RFID 프라이버시 보호 프레임웍 및 프로세스 설계에 관한 연구

김 진 수*

A Framework and Process Design for RFID Privacy Protection

Jin Soo Kim*

Abstract

RFID is an emerging technology and rapidly applied to various industries due to its high-tech characteristic and convenience. Although RFID provides valuable benefits, it might also generate serious privacy problems. Previous studies show that privacy issues should be incorporated in developing RFID systems and more detaild privacy protection methods. However, they just provide basic concept, rough guideline, and simple architecture about RFID privacy protection. Industry needs more structured framework and detailed systematic process to incorporate privacy issues into the RFID system.

The purpose of this paper is to develop a framework and detailed process design of RFID privacy protection issues in retail industries. A framework is developed based on individual sensitivity concept, RFID contents, and interface with EPC global standard. Case study is applied to validate the framework and it turns out to be useful. It is expected that the proposed framework and process design would provide more systematic guide lines to solving RFID privacy problems.

Keywords : RFID, Privacy, EPC Global, Framework

논문접수일 : 2007년 08월 14일 논문게재확정일 : 2007년 9월 14일

* 교신저자, 중앙대학교 상경학부 경영학과 교수, (456-756) 경기도 안성시 대덕면 내리 72-1, Tel : 031-670-3215, e-mail : sunny@cau.ac.kr

1. 서 론

1970년부터 사용해 온 바코드를 대체할 기술인 RFID(Radio Frequency IDentification)는 미래 유비쿼터스 시대를 선도할 핵심 기술로 주목받고 있다. RFID는 근거리 무선 기술을 이용하여 신호를 원격으로 감지 및 인식하여 정보 교환을 가능하게 하는 기술이다[이은곤, 2004]. RFID는 기존 바코드에 비해 판독 거리, 내구성, 재사용성, 저장 용량 등이 뛰어나기 때문에 자동화가 용이하며 다양한 분야에 응용할 수 있다.

IDtechEx[2007]에 의하면, RFID 시장 규모는 매년 빠르게 확대되어, 2005년 18.4억 달러에서 2008년 55.7억 달러, 2010년에 107억 달러, 2013년 188.5억 달러 까지 성장할 것으로 추정하고 있다. 특히, 유통, 물류 분야에서 본격적인 시장 확대가 시작되었고, 타 산업 분야에서도 공정 관리, 재고 관리, 실시간 위치 추적 등에 널리 쓰이기 시작했다[한국유통물류진흥원, 2007].

이같이 RFID가 다양한 산업에 빠르게 적용, 확산되고 있는 반면, 적용과정에서 발생할 수 있는 여러 가지 부작용에 대한 우려역시 증가하고 있다. 가장 심각한 부작용 중의 하나로 RFID 사용 시 발생할 수 있는 개인의 프라이버시 침해가능성이라 할 수 있다[유승화, 2005]. 프라이버시 침해에 대한 우려가 점증됨에 따라, 많은 기업들이 프라이버시 보호를 위해 보다 구체적인 방안과 시스템 구축을 위한 상세설계가 필요한 상황이다.

하지만, 기존 연구동향을 살펴보면, 프라이버시 보호를 위한 하드웨어적인 측면에서의 기술개발과, 법적, 제도적 방안을 제시하는 수준에 머물고 있는 실정이다.

Ari Juels 외 2인[2003]과 김종기 외 2인[2007]은 기술적 측면에서 정보 보안 및 개인 프라이버시 침해 해결을 위한 여러 방안을 제시하였다. 법률적인 측면에는 정부차원에서 국가별로 '개인 프라이버시 보호 가이드라인' 수준에서 프라이버시 보호를 위한 각종 법률, 방안을 개발하여 제시하고 있다[오길영, 2005; 정보통신부, 2005].

즉, Langheinrich[2001]은 유비쿼터스 환경에서 사용자의 프라이버시 보호를 위한 6가지 설계원칙을 제시하였고, Eileen P 외 2인[2005]는 RFID 기술 적용 시 프라이버시를 위한 적정 규제 3원칙을 제시하였다. 또한, Alan R. Peslak [2005]는 FTC(Federal Trade Commission)의 정보 보호 5원칙을 통해 RFID 시스템 도입 시 활용해야할 정보보호 원칙을 제시하였으나, 대부분의 연구결과가 프라이버시 보호를 위한 범용적인 가이드라인 수준에 그치고 있어, 기업에서 구체적인 방안을 수립하는데 활용하기에는 한계가 있다. 한편, 이병길 외 2인[2005]은 프라이버시 해결을 위해 보다 구체적인 보호 등급을 제시하였으나, 이 역시 제시하는 보호 등급의 논리적인 근거가 부족한 측면이 있어 실무에서 활용하기에 어려움이 있는 실정이다.

이에 따라, 본 연구에서는 문헌연구를 통해 이론적으로 타당하고 실무적으로 적용 가능한 RFID 기반 프라이버시 위협 요인 도출 및 보호 프레임웍을 제시하고자 한다. 또한, 프라이버시 보호 프레임웍의 타당성과 실무 적용성을 제고하기 위하여 사례연구를 통한 상세 프로세스를 제시하였다.

본 연구에서 제시한 프레임웍과 프로세스를 통하여 RFID 관련 산업에서 RFID 관련 개인 프라이버시 보호에 보다 효과적으로 대응할 수 있을 것으로 기대된다.

2. 이론적 배경

2.1 RFID 이론적 배경

RFID는 IC 칩을 내장한 태그에 축적된 정보

를 무선 주파수를 이용해 원격에서 인식하는 방식이며[김진노 외 2인, 2006], 자동식별(auto-identification)의 기능적인 측면에서는 기존 바코드 시스템의 진화된 기술이다. 바코드와 가장 큰 차이점은 언제, 어디서나, 자동 확인 또는 위치 추적이 가능하여 정보 갱신 및 수정이 가능하다는 점이다. 이러한 특성을 갖는 RFID가 공급망에 적용됨으로써 얻을 수 있는 실제 장점들 중 가장 큰 것은 공급망의 전체적인 가시성(visibility)을 제공해 줄 수 있다는 것이다[김동민, 2006].

이렇게 RFID는 도입에서부터 조달, 생산, 분배, 최종 소비자까지의 전체 분배 채널을 관리하기 위한 통합시스템을 구축함으로써, 단편적인 단계의 최적화가 아닌 전체 시스템의 최적화를 추구할 수 있는 장점이 있다[과학기술부, 2006]. 그러나 태그 내장 장소의 은닉과 유일한 ID를 가지는 RFID 특성은 보안 및 개인 프라이버시 측면의 침해 가능성 문제를 제기한다.

2.2 프라이버시의 이론적 배경

프라이버시는 1890년 미국의 사뮤엘 워렌(Samuel Warren)과 루이스 브랜다이즈(Luise Brendies)가 하버드 법률 회보에 개제한 논문(The Right to Privacy)에서 처음 정의하였는데, 프라이버시에 대한 권리를 "홀로 있을 권리(The Right to be Alone)", 즉 간섭 받지 않을 권리로서 제시하였다. 초기 프라이버시 개념은 개인 삶의 영역에서 최소한의 방어적 의미로 해석 되었다. 반면 최근에는 자신의 정보에 대한 통제권을 보장하는 정보 프라이버시(Information Privacy)까지 확장된 개념으로 발전하고 있는데[산업자원부, 2006], Davide Bansister 외 1인[2006]은 확장된 프라이버시의 개념을 다음의 네 가지로 정의하고 있다. 개인의 데이터를 통제하는데 관련한 정보 프라이버시(Information Privacy), 신체의 존엄성을 해치는 개인정보 침해와 관련한 신체적 프라이버시(Bodily Privacy), 다양한 통신형태로 의사소통하는 개인의 이해관계와 관련한 통신 프라이버시(Privacy of Communication), 그리고 특정 공간이나 영역으로의 침입을 제한하거나 경계 설정과 관련한 영역적 프라이버시(Territorial Privacy)이다.

정보화 사회로의 진전은 복잡한 방법과 다양한 영역에서 개인 프라이버시를 발생시켰다. 또한, 현대 사회의 복잡성으로 인해 개인 프라이버시 침해는 여러 가지 프라이버시 침해 요소가 복합적이고 동시적으로 일어난다. 결국 개인 정보 침해 문제는 다양한 정보가 여러 영역에서 수집, 저장, 축적, 관리, 활용되는 것에 기인하며, 개인의 다양한 성향을 사전 동의 없이 제 3자에게 제공하여 피해가 발생하게 된다.

