韓國IT서비스學會誌
第11卷 第4號
2012年 12月, pp.107-121
http://dx.doi.org/10.9716/KITS.2012.11.4.107

RFID 기반 정보시스템을 위한 보안감리 점검항목 연구*

전상덕** · 임지영*** · 이기영**** · 한기준*****

A Study on Security Audit Checking Items for the RFID-Based Information System

Sang-Duk Jeon** · Ji-Young Lim*** · Ki-Young Lee**** · Ki-Joon Han*****

■ Abstract ■

The core infra-technology in the ubiquitous era, RFID which has taken action from the public institution with the pilot projects as well as the practical projects is gradually extending its spectrum to the private enterprises. Along with its expansion, the audit required on the RFID-based information system is also growing in the industry. Especially, since RFID-based information systems, especially compared to other information systems, are likely to be exposed to many threats, the security audit for them is being emphasized. This paper suggests security audit checking items for the RFID-based information system, which can be used to perform the efficient security audit. The security audit checking items consist of eight basic checking items, each of which consists of detailed review items and can be applied for each building steps of the system(analysis, design, implementation, testing, and development). Finally, this paper confirmed the efficiency of the security audit checking items proposed in this paper through survey by the experienced auditors and analysis of practical audit cases.

Keyword : RFID, Information System Audit, Security Audit, Checking Items, Review Items

논문투고일 : 2012년 10월 26일 논문수정완료일 : 2012년 12월 10일 논문게재확정일 : 2012년 12월 12일
* 본 연구는 중소기업청에서 지원하는 2012년도 산학연공동기술개발사업(No. C0027296)의 연구수행으로 인한 결과물임을 밝힙니다.
** 김앤장 포렌식팀 전문위원, 책임저자
*** (주)코스콤 대외협력부 팀장
**** 을지대학교 의료IT마케팅학과 교수
***** 건국대학교 컴퓨터공학부 교수, 교신저자

1. 서 론

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[4, 5]. 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 있으며 관련 연구도 활발하게 이루어지고 있다[3, 6, 20, 29].

이러한 시점에 2006년 “정보시스템의 효율적 도입 및 운영 등에 관한 법률”[13]의 시행으로 공공기관을 대상으로 감리 의무화가 시행되었으며, 관련 사업에 대한 감리가 활발하게 이루어지고 있다. 현재 국내에서 이루어지고 있는 정보시스템 감리는 공공부문에서 사업유형기반의 감리 점검체계 적용을 위주로 실시되고 있으나 최근 RFID 기반 정보시스템(이하 “RFID 시스템” 혼용 사용) 구축 사업 추진으로 사업특성 기반의 감리 점검체계를 적용해야 하는 대상사업이 대폭적으로 증가할 것으로 예상된다.

그동안 공공부문 정보화 사업에 대한 정보시스템 감리는 감리시행 회수의 증가라는 양적 성장과 더불어 관련 연구가 체계적으로 이루어져 왔다[22, 26]. 그러나 RFID 기반 정보시스템 구축 사업에 대한 감리는 감리시행 횟수가 증가하고 있음에도 불구하고 기존의 사업유형기반 감리 점검체계 하에서 RFID 특성이 반영된 부분에 감리원 개개인의 경험과 지식에 의존한 점검항목에 의해 감리가 수행되어 왔으며 그에 따라 RFID 특성에 적합한 사업특성기반 감리 점검체계의 필요성을 절실하게 인식하게 되었다[8, 9].

따라서 본 논문은 RFID 기반 정보시스템 구축 사업의 안전성 및 신뢰성 확보를 위해 체계적이고 효율적인 감리수행을 위해서 RFID 기반 정보시스템의 보안위협 요소와 기존에 제시된 국내외 RFID 보안 관련 문서에 대한 분석 고찰을 통해 효율적인 보안감리 점검항목을 제시하는데 그 목적이 있다. 즉, 본 논문은 RFID 기반 정보시스템 구축 사업의 안전성 및 신뢰성을 보장할 수 있는 효율적인 감리 수행을 위해 RFID 사업특성기반의 점검항목 중 보안영역의 감리 점검항목에 대한 연구를 대상으로 하였다.

연구 방법은 RFID 기반 정보시스템의 보안위협 요소와 국내외 RFID 보안 관련 가이드라인에 대한 조사 및 분석을 실시하였고[14, 16-18, 31], 또한 이렇게 분석한 결과를 바탕으로 RFID 특성을 반영한 보안감리 점검항목을 도출하였다. 그리고 감리 전문가의 설문조사 및 감리사례 분석을 통하여 해당 연구결과에 대한 실효성을 검증하였다.

본 논문의 구성은 다음과 같다. 제 2장에서는 정보시스템 보안감리에 대해서 기술하고, RFID 기반 정보시스템의 보안위협 요소와 국내외 RFID 보안 관련 가이드라인에 대해서 분석한다. 제 3장에서는 제 2장에서 분석한 내용에 대한 고찰을 통해 RFID 기반 정보시스템의 보안감리 점검항목을 제안한다. 제 4장에서는 설문조사 및 감리사례 분석을 통해서 본 논문에서 제안한 보안감리 점검항목의 실효성을 검증하고, 마지막으로 제 5장에서 결론에 대해 기술한다.

2. 관련 연구

2.1 정보시스템 보안감리

“정보시스템 감리”라 함은 감리발주자 및 피감리인의 이해관계로부터 독립된 자가 정보시스템의 효율성을 향상시키고 안전성을 확보하기 위하여 제 3자적 관점에서 정보시스템의 구축 및 운영에 관한 사항을 종합적으로 점검하고 문제점을 개선하도록 하는 것을 말한다[27].

공공기관 정보시스템 감리 의무화를 통해 감리를 보다 체계적으로 수행하기 위하여 제정된 “정보시스템의 효율적 도입 및 운영 등에 관한 법률”[13]은 2010년 2월에 폐지되고 대신하여 “전자정

부법"[28]이 제정되었다. 그리고 2010년 12월 전자정부법 제57조 제5항에 따라 새로운 정보시스템 감리기준(행정안전부고시 제2010-85호)[27]이 고시되어서, 감리업무를 수행하는 자는 이것을 준수하여야 하며, 공공기관의 장은 감리결과를 해당 정보시스템에 반영하여야 할 의무를 가지게 되었다.

정보보호란 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적·기술적 수단(정보보호 시스템)을 강구하는 것을 말하며, 일반적으로 정보자산을 공개/노출, 변조/수정, 지체/재난 등의 위협으로부터 보호하여 정보보호의 3요소인 정보의 기밀성, 무결성, 가용성을 확보하는 것을 말한다[23].

