RFID 기반 개인 프라이버시 보호 프로세스 연구*

김진수, 김대진, 황인호

중앙대학교 상경학부 경영학과 교수
456-756, 경기도 안성시 대덕면 내리 72-1
Tel: +82-31-670-3215, Fax:+82-31-675-1384 E-mail:sunny@cau.ac.kr

중앙대학교 일반대학원 경영학과 박사과정
156-756, 서울시 동작구 흑석동 47
Tel: +82-31-670-3215, E-mail: yauchee@cau.ac.kr

중앙대학교 일반대학원 경영학과 석사과정
156-756, 서울시 동작구 흑석동 47
Tel: +82-31-670-3215, E-mail: inho2004@gmail.com

Abstract

유비쿼터스 시대를 견인해나갈 핵심 기술인 RFID가 전 세계적으로 주목 받고 있다. RFID는 향후 관련 산업의 활성화와 고용창출 및 사회적 투명성을 향상시킬 수 있는 기술이지만, RFID가 지니고 있는 기술적 특성으로 인한 보안 및 프라이버시 등의 문제를 내재하고 있어 RFID의 실용화가 더디고 있는 것이 현실이다.

본 연구는 RFID 기반 프라이버시 침해에 대하여 조사, 분석하여 이에 따르는 법적, 기술적인 문제에 대해 연구하고, 문제 해결방안으로 개인 민감성에 따른 프라이버시 해결 프레임워크를 제시하고자 한다. 또한 이를 설명할 프로세스 상세 설계와 CASE를 통한 RFID 도입 시 발생 가능한 프라이버시 해결 방안을 제시한다.

Keywords : RFID, Privacy, 시스템 설계

Ⅰ.서론

1970년부터 사용해 온 바코드를 대체할 기술인 RFID(Radio Frequency IDentification)는 미래 유비쿼터스 시대를 견인해 나갈 핵심 기술로서 주목 받고 있다. RFID는 근거리 무선 기술을 이용하여 원격으로 감지 및 인식하여 정보교환을 가능하게 하는 기술이다(이은곤,2004). 하지만 RFID를 사용하였을 때 개인의 프라이버시 침해라는 심각한 이슈가 제기되고 있다.

RFID 시스템에서 정보는 개인 혹은 기업과 직접적인 연관을 가지기 보다는 RFID 태그를 활용하면서 생성되는 자료가 정보의 효력을 발휘하여 개인화되거나 기업 자료화되는 시점에서 데이터가 정보 보호의 대상이 된다(유승화, 2005).

RFID 시스템 도입으로 발생 가능한 프라이버시 침해 가능성에 대한 해결방안으로 법률·기술적으로 많은 연구들이 진행되고 있으나, 현재 기술적인 측면에서의 RFID 시스템 보안 측면에 치중하고 있다. 또한, 법률적인 측면에서는 각 국가마다 다른 가이드라인 수준으로 제시하고 있으며, 사회적으로 프라이버시 개념이 명확하게 내려져 있지 않은 상황이다. 따

* 이 논문은 2007년 산업자원부 성장동력기술개발사업 연구비 지원에 의하여 연구되었음

라서 급변하는 환경 속에서 기업의 경쟁우위를 차지하기 위한 수단으로 RFID 시스템 활용 시 개인 프라이버시 침해 가능성을 해결하기 위한 방안 마련이 절실한 실정이다. 이병길(2005)는 프라이버시 해결을 위해 보호 등급을 제시하였지만, 태그와 연계된 정보시스템에 저장되는 정보양에 따라 등급이 변화하고, 논리적인 근거가 부족하였다. 본 연구는 RFID 기반 프라이버시 보호 방안 연구를 통해 프라이버시 위협요인 추출 및 보호할 수 있는 프레임워크를 제시한다. 또한, 프라이버시 보호를 위한 시스템 상세 설계와 실제 활용 가능한 CASE를 제시하고자 한다.

Ⅱ. 이론적 배경

1. RFID 이론적 배경

RFID는 IC 칩을 내장한 태그에 축적된 정보를 무선 주파수를 이용해 원격에서 인식하는 방식이며(김진노 외 2, 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 준다는 것이다(김동민, 2006). 이렇게 RFID를 도입하여 조달에서 생산, 분배, 최종 소비자까지의 전체 분배 채널을 관리하기 위한 통합 시스템을 구축함으로써, 단편적인 단계의 최적화가 아닌 전체 시스템의 최적화를 추구할 수 있는 장점이 있다. 그러나, 태그 내장 장소의 은닉과 유일한 ID를 가지는 RFID 특성(과학기술부, 2006)은 보안 및 개인 프라이버시 측면의 침해 가능성 문제를 제기한다.