2.3 RFID의 프라이버시 위협요인 및 보호

(1) RFID의 프라이버시 침해 요인

국가 인원위원회가 한국노동사회연구소에 연구를 의뢰하여 발표한 "사업장 감시 시스템이 노동인권에 미치는 영향 실태 조사" 보고서에 따르면, 전자 감시 기술이 주는 불안감을 최하 1점, 최고 4점으로 매겼을 때 기술 종류에 따른 불안감은 지문 및 생체인식(3.75점), RFID(3.54점), CCTV(3.38점), 전화송수신 내역 모니터링(3.28점), 전사적자원관리(ERP, 3.19점), 출입카드(3.07점), 하드 디스크 모니터링(2.91점), 인터넷 모니터링(2.82점)으로 나타났다[이철호, 2006].

조사와 같이 정보 기술의 발달 중에서 시민의 위협으로 다가온 기술 중 하나가 RFID 기술이다. RFID가 유비쿼터스 환경 구현의 핵심으로 향후 관련 산업의 활성화와 고용 창출 등을 통한 경제적 효과를 제시하지만, 전례 없이 방대

한 정보를 수집 및 활용함으로써, 개인 프라이버시 침해를 가능하게 할 수 있는 것을 짐작할 수 있다.

〈표 1〉 기존시스템과 RFID 시스템과의 차이

구분	기존시스템	RFID 시스템
정보접근 매개요소	사용자 ID, 암호, 공인인증서	RFID 코드 ID
정보생성 주체	개인, 서비스 관련 업체	제조업체[개인과 무관] ID 이력, 실시간 정보 관리시스템
정보	개인신상정보[개인] 부가정보 : 개인의 성향 등 관리 정보[관리자]	물품정보, 제조업체 정보, 이력 정보, 실시간 정보
정보의 특징	정보와 개인간의 관계는 직접적	개인과 직접 연관성이 없는 매개요소를 통한 정보의 생성 및 변화

자료 : 한국유통물류진흥원, "무선인식 개인정보보호에 관한 국내외 동향 조사 연구", 2006.

<표 1>은 기존 시스템과 RFID 시스템과 수집되는 정보의 차이점을 보여준다. 가장 두드러진 차이점은 정보의 연관성이 정보 주체와 직접적인지 간접적인지에 있다고 볼 수 있는데, RFID는 비접촉식으로 정보 주체가 아닌 제 3자를 통해 정보가 수집 및 생성될 수 있기 때문에 문제가 발생한다 할 수 있다.

RFID 관련 프라이버시 문제에 관하여 정부만[2006]은 최근 연구에서 보다 자세히 RFID 시스템을 이용한 프라이버시 침해 경우를 4가지로 구분하여 제시하였는데, RFID 태그에 개인정보를 기록하는 경우, RFID 태그에 기록된 개인 정보를 수집하는 경우, RFID 태그의 물품정보와 특정 개인의 정보를 연계하는 경우, 마지막으로 기타 태그가 부착된 물품을 구매하거나 사용하는 경우로 제시하였다.

이때, 단순히 RFID 태그에 저장된 물품 정보를 활용하여 재고 관리, 창고 관리 등만을 수행하는 경우, 즉 물품 정보와 개인정보가 연계되지 않는 경우는 프라이버시 보호 적용에서 제외할 수 있다.

따라서 실제로 RFID 시스템 적용 시 개인 프라이버시가 침해 받을 수 있는 영역은 Retail에서 소비자가 태그가 부착된 제품을 구매할 때 나타나게 된다.

(2) RFID 프라이버시 보호 동향

RFID 태그에 개인 정보가 포함된 경우는 물론이고 RFID 태그가 단순히 사물에 관한 정보만을 담고 있다고 하더라도 신용카드 결제 등을 통해 개인 정보와 결합하는 경우에는 프라이버시 침해 가능성이 높아진다. 더욱이 RFID 태그에 개인 정보가 포함되고, 여기에 위치 정보까지 결합하는 경우에는 프라이버시 침해 가능성이 더욱 높아진다 할 수 있다[구병문, 2004].

RFID 기술 개발과 도입 속도에 비해 프라이버시 관련 RFID에 대한 규제적 대응은 전반적으로 미흡한 상황이다[오길영, 2005]. 현재의 규제 현황을 살펴보면, RFID 관련 법규를 마련해 강제적 규제방식을 취하는 미국의 경우와, 일본과 우리나라의 경우처럼 규제책으로 가이드라인을 마련하는 방식으로 구분된다. EU에서는 각 나라별로는 프라이버시와 관련된 시민 단체들이 활동하고 있고 RFID 입법안을 만들 것을 요구하고 있으나 아직까지는 미국이나 일본의 입법례에 대하여 주의를 기울이고 있는 상황에 머물러 있다. 우리나라와 일본의 규제책은, 입법을 시도하기 이전의 과도기적 성격으로 가이드라인을 제정하고 있다. 결국 현재의 법률적 규제는 RFID 시스템이 사회 전반적으로 확대되지 않은 상황에서 제시하는 미봉책으로 여겨지며, 향후 RFID 시스템 도입이 활발하게 이루어질 것으로 예상하면, 개인 프라이버시 보호를

위한 해결 방안이 필요한 실정이다.

2.4 FTC(미연방거래 위원회)의 공정정보 사용 원칙

FTC(Federal Trade Commission : 미연방거래 위원회)는 다양한 상품, 서비스 및 정보에 대한 접근 가능성이 높아짐에 따라, 방대한 양의 개인 정보의 원천이기도 한 월드와이드 맵에서 개인 정보를 어떻게 사용하여야 하는지에 대한 정확한 인지 필요성을 제기하였다. FTC는 온라인상의 개인정보와 어린이의 개인정보를 이슈화하여 다루었으며, 문제들에 대한 대응책으로서 산업자치규제, 기술적 해결방안, 소비자와 사업자에 대한 교육, 행정 규제 등에 논의 하였다. FTC는 1997년 6월에 5가지 공정 정보사용 원칙을 제시하였다<표 2>.

〈표 2〉 FTC의 공정 정보 사용원칙

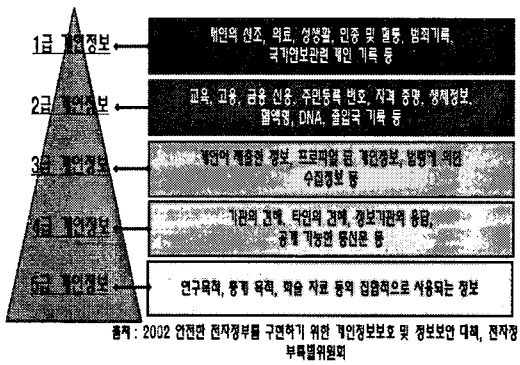
원칙	주요 내용
Notice	어떠한 개인정보가 수집되기 이전에 소비자에게 수집된 정보의 사용에 관한 고지
Choice	소비자에게 수집된 정보가 어떻게 사용되는지에 관해서 개인에게 재량권 부여
Access	자신에 관한 정보에 접근 할 수 있는 권리
Security	정보의 무결성을 보장하기 위해 신빙성 있는 정보 자원 및 익명의 형태로 제공
Enforcement	대안적 강제 집행 차원의 접근법 제시

FTC가 목표하는 바는 크게 3가지로 나누어지는데, 온라인 판매 및 전자상거래와 관련된 잠재적 소비자 보호 문제 확인과 기술과 연구에 관한 프레젠테이션 및 개념과 상황의 변환에 관한 포럼준비, 마지막으로, 효과적인 자율규제 장려를 위함이다.

FTC의 정보 보호 5원칙을 RFID 시스템에 활용할 경우, 기업이 태그 화된 제품 판매 시, 태그에 관한 정보가 고객에게 얼마나 잘 제공되고, 고객이 정보를 받아들이는 정도에 대한 가이드라인으로 활용이 가능하다.

2.5 민감성 적용 프라이버시 보호 등급

개인 정보는 센서와 상황 모델의 적용에 따라 개인의 사적 활동에 대한 정보가 노출되며, 자동 지원 시스템이 증가할수록 개인정보의 노출도 심각하게 된다[송유진 외 1인, 2006]. 정보 노출에 따라 발생 가능한 개인 프라이버시 범위는 개개인의 민감성에 의해 달라지는데, 강용석[2005]은 민감성에 따른 개인정보 5등급을 제시하였다.