정보시스템 보안감리는 정보시스템의 정보보호 활동 적정성에 대한 감리를 수행하여 정보보호의 취약점 및 위협 요소 등을 개선하여 정보시스템의 안정성을 보장할 수 있도록 한다. 정보보호의 중요성이 점차 증대하는 사회적 요구에 대응하고, 보다 비용 효과적인 정보보호를 구현하기 위해 정보시스템의 개발 단계에서부터 정보보호 요구사항 및 기능이 고려될 수 있도록 정보시스템 보안감리가 필요하다[8]. 정보시스템 보안감리를 통하여 정보시스템의 개발 단계 또는 운영 과정에서 보안과 정보보호에 대한 충분한 고려가 이루어진다면 비교적 적은 비용으로 정보시스템을 안전하게 보호할 수 있을 것이다.

현재 정보시스템 보안감리는 정보시스템 감리기준[27], 정보시스템 구축운영 기술지침[15], 정보시스템 개발방법론(시스템 구축 사업자의 개발방법론 등) 등을 기본적으로 적용하며, 여기에 부가적으로 국가 사이버안전 매뉴얼[1], 정보시스템 구축 단계별 정보보호 가이드라인[24], 웹 서버, 라우터 보안관리 가이드[11, 12], 정보통신기반보호법[10], 정보시스템 보안/통제 감리지침[22], 군사보안업무 시행규칙[2] 등을 준용하고 있다.

2.2 RFID 기반 정보시스템의 보안위협

지식경제부 기술표준원은 RFID 태그 간 호환성 확보, RFID 기기의 품질향상 등을 위해 국가표준인 '정보기술-품목관리용 무선인식(RFID)-구현 가이드라인, 제1부, 제2부, 제3부'를 제시하였다[19]. 구현 가이드라인이란 응용분야별 최적 RFID 시스템 구축에 필요한 주파수 대역, 코드, 설치 및 시험방법 등을 이해하기 쉬운 형태로 규정하여 산업계 확산을 위한 지침서로 사용된다.

제1부는 KS X ISO/IEC18000-6C 지원 무선인식용 라벨에 대한 구현 가이드라인으로 공급망에서 무선 인식용 라벨과 포장의 사용에 대한 가이드라인을 제공한다. 제2부는 재활용과 RF 태그에 대한 가이드라인으로 다양한 재활용 경로들이 재활용된 재료, 특히 유리와 철에 부착된 RF 태그의 재사용 가능성을 시험하고 있다. 제3부는 물류 애플리케이션 UHF 무선인식 호출기 시스템 구현과 운영에 대한 가이드라인으로 KS X ISO/IEC 18000-6C의 무선인식 판독기의 선정, 설치와 애플리케이션에서 참조 정보와 실제적인 지식을 제공하기 가이드라인이다.

RFID 기반 정보시스템은 RFID 기술을 실제 비즈니스 영역에 적용하여 서비스를 제공하는 일련의 시스템으로 정의될 수 있다. 즉, 물품 등 관리할 사물에 태그를 부착하고 전파를 이용하여 사물의 ID 정보 및 주변 환경 정보를 인식하여 각 사물의 정보를 수집, 저장, 가공 및 추적함으로써 사물에 대한 측위, 원격처리, 관리 및 사물간 정보교환 등의 다양한 서비스를 제공하는 것이다. RFID 기반 정보시스템은 크게 태그, 리더, 네트워크, 플랫폼(미들웨어), 응용 서비스로 구성되고, 유무선 통신과 연동된다[7].

RFID 기반 정보시스템은 리더와 태그간에 무선통신을 사용하기 때문에 태그의 고유정보가 무분별하게 전송되는 동작으로 인해 여러 위협에 노출되기 쉽다. 이러한 취약점은 공격자가 기존의 다른 시스템에서 보다 적은 노력으로 원하는 정보를 얻을 수 있게 한다. 특히 RFID 기반 정보시스템에서 공격자들은 리더와 태그간의 도청, 태그 위조 등의 공격을 수행할 수 있으며, 이러한 공격을 통

하여 사용자의 프라이버시를 침해할 수 있다.

그러므로 프라이버시 문제점 및 침해유형을 고려하여 RFID 기반 정보시스템을 구축해야 한다[13, 17, 18]. 특히 고려되어야 할 프라이버시 문제는 RFID 태그를 지니고 있는 개인의 태그 코드 추적을 통해 발생할 수 있는 "RFID 위치추적 프라이버시 문제"와 외부의 RFID 리더를 이용하여 개인 소유물에 대한 연결정보를 열람함으로써 발생하는 "RFID 정보 프라이버시 문제"가 있다[7, 25]. 또한 침해유형으로는 "부적절한 RFID 정보의 접근과 수집", "부적절한 RFID 정보 분석" 등이 있다.

RFID 기술은 활용 가능한 범위가 넓고 실제 널리 사용되고 있지만, RFID는 그 특성상 반도체 칩에 기록된 정보를 제 3자가 판독할 수 있고 장기적으로 태그정보와 연동된 데이터베이스를 이용할 수 있다는 점에서 정보의 침해 가능성이 제기되고 있다. RFID 시스템에서 네트워크 공격으로 부터 보호되지 않는 태그는 도청, 트래픽 분석, 스푸핑, 서비스 거부, 세션 가로채기, 중간자 공격 등의 공격에 취약한 것으로 나타났다[18, 21].

RFID 기반 정보시스템의 보안위협으로부터 보호하기 위한 기술은 크게 태그의 개인정보 유출 방지 및 태그와 리더 사이 도청 공격으로부터 보호하기 위한 인증 기술과 리더가 포함된 네트워크 보호를 위한 인프라 기술로 구분될 수 있다. 또한 보안위협 침해방지를 위한 기법으로는 Kill 명령어 접근법, Blocker 태그 기법[30], 해쉬-락(Hash-Lock) 기법[33], 랜더마이즈드 해쉬-락 기법[33], XOR 기반 원타임 패드 기법[22], 외부 재암호화 기법[22], 해쉬 체인(Hash-Chain) 기반 기법[21, 32] 등이 있다.

2.3 NIST RFID 가이드라인

미국 NIST(National Institute of Standards and Technology)는 RFID 사용에 대한 안내 및 모범사례 보고서를 발표하였다[31]. 이 보고서는 RFID 기술에 대한 개략적인 설명과 더불어 RFID 기술관련 보안과 사생활 침해 위험을 극복하고 민감한 정보와 개인 사생활 침해를 보호하기 위한 정책방향을 제시하였다. 특히 자산관리, 추적, 매칭, 접근통제, 자동지불, 공급망 통제 등을 위한 RFID 어플리케이션 보안에 초점을 맞추고 있다.

RFID 기술이 주는 수많은 혜택을 실현하기 위해 관리적, 운영적, 기술적 통제를 통한 보안과 사생활 침해 위험을 세심하게 다뤄야 하나 각각의 RFID 기술은 그 구성요소가 상이하고 상업화를 위한 응용 방법들이 다양하여 보안위험과 이를 통제하기 위한 방법들이 매우 다양한 상황이다. 이런 상황에서 RFID 기술을 구현하는데 공통적인 IT 요소(서버, 데이터베이스, 네트워크 등)들에 대한 통제 및 관리를 통해 보안 문제를 효율적으로 해결할 수 있을 것이며, 이 보고서는 이에 대한 세부적인 정책 방향을 제시하였다.

