개인정보의 가치와 개인정보 침해에 따른 사회적 비용 분석

최종보고서

2013. 11. 28

제출자 : (사) 개인정보보호협회

아래의 연구결과물을 '개인정보의 가치와 개인정보 침해에 따른 사회적 비용 분석'에 대한 최종보고서로 제출합니다.

2013. 11. 28

제출자 : (사) 개인정보보호협회

개인정보보호위원회 귀중

이 보고서를 개인정보보호위원회에서 연구위탁 의뢰하신 '개인정보의 가치와 개인정보 침해에 따른 사회적 비용 분석'의 최종보고서로 제출합니다.

책임연구원　정상호 (개인정보보호협회 팀장)

공동연구원　유진호 (상명대학교 경영학과 교수)

공동연구원　유병준 (서울대학교 경영전문대학원 교수)

공동연구원　한창희 (한양대학교 경영학부 교수)

공동연구원　유승동 (상명대학교 금융경제학과 교수)

< 목 차 >

제1장 서론

제1절 연구의 목적

정보통신기술은 사용자 ID, 이름, 주소, 성향, 신체적 특성 등 개인정보를 공유하기 용이하도록 하였고, 이를 근간으로 누구나 개인정보를 열람, 수집 및 저장할 수 있게끔 발전되어 왔다. 특히, 포털, 오픈마켓, 게임사 등은 콘텐츠를 사용자에게 맞춤판매하기 위해 개인정보를 성역 없이 수집 및 분석하고 있으며, 정보의 정확도에 따라 광고효과의 차이가 발생하기 때문에 수집되는 정보의 민감도 역시 높아지고 있는 실정이다.

디지털경제의 핵심자원으로서 개인정보의 활용은 점차 증가하고 있으나, 이에 따른 역기능 역시 심화되고 있다. 사용자의 부주의나 악의적인 사용자에 의해 개인정보가 유·노출될 경우 음란물 유통 및 배포, 스팸, 저작권 침해, 사이버 폭력 등 직·간접적인 프라이버시 침해를 경험하게 된다.

그러나 아직까지 개인정보 유출에 따른 비용을 계량적으로 파악하고, 피해의 심각성을 연계한 연구는 희소한 것이 사실이다. 따라서 범국민적 차원에서 개인정보보호의 중요성에 대한 인식을 제고하고, 기업적 측면에서 개인정보보호를 위한 적정한 수준의 투자규모를 산정하여 제안할 수 있는 연구가 필요하다.

이번 연구에서는 위와 같은 필요성을 바탕으로 사적재화, 공공재 등 측면에서 개인정보 가치를 분석하고, 개인정보 유출에 따른 사회적 영향 및 다양한 방법론을 통한 사회적 비용을 추정한다. 아울러 개인정보 침해로 인한 사회적 비용을 최소화하기 위해 개인정보 보호의 중요성에 대한 재인식 및 적정수준의 투자규모 산정 등 정책 제언을 제시하고자 한다.

제2절 연구의 범위와 방법

1. 연구의 범위

이 연구는 개인정보의 가치를 측정하고 개인정보 침해로 인한 사회적 비용을 분석함으로써 개인정보 중요성에 대한 재인식 및 적정수준의 투자규모 산정 등을 목적으로 한다.

먼저, 정보재화의 특징을 고찰하고 사적 재화와 공공재화의 차이에 대한 논의를 거쳐 개인정보의 가치를 분석해 본다.

개인정보 유출로 인한 기업 중심의 경제적 피해비용을 측정하기 위해서 피해발생 비용을 직접비용(Direct Costs)과 간접비용(Indirect Costs), 명시적 비용(Explicit Costs)과 잠재적 비용(Implicit Costs)으로 구분한 기존연구(유진호 외(2008), "인터넷 침해사고에 의한 피해손실 측정", 『정보화정책』 제15권 제1호)와 미국의 보안전문 업체인 Information Shied 사의 개인정보 유출 피해액 산출 요소를 참고하여 다음과 같은 프레임워크를 제안 및 활용한다.

< 개인정보 유출사고 피해액 산출 범위 >

<table>
<tr><td rowspan="2">간접비용
(Indirect Costs)</td><td>고객 신뢰도 측정비용
시스템 보완 & 교체비용</td><td colspan="2" rowspan="2">기업 이미지 손실</td></tr>
<tr><td>산업 파급효과</td></tr>
<tr><td>직접비용
(Direct Costs)</td><td>IR 대응비용(브랜드 이미지 방어)
사고 대응 인건비
고객 감소로 인한 매출 감소</td><td>법적비용
(소송, 보상금)
벌금</td><td>보상받지 못한
개인의 정보가치</td></tr>
<tr><td></td><td>명시적 비용
(Explicit Costs)</td><td colspan="2">잠재적 비용
(Implicit Costs)</td></tr>
</table>

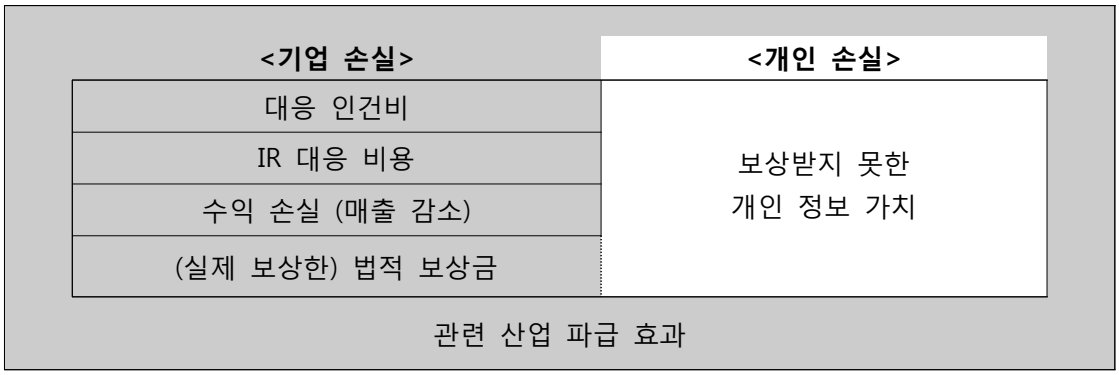
* 법적비용 + 벌금 + 보상받지 못한 개인의 정보가치 = 유출된 정보의 가치

본 연구에서는 직접 산출이 가능한 직접비용을 중심으로 개인정보 유출 피해액을 산출하고, 명시적 직접비용만을 다룬 기존의 연구에서 한 단계 더 나아가

산출이 어려운 간접비용과 잠재적 비용을 추가적으로 고려한다. 또한, 개인정보 유출사고의 영향이 클 것으로 예상되는 관련 산업 파급효과와 기업의 법적 비용・벌금까지 산출의 범위를 확대함으로써 보다 정확한 산출액을 도출한다. 보상 받지 못한 개인의 정보가치는 개인정보의 가치평가 방식과 중복계산 부분을 검토하여 그 범위를 조정한다.

명시적 간접비용인 고객의 신뢰도 측정비용과 시스템 보완&교체비용은 현재보다는 미래 대응적 가치이기에 고려 대상에서 제외했으며, 산업 파급효과는 그 영향이 크고 비교적 즉각적인 반응이 나타날 것으로 예상되는 1차 파급효과만을 고려한다. 기업의 이미지 손실 역시 측정이 어렵고 명시적 직접비용에서 매출감소에 일부분이 포함되기에 산출 대상에서 제외한다.

< 개인정보 침해사고 피해액 다이어그램 >



본 연구에서는 위에 표시된 회색부분인 기업 중심의 경제적 피해비용을 구체적으로 측정하기 위해서 포네몬 연구소, 포레스터 연구소, 테크-404, 인포메이션 쉴드(Information Shield Inc.) 등의 보안 전문 연구소와 기업에서 발행한 보고서와 선행연구의 방법을 활용한다.

피해액을 측정하기 위한 세부 요소들을 도출하기 위해서 인포메이션 쉴드 사의 '개인정보 유출 피해액 계산기'를 중심으로 포네몬 리서치, 포레스터 리서치, 테크-404 등의 연구소에서 제시한 요소들을 검토한다. 또한 경제학의 생산자 이론적 접근법과 계량경제학적 접근법 그리고 원가 계산적 접근법을 기반으로 산출식을 세우고, 산출식을 계산하기 위한 각각의 요소들은 기본적으로 개인과 기

업설문을 통해 얻은 자료를 활용한다. 여기에 추가적으로 관련 항목과 관련된 각계 전문가와의 심층 인터뷰를 통해 결과값의 타당성을 다시 한 번 검증하고, 조정하는 작업을 통해 정확성을 높이고자 한다.

개인정보 유출의 사회적 비용 분석 모형을 개발한다. 이를 위해 가상가치법에서 광범위하게 적용되고 있는 각종 방법론을 고찰하고 이를 개인정보 침해에 적용하는 것을 검토해 본다. 아울러, 개인정보 침해에 따른 사회적 비용을 도출하기 위해 설문결과를 분석하고 이를 통하여 사회적 지불의사를 도출한다.

2. 연구의 방법

먼저, 선행 연구된 개인정보보호 및 개인정보의 가치 산출에 관한 문헌을 바탕으로 관련 정보를 수집하고 이를 통해 개인정보 침해에 따른 사회적 비용분석의 필요성을 명확히 한다.

둘째, 전문 리서치 업체를 통해 대국민을 대상으로 한 개인정보와 개인정보 유출에 대한 인식 현황에 대해 분석한다.

셋째, 연구과정의 객관성과 정확성을 높이기 위해 개인정보의 경제적 가치 관련 연구실적자로 구성된 자문위원들과 협력하는 한편, 경제적, 법·제도적 등 다양한 측면에서 개인정보 침해의 사회적 비용 분석이 실제로 활용될 수 있도록 해당 분야의 기관들과 협력한다.

넷째, 사적재화, 공공재 등으로서의 개인정보의 가치를 분석하고 정보주체, 기업, 사회 차원의 개인정보의 이용효과 및 침해에 따른 영향을 분석한다. 또한, 개인정보 유출의 사회적 비용 분석 모형을 개발하고 개인정보 침해에 따른 사회적 비용을 도출한다.

제2장 개인정보의 개념과 특성

제1절 개인정보의 정의 및 분류

1. 개인정보의 정의

개인정보보호법 제2조에서는 개인정보를 “살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)”로 규정하고 있다. 즉 개인정보보호법에서는 개인정보의 구성요소로 ① 살아있는 개인, ② 특정 개인과의 관련성, ③ 식별 가능성의 세가지를 적시하고 있다. EU, OECD, 미국・영국 등 대부분의 국가에서도 개인정보를 ‘개인을 식별하거나 신원을 확인할 수 있는 정보(자료, 기록)’로 규정하고 있다. 이하에서는 개인정보의 구성요소에 대해 개별적으로 살펴본다.[1)]

(1) 살아있는 개인

보호의 대상인 개인정보는 현재 ‘생존(生存)’하고 있는 개인에 관한 정보에 한한다. 따라서, 이미 사망하였거나 실종선고 등 관계 법령에 의해 사망한 것으로 간주되는 자에 관한 정보는 개인정보로 볼 수 없다. 다만, 사망자의 정보가 사망자와 유족과의 관계를 나타내는 정보이거나 유족 등의 사생활을 침해하는 등의 경우에는 사망자 정보인 동시에 관계되는 유족의 정보이기도 하기 때문에 보호대상이 될 수 있다.

또한, 개인정보의 주체는 자연인(自然人)을 의미한다. 따라서 법인(法人)이나 단체에 관한 정보는 원칙적으로 개인정보에 해당하지 않는다. 예를 들어 법인 또는 단체의 이름(상호), 사업자등록번호, 영업소 주소 및 전화번호, 대표자 성명, 이사・감사 등 임원 정보, 자산 또는 자본의 규모, 주가, 영업실적, 납세실적,

1) 이하 “개인정보 보호법령 및 지침・고시 해설”, 행정안전부, 2011. 12, 6~9p 참조.

영업비밀 등은 개인정보에 해당하지 않는다.

(2) 특정 개인과의 관련성

개인정보는 특정한 개인에 대한 사실, 판단, 평가 등 그 개인과 관련성을 지닌 정보여야 한다. 즉 개인정보는 일반적으로 특정 개인의 정체성(identity)을 구별하거나 밝혀낼 수 있는 정보(성명, 주민등록번호, 생일, 주소, 바이오정보 등) 및 특정 개인의 과거 및 현재의 상황이나 상태를 나타낼 수 있는 정보(교육상황, 재정상황, 진료 및 건강 상태 등)이어야 한다. 현행 법률에서 개인정보에 대한 구체적이고 세부적인 기준이나 요건을 규정하고 있지 않으므로 특정 개인과 관련된 모든 정보는 개인정보에 해당된다고 볼 수 있다.

반면, 특정 개인을 알아볼 수 없도록 가공되었거나 통계적으로 변환된 경우에는 특정 개인과의 관련성이 없고 식별이 어려우므로 개인정보에 해당하지 않는다. 예를 들어 특정 단체 임원들의 평균연봉, 특정 대학의 해당연도 졸업생의 취업률 등의 정보는 단지 전체적인 통계적 정보만을 보여줄 뿐 특정 개인과의 관련성이 없는 정보이므로 개인정보에 해당하지 않는다.

(3) 식별 가능성

개인정보는 개인을 '알아볼 수 있는' 정보이어야 한다. 즉 특정한 개인을 '식별할 수 있는' 정보이어야 한다. 여기에서 '식별'이란 특정 개인을 다른 사람과 구분하거나 구별할 수 있음을 의미한다. 예를 들어 대한민국의 국민 중에서 특정 개인을 구분할 수 있는 신원정보(성명, 주민등록번호, 본적, 주소 등), 학교·직장·단체 등 소속된 곳에서 특정 개인을 구분할 수 있는 정보(성명, 학번, 사번, 학년, 직급 등) 등이 이에 해당한다.

또한 개인을 '알아볼 수 있는' 정보라는 것은 그 특정 개인을 전혀 모르던 사람이더라도 객관적으로 그 특정 개인을 다른 사람과 구분·구별할 수 있다면 모두 개인정보에 포함될 수 있다는 의미이다. 따라서 해당 정보가 이미 통계적으로 변환되어 특정 개인이라는 사실을 식별할 수 없다면 개인정보라 볼 수 없다.

해당 정보만으로 개인을 식별할 수 있는 경우뿐만 아니라 '다른 정보와 쉽게 결합'해서 개인 식별이 가능한 경우에는 그 정보도 개인정보로 볼 수 있다. 예를 들어, 주민등록번호는 개인마다 고유한 것이므로 개인을 손쉽게 식별하는 데 활용할 수 있다. 그러나 성명만 있는 경우에는 동명이인(同名異人)이 존재할 수 있기 때문에 그 정보 하나만으로는 개인정보로 보기 어렵다. 그런데, 성명이 전화번호나 주소 등의 정보와 결합하는 경우에는 특정 개인을 식별할 수 있게 되므로 이 경우에는 개인정보로 볼 수 있다. 따라서 개인정보의 식별성이란 곧 정보의 결합 또는 조합을 통하여 특정 개인을 구분·구별하는 것을 의미한다고 할 수 있다.

[표 2-1] 개인정보의 개념에 대한 각 국의 입법례

구분	법령	정 의
OECD	개인정보보호지침 (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)	개인데이터(personal data)는 식별되거나 식별될 수 있는 개인에 관한 모든 정보를 지칭
EU	개인정보보호지침 (Directive 95/46 EC)	개인데이터(personal data)는 식별되거나 식별될 수 있는 자연인에 관한 모든 정보를 지칭 ※ 식별 가능한 개인은 직접 또는 간접적으로 신원확인번호, 신체적, 생리적, 정신적, 경제적, 사회적 동일성(identity)을 나타내는 요소를 참조하여 그 신원이 확인될 수 있는 사람을 지칭
미국	프라이버시법 (Privacy Act, 1974)	개인기록(Record)은 행정기관이 보유하는 개인에 관한 정보(information about an individual)의 개개 항목 또는 그 집합 ※ 개인기록에는 당해 개인의 이름, 식별번호.부호, 지문, 성문, 자신과 같은 당해 개인의 고유한 식별자(identifying particular)가 포함
영국	개인정보보호법 (Data Protection Act, 1998)	개인기록(personal data)은 신원확인이 가능한 생존하는 개인에 관한 기록으로서, 그 기록 또는 다른 정보로부터 신원확인이 가능한 것을 의미
프랑스	국가정보처리자유법 (Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux livertés)	기명이나 무기명의 형식에 관계없이 직접 또는 간접으로 자연인의 신원을 식별하거나 확인할 수 있는 개인 또는 법인이 처리하는 정보

구분	법령	정 의
독일	데이터보호법 (Bundesdatenschutsgesetz, 1974)	자연인의 신원을 식별하거나 식별할 수 있는 정보주체에 관한 인적 및 물적 환경에 관한 일체의 정보
벨기에	개인정보보호법 (Law of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data)	자연인을 식별하거나 식별할 수 있는 일체의 정보
스웨덴	데이터보호법 (Personal Data Act, 1998)	생존하는 자연인에 관하여 직접 또는 간접으로 식별할 수 있는 모든 유형의 정보
일본	개인정보 보호법 (個人情報の保護に關する法律)	개인정보는 생존하는 개인에 관한 정보로서 성명.생년월일 기타 기술(記述)에 의해 특정 개인을 식별할 수 있는 정보

2. 개인정보의 유형과 분류

개인정보는 개인의 성명, 주민등록번호 등 인적사항에서부터 사회・경제적 지위와 상태, 교육, 건강・의료, 재산, 문화 활동 및 정치적 성향과 같은 내면의 비밀에 이르기까지 그 종류가 매우 다양하다. 또한, 사업자의 서비스에 이용자가 직접 회원으로 가입하거나 등록할 때 사업자에게 제공하는 정보뿐만 아니라, 이용자가 서비스를 이용하는 과정에서 생성되는 통화내역, 로그기록, 구매 내역 등도 개인정보가 될 수 있다.

인터넷, GPS 등 정보통신기술의 발달에 따라 개인정보의 범위는 점차 확대되고 있다. 위치정보, 바이오 정보(지문・홍채 등) 등과 관련된 정보기술의 발전에 힘입어 지금까지 경험하지 못했던 개인정보가 속속 등장하고 있으며, 그 유형은 날로 다양해지고 범위 또한 빠르게 확대되고 있다.

개인정보의 유형은 분류하는 방법이나 관점에 따라 다양한 형태로 기술할 수 있으며 정형화된 법적 개념도 아니다. 이 보고서에서는 정보통신망법 해설서 등 기존 발간된 다양한 자료를 참고하여 개인정보 유형을 다음과 같이 분류하였다.

[표 2-2] 개인정보의 유형

유형	구체적인 예
기본인적 정보	성명, 주소, 아이디 및 패스워드, 가족관계 등. 기본인적정보는 온·오프라인 회원가입 및 서비스 이용, 물품 수령 등에 주로 이용
고유정보	주민등록번호, 여권번호, 운전면허 등록번호 등. 고유정보는 상거래·금융거래 등에서 본인 식별을 위한 확인 수단으로 사용
의료건강 정보	병력, 병원 진료기록, 신체장애 정도, 건강상태 등. 의료건강정보는 병원 진료 및 치료, 보험 가입 및 계약유지, 유전자 분석 등에 이용
경제정보	소득, 신용카드 및 통장계좌번호, 물품 구매내역, 대출 또는 담보설정 등. 경제정보는 상거래 및 금융거래 등 경제활동 전반에서 이용
사회관계 정보	학력 및 학업성적, 친우관계, 동호회 활동 등 사회 활동 관련 정보. 사회관계정보는 취업 시 활용 및 사회 전반적으로 이용
통신위치 정보	휴대폰 번호, 이메일주소, GPS 위치정보 등. 통신위치정보는 신용카드 이용정보 등과 결합하여 기업의 마케팅, 기업 홍보 등에 사용
법적정보	전과 범죄기록, 납세기록, 과태료 부과내역 등. 법적 정보는 정부 행정 전반에 걸쳐 이용

※ 개인정보 유형 분류 예시

□ 2012 개인정보보호 연차보고서 (개인정보보호위원회)

유 형	종 류
일반정보	이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 생년월일, 출생지, 본적지, 성별, 국적
가족정보	가족구성원의 이름, 출생지, 생년월일, 주민등록번호, 직업, 전화번호
교육 및 훈련정보	학교출석사항, 최종학력, 학교성적, 기술 자격증 및 전문 면허증, 이수한 훈련 프로그램, 동아리활동, 상벌사항
병역정보	군번 및 계급, 제대유형, 주특기, 근무부대
부동산정보	소유주택, 토지, 자동차, 기타소유차량, 상점 및 건물
소득정보	현재 봉급액, 봉급경력, 보너스 및 수수료, 기타소득의 원천, 이자소득, 사업소득, 기타 수익보험(건강, 생명 등) 가입현황, 회사의 판공비, 투자프로그램, 퇴직프로그램, 휴가, 병가
신용정보	대부잔액 및 지불상황, 저당, 신용카드, 지불연기 및 미납 횟수, 임급압류 통보에 대한 기록
고용정보	현재의 고용주, 회사주소, 상급자의 이름, 직무수행평가기록, 훈련기록, 출석기록, 상벌기록, 직무태도, 성격 테스트 결과
법적정보	전과기록, 자동차 교통 위반기록, 파산 및 담보기록, 구속기록, 이혼기록, 납세기록
의료정보	가족병력기록, 과거의 의료기록, 정신질환기록, 신체장애, 혈액형, IQ, 약물테스트 등 각종 신체정보
조직정보	노조가입, 종교단체가입, 정당가입, 클럽회원
통신정보	전자우편(E-mail), 전화통화 내용, 로그파일(Log file), 쿠키(Cookies)
위치정보	GPS나 휴대폰에 의한 개인의 위치정보
신체정보	지문, 홍채, DNA, 신장, 가슴둘레
습관 및 취미정보	흡연, 음주량, 선호하는 스포츠 및 오락, 여가활동, 비디오 대여기록, 도박성향

□ 정보통신망법 해설서

유 형		개인정보의 예
인적 사항		성명, 주민등록번호, 주소, 본적지, 전화번호 등 연락처, 생년월일, 출생지, 이메일 주소, 가족관계 및 가족구성원 정보 등
신체적 정보	신체정보	얼굴, 지문, 홍채, 음성, 유전자정보, 키, 몸무게 등
	의료.건강정보	건강상태, 진료기록, 신체장애, 장애등급, 병력(病歷) 등
정신적 정보	기호.성향정보	도서.비디오 등 대여기록, 잡지구독정보, 물품구매내역, 웹사이트 검색내역 등
	내면의 비밀 등	사상, 신조, 종교, 가치관, 정당.노조 가입여부 및 활동내역 등
재산적 정보	개인금융정보	소득, 신용카드번호, 통장계좌번호, 동산.부동산 보유내역, 저축내역 등
	신용정보	신용평가정보, 대출 또는 담보설정 내역, 신용카드 사용내역 등
사회적 정보	교육정보	학력, 성적, 출석상황, 자격증 보유내역, 상벌기록, 생활기록부 등
	법적정보	전과.범죄기록, 재판기록, 과태료 납부내역 등
	근로정보	직장, 고용주, 근무처, 근로경력, 상벌기록, 직무평가기록 등
	병역정보	병역여부, 군번, 계급, 근무부대 등
기타		전화통화내역, 웹사이트 접속내역, 이메일 또는 전화메시지, 기타 GPS 등에 의한 위치정보 등

제2절 개인정보에 대한 경제적 관점 논의

1. 정보재화로서의 개인정보

개인정보를 포함한 정보는 재화(goods)의 한 유형으로 간주될 수 있다. 정보기술의 발전으로 정보재화는 일반 물질재화(physical goods)와 달리 추가 생산을 위한 한계비용(marginal cost)이 상대적으로 낮다. 예를 들어 Varian(1998)는 일반재화와 다른 정보재화의 주요 특징을 기술발전에 따라 정보재화는 손쉽게 복사와 전송이 가능하다는 점을 제시한다.

정보재화의 경우 일반 물질재화(physical goods)와 비교하여 추가생산을 위한 비용이 낮게 소요된다는 것을 의미한다. 특히 최근 급격한 산업기술의 발전에 따라 전문 기술자가 아닌 평범한 일반인도 정보재화의 추가생산이 가능하게 되었다. 정보재화가 일반적 물질재화와 비교하여 초기 생산비용이 낮다고 이야기할 수 없으며, 최근 영화, 신문, 방송 등의 사례들에서 확인할 수 있듯이 정보재화의 생산에 대규모 투자가 들어간다.

유럽연합(EU) 집행위원인 Meglena Kuneva는 개인정보는 인터넷의 새로운 석유이자 디지털 세계의 새로운 화폐가 될 것이라고 말했다. 그리고 세계경제포럼에서 보스턴 컨설팅 그룹(Boston Consulting Group)의 보고서는 개인정보가 물이나 금, 기름과 같이 거래 가능한 자산으로 분류될 수 있으며, 이런 자산들과 같이 마이닝이나 공유 활용이 가능하다고 말했다. 그러나 유형자산과는 달리 개인정보는 소비되지 않으며, 정보의 요소들이 축적됨으로써 가치가 상승한다고 분석했다.[2)]

김정은 외[3)](2010)은 현대사회는 농업과 산업혁명을 거쳐 정보화 시대로 접어들게 되었고 이렇게 사회적인 패러다임이 바뀌면서 새롭게 생겨난 개념인 '재화로써의 정보'에 대한 관심이 늘어나는 가운데 소비자는 기업이 제공하는 제품, 서비스를 단순히 수용하는 것에서 벗어나 정보 제공자 또는 판매자라는 새로운 지위를 갖게 되었고 말했다. 정석균(2012)[4)]는 개인정보는 일반 상품 못지않은 경

2) Boston Consulting Group, Rethinking Personal Data: Strengthening Trust, 2012
3) 김정은 외, 소비자의 개인정보 가치평가에 영향을 미치는 요인에 대한 연구, 2011

제적 가치를 가지는 중요한 경제재(economic goods)의 하나이고 소비자가 온라인상에서 물품을 구매하거나 서비스를 이용하는 경우 누구도 개인정보의 누출위험으로부터 자유로울 수 없으며 프라이버시 침해가 필연적으로 수반될 수 있다고 했다. 인터넷은 (i) 개인정보가 오가는 시장(market)이며, (ii) 소비자는 물품을 구매하고 서비스를 이용하며 개인정보를 제공하는 주체이고, (iii) 기업(온라인상의 물품 판매자는 물론 서비스를 제공하는 모든 기관을 포함)은 물품을 판매하고 서비스를 제공하면서 개인정보를 수집하여 활용하는 경제주체로 볼 수 있다고 제시했다.