〈그림 1〉 민감성에 따른 개인 정보 보호 등급(강용석, 2005)

민감성 등급	분류기준	상세명세
1등급	개인중요 신용정보	범죄기록, 개인 채무 정보
2등급		대출, 보증, 신용카드 정보, 금융 정보
3등급		교육, 주민등록번호, 자격증명, 생체정보
4등급	개인기본 신상정보	프로파일된 개인신상정보
5등급		연구목적 등으로 사용되는 개인 기본 정보(이름, 성별, 주소 등)

〈그림 2〉 개인 민감성 등급

제시한 5등급에서 상위 개인 정보는 출생과 함께 또는 생활 이력에 의해 발생하는 정보이며 개인의 동의와 무관하게 수집되고 보유하게 되는 정보가 대부분이기 때문에, 프라이버시 권리 측면에서 매우 세심하게 다루어져야 한다고 주장하였다. 이는 RFID 적용 시 개인 민감성이 개인 정보 보호 측면에서 세심히 다루어져야 함을 의미한다.

〈표 3〉 호주의 NPP의 민감성 정보

구 분	Nation Privacy Principles 원칙
호주의 National Privacy Principles	NPP 1 - Collection
	NPP 2 - Use and Disclosure
	NPP 3 - Data Quality
	NPP 4 - Data Security
	NPP 5 - Openness
	NPP 6 - Access & Correction
	NPP 7 - Identifiers
	NPP 8 - Anonymity
	NPP 9 - Transborder Data Flows
	NPP 10 - Sensitive Information

자료 : The National Privacy Principles, 2005.

호주의 경우, 개인 프라이버시 원칙을 제시함에 있어, Privacy Notices, Direct Marketing, Due Diligence로 이루어져 있던 1988년의 프라이버시 법(Privacy Act)의 프라이버시 부분을 재검토하여, 2005년 국가 프라이버시 10 원칙(National Privacy Principles)을 제시하였다.

그 중 NPP 10번째 원칙인 민감성 정보는 "개인 동의가 없고, 법적으로 타당한 정보 수집이 이루어지지 않거나, 불법 또는 클레임이 발생될 수 있는 정보 또는 수집하는 정보가 개인의 삶 또는 건강을 심각하게 위협할 경우 조직은 개인 정보를 수집할 수 없음"으로 정의한다[NPP, 2005]. 이는 개인 프라이버시의 경우, 개인 정보에 대한 개개인의 민감성 정보에 대한 동의가 없을 경우, 어떠한 조직도 개인 정보를 수집할 수 없음을 의미한다.

(1) 고객 민감성 등급

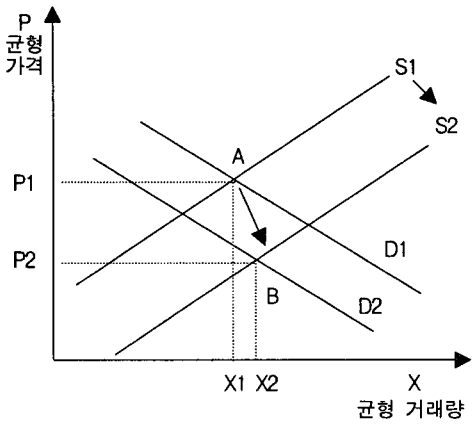
강용석[2005]이 제안한 개인정보 5등급 개인정보는 일반적인 개인정보 분류이다. 개인정보 5등급을 본 연구에 적용하기 위해서는 RFID 특성을 고려한 재정의가 필요하다. 기존의 개인정보를 개인 신용정보의 중요도를 적용시켜 개인정보 등급을 RFID가 활용되는 현실에 맞게 제시하였다.

개인신용정보는 법률 제 7344(2005년 1월 27일 공포, 2005년 4월 28일 시행)에서 자세하게 개념을 제시하는데 다음과 같다.

- 금융실명거래 및 비밀보장에 관한 법률 제 4조의 규정에 의한 금융거래 내용에 관한 정보
- 고객 성명, 주소, 주민등록번호(외국인의 경우 외국인등록번호 또는 여권번호), 성별, 국적 등 거래 주체를 식별할 수 있는 정보
- 증권회사 매매계좌에 예탁한 금전 또는 유가증권 총액에 관한 정보
- 대출 · 보증 · 담보제공 · 당좌예금 · 신용카드 · 할부금융 등 금융거래 내용
- 개인 재산 · 채무 · 소득의 총액 · 납세실적 등 신용도 판단을 위하여 필요한 정보

(2) 프라이버시 보호 수준 측정

개인 정보를 권리가 아닌 이익 관점에서 접근하여 수요 · 공급 측면에서 살펴보면 개인은 개인 정보 공급자가 되며, 기업 및 공공기관(혹은 정부)는 개인 정보 수요자가 된다. 채승완 외 3인[2007]은 개인 정보 보호 수준을 측정하기 위해, 개인 정보도 시장에서 수요 · 공급에 의해 균형가격과 균형 거래량이 결정된다고 보았다.



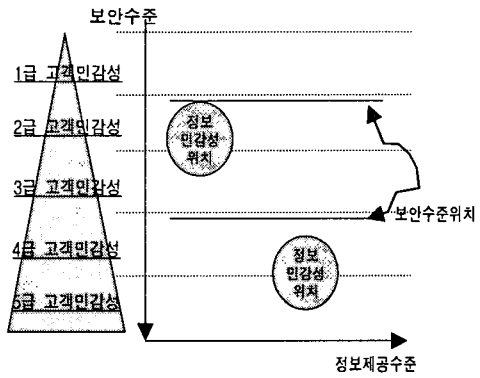
〈그림 3〉 정보보호수준의 변화와 가격 및 거래량
(채승완외 3인, 2007)

<그림 3>은 개인 정보보호 수준이 강화되면 개인 정보 공급자인 개인은 동일한 가격에서 개인정보 제공 리스크가 감소하므로 개인 정보공급량을 증가시키게 되어 결국 공급곡선이 S2로 우측 이동하는 것을 의미한다. 마찬가지로 개인정보 보호 수준 강화는 개인정보 수요자인 기업의 개인정보 수집 관련 비용 증가 및 침해사고 발생에 대한 배상비용 증가로 개인 정보 수요량이 감소하게 되고 결국 수요 곡선이 D2로 이동하는 것을 의미한다[채승완 외 3인, 2007].

공급-수요 곡선의 의미는 효율적인 개인 정보보호 수준을 측정을 할 경우, 개인이 원하는 정보보호 수준보다 높은 보호 정책을 제공하면 개개인의 개인 정보 차이에서 제기되는 불안감을 효과적으로 만족할 수 있다는 점이다.

개인 정보보안 수준은 고객이 선택한 5가지 민감성 등급에 따라 달라지는데, <그림 4>는 고객 민감성으로 선택된 개인 정보 보안 수준을 제시한다.

예를 들어 고객이 4급 민감성 정도를 선택하였다면, 3급 수준에서 개인 정보보호 등급을 제공함으로써, 정보보안 수준의 신뢰성을 얻을 수 있음을 의미한다.



〈그림 4〉 개인 정보보안 수준

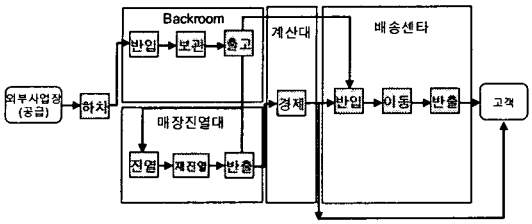
(3) 유통단계에서 프라이버시 침해 가능성

RFID 프라이버시 관련 침해가 여러 부문에서 발생할 수 있지만, 침해가능성이 높고, 시급히 대책을 마련해야할 부문이 유통단계라 할 수 있다. 따라서 유통단계에서 발생할 수 있는 프라이버시 침해가능성을 보다 심층적으로 분석하여, 프라이버시 보호를 위한 방안을 도출하고자 한다.

RFID 시스템은 SCM상에서 실시간 정보를 제공함으로써 제조에서부터 고객에 이르기 까지 정보를 실시간으로 통합 관리할 수 있게 한다. 시스템 도입은 데이터 흐름 커뮤니티를 통하여 수많은 데이터를 수집할 수 있는데, 특히 고객과의 접점인 유통단계에서 개인 위치 정보, 판매정보 등과 같은 많은 데이터 수집이 가능하다.

한국유통물류진흥원[2007]에 따르면, RFID를 기반으로 하는 제품의 흐름상에서 발생하는 실시간 정보들은 EPC Network상에 저장되며, 유통단계에서 RFID 적용 제품의 흐름은 <그림 5>와 같다.