주요 RFID 보안 권고 사항을 요약하면 다음과 같다.

- 회사내 정보 시스템에 RFID 데이터베이스를 다른 데이터베이스와 분리하기 위한 방화벽 설치
- 라디오 신호 암호화
- 승인된 RFID 사용자들에 대한 인증
- 인가되지 않은 접근을 막기 위한 태그 은폐
- 보안 침해를 탐지하기 위한 감사 절차 채택
- 민감한 데이터를 영구적으로 제거하기 위한 태그 재활용 또는 파괴
- 태그에 저장되는 민감한 데이터 최소화

또한 NIST의 상세한 단계별 RFID 보안 체크리스트는 개시, 계획 및 설계, 조달, 구현, 운영/유지 단계별로 보안 실제 예제를 "추천", "필수"로 구분하여 제시하고 있다. 여기서 "추천"은 반드시 적용하지 않으면 보안 실패 위험성의 심각한 증가를 초래하는 것을 의미하고, "필수"는 구현 불가능하거나 비용을 맞출 수 없는 경우에만 미적용 가능한 것을 의미한다.

이러한 RFID 시스템 보안 관련 NIST 가이드라

인은 RFID 기술의 문제 및 관련 위험을 정확히 인식하고 이를 극복하기 위한 다양한 방안들을 고려하였기 때문에 RFID 기술의 성장을 마련하기 위한 기본가 될 것으로 예상된다.

2.4 RFID 프라이버시 보호 가이드라인

정보통신부에서는 RFID 시스템 이용에 따른 이용자의 프라이버시를 보호하고 안전한 RFID 이용환경을 조성하기 위해서 “RFID 프라이버시 보호 가이드라인”[14]을 발표하였다. 개인이 RFID 태그가 부착된 사물을 착용·휴대할 경우 RFID 태그 내 고유 정보가 판독되어 개인에 대한 성향 파악 및 위치 추적 등에 오·남용되거나 개인 프라이버시를 침해할 수 있다. 그러므로, 이 가이드라인은 RFID 태그, 리더 등을 비롯한 전체 시스템을 취급함에 있어 준수하여야 할 기준을 제시함으로써 취급사업자는 제시된 기준 하에서 사업을 안정적으로 추진할 수 있고 이용자는 프라이버시에 대한 우려를 최소화할 수 있다.

이 가이드라인은 RFID 태그에 개인정보를 기록하여 당해 개인정보를 수집하거나 RFID를 통하여 수집한 물품정보와 개인정보를 연계하는 등 RFID 시스템을 이용하여 개인 프라이버시를 침해할 수 있는 경우에 한하며, 개인정보와 프라이버시 침해 위험 없이 물품정보를 수집하여 이용하는 경우에는 적용되지 않는다. 주요 내용으로는 개인정보 기록·수집 및 연계에 대한 부분, RFID 태그 부착 표시, 태그 제거방법 표시 등 태그 관련 부분, 관리적·기술적 보호조치 등이 있다.

특히 RFID 시스템의 개인정보보호를 위한 관리적·기술적 보호조치는 관리 체계 수립 및 시행, 접근통제, 암호화 및 인증 등 기술적 보호조치, 태그 기능 제거 또는 중지 등으로 구분하여 조치사항을 제시하고 있다. 관리 체계 수립 및 시행에서는 RFID 시스템 운영시 태그내 개인정보를 기록하거나 개인정보와 연계하는 경우 안전한 취급을 위한 내부규정을 마련하고, RFID 시스템 운영시 처리되는 개인정보의 도난·분실·누출 등 사고 발생시 조치 및 보고에 대한 체계적인 대응지침을 마련하도록 한다. 접근통제에서는 RFID 시스템을 운영할 경우 접근권한자를 지정하고 접근권한을 구분하도록 한다. 암호화 및 인증 등 기술적 보호조치에서는 RFID 시스템 운영시 권한없는 접근을 차단하기 위한 암호화, 인증 등의 보호조치를 시행하고, 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단 시스템 등의 접근 통제장치를 설치·운영하고, RFID 시스템을 운영시 정보 접근 기록(로그)에 대한 안전한 관리 장치를 운영하며, 바이러스 침투를 방지하기 위해 백신소프트웨어를 설치·운영하도록 한다. 마지막으로 태그 기능 제거 또는 중지에서는 이용자가 용이하게 RFID 태그의 기능을 제거·중지할 수 있는 물리적·전자적 수단을 제공하도록 한다.

또한, 한국정보보호진흥원은 ‘RFID 프라이버시 보호 가이드라인’의 각 조항별 주안점 및 구체적인 예시를 제시함으로써 해석상 오해의 소지를 없애고 가이드라인에 대한 올바른 이해를 통하여 RFID 취급사업자의 개인정보보호 조치 이행을 지원하기 위하여 이에 대한 해설서[16]를 작성·배포하였다.

3. RFID 기반 정보시스템의 보안 감리 점검항목

본 장에서는 RFID 기반 정보시스템의 신뢰성, 안정성 및 효율성 향상과 보안 분야의 체계적인 점검을 위한 보안감리 점검항목을 제안한다. 보안감리 점검항목은 8개 부문의 기본 점검항목과 각각의 기본 점검항목에 대한 세부 검토항목으로 구성된다.

3.1 RFID 시스템의 보안위협 고찰을 통한 점검항목

본 절에서는 RFID 시스템의 특성과 RFID 시스

템의 프라이버시 침해 및 취약점 공격을 고찰하여 보안감리 점검항목을 도출하였다.

3.1.1 RFID 시스템의 특성 고찰을 통한 점검항목

RFID 기반 정보시스템은 크게 태그, 리더, 네트워크, 플랫폼(미들웨어), 응용 서비스로 구성되어 유·무선 통신과 연동되어 사용되므로 이 과정이 올바르게 이루어지기 위해서는 데이터 전송에서 위변조를 막아 데이터가 안전하게 전송되도록 해야 한다. 이러한 RFID 기반 정보시스템의 특성상 발생할 수 있는 위협사항들을 조사 분석하여 RFID 기반 정보시스템을 위한 보안감리 점검항목을 <표 1>과 같이 도출하였다.

<표 1>에서 보는 바와 같이 표 왼쪽 편에 기술된 주요 4가지 RFID 기반 정보시스템의 특성을 고려하여 감리 시점별 보안감리 점검항목을 제시하였다.