정보재화는 공공재화(public goods)의 특성을 보유하고 있다. 경제학에서 공공재화의 가장 중요한 특징은 공공재화는 비경합성(non-rivalry)과 비배제성(non-excludability)이다. 경합성이란 한 사람이 소비하는 경우 다른 사람이 소비를 하지 못하는 것을 의미한다. 따라서 비경합성은 한 사람이 재화를 이용하는 경우 다른 사람이 그 재화를 이용할 수 있는 경우를 의미한다. 배제성이란 소비에 대한 비용을 내지 않는 경우 소비를 하지 못한다는 것을 의미한다. 따라서 비배제성은 정보이용에 대하여 비용을 부담하지 않은 사람이 그 재화를 이용하지 못하게 할 수 없음을 의미한다.

정보재화의 경우 한 사람이 그 정보를 이용한다고 하여도 다른 사람이 그 정보의 이용을 막을 수는 없어 비경합성을 보유하고 있다. 소비재와 같은 일반 재화와 달리 예를 들어 한 사람이 정보재화의 일종인 개인정보를 이용하였다고 하더라도 다른 사람이 또 그 정보재화를 이용할 수 있다. 비배제성의 경우 정당한 비용을 지불하지 않는 무임승차자(free riders)의 문제와 관련이 되어 있다. 다시 말해 정보재화 가운데 홈페이지에 게시된 개인정보는 누구나 비용을 지불하지 않고도 이용 가능하다. 따라서 인터넷 사용자가 인터넷에 게시된 정보에 대한 필요성을 매우 낮게 평가할 수 있는 가능성을 배제할 수 없다[5].

개인정보는 정보재화의 일종으로 공공재화적 성격을 보유하고 있기도 하다. 우선 한번 수집된 개인정보는 한번 이용한다고 하여도 그 개인정보가 사라지지

4) 정석균, 인터넷 개인정보보호의 시장자체해결가능성에 대한 연구, 2012
5) 즉 인터넷 이용자는 인터넷에 게시된 정보에 대하여 자신의 지불용의(williness to pay)를 표현하지 않을 수 있는 것이다.

는 않으며, 다음에 동일한 개인정보를 이용할 수 있다. 따라서 수집된 개인정보는 비경합성을 보유하고 있다고 할 수 있다. 또한 여러 사람 혹은 기업이 동시에 다발적으로 개인정보를 이용할 수 있으며 미래에도 지속적으로 이용이 가능하다. 한 번 수집된 정보는 저장 가능성과 복사 가능성에 의하여 사라지지 않고, 추가로 재생산 될 수 있다. 물론 정보기술의 발전은 이와 같은 정보재화의 비경합성을 증진시킨다고 할 수 있다.

개인정보가 완전 비배제성을 보유하고 있다고 볼 수는 없다. 왜냐하면 일부 개인정보는 불법적인 침해가 있지 않는 범위에서 일반 공공재화와 달리 비용을 지불하지 않은 주체가 이용을 할 수 없기 때문이다. 그러나 일부 개인정보는 비배제성을 보유할 수도 있으며, 예를 들어 인터넷 동호에 가입한 회원이 회원들의 개인정보를 이용할 수 있다. 다양한 SNS의 개발 및 발전과 더불어 동아리에 가입한 사람들이 누구나 손쉽게 개인정보를 이용할 수도 있다. 따라서 최근에는 SNS에 가입하더라도 개인들이 다른 사람의 개인정보에 대한 접근을 제한하는 추세가 증가하고 있다.

OECD(2011; 10)에 의하면 개인정보의 수집유형은 크게 세 가지로 분류할 수 있다. 첫째로 개인이 자발적으로 개인집단 혹은 기업에게 정보를 제공하는 것이다. 소셜 네트워크 가입, 개인의 신용카드 사용 혹은 가족, 친구, 직장동료 등에게 개인정보를 제공할 수 있다. 두 번째로 불법적으로 개인정보를 수집할 수 있다. 정보제공자의 자발적 의사와 별개로 전화와 인터넷 등에서 개인정보를 수집하는 방법이 이에 해당한다. 세 번째로 개인정보를 통해 가공, 추정, 재생산하는 방법이 존재한다. 대표적인 예로 개인의 신용정보로 이는 과거 기록에 근거하여 재생산된 개인정보에 해당한다.

개인이 자발적으로 제공한 정보의 경우 정보를 열람 혹은 이용할 수 있는 주체들이 정당한 비용을 지불하지 않고 개인정보를 이용할 수 있다. 개인이 프라이버시를 보호받고자 원하는 경우 이에 대한 보호가 필요하며, 개인이 원하지 않는 경우 그 개인정보를 이용하는 주체는 정당한 비용을 지불하거나 해당되는 개인에게 효용을 제공할 수 있어야 한다. 그러나 디지털 사회에서 비공식적인 방법으로도 개인정보의 획득이 가능해 졌다. 예를 들어 과거 인터넷에서 금융기관 및 공공기관의 업무담당자 이름과 전화번호를 손쉽게 획득이 가능하여 이것

이 악용되기도 하였다.[6] 또한 비공식적인 시장에서 개인정보가 거래되고 있는 상황을 언론을 통하여 확인할 수도 있다. 정보이용의 무임승차자와 불법적 정보 이용자를 제외하는 방법으로 Varian(1998)은 정보재화를 물질재화로 전환·생산(과거 전화번호부 등)할 수 있다고 한다. 개인정보에 보완장치 등을 통하여 무임승차자의 개인정보 이용을 배제할 수도 있으며, 관련 법률의 구속력을 강화할 수도 있다.

정보재화로서 개인정보의 가치에 정의와 경제적 접근법에서 중요한 이슈는 다음 절에서 살펴볼 수 있는 것처럼 과연 개인정보를 공개하여, 다른 사람이 이를 이용하는 경우 해당 개인에게 양의 효과 혹은 음의 효과를 창출하는가의 여부라고 볼 수 있다.

2. 초기 정보경제학에 대한 고찰

개인정보에 대한 경제적 논의의 이해는 정보재화에 대한 논의에 대한 이해에서 출발한다. 초기 정보경제학에서는 모든 정보의 완전한 공개가 사회의 효율성을 증진할 수 있다고 주장하였다. 개인은 자신의 정보 가운데 유리한 것은 공개하고 불리한 것은 공개를 하지 않는 합리적(rational)인 의사결정 주체이다(Stigler, 1980). 따라서 시장에서 정보와 관련된 비효율성을 제거하기 위하여 초기 시카고(Chicago)학파의 접근방식은 개인정보를 포함한 모든 정보가 완전 공개되어야 한다고 생각하였다(Acquisti, 2010). 개인정보를 포함한 모든 정보를 완전하게 공개하는 경우, 소비자는 개인의 선호에 적절한 정보를 제공받아 적합한 의사결정을 내릴 수 있다. 기업도 이와 같은 완전정보 하에서는 영업활동에 효율적인 의사결정을 내릴 수 있다. 예를 들어 Posner (1980)는 노동시장 및 결혼시장 등에서 개인정보를 공개하지 않도록 정부에서 개입하는 것은 생산자가 자신이 생산한 상품의 결정을 소비자에게 알리지 않는 것과 유사하다는 주장을 하기도 한다.

6) 불법적인 행위가 증가함에 따라 이와 같은 정보는 점차 일반인에게 접근이 가능하지 않다.

3. 정보공개의 대한 논의의 발전

개인정보를 포함한 정보의 공개가 경제에 미치는 긍정적인 측면은 간과할 수 없다. 그러나 시카고학파의 논의는 이후 다양한 반론에 직면하게 된다. Varian (1996)은 예를 들어 컴퓨터를 구입한 소비자가 자신의 개인정보 즉 구매정보를 공개하는 경우 그 컴퓨터에 적합한 액세서리 등 부속품을 구매하기 위한 유용한 정보를 받을 수 있음을 인정한다.

그러나 이와 더불어 이미 구입한 컴퓨터에 대한 정보도 제공받고 있고, 관심이 없는 다른 컴퓨터에 대한 정보도 제공받을 수 있다. 다시 말해 과다한 정보의 제공을 지적한다. 컴퓨터를 판매한 회사로부터 구매정보를 획득한 업체는 개인에게 불편할 정도로 과다한 정보를 제공하고, 이로 인하여 개인뿐만 아니라 기업에게도 정보제공의 비용을 증가시켜 비효율을 초래할 수 있다는 것이다. 이에 추가적으로 생산자가 구매정보를 이용하여 소비자의 효용을 약탈할 수도 있다. 예를 들어 특정 컴퓨터를 구매한 고객에서 그가 선호할 수 있는 부수 기자재를 정상가격 보다 높은 가격을 제시하는 것이다. 즉 개인은 시장가격보다 높은 가격에 부수 기자재를 구입할 가능성을 배제할 수 없다.

Acquisti (2010)은 개인정보 공개가 두 가지 양면을 가지고 있음을 지적한다. 개인은 개인정보 공개를 통하여 새로운 정보 획득이 가능하고[7], 기업은 소비자에게 적절한 정보를 제공할 수 있다. 그러나 동시에 개인정보 공개는 부정적 효과도 창출하고 있다. 개인은 개인정보 공개로 정보의 홍수에서 불편함을 느낄 수 있고, 기업은 과다한 정보제공 투자를 할 수 있다. 일부 기업들은 개인정보를 불법적으로 악용하여, 개인은 심리적이고 정신적인 비용을 부담함과 동시에 사생활을 침해받을 수도 있다.

4. 개인정보의 보호와 침해에 대한 논의

최근에는 개인정보를 보호함으로써 개인의 효용극대화, 기업의 이윤극대화, 사회적 효용극대화를 달성할 수 있다는 주장이 제기되고 있다. Taylor (2004)는 소

7) 자신에게 적절한 정보제공을 보장받을 수 있어 합리적인 소비가 가능한 것이다.

비자가 개인정보에 대한 프라이버시를 통하여 효용을 달성할 수 있다고 주장한다. 특히 소비자가 자신의 개인정보가 매매될 것이라고 기대하지 않는 상황 하에서, 개인정보를 보유하고 있는 기업이 그 개인정보를 매매할 유인이 발생할 수 있으며 따라서 이는 궁극적으로 사회의 효용을 낮출 수 있음을 지적한다. 그리고 이와 같은 개인정보를 이용하여 기업은 개인의 프라이버시를 침해하여, 부적절한 수익을 창출할 가능성을 완전히 배제할 수 없다. Brunk (2002)는 소프트웨어 회사들이 프라이버시 기능을 강화하고 있다는 것은 프라이버시가 중요한 이슈로 자리 잡았음을 반증한다고 주장한다. 이는 또한 개인정보를 보호하는 것이 결국 기업의 이윤증가로 이어질 수 있는 상황으로 변화하고 있음을 보여주는 것이다. 예를 들어 미국 연방거래위원회에 따르면 99%의 온라인 업체가 개인정보를 보관하고 있다고 한다. 미국 최대의 온라인 거래업체 중에 하나인 아마존(Amazon.com)은 약 2천 3백만명의 소비자들에게 구매정보를 이용하여 상품의 가격책정을 하였고 이와 같은 부적절한 판매행위로 인하여 이미 6,896명에게 상품반품 조치를 실시하기도 하였다.

5. 개인정보 공개의 양면성

개인정보에 대한 정보경제학적 논의를 살펴본 결과 개인정보의 가치는 두 가지 측면이 존재한다는 것을 확인할 수 있었다. 개인정보 공개가 개인과 기업 즉 사회적으로 긍정적 효과를 창출한다는 한 측면과, 개인정보의 공개가 개인과 기업 즉 사회적으로 부정척인 효과를 창출한다는 다른 측면이다. 개인정보의 공유는 사회적 가치의 증진을 유도할 수 있지만, 이와 반대로 개인정보의 공유는 사회적 가치의 하락을 유도할 수도 있다는 상반된 견해인 것이다. 적정수준의 개인정보 공개는 개인과 기업 사이의 정보의 비대칭을 극복할 수도 있지만, 적정수준 이상의 개인정보 공개는 개인의 프라이버시를 침해하며, 개인과 기업에게 불이익을 줄 수 있다는 평가이다. 이와 함께 만일 개인과 기업이 비합리적인 주체로 간주하는 경우 개인정보의 공유 혹은 침해가 야기할 수 있는 사회적 문제는 더욱 증가할 수 있다. 예를 들어 단순(naive)한 개인은 자신의 개인정보에 대한 침해의 가능성을 제대로 인식하지 못하고, 비합리적인 기업은 약탈적

(predatory)으로 개인정보를 이용할 수 있음을 배제할 수 없다는 것이다. 따라서 적정수준의 개인정보의 공개는 사실 그 범위를 정의하기 어려운 측면이 존재하며, 경제주체들의 비합리적인 의사결정을 방지하는 것도 개인정보 보호의 중요한 이슈가 될 수 있다.

제3장 개인정보 유출사고 동향분석

현재 국내 개인정보 유출 사고의 규모를 정확히 파악하는 것은 어렵다. 일본의 경우 개인정보 유출 사건이 일어나면 이를 공표하는 것이 법률로 정해져 있어 실제 일어난 유출 사고의 규모를 검색을 통해 매우 정확히 추적할 수 있다. 하지만 국내의 경우에는 이러한 법적 제도가 마련되어 있지 않기 때문에 정확한 개인정보 유출사고의 규모를 추정하는 데에 어려움을 겪고 있다.

본 보고서에서는 그 피해액을 최대한 정확히 추정하고자 뉴스·신문 검색을 통해 미디어를 통해 알려진 모든 유출 사건을 조사했으며, 이러한 방식으로 2006년부터 2012년에 이르는 유출 사고 관련 데이터를 수집했다. 그 결과는 아래의 [표 3-1]과 같다.

[표 3-1] 국내 연도별 유출 사건 및 유출 개인정보 수

(단위 : 건)

연도	사건 수	개인정보 수	사건 당 유출정보 수
2006	136	77,650,803	570,962
2007	198	67,091,626	338,847
2008	70	43,972,833	628,183
2009	41	16,837,379	410,668
2010	50	16,922,404	338,448
2011	-	50,486,783	-
2012	-	12,930,317	-

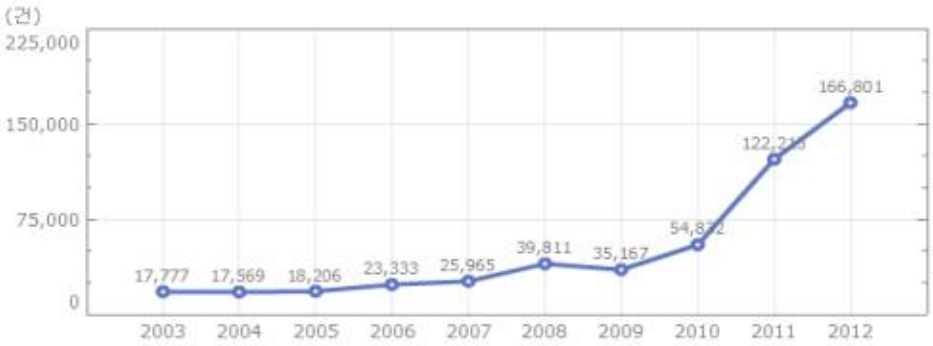
출처) 메타검색과 인터넷진흥원 제공 자료를 바탕으로 저자 작성

결과를 보면 유출된 개인정보 수가 2006년 7,700만 건을 최고점으로 점차 감소하는 추세지만, 2011년에 예외적으로 5,000만 건의 대규모 유출이 있었다는 사실을 확인할 수 있다. 이는 2011년에 발생한 SK컴즈의 3,500만 건에 이르는 대형 유출사고의 영향이며, 이를 제외하면 전반적으로 개인정보 유출 건수가 감소

하는 추세라는 점을 알 수 있다. 비록 정보의 출처가 신문과 뉴스 등의 언론 자료들이기 때문에 미디어에 노출되지 않은 정보의 규모를 알 수 없다는 점에서 정확한 정보라 단정 지을 수는 없다. 그러나 개인정보 유출 건수가 감소세에 있다는 점을 통해 사회 전반의 정보보호에 관한 의식이 높아지고 개인정보 유출 방지를 위한 노력이 커지고 있음을 추측해 볼 수 있다.

그러나 인터넷 이용인구가 3,650만 명 정도인 상황에서 언론에 노출된 개인정보 유출 건수만 헤아려도 몇 천만 건에 이른다는 사실은 아직 정보보안 의식의 개선과 정보보안에 대한 더 많은 투자가 필요하다는 점을 시사하고 있다.

(그림 3-1) 개인정보 침해 신고 및 상담 현황



출처) 방송통신위원회 (한국인터넷진흥원 개인정보침해신고센터 접수자료)

또한 (그림 3-1)의 한국인터넷진흥원에서 조사한 '개인정보 침해와 관련된 신고 및 상담 현황'을 살펴보면 2003년부터 2012년까지 침해 신고 및 상담이 꾸준히 증가하고 있으며, 2012년에는 166,801건으로 가장 높은 상담 건수를 기록하고 있다. 이는 아직도 수많은 사람들이 개인정보 유출로 인한 피해를 입고 있으며 이러한 추세가 쉽사리 줄어들지 않고 있다는 사실을 보여준다.

제4장 개인정보 침해에 따른 사회적 비용분석 관련 선행연구 분석

제1절 일본 JNSA

일본의 JNSA(Japan Network Security Association)에서는 수년 전 부터 기업의 개인정보 유출에 따른 피해액을 산정하기 위한 보고서를 작성하기 시작했다. 초창기였던 2003년의 자료[8]를 보면 보고서는 그 내용에 따라 두 개의 섹션으로 나누어져 있으며, 각각의 섹션은 다음과 같은 내용을 담고 있다.

섹션 1은 정보 유출 환경에 관한 다양한 자료 조사를 토대로 유출에 따른 피해액 추정과 그 대응비용에 관한 논의를 다루고 있으며, 섹션 2는 정보 유출과 관련된 법적 보상비용을 산정하고 여기에 주가 변화를 통해 단기·중기적 피해액을 산출하는 방법을 추가적으로 논의하고 있다.

그러나 2010년 보고서[9]에서는 그 타당성에 관한 의문이 제기되고 산정이 어렵다고 평가되는 직접 복구 비용, 기회비용 등 사고비용의 제산정과 관련된 과거 보고서의 섹션 1과 관련된 부분을 제외하고, 섹션 2의 적정 법정 보상액 산정에 관한 부분의 경우 판사의 판결에 따라 보상 판결액이 바뀌는 등 추정과 실제가 차이가 발생하는 문제점이 있다는 점 등을 고려해서 유출된 정보의 기본 가치액을 추정하는 원론적 형태로 모델의 방향을 수정하였다. 또한 2003년도 보고서에서 잠시 시도되었던 주가를 이용한 피해액 산정 방법은 그 예측의 타당성 여부에 대한 문제점으로 현재는 사용하지 않고 있다.

JNSA는 일본에서 법으로 강제하여 공시하게 되어있는 개인정보 유출 관련 사건을 집계, 상기 개발된 모델에 대입하고, 정보의 기본 가치 추정 모델인 'JO모델'(JNSA Damage Operation Model for Individual Information Leak, 이하 JO모델)을 가치 추정에 적용함으로써 그 피해액을 추정하였다.

'JO모델'은 JNSA에서 유출된 정보의 가치를 측정하기 위해 자체적으로 개발

8) JNSA(2003) 情報セキュリティインシデントに關する 調査報告書
9) JNSA(2010) 情報セキュリティインシデントに關する 調査報告書

한 가치 측정 모델이다. 이는 유출된 정보의 가치 금액을 개인정보 유출 유형에 따라 경제적 정신적 기준으로 3 X 3 단계로 분류하고 있다. 이를 스케일 업(1이상 곱하기)하는 형태의 산출식이며, 수집된 자료를 대입해 그 피해액을 추정할 수 있다.

[표 4-1] JO 모델

손해배상액 = 누설 개인정보 가치
× 정보 누설원조직의 사회적 책임도
× 사후 대응 평가
= (기초 정보 가치× 정보 민감도× 본인 추정 가능도)
× 정보 누설원조직의 사회적 책임도
× 사후 대응 평가
= **기초 정보 가치[500]**
× 정보 민감도(=EP MAP[Max($10^{max(x)-1}+5^{max(y)-1}$)]
× 본인 추정 가능도[6, 3, 1]
× 사회적 책임도[2, 1]
× 사후 대응 평가[2, 1]

출처) JNSA(2010), "情報セキュリティインシデントに関する 調査報告書"

JO 모델은 기본적으로 500점의 정보 가치를 시작으로 여기에 여러 가지 상황에 따라 상황별 분류표에서 가중치를 찾아 곱해서 최종 점수를 산출한 다음 특정 범위의 점수대의 정보 가치를 얼마로 한다는 방식으로 그 가치를 산정한다.

EP 맵은 [표 4-2]를 참고하면, 개인정보가 유출되었을 때 피해자가 느끼는 정신적 고통과 경제적 고통을 3 X 3단계로 분류한 정보이다. 예를 들어, 유출 정보가「이름, 주소, 생년월일, 성별, 전화 번호」이면 (1,1), 「병명」이면 (2,1), 「계좌 번호」이면 (1,3) 인 형식이다. 계좌 번호와 병명이 유출되었을 때, JO 모델의 세부 정보도 관련 식인 [Max($10^{\max(x)-1}+5^{\max(y)-1}$]에 계좌번호와 병명에 해당하는 (1,3)과 (2,1)을 적용하면[10] [Max($10^{2-1}+5^{3-1}$]=10+25=35란 가중치를 얻을 수 있다.

10) 계좌번호(x=1, y=3), 병명(x=2,y=1) 이므로 Max(x)=2, Max(y)=3

[표 4-2] EP MAP

경제적 손실 레벨				
	3	계좌번호＆비밀번호, 카드번호＆유효기한, 금융계 웹사이트의 로그인 어카운트&패스워드	유언서	전과전력, 범죄력, 블랙리스트
	2	패스포트 정보, 상품 구입 기록, ISP 계정과 패스워드, 계좌번호, 크레디트 카드번호, 금융계 웹사이트의 로그인 계정, 인감증명서	연수입, 자산, 건물, 땅, 잔고, 빚, 소득, 차입기록, 구입 이력, 급여액, 상여액, 납세금액	
	1	이름, 주소, 생년월일, 성별, 금융기관명, 주민등록번호, 메일주소, 건강보험번호, 연금증서번호, 면허증번호, 회원번호, 전화번호, 핸드폰, 연금정보, 회사이름, 학교명, 직무, 직업, 신장, 체중, 혈액형, 신체특성, 사진, 음성, 체력측정치, 가족구성, ISP 계정명 등	건강진단결과, 성격판단결과, 병력, 신체검사기록, 지문, 장애정보, DNA정보, 생체인증정보, 스리사이즈, 인종, 방언, 국적, 취미, 특기, 기호, 민족, 상벌, 직업 경력, 학력, 성적, 시험득점, 메일 내용, 위치정보, 보험가입 상황, 일기 등	가맹정당.노동조합, 정치적 견해, 신조, 사상, 종교, 신앙, 본적, 병상, 보유 감염증, 버릇, 진료기록카드, 정신적 장애 정보, 성생활의 정보
		1	**2**	**3**
		정신적 피해		

출처) JNSA(2010), "情報セキュリティインシデントに関する 調査報告書"

본인 추정 가능도는 누설된 개인정보로부터 얼마나 본인 확인이 쉬운지를 나타내는 척도다. 예를 들어 은행의 계좌번호나 주소 등의 정보는 단독으로 유출되어도 이름이나 전화번호 등의 추가 정보가 수반하지 않으면 본인 확인이 어렵다. 반면 추가 정보가 주어지면 좀 더 쉽게 본인 확인이 가능한데 이러한 특징을 일정 기준에 따라 표로 정리한 것이 본인 추정 가능도이다.

[표 4-3] 본인 추정 가능도

판정 기준	본인 추정 가능도
간단히 개인을 추정 가능한 경우 (예 : 이름과 주소가 함께 포함되는 경우)	6
비용을 들이면 개인을 추정할 수 있는 경우 (예 : 이름 또는 주소와 전화번호가 함께 포함되는 경우)	3
개인을 특정하기 곤란한 경우	1

출처) JNSA(2010), "情報セキュリティインシデントに関する 調査報告書"

사회적 책임도는 개인정보 유출 사고가 일어난 주체의 사회적 영향력과 책임을 나타내는 지표로서 [표 4-4]와 같이 「일반보다 높다」와 「일반적」인 '상, 중'의 2단계로 나뉜다. 사회적 책임도가 일반보다 높은 조직은 일본의 법률인 「개인정보의 보호에 관한 기본방침」에 '적정한 취급을 확보해야 할 개별 분야'로서 정부기관 등 공적 기관과 지명도가 높은 대기업을 포함하고 있다. 사회적 책임도는 다음과 같다.

[표 4-4] 사회적 책임도

판정 기준		책임도
상	취급수단 등을 확보해야 할 개별 분야의 업종(의료, 금융·신용, 정보 통신 등), 공적 기관, 지명도가 높은 대기업	2
중	그 외 일반적인 기업, 및 단체, 조직	1

출처) JNSA(2010), "情報セキュリティインシデントに関する 調査報告書"

마지막으로 사후 대응 평가는 명확한 기준이 없기에 과거의 정보 유출 관련 케이스를 적절과 부적절로 나눠 어느 쪽에 더 가까운 대응을 했는지에 따라 평가한다. 잘 했을 경우 적절하거나 불명확하면 1점, 부적절 했다면 2점의 점수를 부여한다. 이렇게 개별 사건을 다양한 표를 통해 요소별 점수를 계산한 다음 JO 모델에 적용하면 각 사건별 점수가 나오는데 이 점수를 피해액으로 변환하는 것이 JNSA의 방식이다.

제2절 미국 Ponemon

미국의 정보 및 시큐리티 관련 단체인 포네몬 연구소는 2005년 개인정보 유출에 따른 비용[11](직접비용과 간접비용 및 기회비용) 추정을 시도한 첫 연구를 시작으로 2009년까지 보고서를 출간해 오고 있다. 이 중 미국의 경우 15개 산업에 걸친 45개 기업을 설문 기법을 이용해 심층 조사함으로써 개인정보 유출에 따른 직·간접비용뿐만 아니라 고객의 신뢰도 하락과 고객이탈에 이르는 총체적인 피해 규모를 조사하고 있다.

포네몬 연구소는 미국뿐만 아니라 영국, 독일, 오스트레일리아, 프랑스를 조사 대상으로 삼고 있으며, 매 년 관련 국가의 개인정보 유출 보고서를 발표하고 있다. 또한 이 보고서들을 하나로 모아 비교 분석한 'Global Cost of Data Breach'라는 보고서도 함께 내놓고 있는데, 이는 보안 환경과 경제 규모에 따른 국가들의 피해액을 체계적으로 비교·분석할 수 있는 자료로 활용되고 있다. 이들이 조사하는 대상은 2009년 기준으로 전 세계 18개 산업에 걸친 130여개의 기업에 이른다.

2009년 미국 포네몬 보고서의 주요 내용은 연간 개인정보 유출 사건의 기록당 소요비용과 직·간접비용, 연간 총 피해비용, 산업별·단계별 피해비용, 세부 항목별 소요비용 등으로 이루어져 있으며 상세 내용은 다음과 같다.