2. 개인 프라이버시의 이론적 배경

개인 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 해석되었던 반면 최근에는 자신의 정보에 대한 통제권을 보장하는 정보 프라이버시(Information Privacy)까지 확장된 개념으로 발전하였다(산업자원부, 2006).

RFID 시스템 도입으로 인한 개인정보 침해 문제의 심각성은 개인 신상정보의 단순한 수집·이용보다 개인의 여러 가지 거래 내용, 사회활동 내용과 신상정보를 조합함으로써 개인의 내면적 가치가 본인이 모르는 사이에 분석·활용할 수 있다는 점이다(정국환, 1997). 결국 기본적으로 개인정보 침해 문제는 정보가 여러 영역에서 수집, 저장, 축적, 관리, 활용되는 것에 기인하며, 개인의 다양한 성향을 사전 동의 없이 제 3자에게 보여주게 되는 것이다.

3. RFID 시스템의 프라이버시 침해 가능성

정부만(2006)은 RFID 시스템을 이용한 프라이버시 침해 경우를 다음 4가지 경우로 구분한다. ① RFID 태그에 개인 정보를 기록하는 경우, ② RFID 태그에 기록된 개인 정보를 수집하는 경우, ③ RFID 태그의 물품정보와 특정 개인의 정보를 연계하는 경우, ④ 기타 태그가 부착된 물품을 구매하거나 사용하는 경우 등이다. 이때, 단순히 RFID 태그의 물품정보를 활용하여 재고관리, 창고관리 등만을 수행하는 경우, 즉 물품정보와 개인정보가 연계되지 않는 경우는 프라이버시 보호 적용에서 제외할 수 있다.

따라서, 실제로 RFID 시스템 적용시 개인 프라이버시가 침해받을 수 있는 영역은 Retail에서 소비자가 태그가 부착된 제품을 구매할 때 나타나게 된다.

4. FTC(미연방거래 위원회)의 공정정보 사용 원칙

FTC(Federal Trade Commission : 미연방거래 위원회)는 다양한 상품, 서비스 및 정보에 대한 접근의 가능성이 높아짐에 따라, 방대한 양의 개인정보의 원천이기도 한 월드와이드 맵에서 개인정보를 어떻게 사용하여야 하는지에 대한 정확한 인지의 필요성에 의해, 1997년 6월에 5가지 공정 정보 사용원칙을 제시하였다.

<표 1> 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

이러한 내용은 기업이 태그 화된 제품 판매 시, 태그에 관한 정보가 고객에게 얼마나 잘 제공되고, 고객이 받아들이는 정도에 대한 가이드라인으로 활용이 가능하다.

Ⅲ. 개인 프라이버시 보호 프레임워크

1. 민감성 적용 개인 프라이버시 보호 프레임워크

개인 프라이버시 범위는 개개인의 민감성에 의해 달라지는데, 강용석(2005)은 민감성에 따른 개인정보 5 등급을 제시하면서, 상위 개인정보는 출생과 함께 또는 생활이력에 의해 발생하는 정보이며 개인의 동의와 무관하게 수집되고 보유하게 되는 정보가 대부분이기 때문에, 프라이버시 권리 측면에서 매우 세심하게 다루어져야한다고 주장하며, 이는 RFID 적용시 개인 민감성이 개인 정보보호 측면에서 세심히 다루어져야 함을 의미한다.

호주의 경우, 개인프라이버시 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.