3.1.2 RFID 시스템의 프라이버시 침해 및 취약점 공격 고찰을 통한 점검항목

RFID 기반 정보시스템은 여러 가지 보안 위협에 노출되기 쉬우며 이로 인하여 여러 가지 문제점이 발생하게 된다. 따라서 본 절에서는 RFID 기반 정보시스템에서 발생할 수 있는 프라이버시 침해 및 취약점 공격에 대한 대처방안이 적정하게

〈표 1〉 RFID 시스템 특성 고찰을 통한 점검항목

RFID 시스템 특성	감리 시점	보안감리 점검항목
리더와 태그간의 무선통신 사용에 따른 보안위협사항 존재	분석	RFID 시스템의 보안요구사항 분석 및 도출의 충분성, 적정성
	분석	RFID 시스템의 보안정책 수립 및 보안대책의 적정성
RFID 태그의 신상정보 노출 가능성 존재	설계	RFID 시스템에 대한 보안에 상세설계의 적정성
	설계	RFID 적용 보안기술에 대한 현장 실증계획 수립여부
사용자의 위치 추적 문제(프라이버시 침해)	구현	RFID 보안솔루션의 설치 및 보안환경 구현의 적정성
RFID 기반 정보시스템의 구성요소간 데이터 전송경로상의 정보 위협사항 존재	구현	RFID 태그정보 보호의 적정성
	시험	RFID 적용 보안기술에 대한 현장 실증실험 실시

〈표 2〉 프라이버시 침해 및 취약점 공격 고찰을 통한 점검항목

RFID 시스템의 프라이버시 침해 및 취약점 공격	감리 시점	보안감리 점검항목
프라이버시 침해 ◦ 개인 신상정보 노출 ◦ 개인의 물품보유현황 노출 ◦ 개인 위치정보 노출 ◦ 개인의 구매패턴 및 선호도 노출 ◦ 타 정보와 결합을 통한 개인 정보화 ◦ 개인의 의사와 무관한 불법 거래	분석	RFID 시스템의 보안요구사항 분석 및 도출의 충분성, 적정성
	분석	RFID 시스템의 보안정책 수립 및 보안대책의 적정성
	구현	RFID 태그정보 보호의 적정성
취약점 공격 ◦ 도청 ◦ 트래픽 분석 ◦ 스푸핑 ◦ 서비스 거부 ◦ 세션 가로채기 ◦ 재생 ◦ 중간자 ◦ 물리적 공격 등	분석	RFID 시스템의 보안요구사항 분석 및 도출의 충분성, 적정성
	분석	RFID 시스템의 보안정책 수립 및 보안대책의 적정성
	설계	RFID 시스템에 대한 보안 상세설계의 적정성
	구현	RFID 보안솔루션의 설치 및 보안환경 구현의 적정성
	시험	RFID 적용 보안기술에 대한 현장 실증실험 실시
	전개	RFID 시스템 감사통제의 적정성

수립되었는지를 중심으로 RFID 기반 정보시스템을 위한 보안감리 점검항목을 <표 2>와 같이 도출하였다.

<표 2>에서와 같이 표 왼쪽 편에 기술된 다양한 프라이버시 침해 및 취약점 공격에 대한 대처 방안으로써 감리 시점별 보안감리 점검항목을 제시하였다.

3.2 NIST RFID 가이드라인 고찰을 통한 점검항목

본 절에서는 NIST RFID 가이드라인에서 RFID 시스템의 보안 권고사항과 단계별 RFID 보안 체크리스트의 추천 및 필수를 중심으로 하여 보안감리 점검항목을 도출하였다.

3.2.1 NIST RFID 가이드라인의 보안 권고사항 고찰을 통한 점검항목

NIST에서 마련한 RFID 시스템 보안 관련 가이드라인은 RFID 시스템의 적절한 보안 통제 수단 강구, RFID 실행과 관련된 다양한 위험의 통제, RFID의 기술적 보안 통제 관리방법 선택 등으로 구성되어 있다. NIST RFID 가이드라인에서 제시된 주요 보안 권고사항을 중심으로 <표 3>과 같이 RFID 기반 정보시스템을 위한 보안감리 점검항목을 도출하였다.

<표 3>에서 보는 바와 같이 표 왼쪽 편에 기술된 7가지 NIST RFID 가이드라인의 보안 권고사항을 분석하여 감리 시점별 보안감리 점검항목을 제시하였다.

3.2.2 NIST RFID 보안 체크리스트의 추천 고찰을 통한 점검항목

NIST RFID 보안 체크리스트에서 제시한 RFID 기술을 구현하는데 있어 각 단계별로 반드시 적용하지 않으면 보안 실패 위험성의 심각한 증가를 초래할 수 있는 “추천”을 중심으로 RFID 기반 정보시스템을 위한 보안감리 점검항목을 <표 4>와 같이 도출하였다.

<표 4>에서와 같이 표 왼쪽 편에 기술된 단계(즉, 개시, 계획 및 설계, 조달, 구현, 운영/유지 단계)별 NIST RFID 보안 체크리스트의 추천 고려사항을 분석하여 감리 시점별 보안감리 점검항목을 제시하였다.

3.2.3 NIST RFID 보안 체크리스트의 필수 고찰을 통한 점검항목

NIST RFID 보안 체크리스트에서 제시한 RFID 기술을 구현하는데 있어 각 단계별로 구현 불가능하거나 비용을 맞출 수 없는 경우에만 미적용 가능한 “필수”를 중심으로 RFID 기반 정보시스템을 위한 보안감리 점검항목을 <표 5>와 같이 도출하였다.

〈표 3〉 보안 권고사항 고찰을 통한 점검항목

NIST RFID 가이드라인의 보안 권고사항	감리 시점	보안감리 점검항목
태그에 저장되는 민감한 데이터 최소화	분석	RFID 시스템의 보안요구사항 분석 및 도출의 충분성, 적정성
라디오 신호 암호화	설계	RFID 시스템의 보안에 대한 상세설계의 적정성
승인된 RFID 사용자들에 대한 인증	설계	RFID 시스템의 보안에 대한 상세설계의 적정성
회사내 정보시스템에 RFID 데이터베이스를 다른 데이터베이스와 분리하기 위한 방화벽 설치	구현	RFID 보안솔루션의 설치 및 보안환경 구현의 적정성
인가되지 않은 접근을 막기 위한 태그 은폐	구현	RFID 태그정보 보호의 적정성
민감한 데이터를 영구적으로 제거하기 위한 태그 재활용 또는 파괴	구현	RFID 태그정보 보호의 적정성
보안침해를 탐지하기 위한 감사절차 채택	전개	RFID 시스템 감사통제의 적정성