1. 주요 내용

(1) 산업분야별 개인정보 유출건수 및 유출경로

포네몬 보고서는 15개의 산업분야별 개인정보 유출 사고 건수를 기록하고 있으며 유출경로가 내부인지 협력업체인지 분류하고 있다. 내부 유출은 회사 내부에서 직접 유출된 개인정보 사고 건수를 의미하고 있으며, 협력업체 유출은 위탁, 제공 등의 위임업무를 수행하는 외부 협력업체에 발생한 개인정보 유출을

11) Ponemon(2005~2009)에서의 비용(Cost)은 기업이 개인정보 유출사고로 인한 부(-)의 파급효과를 최소화하기 위하여 기업이 지출할 것으로 예상되는 금전적 비용을 말한다.

의미한다.

[표 4-5]를 보면 15개의 산업분야에서 소매업과 금융 분야의 개인정보 유출사고 건수가 8건으로 가장 높은 것을 볼 수 있다. 소매업에서의 내부 유출은 6건, 협력업체는 2건으로 내부유출이 높게 나온 반면에 금융업에서는 내부유출이 3건, 협력업체 유출이 5건으로 협력업체 개인정보 유출이 높게 나온 것을 볼 수 있다. 15개의 사업군의 전체 개인정보 유출사고 45건 중 내부 유출은 총 26건이며 협력업체 유출은 19건으로 내부 유출로 인한 개인정보 유출이 높은 것을 볼 수 있다. 이는 향후 데이터를 분류하는 기준이 되며, 다양한 방향으로 연구를 발전시키는데 기본 틀이 된다.

[표 4-5] 산업분야별 개인정보 유출건수

분야	내부유출[1]	협력업체 유출[2]	총 유출사고 수
통 신	1	0	1
소비재	2	1	3
교 육	2	1	3
에너지	0	1	1
금 융	3	5	8
건 강	2	3	5
숙박업	1	0	1
제조업	1	0	1
미디어	1	0	1
제 약	0	1	1
연 구	1	0	1
소매업	6	2	8
서비스	2	3	5
기 술	2	2	4
운송업	2	0	2
합 계	26	19	45

출처) Ponemon Institute(2010), "Fifth Annual US Cost of Data Breach, January 2010".

1) 회사 내부에서 직접 유출된 개인정보 사고 건수를 의미함.

2) 위탁, 제공 등의 위임업무를 수행하는 외부업체에서 발생한 개인정보 유출건수를 의미함.

(2) 개인정보 유출 피해액의 연간 추이

포네몬 연구소에서는 매년 개인정보 유출에 관한 평균 피해액을 조사하고 있다. 2005년부터 2009년까지 개인정보 유출 기록(1인 기준)당 평균 피해액을 직접비용과 간접비용으로 구분하여 그 비용을 추정하고 있으며, 개인정보 유출 사고 한건 당(사고기준)으로 평균 피해액을 제시하고 있다.

[표 4-6] 유출된 개인정보 건당 연간 평균 피해액

(단위 : US 달러, %)

연도	유출 개인정보 건당 피해액	전년대비 증감률
2005	138	-
2006	182	31.9 ▲
2007	197	8.2 ▲
2008	202	2.5 ▲
2009	204	1.0 ▲

출처) Ponemon Institute(2010), "Fifth Annual US Cost of Data Breach, January 2010".

[표 4-6]을 참고해 보면 2005년에는 138건, 2006년에는 182건, 2007년에는 197건으로부터 2009년 204건까지의 유출된 개인정보 기록 1건당 평균 피해액을 보면 건당 피해액은 꾸준히 증가하고 있는 반면 피해액의 증가율은 점점 줄어들고 있는 점을 알 수 있다. 이는 지난 5년간 해당 기업들이 개인정보 유출사고를 경험하며 나름의 노하우를 쌓고 이를 바탕으로 대응체계와 방법에 변화를 주었기 때문으로 볼 수 있다.

이러한 사실은 보고서에서 제시한 피해액의 구성요소, 단계별 피해비용 그리고 피해액의 세부 항목별 비율 등의 자료를 통해 확인할 수 있다.

[표 4-7] 유출된 개인정보 건당 피해액의 직·간접비 구성

(단위 : US 달러, %)

연도	직 접 비		간 접 비	
		전년대비 증감률		전년대비 증감률
2005	88	-	50	-
2006	128	45.5 ▲	54	8 ▲
2007	145	13.3 ▲	52	3.7 ▼
2008	152	4.8 ▲	50	3.8 ▼
2009	144	5.3 ▼	60	20 ▲

출처) Ponemon Institute(2010), "Fifth Annual US Cost of Data Breach, January 2010".

[표 4-7]에서 볼 수 있듯이 과거 5년간 직접비[12]의 변화가 간접비[13]의 변화에 비해 큰 폭으로 증가하였다. 이는 다음 페이지에서 다룰 각 단계별 비용 및 세부 항목별 비용에서 자세하게 설명하겠지만 직접비용에 해당하는 법적 대응비용과 고객감소로 인한 매출손실이 크게 늘었기 때문이다.

[표 4-8] 유출 사고 건당 평균 피해비용 및 표본 수

(단위 : US 달러, %)

연도	평균 피해비용	전년대비 증감률	조사 기업수
2005	4,541,429	-	13
2006	4,789,637	5.5 ▲	31
2007	6,355,132	32.7 ▲	35
2008	6,655,758	4.7 ▲	43
2009	6,751,451	1.4 ▲	45

출처) Ponemon Institute(2010), "Fifth Annual US Cost of Data Breach, January 2010".

12) 원가직접대상에 명백하게 추척할 수 있는 원가. 여기서는 사고대응 인건비, 법적 비용 등과 같이 개인정보 유출사고와 직접적으로 연결되는 비용을 말한다.
13) 직접대상에 명백하게 추척할 수 없는 원가. 시스템 교체비용 등 특정 개인정보 유출사고 이외의 사건과도 연결되는 비용을 말한다.

유출 사고 건당 평균 피해비용은 증가추세에 있으나, 증가폭은 경우 2007년을 제외하면 위의 개인정보 건당 평균 피해액과 마찬가지로 점차 줄어들고 있는 추세다.

(3) 유출 단계 모형

포네몬 보고서에서는 유출의 단계를 크게 발견(Detection)&확대(Escalation), 통지(Notification), 사후대응(Ex-post Response), 매출피해(Lost Business)의 단계로 나누어 그 피해액을 산출하고 있다. 여기서 발견과 확대는 개인정보 유출이 일어난 것을 최초로 발견하고 알려진 피해 규모가 확인되어 감에 따라 점점 커져가는 단계를 의미한다. 2단계 통지는 이러한 피해사실을 고객들에게 알리는 단계를 말하며, 3단계 사후대응은 피해의 확산을 막고 피해액을 최소화 하기 위해 노력하는 단계를 의미한다. 마지막 4단계 매출피해는 개인정보 유출사고가 고객 이탈로 이어져 매출에 손해를 보는 단계를 말한다.

[표 4-9] 개인정보 유출사고의 단계

단 계	설 명
발견 & 확대	· 개인정보 유출이 일어난 것을 최초 발견하고, 알려진 피해규모가 확인되어감에 따라 점점 커져가는 단계
통지	· 피해사실을 고객들에게 알리는 단계
사후대응	· 피해의 확산을 막고 피해액을 최소화하기 위한 노력을 하는 단계
매출피해	· 개인정보 유출사고가 고객이탈로 이어져 매출에 손해를 보는 단계

출처) Ponemon Institute(2010), "Fifth Annual US Cost of Data Breach, January 2010".

이러한 분류는 체계적인 비용 집계를 위한 카테고리의 역할 뿐만 아니라 향후 각 단계별 어떤 조치에 따라 비용이 변하는지 등의 추가 연구에 활용하게 된다.

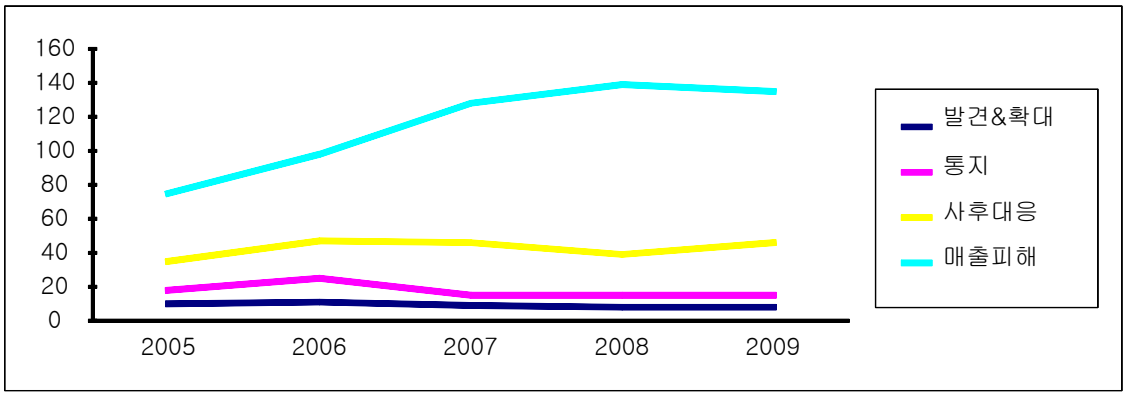
[표 4-10] 각 단계별 피해비용

(단위 : US 달러)

	발견 & 확대	통지	사후대응	매출피해
2005	10	18	35	75
2006	11	25	47	98
2007	9	15	46	128
2008	8	15	39	139
2009	8	15	46	135

출처) Ponemon Institute(2010), "Fifth Annual US Cost of Data Breach, January 2010".

(그림 4-1) 각 단계별 피해비용 그래프



출처) Ponemon Institute(2010), "Fifth Annual US Cost of Data Breach, January 2010"를 바탕으로 저자작성

[표 4-10]과 (그림 4-1)은 2005년부터 2009년까지의 유출에 따른 피해비용을 각 단계별로 구분하고 있다. 이를 통해 단계별 비용이 어떻게 구성되어 있는지와 이것이 매 년 어떻게 변해왔는지 한 눈에 알 수 있다. 1단계인 발견과 확대 비용은 매년 감소하는 것을 볼 수 있는 반면에 4단계인 매출 피해의 경우 지난 5년간 큰 폭으로 상승한 것을 볼 수 있다.

이것이 시사하는 바는 상품과 서비스를 소비하는 고객들이 개인정보 유출사고에 점점 더 민감하게 반응하고 있으며 나아가 유출사고가 매출에 더 직접적으로 영향을 미치게 되었다는 것을 보여준다.

(4) 개인정보 유출로 인한 산업별 고객 이탈비율

개인정보 유출로 인한 고객 이탈은 매우 직접적이고 규모가 큰 피해이다. 이를 추정하기 위해서는 고객 1인이 갖는 경제적 가치뿐만 아니라 얼마만큼의 고객이 사고로 인해 서비스를 이탈했는지에 관한 정보가 필요한데, 포네몬 보고서에서는 이를 각 산업 분야별 고객 이탈율을 조사해서 해결하고 있다.

[표 4-11] 개인정보 유출로 인한 산업별 고객 이탈비율

(단위 : %)

순위	산업군	고객 이탈비율
1	건강관련	6.0
	제약	
	통신	
2	금융	5.0
	서비스	
3	소비재	4.0
	숙박업	
4	교육	3.0
	연구	
5	기술	2.0
	소매업	
	운송업	
6	미디어	1.0
	에너지	
	제조업	

출처) Ponemon Institute(2010), "Fifth Annual US Cost of Data Breach, January 2010".

이를 통해 고객 전환이 활발하게 이루어지는 분야와 그렇지 않은 분야를 구분할 수 있으며, 고객 이탈로 인해 상대적으로 큰 피해를 입는 회사와 그렇지 않은 회사를 쉽게 추정해 볼 수 있다.

실제 가장 큰 대비를 보인 통신, 제약, 건강관련 서비스 군과 제조업, 에너지,

미디어 군의 경우 6배에 이르는 고객 이탈율의 차이를 보이고 있다.

(5) 세부 항목별 소요 비용

실제 어떤 항목에서 어떤 비용이 얼마만큼 들었는지 아는 것은 향후 정보보안과 관련된 정책을 세우는데 좋은 참고가 된다. 또한 이는 체계적인 손실 추정을 위한 기준 항목이 된다는 점에서도 큰 의의가 있다.

포네몬에서 조사한 세부 항목별 피해 비용을 분석해보면 전체 비용 중 평균적[14]으로 인건비가 약 32%, 홍보비용이 2%, 법적 비용은 10%, 고객 이탈로 인한 수익감소와 새로운 고객을 유치하는데 드는 비용이 약 50% 정도를 차지하는 것을 알 수 있다.

[표 4-12] 세부 항목별 피해 비용 비율 2005-2009

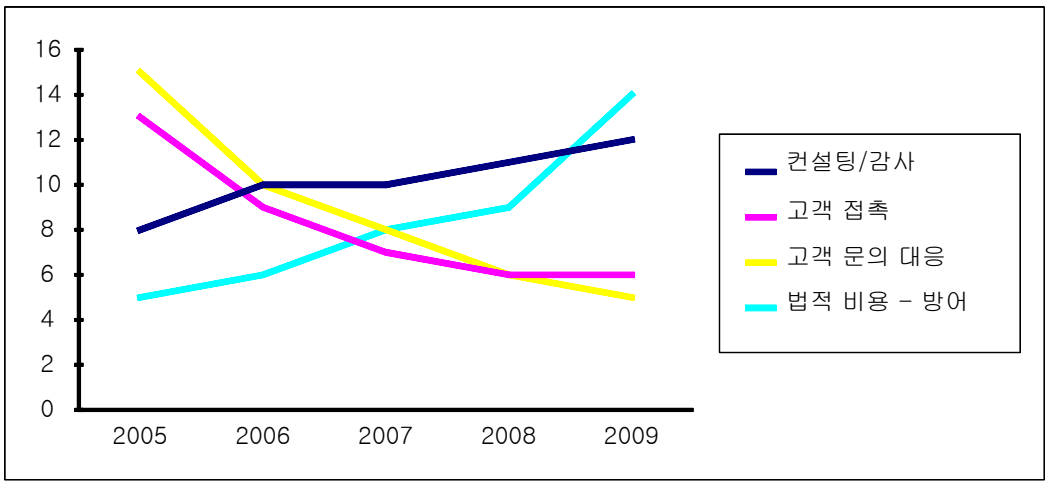
(단위 : %)

비용 항목	2005	2006	2007	2008	2009
조사 비용	8	8	8	9	8
***컨설팅 / 감사 비용**	**8**	**10**	**10**	**11**	**12**
***고객 접촉 비용**	**13**	**9**	**7**	**6**	**6**
***고객 문의 대응 비용**	**15**	**10**	**8**	**6**	**5**
홍보 비용	0	1	3	1	1
***법적 비용 - 방어**	**5**	**6**	**8**	**9**	**14**
법적 비용 - 선고 이행 비용	3	3	3	1	2
공짜 / 할인된 서비스 비용	4	2	1	2	1
브랜드 방어 비용	3	3	2	2	2
매출 손해 (고객 이탈)	35	39	41	43	40
신규 고객 유치 비용	6	8	9	9	9

출처) Ponemon Institute(2010), "Fifth Annual US Cost of Data Breach, January 2010".

14) 2005~2009년, 5년간의 평균

(그림 4-2) 세부 항목별 피해 비용 비율 2005-2009



이 중 5년간 일정한 변화의 추이를 보인 몇 가지 요소를 살펴보면 기업들의 대응방식이 어떻게 변했는지를 알 수 있다. 컨설팅 비용과 법적 방어 비용은 증가한 반면, 고객 접촉 비용과 고객 문의 대응 비용은 큰 폭으로 감소한 것을 확인할 수 있는데 이는 기업이 고객과 접촉해서 사건을 해결하기 보다는 컨설팅 비용을 들여 전략적인 계획을 짜고, 소송을 통해 방어하는 것을 더 선호하게 되었다는 점을 보여준다.

2. 추가 연구

추가 연구는 단순 데이터 분석을 넘어 보안 정책 수립과 향후 나아갈 방향을 설정하기 위한 자료 수집 및 분석 단계다. 이를 바탕으로 포네몬 보고서에서는 결론적으로 몇 가지 의견을 제안하며 마무리를 짓는다.

(1) 정보 유출 형태와 협력업체 관리의 중요성

포네몬의 연구결과에 따르면 개인정보 유출에 있어 가장 큰 비중을 차지하고, 현재도 계속 증가하고 있는 채널은 협력업체에 의한 유출이다. 이는 내부 보안뿐만 아니라 외부 협력업체의 체계적인 관리가 매우 중요하다는 사실을 보여주는 결과다.

[표 4-13] 정보 유출의 주된 원인

(단위 : %)

유출 원인	책임 비율
협력 업체	**42**
취급 부주의 / 태만	40
장치 분실	36
시스템 문제	36
공격 범죄	24

출처) Ponemon Institute(2010), "Fifth Annual US Cost of Data Breach, January 2010".

(2) 정보보호 관리자 유무에 따른 손실 비용 차이

[표 2-14]는 정보보호 관리자 존재 유무에 따른 비용 차이를 보여주고 있다. 정보보호 관리자가 없을 경우에는 평균 235달러의 비용이 들며 정보보호 관리자가 없을 경우에는 156달러로 약 78달러의 비용 차이가 나는 것을 볼 수 있다. 이는 정보보호 관리하의 체계적인 대처가 평균적으로 약 50%의 비용을 줄인다는 사실을 보여주고 있다.

[표 4-14] 정보보호 관리자 존재유무에 따른 비용차이

(단위 : $ / 건)

	정보보호 관리자 있음	정보보호 관리자 없음	추가 부담률
비용	약 157	약 236	약 50% (79)

출처) Ponemon Institute(2010), "Fifth Annual US Cost of Data Breach, January 2010".

(3) 회사의 경계 태도에 따른 비용 차이

[표 4-15]는 유출에 대한 경계 태도에 따른 비용차이를 보여주고 있다. 유출 경계에 적극적인 자세를 보이는 회사일수록 더 적은 유출 비용을 지출하고 있는

데 포네몬 보고서에서는 평균 미만의 경계 태도를 보이는 기업의 경우 평균 이상의 경계 태도를 보이는 기업에 비해 약 2.5%의 비용을 추가적으로 지출하고 있다는 사실을 통해 이를 증명하고 있다.

[표 4-15] 경계 태도에 따른 비용차이

(단위 : $ / 건)

	평균 이상의 경계	평균 미만의 경계	추가 부담률
비용	약 202	207	약 2.5% (5)

출처) Ponemon Institute(2010), "Fifth Annual US Cost of Data Breach, January 2010".

(4) 외부 보안 컨설턴트의 유무에 따른 비용 차이

[표 4-16]은 개인 정보 유출사고 발생 했을 때 외부 보안 컨설턴트 존재 유무에 따른 비용 차이를 보여주고 있다. 사고 대응에 외부 컨설턴트가 관련되어 있을 때 소요되는 피해 비용은 그렇지 않은 경우에 비해 현저히 낮아지는 점을 볼 수 있다. 포네몬 보고서에 따르면 외부 보안 컨설턴트가 있는 경우 약 36%의 비용이 절감되는 것을 알 수 있는데 이는 사고가 났을 때 안일하게 대처할 생각은 버리고 전문가의 조언을 통해 체계적으로 대처한다면 사고 대응 비용을 오히려 크게 줄일 수 있다는 점을 보여준다.

[표 4-16] 외부 보안 컨설턴트 존재 유무에 따른 비용차이

(단위 : $/ 건)

	컨설턴트 있음	컨설턴트 없음	추가 부담률
비용	약 170	약 231	약 36% (61)

출처) Ponemon Institute(2010), "Fifth Annual US Cost of Data Breach, January 2010".

3. 포네몬 리서치의 결론

지금까지 살펴본 포네몬(Ponemon) 리서치의 결론을 몇 가지로 요약해 보면 다음과 같다.

① 외부 IT Security 전문가를 고용하면 유출 피해 비용을 크게 줄일 수 있다.

② 서드파티(협력업체)를 통한 정보 유출의 피해는 매우 큰 비중을 차지하고 있으며 날로 커지고 있다. 이를 위해 추가적인 연구와 컨설팅 비용을 지출해야 한다.

③ 1/3이 넘는 정보유출이 노트북의 분실에서 비롯되며, 이는 일반적인 정보유출에 비해 훨씬 큰 비용을 소모한다.

④ 데이터 유출을 처음 겪는 회사의 경우 미리 경험이 있었던 회사에 비해 더 큰 비용을 지출한다.

⑤ 내부 부주의에 의한 개인정보 유출은 조금씩 줄어들고 있다.

⑥ 기업들은 점점 더 많은 비용을 법적 비용 등의 사후 비용으로 지출하기 시작했다.

⑦ 빠른 대응이 언제나 비용을 줄여주는 것만은 아니다. 어떤 상황에서는 비용을 줄여주지만, 어떤 경우에서는 그렇지 않다.

⑧ 암호화된 기술을 적극적으로 활용하는 것이 정보 유출을 막는 가장 저렴하고 효과적인 방법 중 하나이다.

제5장 개인정보의 가치 평가 및 개인정보 침해에 따른 사회적 비용

제1절 시장을 통한 수익평가

개인정보에 대한 가치추정에 있어서 개인정보 제공이 개인에게 긍정적인 효과를 창출할 수 있지만, 반대로 부정적인 효과를 창출할 수 있음을 살펴보았다. 정보주체가 개인정보를 제공을 통하여 효용을 얻을 수 있는 경우, 개인정보 제공에 대한 비용을 지출하더라도 정보를 제공할 유인이 존재할 것이다. 예를 들어 특정 단체에 가입을 원하는 개인들이 회비를 납입하는 경우가 이에 해당할 수 있다. 개인들은 특정 단체에 가입함으로써 특정 단체에게 제공하는 정보에 대한 혜택을 고려하여 비용을 납입할 유인이 존재하는 것이다. 개인정보를 제공으로 정보주체의 효용감소가 발생하는 경우 개인은 이에 합당한 보상이 존재하지 않는다면 개인정보를 제공할 유인이 발생하지 않을 것이다. 개인정보의 가치평가의 경우 그 개인정보가 개인에게 어떠한 경제적 (비)효용을 창출하는 가에 따라 달라질 수 있는 것이다.

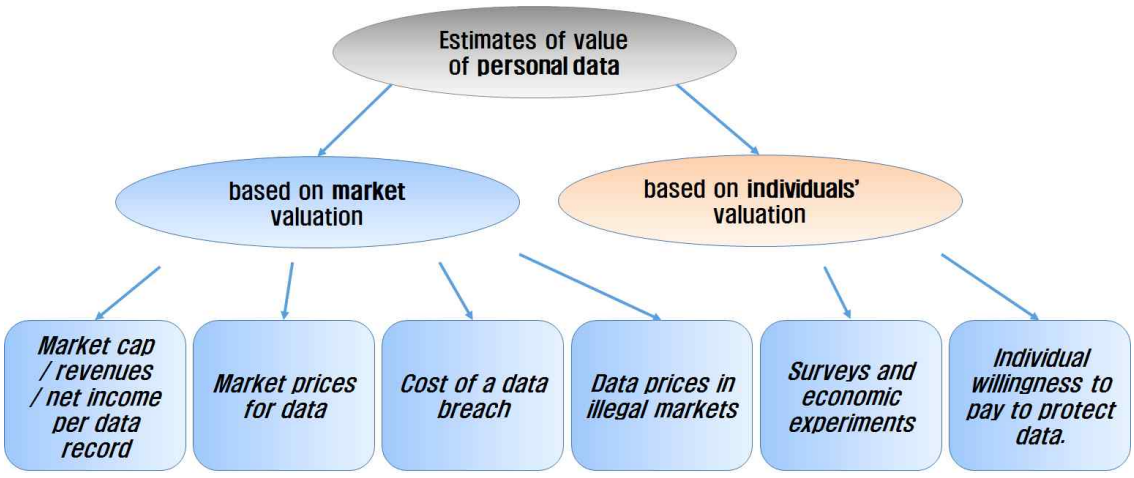
개인정보를 제공하는 주체뿐만 아니라 개인정보를 수입하는 정보수집자 즉 기업측면에서도 개인정보의 가치평가는 개인정보에 특성에 따라 변화할 수 있다. 기업이 보유하고 있는 개인정보는 기업의 유형과 개인정보의 활용도에 대하여 다른 평가를 내릴 것이다. 기업들이 마케팅을 위해 소비자 정보에 민감해지면서 미국의 개인정보 거래시장은 1조 8000억 달러의 규모로 추산되고 있으며 '데이터 브로커'라 불리는 정보수집·판매 업체들이 경쟁적으로 다양한 방법을 동원해 자료를 수집하고 있기도 하다. 예를 들어 일반 개인정보의 거래는 헐값에 이루어지고 있으며 암환자 목록이나 신생아 정보 같이 기업의 매출에 직결될 수 있는 민감한 개인정보의 경우에는 더 높은 가치가 측정된다.

개인정보 거래업체인 리즈플리스는 1,000명의 암환자 개인정보 목록을 관련 기업과 병원 등에 260달러에 팔고 있으며, 아기를 갓 출산한 부부 목록과 주택을 구매하려는 사람 목록은 1,000명 기준 85달러로 거래하고 있다.[15] 미국 정보

기관의 개인정보 비밀수집이 논란이 되면서 개인정보 수집이 거센 역풍을 맞고 있지만, 기업들의 개인정보 수집 노력이 강하기 때문에 은밀하게 계속 자행되고 있는 실정이다.

개인정보는 인터넷 경제 발전에 중요한 역할을 수행하게 될 것이며, 이 금액은 G-20국가에서 2016년까지 4.2조 달러가 될 것이라고 예상했다. 정석균(2012)[16]은 기업이 소비자와 온라인 거래를 통해 정상적인 수입을 얻는 것 외에 고객의 개인정보를 당초 수집목적 외로 활용하거나 제3자에게 판매하여 불법적인 수입을 얻을 수 있다고 하였다. 기업의 정상적인 수입은 기업의 규모와 평판도 등 기업유형에 따라 차이가 있으며 좋은 기업이어서 그 값이 클수록 정상적인 수입규모는 커진다고 하였다. 기업의 의사결정은 이윤에 기초하여 이루어지며, 이윤이 더 크면 개인정보를 수접하여 활용하며 온라인 비즈니스를 할 것이라고 하였다. 즉 기업은 개인정보에 기초한 수입이 클수록, 그리고 개인정보 수집비용이 적을수록 보다 많은 양의 개인정보를 수집하여 활용하며, 정보통신기술의 발달로 개인정보의 활용가치가 커지고 개인정보 수집비용은 점차 감소한다는 점에서 앞으로 기업의 개인정보 수집 및 활용규모는 더욱 확대될 것으로 예상했다.