<표 2> 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

출처 : The National Privacy Principles, 2005

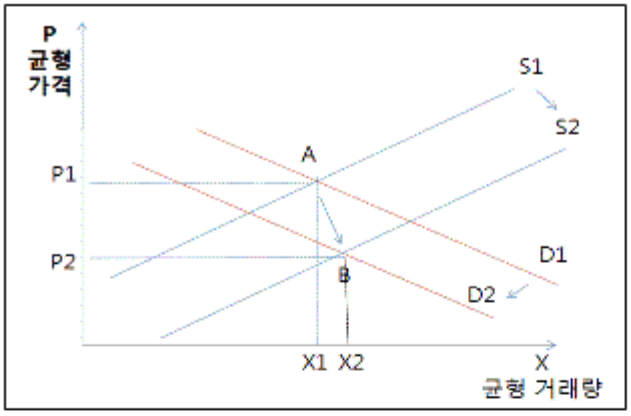
NPP 10번째 원칙인 민감성 정보는 "개인 동의가 없고, 법적으로 타당한 정보 수집이 이루어지지 않거나, 불법 또는 클레임이 발생될 수 있는 정보 또는 수집하는 정보가 개인의 삶 또는 건강을 심각하게 위협할 경우 조직은 개인 정보를 수집할 수 없음"을 제시하였다(NPP, 2005). 따라서 개인 프라이버시의 경우, 개인 정보에 대한 개개인의 민감성에 따라 정보의 중요성이 달라짐을 알 수 있다.

(1) 고객 민감성 등급

강용석(2005)이 제안한 개인정보 5등급 개인정보는 범용적 개인정보 분류이므로, 본 연구에 적용하기 위해서는 RFID 특성을 고려한 재정의가 필요하다. <그림 1>은 개인 중요 신용정보와, 개인 기본 신용정보의 상대성을 고려한 개인 민감성 등급이다.

민감성 등급	분류 기준	상세 명세
1등급	개인중요 신용정보	범죄기록, 개인 채무 정보
2등급		대출, 보증, 신용카드 정보, 금융 정보
3등급		고유, 주민등록 번호, 자격 증명, 생체정보
4등급	개인기본 신상정보	프로파일된 개인신상 정보
5등급		연구목적 등으로 사용되는 개인 기본 정보 (이름, 성별, 주소 등)

<그림 1> 개인 민감성 등급



출처: 한국정보보호진흥원, "개인정보의 경제적 가치 분석에 관한 고찰", 2007.3
<그림 2> 정보보호수준의 변화와 가격 및 거래량

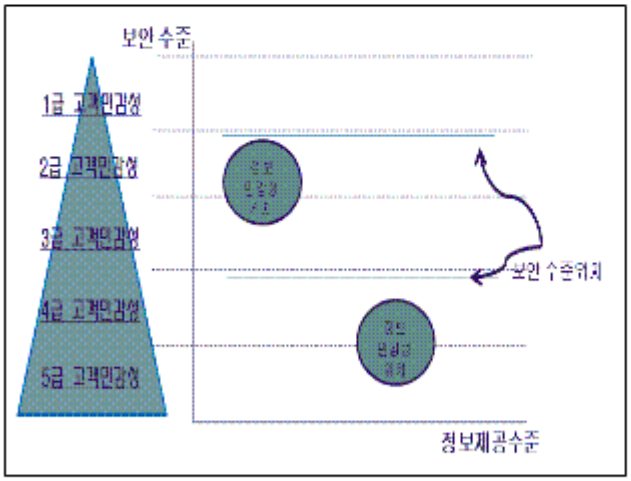
(2) 개인 프라이버시 보호 수준 측정

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

<그림 2>는 개인정보보호 수준이 강화되면 개인정보 공급자인 개인은 동일한 가격에서 개인정보 제공 리스크가 감소하므로 개인정보 공급량을 증가시키게 되어 결국 공급곡선이 S2로 우측 이동하는 것을 의미한다. 마찬가지로 개인정보 보호수준 강화는 개인정보 수요자인 기업의 개인정보 수집 관련 비용 증가 및 침해 사고 발생에 대한 배상비용 증가로 개인정보 수요량이 감소하게 되고 결국 수요 곡선이 D2로 이동하는 것을 의미한다(채승완 외3, 2007).

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

개인정보보안 수준은 고객이 선택한 5가지 민감성 등급에 따라, 달라지는데, <그림 3>은 고객 민감성으로 선택된 개인 정보 보안 수준을 제시한다. 예를 들어 고객이 4급 민감성 정도를 선택하였다면, 3급 수준에서 개인 정보 보호 등급을 제공함으로써, 정보보안 수준의 신뢰성을 얻을 수 있다.