〈표 4〉 RFID 보안 체크리스트(추천) 고찰을 통한 점검항목

단계	RFID 보안 체크리스트의 추천 고려사항	감리 시점	보안감리 점검항목
개시	RFID 위협의 실현 가능성, 그로 인한 조직 자산에 대한 잠재적 영향을 이해하기 위한 위험 측정 실행	분석	RFID 시스템의 보안정책 수립 및 보안대책의 적정성
	RFID 사용 정책 수립		
	RFID 프라이버시 정책 수립		
	HERF/HERO/HERP 정책 수립		
	RFID 시스템의 존재를 설명하는 네트워크 보안정책 수립		
계획 및 설계	RFID 시스템이 따라야 하는 RFID 표준 식별	분석	RFID 시스템의 보안요구사항 분석 및 도출의 충분성, 적정성
	RFID 시스템 투자와 예산 요구사항에 보안과 정보보호 고려사항 포함		
	리더와 다른 장치간의 적절한 배치를 결정하기 위한 위치 조사	설계	RFID 시스템의 보안에 대한 상세설계의 적정성
	RF 방사 통제에 대한 접근 방법 결정		
	가용 전용 네트워크와 암호를 사용하여 네트워크 관리 트래픽을 보호하는 접근 방법 식별		
	보안 사건 유형을 식별하는 RFID 감사 프로세스와 과정 개발 및 감사 기록의 안전한 저장방법 결정		RFID 시스템의 보안에 대한 상세설계의 적정성
	패스워드 보호 특성을 지원하는 태그의 패스워드 관리 체계 개발		
	태그 메모리 보호를 위한 접근방법 결정		
조달	FIPS-인증 암호모듈을 상용하는 제품 조달	구현	RFID 보안솔루션의 설치 및 보안환경 구현의 적정성
	보안정책을 기능적으로 지원 가능한 제품 조달		
	로그 보안 관련 사건을 원격 감사 서버에 실시간으로 전송하는 리더, 미들웨어, 분석 시스템 조달		
	네트워크 관리 트래픽을 보호하는 선택적 접근 방법을 지원하는 리더와 서버 플랫폼 조달		
	NTP(Network Time Protocol)를 지원하는 리더와 서버 플랫폼 조달		
	소프트웨어나 펌웨어를 통해 쉽게 업그레이드 가능한 리더 조달		
구현	RFID 구성요소를 지원하는 플랫폼 강화	구현	RFID 태그정보 보호의 적정성
	리더의 사용자 인증용 패스워드 강화 보증		
	리더의 무선 인터페이스 구성		
	태그 메모리 잠금		
	리더와 기업 서브시스템의 불안하거나 사용하지 않는 관리 프로토콜 폐기		
	HERF/HERO/HERP 준수 프로그램에 운영자 훈련, 통지 포스팅, 민감한 물건에 라벨 적용 등 포함		
	소프트웨어 패치와 업그레이드 테스트 수행	시험	RFID 적용 보안기술에 대한 현장 실증실험 실시
운영/ 유지	지속적인 감사 로그 검토	전개	RFID 시스템 감사통제의 적정성
	정기 · 비정기적으로 종합적인 보안 측정 시행		
	RFID 구성요소 처분시 감사 기록의 보유 또는 파괴 보증		

<표 5>에서 보는 바와 같이 표 왼쪽 편에 기술된 단계(즉, 개시, 계획 및 설계, 조달, 구현, 운영/유지 단계)별 NIST RFID 보안 체크리스트의 필수 고려사항을 분석하여 감리 시점별 보안감리 점

〈표 5〉 RFID 보안 체크리스트(필수) 고찰을 통한 점검항목

단계	RFID 보안 체크리스트의 필수 고려사항	감리 시점	보안감리 점검항목
개시	RFID 시스템 운영자를 위한 RFID 보안 훈련 프로그램 수립	분석	RFID 시스템의 보안에 대한 상세설계의 적정성
계획 및 설계	RF 서브시스템과 기업 네트워크간의 네트워크 방화벽 설계	설계	RFID 시스템의 보안에 대한 상세설계의 적정성
조달	RFID 감사 데이터 검토를 자동화하는 감사 도구 조달	구현	RFID 보안솔루션의 설치 및 보안환경 구현의 적정성
구현	각 태그마다 유일한 패스워드 지정	구현	RFID 태그정보 보호의 적정성
	로깅 활성화와 로그 엔트리를 원격 감사 서버에서 관리		RFID 보안솔루션의 설치 및 보안환경 구현의 적정성
운영/유지	개인 또는 그룹에게 RFID 취약성 및 무선 보안 동향 분석 임무 부여	전개	RFID 시스템의 보안정책 수립 및 보안대책의 적정성
	태그 처분시 폐기 또는 파괴		RFID 태그정보 보호의 적정성

〈표 6〉 RFID 프라이버시 보호 가이드라인 고찰을 통한 점검항목

RFID 프라이버시 보호 가이드라인의 관리적·기술적 보호조치	감리 시점	보안감리 점검항목
RFID 태그정보와 개인정보 연계시 세부 관리절차 및 지침 마련	분석	RFID 시스템의 보안정책 수립 및 보안대책의 적정성
RFID 시스템 운영시 개인정보 도난, 분실, 누출 등의 방지를 위한 보안대책 및 발생시의 대응지침 마련	분석	RFID 시스템의 보안정책 수립 및 보안대책의 적정성
RFID 시스템 운영시의 접근 권한자 지정 및 접근권한 구분	설계	RFID 시스템의 보안에 대한 상세설계의 적정성
RFID 시스템 운영시 권한 없는 접근을 차단하기 위한 암호화 및 인증 등 기술적 보호조치 마련	분석	RFID 시스템의 보안요구사항 분석 및 도출의 충분성, 적정성
	설계	RFID 시스템의 보안에 대한 상세설계의 적정성
	구현	RFID 보안솔루션의 설치 및 보안환경 구현의 적정성
	시험	RFID 적용 보안기술에 대한 현장 실증실험 실시
RFID 태그 기능 제거 또는 중지할 수 있는 수단 제공	구현	RFID 태그정보 보호의 적정성

검항목을 제시하였다.

3.3 RFID 프라이버시 보호 가이드라인 고찰을 통한 점검항목

본 절에서는 RFID 프라이버시 보호 가이드라인에서 제시된 RFID 시스템의 개인정보보호를 위한 관리적·기술적 보호조치사항을 중심으로 하여 RFID 기반 정보시스템을 위한 보안감리 점검항목을 <표 6>과 같이 도출하였다.

<표 6>에서와 같이 표 왼쪽 편에 기술된 RFID 프라이버시 보호 가이드라인의 5가지 주요 관리적·기술적 보호조치를 분석하여 감리 시점별 보안감리 점검항목을 제시하였다.

3.4 RFID 기반 정보시스템의 보안감리 점검항목

본 절에서는 앞 절에서 도출한 보안감리 점검항목들을 종합적으로 정리하여 RFID 기반 정보시스

템의 사업특성기반 보안감리의 점검항목 및 검토 항목을 <표 7>과 같이 제안한다.