(그림 5-1) 개인정보가치의 측정



출처) OECD, 2013

15) 파이낸셜타임스, 자체조사, 2013.6
16) 정석균, 인터넷 개인정보보호의 시장자체해결가능성에 대한 연구, 2012

OECD(2013)[17]에서는 개인정보의 사회경제적 가치를 측정하기 위한 방법론 연구에서 개인정보의 가치를 측정하기 위해 시장 관점과 개인 관점에서 6가지 방법론을 제시하고 각각의 장단점을 정리하였다. 그 중 개인정보 건수 대비 경제지표는 회사의 시가총액, 수익, 순이익 등의 경제지표를 회사가 사용하는 개인정보의 총합으로 나눈 값으로, 개인정보를 통해 창출된 실질적 부가가치가 반영되어 있다는 장점이 있지만 경제지표에 영향을 미치는 요소가 많기 때문에 부정확하며, 대용량 데이터의 경우 시너지 효과로 인해 개인정보 가격이 과대평가될 수 있다는 단점이 있다. 데이터의 시장가격은 데이터 브로커가 시장에 제공하는 개인정보 건수 당 가격을 말하는 것으로 수요와 공급에 따른 시장가치가 반영되어 있다는 장점이 있지만 개인정보 자체의 가치 이외에 데이터 검색·처리 비용이 포함되어 있으며 데이터가 판매되는 맥락에 따라 수요와 가격이 변동될 수 있다는 단점이 있다.

개인정보가 자신의 기업의 영업활동에 긍정적인 영향을 미치는 경우 이에 대한 평가는 높을 것이며, 그렇지 않다면 평가는 낮아질 수 있다. 예를 들어 개인정보를 보유하고 있는 기업은 개인정보를 구입한 기업이 그 정보를 이용하여 판매한 기업의 영업활동을 저해할 수 있는 개인정보를 판매하지 않을 것이다. 그러나 그렇지 않은 경우 개인정보를 보유하고 있는 기업은 이를 제공할 유인이 발생한다. 물론 이것은 개인정보가 비경합성을 보유하고 있어서 자신이 수집한 개인정보를 이용한 이후 다른 사람이 이를 다시 이용할 수 있는 특성에서 발생한다. 개인정보를 이용하려는 기업들은 개인정보의 종류와 유형에 따라 그 가치에 평가가 다양할 수 있으며, 또한 개인정보를 이용하려는 사업목적에 따라 다양한 평가를 할 수 있다.

17) OECD, Exploring the Economics of Personal Data - A SURVEY OF METHODOLOGIES FOR MEASURING MONETARY VALUE, 2013

제2절 기업의 개인정보 유출로 인한 경제적 피해비용 평가

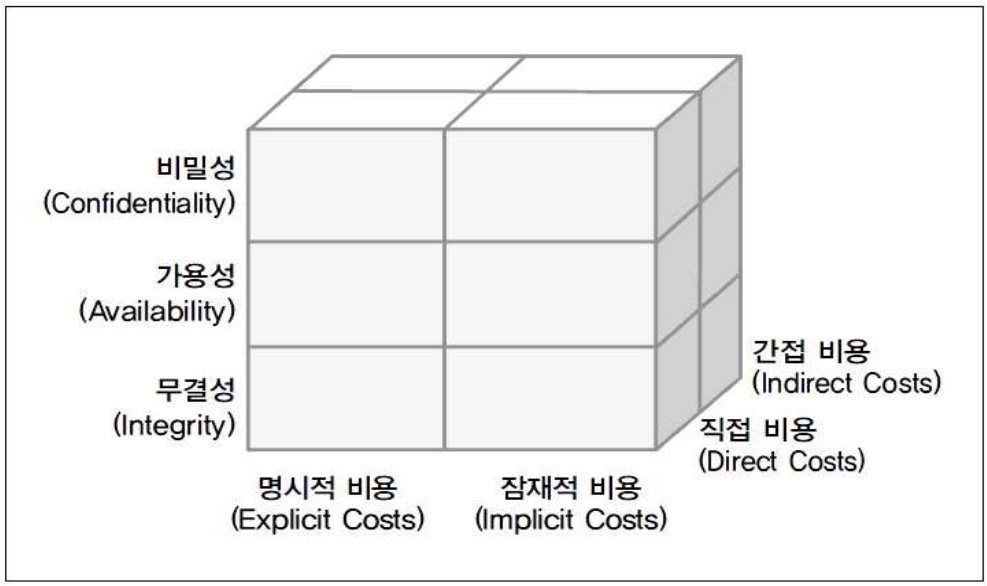
1. 개인정보 유출로 인한 피해요소의 구성

(1) 평가요소의 개념적 정의 및 구분

기업의 개인정보 유출로 인한 피해유형과 발생된 피해요소에 대한 개념적인 정의 및 구분은 Gordon & Loeb(2006)의 연구를 활용하고자 한다.

Gordon & Loeb(2006)은 (그림 5-2)와 같이 피해유형인 비밀성, 가용성, 무결성의 상실에 따른 피해 발생 비용을 직접비용(Direct Costs)과 간접비용(Indirect Costs), 명시적 비용(Explicit Costs)과 잠재적 비용(Implicit Costs)으로 구분하여 정의하였다.

(그림 5-2) 정보보호 침해사고 피해비용 구조



출처) Gordon & Loeb(2006)

여기서 비밀성[18](기밀성), 무결성[19], 가용성[20]은 정보보안의 3요소로 불린다.

18) 비밀성은 정보의 소유자가 원하는 대로 비밀이 유지되어야 하는 원칙을 말하는 것이며, 허가되지 않은 유저나 노드에 데이터나 전송되거나 접근이 허가되는 것을 방지하는 것이다. 이러한 비밀성을 유지하기 위해서 반드시 비인가자가 아닌 인가자에게만 접근이

비밀성은 정보가 비인가된 개인, 프로그램 및 프로세스에 공개되지 않음을 보장하는 것이며, 무결성은 정보가 변경되지 않음을 보장하는 것으로 정보의 정확성 및 완전성을 보호하는 것이다. 또한 가용성은 인가된 사용자가 요구하는 정보, 시스템 및 자원의 접근이 적시에 제공되는 것을 의미한다.

직접비용은 특정 침해사고에 명확하게 연계(link)될 수 있는 비용**을** 의미하는 것으로 해당사고에 의해 발생하는 인력손실, H/W 손실, S/W 손실 등을 의미한다. 반면에 간접비용은 다른 사고에 의해서도 영향을 받을 수 있는 피해비용을 의미한다. 예를 들어 침해사고 예방을 위해 투입된 보안장비 구입비용은 특정사고만을 위한 비용이 아니라 다양한 사고의 예방을 위해 투자한 비용이므로 특정 침해사고에 의해 손실이 되었다면 간접비용의 손실이 발생한 것이다.

한편 명시적 비용은 특정 침해사고를 예방하고, 탐지하고, 복구하기 위해서 침해사고 기간 동안 발생한 명백한 비용을 의미한다. 예를 들어 복구 인력 비용, 매출 손실 비용 등이 해당한다. 반면에 잠재적 비용은 침해사고에 의한 기업의 이미지 손실, 잠재적 법적 책임비용 등 기회손실과 연관된 비용으로 Gordon & Loeb은 이를 계량화하기가 쉽지 않다고 하였다.

본 보고서에서는 비밀성과 완결성이 상실된 개인정보 유출사고 피해액을 산출하기 위해 Gordon & Loeb의 개념적인 정의를 활용하였으며 이를 본 상황에 맞게 수정하는 과정을 거쳤다. 그 결과 개인정보 유출사고로 인해 발생할 수 있는 모든 가시적인 비용과 비가시적인 비용을 명시적・잠재적・간접・직접의 기준에 따라 분류했으며 그 결과는 아래의 표와 같다.

허용되어야 한다. 비밀성을 유지하기 위해서 취하는 방법으로는 접근통제와 암호화가 있다.

19) 무결성은 정보의 전송과정에서 비인가자에 의한 정보의 변경, 삭제, 생성 등이 원천적으로 봉쇄되어 전송되는 데이터의 정확성과 안정성이 보장되어야 하는 원칙을 말한다. 무결성을 유지하기 위해서는 물리적인 통제를 가하거나 접근자체를 통제하는 방법이 있다.

20) 가용성은 인가자에게만 정보에 대한 접근이 허용되도록 하는 것을 말한다. 가용성을 확립하기 위한 방법으로는 데이터의 백업, 중복성의 유지, 물리적 위협요소로부터의 보호를 들 수 있다.

[표 5-1] 개인정보 유출사고 피해액 산출 프레임

간접 비용 (Indirect Costs)		
직접 비용 (Direct Costs)		
	명시적 비용(Explicit Costs)	**잠재적 비용(Implicit Costs)**

출처) 유진호 외(2008), "인터넷 침해사고에 의한 피해손실 측정"을 참고하여 저자작성

개인정보 유출에 관한 정확한 피해액 산출은 쉬운 일이 아니다. 특히나 측정하기 어려운 잠재적 비용이 전체에서 큰 비중을 차지하는 개인정보 유출과 같은 문제는 더더욱 산출에 어려움을 겪는다. 실제로 비슷한 시기에 이뤄진 미국의 경우를 보면 CSI/FBI에서 조사한 2005년 정보유출 사고 1회 당 평균 피해액은 $167,000이다. 하지만 이듬해 정보보안 관련 연구 기관인 포네몬에서 조사한 바로는 그 피해액이 $4,800,000에 이르는 것으로 조사되었으며, 같은 시기의 미 법무부의 조사에는 $1,500,000이라는 액수가 집계되었다.

이러한 결과가 일어난 이유는 각 기관들이 결과 산출 시 서로 다른 요소들을 뽑아냈거나 아니면 각 요소에 대한 구체적인 추정 과정이 달랐기 때문이라고 추측해 볼 수 있다. 따라서 실제와의 오차를 줄이고 정교한 산출액을 도출하기 위해서는 가장 먼저 서로 겹치지 않으면서도 실제 요소들의 전 범위를 커버할 수 있는 예상 목록 도출이 이뤄져야 한다.

(2) 산출요소 선정 및 적용

위에서 언급한 예상 목록 도출을 위해 본 보고서에서는 포네몬 연구소, 포레스터 연구소, 테크-404, 인포메이션 쉴드(Information Shield Inc.) 등의 보안 전문 연구소와 기업에서 발행한 보고서를 수집·정리함으로써 예상 요소들을 도출하였다. 그 중 본 연구의 목적과 가장 잘 맞는다고 판단한 인포메이션 쉴드(Information Shield Inc.)사의 예상 요소를 기준점으로 사용하게 되었다. 이를

위에서 도출한 '개인정보 유출사고 피해액 산출 모형' 프레임 워크에 적용함으로써 보다 체계적이고 정교한 산출이 가능해졌다.

인포메이션 쉴드 사의 개인정보 피해액 산출을 위한 예상요소는 다음과 같다.

[표 5-2] Information shield Inc.의 피해액 산출 요소

1. 인건비 (단위 : 시간)
유출사고가 일어났는지 결정을 내리는데 드는 사전 비용
상황 처리를 위해 전문가와 상의하고 내부회의를 거치는 비용
얼마나 많은 고객의 정보가 빠져나갔는지 파악하는 비용
정보가 빠져나간 고객들과 전화 연락을 취하는데 드는 비용
이메일과 공지를 통해 고객들과 연락을 취하는데 드는 비용
추가적인 인건비
2. 추가적 사후 비용
회사의 이미지를 회복하기 위해 고객들에게 전화하는 비용
고객과의 관계회복을 위한 비용
사고 관련 문의전화를 받는데 드는 비용
범죄로 인한 유출인지 조사하고 수사를 의뢰하는데 드는 비용
시스템을 교체하는데 드는 비용
3. 고객 신뢰도 측정
고객 신뢰도 측정 비용
4. 잠재적 법적 비용
과태료 및 벌금
소송비용
배상금
5. 수익 감소적 측면
고객 감소로 인한 수익 하락

출처) Information Shield Inc. 홈페이지, (http://www.informationshield.com/privacybreachcalc.html)

본 보고서에서는 Information Shield Inc.의 예상 요소를 앞서 변형한 Gordon & Loeb 프레임워크에 적용하여 다음과 같은 프레임워크를 제안한다.

[표 5-3] 개인정보 유출사고 피해액 산출 범위

<table>
<tr><td rowspan="2">간접비용
(Indirect Costs)</td><td>고객 신뢰도 측정비용
시스템 보완 & 교체비용</td><td colspan="2" rowspan="2">기업 이미지 손실</td></tr>
<tr><td>산업 파급효과</td></tr>
<tr><td>직접비용
(Direct Costs)</td><td>IR 대응비용(브랜드 이미지 방어)
사고 대응 인건비
고객 감소로 인한 매출 감소</td><td>법적비용
(소송, 보상금)
벌금</td><td>보상받지 못한
개인의
정보가치</td></tr>
<tr><td></td><td>명시적 비용
(Explicit Costs)</td><td colspan="2">잠재적 비용
(Implicit Costs)</td></tr>
</table>

출처) Gordon&Loeb(2006)과 인포메이션 쉴드사의 산출요소를 참고하여 저자작성

* 법적비용 + 벌금 + 보상받지 못한 개인의 정보가치 = 유출된 정보의 가치

본 연구에서는 직접 산출이 가능한 직접 비용을 중심으로 개인정보 유출 피해액을 산출해가고자 한다. 또한 명시적 직접비용만을 다룬 기존의 연구에서 한 단계 더 나아가 산출이 어려운 간접비용과 잠재적 비용을 고려하였다. 또한 개인정보 유출사고의 영향이 클 것으로 예상되는 관련 산업 파급효과와 기업의 법적 비용·벌금 및 보상 받지 못한 고객의 손실까지 산출의 범위를 확대함으로써 보다 정확한 산출액을 도출하려 한다.

이때 명시적 간접비용인 고객의 신뢰도 측정비용과 시스템 보완 & 교체비용은 현재보다는 미래 대응적 가치이기에 고려 대상에서 제외했으며, 산업 파급효과는 그 영향이 크고 비교적 즉각적인 반응이 나타날 것으로 예상되는 1차 파급효과만을 다루기로 한다. 또한 기업의 이미지 손실 역시 측정이 어렵고 명시적 직접비용에서 매출감소에 일부분이 포함되기에 역시 산출 대상에서 제외했다.

추가적으로 용어에 대한 설명을 하면 명시적 직접비용은 침해사고에만 명확하

게 연계될 수 있는 비용 중 침해사고 기간 동안 발생한 명백한 비용을 말한다. 여기에 해당하는 요소로는 사고 대응 인건비와 IR 대응비용 그리고 고객 감소로 인한 매출 감소가 있다. 또한 침해 사고와는 명확하게 연결되지만 침해 사고 기간을 넘어 발생할 수 있는 암묵적 비용인 직접적 잠재비용으로는 법적비용과 벌금, 보상받지 못한 개인의 정보가치 등이 있다.

단일 침해사고 뿐만 아니라 다른 사고에 의해서도 영향을 받을 수 있는 간접비용 역시 침해사고 기간 동안 명백하게 발생하는 명시적 비용과 그렇지 않은 잠재적 비용으로 분류할 수 있다. 이 경우 각각 명시적 간접비용과 잠재적 간접비용이라 부르는데, 명시적 간접비용은 산업파급효과, 고객 신뢰도 측정비용, 시스템 보완&교체 비용 등이 있으며, 잠재적 간접비용은 기업 이미지 손실 등이 포함된다.

(3) 선행연구와의 비교

개인정보 유출에 따른 피해액을 기업과 개인의 손실로 구분하면 아래의 표와 같이 구성된다. 실제 정보가 유출되면 기업은 대응 인건비, IR(Investor relations) 대응 비용[21], 수익 손실, 법적 보상금 등의 피해를 입으며, 동시에 개인은 유출된 개인정보가 갖는 가치만큼의 손해를 보게 된다. 다만 기업이 개인에게 보상한 법적 보상금은 유출된 개인정보가 갖는 가치의 일부분이기에 산정 시 중복을 피하고자 기업의 손실로 산정하며, 개인의 순손실은 유출된 개인정보의 가치 중 기업이 보상한 법적 보상금을 제외한 그 나머지를 산정한다. 이렇게 산정한 기업 손실과 개인 손실은 관련 산업 파급효과와 더해져 개인정보 유출에 따른 전체 피해액으로 계산한다.

21) IR(Investor relations) 대응비용 : 기업이 자본시장에서 정당한 평가를 얻기 위하여 실시하는 홍보활동

[표 5-4] 개인정보 침해사고 피해액 다이어그램

<기업 손실>	<개인 손실>
대응 인건비 IR 대응 비용 수익 손실 (매출 감소) (실제 보상한) 법적 보상금 관련 산업 파급효과	보상받지 못한 개인정보 가치

출처) Ponemon(2010)과 JNSA(2010)을 참고하여 저자작성

위의 다이어그램에서 제안한 피해요소를 구성하기 위해 본 보고서에서는 선행연구인 미국의 포네몬 보고서와 일본의 JNSA를 참고했는데 그 내용은 다음과 같다.

미국의 포네몬 보고서와 일본의 JNSA는 정보 유출에 따른 비용을 각각 기업의 입장과 정보 가치에 기반한 관점에서 산출했다. 하지만 포괄적인 사회적 파급효과를 측정하기 위해서는 정보 유출로 인해 기업과 개인이 겪는 양쪽 모두의 피해액을 동시에 고려하는 것이 필수적이다.

실제 포네몬의 연구는 기업의 손실분을 대상으로 하고 있으며, JNSA가 측정한 정보 가치는 유출로 인해 개인이 받는 피해라고 볼 수 있다. 따라서 기업과 개인 모두의 피해를 동시에 측정할 때 두 사례를 참고하고 적절히 통합하는 방법을 사용하였다. 이를 위에서 제시한 손실액 다이어그램과 요소별로 비교해서 정리하면 아래와 같다.

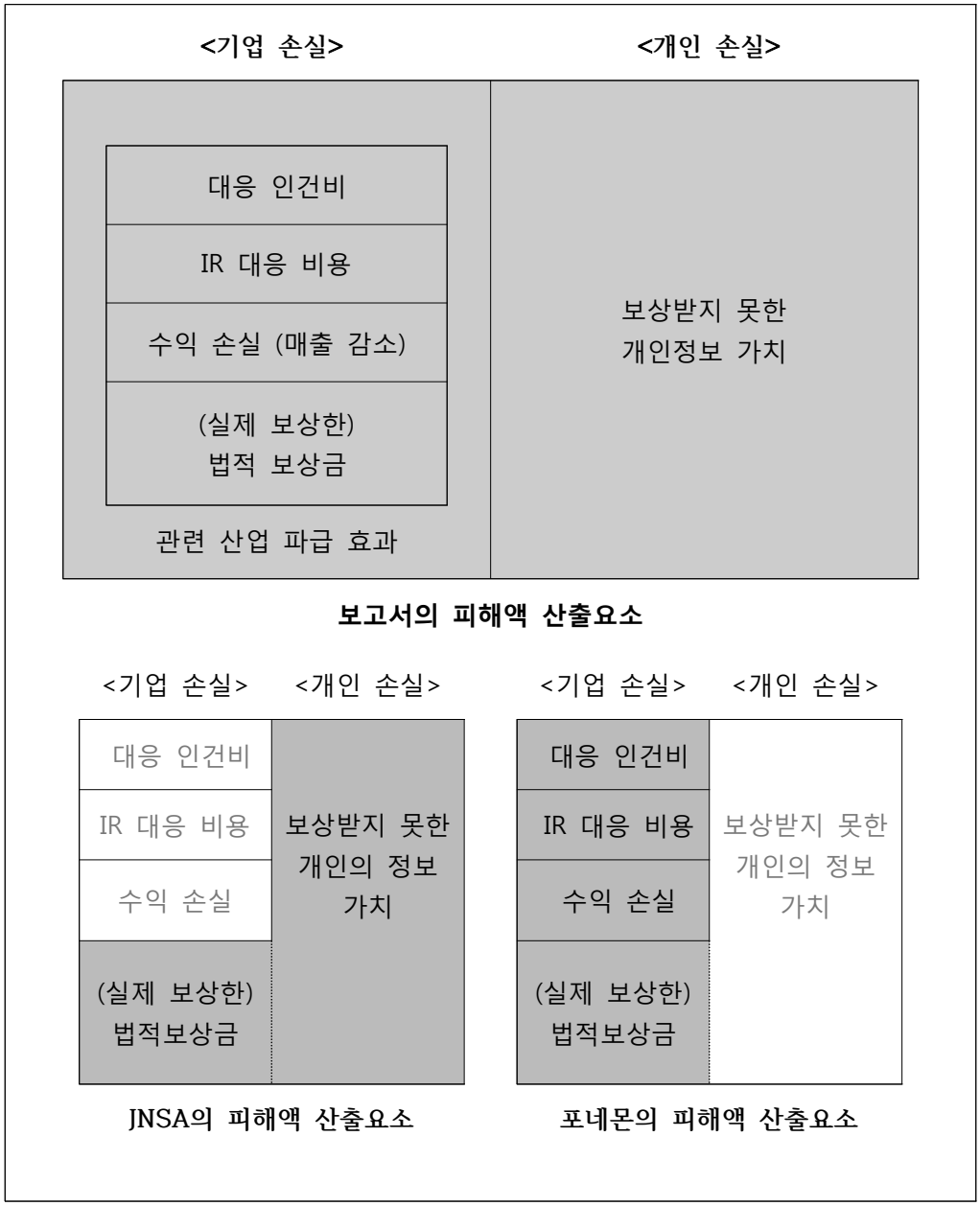
[표 5-5] 측정요소와 선행연구와의 비교

Ponemon = 대응 인건비 + IR 대응비용 + 수익 손실 + 실제 보상한 정보가치 (즉, 기업의 입장에서 <기업 손실> 부분을 측정)
JNSA = 유출된 정보의 가치 = 실제 보상한 개인의 정보 가치 + 보상 받지 못한 개인의 정보가치 (즉, <개인손실> + <기업손실> 중 실제 보상한 정보가치 부분)

출처) Ponemon(2010)과 JNSA(2010)을 참고하여 저자작성

결과적으로 본 보고서에서 측정하는 피해액은 포네몬 보고서에서 산출한 기업 중심의 피해액과 JNSA 보고서에서 산출한 유출된 정보 자체의 가치를 모두 고려한 후 이러한 피해가 관련 산업에 미치는 파급 효과까지 측정하였다고 볼 수 있다. 기존 연구인 JNSA와 포네몬에서 제안한 피해측정요소와 본 보고서의 피해측정요소를 비교하면 아래의 [표]와 같다.

[표 5-6] 측정요소와 선행연구와의 비교 다이어그램



자료) Ponemon(2010)과 JNSA(2010)을 참고하여 저자작성

피해액 산출에 있어 JNSA의 피해액 산출요소는 보상받지 못한 개인의 정보 가치와 기업이 실제 보상한 법적 보상금으로 이는 정보 자체 가치의 손실에 초점을 두고 있다. 개인정보 유출로 인해 보상받지 못한 개인의 손실과 법적 보상금 지불로 인한 기업의 손실 두 측면에서의 피해를 포괄하여 산출한다. 반면 포네몬(Ponemon) 연구소의 피해액 산출요소는 대응인건비, IR 대응비용, 수익 손실, 기업이 실제 보상한 법적 보상금으로 구성되어 있으며 이는 기업 손실에 중점을 두고 있다.

(4) 시장을 통한 수익평가(CVM)와의 연계방안

실제 개인정보 유출 사건이 벌어진 후 기업이 피해자들에게 보상한 사례가 몇 건 없는데다, 그 액수도 그리 크지 않다. 또한 이 조차도 소송에 참여한 극소수의 피해자에게만 지급되기 때문에 위 모델에서 제시한 '(실제 보상한) 법적 보상금'은 개인정보 그 자체의 가치에 비하면 무시해도 좋을 만큼 작은 부분만을 차지하고 있다. 따라서 현재로선 보상받지 못한 개인정보 가치를 개인정보의 가치 그 자체로 봐도 무방하다.

따라서 '실제 보상한 법적 보상금'과 '보상받지 못한 개인정보 가치'를 하나로 묶어 사회재화, 공공재 등 측면에서의 개인정보 가치 분석(CVM)적 측면의 분석으로 대체하는 방안을 제시하고자 한다. 선행연구에서도 설문과 개인정보분쟁조정위원회의 자료 그리고 실제 판례를 기준으로 보상받지 못한 개인정보 가치에 관한 가격을 측정했지만 그 과정에서 기업과 개인 간 인식의 격차가 발생하는 등의 문제점이 나타났으며, 이를 CVM적 기법을 통해 정확성을 높일 수 있길 기대한다.

[표 5-7] 시장을 통한 수익평가 모델 (CVM) 활용방안

<기업 손실>	<개인 손실>
대응 인건비	보상받지 못한 개인정보 가치 **(시장을 통한 수익평가 모델 : CVM 활용)**
IR 대응 비용	
매출감소로 인한 손실	
(실제 보상한) 법적 보상금	

결과적으로 이번 장에서는 개인손실 부분을 뺀 순수 기업 손실만을 논의 대상으로 한정지으며, 이를 다이어그램으로 표시하면 다음과 같다.

[표 5-8] 기업 측면에서의 피해액 산출 다이어그램

<기업 손실>	<개인 손실>
대응 인건비	보상받지 못한 개인정보 가치 **(시장을 통한 수익평가 모델 : CVM 활용)**
IR 대응 비용	
매출감소로 인한 손실	
(실제 보상한) 법적 보상금	

2. 기업의 개인정보 유출 사고 피해액 산출방법

(1) 선행연구

미국의 정보·보안 관련 단체인 포네몬 연구소는 2005년 직접비용과 간접비용 및 기회비용의 추정을 시도한 첫 연구를 시작으로 2013년 최신 보고서에서는 16

개 산업군의 199개 회사를 대상으로 설문 기법을 통해 심층 조사함으로써 유출에 따른 직·간접비용뿐만 아니라 고객의 신뢰도 하락과 전환에 이르는 총체적인 피해규모를 조사하고 있다.

최근 글로벌 보안기업인 시만텍의 후원을 받은 포네몬 연구소는 미국, 영국, 독일, 이탈리아, 프랑스, 일본, 인도, 브라질을 대상으로 보고서를 발표했으며 이 리포트를 통해 개인정보 유출 유형을 3가지로 세분화하고 각 대응단계에 따른 기업의 지출비용을 총 48가지의 케이스에 따라 분류했다.

본 연구에서는 포네몬의 2013년 보고서를 바탕으로 이에 활용된 방법론과 수치를 한국 실정에 맞게 변형하는 방식으로 대응인건비와 IR 대응비용, 매출감소로 인한 수익손실을 측정할 것이며, 여기에 법적비용과 관련 산업 파급효과를 따로 측정하여 추가하기로 한다.

(2) 산출방법

① 포네몬 리포트를 활용한 비용 전환

포네몬 보고서에서 다루는 국가 중 한국과 가장 비슷한 보안환경을 보이는 국가는 영국이다. 세계경제포럼의 'The Global Information Technology Report 2012'의 자료에는 인구에 따른 보안서버 개수(Security Internet Servers)가 명시되어 있는데 이는 한 국가에서 얼마나 보안에 대한 투자를 했는지를 간접적으로 보여주는 지표로 활용할 수 있다. 또한 동 보고서의 인터넷 사용률, 인구, 법제환경, 인프라 등의 점수를 종합적으로 고려했을 때 한국과 가장 비슷한 환경의 국가가 영국이라는 사실을 밝혀냈다.

