RFID 기반 정보시스템을 위한 보안감리 점검항목

임지영*○, 김동오**, 한기준**

*KOSCOM, **건국대학교 정보통신대학교 강의교수,
***건국대학교 정보통신대학교 교수

Security Audit Checking Items for the RFID-Based Information Systems

Lim, Ji-Young, Kim, Dong-Oh, Han, Ki-Joon
KOSCOM, Konkuk University, Konkuk University
E-mail : jylim@koscom.co.kr, dokim@db.konkuk.ac.kr, kjhan@db.konkuk.ac.kr

요 약

유비쿼터스 시대의 핵심 기반기술인 RFID와 관련하여 공공기관을 중심으로 시범 사업 및 본 사업이 활발하게 추진되고 있다. 또한 RFID 기반 정보시스템에 대한 감리 수요도 계속 증가하고 있으며, 특히 개인정보보호에 대한 관심이 확산되면서 보안감리의 비중도 높아지고 있다. 이와 관련하여 RFID 기반 정보시스템의 사업특성을 적절히 반영한 보안감리 점검항목이 요구되고 있다. 따라서 본 논문에서는 현행 RFID 기반 정보시스템에 대한 감리를 보다 체계적이고 효율적으로 수행하는데 활용될 수 있는 RFID 사업특성기반의 보안감리 점검항목을 제안한다.

1. 서론

정보통신기술의 발전과 더불어 유비쿼터스 환경이 실생활 곳곳으로 확산되는 가운데에 사물과 사물, 사물과 사람을 연결해 주는 RFID(Radio Frequency IDentification) 기술이 유비쿼터스 사회의 핵심으로 자리 잡고 있다(김도훈, 2003). RFID 기술은 이미 오래 전부터 물류 관리, 교통요금 징수 등에 사용되어 왔으나 최근 태그의 소형화, 인식률 향상, 가격 하락 등으로 인하여 그 활용범위가 급속하게 확산되고 있다(오경희 외, 2006).

이러한 시점에 2006년 "정보시스템의 효율적 도입 및 운영 등에 관한 법률"의 시행으로 공공기관을 대상으로 정보시스템 구축에 대한 감리가 의무화되었으며(정보통신부, 2005a), 이에 따라 다양한 사업 분야에서 감리가 활발하게 이루어지고 있다.

특히 공공기관을 중심으로 여러 유비쿼터스 사업이 활발하게 진행됨에 따라 RFID 기반 정보시스템에 대한 감리 수요도 증가하고 있는데, RFID와 같은 신기술을 적용한 정보시스템에 대한 감리 시에는 RFID 사업의 특성을 반영한 감리 점검체계 즉, 사업특성기반 감리 점검체계를 적용하여야 한다(한국정보사회진흥원, 2007).

또한, RFID 기술의 특성상 기록된 정보를 제3자가 판독할 수 있고 장기적으로 태그정보와 연동된 데이터베이스를 축적·이용할 수 있다는 점에서 정보의 침해 가능성이 제기됨에 따라 RFID 기반 정보시스템의 분석·설계 단계에서부터 정보보호 요구사항 및 기능을 고려하는 정보시스템 보안감리에 대한 필요성이 증가하고 있다(전상덕, 2007).

따라서 본 논문에서는 RFID 기반 정보시스템 구축 사업의 안전성 및 신뢰성을 확보하기 위한 체계적이고 효율적인 감리를 위해 RFID 사업의 특성을 반영한 보안감리 점검항목을 제시하는데 그 목적이 있다.

2. 관련 연구

2.1. RFID 기반 정보시스템의 특성

RFID 기반 정보시스템은 일반적으로 태그, 리더, 네트워크, 플랫폼(미들웨어), 응용 서비스로 구성된다(이재호 외, 2004). 태그(Tag)는 데이터를 저장하는 RFID의 핵심기능을 담당하며 리더의 질의에 대하여 사물, 사람 등의 식별 정보를 무선 통신을 사용하여 전송하는 장치이다. 리더(Reader)는 태그 인식 및 태그 데이터를 수신하거나 태그에 정보를 다시 쓰는 역할을 수행하는 장치이며, 리더가 받은 정보는 네트워크 및 플랫폼을 통하여 데이터베이스에 전송된다.

RFID 기반 정보시스템은 기존의 정보시스템 구축절차인 ISO12207 규정을 따르거나 일반적인 정보시스템 개발방법론을 따르며, 구축되는 환경에 따라 각 과정별로 절차를 조정할 수 있다. RFID 기반 정보시스템의 구축은 일반적으로 비즈니스 및 요구사항 모델링, 아키텍처 및 설계, 개발 및 테스트, 인도 및 유지보수, 프로젝트 관리의 과정으로 진행된다(정보통신부, 2007).