<표 7>에서 보여주는 바와 같이 분석단계의 보안감리 점검항목은 보안위협에 효과적으로 대처하

〈표 7〉 RFID 기반 정보시스템의 보안감리 점검항목

감리 시점	기본 점검항목	검토항목
분석	RFID 시스템의 보안요구사항 분석 및 도출의 충분성, 적정성	1. RFID 시스템의 보안요구사항이 적절하게 도출되었는가? ◦ RFID 태그 데이터 보호를 위한 보안요구 사항 도출 여부 ◦ RFID 시스템 데이터 전달경로에서의 태그 데이터 보안요구사항 도출 여부 ◦ RFID 시스템 구성 및 아키텍처 등에 대한 보안요구사항 도출 여부(태그, 단말기, 네트워크, 미들웨어, 서버 등) ◦ RFID 응용 시스템의 보안요구사항 도출 여부 ◦ 서비스별 개인 프라이버시 보호대상 식별 여부
	RFID 시스템의 보안정책 수립 및 보안대책의 적정성	2. RFID 시스템의 보안정책이 적정하게 수립되었는가? ◦ RFID 시스템의 특성을 반영한 보안정책 수립 여부 ◦ RFID 태그정보와 개인정보의 연계시 세부 관리절차 및 지침 마련 여부 3. RFID 시스템의 보안 취약점에 대한 분석 및 체계적인 대응지침이 마련되었는가? ◦ RFID 시스템의 위협요인 및 취약성 분석을 통한 적절한 대응책 마련 여부 ◦ RFID 시스템 운영시의 개인정보 도난, 분실, 누출 등의 방지를 위한 보안대책 및 발생시의 대응지침의 적정성 ◦ RFID 단말기 분실시의 대비책 ◦ RFID 시스템 Login 패스워드 관리규정
설계	RFID 시스템의 보안에 대한 상세 설계의 적정성	4. RFID 시스템의 적용 보안기술의 분석 및 설계를 적정하게 수행하였는가? ◦ RFID 시스템 적용 보안 솔루션(기술)의 적정성 ◦ RFID 시스템의 관리적, 물리적, 기술적보안 대책 ◦ RFID 시스템에 대한 접근권한 통제의 적정성
	RFID 적용 보안기술에 대한 현장 실증 계획 수립여부	5. RFID 적용 보안기술에 대한 현장 실증실험(검증)을 위한 계획이 적정하게 수립되었는가? ◦ RFID 적용 보안기술에 대한 현장 실증실험(검증) 방법 및 절차
구현	RFID 보안 솔루션의 설치 및 보안환경 구현의 적정성	6. RFID 시스템의 보안기능 구현 및 각종 보안 Profile 값의 설정이 적정하게 수행되었는가? ◦ RFID 보안 솔루션의 설치 적정성 ◦ RFID 시스템(서버, 무선통신, 미들웨어, 서비스 단말기, 클라이언트)의 보안기능 구현의 적정성 ◦ RFID 보안 Profile 값 설정의 적정성
	RFID 태그정보 보호의 적정성	7. RFID 태그정보가 적정하게 보호되고 있는가? ◦ RFID 태그의 신상정보 노출 가능성 점검 ◦ RFID 태그정보가 허가되지 않은 리더에 노출 가능성 점검 ◦ RFID 태그와 태그 소유자 사이의 장기간 유지되는 추적정보 수집 가능성 점검 ◦ RFID 태그 기능을 제거/중지할 수 있는 물리적 전자적 수단(태그 자체 제거, 스크래칭 등 전자적 태그정보 판독불가 조치, 리더 판독차단 등) 제공 여부
시험	RFID 적용 보안기술에 대한 현장 실증실험 실시	8. RFID 시스템의 적용 보안기술에 대한 현장 실증실험을 통하여 보안성 검증이 적정하게 수행되었는가? ◦ RFID 사용자 인증 ◦ 데이터 송수신 채널별 암호화 등 보호조치 ◦ 민감한 데이터 보호를 위한 태그 재활용 및 제거 ◦ 태그와 리더간의 상호 인증 및 취약점(스푸핑, 세션 가로채기 등) 존재 여부 ◦ 각종 공격(전력분석 해석 등 사이드 채널 공격, 물리적 공격 등)으로 인한 취약점 존재 여부 ◦ 바이러스 침투 가능성 여부
전개 (운영 준비)	RFID 시스템 감사통제의 적정성	9. RFID 시스템의 보안침해 방지를 위한 감사절차/기록 및 추적기능을 사용하고 있는가? ◦ RFID 시스템 보안침해 탐지절차 채택 여부 ◦ RFID 시스템 정보접근 기록(로그)에 대한 안전한 관리장치 운영 여부 ◦ 응용 프로그램 감사기록 및 추적기능 사용 여부 ◦ 시스템 감사도구의 오용 및 손상을 예방하기 위한 통제의 적정성

고 보안사고 노출을 예방하도록 하였고, 설계단계의 보안감리 점검항목은 사용자의 보안요구사항의 만족여부(기밀성, 무결성, 가용성 확보 및 시스템 자원의 사용자 보안요구사항)를 검증하도록 하였다. 구현단계의 보안감리 점검항목은 시스템의 안정성을 기하고 보안 취약점을 예방하도록 하였고, 시험단계의 보안감리 점검항목은 보안요구사항의 충족여부와 사업목표 달성여부를 확인하도록 하였다. 마지막으로 전개단계의 보안감리 점검항목은 안전한 시스템 운영을 확인하고 보안침해 사고를 방지 및 대응할 수 있도록 하였다.

4. 보안감리 점검항목 검증

4.1 설문 조사 분석을 통한 검증

본 절에서는 설문 조사를 통해 본 논문에서 제안한 RFID 기반 정보시스템의 보안감리 점검항목에 대한 실효성을 검증하였다. 본 논문에서 설문 대상자로 선정한 모집단은 <표 8>과 같이 현 정보시스템 감리기준에 따라 정보시스템 감리업무를 수행하거나 보안 감리에 관련이 많을 것으로 여겨지는 감리 전문가를 대상으로 하였다.

E-mail로 배포된 질문서 중 53매가 회수되었는데, 사업특성기반의 감리에 관심이 많은 감리원에서 회수율이 높게 나타났으며, 피감리기관인 SI 집단에서는 상대적으로 낮은 회수율이 나타났다.

〈표 8〉 설문지 배포 대상 모집단

구 분	배포인원	비율(%)	비고
정보시스템 감리법인	50	41.7	감리원
SI	50	41.7	SI업체 근무자
기타(공공)	20	16.6	공공기관 보안전문가
합계	120	100	

RFID 기반 정보시스템의 보안감리 점검항목에 대한 타당성(중요도)을 조사하기 위하여 질문서는 크게 ① 보안요구사항 분석 및 도출 ② 보안정책 수립 및 요건 분석 ③ 적용 보안기술 설계 ④ 실증실험 계획 ⑤ RFID 보안환경 구축 ⑥ RFID 태그정보 ⑦ 현장 실증실험 ⑧ 시스템 감사의 8개 부문에 대한 세부 점검항목으로 구성되고, 수집된 질문서에 대해서는 Likert의 5점 척도법을 적용하여 분석하였다.