[표 5-9] The Global Information Technology Report 2012 각종 지표

	Security Internet Servers (per mil pop)	Individuals using Internet (%)	SIS/IUI	인구	Political and regulatory environment	Infra and digital content
한국	**1140.4 (15)**	**83.7 (10)**	**13.6**	**4,900만**	**4.1**	**6.0**
미국	1446.3 (8)	74.0 (22)	19.5	3억 1,600만	5.0	6.8
일본	649.8 (20)	78.2 (17)	8.3	1억 2,700만	5.2	5.7
영국	**1396.3 (10)**	**85.0 (8)**	**16.4**	**6,300만**	**5.5**	**6.2**
독일	872.8 (17)	82.0 (12)	10.6	8,100만	5.3	6.1
호주	1760.8 (5)	76.0 (19)	23.1	2,200만	5.5	6.6

포네몬 보고서에서는 개인정보 유출 건당 비용을 16개 산업분야와 사고유형에 따라 총 48가지의 경우로 세분화했다. 이를 영국의 경우에 맞춰 정리하면 다음의 표와 같다.

[표 5-10] 영국의 산업분야 및 개인정보 유출유형별 건당 대응 비용

분야	Malcious Attack (악의적인 공격)	System Glitch (시스템 장애)	Human Factor (인적 요인)
헬스케어	$268.98	$209.01	$200.45
금융	$248.20	$192.87	$184.96
제약	$238.96	$185.69	$178.08
운송	$195.10	$151.60	$145.39
통신	$173.16	$134.56	$129.04
서비스	$154.69	$120.21	$115.28
기술	$148.92	$115.72	$110.98
연구	$144.30	$112.13	$107.54
에너지	$144.30	$112.13	$107.54
관광	$131.60	$102.26	$98.07

소비재	$130.45	$101.37	$97.21
교육	$128.14	$99.57	$95.49
미디어	$118.90	$92.40	$88.61
공업	$118.90	$92.40	$88.61
공공 서비스	$93.51	$72.66	$69.68
소매	$90.04	$69.97	$67.10

이렇게 산출된 비용을 대응인건비와 IR 대응비용 그리고 매출감소로 인한 기업손실로 분류해서 표로 정리하면 다음과 같다.

[표 5-11] 영국의 산업분야 및 개인정보 유출유형별 건당 대응인건비, IR 대응비용, 기업손실

분야	영국 - Malcious Attack			영국 - System Glitch			영국 - Human Factor		
	대응인건비	IR 대응비용	기업손실	대응인건비	IR 대응비용	기업손실	대응인건비	IR 대응비용	기업손실
헬스케어	$80.75	$66.95	$121.28	$62.75	$52.02	$94.24	$60.17	$49.89	$90.38
금융	$74.51	$61.78	$111.91	$57.90	$48.00	$86.96	$55.53	$46.04	$83.40
제약	$71.74	$59.48	$107.75	$55.74	$46.22	$83.73	$53.46	$44.32	$80.30
운송	$58.57	$48.56	$87.97	$45.51	$37.73	$68.36	$43.65	$36.19	$65.56
통신	$51.98	$43.10	$78.08	$40.39	$33.49	$60.67	$38.74	$32.12	$58.19
서비스	$46.44	$38.50	$69.75	$36.09	$29.92	$54.20	$34.61	$28.69	$51.98
기술	$44.71	$37.07	$67.15	$34.74	$28.80	$52.18	$33.32	$27.62	$50.04
연구	$43.32	$35.92	$65.07	$33.66	$27.91	$50.56	$32.28	$26.77	$48.49
에너지	$43.32	$35.92	$65.07	$33.66	$27.91	$50.56	$32.28	$26.77	$48.49
관광	$39.51	$32.76	$59.34	$30.70	$25.45	$46.11	$29.44	$24.41	$44.22
소비재	$39.16	$32.47	$58.82	$30.43	$25.23	$45.71	$29.18	$24.20	$43.83
교육	$38.47	$31.89	$57.78	$29.89	$24.78	$44.90	$28.67	$23.77	$43.06
미디어	$35.70	$29.60	$53.61	$27.74	$23.00	$41.66	$26.60	$22.06	$39.95
공업	$35.70	$29.60	$53.61	$27.74	$23.00	$41.66	$26.60	$22.06	$39.95
공공 서비스	$28.07	$23.27	$42.16	$21.81	$18.09	$32.76	$20.92	$17.34	$31.42
소매	$27.03	$22.41	$40.60	$21.01	$17.42	$31.55	$20.14	$16.70	$30.26

다음은 이를 다시 한국 실정에 맞게 변환하려 한다. 우선 대응인건비와 IR 대응비용의 경우 인력을 기준으로 운용하는 비용이기에 한국과 영국의 인건비 비율을 비교해서 적용하기로 한다. 한국과 영국의 임금차이는 OECD의 2012년 자료를 보면 각각 $29,053와 $50,366로써 이 경우 한국기업의 대응인건비와 IR 대응비용은 영국기업의 약 58%(=29053/50366) 정도로 추정할 수 있다.

매출감소로 인한 기업의 수익손실의 경우 한국과 영국의 소비자 1인당 소비력의 차이를 고려하고자 한다. 이를 위해 한국과 영국의 1인당 실질 국내총생산을 비교해 보면 이는 IMF의 2012년 자료 기준으로 각각 $23,680와 $38,891이다. 이 경우 한국기업의 매출 감소로 인한 수익손실의 경우 영국의 약 61% (=23680/38891) 정도로 추정할 수 있다. 이렇게 산출된 결과를 표로 정리하면 다음과 같다.

[표 5-12] 한국의 산업분야 및 개인정보 유출유형별 건당 대응인건비, IR 대응비용, 기업손실

분야	한국 - Malcious Attack			한국 - System Glitch			한국 - Human Factor		
	대응인건비	IR 대응비용	기업손실	대응인건비	IR 대응비용	기업손실	대응인건비	IR 대응비용	기업손실
헬스케어	$46.58	$38.62	$73.85	$36.19	$30.01	$57.38	$34.71	$28.78	$55.03
금융	$42.98	$35.64	$68.14	$33.40	$27.69	$52.95	$32.03	$26.56	$50.78
제약	$41.38	$34.31	$65.61	$32.16	$26.66	$50.98	$30.84	$25.57	$48.89
운송	$33.78	$28.01	$53.56	$26.25	$21.77	$41.62	$25.18	$20.87	$39.92
통신	$29.99	$24.86	$47.54	$23.30	$19.32	$36.94	$22.35	$18.53	$35.43
서비스	$26.79	$22.21	$42.47	$20.82	$17.26	$33.00	$19.96	$16.55	$31.65
기술	$25.79	$21.38	$40.88	$20.04	$16.61	$31.77	$19.22	$15.93	$30.47
연구	$24.99	$20.72	$39.62	$19.42	$16.10	$30.79	$18.62	$15.44	$29.52
에너지	$24.99	$20.72	$39.62	$19.42	$16.10	$30.79	$18.62	$15.44	$29.52
관광	$22.79	$18.89	$36.13	$17.71	$14.68	$28.08	$16.98	$14.08	$26.93
소비재	$22.59	$18.73	$35.81	$17.55	$14.55	$27.83	$16.83	$13.96	$26.69
교육	$22.19	$18.40	$35.18	$17.24	$14.30	$27.34	$16.54	$13.71	$26.22
미디어	$20.59	$17.07	$32.64	$16.00	$13.27	$25.37	$15.34	$12.72	$24.33
공업	$20.59	$17.07	$32.64	$16.00	$13.27	$25.37	$15.34	$12.72	$24.33
공공 서비스	$16.19	$13.43	$25.67	$12.58	$10.43	$19.95	$12.07	$10.00	$19.13
소매	$15.59	$12.93	$24.72	$12.12	$10.05	$19.21	$11.62	$9.63	$18.42

② 매출감소로 인한 손실

매출감소로 인한 손실을 측정하기 위해서 포네몬 보고서의 개인정보 유출사고로 인한 고객이탈비율을 이용하기로 한다. 포네몬 보고서의 조사결과 개인정보 유출사고로 인해 일어나는 고객들의 비정상적인 이탈의 경우 국가에 따라 약 2.4~4.4% 정도로 측정되고 있다. 또한 이 중 한국의 비교대상으로 정한 영국의 경우 약 3.1%의 이탈율을 보이고 있다.

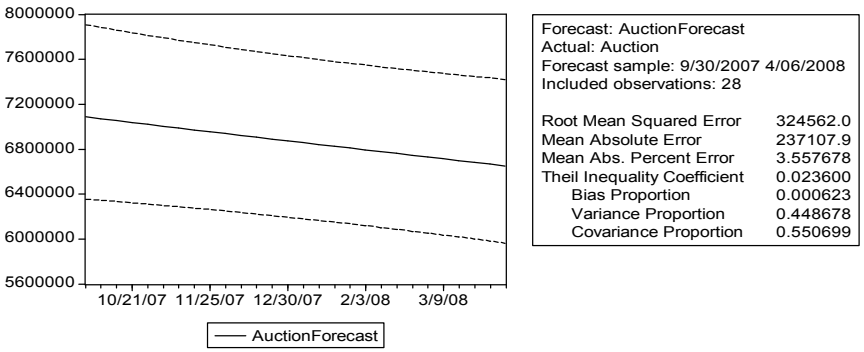
이 수치가 타당한지 검증하기 위해서 본 연구에서는 2008년 옥션의 대규모 개인정보 유출사고 때의 트래픽 분석결과를 활용하기로 한다.

2,000여 만 명의 개인정보가 유출된 옥션의 경우, 유출 시점을 기준으로 트래픽이 일시적으로 크게 증가했다 다시 줄어드는 것을 아래 (그림 5-3)의 트래픽 변화 그래프를 통해 확인할 수 있다. 이 때 트래픽이 일시적으로 급증한 것은 자신의 개인정보가 유출됐는지 확인하기 위해 방문하는 유저들 때문이며, 실질적인 트래픽 감소는 그 직후에 일어난다.

(그림 5-3) 옥션 개인정보 유출사고 이후 트래픽 변화 그래프

트래픽이 얼마나 감소했는지를 계산하기 위해서 통계 패키지를 활용하는 방법을 택했으며, 이를 위해 제일 먼저 해야 할 일은 유출시점 이전의 트래픽 추이를 분석해서 만약 유출이 일어나지 않는다면 어떻게 트래픽 그래프가 전개되었을지 예측하는 것이다.

(그림 5-6) 사고 시점 전 6개월 간의 트래픽 및 사고 시점 트래픽 예측



유출 사고 6개월 전부터 유출 시점까지의 장기적 추세를 분석해 보면 일단 전체적인 트래픽은 하향하는 상황이었으며, 이 경우 유출 시점에서의 예상 트래픽

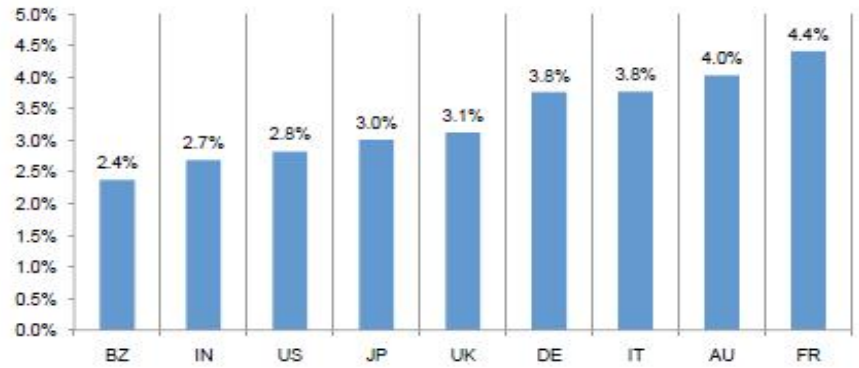
은 약 6,700,000 정도라는 사실을 알 수 있다. 이를 바탕으로 추정 이탈율을 계산해 보면 [표 5-11]과 같다.

[표 5-11] 사고시점 예상 및 실제 트래픽

	옥션 트래픽
예상 트래픽 (사고가 없다고 가정 시)	6,700,000
첫 회복시점 트래픽 (사고 후 단기적으로 완전 회복 2008년 5월 3주)	6,488,694
추정 이탈율	약 3.15%

결과적으로 옥션의 경우 개인정보 유출 이후 약 3.15%의 회원이 단기적으로 이탈한 것을 알 수 있다. 또한 여기서 개인정보 유출 시점 전후의 트래픽 변화를 분석한 결과 추정된 고객의 이탈율이 약 3.15%인 점을 미루어볼 때 포네몬 보고서의 영국 이탈율 3.1%는 한국 실정에 적용하기에 타당하다고 볼 수 있다.

(그림 5-5) 포네몬 보고서의 유출사고 이후 고객이탈비율



이 결과를 바탕으로 개인정보 유출로 인한 기업의 매출감소는 개인정보가 유출된 고객 중 약 3.1%가 이탈한다는 가정 하에 산출하고자 한다. 이를 정리해보면 매출감소로 인한 기업의 손해는 '기업의 연매출액 X 전체 고객 중 개인정보가 유출된 고객의 비율 X 한국과 가장 비슷한 환경을 가진 영국의 고객이탈율 3.1%'를 적용해서 산출할 수 있다.

② (실제 보상한) 법적 보상금

실제 보상한 법적 보상금의 경우 국내에서 판례가 극히 드물다. 2005년부터 연간 수 천만 건에 이르는 개인정보 유출사고가 일어났음에도 불구하고 실제 보상판결이 난 경우는 단 3건에 불과하며, 그 대상도 수백에서 수천 명의 소송자들에 한정되어 있다.

물론 그렇다고 해서 법적 보상금이 의미가 없다는 것은 아니다. 다만 국내법의 경우 미국과는 달리 조치를 취했더라도 유출된 정보의 책임을 기업이 모두 지는데다 징벌적 배상까지 떠안아야 하는 상황이기에 대규모 사건의 경우 기업의 지속가능성이 무너질 수 있을 정도의 배상액이 산정된다. 이러한 이유에서 현실적으로 제대로 된 보상판결이 나지 못하고 있는 상황이기에 피해액 측정 시 이를 고려하는 것이 타당하다.

이러한 상황을 고려해 볼 때 기업의 법적 보상적 측면의 손실을 측정하기 모호하며, 실제 일어난 보상의 경우 다른 요소에 비해 무시해도 좋을 정도의 극히 적은 금액이기에 이를 보상받지 못한 개인의 정보가치와 함께 묶어 정보 자체의 가치로 보고, 이를 다음 장에서 다룰 “시장을 통한 수익평가 모델(CVM 모델)”의 영역에 포함시키고자 한다.

따라서 (실제 보상한) 법적 보상금은 개인정보 유출로 인한 기업의 손실을 측정하는 이 장에서는 다루지 않기로 한다.

[표 5-12] 국내 판결사례

사건	일시	보상금 판결액
네이트 / 싸이월드 (아이디, 패스워드, 개인정보)	2013년 2월	20 만원
국민은행(개인정보)	2006년 3월	20 만원
NC 소프트 (아이디와 패스워드)	2005년 5월	10 만원

3. 최근 개인정보 유출 사고 사례에 대한 피해액 산출

최근 개인정보유출 사고 사례에 대한 피해액을 산출하기 위해 언론을 통해 알려진 2011년과 2012년의 개인정보 유출사고를 정리해 보면 [표 5-12]와 같다. 하지만 이를 단순히 위에서 수립한 계산방식에 적용하기에는 문제가 있다.

예를 들어 2011년 SK컴즈의 경우 약 3,500만 명의 개인정보 유출이 일어났다. 이는 국내 인터넷 사용인구와 맞먹는 비정상적인 규모다. 또한 넥슨, KT, EBS 등의 사건도 수백만 건에 이르는 대규모 유출이 이루어졌다. 이 정도 규모의 유출사고는 해외에서도 드물며, 선행연구로 참고한 포네몬 보고서의 경우 10만 건 이하의 사건만을 대상으로 했기 때문에 수백, 수천 만 건의 유출이 빈번하게 일어나는 국내의 경우 피해액 산출시 반드시 항목별 대량사건에 대한 비용적 고려가 필요하다.

[표 5-13] 최근 개인정보 유출사고 사례

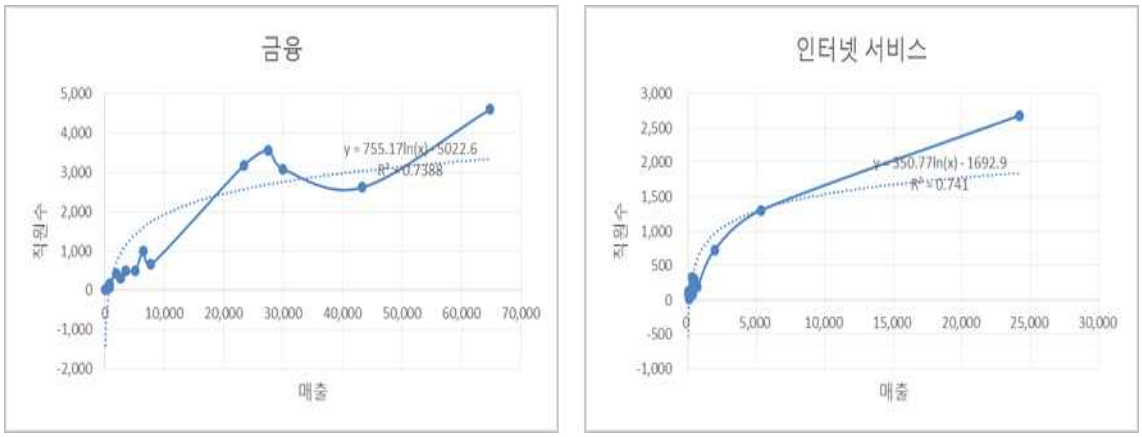
사건	유출건수	유출내용	분야	유형
2011년				
현대캐피탈	175만	기본	금융	MA
한화손해보험	16만	기본	금융	MA
리딩투자증권	2.6만	기본	금융	MA
sk컴즈(네이트, 싸이월드)	3500만	기본	서비스	MA
엡손	35만	기본	기술	MA
넥슨	1320만	기본	서비스	MA
2012년				
KT	873만	기본	통신	MA
EBS	420만	기본	교육	MA

우선 인건비와 IR 비용의 경우 대응하는 노동력에 비례하는 비용이다. 하지만 통상적으로 회사의 구조를 보면 처리하는 고객이 급격히 늘어난다고 해서 그에

비례해서 인력이 늘어나지는 않는다. 시스템이 갖는 효율 때문에 한 명의 인력이 처리할 수 있는 업무량이 수확체증하기 때문이다.

이를 측정하기 위해 각 분야별 대표 15개 기업을 대상으로 동종 업계에서 매출과 실고객수가 비례한다고 가정하고 매출 대비 직원수의 비율을 비교했다. 그 결과 매출이 커질수록 매출당(실고객수당) 필요인력이 로그형태로 감소한다는 사실 확인했으며, 이를 바탕으로 비정상적으로 큰 유출의 경우 인력중심의 인건비와 IR 대응비용을 로그비율로 다운사이징 해야 한다는 결론을 내렸다.

(그림 5-6) 금융과 인터넷 서비스 분야 매출별 직원수



고객이탈로 인한 매출손실의 경우는 처음부터 건당 비용이 아닌 매출액과 고객이탈율을 기준으로 산정했기 때문에 추가적인 조정을 하지 않는다.

다운사이징을 고려해서 2011년과 2012년 언론에 공표된 사건들을 대상으로 기업 측면에서의 피해액을 계산하면 다음과 같다. SK컴즈, 넥슨 등의 거대규모의 개인정보 유출이 일어난 2011년의 경우 약 2,400억 원, KT와 EBS의 개인정보 유출이 일어난 2012년의 경우 약 1,780억 원 정도의 피해가 일어난 것으로 추정된다. 이는 언론을 통해 알려진 대형사고만을 대상으로 한 보수적인 추정 값이며 실제로 알려지지 않은 사건사고까지 고려하면 그 피해액은 더욱 커질 것으로 예상된다.

사건	유출건수	유출내용	분야	유형	대응인건비	IR 대응비용	기업손실	합계
2011년								
현대캐피탈	175만	기본	금융	MA	₩5,747,503,079	₩4,765,961,138	₩130,495,361,111	₩141,008,825,328
한화손해보험	16만	기본	금융	MA	₩5,446,916,861	₩4,516,708,165	₩15,500,000,000	₩25,463,625,027
리딩투자증권	2.6만	기본	금융	MA	₩1,196,812,823	₩992,294,176	₩4,030,000,000	₩6,219,106,999
sk컴즈(네이트, 싸이월드)	3500만	기본	서비스	MA	₩4,329,062,539	₩3,588,968,981	₩6,113,200,000	₩14,031,231,520
엡손	35만	기본	기술	MA	₩3,062,664,048	₩2,538,959,184	₩5,735,000,000	₩11,336,623,232
넥슨	1320만	기본	서비스	MA	₩4,086,082,961	₩3,387,529,024	₩34,317,000,000	₩41,790,611,985
합계					₩23,869,042,312	₩19,790,420,669	₩196,190,561,111	₩239,850,024,091
2012년								
KT	873만	기본	통신	MA	₩4,458,808,988	₩3,696,098,414	₩160,959,898,800	₩169,114,806,202
EBS	420만	기본	교육	MA	₩3,148,095,296	₩2,610,407,996	₩3,540,200,000	₩9,298,703,292
합계					₩7,606,904,283	₩6,306,506,410	₩164,500,098,800	₩178,413,509,494

실제 개인정보 유출사고의 경우 보안 관련 인프라와 인력이 갖춰져 있는 대기업을 제외하고 나면 대부분 유출이 일어났는지도 모를 만큼 그 대비에 취약한 것으로 알려져 있다. 또한 법적 책임을 떠안지 않기 위해 취해야 하는 조치들을 미리 시행하지 못하는 중소규모 이하의 기업들의 경우 유출사고가 일어났음을 인지했더라도 이를 은폐하는 것이 일반적이다.

결국 언론에 공표되는 대기업뿐만 아니라 이러한 중소규모 기업의 유출사고까지 고려해야 보다 정확한 피해액을 추정할 수 있다. 이를 위해 본 연구에서는 개인정보 유출시 언론에 공표되는 대규모 기업을 100대 기업으로 가정하고, 이들이 국내 전체 매출액에서 차지하는 비율을 통해 중소규모 유출의 피해액을 추정하고자 한다.

대한상공회의소의 2011년 자료를 보면 2010년 기준 국내 100대 기업이 국내 매출에 있어 차지하는 비율이 약 64%라는 사실을 알 수 있다. 개인정보 유출로 인한 피해액이 기업의 규모와 고객수를 반영하는 매출액에 비례한다고 가정한다면 위에서 다룬 언론에 공표된 유출사건을 기준으로 추정한 피해액에 비해 약 56%의 추가적인 피해가 발생한다고 볼 수 있다. 또한 이는 보수적인 추정이며, 실제 보안에 취약한 중소규모 회사의 상황을 고려해 볼 때 그 피해액은 더 클

것으로 예상할 수 있다.

결과적으로 중소규모 개인정보 유출사건을 고려한 기업측면의 연간 피해액은 2011년과 2012년 각각 약 3,750억과 2,800억 원으로 추정할 수 있다.

[표 5-14] 중소규모 개인정보 유출사건을 고려한 피해액 (단위 : 원)

	대응인건비	IR 대응비용	매출 손실	최종 피해액
2011년	37,295,378,612	30,922,532,295	306,547,751,736	**374,765,664,654**
2012년	11,885,787,942	9,853,916,265	257,031,404,375	**278,771,110,594**

제3절 개인정보 보호의 편익 평가

1. 가상가치측정법의 활용[22)]

개인정보의 피해 사례를 보면, 개인의 경우 주민등록번호가 도용되거나 기타 정보의 훼손 및 침해 등으로 피해를 보는 경우를 들 수 있다. 개인에 대한 정보의 수준이 기업의 마케팅 전략에 적극 이용되고 있으며, 이를 수집·관리·이용하는 기업이 늘수록 개인정보의 유출 가능성은 커지고 있는 것이다. 기업의 경우는 개인정보를 수집, 저장 및 관리, 이용 및 제공, 파기의 과정에서 임의 혹은 관리소홀로 개인정보가 누출되는 경우를 들 수 있다. 즉, 수집단계에서는 개인의 동의없이 수집, 수집 시 고지 또는 명시의무 불이행, 과도한 개인정보 수집, 법정대리인의 동의없는 아동의 개인정보 수집 등을 들 수 있다. 저장 및 관리단계에서는 개인정보 취급자에 의한 훼손·침해·누설, 개인정보관리책임자 미지정, 기술적 조치 미비로 인한 개인정보 누출 등이 있으며, 이용 및 제공단계에서는 개인정보 처리 위탁시 고지의무 불이행, 영업의 양수 등의 통지의무 불이행, 동의 범위를 넘는 이용 또는 제3자 제공 등이 있다. 또한 파기단계에서는 수집 또는 제공받은 목적 달성 후 개인정보 미파기 등 다양한 형태로 발전하고 있다. 인터넷의 이용이 보편화되자 개인정보는 기본인적정보, 고유정보, 의료정보 등 여러 유형으로 다양화되었으며 이러한 정보의 유형에 따라 유출에 대한 피해도 증가하고 있는 추세이다.

이러한 현상은 개인정보의 유출이 피해 당사자의 개인적 차원이 아니라 사회적 문제로 발전하고 있는 것으로 이해할 수 있다. 따라서 개인정보 유출에 대한 경제 사회적 비용을 추정하여 그 피해정도를 감소시켜야할 시점에 와 있다. 이에 본 연구에서는 개인정보 침해 피해의 경제적 손실가치를 추정하고자 한다. 사용되는 방법론으로는 가상가치측정법(contingent valuation methods, 이하 CVM)을 이용하고자 한다.

본 장에서 진행하고자 하는 CVM 방법론은 비시장재화의 사회적 가치를 추정

22) 김여라, 이해춘, 유진호, 개인정보보호의 가치 산출, KISA 정보보호정책동향 2007의 내용을 인용하여 작성함.

하는데 이용하는 방법이다. 즉, 이 방법론을 이용하면, 개인정보 유출 피해라는 사회적 손실을 회피하기 위한 평균적 응답자의 지불의사금액(WTP: Willing to Pay)을 직접적으로 확인하여 사회적 손실을 추정할 수 있다는 이점이 있다.