2.2. RFID 기반 정보시스템의 보안위협요소

RFID 기술은 활용 가능한 범위가 넓고 실제 적용되어 사용되고 있는 상황이지만, RFID에 기록된 정보를 제3자가 판독할 수 있고 장기적으로 태그 정보와 연동된 데이터베이스를 축적·이용할 수 있다는 점에서 정보의 침해 가능성이 제기되고 있다(한국정보사회진흥원, 2004a). 또한, 리더와 태그 간에 주로 무선통신을 사용하는 특성으로 인하여 [표 1]과 같은 문제점 및 침해유형이 야기된다.

[표 1] RFID 기반 정보시스템에서의 문제점 및 침해유형

구분	내용
발생 가능한 문제점	-RFID 정보를 이용한 개인 신상정보 노출 -RFID 정보를 활용한 개인의 물품보유현황 노출 -RFID 인식 기술을 이용한 위치정보 노출 -RFID 정보가 상품에 활용될 때 개인의 구매 패턴 및 선호도 노출 -타 정보와 결합을 통한 개인정보화
태그 정보의 침해 유형	-부적절한 RFID 정보의 접근과 수집 -부적절한 RFID 정보 분석 -부적절한 RFID 관련 정보의 이전 -RFID 태그정보를 활용하여 원하지 않는 영업행위

RFID 기반 정보시스템의 프라이버시 보호를 위한 보안 기술은 크게 태그의 개인정보 유출 방지 및 태그와 리더 사이에서 도청 등의 공격으로부터 보호하기 위한 인증 기술과 리더가 포함된 네트워크 보호를 위한 인프라 기술로 구분할 수 있다.

2.3. 정보시스템 보안감리

정보시스템 보안감리는 현재 정보시스템 감리기준(정보통신부, 2006a), 정보시스템 구축운영 기술지침(정보통신부, 2006b), 정보시스템 개발방법론(시스템 구축 사업자의 개발방법론 등) 등을 기본적으로 적용하며, 여기에 부가적으로 필요에 따라 정보통신기반보호법(정보통신부, 2002), 정보시스템 구축단계별 정보보호 가이드라인(한국정보사회진흥원, 2004b) 등을 준용한다.

2.4. RFID 관련 국내·외 보안 가이드라인

2.4.1 NIST의 RFID 보안 가이드라인

미국의 표준기술연구소(NIST, National Institute of Standards and Technology)는 RFID 사용 안내 및 모범사례 보고서를 발표하였다(NIST, 2007).

각각의 RFID 기술들은 그 구성요소가 상이하고 상업화를 위한 응용방법들이 다양하며, 보안위험과 이를 통제하기 위한 방법들이 매우 다양하므로 NIST는 RFID 기술을 구현하는데 필요한 공통적인 IT 요소들(서버, 데이터베이스, 네트워크 등)의 통제 및 관리를 통해 보안문제를 해결하기 위하여 RFID 시스템 보안 관련 가이드라인을 제시하였다.

주요 RFID 보안 권고 사항은 방화벽 설치, 라디오 신호의 암호화, 승인된 RFID 사용자들에 대한 인증, 태그의 은폐, 보안감사 절차의 채택, 태그에 저장되는 민감한 데이터의 최소화 등이다.

2.4.2 정통부 RFID 프라이버시 보호 가이드라인

정보통신부에서는 안전한 RFID 이용환경 조성을 위해 RFID 프라이버시 보호 가이드라인을 발표하였다(정보통신부, 2005b). RFID 태그를 통해 직접 개인정보를 수집하거나 RFID를 통하여 수집한 물품정보와 개인정보를 연계하는 등 RFID 시스템을 이용한 개인 프라이버시 침해의 경우를 대비하며 RFID 태그, 리더기를 비롯한 전체 시스템을 취급함에 있어 준수해야 할 기준을 제시하였다.

3. RFID 기반 정보시스템의 보안감리 점검항목

3.1 RFID 기반 정보시스템의 보안감리 점검항목 도출

NIST RFID 보안 가이드라인의 보안 권고사항과 단계별 RFID 보안 체크리스트의 요소를 중심으로 하여 RFID 시스템의 적절한 보안 통제 수단 강구, RFID 실행과 관련된 다양한 위험 통제, RFID의 기술적 보안 통제 관리방법 선택 등 주요 보안 권고사항 및 추천 요소, 필수 고려 요소를 중심으로 RFID 기반 정보시스템의 보안감리 점검항목을 도출하였다.

