net/download/SCM_guide.pdf, 2005
[2] 안규희, 이기열, 정목동, "RFID 애플리케이션을 위한 엔터프라이즈 애플리케이션 프레임워크와 비즈니스 프로세스 모델," 한국정보과학회 가을 학술 논문집, 제 33권 제2호, 2006.10
[3] 최길영, 성낙선, 모희숙, 박찬원, 권성호,"RFID 기술 및 표준화 동향," 전자통신동향분석 제22권 제3호, 2007. 6
[4] 산은경제연구소. "RFID산업의 동향과 전망," 2007.09
[5] EPCglobal. "The EPCglobal architecture framework final version," July 1,2005
[6] EPCglobal. "EPC Information Services(EPCIS) Version 1.0 Specification," April 12, 2007
[7] EPCglobal. "Object Naming Service(ONS) Version 1.0," October 4,2005

[8] EPCglobal, "EPCglobal Tag Data Standard Version 1.3 Ratified Specification," http://www.epcglobalinc.org, March 8, 2006.

[9] EPCglobal, "Reader Protocol Standard, Version 1.1 Ratified Standard," http://www.epcglobalinc.org, June 21, 2006.

[10] NIST(National Institute of Standards and Technology). "Guidelines for Securing Radio Frequency Identification System," April, 2007.

[11] EPCglobal, "EPCglobal Data Exchange Joint Discussion Group," September 19, 2006.

[12] A Basic Introduction to RFID Technology and Its use in the Supplychain, http://www.printronix.com/uploadedFiles/Laran_WhitePaper_RFID.pdf,January2004

[13] N.Mayer, A. Rifaut and E.Dubois, "Towards Risk-Based Security Requirements Engineering Framework," In Proceedings of the 11the International Workshop on Requirements Engineering: Foundation for Software Quality, 2005.

[14] L.Liu, E.S.K.Yu and J.Mylopoulus, "Security and Privacy Requirements Analysis within a Social Setting," In Proceedings of the 11the IEEE International Workshop on Requirements Engineering Conference, 2003.

[15] S.Lee, R.Gandhi and G.Ahn "Security Requirements Driven Risk Assessment for Critical Infrastructure Information Systems," In Proceedings of the 3rd Symposium on Requirements Engineering for Information Security, 2005.

[16] A. Poniszewska-Maranda, "Role Engineering of information system using extended RBAC," In Proceedings of the 14th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise, WETICE 2005.

[17] P. Epstein, R. Sandhu, "Toward A Uml Based Approach to Role Engineering," In Proceedings of the fourth ACM workshop on Role-based access control table of contents, 1999.

[18] I. Ray, N. Li, R. France, "Using UML To Visualize Role-Based Access Contol Constraints," In Proceedings of the ninth ACM symposium on Access control models and technologies table of contents, 2004.

황 정 희

E-mail : jhhwang@nsu.ac.kr

1991년 충북대학교 전산통계학과(이학사)

2001년 충북대학교 전자계산학과(이학석사)

2005년 충북대학교 전자계산학과(이학박사)

2001년~2005년 정우씨스템(주) 연구소장

2006년~현 재 남서울대학교 컴퓨터학과 전임강사

관심분야 : XML 및 웹 데이터베이스, 스트림 데이터 관리, 데이터 마이닝, 유비쿼터스 컴퓨팅, 시공간 데이터베이스, RFID 보안

신 문 선

E-mail : msshin@kku.ac.kr

1987년 충북대학교 전산통계학과(학사)

1997년 충북대학교 전자계산학과(석사)

2004년 충북대학교 전자계산학과(박사)

2005~현 재 건국대학교 컴퓨터시스템학과 강의교수

관심분야 : 데이터베이스, 데이터마이닝, 센서네트워크, RFID보안

이 종 연

E-mai : jongyun@chungbuk.ac.kr

1985년 충북대학교 전자계산기공학과(공학사)

1987년 충북대학교 전자계산기공학과(공학석사)

1999년 충북대학교 전자계산학과(이학박사)

1989년 비트컴퓨터(주) 개발부

1990년~1994년 현대전자산업(주) 소프트웨어연구소 주임연구원

1994년~1996년 현대정보기술(주) CIM사업부 책임연구원

1999년~2003년 삼척대학교 정보통신공학과 조교수

2003년~현 재 충북대학교 컴퓨터교육과 부교수

관심분야 : 질의 최적화, 시공간 데이터베이스, Ubiquitous Computing, u-learning, RFID 보안, GIS

황 익 수

E-mail : ishwang@ktnet.co.kr

1984년 세종대학교 경영학과(학사)

1993년 한국외국어대학교 무역대학원 정보관리학과 수료

1990년~현 재 한국무역정보통신 근무

2005년 eBiz사업본부장

2008년 전자무역사업본부장

2008년 지식경제부 성장동력기술개발사업 'RFID기반 국제물류 통합 Platform 기술개발' 총괄책임자

관심분야: 정보관리, EPCGlobal network, RFID기반 국제물류 시스템