CVM 방법론을 활용하여 손실비용을 추정한 사례로 김여라, 이해춘, 유진호(2007)는 가상가치접근법(CVM)을 활용하여 이용자가 개인정보 유출 방지를 위해 금전적으로 지불할 수 있는 금액(WTP: Willingness to Pay)을 추정하였다. 연구 결과 이용자는 자신의 개인정보 보호를 위해 부가적인 통신서비스 요금을 낼 경우, 1개월에 약 3,900원을 지불할 의사가 있는 것으로 나타났다. 유승훈 외(2003) 또한 CVM을 이용하여 스팸메일의 불편회피를 위한 지불의사액을 추정하였다. 이해춘 외(2008)는 개인정보 유출로 피해 가능성이 있는 응답자가 기업이 제시하는 손해배상을 수용하는 WTA(Willingness to Accept)를 화폐액으로 추정하여 개인정보 유출의 잠재적 손실액을 추정하였다. 일반적으로 WTA에 의한 추정치는 WTP에 비해 과추정의 우려가 있기 때문에, 전문가들은 WTP에 의한 방법을 더 권장하고 있다.

CVM 방법론은 이론적인 배경은 강점을 가지고 있으나, 실제 기업의 업무 환경을 직접적으로 반영하는 것 보다는 간접적인 측정방법으로서 한계점을 가진다. 특히 CVM 방법론은 이용자에게 제시하는 초기금액이나 가상시나리오에 의해 크게 영향을 받거나 조사자에 의한 편의(bias)가 발생할 수 있기 때문에 관련 분야 전문가들의 면밀한 검토가 없으면 조사 시점마다 크게 달라질 수 있다.

본 연구에서는 개인정보를 보호하기 위한 평균적 응답자의 지불의사액을 화폐액으로 추정하고자 한다. 이를 위한 이중양분선택형 CVM 방법론을 이용하였다. 이용자의 WTP를 유도하는 방법은 크게 개방형질문(open-ended questionnaire)과 폐쇄형질문(closed-ended questionnaire)으로 대별된다. 개방형질문법은 직접질문법이라고도 불리며, 응답자에게 아무런 보조자료의 제시없이 평가하고자 하는 재화에 대한 WTP를 직접 질문하는 방법으로 가장 간단하면서도 단순한 방법이다. 이 경우 응답자가 해당 재화에 대한 가치평가에 어려움을 느낄 경우 비합리적인 금액을 말하거나 또는 응답 자체를 회피하는 문제가 발생하는 단점을 가지고 있다. 폐쇄형질문법은 개방형질문법과 달리 응답자에게 다양한 형태의 정보제공 혹은 보조자료를 사용하여 WTP를 유도하는 방법으로, 경매법, 지불카

드법, 양분선택형법 등이 있다.

경매법은 조사자가 응답자에게 일정금액을 사전에 제시하고 “예/아니오”의 응답방식을 통해 최종적으로 조사자가 제시하는 금액이 응답자의 지불의사금액과 일치할 때까지 질문을 계속하는 방법으로, 조사원의 경험도에 따라 응답자의 진정한 지불의사금액을 정확히 유도해 낼 수 있는 장점이 있다. 그러나 경매방식은 조사자가 처음 제시하는 액수에 따라 응답자의 WTP가 영향을 받게 되는 시작점 편의(starting point bias)가 발생할 가능성이 크며, 응답자의 진정한 WTP를 유도해 내기까지 많은 시간이 걸린다는 단점이 있다.

지불카드법은 응답자의 지불의사금액 결정을 보다 정확하고 용이하게 하기 위한 제시액의 숫자가 적혀있는 카드를 응답자에게 제시한 후, 응답자의 지불의사금액에 해당하는 금액 하나를 선택하도록 하는 방법이다. 이 방법은 경매법에 비해 시작점 편의가 발생할 가능성이 낮고, 직접질문법에 비해 높은 응답률을 가져올 수 있으며, 양분선택법에 비해 상대적으로 적은 수의 표본을 필요로 하여 조사비용을 줄일 수 있는 장점이 있다. 그러나 지불카드법은 응답자에게 제시되는 지불카드상의 WTP 범위와 구간 수에 따라 응답자의 진정한 지불의사금액이 영향을 받게 되는 단점이 있으며, 제시된 금액 중 특정 금액에 응답이 집중되는 정박효과(anchoring effect)가 발생할 가능성이 있다.

양분선택형법은 해당 재화를 획득하기 위해 조사자가 사전적으로 설정한 금액만큼을 응답자가 기꺼이 지불할 용의가 있는가를 물어보면, 응답자가 “예/아니오”로 대답하는 방식이다. 이 방법은 대답이 용이하여 응답률이 높고 시작점 편의 발생가능성이 낮으며 비합리적인 지불의사금액이 발생할 가능성이 적은 반면, 다른 방법들에 비해 상대적으로 많은 수의 표본이 필요하며 WTP 추정의 어려움 등과 같은 단점을 가지고 있다.

따라서 다양한 CVM 중 응답자가 제시된 금액에 동의하는지의 여부만을 묻는 양분선택형 질문법이 흔히 사용된다. 양분선택형 질문법은 제시하는 금액의 회수에 따라 다시 이중양분선택형, 삼중양분선택형 등으로 구분한다. 즉 초기에 제시액을 한번 제시하고 이 제시액에 대한 응답자의 수락 여부를 근거로 WTP를 추정하면 양분선택형, 이 양분선택형 질문이 두 번 제시되면 이중양분선택형, 세 번 제시되면 삼중양분선택형이 된다.

실증분석에 자주 이용되는 방법론은 이중양분선택형(double bound dichotomous choice)이다. 이중양분선택형 질문 형식은 양분선택의 질문을 두 번 반복하는 것이다. 즉, 예정된 특정 제시액을 응답자에게 제시한 후 초기 제시액에 대해 지불의사가 있으면 두 번째는 더 높은 금액을 제시하고, 초기 제시액에 대해 지불의사가 없으면 다음에는 더 낮은 금액을 제시하여 지불의사를 조사하는 것이다. 이중양분선택형의 추정식 전개과정은 다음과 같다.

우선 응답자 i에게 제시한 초기 제시액을 B_i라 하자. 이 초기 제시액에 대해 응답자가 yes로 답할 경우 더 높게 제시한 금액을 B_i^u, no로 답할 경우 더 낮게 제시한 금액을 B_i^d라고 하자. 이 경우 각 제시액에 대한 수락여부에 따른 확률은 다음과 같이 정의될 수 있다.

$$\pi^{yy}(B_i, B_i^u) = Prob\{B_i^u \le WTP_i\} = 1 - F(B_i^u;\Theta)$$

$$\pi^{yn}(B_i, B_i^u) = Prob\{B_i \le WTP_i < B_i^u\} = F(B_i^u;\Theta) - F(B_i;\Theta)$$

$$\pi^{ny}(B_i, B_i^d) = Prob\{B_i^d \le WTP_i < B_i\} = F(B_i;\Theta) - F(B_i^d;\Theta)$$

$$\pi^{nn}(B_i, B_i^d) = Prob\{WTP_i < B_i^d\} = F(B_i^d;\Theta)$$

여기서 $\pi^{yy}(B_i, B_i^u)$: B_i에 yes, B_i^u에 yes로 응답한 경우의 확률

$\pi^{yn}(B_i, B_i^u)$: B_i에 yes, B_i^u에 no로 답한 경우의 확률

$\pi^{ny}(B_i, B_i^u)$: B_i에 no, B_i^d에 yes로 답한 경우의 확률

$\pi^{nn}(B_i, B_i^d)$: B_i와 B_i^d에 대해 모두 no로 답한 경우의 확률

WTP_i : 응답자 i의 잠재 지불의사금액

Θ : 파라메타 벡타

$F(\cdot)$: 로지스틱(혹은 정규) 누적확률 분포함수이다.

로지스틱 누적확률 분포함수 $F(B; \Theta)$는 다음과 같이 설정한다.

$$F(B) = F(-\alpha - x_i^{'}\beta - \beta_{bid}\ln B)$$

여기서 a는 상수항, x_i는 응답자의 특성을 나타내는 벡타, β는 x_i의 계수 파라메타 벡타이다. β_{bid}는 lnB의 계수 파라메타, B는 제시액으로 양의 값을 가진다. $F(B)$는 로지스틱 분포함수 혹은 정규분포함수를 가정한다.

파라메타를 조건부로 각 응답자의 응답확률을 로그변환하여 로그확률함수를 만들면, 특정 N명의 응답자에 의한 특정 응답관측치(1, ... ,N)가 관측될 확률은 다음과 같은 우도함수(likelihood function)로 나타낼 수 있다.

$$\ln L(\Theta) = \Sigma_{i=1}^{N} \{ d_i^{yy} \ln \pi^{yy}(B_i, B_i^u) + d_i^{yn} \ln \pi^{yn}(B_i, B_i^u)$$

$$+ d_i^{ny} \ln \pi^{ny}(B_i, B_i^d) + d_i^{nn} \ln \pi^{nn}(B_i, B_i^d) \}$$

N은 관측치 수이며, d_i^{yy}, d_i^{yn}, d_i^{ny}, d_i^{nn}는 더미변수로 그 값은 다음과 같다.

즉 d_i^{yy} :(yes, yes)=1, 이 외는 0, d_i^{yn} :(yes, no)=1, 이 외는 0,

d_i^{ny} :(no, yes)=1, 이 외는 0, d_i^{nn} : (no, no)=1, 이 외는 0 이다

파라메타 Θ의 최우추정량은 우도함수의 값을 극대화하는 Θ값으로서, 이는 로그우도함수 $\ln L(\Theta)$를 Θ에 대해 미분한 값을 '0'으로 놓고 그 최대값을 구하는 방식으로 다음과 같이 구할 수 있다.

$$\partial \ln L(\Theta) / \partial \Theta = 0$$

추정된 파라메타와 각 속성의 평균치로 구성된 벡타 x_i를 F(B)에 대입하면 평균적 응답자의 제시액 B에 대한 수락확률을 구할 수 있다. 이 확률함수는 로지스틱(혹은 노말)함수로 가정된다.

WTP의 평균값은 일반적으로 이 확률함수를 모든 WTP에 대해 적분하여 구할 수 있다. 그러나 이 함수가 '0'에 수렴할 경우 평균값이 발산할 가능성이 있으므로 절단 평균값을 취하는 경우도 있다.

평균적 응답자의 각 제시액 B에 대한 수락확률을 $S(WTP)$, 최대제시액에 대한 수락확률을 $S(WTP_{MAX})$라 하면, 수정된 절단 평균값은 다음과 같이 계산된다.

$$E(WTP) = \int_0^{WTP_{MAX}} \frac{S(WTP)}{1 - S(WTP_{MAX})} \, d\,WTP$$

*WTP*의 중앙값은 아래와 같이 계산될 수 있다.

$$Me(WTP) = \exp[\frac{-(\hat{\alpha} + \bar{x}'\hat{\beta})}{\hat{\beta}_{bid}}]$$

2. 조사 개요

본 조사는 개인정보 유출에 따른 사회적 비용을 수량적으로 추정하고, 이를 통하여 개인정보 유출에 따른 피해의 심각성, 개인정보 보호의 중요성 그리고 개인정보 보호를 위한 정책적 제언을 수립하기 위하여 기획되었다.

먼저 이용자들이 개인정보에 대한 이해를 쉽게 하도록 하기 위해 개인정보를 유형에 따라 분류하였다. 개인정보의 유형을 분류하기 위하여 본 연구에서는 다양한 의견수렴 절차를 거쳤다. 우선 전문가 의견수렴 절차와 개인정보보호위원회 담당자들과 여러 차례 협의를 진행하였다. 전문가 의견 수렴결과를 반영하여 정보통신망법 해설서 기준으로 아래와 같이 7가지의 개인정보의 유형을 분류하였다. 의견수렴을 거치면서 개인정보에 대한 분류에는 다양한 의견이 존재할 수 있다는 것을 확인할 수 있었다.

[표 5-15] 개인정보의 유형

유형 1)	**기본인적 정보**: 성명, 주소, 아이디 및 패스워드, 가족관계 등. 기본인적정보는 온·오프라인 회원가입 및 서비스 이용, 물품 수령 등에 주로 이용
유형 2)	**고유정보**: 주민등록번호, 여권번호, 운전면허 등록번호 등. 고유정보는 상거래·금융거래 등에서 본인 식별을 위한 확인 수단으로 사용
유형 3)	**의료건강정보**: 병력, 병원 진료기록, 신체장애 정도, 건강상태 등. 의료건강정보는 병원 진료 및 치료, 보험 가입 및 계약유지, 유전자 분석 등에 이용
유형 4)	**경제정보**: 소득, 신용카드 및 통장계좌번호, 물품 구매내역, 대출 또는 담보설정 등. 경제정보는 상거래 및 금융거래 등 경제활동 전반에서 이용
유형 5)	**사회관계정보**: 학력 및 학업성적, 친우관계, 동호회 활동 등 사회 활동 관련 정보. 사회관계정보는 취업 시 활용 및 사회 전반적으로 이용
유형 6)	**통신위치정보**: 휴대폰 번호, 이메일주소, GPS 위치정보 등. 통신위치정보는 신용카드 이용정보 등과 결합하여 기업의 마케팅, 기업 홍보 등에 사용

유형 7) **법적정보**: 전과 범죄기록, 납세기록, 과태료 부과내역 등. 법적 정보는 정부 행정 전반에 걸쳐 이용

개인정보 유형을 7가지로 분류한 후 설문조사 항목을 개발하였는데, 그 내용은 크게 6가지로 분류할 수 있다.

① 개인정보 및 개인정보 침해에 대한 인지도

② 개인정보 침해 경험

③ 개인정보보호에 대한 중요도

④ 개인정보 유형별 가치 및 유형별 순위

⑤ 개인정보 보호를 위한 지불의사액(Willingness To Pay)

⑥ 응답자의 특성(나이, 성별 등) 및 경제적 특성(소득 등)에 관한 질문

본 조사의 모집단은 최근 1개월 이내 1회 이상 유·무선 인터넷을 이용한 경험이 있는 만20세 이상 전국 남녀를 대상으로 컴퓨터를 이용한 웹 조사 방식으로 진행되었다. 표본구성은 『2012년 인터넷 이용실태 조사』의 성별(남녀), 연령별(20대, 30대, 40대, 50대, 60세 이상), 지역별(전국 16개 광역시도, 세종시는 대전에 포함하여 진행) 인터넷 이용률을 감안하여 비례할당으로 표집하였다. 이 과정을 거쳐 전체 800명의 유효 조사데이터를 수집하였으며, 조사 결과는 표집오차 ±3.4% 이내에서 95%의 신뢰수준을 가진 것으로 나타났다.

[표 5-16] 조사 설계

구 분	내 용
모 집 단	최근 1개월 이내 1회 이상 유선 또는 무선 인터넷을 이용한 경험이 있는 만 20세 이상 남녀
표본 크기	800명
표본 추출	2012년 인터넷 이용실태 조사의 인터넷 이용률 비중을 감안한 성·연령·지역별 유의할당
허용 오차	95% 신뢰수준에서 ±3.4%
조사 방법	컴퓨터를 이용한 웹 조사(CAWI)
조사 기간	2013. 9. 18 ~ 2013. 9. 24 (7일간)

(1) 개인정보의 중요도와 앞에서 분류한 개인정보의 유형과 연관된 질의를 통하여 응답자들이 개인정보 유형에 대한 인식을 가질 수 있도록 설계하였다. KISA(2007)의 경우 개인정보 유출에 따른 피해경험, 개인정보 보호 수준, 인식, 개인정보 유출의 심각성을 반복적으로 질의하였으나, 이 연구에서는 개인정보 유·노출에 대한 객관적 시각을 유지할 수 있도록 설문하였다.

(2) 개인정보 침해 예방에 대한 지불의사를 조사하기 위해 아래와 같이 가상적 상황을 설정하였다. 우선 기존 문헌과 달리 개인정보 유출에 대하여 최대한 객관성을 유지하려고 노력하였다. 즉 개인정보 유출에 대한 심각성을 부각하기보다는 객관적 데이터를 제공하도록 노력하였다. 동시에 기존 문헌과 유사하게 최대기간을 10년으로 설정하였으며, 비용지불은 매달 지불한다고 가정하였다. 또한 응답자의 소득이 한정되어 있으며, 만일 개인정보 침해를 방지하기 위하여 비용을 지불하는 경우 다른 소비가 동시에 감소할 수밖에 없다는 정보를 제공함으로써, 예산제약을 고려하지 않고 응답을 하는 오류를 제거하도록 노력하였다.

인터넷 등을 통해 개인정보가 침해되면 해당 당사자는 상당 수준의 정신적.물질적 손해를 볼 수 있습니다. 이러한 개인정보 침해의 심각성은 이제 개인의 문제가 아니라 사회적 문제로 이슈화되기 시작했습니다.

예를 들어 안전행정부에 따르면 개인정보침해신고센터로 접수된 개인정보 침해 신고 및 상담건수는 2012년 약 17만 건으로 이는 2011년과 비교하여 36%가 증가하였습니다.

위에서 언급한 개인정보 유출과 그 피해가 확대되어 피해 당사자 개인이 해결하기 보다는 사회적으로 이 문제를 해결해야 할 단계에 와 있습니다.

개인정보를 보호하고 관리하기 위해서는 투자가 필요하며 많은 사람들이 이에 동의하는 경우, 국민들이 부담하는 <개인정보보호를 위한 부가서비스 비용>으로 개인정보 유출 및 노출을 효과적으로 예방할 수 있다고 가정하십시오. 많은 사람들이 그 비용을 지불하려 하지 않는다면 개인정보의 보호 방안은 시행될 수 없습니다.

또한 귀하의 소득은 제한되어 있으며, 그 소득은 다른 여러 용도에도 지출되어야 합니다. **향후 10년 동안** 개인정보의 유출과 노출을 예방하기 위하여 비용을 지불한다고 가정했을 때, <개인정보보호를 위한 부가서비스 비용>을 매달 얼마를 지불하실 의사가 있으신지 여쭙고자 합니다.

(3) 개인정보 침해에 대한 가능성을 고려하여 이를 방지하기 위한 WTP를 조사함으로서 기존의 개인정보 유출에 따른 손해배상액을 조사하는 연구들과 차별화를 추구했다. 예컨대, 차건상(2011)의 경우 가상의 사건이 발생한 즉 개인정보 침해에 따른 손해배상 수용의사금액(Willness to Accept: WTA)를 조사하였으나, 이 연구에서는 WTA를 질의하는 경우와 달리 WTP의 경우 가상의 사건이 발생할 가능성에 대한 확률을 고려하여 응답자가 설문에 답변하도록 구성했다. Horowitz and McConnell (2002)[23]에서 기존 문헌을 통하여 WTA/WTP가 1보다 높음을 보고하였다. 이는 개인정보 침해가 발생한 경우 정보보유자들이 요구하는 WTA를 추정하는 권홍 외 (2012)와 달리 본 연구에서는 개인정보 유출과 노출을 예방하기 위한 WTP를 추정하는데 그 목적이 있다. 또한 WTP에 대한 조사는 기존 KISA(2007)의 연구방법과 동일하다.

(4) 사회적 비용을 최대한 보수적으로 도출하기 위한 방안으로서 다음과 같이 단계별 조치를 취하였다.

- o 1단계: 개인정보 유·노출에 대한 객관적 정보제공
- o 2단계: 예산제약을 상세히 설명, 즉 소득이 제한되어 있으며, 그 소득은 다른 여러 용도로 지출되어야 함을 명시적으로 설명(곽승준 외 (2001) 참조)
- o 3단계: 가구기준으로 WTP 질의

특히 가구기준을 통하여 미성년자 등 경제활동에 참여하지 않는 개인들의 정보보호를 포괄할 수 있도록 하였고, 가구의 소득을 반영한 실질적 지불의사를 바탕으로 보수적으로 추정하고자 하였다. 그러나 개인정보를 보호하기 위해서 개인의 지불금액을 조사하여야 한다는 의견이 존재할 수도 있다.

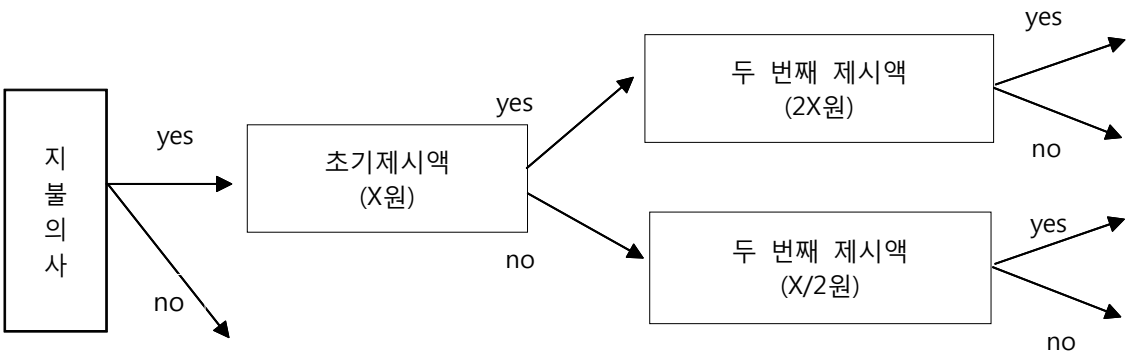
(5) 개인정보의 유·노출의 경우 인터넷을 포함하여 오프라인 등에서도 다양

23) Horowitz and McConnell, 2002, A Review of WTA/WTA Studies, Journal of Environmental Economics and Management 44, 426-447.

한 사례가 존재할 수 있음으로 포괄적인 질의를 수행하였다. 반면에 KISA(2007)의 경우에는 인터넷 사용자 중심으로 조사를 실시한 바 있다.

(6) 이중양분선택형으로 질문을 수행하였다. (그림 5-7)과 같이 먼저 WTP를 물어 '네'라고 답한 경우 초기제시액을 제시하고, 다시 '네'라고 답한 응답자에게 두 번째 제시액을 제시하였다. 예를 들어, 1,000원 제시액의 경우 응답자가 '네' 하면 2,000원을 제시하고 지불의사가 없다('아니오')고 하면 500원을 제시하여 조사하였다.

(그림 5-7) 이중양분선택형 질문 방법



(7) 지불금액의 범위를 미리 설정하고 질문을 수행하였다. 지불금액의 범위는 월 기준 1,000원, 2,000원, 3,000원, 4,000원, 5,000원, 6,000원, 7,000원, 8,000원, 9,000원, 10,000원의 10개 그룹으로 설정하였다. 본 방법론의 경우 동 분야에서 광범위하게 활용되는 곽승준(2001)과 동일한 접근방식이다. KISA(2007)에서는 300원, 600원, 1,000원, 5,000원, 10,000원의 5개 그룹으로 분류하였으며, 김재홍(2010), 한국개발연구원(2004) 등을 고려하는 경우 그룹설정에 정형화된 방법은 존재하지 않는 것으로 판단된다. 응답자의 소득을 고려하여 각 그룹당 고른 분포를 이루도록 조사하였고, 각 유형별 질문수행 이후 전체 개인정보 침해에 대한 질문은 각각 앞의 월 기준의 2배, 즉 2,000원, 4,000원, 6,000원, 8,000원, 10,000원, 12,000원, 14,000원, 16,000원, 18,000원, 20,000원의 10개 그룹으로 설정하였다.

3. 주요 변인에 대한 구분

(1) 권역

권역은 총 16개 광역시도를, 서울, 경기・인천, 충청권, 전라권, 경상권, 기타(강원・제주) 6개 권역으로 재분류하여 분석하였다. 충청권은 대전을 포함하고 있으며, 전라권은 광주를, 경상권은 대구, 울산, 부산을 포함하고 있다.

(2) 결혼 여부

결혼 여부는 결혼을 했던 경험까지 포함하였다. 이혼이나 사별의 경우에도 기혼으로 간주하여 기혼과 미혼의 2개 집단으로 분류하였다.

(3) 세대주 여부

세대주 여부는 응답자의 세대주 여부를 “그렇다”와 “아니다”로 구분하여 세대주와 비세대주 2개 집단으로 분류하였다.

(4) 수입가족 수

수입가족 수는 조사 시점에서 수입이 있는 전체 가족 수를 사례수를 기준으로 1명 이하, 2명, 3명 이상으로 분류하였다.

(5) 기혼자 자녀 수

기혼자 자녀 수는 기혼자에 한하여 자녀가 없는 경우와 자녀가 있는 경우로 나누어 실제 사례수를 기준으로 없음, 1명, 2명, 3명 이상으로 분류하였다.

(6) 취업 여부

취업 여부는 응답자가 현재 취업 상태인지 미취업 상태인지를 구분하여 분석하였다.

(7) 총 가족 수

총 가족 수는 응답자 본인을 포함하여 현재 함께 거주하고 있는 전체 가구원

의 수를 말하며, 실제 사례수를 기준으로 2명 이하, 3~4명, 5명 이상으로 분류하여 분석하였다.

(8) 직업

직업은 총 12개의 카테고리로 조사하였으며, 농업・어업・임업, 자영업, 판매・서비스직, 기능・숙련공, 일반작업직, 사무・기술직, 경영・관리직, 전문・자유직, 가정주부, 대학생・대학원생, 무직, 기타로 구분하였다. 실제 분석 단계에서는 12개의 카테고리를 1)자영업, 2)블루칼라, 3)화이트칼라, 4)가정주부, 5)학생, 6)무직・기타 직군의 6개 집단으로 재분류하여 분석하였다.

(9) 학력

학력은 무학(1), 초등학교(6), 중학교(3), 고등학교(3), 대학교(4), 대학원 이상(4)의 21개의 카테고리로 구분하여 측정하였으며, 실제 분석에서는 응답자 수를 고려하여 고졸 이하, 대재・대졸 이하, 대학원 이상(재학 포함)으로 재분류하여 분석하였다.

(10) 가구 소득

소득은 보너스와 이자수입, 임대수입 등을 모두 포함한 월평균가구소득으로 측정하였으며, 100만원 미만부터 1,000만원 이상까지 9개의 카테고리로 나누어 조사하였다, 소득 역시 실제 분석에서는 사례수를 기준으로 299만원 이하, 300~499만원, 500만원 이상으로 재분류하여 분석하였다.

(11) 가구통신요금

가구통신요금은 2012년 9월부터 2013년 8월까지 개인적으로 TV, 인터넷, 모바일 등의 상품이나 서비스 구매 금액의 월평균 값으로, 실제 분석에서는 사례수를 기준으로 월10만원 미만, 월10~20만원 미만, 월20만원 이상으로 재분류하여 분석하였다.

4. 응답자 특성 분포

개인정보 침해에 따른 사회적 비용분석 조사 전체 응답자는 총 800명이다. 하위 집단별 분포를 살펴보면 성별로는 남성 51.4%, 여성 48.6%이고, 연령별로는 20대 23.8%, 30대 27.5%, 40대 26.3%, 50대 16.3%, 60세 이상 6.3%로 나타났다. 결혼 여부별로는 기혼 60.8%, 미혼 39.3%이며, 직업별로는 자영업 8.4%, 블루칼라 10.6%, 화이트칼라 51.9%, 가정주부 13.0%, 학생 7.0%, 무직・기타 9.1%로 나타났다. 학력은 고졸이하 18.5%, 대재・대졸 69.4%, 대학원 이상 12.1%로 나타나며, 가구 소득은 299만원 이하, 300~499만원, 500만원 이상 계층이 각각 28.5%, 39.0%, 32.5%로 나타났다.