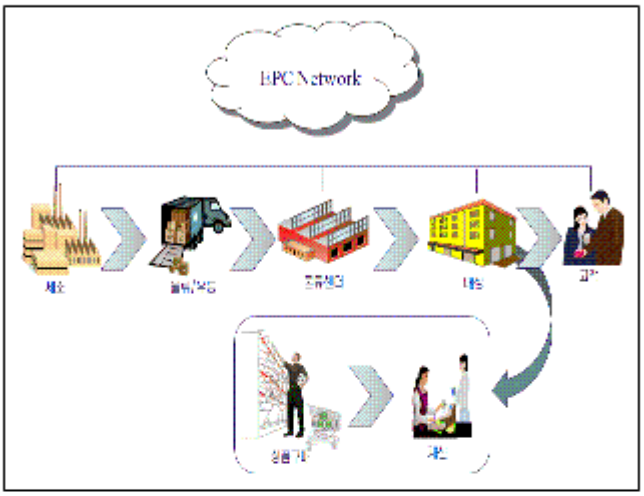
<그림 3> 프레임워크 정보보안 수준

(3) Retail에서 개인 프라이버시 침해 가능성

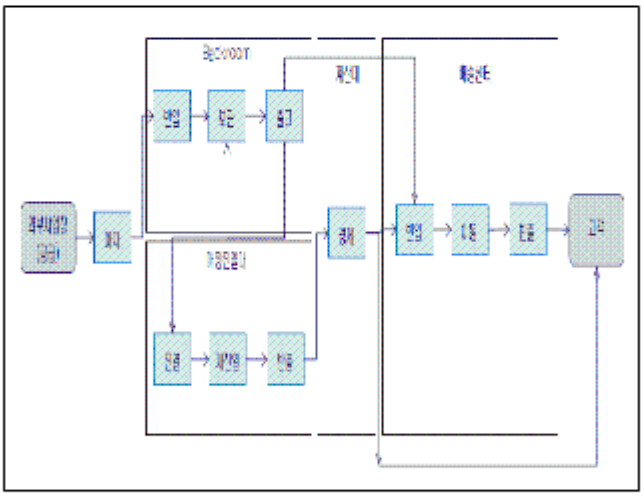
RFID 시스템 도입은 데이터 흐름 커뮤니티를 통

하여 수많은 데이터를 수집할 수 있는데, 특히 고객과의 접점인 Retail에서 개인 정보와 같은 많은 데이터 수집이 가능하다.

RFID를 기반으로 하는 제품의 흐름상에서 발생하는 실시간 정보들은 다음 <그림 4>와 같이 EPC Network상에 저장되며, 특히 Retail에서 RFID 적용 제품의 흐름은 <그림 5>과 같다.



<그림 4> SCM 상의 제품 흐름



출처 : 산업자원부 한국유통물류진흥원, "주요 산업별 표적용 모델(템플릿) 및 ROI 분석 툴 개발", 2007

<그림 5> RFID 적용 매장에서 제품 흐름

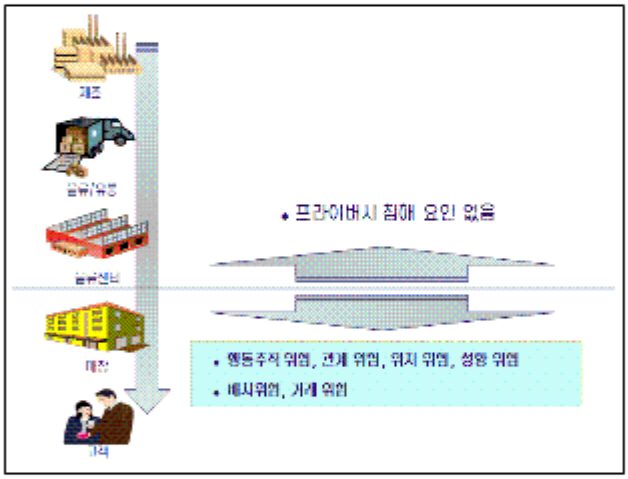
Gerasimos Marketos외 1(2006)은 Retail Industry 상에서의 RFID 시스템 도입은 기업에게 3가지 측면의 정보를 제공할 수 있다고 정의한다.

◎ **구매 전·후 결과(Sequence of Purchase)** : 고객의 제품 구매에 대한 데이터를 알 수 있다. 구매자의 패턴을 파악하고, Retailer는 그러한 패턴을 통해 더 확실한 예측을 할 수 있다.