정보통신부의 RFID 프라이버시 보호 가이드라인에서 RFID 시스템의 개인정보보호를 위한 관리적·기술적 보호 조치사항을 주안점으로, 관리절차 및 지침 마련, 보안대책 및 발생 시 대응지침 마련 등의 요구사항에 대하여 보안정책 수립 및 보안대책의 적정성, 보안 상세설계의 적정성 등과 같은 보안감리 점검항목을 분석・설계・시험・구현 등 각 시점 별로 도출하였다.

RFID 기반 정보시스템은 크게 태그, 리더, 네트워크, 플랫폼(미들웨어), 응용 서비스로 구성되어 유·무선 통신과 연동되어 사용되므로 이 과정이 올바르게 이루어지기 위해서는 데이터 전송에 있어서 위변조를 막아 데이터가 안전하게 전송되어야 한다. 이러한 RFID 기반 정보시스템의 특성상 발생할 수 있는 위협사항들을 중심으로 보안감리 점검항목을 도출하였다.

또한, RFID 기반 정보시스템의 특성상 여러 가지 위협요소에 노출되기 쉬우며 이로 인하여 여러 가지 문제점이 발생하게 된다. 따라서 RFID 기반 정보시스템에서 발생할 수 있는 보안위협 요소들과 이에 대한 대처방안이 적정하게 수립되었는지를 중심으로 보안감리 점검항목을 도출하였다.

3.2 RFID 기반 정보시스템의 보안감리 점검항목 제안

본 논문에서는 RFID 기반 정보시스템 및 보안감리의 이론적 연구배경을 토대로 RFID 기반 정보시스템을 위한 사업특성기반 보안감리의 기본 점검항목 및 세부 검토항목을 [표 2]와 같이 제안하며, 세부 검토항목별 상세 내용과 목적 및 필요성, 감리관점 및 기준 등 검토항목별 세부 내용은 페이지 한계로 생략하였다.

[표 2] RFID 기반 정보시스템의 보안감리 점검항목

감리 시점	기본 점검항목	세부 검토항목
분석	RFID 시스템의 보안요구사항 분석 및 도출의 충분성, 적정성	1. RFID 시스템의 보안요구사항이 적절하게 도출되었는가?
	RFID 시스템의 보안정책 수립 및 보안대책의 적정성	2. RFID 시스템의 보안정책이 적정하게 수립되었는가? 3. RFID 시스템의 보안 취약점에 대한 분석 및 체계적인 대응지침이 마련되었는가?
설계	RFID 시스템의 보안에 대한 상세설계의 적정성	4. RFID 시스템의 적용 보안기술의 분석 및 설계를 적정하게 수행하였는가?
	RFID 적용 보안기술에 대한 현장 실증 계획 수립여부	5. RFID 적용 보안기술에 대한 현장 실증실험(검증)을 위한 계획이 적정하게 수립되었는가?
구현	RFID 보안솔루션의 설치 및 보안환경 구현의 적정성	6. RFID 시스템의 보안기능 구현 및 각종 보안 Profile 값의 설정이 적정하게 수행되었는가?
	RFID 태그정보 보호의 적정성	7. RFID 태그정보가 적정하게 보호되고 있는가?
시험	RFID 적용 보안기술에 대한 현장 실증실험 실시	8. RFID 시스템의 적용 보안기술에 대한 현장 실증실험을 통하여 보안성 검증이 적정하게 수행되었는가?
전개 (운영준비)	RFID 시스템 감사통제의 적정성	9. RFID 시스템의 보안침해 방지를 위한 감사절차/기록 및 추적기능을 사용하고 있는가?

4. 보안감리 점검항목의 검증

본 논문은 설문을 통한 보안감리 점검항목의 검증을 위해 설문 대상 및 설문지에 대해서 설명하고, 설문 결과 분석을 통해 본 논문에서 제안한 보안감리 점검항목의 실효성을 검증한다. 설문 대상자로 선정하기 위한 모집단은 현 정보시스템 감리기준에 따라 정보시스템 감리업무를 담당하거나 가장 관심이 많을 것으로 여겨지는 감리전문가 120명을 대상으로 하였다.

설문지를 작성하기 위한 준비과정으로 조사 대상인 감리원을 3명 선정하여 준비된 예비 설문지로 사전검사 및 토론을 실시함으로써 실증분석의 토대를 마련하였다. 설문지는 본 논문에서 제시한 보안감리 점검항목으로 구성되었고, 평가 시 Likert의 5점 척도법(5.0: 매우 중요, 4.0: 중요, 3.0: 보통, 2.0: 미흡, 1.0: 부적절)을 사용하였다.