이외에 각 집단별 구성 비율은 [표 5-17]에 제시되어 있다.

[표 5-17] 응답자 특성표

		사례수	%
전체		(800)	100.0
성 별	남성	(411)	51.4
	여성	(389)	48.6
연 령	20대	(190)	23.8
	30대	(220)	27.5
	40대	(210)	26.3
	50대	(130)	16.3
	60세 이상	(50)	6.3
권역	서울	(163)	20.4
	경기/인천	(236)	29.5
	충청권	(87)	10.9
	전라권	(83)	10.4
	경상권	(197)	24.6
	기타(강원/제주)	(34)	4.3
결혼 여부	기혼	(486)	60.8
	미혼	(314)	39.3
세대주 여부	세대주	(318)	65.4
	비세대주	(168)	34.6
수입 가족 수	1명 이하	(207)	25.9

	2명	(302)	37.8
	3명 이상	(291)	36.4
기혼자 자녀수	없음	(44)	9.1
	1명	(134)	27.6
	2명	(263)	54.1
	3명 이상	(45)	9.3
취업 여부별	취업	(575)	71.9
	미취업	(225)	28.1
총 가족 수	2명 이하	(136)	17.0
	3~4명 이상	(555)	69.4
	5명 이상	(109)	13.6
직 업	자영업	(67)	8.4
	블루칼라	(85)	10.6
	화이트칼라	(415)	51.9
	가정주부	(104)	13.0
	학생	(56)	7.0
	무직/기타	(73)	9.1
학 력	고졸 이하	(148)	18.5
	대재/대졸	(555)	69.4
	대학원 이상	(97)	12.1
가구 소득	299만원 이하	(228)	28.5
	300~499 만원	(312)	39.0
	500만원 이상	(260)	32.5
가구통신요금	월10만원 미만	(303)	37.9
	월10~20만원 미만	(294)	36.8
	월20만원 이상	(203)	25.4

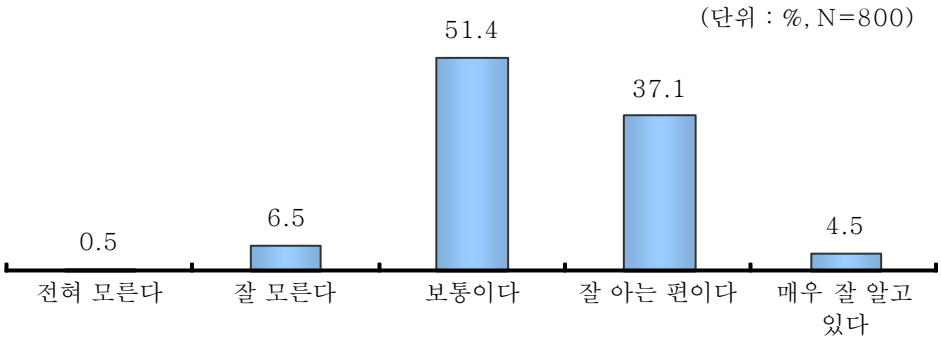
5. 개인정보에 대한 인지도 조사

(1) 개인정보 침해의 의미에 대한 인지도

개인정보 침해의 의미에 대한 인지도는 평균 3.39점으로 '보통이다'는 비중이 가장 높게 나타나고 있어 그다지 높지 않은 것으로 나타나고 있다.

하위 집단별로는 남성, 50세 이상 연령층, 서울 거주자, 취업자, 직업이 자영업 또는 화이트칼라인 응답자 계층에서 상대적으로 인지도가 높게 나타나고 있으며, 학력 수준 및 가구 소득 수준, 가구통신요금 등이 높을수록 인지도가 높아지는 경향이 나타나고 있다.

[표 5-18] 개인정보 침해의 의미에 대한 인지도



(단위 : %)

		사례수	전혀 모른다	잘 모른다	보통 이다	잘아는 편이다	매우잘 알고있다	평균 (점)
전체		(800)	0.5	6.5	51.4	37.1	4.5	3.39
성 별	남성	(411)	0.7	6.3	47.7	39.9	5.4	3.43
	여성	(389)	0.3	6.7	55.3	34.2	3.6	3.34
연 령	20대	(190)	0.5	7.4	49.5	37.4	5.3	3.39
	30대	(220)	0.0	9.1	53.2	34.1	3.6	3.32
	40대	(210)	1.0	4.8	54.8	35.2	4.3	3.37
	50대	(130)	0.0	3.8	46.2	47.7	2.3	3.48
	60세 이상	(50)	2.0	6.0	50.0	30.0	12.0	3.44
권 역	서울	(163)	0.0	5.5	46.0	42.3	6.1	3.49
	경기/인천	(236)	0.4	4.2	55.1	36.0	4.2	3.39
	충청권	(87)	0.0	8.0	57.5	32.2	2.3	3.29
	전라권	(83)	0.0	7.2	54.2	32.5	6.0	3.37
	경상권	(197)	1.0	8.6	49.2	38.1	3.0	3.34
	기타(강원/제주)	(34)	2.9	8.8	41.2	38.2	8.8	3.41

결혼 여부	기혼	(486)	0.2	6.0	51.6	37.4	4.7	3.41
	미혼	(314)	1.0	7.3	51.0	36.6	4.1	3.36
세대주 여부	세대주	(318)	0.3	6.0	46.2	41.5	6.0	3.47
	비세대주	(168)	0.0	6.0	61.9	29.8	2.4	3.29
수입 가족수	1명 이하	(207)	1.0	7.7	54.1	33.8	3.4	3.31
	2명	(302)	0.3	5.6	53.3	35.8	5.0	3.39
	3명 이상	(291)	0.3	6.5	47.4	40.9	4.8	3.43
기혼자 자녀수	없음	(44)	0.0	9.1	59.1	29.5	2.3	3.25
	1명	(134)	0.0	1.5	50.7	40.3	7.5	3.54
	2명	(263)	0.0	7.2	51.0	39.2	2.7	3.37
	3명 이상	(45)	2.2	8.9	51.1	26.7	11.1	3.36
취업 여부별	취업	(575)	0.7	5.7	48.7	39.5	5.4	3.43
	미취업	(225)	0.0	8.4	58.2	31.1	2.2	3.27
총가족 수	2명 이하	(136)	1.5	6.6	52.2	34.6	5.1	3.35
	3~4명 이상	(555)	0.4	6.1	50.6	38.6	4.3	3.40
	5명 이상	(109)	0.0	8.3	54.1	33.0	4.6	3.34
직 업	자영업	(67)	1.5	4.5	46.3	43.3	4.5	3.45
	블루칼라	(85)	1.2	7.1	47.1	42.4	2.4	3.38
	화이트칼라	(415)	0.5	5.5	47.7	39.5	6.7	3.47
	가정주부	(104)	0.0	7.7	60.6	30.8	1.0	3.25
	학생	(56)	0.0	8.9	46.4	42.9	1.8	3.38
	무직/기타	(73)	0.0	9.6	72.6	16.4	1.4	3.10
학 력	고졸 이하	(148)	1.4	8.1	54.7	31.1	4.7	3.30
	대재/대졸	(555)	0.4	6.3	50.3	38.7	4.3	3.40
	대학원 이상	(97)	0.0	5.2	52.6	37.1	5.2	3.42
가구 소득	299만원 이하	(228)	1.3	8.3	58.3	27.2	4.8	3.26
	300~499만원	(312)	0.3	7.1	49.0	39.4	4.2	3.40
	500만원 이상	(260)	0.0	4.2	48.1	43.1	4.6	3.48
가구 통신 요금	월10만원 미만	(303)	1.3	8.3	52.5	33.7	4.3	3.31
	월10~20만원 미만	(294)	0.0	6.1	49.7	40.8	3.4	3.41
	월20만원 이상	(203)	0.0	4.4	52.2	36.9	6.4	3.45

* [문1] 귀하는 '개인정보침해'의 의미에 대해서 얼마나 잘 알고 있습니까?

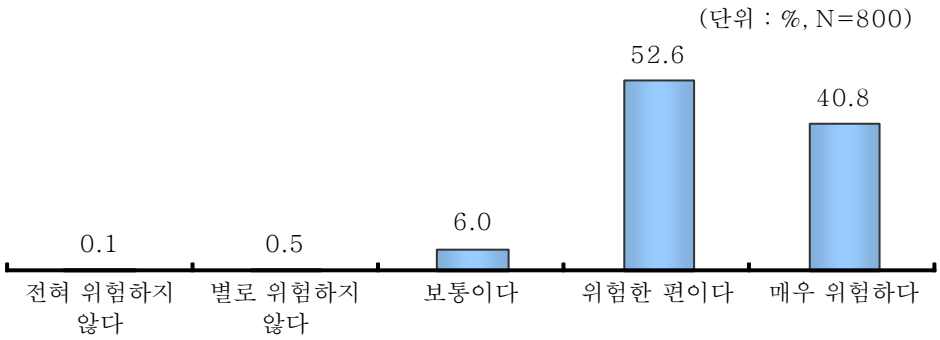
** 5점 척도: 전혀 모른다(1점) - 매우 잘 알고 있다(5점)

(2) 개인정보 침해의 위험도 인식

개인정보 침해의 위험도에 대해 전체 응답자의 대부분(93.4%)이 위험한 편(52.6%)이거나 매우 위험하다(40.8%)고 응답하고 있어, 개인정보 침해의 위험도를 심각하게 인식하고 있는 것으로 나타났다.

하위 집단별로는 특히, 20대 연령층 및 여성, 학생 집단에서 개인정보 침해의 위험도에 대해 보다 심각하게 인지하고 있는 것으로 나타났다.

[표 5-19] 개인정보 침해의 위험도 인식



(단위 : %)

		사례수	전혀 위험하지 않다	별로 위험하지 않다	보통 이다	위험한 편이다	매우 위험하다	평균 (점)
전체		(800)	0.1	0.5	6.0	52.6	40.8	4.33
성 별	남성	(411)	0.2	1.0	6.8	52.6	39.4	4.30
	여성	(389)	0.0	0.0	5.1	52.7	42.2	4.37
연 령	20대	(190)	0.0	0.0	5.3	49.5	45.3	4.40
	30대	(220)	0.0	0.5	7.7	54.5	37.3	4.29
	40대	(210)	0.5	1.4	4.3	52.9	41.0	4.32
	50대	(130)	0.0	0.0	5.4	53.8	40.8	4.35
	60세 이상	(50)	0.0	0.0	10.0	52.0	38.0	4.28

권 역	서울	(163)	0.0	1.8	7.4	48.5	42.3	4.31
	경기/인천	(236)	0.0	0.0	5.1	53.0	41.9	4.37
	충청권	(87)	0.0	0.0	9.2	59.8	31.0	4.22
	전라권	(83)	0.0	1.2	6.0	56.6	36.1	4.28
	경상권	(197)	0.5	0.0	4.1	54.3	41.1	4.36
	기타(강원/제주)	(34)	0.0	0.0	8.8	32.4	58.8	4.50
결혼 여부	기혼	(486)	0.0	0.2	6.4	54.9	38.5	4.32
	미혼	(314)	0.3	1.0	5.4	49.0	44.3	4.36
세대주 여부	세대주	(318)	0.0	0.3	6.3	54.7	38.7	4.32
	비세대주	(168)	0.0	0.0	6.5	55.4	38.1	4.32
수입 가족수	1명 이하	(207)	0.0	0.5	5.3	53.1	41.1	4.35
	2명	(302)	0.0	0.0	6.0	56.0	38.1	4.32
	3명 이상	(291)	0.3	1.0	6.5	48.8	43.3	4.34
기혼자 자녀수	없음	(44)	0.0	0.0	4.5	61.4	34.1	4.30
	1명	(134)	0.0	0.0	7.5	53.7	38.8	4.31
	2명	(263)	0.0	0.4	6.1	55.1	38.4	4.32
	3명 이상	(45)	0.0	0.0	6.7	51.1	42.2	4.36
취업 여부별	취업	(575)	0.2	0.7	5.6	52.3	41.2	4.34
	미취업	(225)	0.0	0.0	7.1	53.3	39.6	4.32
총가족 수	2명 이하	(136)	0.0	0.0	5.9	54.4	39.7	4.34
	3~4명 이상	(555)	0.2	0.5	6.7	51.5	41.1	4.33
	5명 이상	(109)	0.0	0.9	2.8	56.0	40.4	4.36
직 업	자영업	(67)	1.5	1.5	6.0	56.7	34.3	4.21
	블루칼라	(85)	0.0	0.0	8.2	48.2	43.5	4.35
	화이트칼라	(415)	0.0	0.7	4.3	53.0	41.9	4.36
	가정주부	(104)	0.0	0.0	8.7	55.8	35.6	4.27
	학생	(56)	0.0	0.0	5.4	48.2	46.4	4.41
	무직/기타	(73)	0.0	0.0	9.6	50.7	39.7	4.30
학 력	고졸 이하	(148)	0.0	0.0	8.1	52.0	39.9	4.32
	대재/대졸	(555)	0.2	0.7	5.0	53.5	40.5	4.34
	대학원 이상	(97)	0.0	0.0	8.2	48.5	43.3	4.35

가구 소득	299만원 이하	(228)	0.0	0.9	7.9	50.9	40.4	4.31
	300~499만원	(312)	0.3	0.3	5.8	51.0	42.6	4.35
	500만원 이상	(260)	0.0	0.4	4.6	56.2	38.8	4.33
가구 통신 요금	월10만원 미만	(303)	0.3	1.0	6.9	54.1	37.6	4.28
	월10~20만원 미만	(294)	0.0	0.3	5.1	51.7	42.9	4.37
	월20만원 이상	(203)	0.0	0.0	5.9	51.7	42.4	4.36

* [문2] 귀하는 현재 우리 사회에서의 개인정보 침해가 얼마나 위험하다고(위협적이라고) 생각하십니까?
** 5점 척도: 전혀 위험하지 않다(1점) - 매우 위험하다(5점)

개인정보 침해가 '전혀 위험하지 않다' 그리고 '별로 위험하지 않다'는 비중은 단지 0.6%에 불과한 것을 나타났다. 그리고 개인정보 침해가 '위험하지 않다'고 응답한 비중('보통이다' 포함)은 단지 6.6%에 불과한 것을 확인할 수 있다.

KISA(2007)의 연구와 비교하면, 당시 89.4%가 위험하다고 인식한 것에 비해 지금은 93.4%가 위험하다고 인식하고 있기 때문에 위험에 대한 인식도는 2007년의 연구에 비해 4% 포인트 증가한 것으로 나타났다. 즉, 대형화된 개인정보 유출 사고가 발생하고, 언론을 통해 개인정보에 대한 유출 피해를 자주 접했기 때문에 이용자들의 개인정보 침해에 대한 위험도 인식은 2007년에 비해 증가한 것으로 판단된다.

(3) 개인정보 침해 경험

전체 응답자의 약 절반 정도인 47.5%가 개인정보 침해 경험이 있는 것으로 나타났다. 하위 집단별로는 20~30대 연령층, 서울 거주자, 미혼, 취업자, 직업이 자영업 및 화이트칼라인 응답자 계층에서 상대적으로 침해 경험률이 다소 높게 나타나고 있으며, 학력 수준이 높을수록 개인정보 침해 경험률이 높아지는 경향이 나타나고 있다.

[표 5-20] 개인정보 침해 경험

(단위 : %)

		사례수	예 (경험 있음)	아니오 (경험 없음)
전체		(800)	47.5	52.5
성 별	남성	(411)	48.4	51.6
	여성	(389)	46.5	53.5
연 령	20대	(190)	57.4	42.6
	30대	(220)	52.3	47.7
	40대	(210)	44.8	55.2
	50대	(130)	36.9	63.1
	60세 이상	(50)	28.0	72.0
권 역	서울	(163)	54.6	45.4
	경기/인천	(236)	44.1	55.9
	충청권	(87)	50.6	49.4
	전라권	(83)	48.2	51.8
	경상권	(197)	43.7	56.3
	기타(강원/제주)	(34)	50.0	50.0
결혼 여부	기혼	(486)	43.4	56.6
	미혼	(314)	53.8	46.2
세대주 여부	세대주	(318)	46.9	53.1
	비세대주	(168)	36.9	63.1
수입 가족수	1명 이하	(207)	42.0	58.0
	2명	(302)	46.7	53.3
	3명 이상	(291)	52.2	47.8

기혼자 자녀수	없음	(44)	52.3	47.7
	1명	(134)	45.5	54.5
	2명	(263)	39.2	60.8
	3명 이상	(45)	53.3	46.7
취업 여부별	취업	(575)	49.9	50.1
	미취업	(225)	41.3	58.7
총가족 수	2명 이하	(136)	53.7	46.3
	3~4명 이상	(555)	45.9	54.1
	5명 이상	(109)	47.7	52.3
직 업	자영업	(67)	52.2	47.8
	블루칼라	(85)	36.5	63.5
	화이트칼라	(415)	52.5	47.5
	가정주부	(104)	35.6	64.4
	학생	(56)	50.0	50.0
	무직/기타	(73)	42.5	57.5
학 력	고졸 이하	(148)	33.1	66.9
	대재/대졸	(555)	50.3	49.7
	대학원 이상	(97)	53.6	46.4
가구 소득	299만원 이하	(228)	42.1	57.9
	300~499만원	(312)	50.3	49.7
	500만원 이상	(260)	48.8	51.2
가구통신요금	월10만원 미만	(303)	47.2	52.8
	월10~20만원 미만	(294)	45.6	54.4
	월20만원 이상	(203)	50.7	49.3

* [문3] 지난 1년 간 귀하는 온라인을 포함한 일상생활에서 개인정보 또는 프라이버시 침해로 인한 피해를 입으신 경험이 있으십니까?

(4) 유형별 개인정보 침해 경험률

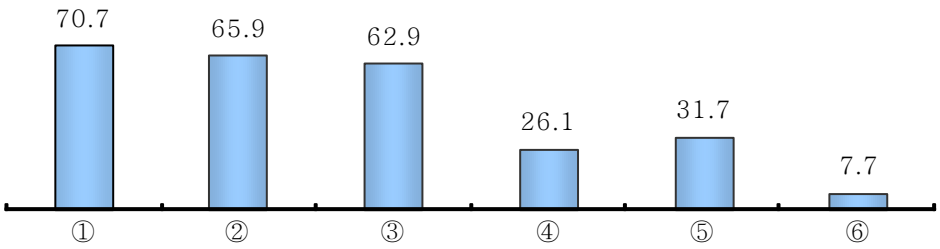
개인정보 침해 유형 중 '①관리 소홀로 개인정보가 유출된 경우'가 70.7%로 가장 높게 나타나고 있으며, 그 다음으로는 '②목적 이외 용도 이용 및 제3자 제

공(65.9%)'과 '③텔레마케팅 목적 이용 및 무단 회원 가입(62.9%)'이 가장 많이 발생하는 침해 유형으로 나타나고 있다(복수응답 결과). 피해자들은 대부분 개인정보 침해가 사업자의 의도적 아니면 부주의한 관리 소홀에서 발생한다고 생각하고 있는 것이다.

하위 집단별로 살펴보면, 20대 연령층, 남성, 서울 거주자, 직업 화이트칼라 및 학생인 집단에서 타 집단에 비해 '④주민번호 도용' 및 '⑤ ID/비밀번호 도용' 경험이 다소 높은 특징을 보이고 있으며, 세부 유형별로 다소 차이는 있으나 전반적으로 학력 수준 및 가구통신요금이 높을수록 개인정보 침해 경험률이 높아지는 경향이 나타나고 있다.

[표 5-21] 유형별 개인정보 침해 경험률

(단위 : %, N=800)



<보기> 개인정보 침해 유형

①	사업자의 관리 소홀로 개인정보가 유출된 경우
②	사업자가 귀하의 동의 없이 개인정보를 본래 목적 이외의 용도로 이용하거나 제3자에게 제공한 경우
③	사업자가 귀하의 개인정보를 무단 수집하여 텔레마케팅 목적으로 이용하였거나 무단으로 회원으로 가입시킨 경우
④	주민번호 도용으로 웹사이트 회원가입이 되지 않았거나 경제적인 피해를 입은 경우
⑤	ID 및 비밀번호 도용으로 게임 아이템, 사이버머니, 캐릭터 등을 도난당한 경우
⑥	기타

(단위 : %)

		사례수	①	②	③	④	⑤	⑥
전체		(375)	70.7	65.9	62.9	26.1	31.7	7.7
성 별	남성	(198)	71.2	63.1	62.6	31.3	36.4	5.6
	여성	(177)	70.1	68.9	63.3	20.3	26.6	10.2
연 령	20대	(106)	69.8	68.9	57.5	32.1	46.2	5.7
	30대	(114)	75.4	66.7	66.7	26.3	29.8	8.8
	40대	(93)	72.0	63.4	64.5	23.7	23.7	7.5
	50대	(48)	58.3	54.2	66.7	16.7	22.9	10.4
	60세 이상	(14)	71.4	92.9	50.0	28.6	21.4	7.1
권 역	서울	(87)	72.4	63.2	64.4	34.5	39.1	5.7
	경기/인천	(104)	75.0	73.1	71.2	21.2	22.1	9.6
	충청권	(43)	62.8	60.5	48.8	23.3	37.2	9.3
	전라권	(40)	77.5	77.5	57.5	25.0	37.5	7.5
	경상권	(84)	61.9	59.5	59.5	26.2	29.8	7.1
	기타(강원/제주)	(17)	82.4	52.9	70.6	23.5	35.3	5.9
결혼 여부	기혼	(210)	67.6	67.6	66.2	27.1	28.1	8.6
	미혼	(165)	74.5	63.6	58.8	24.8	36.4	6.7
세대주 여부	세대주	(149)	70.5	67.8	69.8	30.2	32.2	6.7
	비세대주	(61)	60.7	67.2	57.4	19.7	18.0	13.1
수입 가족수	1명 이하	(86)	70.9	65.1	60.5	24.4	34.9	4.7
	2명	(141)	70.2	68.8	63.8	23.4	25.5	6.4
	3명 이상	(148)	70.9	63.5	63.5	29.7	35.8	10.8
기혼자 자녀수	없음	(23)	56.5	60.9	69.6	30.4	26.1	0.0
	1명	(61)	72.1	62.3	57.4	29.5	29.5	8.2
	2명	(102)	69.6	73.5	70.6	24.5	25.5	11.8
	3명 이상	(24)	58.3	62.5	66.7	29.2	37.5	4.2
취업 여부별	취업	(283)	72.8	66.1	66.4	26.5	32.2	7.4
	미취업	(92)	64.1	65.2	52.2	25.0	30.4	8.7
총가족 수	2명 이하	(73)	74.0	61.6	67.1	17.8	24.7	2.7
	3~4명 이상	(250)	71.6	68.0	62.0	27.2	31.2	9.6
	5명 이상	(52)	61.5	61.5	61.5	32.7	44.2	5.8

직 업	자영업	(35)	65.7	54.3	65.7	25.7	25.7	2.9
	블루칼라	(30)	80.0	66.7	60.0	36.7	50.0	3.3
	화이트칼라	(215)	74.0	67.4	68.4	25.6	30.7	8.4
	가정주부	(36)	55.6	61.1	55.6	19.4	19.4	13.9
	학생	(28)	67.9	75.0	53.6	28.6	53.6	7.1
	무직/기타	(31)	64.5	64.5	41.9	25.8	22.6	6.5
학 력	고졸 이하	(48)	66.7	62.5	45.8	29.2	29.2	10.4
	대재/대졸	(275)	71.3	65.5	65.8	23.3	31.3	7.3
	대학원 이상	(52)	71.2	71.2	63.5	38.5	36.5	7.7
가구 소득	299만원 이하	(94)	73.4	60.6	57.4	29.8	36.2	8.5
	300~499만원	(156)	71.8	64.7	60.9	28.2	34.6	6.4
	500만원 이상	(125)	67.2	71.2	69.6	20.8	24.8	8.8
가구 통신 요금	월10만원 미만	(142)	69.7	62.0	62.7	23.2	26.8	8.5
	월10~20만원 미만	(130)	71.5	66.2	63.1	23.8	33.1	8.5
	월20만원 이상	(103)	70.9	70.9	63.1	33.0	36.9	5.8

* [문3-1] 귀하는 어떤 유형의 개인정보/프라이버시 침해를 경험하셨습니까?

6. 개인정보보호에 대한 중요도 조사

(1) 개인정보 관련 중요도 인식

개인정보와 관련하여 '①개인정보 보호의 중요성'에 대해 평균 4.66점(5점 만점)으로 가장 높은 동의율을 보이고 있으며, 그밖에 '⑤보이스피싱 피해 심각성', '②해킹 및 바이러스 피해 심각성', '③개인정보 및 프라이버시 침해 피해 심각성', '④휴대전화 스팸, 스마트폰 스팸, 스팸메일 피해 심각성'등에 대해서도 평균 4.4 ~ 4.5점대의 높은 동의율을 보이고 있다.

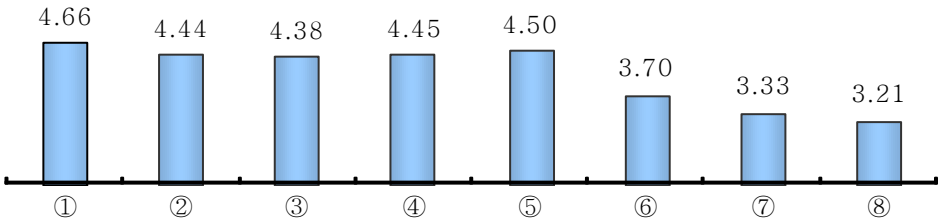
반면, 웹사이트 내에서의 '⑥개인정보 관리수준 확인', '⑦개인정보 파기 여부 확인', '⑧이용약관/개인정보 보호정책의 도움 여부' 등에 대해서는 평균 3.7점 이하의 상대적으로 낮은 동의 정도를 보이고 있다.

하위 집단별로 살펴보면, 상대적으로 연령이 낮을수록 '③개인정보 및 프라이

버시 침해 피해 심각성'에 대한 동의율이 다소 높은 특징을 보이고 있으며, 연령이 높을수록 '⑧이용약관/개인정보 보호정책이 도움이 된다'고 인식하는 비율이 다소 높게 나타나고 있다.