Gerasimos Marketos 외 1인[2006]은 유통산업에서의 RFID 시스템 도입은 기업에게 다음과 같은 3가지 측면의 정보를 제공할 수 있다고 제시한다. 구매 전·후의 결과(Sequence of Purchase), 긍정적/부정적 성향(Positive/Negative Prefer-



〈그림 5〉 RFID 적용 매장에서 제품 흐름
(한국유통물류진흥원, 2007)

ences)파악, 고객 노선(Routes of Customers) 분석을 통한 상품배열의 최적화 등이다. 이같이 RFID 시스템은 기업에게 유용한 정보를 제공하지만, 개인정보와 관련된 여러 측면의 정보를 제공한다는 것은 정보의 제공 정도에 따라 개인 프라이버시 침해가 발생할 수 있음을 의미한다.

즉, Garfinkel, et al.[2005]은 SCM 상에서 RFID에 의한 개인 프라이버시 침해 요인 발생 가능한 영역을 제시하는데, SCM 전체 영역에서 프라이버시 침해가 일어나는 것이 아니라, 고객과 만나는 접점인 유통단계에서부터 나타나게 된다.

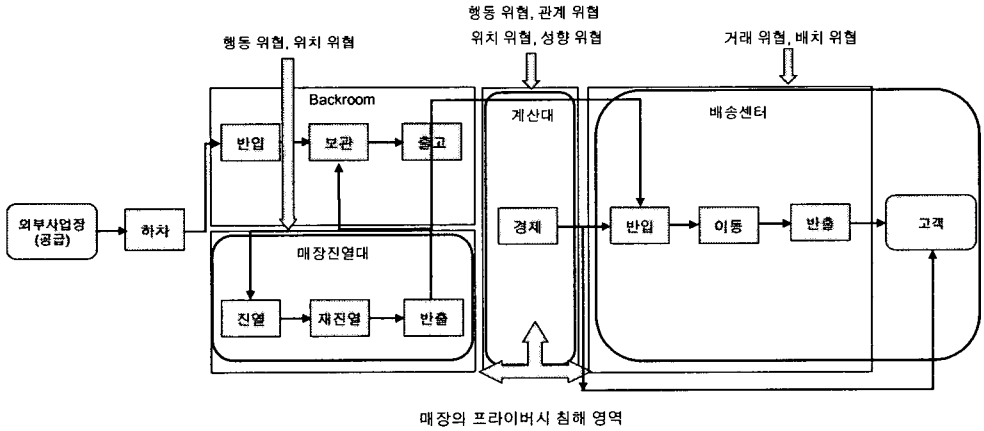
유통단계에서 개인 프라이버시 침해 요인은 크게 행동추적 위협, 관계 위협, 위치위협, 성향 위협, 배치위협, 거래위협으로 분류되며 이를 구체적으로 살펴보면 다음과 같다[Garfinkel, et al., 2005].

행동 위협(Action Threat)은 개인과 관련 있는 다수의 태그 정보들을 모니터링하여 종합함으로써 개인의 행동을 유추할 수 있음을 의미한다.

관계의 위협(Association Threat)은 고객이 태그가 부착된 제품을 구매할 때 고객의 정체성(Identity)은 제품의 전자적 시리얼 번호와 함께 기록되며, 이는 개인 프라이버시 침해 문제를 발생시킨다. 또한 제품군이 아니라, 태그가 부착된 경우 하나의 특정 제품을 알려주는 특성이 있으므로, 이는 개인 프라이버시 침해의 요소로 부각될 수 있다.

위치 위협(Location Threat)은 여러 개의 리더기를 특정 장소에 분산 배치함으로써 두 가지 프라이버시 위협 요인을 유발한다. 우선 개인이 운반하는 특정 태그로 인하여 그 사람의 위치가 모니터링 되며, 두 번째는 태그가 부착된 물건의 위치가 여과 없이 노출되는 것을 의미한다.

좋아하는 성향 위협(Preference Threat)은 EPC 네트워크와 함께 태그가 부착된 제품은 생산업자, 상품의 종류, 상품의 특성이 제품을 구매한 개인의 구매성향과 일체화됨으로써 개인이 무엇을 좋아하는지 예상이 가능하게 된다.



〈그림 6〉 매장 업무 흐름 별 프라이버시 침해 위협 요인

배치 위협(Constellation Threat)은 태그가 부착된 제품이 소비자가 인식하지 못한 상황에서 놓여지고, 제품에 부착된 다수의 태그 정보를 바탕으로 추적이 가능하기 때문에, 소비자들은 불안함을 가지게 된다.

마지막으로 거래 위협(Transaction Threat)은 태그가 부착된 제품이 다른 장소로 이동할 때, 사람들 사이의 거래내용이 쉽게 추론 가능해지며, 무엇을 샀는지, 어떻게 거래를 하였는지 등등의 거래 관련 정보를 제 3자가 알게 됨을 의미한다.

RFID를 적용 시 나타날 수 있는 개인 프라이버시 침해 요인들을 매장 업무 흐름별로 제시하면 <그림 6>과 같다. 일반적으로 유통업체에서 구매 부서를 통해서 입고된 제품은 매장 진열대에서 고객의 카트를 통해 계산대로 이동을 한다. 그리고 고객이 제품을 폐기할 때까지 태그는 존재하게 된다.

RFID 시스템에 의해 프라이버시 침해 가능성이 존재하는 부분은 매장에 진열될 때부터 시작된다. 매장 진열대에서는 행동 위협, 위치위협이 발생 가능하다. 고객이 제품을 선택해서 계산대에 이르렀을 때는 행동 위협, 관계 위협, 위치 위협, 성향 위협이 발생가능하다. 제품을 구매한 후에도 개인 프라이버시 위협은 사라지지 않는다. 즉, 제품 내 부착된 태그는 전 세계에서 유일한 것이고, 고객이 제품을 폐기할 때까지 고객이 구입한 제품에 부착되어 있다. 또한 고객의 입장에서는 사후 서비스를 받아야하기 때문에 RFID 태그를 제거할 수 없기에, 제품이 매장을 떠났을 때부터 고객이 제품을 폐기할 때까지 발생 가능한 위협은 거래 위협과 배치 위협이 존재할 수 있다.

따라서, RFID가 고객과의 접점 시 발생하는 6가지의 위협 요인들에 대하여, RFID 시스템 보안 기술들이 완벽하게 이루어져야 한다. 또한, 제 3자가 악의를 가지고 타인의 개인정보를 수집할 수 없도록 프라이버시 보호 관련 법규를 법제화하여 시행하여야만 한다. 하지만, RFID 기술이 도입 초기에 있고, 산업에 적용하는 수준도 시범사업 단계에 머물러 있어 자칫 지나치게 엄격한 법제화 시도는 이제 관심이 증가되는 RFID 개발 및 도입활동을 위축시킬 문제점이 있다.

이에 따라, 유통단계에서 고객 접점에서 발생할 수 있는 개인 프라이버시 침해 요인을 해결하기 위한 체계적인 프레임웍과 상세한 가이드라인을 제시하는 것이, 법제화 이전에 기업 자체적으로 해결할 수 있는 보다 현실적인 방안이라 할 수 있다.

따라서, 본 연구에서는 앞에서 제시한 개인 민감성 등급과 개인 프라이버시 보호 수준을 이용하여 "고객 민감성 적용 프라이버시 보호 프레임웍"을 제안하고자 한다.

3. 고객 민감성 적용 프라이버시 보호 프레임웍 개발

RFID 시스템 도입으로 인해 발생할 수 있는 개인 프라이버시 침해에 대한 방안으로 이병길 외 2인[2005]은 제품 라이프 사이클과 관련 있는 사용자(공급자, 유통업자, 고객)들에게 정보의 접근 권한을 부여하여 권한에 맞는 정보만을 제공하여 프라이버시 침해를 막고자 하였다. 즉, 제품관련 프라이버시 등급을 9등급으로 제시하고 정보 접근 권한이 높은 사용자는 프라이버시 8~9등급을 부여 받아 제공하는 정보를 모두 볼 수 있고, 권한이 낮은 사용자는 프라이버시 1~2등급을 부여받아 적은 정보만을 제공하도록 하였다. 본 연구는 프라이버시 등급을 제시한 측면에서는 긍정적이나, RFID 태그에 저장된 정보에 대해서 개인들이 인지하는 프라이

버시 수준은 개인별로 차이가 있을 수 있음에도 불구하고, 태그 및 태그와 연계된 정보시스템에 저장되는 정보의 개수에 따라 프라이버시 등급을 결정하였다. 이에 따라, 정보시스템에 저장되는 개인 정보의 상대적 중요도의 차이는 물론, 개개인 마다 상이한 프라이버시 민감도를 해결하기에는 어려움이 있다.