본 논문에서는 RFID 기반 정보시스템의 보안감리 점검항목에 대한 타당성을 검증하기 위하여 설문지의 8개 조사요소에 대한 결과를 분석하였다.

대상 점검항목별로 IT 및 감리경력, 감리경험, 감리사 자격 등 다양한 측면에서 설문조사 결과를 상세하게 분석해 본 결과 [표 3]에서 보여주는 것과 같이 모든 면에서 일관성 있게 긍정적으로 평가한 것으로 조사되었으며, 전체 스케일 5.0 기준일 경우 종합 평균 4.12로 매우 긍정적인 것으로 조사됨으로써 본 논문에서 제안한 점검항목이 매우 실효성 있다고 판단된다.

[표 3] 기본 점검항목별 중요도 평균 점수

기본 점검항목	평균
RFID 시스템의 보안요구사항 분석 및 도출의 충분성, 적정성	4.17
RFID 시스템의 보안정책 수립 및 보안대책의 적정성	4.08
RFID 시스템의 보안에 대한 상세설계의 적정성	3.87
RFID 적용 보안기술에 대한 현장 실증실험 계획 수립여부	4.42
RFID 보안 솔루션의 설치 및 보안환경 구현의 적정성	4.00
RFID 태그정보의 보호의 적정성	4.25
RFID 적용 보안기술에 대한 현장 실증실험 실시	3.94
RFID 시스템 감사통제의 적정성	4.20
종합 평균	4.12

5. 결론

본 논문에서는 현행 RFID 기반 정보시스템에 대한 감리를 보다 체계적이고 효율적으로 수행하는데 활용될 수 있는 RFID 사업특성기반의 보안감리 점검항목을 정보시스템 구축단계(분석, 설계, 구현, 시험, 전개)별 필요에 따라 제안하였다. 또한 본 논문에서 제안한 RFID 기반 정보시스템의 보안감리 점검항목에 대한 설문조사를 통해 점검항목의 타당성 및 중요도 등을 종합적으로 분석함으로써 도출된 점검항목의 실효성을 검증하였다.

본 논문에서는 RFID 기반 정보시스템의 보안감리 시 적절한 기준이 될 수 있는 보안감리 점검항목을 도출 및 제안함으로써 RFID 기반 정보시스템의 안전성 및 신뢰성 보장에 기여하고자 하였으며, 또한 본 논문에서 제시한 점검항목은 앞으로 효율적인 RFID 기반 정보시스템 보안감리를 위해 적절하게 활용될 수 있을 것이라 판단된다.

[참고문헌]

[1] 김도훈 (2005), “u-사회의 역기능과 대응과제, RFID 도입과 프라이버시 문제를 중심으로,” 「Telecommunications Review」, 15(1):117-131.

[2] 오경희・김호원 (2006), “RFID 환경에서의 프라이버시 보호기술,” 「한국통신학회지」, 23(9):103-112.

[3] 이재호 외 (2004), “IT839 전략 기술개발 마스터플랜 - 차세대 이동통신 기술개발 현황 및 전략,” 「정보과학회지」, 23(2):66-76.

[4] 전상덕 (2007), “정보보호 위해 보안감리는 필수,” 「월간 정보보호21c」, 86:86-88.

[5] 정보통신부 (2002), 「정보통신기반보호법, 법률 제6796호」.

[6] 정보통신부 (2005a), 「정보시스템의 효율적 도입 및 운영 등에 관한 법률, 법률 제7816호」.

[7] 정보통신부 (2005b), 「RFID 프라이버시 보호 가이드라인」.

[8] 정보통신부 (2006a), 「정보시스템 감리기준, 정보통신부 고시 제2006-42호」.

[9] 정보통신부 (2006b), 「정보시스템 구축운영 기술지침, 정보통신부 고시 제2006-37호」.

[10] 정보통신부 (2007), 「RFID 적용을 위한 가이드북 - RFID 개요 및 도입절차」.

[11] 정보통신부・한국정보보호진흥원 (2007), 「RFID 프라이버시 보호 가이드라인 해설서」.

[12] 한국정보사회진흥원 (2004a), 「전파식별(RFID) 보급 활성화를 위한 역기능 및 정보보호대책 연구」.

[13] 한국정보사회진흥원 (2004b), 「정보시스템 구축단계별 정보보호 가이드라인」.

[14] 한국정보사회진흥원 (2004c), 「유비쿼터스 컴퓨팅 환경에서 보안 및 인증서비스 방향연구」.

[15] 한국정보사회진흥원 (2007), 「정보시스템 감리점검 해설서 V2.0」.

[16] NIST(National Institute of Standards and Technology), (2007), 「Guidelines for Securing Radio Frequency Identification Systems」, NIST.