◎ **긍정적/ 부정적 성향(Positive/Negative Preferences)** : 고객의 구매 아이템에 대한 성향을 파악 할 수 있으며, 제품 환불 및 보상에 대한 문의시 적절한 대처방안을 제시 할 수 있다.

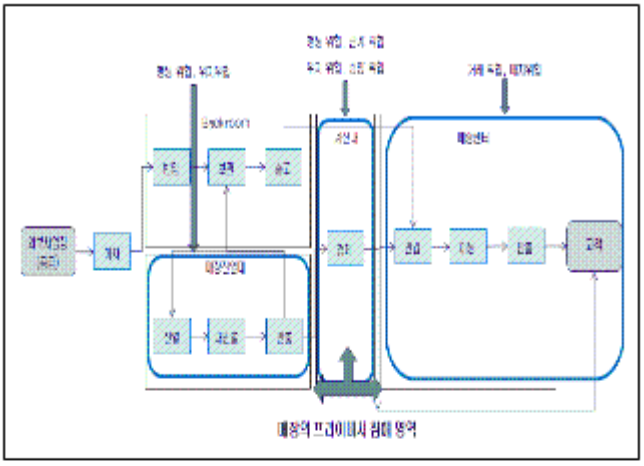
◎ **고객 노선(Routes of Customers)** : Retailer는 상점에서 RFID 태그가 장착된 제품을 구매한 고객의 쇼핑 동선을 매장 곳곳에 설치된 리더기에 의해 파악할 수 있다. 고객 움직임을 파악함으로써, 가장 많이 이동하는 부분에 고객이 좋아하는 상품을 배치시킬 수 있다.

반면, SCM 상에서 RFID에 의한 개인 프라이버시 침해 요인은 공급사슬의 전체 영역에서 나타나지 않는다. 프라이버시 침해 영역은 고객과 만나는 접점인 Retail에서부터 나타나게 되는데 <그림 6>은 프라이버시 침해 영역을 제시하였다.



<그림 6> 프라이버시 침해 영역

개인 프라이버시 침해 요인은 행동추적 위협, 관계위협, 위치위협, 성향위협, 배치위협, 거래위협으로 분류된다(Simson L. Garfinkel, 2005). <그림 7>은 RFID를 적용 시 나타날 수 있는 개인 프라이버시 침해 요인들을 매장 업무 흐름별로 제시한다.



<그림 7> 매장 업무 흐름 별 프라이버시 침해 위협 요인

<표 3> RFID 프라이버시 보호 등급

RFID 정보 / 고객 민감성 등급	Service Contents												비고
	Tag Information			EPC Information Service									
				제품 정보						유통정보	고객 정보		
	EPC 코드	자사코드	상품인덱스	제조일	가격	제품명	제품명세	A/S정보	태그삭제일		고객 ID	고객명세	
1	○	○	○	×	×	×	×	×	×	×	×	×	태그 제거
2	○	○	○	×	×	×	×	×	×	×	○	×	보호 기술 사용
3	○	○	○	○	○	×	×	○	×	○	○	×	
4	○	○	○	○	○	○	○	○	×	○	○	×	
5	○	○	○	○	○	○	○	○	×	○	○	○	태그 유지

(4) 고객 민감성 적용 프라이버시 보호 프레임워크

RFID 기술은 SCM(Supply Chain Management) 상에서 제품의 흐름에 적용할 수 있으며, 공급업자로부터 최종 소비자까지의 정보를 실시간으로 획득하여 이용함으로써 기업에 필요한 정보를 실시간으로 수집하여 정보화 할 수 있는 장점을 지닌 반면, 개인 프라이버시 침해 가능성을 지니고 있다.

본 연구는 RFID 적용 시 발생 가능한 프라이버시 침해 문제를 해결하기 위해 고객 민감성에 따른 보호 프레임워크를 제안한다.

RFID 시스템 적용 시, 네트워크상에서 수집되어지는 정보는 Tag Information과 EPC 네트워크상에 저장되는 정보들로 분류된다. 네트워크상에 수집된 정보는 직접적으로 프라이버시 침해로 진행되는 것보다는 정보의 수집, 가공에 의해 프라이버시 침해가 정도가 커지게 된다.

따라서, <표 3>에서 네트워크상에 수집되는 정보들을 고객 민감성 등급에 의해 선택적 제거 및 파기를 가능하게 하는 "RFID 프라이버시 보호 등급 프레임워크"를 제안한다.