한편, Alan R. Peslak[2005]는 FTC(Federal Trade Commission)에서 제시한 정보 5원칙을 이용하여 RFID 시스템과 고객이 만나는 시점인 유통단계에서 발생할 프라이버시 침해 해결을 위한 정책적 체크리스트를 제시하였다. Simson Garfinkel[2002]는 "RFID Bill of Right"에서 RFID 태그에 저장되는 정보 수집 방법을 공개해야 한다는 정보공개 5원칙을 제시하였다. 하지만, 이들 연구는 범용적인 가이드라인 수준에 그쳐 기업에서 도입하여 활용하기에는 어려움이 있는 실정이다.

즉, 기존의 프라이버시 침해 해결 방안의 문제점은 프라이버시 수준을 정보의 양만으로 분류하고, 제공되는 정보의 상대적 중요도와 적용 단계에서 필수적인 개인의 민감성 부분을 감안하지 못한 점이다, 또한, 기업들이 실무적으로 운용할 수 있는 구체적인 프로세스 설계가 제시되지 않아, 프라이버시 보호를 위한 대책수립이 어려운 점이다.

따라서, 본 연구에서는 "개인 민감성에 따른 프라이버시 보호 프레임웍"을 제안하고자 한다. 개개인의 정보보호에 대한 만족은 당사자가 느끼는 침해수준의 민감성 정도에 따라 달라진다. 개인정보 제공을 개인 민감성에 의해 직접 선택하도록 한다면, 적절한 정보 제공 수준을 파악할 수 있을 뿐 아니라 개인이 느끼는 수준 이상의 프라이버시 등급을 제시함으로써 프라이버시 침해를 방지할 수 있다[채승완 외 3인, 2007].

제안하는 "개인 민감성에 따른 프라이버시 보호 프레임웍"은 "Service Contents"와 "고객 민감성 등급"으로 구성되는데, RFID를 적용했을 때, 네트워크에 수집되는 정보인 "Service Contents"를 고객이 선택한 "민감성 등급"의 수준으로 조절하기 위함이다.

Service Contents는 RFID 시스템 적용 시 EPCglobal 네트워크상에서 수집되어지는 정보들을 지칭하며, 크게 EPC코드, 자사코드, 상품 일련번호로 이루어지는 Tag Information과 EPC 네트워크상에 저장되는 정보인 제품 정보, 유통 정보, 고객 정보들로 분류된다.

고객 민감성 등급은 앞에서 제시했던 공개되는 개인 정보의 중요도에 따른 민감성 등급에 의해 1등급에서 5등급으로 나타난다. 받아들일 수 있는 프라이버시 민감도는 개개인 마다 틀리고, 네트워크상에 수집된 정보가 직접적으로 프라이버시 침해로 진행되는 것보다 정보의 수집, 가공에 의해 프라이버시 침해가 정도가 커지게 됨을 감안하면, 개인 정보보호는 고객마다 차이가 난다. 즉, 수집되는 정보가 같더라도 개개인 마다 상이한 프라이버시 수준 때문에 적용할 프라이버시 보호 수준이 상이하게 달라진다. 이러한 문제를 해결하기 위해, 본 연구에서는 민감성 등급을 고객이 직접 선택하고 등급 수준에 맞는 정보만을 기업에게 제공하는 방안을 제시하고자 한다.

즉, RFID 정보와 고객민감성 등급으로 제시된 프레임웍에서 고객이 제시하는 민감성 등급에 따라 EPC IS에 저장되는 개인정보의 양을 제한한다. 이를 통해 개인이 정보를 제공하더라도 제공하는 정보의 양을 직접 선택하기 때문에, 프라이버시 침해 가능성은 사라지게 된다. 더불어 등급에 따른 태그 삭제 정보들은 기업 정책과 외부 현황에 따라 달라진다.

<표 4>는 네트워크상에 수집되는 정보들을 고객 민감성 등급에 의해 선택적 제거 및 파기

〈표 4〉 RFID 프라이버시 보호 등급 프레임웍

RFID 정보 / 고객 민감성 등급	Service Contents											
	Tag Information			EPC Information Service								
				제품 정보						유통 정보	고객정보	
	EPC 코드	자사 코드	상품 일련 번호	제조일	가격	제품명	제품 명세	A/S 정보	태그 삭제일		고객 ID	고객 명세
1	O	O	O	×	×	×	×	×	×	×	×	×
2	O	O	O	×	×	×	×	×	×	×	O	×
3	O	O	O	O	O	×	×	O	×	O	O	×
4	O	O	O	O	O	O	O	O	×	O	O	×
5	O	O	O	O	O	O	O	O	×	O	O	O

를 가능하게 하는 제안하는 "RFID 프라이버시 보호 등급 프레임웍"이다.

제안하는 고객 민감성에 따른 프라이버시 등급은 다음과 같다.

- 1급 고객 민감성 : 고객 민감성 등급 중 가장 민감하게 받아들이는 등급이며, 개인 사생활 침해가 큰 제품들의 경우, 고객이 1등급으로 제시할 가능성이 크다. 1등급의 경우 태그, EPC IS에 들어가는 정보들을 모두 파기하는 것을 원칙으로 한다.
- 2급 고객 민감성 : 태그 정보만 남겨 두고 모두 파기를 함으로써, 고객이 민감하게 생각하는 정보를 제거할 수 있다. 본 연구에서는 고객이 3등급으로 제품에 대한 민감성을 정할 경우 고객이 생각하는 고객 민감성에 대한 만족을 느끼게 하기 위해 2등급을 선택하여 관련 정보를 부분 파기함으로써 개인 프라이버시를 보호한다.
- 3급 고객 민감성 : EPCIS에 들어가는 정보들 중 제품명, 제품명세, 태그 삭제일, 고객 정보를 제외한 정보를 남기며, 고객이 향후 제품에 대한 A/S를 받을 때 좀 더 쉽게 서비스를 받도록 도움을 주게 된다. 또한, 고객이 4등급 선택 시 본 등급을 선택하여 관련 정보를 부분 파기를 한다.
- 4급 고객 민감성 : 태그 정보, 상품 정보, 유통 정보를 모두 남기고 고객 정보 중 고객명세를 제거함으로써, RFID 프라이버시 침해 요소가 보다 적은 경우 사용할 수 있게 한다.
- 5등급 고객 민감성 : 민감성 등급 중 개인 사생활 침해가 별로 없는 제품이라 생각하는 경우 5등급을 선택 할 가능성이 크다. 5등급의 경우, 모든 정보를 남겨둠으로써, A/S 및 기업적 서비스 활동에 도움을 주게 된다.

제안한 "개인 민감성에 기반한 프라이버시 보호 프레임웍"은 개개인 마다 틀린 프라이버시를 고객이 직접 자신이 허용할 수 있는 정보양을 제시하는 등급을 선택함으로써, 기존 연구가 해결하지 못했던 개개인 마다 상이하게 틀린 프라이버시 보호 수준 측정과 수준에 맞는 정보제공이 가능하며, 시스템에 적용이 가능하다.

개인 프라이버시 보호 수준 제시와 더불어 기업이 실제 사용할 수 있도록 제안한 프레임웍 상세 설계 및 사례 연구를 통해 현실성 있는 방안으로서 제안하고자 한다.

4. 프레임웍의 상세설계 및 사례 연구

제시된 프레임웍의 실무적용 타당성과 기업

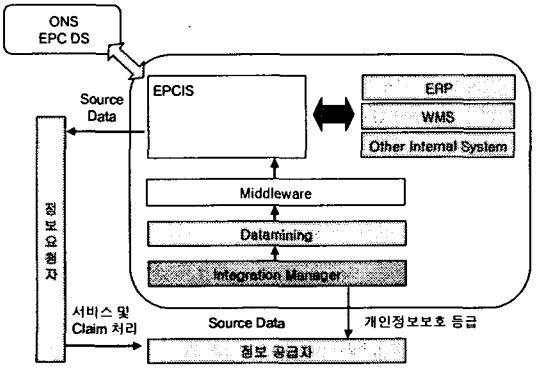
들에게 보다 구체적인 가이드라인을 제시하기 위해서는 프레임웍에 대한 상세 설계가 필요하다. 이에 따라, 보다 구체적인 상세 설계와 사례 적용을 검토하고자 한다.