분석된 결과를 종합해 보면 <표 9>와 같이 전체 스케일 5.0 기준 평균 4.12로 매우 긍정적(타당성)인 것으로 조사되었다. 특히 '실증실험 계획' 항목의 중요도가 4.42로 가장 높았고, 가장 낮은 '적

〈표 9〉 점검항목별 중요도 평균점수

구 분	점검항목	중요도 평균	비고
보안요구사항 분석 및 도출	◦ RFID 시스템의 보안요구 사항 분석 및 도출의 충분성, 적정성	4.17	5.0 : 매우 중요
보안정책 수립 및 요건 분석	◦ RFID 시스템의 보안정책 수립 및 보안대책의 적정성	4.08	4.0 : 중요
적용 보안기술 설계	◦ RFID 시스템의 보안에 대한 상세설계의 적정성	3.87	
실증실험 계획	◦ RFID 적용 보안기술에 대한 현장 실증실험 계획 수립여부	4.42	3.0 : 보통
RFID 보안환경 구축	◦ RFID 보안솔루션의 설치 및 보안환경 구현의 적정성	4.00	
RFID 태그정보	◦ RFID 태그정보의 보호의 적정성	4.25	2.0 : 미흡
현장 실증실험	◦ RFID 적용 보안기술에 대한 현장 실증실험 실시	3.94	
시스템 감사	◦ RFID 시스템 감사통제의 적정성	4.20	1.0 : 부적절
종합		4.12	

용 보안기술 설계' 항목의 중요도도 3.87로 4.0에 가까운 중요도를 보여주었다. 또한 대상 점검항목별로 다양한 측면에서 상세하게 분석해 본 결과 모든 면에서 일관성 있게 긍정적으로 평가되어 본 논문은 실효성 있는 점검항목을 도출한 것으로 판단될 수 있다.

4.2 감리사례 분석을 통한 검증

본 논문에서 제안한 RFID 기반 정보시스템의 보안감리 점검항목에 대하여 그 실효성을 검증하기 위해 기존 감리보고서를 수집하여 분석하려 했다. 그러나, 법률상 기존 정보시스템 감리보고서의 열람이 불가능하여 정보시스템 감리법인이 실제 RFID 기반 정보시스템의 감리에서 사용하는 점검항목(검토기준)을 조사하였다.

현재 사업유형기반 감리 점검체계를 적용하여 감리를 수행하는 대부분의 경우에 RFID의 특성을 반영한 세부적인 점검항목의 적용은 전무한 상황이며, 감리원 개개인이 정보시스템 감리기준의 점검항목을 위주로 필요한 점검항목을 개인적으로 추가하여 감리를 수행하고 있었다. 본 논문에서는 기존 RFID 기반 정보시스템 감리에서 사용된 감리 점검항목과 본 논문에서 제안한 감리 점검항목을 비교해 보았다.

<표 10>은 본 논문에서 제안한 RFID 기반 정보시스템 보안감리 점검항목과 최근 실제 감리 사례로 "A" 와 "B" RFID 기반 정보시스템 구축사업 프로젝트의 감리 수검 시 사용된 감리 점검항목을 비교한 내용을 보여준다.

<표 10>에서와 같이 현재 실제 RFID 기반 정보시스템 감리에서 사용된 보안감리 점검항목은 너무 포괄적이고 감리원 개개인에 따라 좌우되는 경향이 크다. 그러나 본 논문에서 제안한 RFID 기반 정보시스템 보안감리 점검항목은 실제 감리 수행 시에 사용된 감리 점검항목 보다 구체적일 뿐

〈표 10〉 제안 보안감리 점검항목과 기존 보안감리 점검항목 비교

구 분	제안 점검항목	"A" 사례 점검항목	"B" 사례 점검항목
보안 요구사항 분석 및 도출	RFID 시스템의 보안요구사항 분석 및 도출의 충분성, 적정성	보안요건 분석 및 설계의 적정성	RFID 시스템의 보안요구사항 도출의 충분성, 적정성
보안정책 수립 및 요건 분석	RFID 시스템의 보안정책 수립 및 보안대책의 적정성		보안정책 수립여부 사용자 접근제어 정책 수립여부
적용 보안기술 설계	RFID 시스템의 보안에 대한 상세설계의 적정성		RFID 표준 적용여부
실증실험 계획	RFID 적용 보안기술에 대한 현장 실증계획 수립여부	시스템 설치 및 검증계획 수립의 적정성 RFID 태그 설계 적정성	시스템 시험계획(현장 실증실험)의 적정성
RFID 보안환경 구축	RFID 보안솔루션의 설치 및 보안환경 구현의 적정성	RFID 태그의 발행 및 사용 시 위변조 방지방안의 적정성	시스템 도입 및 보안환경 구축의 적정성
RFID 태그정보	RFID 태그정보 보호의 적정성	프로토콜 표준화 및 암호화 기술 적용의 적정성	휴대용 리더기, 클라이언트 보안 적정성 태그의 발행 및 폐기/운영방안의 적정성
현장 실증실험	RFID 적용 보안기술에 대한 현장 실증실험 실시	RFID 태그 및 리더기 품질 및 신뢰성 장애발생 대비책 마련여부 등	시스템 구성요소에 대한 실증실험(검증)의 적정성
시스템 감사	RFID 시스템 감사통제의 적정성	-	-

만 아니라 모든 구분 분야에서 포괄적인 동일성을 보여주기 때문에 본 논문에서 제안한 보안감리 점검항목의 실효성을 간접적으로 확인할 수 있었다.

5. 결 론

정보시스템의 감리영역은 일반적으로 응용시스템, 데이터베이스, 시스템 아키텍처 등으로 나누어 볼 수 있는데, 보안감리 분야는 각 영역에서 해당 보안 점검사항을 점검하도록 되어 있다. 그러나 기존의 사업유형기반의 보안감리 점검항목은 최근 시범사업 및 확산사업에 이어 공공부문의 전면도입 및 민간 분야로 확산되고 있는 RFID 기반 정보시스템의 사업특성을 반영하는 감리요구사항에 부합하지 못하고 있다.

이에 따라 본 논문에서는 RFID와 같은 신기술과 관련한 사업특성기반의 감리 점검항목의 필요성 및 중요성을 인식하여 RFID 기반 정보시스템의 사업특성을 반영한 보안감리 점검항목을 도출하였고, 설문조사 및 감리사례 분석을 통해 본 논문에서 제안한 보안감리 점검항목에 대한 실효성을 검증하였다. 그러므로 본 논문은 RFID 기반 정보시스템 보안감리시 사용될 수 있는 보안감리 점검항목을 제안함으로써 RFID 기반 정보시스템의 안전성 및 신뢰성 보장에 기여할 수 있을 것으로 판단된다.

그러나 본 논문에서는 연구의 범위를 RFID 기반 정보시스템의 사업특성을 반영한 보안감리 점검항목 제시로 한정하였기 때문에 RFID 기반 정보시스템의 업무적 특성을 반영한 응용시스템 및 데이터베이스, 시스템 아키텍처 영역 등의 감리 점검항목에 관한 전반적이고 체계적인 연구가 추후에 계속 이루어질 필요가 있을 것이다.