즉, RFID 정보와 고객 민감성 등급으로 제시된 프레임워크는 고객이 제시하는 민감성 등급에 따라, EPC IS에 저장되는 개인정보의 양을 제한하며, 등급에 따른 태그 삭제 정보들은 기업 정책과 외부 현황에 따라 달라진다.

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** : EPC IS에 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 5

등급을 선택 할 가능성이 크다. 5등급의 경우, 모든 정보를 남겨둠으로써, A/S 및 기업적 서비스 활동에 도움을 주게 된다.

Ⅴ. 프라이버시 보호 프레임워크 상세 설계 및 사례 연구

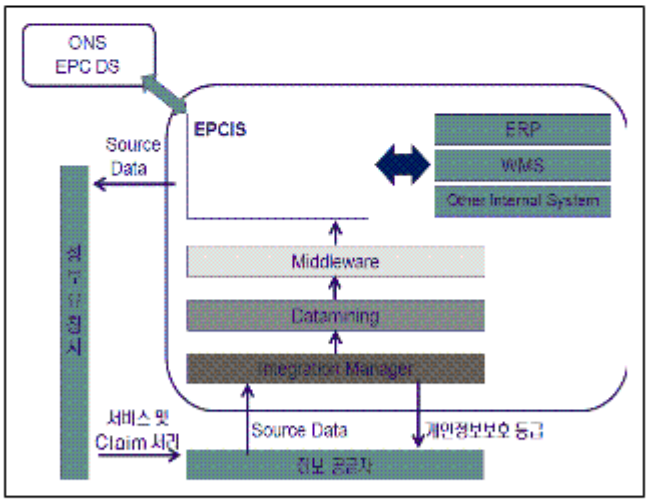
1. 프라이버시 보호 프레임워크 상세 설계

(1) RFID Architecture

EPC를 유일한 코드값으로 상품의 추적성(Traceability)과 가시성(Vistibility)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).

EPCglobal 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 8>과 같이 제시할 수 있다.

<그림 8> RFID Architecture



◎ **정보 공급자** : RFID 적용 제품과 관련된 사람을 의미하며, 정보 공급자는 Sorce Data를 제공하고, 개인정보보호 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 정보 보호 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.

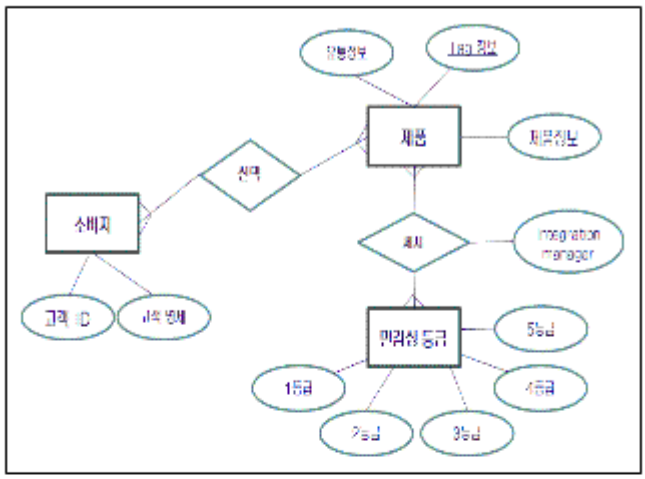
(2) 프라이버시 대응 상세 설계 방향

RFID시스템의 장점은 반대로 개인 프라이버시 침해를 가져오는 문제로서 제기된다. 이러한 문제를 해결하기 위해, 본 연구에서는 앞에서 제시한 "개인 민감성 등급" 프레임워크와 RFID Architecture를 이용하여 "RFID 대응 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 Manager에 의해 제품의 네트워크상에 적용된다. 이때, 민감성 등급에 따라 삭제되어야 할 RFID 정보들은 기업에

제공되기 전에 삭제되어 제공된다.

<그림 9>는 프라이버시 대응을 위한 프로세스 상세 설계를 위한 간단한 ER-Diagram이다.