4.1 프라이버시 보호 프레임웍 상세 설계

(1) RFID Architecture

EPC를 유일한 코드 값으로 상품의 추적성(Traceability)과 가시성(Visibility)을 제공하는 EPCglobal 네트워크는 태그, RFID 리더, ALE (Application Level Events), EPCIS(EPC Information Service), ONS(Object Naming Servie), EPCIS DS(Discovery Service)로 구성된다[리테일테크, 2006].

EPC global 네트워크는 기본적인 RFID 적용 제품 및 위치 등과 같은 정보들의 흐름만을 정제하여 저장 및 필요 요소들마다 제공한다. 따라서 프라이버시 침해 해결을 위한 Architecture는 다음 <그림 7>과 같이 제시할 수 있다.



〈그림 7〉 RFID Architecture

본 RFID Architecture의 주요개념은 다음과 같다.

- 정보 공급자 : RFID 적용 제품과 관련된 사람을 의미하며, 정보 공급자는 Source Data를 제공하고, 개인 정보보호 등급을 제공받는다.
- 정보 요청자 : RFID 전 단계에서 누구나 정보 요청자가 될 수 있으며, 정보 공급자가 제시하는 개인 정보 보호 등급만큼 Source Data를 제공받을 수 있으며, 정보를 활용할 수 있다.
- Integration Manager : 정보 공급자가 원하는 민감성 등급 수준, 각종 정보 공급자의 정보와 RFID 흐름에서 수집되는 정보들을 취합하는 부분이며, Integration manager의 특징은 정보 공급자의 정보 중 고객이 선택한 민감성 등급의 수준에 맞추어 정보를 미들웨어로 보내는 역할과 고객이 선택한 등급 수준의 개인 정보보호 기능을 제시한다.
- Datamining : RFID 리더를 통해 판독한 RFID 정보로부터 정제되고 통합된 EPC 데이터를 얻을 수 있도록, 각종 정보를 상황에 맞게 정제 및 통합하여 EPCIS로 정보를 보내는 역할을 한다.
- Middleware : EPCglobal 네트워크의 ALE (Application Level Events)을 포함하는 개념으로써, RFID 정보로부터 정제하여 통합된 EPC 데이터를 얻는 소프트웨어 인터페이스로서 어플리케이션을 위한 인터페이스를 제공 및 각종 데이터를 처리하는 역할을 한다[김동민, 2006].
- EPCIS(EPC Information Service) : EPCglobal 네트워크에서 게이트웨이 역할을 담당하는 구성 요소이며, 미들웨어로부터 태그 및 RFID 각종 이벤트 정보를 제공 받아 이를 이용하여 객체(제품/상품, 박스, 팔레트 등)의 상태 및 정보 관리를 하며 이러한 행동을 통해 거래 파트너 간에 가시성과 추적성을 제공하기 위한 객체 정보를 공유하는 역할을 한다.

EPCglobal 네트워크를 중심으로 태그가 부착된 객체의 흐름을 통해 EPC 정보 공유 및 프라

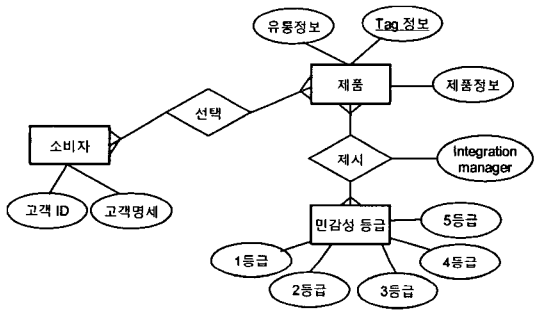
이버시 침해 해결을 방향인 개인정보보호 등급 제시를 위한 절차는 다음과 같다. 첫째, 제품 라이프사이클의 각 단계에서 제품의 이동이 발생하면 제품 이동과 더불어 제품이 지나가게 되는 위치의 RFID 리더에 의해 RFID 태그의 정보가 수집된다. RFID 관련 정보 수집 시, 개인 프라이버시와 관련된 정보가 수집될 경우, 정보공급자(고객)은 자신이 원하는 만큼 데이터(Source Data)를 제공한다. 둘째, 이렇게 수집된 많은 RFID 관련 정보들은 1차적으로 Integration Manager에게 보내지고 Integration Manager는 태그정보를 비롯해서 개인정보부분을 정보 공급자가 원하는 만큼의 정보만 미들웨어에 제공된다. 셋째, 이렇게 수집된 정보는 미들웨어에 보내지기 전 데이터마이닝을 걸쳐 필요 정보로 전환이 된다. 넷째, 1차적으로 RFID 미들웨어에 의해 EPCIS에서 요구되는 이벤트 스펙에 따라 처리되고, 미들웨어에서 걸러진 EPC 이벤트 정보는 EPCIS에 전달되어 리파지토리에 저장되거나 EPC 이벤트 정보를 필요로 하는 기간 운영시스템(ERP, WMS 등)에 전송되어진다. 마지막으로, EPCIS에 저장된 EPC 이벤트 정보는 EPCIS에 의해 ONS와 EPCDS에 전송되어 저장되고, EPCDS에 저장된 제품에 대한 EPC 이벤트 이력 정보들은 이후 정보 요청자의 요청으로 EPC를 통한 제품 이력 조회 및 실시간 제품 정보 조회 시 사용된다.

(2) 프라이버시 대응 상세 설계 방향

RFID 시스템의 장점은 반대로 개인 프라이버시 침해를 가져오는 문제로서 제기되고 있다. 이러한 문제를 해결하기 위해, 본 연구에서는 앞에서 제시한 "개인 민감성 등급" 프레임웍과 RFID Architecture를 이용하여 "RFID 대응 개인 프라이버시 보호 프로세스 설계 방향"을 제시하고자 한다.

소비자는 제품을 매장에서 선택하여 구매 결정을 할 때, "개인 민감성 등급"을 개인 주관에 의해 제시하며, 제시된 민감성 등급은 "Integration Manager"에 의해 제품의 네트워크상에 적용된다. 이때, 민감성 등급에 따라 삭제되어야 할 RFID 정보들은 기업에 제공되기 전에 삭제되어 제공된다.

<그림 8>은 프라이버시 대응을 위한 프로세스 상세 설계를 위한 간단한 ER-Diagram이다.



〈그림 8〉 프라이버시 대응을 위한 E-R Diagram

제시한 ER-Diagram 모형은 <표 5>의 Pseudo code로 표현할 수 있다.

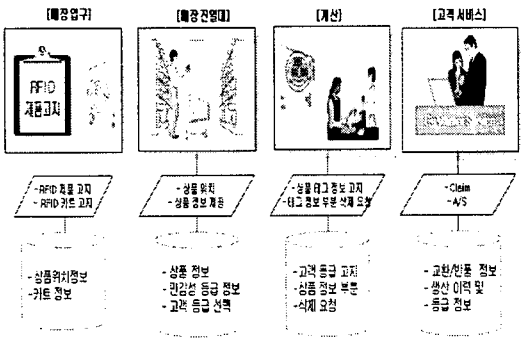
〈표 5〉 Pseudo Code(수도코드)

```
1          소비자 = 고객ID
2          select 상품 (tag information)
           // 상품 구매(결제)시 민감성 등급 제시
3          grade = 1, 2, 3, 4, 5
          // Set data when program beginning
4          if 1등급 than
5            delete 제조일, 가격, 제품명, 제품명세, A/S
                 정보, 태그 정보, 유통정보, 고객 ID,
                 고객 명세
6          else if 2등급 than
7                delete 제조일, 가격, 제품명, 제품명세,
                 A/S정보, 태그삭제일, 유통정보, 고객
                 명세
8              else if 3등급 than
9                  delete 제품명, 제품명세, 태그삭제
                       일, 고객명세
10                 else if 4등급 than
11                     delete 태그삭제일, 고객명세
12                 else if 5등급 than
13                     delete 태그삭제일
14                   endif
15                endif
16             endif
17         endif
18     endif
19         save DB
```

4.2 프라이버시 대응 프로세스 사례

앞에서 제시한 "개인 민감성 등급 프레임워크"와 "RFID 대응 프로세스 설계 방향"은 RFID 도입 기업이 실제 적용 가능한 이론적인 내용이라 할 수 있다. 실제 유통단계에서 RFID가 적용될 경우, 단순히 민감성 등급 프레임웍과 상세 설계만으로는 고객이 RFID 제품을 구매할 때, 프라이버시 침해까지 고려할 것이라고 장담할 수 없다. 따라서 제안한 내용들을 기반으로 가상 사례를 이용하여 프로세스를 제시함으로써, 보다 효과적으로 본 연구의 내용을 이해 할 수 있도록 제시하고자 한다.