참 고 문 헌

[1] 국가사이버안전센터, 「국가사이버안전매뉴얼」, 대통령 훈령 제141호, 2005.

[2] 국방부, 「군사보안업무시행규칙」, 국방부 훈령 제697호, 2001.

[3] 박남제, “RFID 가상 태그를 활용한 개인화된 광고 및 정보 응용 서비스 개발”, 「한국IT서비스학회지」, 제8권, 제4호(2009), pp.151-163.

[4] 박춘식, “유비쿼터스 네트워크와 시큐리티 고찰”, 「정보보호학회지」, 제14권, 제1호(2004), pp.12-20.

[5] 서대희, 이임영, “유비쿼터스 환경을 위한 RFID 태그의 인증과 관리에 관한 연구”, 「정보보호학회논문지」, 제16권, 제2호(2006), pp.81-94.

[6] 오경희, 김호원, “RFID 환경에서의 프라이버시 보호기술”, 「한국통신학회지」, 제23권, 제9호(2006), pp.103-112.

[7] 여상수, 김순석, 김성권, “안전한 RFID 프라이버시 보호 프로토콜을 위한 백엔드 서버의 태그 판별 시간 절감 기법”, 「정보보호학회논문지」, 제16권, 제4호(2006), pp.13-26.

[8] 임지영, 「RFID 기반 정보시스템을 위한 보안감리 점검항목」, 건국대학교 정보통신대학원 학위논문, 2008.

[9] 임지영, 김동오, 한기준, “RFID 기반 정보시스템을 위한 보안감리 점검항목”, 「한국IT서비스학회 추계학술대회논문집」, (2008), pp. 419-422.

[10] 정보통신부, 「정보통신기반보호법」, 법률 제6796호, 2002.

[11] 정보통신부, 「라우터 보안관리 가이드」, 2003.

[12] 정보통신부, 「웹 서버 보안관리 가이드」, 2003.

[13] 정보통신부, 「정보시스템의 효율적 도입 및 운영 등에 관한 법률」, 법률 제7816호, 2005.

[14] 정보통신부, 「RFID 프라이버시 보호 가이드라인」, 2005.

[15] 정보통신부, 「정보시스템 구축운영 기술지침」, 정보통신부 고시 제2006-37호, 2006.

[16] 정보통신부, 한국정보보호진흥원, 「RFID 프라이버시 보호 가이드라인 해설서」, 2007.

[17] 정보통신부, 한국정보사회진흥원, 「RFID 적용

을 위한 가이드북-RFID 개요 및 도입절차」, 2007.

[18] 정보통신부, 한국정보사회진흥원, 「RFID 적용을 위한 가이드북-RFID 정보보호」, 2007.

[19] 지식경제부, 기술표준원, 「정보기술-품목관리용 무선인식(RFID)-구현 가이드라인, 제1부, 제2부, 제3부」, 2008.

[20] 최은영, 이수미, 임종인, 이동훈, "분산 시스템 환경에 적합한 효율적인 RFID 인증 시스템", 「정보보호학회논문지」, 제16권, 제6호(2006), pp.25-35.

[21] 한국전산원, 「유비쿼터스 컴퓨팅 환경에서 보안 및 인증서비스 방향연구」, 2004.

[22] 한국정보사회진흥원, 「정보시스템 보안/통제 감리지침」, 1998.

[23] 한국정보사회진흥원, 「정보보호정책수립 지침」, 2002.

[24] 한국정보보호진흥원, 「정보시스템 구축단계별 정보보호 가이드라인」, 2004.

[25] 한국정보통신기술협회, 「RFID 서비스 보안 요구사항」, 정보통신단체표준 TTAS.KO-06.0144, 2007.

[26] 한국정보화진흥원, 「정보화사업 감리 수행 가이드」, 2011.

[27] 행정안전부, 「정보시스템 감리기준」, 행정안전부 고시 제2010-85호, 2010.

[28] 행정안전부, 「전자정부법」, 법률 제10012호, 2010.

[29] Juels, A., Privacy and Authentication in Low-Cost RFID Tags, http://www.rsa.com/.

[30] Juels, A., R. L. Rivest, and M. Szydlo, "The Blocker Tag : Selective Blocking of RFID Tags for Consumer Privacy", *Proceedings of 10th ACM Conference on Computer and Communications Security*, 2003.

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

[32] Ohkubo, M., K. Suzuki, and S. Kinoshita, "Forward-secure RFID Privacy Protection using Hash Chain", NTT Laboratories, 2003.

[33] Weis, S., S. Sarma, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", *Proceedings of the 1st Security in Pervasive Computing*, 2003.

◈ 저 자 소 개 ◈

전 상 덕 (zauri3@naver.com)

충북대학교 컴퓨터공학과에서 공학사를 취득하였으며, 연세대학교 공학대학원에서 공학석사를 취득하였다. 현재 건국대학교 컴퓨터공학과에서 박사과정 중에 있으며, 또한 김앤장에서 전문위원으로 재직 중이다. 주요 관심분야는 정보시스템감리, 데이터베이스, 컴퓨터 보안/포렌식 등이다.

임 지 영 (jylim@koscom.co.kr)

경북대학교 컴퓨터공학과에서 공학사를 취득하였으며, 건국대학교 정보통신대학원 정보시스템감리 전공에서 공학석사를 취득하였다. (주)코스콤 전자인증센터의 전자인증센터장을 역임하였고, 현재 (주)코스콤 대외협력부 팀장으로 재직 중이다. 주요 관심분야는 정보시스템 보안감리, 전자인증 등이다.

이 기 영 (kylee@eulji.ac.kr)

숭실대학교 전자계산학과에서 공학사를 취득하였으며, 건국대학교 컴퓨터공학과에서 공학석사 및 공학박사 학위를 취득하였다. 한국해양과학기술원에서 연구원으로 근무하면서 해양자료 검색 및 데이터베이스화에 관한 여러 프로젝트를 수행하였고, 현재 을지대학교 의료IT마케팅학과 교수로 재직 중이다. 주요 관심분야는 u-Healthcare, 유비쿼터스, 공간 DB, GIS, LBS, USN, 텔레매틱스, 정보시스템 감리 등이다.

한 기 준 (kjhan@db.konkuk.ac.kr)

서울대학교에서 이학사를 취득하였고, KAIST 전산학과에서 공학석사 및 공학박사 학위를 취득하였으며, 현재 건국대학교 컴퓨터공학부 교수로 재직 중이다. 또한 Stanford 대학 전산학과 Visiting Scholar, 한국정보과학회 데이타베이스연구회 운영위원장, 한국ITS학회 기획위원장, 한국공간정보시스템학회 회장, 한국정보시스템감리사협회 회장 등을 역임하였다. 주요관심분야는 데이타베이스, GIS, LBS, 텔레매틱스, 정보시스템 감리 등이다.