<그림 9>프라이버시 대응을 위한 E-R Diagram

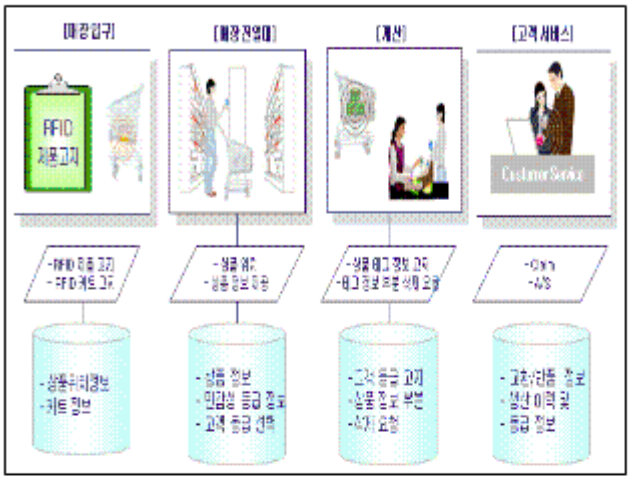
제시한 ER-Diagram 모형은 <표 4> Pseudo code로 제시하였다.

<표 4> 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 then
5            delete 제조원, 가격, 제품명, 제품명세, A/S정보, 태그
정보,
               유통정보, 고객 ID, 고객 명세
6          else if 2등급 then
7                delete 제조원, 가격, 제품명, 제품명세, A/S정보,
                 태그삭제원, 유통정보, 고객명세
8              else if 3등급 then
9                    delete 제품명, 제품명세, 태그삭제원, 고객명
세
10                 else if 4등급 then
11                       delete 태그삭제원, 고객명세
12                   else if 5등급 then
13                       delete 태그삭제원
14                     endif
15                 endif
16             endif
17         endif
18     endif
19         save DB
```

2. 프라이버시 대응 프로세스 사례

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 SCM 에서 Retail에서 주로 나타난다. 다음 <그림 10>은 제품이 고객과 만나는 시작점인 매장 입구에서 부터 사후 고객 관리까지의 프로세스를 제시하였다.



<그림 10> CASE 프라이버시 프로세스

RFID 적용시 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. Retail에서는 고객에게 RFID 제품이 매장에 있다는 것과 어떠한 영역에서 사용되고 있는지를 정확하게 고지할 필요가 있으며, 고객에게 개인정보가 EPCIS에 들어갈 수 있음을 정확하게 알려야한다. 또한, 고객이 RFID가 적용된 제품을 구매하려할 때, 개인정보의 정확한 사용 방향과 고객이 제공할 수 있는 정보를 직접 선택할 수 있는 권리를 제공하여야 한다.

따라서, Retail에서 고객과 RFID가 접촉하게 되는 쇼핑 동선에 따라 발생 가능한 프라이버시 침해 요소와 해결 방향을 가상 CASE를 통하여 제안하고자 한다. <표 5>는 매장 입구에서부터 고객의 사후 관리 시점까지 RFID 적용 프라이버시 침해 위협 요인, 관련 CASE, 그리고 FTC의 제 5원칙을 통한 개인정보보호 해결 방향을 제시한 것이다.

<표 5> 프라이버시 CASE 프로세스 - 콘돔 구매

위치	프라이버시 침해 위협 요인	CASE 주요 사항	비고
매장 입구	행동 위협	- 매장 입구에서 RFID 관련 정보 제공	Notice

		- Display 설치 카트 정보 제공	
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 비치 위협	- 클레임, A/S를 위해 인터넷 및 고객 서비스센터를 이용가능 - Display에는 제품ID와 등급만을 제시 - 서비스 제공 후, 개인 민감성 등급 재인지 및 선택권 제시	Access, Notice, Security, Enforcement

VI. 결론

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 프레임워크를 제시하고, RFID 시스템 적용 시 발생할 수 있는 프라이버시 침해 요소 해결을 위한 프로세스 설계를 제안함으로써, 프레임워크를 기업에서 실제 활용할 수 있도록 하였다. 또한, 제안한 프로세스 설계 방안을 사례연구를 통해 적용시켜 봄으로써, 실제 Retail에서 RFID 적용 시 단계마다 나타날 수 있는 문제점을 분석하고, 개인정보보호 흐름을 제시하였다.

현재 제시한 프레임워크는 범용적으로 사용할 수 있는 형태로 제시하였기 때문에, 다양한 산업군에서 사용하기 위해서는 관련 분야에 대한 선행 연구를 실시하여 해당 산업별 특징을 프레임워크에 적용하는 것이 필요할 것이다.

References

필요하시면 저자(sunny@cau.ac.kr)에게 문의바랍니다.