RFID 특징인 실시간 이력정보 제공은 SCM 상에서 획기적인 비용절감을 가져오는 반면, 프라이버시 침해의 가능성을 가지게 된다. 그 중 프라이버시 침해의 부분은 제품과 고객이 만나는 접점이며, 고객과 만나는 접점은 SCM에서 유통단계에서 주로 나타난다. 다음 <그림 9>는 제품이 고객과 만나는 시작점인 매장 입구에서부터 사후 고객 관리까지의 프로세스를 제시하였다.



〈그림 9〉 CASE 프라이버시 프로세스

RFID 적용 시 발생 가능한 프라이버시 침해 해결은 FTC(Federal Trade Commission)에서 1997년에 언급한 다섯 가지 요소인 Notice(공지), Choice(선택), Access(접근), Security(보안), 그리고 Enforcement(집행/시정)으로 가능하다. 유통단계에서는 고객에게 RFID 제품이 매장에 있다는 것과 어떠한 영역에서 사용되고 있는지를 정확하게 고지할 필요가 있으며, 고객에게 개인 정보가 EPCIS에 들어갈 수 있음을 정확하게 알려야한다. 또한, 고객이 RFID가 적용된 제품을 구매하려할 때, 개인 정보의 정확한 사용 방향과 고객이 제공할 수 있는 정보를 직접 선택할 수 있는 권리를 제공하여야 한다.

따라서, 유통단계에서 고객과 RFID가 접촉하게 되는 쇼핑 동선에 따라 발생 가능한 프라이버시 침해 요소와 해결 방향을 가상 사례를 통하여 제안하고자 한다. <표 6>은 매장 입구에

〈표 6〉 프라이버시 가상 사례 프로세스 - 콘돔 구매

위치	프라이버시 침해 위협 요인	가상사례 주요 사항	비고
매장 입구	행동 위협	- 매장 입구에서 RFID 관련 정보제공 - Display 설치 카트 정보 제공	Notice
매장 진열대	행동 위협, 위치 위협	- 콘돔제품 위치 및 관련 정보 제공 - RFID 적용 제품임을 인지 - 고객이 "개인 민감성 등급" 제시, 선택	Notice, Choice
계산대	행동 위협, 관계 위협, 위치 위협, 성향 위협	- 계산원 Display에 제품 ID, 가격, 등급만을 제시(프라이버시 침해 가능성 존재) - RFID 정보 및 고객 선택 등급 재인지 - 등급에 맞는 RFID 정보 삭제 요청	Notice, Choice, Security, Enforcement
사후 관리	거래 위협, 배치 위협	- 클레임, A/S를 위해 인터넷 및 고객 서비스센터를 이용 가능 - Display에는 제품ID와 등급만을 제시 - 서비스 제공 후, 개인 민감성 등급 재인지 및 선택권 제시	Access, Notice, Security, Enforcement

서부터 고객의 사후 관리 시점까지 RFID 적용 프라이버시 침해 위협 요인, 관련 가상 사례, 그리고 FTC의 제 5원칙을 통한 개인정보보호 해결 방향을 제시한 것이다.

(1) 매장입구

유통매장에서는 직접적으로 고객에게 프라이버시 침해 요인을 제공하지 않지만, 간접적으로 고객의 프라이버시 침해 요소가 나타나게 되는데, 고객이 매장에서 리더기를 장착한 카트를 가지고 위치 이동 시 고객 위치정보가 드러날 수 있다. 즉, 쇼핑 동선은 고객이 입장하여 퇴장할 때 까지 매장 안에서 상품의 구매를 위해 쇼핑하는 이동경로를 말하며, 이러한 이동 경로를 도식화하여 고객이 쇼핑을 하면서 방문한 장소, 머무른 장소, 머무른 시간, 지나간 통로들을 파악할 수 있고, 파악한 정보를 기반으로 기업은 매장의 통로를 변경하거나 상품을 재배치하기 위하여 사용하고 있다. 따라서 유통매장 입구에서 고객에게 다음과 같이 프라이버시 침해 요인에 대한 고지를 할 필요가 있다.

첫째, RFID 제품이 매장에 있으며, 어떠한 종류의 제품들이 RFID가 적용되었는지를 사전에 고지한다(Notice).

둘째, RFID 제품을 구매하길 원할 경우 Display를 설치한 Cart를 선택할 수 있는 권리를 고지한다(Notice).

(2) 매장 진열대

Store Shelf 위치에서는 고객이 제품을 선택하기 위해 여러 가지 선택을 하는 단계이다. 이 단계에서 개인 프라이버시 침해 요소는 "행동 위협"이 존재한다. 매장 진열대에서 프라이버시 방지를 위한 행동은 다음과 같다.

첫째, 카트에 장착된 Display에 고객이 선택한 RFID 적용 제품에 대한 고지(Notice) 및 RFID가 사용될 경우 발생 가능한 프라이버시 침해 요인을 고지한다(Notice).

둘째, 고객이 RFID 제품을 선택 할 경우, 연관성이 있는 프라이버시 해결 방안으로 앞서 제시한 "5단계 민감성에 따른 프라이버시 보호 등급"을 Display에 제시한다(Notice). 고객이 제품을 선택하였을 때, 보호 등급을 제시하는 이유는 고객이 미리 자신의 민감성에 의해 등급을 선정할 수 있도록 하는 의미와 더불어 계산 시 업무의 복잡성을 줄이기 위한 방법이다.

셋째, 고객은 제시된 등급에서 자신의 민감성에 맞게 등급을 선정하여 카트의 Display에 입력한다(Choice).

넷째, 선택된 등급은 실시간으로 Integration manager로 이동하여 그 카트에 포함된 제품 등급을 저장한다.

(3) 계산대

개인 프라이버시 침해 가능성이 가장 큰 영역은 Check-out의 단계이다. Check-out 단계에서 고객이 선택한 RFID 적용 제품과 개인 신용정보가 결합하여 프라이버시 침해 부분 존재하게 되며, 이러한 프라이버시 위협 요인은 "행동 위협", "관계 위협", "위치위협", "성향위협"이 있다. 따라서, 이 영역에서 개인 정보보호를 위해 가장 많은 노력을 해야 하며, 개인 정보가 빠져나갈 가능성이 크므로 보안에도 신경을 써야하는 부분이다. 이 단계의 일반적인 프로세스는 다음과 같다.

첫째, 고객은 RFID 적용 제품을 계산 시 계산원은 고객에게 RFID 사용제품임을 재인지 및 고객의 동의를 받는다(Notice, Choice).

둘째, 고객이 선택한 '민감성 등급'과 함께 제시한 등급 보다 한 단계 높은 레벨을 사용함을 공지한다(Notice, Choice).

셋째, 고객이 동의할 경우, 계산대의 디스플

레이에 관련 등급을 클릭한다(이 경우, 각종 제품 정보 중 제품 ID, 제품 가격, 그리고 고객 민감성 등급만 계산원 Display에 제시하여야 한다. 그 까닭은 제품 ID 정보를 제외한 각종 제품정보가 Display에 제공시 개인 프라이버시 침해 가능성 존재하기 때문이다(Notice)).

넷째, Integration Manager로 정보 이동 및 EPCIS상 RFID 정보를 부분을 삭제한다(Enforcement).

다섯째, 고객이 제안한 등급을 언제든 사이트나 고객 서비스 센터를 통해 현재의 등급보다 높은 등급으로 재설정 가능함을 공지한다(Notice, Access).

(4) 사후관리

고객은 구매한 제품을 사용하면서 불만사항이 있을 경우 Claim을 걸거나, 제품에 하자가 생겼을 경우 고객 서비스 센터에서 A/S를 받을 수 있다. 사후 관리 프로세스는 다음과 같다.

첫째, 고객은 RFID 적용 제품에서 자신이 정한 등급을 언제든 상위 등급으로 선택할 권리가 있기 때문에, A/S 또는 Claim을 위해 고객은 인터넷 혹은 고객 서비스 센터에서 제품 번호 및 현재 남은 RFID 정보를 확인할 수 있다(Access, Enforcement).

둘째, Internet Display, 고객 서비스 센터에서는 고객이 선택한 등급을 고객에게 제시하여야 하며, 받을 수 있는 고객 서비스 종류를 제시하여야 한다.

셋째, 고객 서비스 혹은 고객 불만사항 해결 후 고객에게 정보가 어떻게 사용되었는지를 고객에게 공지한다(Notice).

5. 결론 및 향후 연구과제

본 연구는 RFID 시스템 도입으로 발생 가능한 프라이버시 침해 가능성에 대한 해결방안을 찾고자, RFID 시스템 전반적인 이슈를 분석하였다. 분석 결과 나온 침해요소 유형별 위협 요인을 분석하여 RFID 기술에 대한 사회적 우려 요인을 고려한 해결 방향을 제시하였다.

개인 마다 다른 민감성 정보를 EPC 네트워크에 적용할 수 있는 "고객 민감성 적용 프라이버시 등급" 적용 프레임웍을 제시하고, RFID 시스템 적용 시 발생할 수 있는 프라이버시 침해 요소 해결을 위한 프로세스 설계를 제안함으로써, 프레임웍을 기업에서 실제 활용할 수 있도록 하였다. 또한, 제안한 프로세스 설계 방안을 사례연구를 통해 적용시켜 봄으로써, 실제 유통단계에서 RFID 적용 시 단계마다 나타날 수 있는 문제점을 분석하고, 개인 정보보호 프로세스를 제시하였다. 이에 따른 해결방안을 "고객민감성등급"과 FTC의 "개인 프라이버시 5원칙(Notice, Choice, Access, Security, Enforcement)"을 통해 제시하였다.

현재 제시한 프레임웍은 유통단계를 중심으로 사용할 수 있는 형태로 제시하였기 때문에, 다양한 산업에서 사용할 수 있는 범용적 프레임웍 개발을 위해서는 분야에 대한 선행 연구를 실시하여 해당 산업별 특징을 프레임웍에 적용하는 것이 필요하다. 또한, 개발된 프레임웍의 심층적 타당성 분석과 실무적용 가능성을 제고시키기 위해서는 대상 업무에 적용, 실제 시스템 개발과 적용이 필요하다.

참 고 문 헌

[1] 강용석, "개인정보의 정의 및 보호 트랜드", IT Solution 칼럼, 2005.

[2] 구병문, "RFID 도입과 프라이버시 보호 관련 법제 현한 분석", *한국전산원*, 2004.

[3] 김동민, u-SMC하의 제품 수명주기(이력)

관리 시스템 설계 및 구축에 관한 연구, 동국대학교 박사학위논문, 2006.

[4] 김동민, 이종태, "RFID 기반 상품의 효율적 라이프사이클관리를 위한 통합시스템 설계", *대한산업공학회*, 산업공학, 2006.

[5] 김진노, 소홍석, 정하재, "RFID 구축사례 심층 분석", *전자통신동향분석*, 제21권 제2호, 2006년, p. 163.

[6] 김진백, 이동호, "유비쿼터스 2 ; 이력관리 시스템의 900MHz RFID Gen 2의 적용 실험", *한국경영정보학회, 추계학술대회*, 2006.

[7] 리테일테크, "RFID 활용을 위한 네트워크 기술 조사 요구 *최종보고서*", *한국유통물류진흥원*, 2006.

[8] 산업자원부, "무선인식(RFID) 개인 정보호에 관한 국내외 동향 조사연구", 2006년 5월.

[9] 송유진, 이동혁, "개인정보 라이프사이클에 따른 프라이버시 보호 프레임워크, *정보보호학회지*, 2006.

[10] 오길영, "개인정보보호를 위한 RFID 규제에 관한 연구", *정보화정책*, 제12권 제2호, 2005.

[11] 이철호, "RFID와 프라이버시 보호", 한국콘텐츠학회 2006 추계종합학술대회 논문집 제4권 제2호, 2006.

[12] 유승화, 유비쿼터스 사회의 RFID, 전자신문사, 2005.

[13] 전홍배, "제품 라이프 사이클 관리에서 RFID 응용에 관한 연구", *대한산업공학회*, 산업공학, 2006.

[14] 정민화, "무선인식 동향 및 표준화 대응 방향", *기술표준*, 2006.

[15]표정민화, "RFID 국제 및 국가 표준동향", RFID Journal Korea, 2007, p. 36.

[16] 정보통신부, "개인정보보호 지침 해설서", 2005.

[17] 채승완, 민경식, 황성원, 원승재, "개인정보의 경제적 가치 분석에 관한 고찰", 정보보호 Issue Report, 2007.

[18] 한국과학기술평가원, "2005년도 RFID 기술영향 평가 보고서", 2006년 2월.

[19] 한국유통물류진흥원, "무선인식 (RFID) 개인정보보호에 관한 국내외 동향 조사연구", 2006.

[20] EPCglobal, "EPC Information Services", Ver1.0, 2006.

[21] EPCglobal, "The EPCglobal Architecture Framework EPCglobal Final Version", 2005.

[22] Garfinkel, S. L., Juels, A., and Pappu, R., "RFID Privacy : An Overview of Problems and Proposed Solutions", *IEEE SECURITY & PRIVACY*, 2005.

[23] Garfinkel, S., "An RFID Bill of Right", Tech. Rerivew, October 2002, www.technologyreview.com/article/02/01/garfinkel1002.asp

[24] Juels, A., Rivest, R. L., and Szydlo, M., "The blocker tag : selective blocking of RFID tags for consumer privacy", Proceedings of the 10th ACM conference on Computer and communications security, October 2003.

[25] Kelly, E. P. and Erickson, G. Scott, "RFID tags : commercial applications v. privacy rights", *Industrial Management & Data Systems*; Vol. 105, No. 6, 2005.

[26] Kim, J. K., Yang, Chao., and Jeon, J. W., "Issues Related to RFID Security and Privacy", 한국경영정보학회, 춘계학술대회, 2007.

[27] Lee, B. G., Kim, H. W., and Chung, K, I., "Security and Privacy; Security and

Privacy Management for Effective RFID Lifecycle", 한국경영정보학회, 추계학술대회, 2005.

[28] Lee, S. Strickland., and Hunt, L. E., "Technology, security, and individual privacy : New tools, new threats, and new public perceptions", *Journal of the American Society for Information Science and Technology*, Vol. 56, No. 3, 2005.

[29] Lockton, V. and Rosenberg, R. S., "RFID The next serious threat to privacy, Ethics and Information Technology", *Issue* Vol. 7, No. 4, 2005.

[30] Marketos, G. and Theodoridis, Y. "Measuring Performence in the Retail Industry", BPM 2006 Workshops, LNCS 4103, pp. 129-140.

[31] Marc Langheinrich, "Privacy by Design - Principles for Privacy-Aware Ubiquitous System", Ubicomp 2001 Conference, Atlanta, GA, October 2001.

[32] Mohamed, Arif., "RFID privacy guidelines established", *Computer Weekly*, 2006, 5. 9.

[33] Rayhu Das, Peter Harrop, "RFID Forcasts, Player & Opportunities, 2007~2017", IDTechEX, 2007.

[34] Soppera, A. and Burbridge, T. "Wireless identification-privacy and security", *Journal BT Technology Journal,* Issue Vol. 23, 2005.

[35] Stuart C. K., "Securing RFID Applications : Issues, Methods, and Controls", *Information Systems Security*, Vol. 15, No. 4, 2006, pp. 43-50.

[36] Thiesse, F., and Michahelles, F., "An overview of EPC technology", *Sensor Review*, Vol. 26, No. 2, 2006.

[37] The National Privacy Principles, 2005.

저자소개

김 진 수

저자는 연세대 상경대학 응용통계학과, 텍사스 주립대학 MBA를 거쳐, 루이지애나 주립대학(LSU)에서 경영정보학 박사학위를 수여하였다. 현재, 중앙대학교 사회과학대학 상경학부 교수로 재직중이며, 중앙대 창업보육센터 소장, 창업대학원 부원장을 겸임하고 있으며, 한국데이터베이스학회 부회장으로 봉사하고 있다. 이외에도, 한국창업보육협회 교육이사, 정부투자기관 경영평가위원, 산업자원부, 정통부 등에서 IT관련 사업에 대한 자문과 기술평가위원으로 활동하고 있다. 주요 관심분야는 데이터베이스설계, 중소기업 정보화, ERP/SCM, RFID 비즈니스 전략 및 프라이버시 보호, e-business 전략 등이다.

◈ 이 논문은 2007년 08월 20일 접수하여 1차 수정을 거쳐 2007년 09월 12일 게재 확정되었습니다.