[표 5-22] 개인정보 관련 중요도 인식

(단위 : 점/5점만점, N=800)



<보기> 개인정보 관련 현상

①	개인정보 보호는 중요하다
②	해킹 및 바이러스로 인한 사회 전반의 피해는 심각하다
③	개인정보 및 프라이버시 침해로 인한 사회 전반의 피해는 심각하다
④	휴대전화 스팸, 스마트폰 스팸, 스팸메일로 인한 사회 전반의 피해는 심각하다
⑤	보이스 피싱으로 인한 사회 전반의 피해는 심각하다
⑥	웹사이트에 회원가입, 경품응모, 물품구입 등을 위해 개인정보를 제공하실 때, 해당 사이트의 개인정보 관리 수준을 확인한다
⑦	특정 웹사이트의 회원을 해지할 때 개인정보 파기여부를 확인한다
⑧	웹사이트에 게시되어 있는 '이용약관' 이나 '개인정보 보호정책' 등은 나의 개인정보보호에 도움이 된다

(단위 : 점/5점만점)

		사례수	①	②	③	④	⑤	⑥	⑦	⑧
전체		(800)	4.66	4.44	4.38	4.45	4.50	3.70	3.33	3.21
성 별	남성	(411)	4.63	4.41	4.36	4.41	4.49	3.71	3.31	3.25
	여성	(389)	4.68	4.47	4.41	4.49	4.50	3.68	3.34	3.18

연 령	20대	(190)	4.66	4.47	4.48	4.58	4.53	3.67	3.41	3.12
	30대	(220)	4.61	4.41	4.40	4.45	4.50	3.75	3.39	3.23
	40대	(210)	4.65	4.49	4.33	4.39	4.51	3.69	3.25	3.23
	50대	(130)	4.75	4.41	4.35	4.40	4.43	3.74	3.30	3.26
	60세 이상	(50)	4.62	4.32	4.22	4.26	4.50	3.48	3.18	3.30
권 역	서울	(163)	4.58	4.49	4.47	4.42	4.54	3.62	3.35	3.17
	경기/인천	(236)	4.71	4.42	4.36	4.42	4.50	3.70	3.20	3.17
	충청권	(87)	4.70	4.39	4.31	4.34	4.43	3.69	3.21	3.10
	전라권	(83)	4.54	4.43	4.29	4.46	4.48	3.81	3.59	3.37
	경상권	(197)	4.66	4.42	4.37	4.50	4.47	3.70	3.40	3.26
	기타(강원/제주)	(34)	4.79	4.62	4.65	4.71	4.68	3.76	3.35	3.29
결혼 여부	기혼	(486)	4.66	4.43	4.36	4.40	4.48	3.72	3.34	3.28
	미혼	(314)	4.66	4.46	4.43	4.51	4.53	3.66	3.31	3.11
세대주 여부	세대주	(318)	4.66	4.44	4.38	4.41	4.50	3.71	3.32	3.34
	비세대주	(168)	4.64	4.41	4.32	4.39	4.43	3.73	3.37	3.17
수입 가족수	1명 이하	(207)	4.70	4.46	4.38	4.45	4.53	3.66	3.32	3.20
	2명	(302)	4.66	4.46	4.43	4.46	4.53	3.72	3.29	3.16
	3명 이상	(291)	4.62	4.41	4.34	4.42	4.44	3.69	3.37	3.28
기혼자 자녀수	없음	(44)	4.59	4.41	4.43	4.64	4.59	3.68	3.41	3.16
	1명	(134)	4.70	4.49	4.44	4.47	4.49	3.79	3.43	3.34
	2명	(263)	4.62	4.42	4.31	4.34	4.48	3.70	3.27	3.25
	3명 이상	(45)	4.78	4.33	4.31	4.33	4.36	3.67	3.42	3.40
취업 여부별	취업	(575)	4.64	4.45	4.38	4.47	4.52	3.72	3.35	3.25
	미취업	(225)	4.69	4.42	4.40	4.39	4.45	3.64	3.28	3.11
총가족 수	2명 이하	(136)	4.68	4.46	4.43	4.55	4.60	3.66	3.36	3.21
	3~4명 이상	(555)	4.65	4.46	4.38	4.43	4.48	3.72	3.31	3.22
	5명 이상	(109)	4.67	4.32	4.35	4.41	4.45	3.63	3.37	3.18

직 업	자영업	(67)	4.52	4.40	4.27	4.40	4.51	3.87	3.43	3.33
	블루칼라	(85)	4.67	4.44	4.42	4.42	4.46	3.74	3.38	3.25
	화이트칼라	(415)	4.65	4.47	4.40	4.49	4.53	3.70	3.33	3.26
	가정주부	(104)	4.71	4.37	4.33	4.30	4.43	3.66	3.33	3.14
	학생	(56)	4.75	4.50	4.55	4.55	4.54	3.75	3.50	3.20
	무직/기타	(73)	4.67	4.37	4.30	4.38	4.42	3.47	3.04	2.93
학 력	고졸 이하	(148)	4.63	4.35	4.26	4.32	4.40	3.64	3.28	3.24
	대재/대졸	(555)	4.66	4.47	4.41	4.48	4.52	3.68	3.34	3.22
	대학원 이상	(97)	4.65	4.38	4.39	4.43	4.54	3.85	3.31	3.12
가구 소득	299만원 이하	(228)	4.67	4.45	4.38	4.43	4.45	3.58	3.37	3.18
	300~499만원	(312)	4.63	4.43	4.36	4.45	4.49	3.71	3.24	3.24
	500만원 이상	(260)	4.68	4.45	4.41	4.46	4.55	3.77	3.39	3.20
가구 통신 요금	월10만원 미만	(303)	4.60	4.43	4.35	4.46	4.47	3.70	3.36	3.24
	월10~20만원 미만	(294)	4.67	4.47	4.40	4.46	4.52	3.67	3.35	3.18
	월20만원 이상	(203)	4.71	4.41	4.41	4.41	4.52	3.72	3.26	3.23

* [문4] 귀하는 다음에 대하여 얼마나 그렇다고 생각하십니까?
** 5점 척도: 전혀 그렇지 않다(1점) - 매우 그렇다(5점)

(2) 개인정보 유형별 절대적 가치평가 응답

유형별 개인정보의 절대적 가치에 대한 평가를 위하여 개인정보 유형별로 개인정보가 1) '가치가 없다', 2) '거의 가치가 없다', 3) '가치가 있다', 4) '가치가 높다' 그리고 5) '매우 가치가 높다'라고 응답한 설문조사 결과는 아래의 표와 같다. 기본인적정보에 대하여 311명의 응답자가 '가치가 높다'고 응답하였으며, 223명의 응답자가 '가치가 있다' 그리고 217명이 '매우 가치가 높다'고 응답하였다. 고유정보의 경우 377명의 응답자가 '매우 가치가 높다'고 응답하였으며, 경제정보의 경우도 373명이 '매우 가치가 높다'고 응답하였다.

그러나 의료건강정보의 경우 기본인적정보와 마찬가지로 '가치가 높다'고 반응한 응답자가 가장 높았다. 사회관계정보의 경우 '가치가 있다'와 '가치가 높다'는 비중이 각각 280명과 275명이였으며, 통신위치정보의 경우 '가치가 높다'는

응답이 293명 그리고 '매우 가치가 높다'고 응답한 비중이 254명으로 나타났다. 법적정보는 285명이 '매우 가치가 높다'고 응답하였으며, 272명이 '가치가 높다 ' 그리고 204명의 응답자가 '가치가 있다'고 응답하였다. '매우 가치가 높다'고 응답한 빈도수가 가장 많은 것은 고유정보, 경제정보, 법적정보였고, '가치가 높다'고 응답한 빈도수가 가장 많은 것은 기본인적정보, 의료건강정보, 그리고 통신위치정보이다. 반면 사회관계정보의 경우 '가치가 있다'고 응답한 빈도수가 가장 높았다.

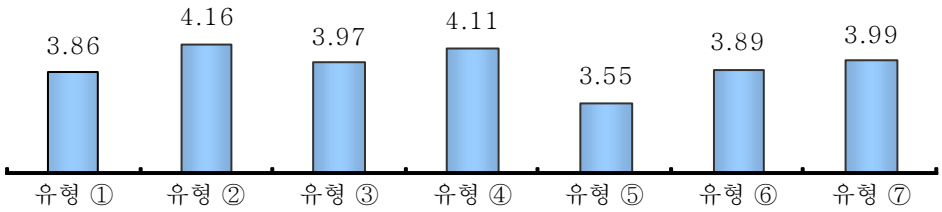
	가치가 없다	거의 가치가 없다	가치가 있다	가치가 높다	매우 가치가 높다	계
유형 1) 기본인적 정보: 성명, 주소, 아이디 및 패스워드, 가족관계 등	6	43	223	311	217	800
유형 2) 고유정보: 주민등록번호, 여권번호, 운전면허 등록번호 등	14	36	139	234	377	800
유형 3) 의료건강정보: 병력, 병원 진료기록, 신체장애 정도, 건강상태 등	13	31	183	315	258	800
유형 4) 경제정보: 소득, 신용카드 및 통장계좌번호, 물품 구매내역, 대출 또는 담보설정 등	17	40	153	217	373	800
유형 5) 사회관계정보: 학력 및 학업성적, 친우관계, 동호회 활동 등 사회 활동 관련 정보	25	74	280	275	146	800
유형 6) 통신위치정보: 휴대폰 번호, 이메일주소, GPS 위치정보 등	21	49	183	293	254	800
유형 7) 법적정보: 전과 범죄기록, 납세기록, 과태료 부과내역 등	15	24	204	272	285	800

즉, 전체 응답자들은 개인정보 중 주민등록번호 등의 '②고유정보'에 대한 가치를 가장 높게 평가하고 있으며, 그 다음으로는 '④경제정보', '⑦법적정보', '③의료건강정보' 순으로 그 가치를 높게 평가하고 있다.

하위 집단별로 살펴보면, 저연령층 및 고학력자 집단에서 개인정보의 가치를 높게 평가하는 경향이 나타나고 있으며, 유형별로 다소 차이는 있으나 전반적으로 가구소득 및 가구통신요금 수준이 높을수록 개인정보의 가치를 높게 평가하는 경향이 나타나고 있다.

[표 5-23] 개인정보 유형별 가치 평가

(단위 : 점/5점만점, N=800)



<보기> 개인정보 유형

유형 ① **기본인적정보** : 성명, 주소, 아이디 및 패스워드, 가족관계 등
(기본인적정보는 온·오프라인 회원가입 및 서비스 이용, 물품 수령 등에 주로 이용)

유형 ② **고유정보** : 주민등록번호, 여권번호, 운전면허등록번호 등
(고유정보는 상거래·금융거래 등에서 본인 식별을 위한 확인수단으로 사용)

유형 ③ **의료건강정보** : 병력, 병원진료기록, 신체장애정도, 건강상태 등
(의료건강정보는 병원 진료 및 치료, 보험 가입 및 계약 유지, 유전자 분석 등에 이용)

유형 ④ **경제정보** : 소득, 신용카드 및 통장계좌번호, 물품구매내역, 대출 또는 담보설정 등
(경제정보는 상거래 및 금융거래 등 경제 활동 전반에서 이용)

유형 ⑤ **사회관계정보** : 학력 및 학업성적, 친우 관계, 동호회 활동 등 사회활동 관련 정보
(사회관계정보는 취업 시 활용 및 사회 전반적으로 이용)

유형 ⑥ **통신위치정보** : 휴대폰번호, 이메일주소, GPS위치정보 등
(통신위치정보는 신용카드 이용 정보 등과 결합하여 기업의 마케팅, 기업홍보 등에 사용)

유형 ⑦ **법적정보** : 전과범죄기록, 납세기록, 과태료부과내역 등
(법적정보는 정부 행정 전반에 걸쳐 이용)

(단위 : 점/5점만점)

		사례수	①	②	③	④	⑤	⑥	⑦
전체		(800)	3.86	4.16	3.97	4.11	3.55	3.89	3.99
성 별	남성	(411)	3.85	4.15	4.00	4.11	3.55	3.87	3.97
	여성	(389)	3.88	4.16	3.94	4.11	3.55	3.91	4.00
연 령	20대	(190)	4.01	4.34	3.98	4.34	3.63	4.08	4.18
	30대	(220)	3.85	4.21	4.04	4.09	3.69	3.95	4.01
	40대	(210)	3.84	4.10	3.90	4.00	3.48	3.77	3.90
	50대	(130)	3.78	3.99	3.99	4.08	3.48	3.83	3.93
	60세 이상	(50)	3.66	3.88	3.82	3.88	3.18	3.54	3.60

권 역	서울	(163)	3.85	4.15	4.07	4.17	3.61	3.90	3.96
	경기/인천	(236)	3.84	4.13	3.94	4.08	3.53	3.92	3.92
	충청권	(87)	3.90	4.18	3.86	4.11	3.44	3.85	3.97
	전라권	(83)	3.93	4.22	4.02	4.18	3.57	4.02	4.16
	경상권	(197)	3.84	4.15	3.92	4.07	3.57	3.78	3.96
	기타(강원/제주)	(34)	3.97	4.18	4.06	4.18	3.59	3.94	4.35
결혼 여부	기혼	(486)	3.78	4.03	3.92	4.02	3.50	3.77	3.91
	미혼	(314)	4.00	4.35	4.05	4.25	3.64	4.07	4.11
세대주 여부	세대주	(318)	3.81	4.08	3.96	4.03	3.51	3.79	3.90
	비세대주	(168)	3.70	3.94	3.83	4.00	3.47	3.73	3.92
수입 가족수	1명 이하	(207)	3.84	4.15	3.97	4.11	3.49	3.86	3.97
	2명	(302)	3.84	4.19	3.96	4.12	3.52	3.85	4.01
	3명 이상	(291)	3.91	4.13	3.97	4.10	3.63	3.95	3.98
기혼자 자녀수	없음	(44)	3.73	4.09	3.98	4.02	3.70	3.84	4.14
	1명	(134)	3.66	4.09	3.93	4.19	3.52	3.86	3.96
	2명	(263)	3.86	4.00	3.88	3.96	3.46	3.72	3.88
	3명 이상	(45)	3.67	3.96	4.00	3.87	3.47	3.73	3.71
취업 여부별	취업	(575)	3.88	4.14	3.96	4.10	3.55	3.90	3.98
	미취업	(225)	3.81	4.19	3.98	4.14	3.55	3.85	4.00
총가족 수	2명 이하	(136)	3.81	4.18	3.96	4.04	3.60	3.94	4.04
	3~4명 이상	(555)	3.87	4.15	3.96	4.13	3.53	3.87	3.96
	5명 이상	(109)	3.88	4.17	4.00	4.09	3.63	3.91	4.02
직 업	자영업	(67)	3.93	4.00	3.90	4.16	3.52	3.84	3.81
	블루칼라	(85)	3.94	4.08	4.02	4.02	3.55	3.84	3.92
	화이트칼라	(415)	3.89	4.21	3.99	4.14	3.58	3.96	4.02
	가정주부	(104)	3.74	3.95	3.89	4.02	3.57	3.68	3.88
	학생	(56)	4.04	4.57	4.05	4.39	3.75	4.16	4.34
	무직/기타	(73)	3.59	4.03	3.90	3.93	3.27	3.67	3.89
학 력	고졸 이하	(148)	3.70	3.87	3.78	3.86	3.24	3.65	3.72
	대재/대졸	(555)	3.90	4.20	3.98	4.16	3.60	3.94	4.03
	대학원 이상	(97)	3.91	4.31	4.19	4.19	3.74	3.95	4.13

가구 소득	299만원 이하	(228)	3.79	4.07	3.92	4.04	3.43	3.83	3.91
	300~499만원	(312)	3.89	4.21	3.91	4.10	3.56	3.88	4.04
	500만원 이상	(260)	3.89	4.16	4.08	4.18	3.65	3.95	3.99
가구 통신 요금	월10만원 미만	(303)	3.86	4.06	3.95	4.00	3.48	3.85	3.88
	월10~20만원 미만	(294)	3.87	4.21	3.94	4.19	3.60	3.89	4.00
	월20만원 이상	(203)	3.85	4.21	4.02	4.15	3.59	3.93	4.12

* [문5] 여러분들이 제공하는 개인정보는 가치를 가질 수 있습니다. 귀하께서는 다음 유형의 정보들이 얼마나 가치가 있다고 생각하십니까?

** 5점 척도: 가치가 없다(1점) - 거의 가치가 없다(2점) - 가치가 있다(3점) - 가치가 높다(4점) - 매우 가치가 높다(5점)

(3) 개인정보 유형별 상대적 중요도 순위 응답

7가지 유형의 개인정보에 대하여 순위를 정하도록 설문한 결과 고유정보, 기본인적정보를 1순위로 선정한 응답자가 각각 211명과 412명에 해당하였다. 특히 과반수 이상의 응답자들이 주민등록번호, 여권번호, 운전면허 등록번호 등 고유정보가 1순위로 중요하다고 응답하였다. 반면 사회관계정보의 경우 274명이 7순위에 245명의 응답자가 6순위의 중요도를 나타낸다고 응답하였다. 이는 일상생활에서 상대적으로 학력 및 학업 혹은 친우 동호회 활동 등의 정보는 사람들 간에 공유가 이루어지고 있기 때문으로 생각된다.

법적정보 즉 전과, 범죄기록, 과태료 등의 정보는 응답자의 364명이 7순위 그리고 180명이 6순위에 중요도에 응답하였으며, 법적정보가 중요한 사람들의 비중이 상대적으로 높지 않다는 것을 확인할 수 있다. 법적으로 이슈가 있는 응답자는 상대적으로 법적정보의 침해에 대한 비중을 높게 평가할 수 있지만, 그렇지 않은 일반인들의 경우 법적정보에 대한 이슈에 민감하게 반응하고 있지 않다는 것은 흥미로운 조사결과이다. 소득, 신용카드 및 통장계좌번호, 물품 구매내역, 대출 또는 담보설정 등 경제정보의 경우 2순위 혹은 3순위로 응답한 비중이 상대적으로 높았다. 이는 기본인적정보와 고유정보와 더불어 경제정보의 중요성을 일반인들이 높게 평가하고 있다는 것을 반영한 결과라고 볼 수 있다. 의료건강정보와 통신위치정보는 상대적으로 3순위 혹은 4순위로 응답한 빈도수가 높은

것을 확인할 수 있다.

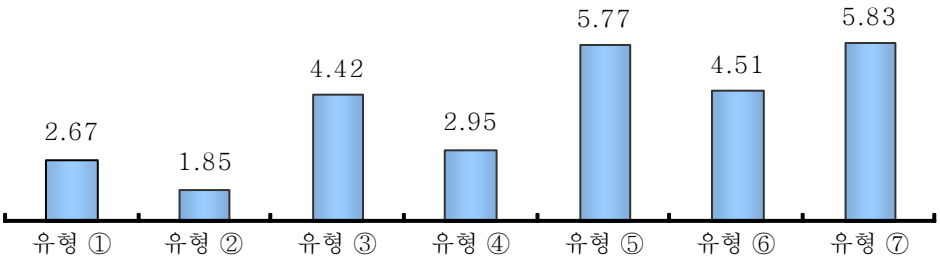
즉, 이용자들은 개인정보 유형별 상대적인 중요도에서 고유정보, 기본인적정보, 경제정보, 통신위치정보, 의료건강정보, 사회관계정보, 법적정보 순으로 중요하다고 판단하는 것으로 나타났다. 이는 절대적인 중요도 조사의 결과와는 약간 다름을 알 수 있어, 절대적으로 묻는 방식에서의 이용자 답변과 상대적 조사에서의 이용자 답변에는 차이가 존재함을 의미한다.

	7순위	6순위	5순위	4순위	3순위	2순위	1순위	계
유형 1) 기본인적 정보: 성명, 주소, 아이디 및 패스워드, 가족관계 등.	33	34	36	96	149	241	211	800
유형 2) 고유정보: 주민등록번호, 여권번호, 운전면허 등록번호 등.	7	12	18	34	86	231	412	800
유형 3) 의료건강정보: 병력, 병원 진료기록, 신체장애 정도, 건강상태 등.	57	136	230	164	121	60	32	800
유형 4) 경제정보: 소득, 신용카드 및 통장계좌번호, 물품 구매내역, 대출 또는 담보설정 등	8	36	60	133	242	207	114	800
유형 5) 사회관계정보: 학력 및 학업성적, 친우관계, 동호회 활동 등 사회 활동 관련 정보	274	245	163	79	21	14	4	800
유형 6) 통신위치정보: 휴대폰 번호, 이메일주소, GPS 위치정보 등.	57	157	176	218	147	31	14	800
유형 7) 법적정보: 전과 범죄기록, 납세기록, 과태료 부과내역 등.	364	180	117	76	34	16	13	800
	800	800	800	800	800	800	800	

하위 집단별로 살펴보면, 저연령층 집단에서 상대적으로 '②고유정보', '⑥통신위치정보', '⑦법적정보'를 보다 중요하게 인식하고 있으며, 고연령층 집단에서는 '③의료건강정보', '④경제정보', '⑤사회관계정보'를 보다 중요하게 인식하고 있는 것으로 나타났다.

[표 5-24] 개인정보 유형별 중요도 순위

(단위 : 순위/7순위만점, N=800)



(단위 : 순위/7순위만점)

		사례수	①	②	③	④	⑤	⑥	⑦
전체		(800)	2.67	1.85	4.42	2.95	5.77	4.51	5.83
성 별	남성	(411)	2.64	1.91	4.39	3.04	5.68	4.55	5.79
	여성	(389)	2.71	1.78	4.46	2.85	5.86	4.47	5.87
연 령	20대	(190)	2.66	1.81	4.39	3.13	5.93	4.37	5.70
	30대	(220)	2.79	1.78	4.43	3.00	5.80	4.45	5.74
	40대	(210)	2.66	1.80	4.61	2.87	5.66	4.45	5.95
	50대	(130)	2.55	2.00	4.28	2.80	5.66	4.82	5.88
	60세 이상	(50)	2.60	2.08	4.02	2.72	5.72	4.78	6.08
권 역	서울	(163)	2.80	1.93	4.28	3.03	5.67	4.45	5.85
	경기/인천	(236)	2.61	1.85	4.57	2.83	5.80	4.45	5.89
	충청권	(87)	2.31	1.78	4.53	3.02	5.83	4.55	5.98
	전라권	(83)	2.95	1.86	4.46	2.90	5.81	4.40	5.63
	경상권	(197)	2.64	1.87	4.31	2.96	5.73	4.68	5.80
	기타(강원/제주)	(34)	2.97	1.50	4.32	3.18	6.00	4.41	5.62
결혼 여부	기혼	(486)	2.69	1.92	4.37	2.83	5.69	4.62	5.88
	미혼	(314)	2.65	1.75	4.50	3.12	5.88	4.34	5.75
세대주 여부	세대주	(318)	2.67	1.99	4.36	2.84	5.64	4.67	5.84
	비세대주	(168)	2.73	1.78	4.38	2.83	5.79	4.54	5.96
수입 가족수	1명 이하	(207)	2.64	1.86	4.47	2.84	5.76	4.57	5.87
	2명	(302)	2.77	1.72	4.54	2.91	5.85	4.48	5.73
	3명 이상	(291)	2.60	1.98	4.26	3.06	5.69	4.51	5.90

기혼자 자녀수	없음	(44)	2.59	1.84	4.45	2.98	5.98	4.27	5.89
	1명	(134)	2.84	1.87	4.40	2.75	5.69	4.61	5.85
	2명	(263)	2.67	1.93	4.37	2.81	5.68	4.70	5.84
	3명 이상	(45)	2.44	2.04	4.16	3.09	5.49	4.58	6.20
취업 여부별	취업	(575)	2.70	1.84	4.43	2.95	5.74	4.49	5.84
	미취업	(225)	2.60	1.87	4.38	2.93	5.85	4.56	5.81
총가족 수	2명 이하	(136)	2.74	1.78	4.46	2.88	5.96	4.36	5.82
	3~4명 이상	(555)	2.66	1.85	4.41	2.95	5.75	4.57	5.81
	5명 이상	(109)	2.68	1.95	4.44	3.01	5.60	4.40	5.92
직 업	자영업	(67)	2.70	2.22	4.34	2.75	5.51	4.51	5.97
	블루칼라	(85)	2.88	2.07	4.46	2.96	5.81	4.21	5.60
	화이트칼라	(415)	2.70	1.75	4.46	2.93	5.77	4.54	5.85
	가정주부	(104)	2.52	1.86	4.33	2.85	5.73	4.70	6.02
	학생	(56)	2.59	1.93	4.46	3.29	5.91	4.38	5.45
	무직/기타	(73)	2.53	1.71	4.32	3.07	5.90	4.56	5.90
학 력	고졸 이하	(148)	2.51	1.87	4.47	3.12	5.91	4.29	5.82
	대재/대졸	(555)	2.62	1.84	4.46	2.89	5.80	4.54	5.85
	대학원 이상	(97)	3.21	1.89	4.13	2.99	5.37	4.67	5.74
가구 소득	299만원 이하	(228)	2.64	1.75	4.42	3.02	5.82	4.54	5.80
	300~499만원	(312)	2.66	1.83	4.48	2.91	5.72	4.57	5.83
	500만원 이상	(260)	2.72	1.95	4.35	2.93	5.78	4.42	5.85
가구 통신 요금	월10만원 미만	(303)	2.54	1.85	4.48	2.99	5.76	4.49	5.89
	월10~20만원 미만	(294)	2.72	1.80	4.47	2.88	5.78	4.53	5.82
	월20만원 이상	(203)	2.81	1.92	4.26	2.98	5.76	4.52	5.75

* [문11] 귀하가 앞에서 개인정보보호에서 중요한 항목들에 대하여 순위를 매겨 주십시오.

7. 개인정보보호를 위한 금전적 부담 의사

(1) 개인정보 유출 방지를 위한 금전적 부담 의사

전체 응답자의 약 77%가 개인정보 유출 방지를 위해 금전적 부담을 할 의사

가 있다고 응답하였다. KISA(2007)의 연구에서는 전체 응답자의 약 61%가 개인정보 유출 방지를 위해 금전적 부담을 할 의사가 있다고 응답하였는데, 지불의사를 가진 적극적인 이용자가 증가하였다는 것은 국민들의 개인정보에 대한 보호 의지가 높아진 것을 의미한다. 한편 전체 응답자의 약 23%는 개인정보 유출 방지를 위해 단 1원도 부담을 할 의사가 없다고 응답하였다.

[표 5-25] 개인정보 유출 방지를 위한 금전적 부담 의사

	금전적 부담 의사 (%)
있음	617 (77.1)
없음	183 (22.9)
합계	800 (100)

[표 5-26] 개인정보 유출 방지를 위한 금전적 부담의사가 1원도 없는 응답자

	전체(A)	빈도(B)	비중(B/A)
전체	800	183	**23%**
유형 1) 기본인적 정보: 성명, 주소, 아이디 및 패스워드, 가족관계 등.	800	183	23%
유형 2) 고유정보: 주민등록번호, 여권번호, 운전면허 등록번호 등.	800	184	23%
유형 3) 의료건강정보: 병력, 병원 진료기록, 신체장애 정도, 건강상태 등.	800	308	39%
유형 4) 경제정보: 소득, 신용카드 및 통장계좌번호, 물품 구매내역, 대출 또는 담보설정 등	800	223	28%
유형 5) 사회관계정보: 학력 및 학업성적, 친우관계, 동호회 활동 등 사회 활동 관련 정보	800	433	**54%**
유형 6) 통신위치정보: 휴대폰 번호, 이메일주소, GPS 위치정보 등.	800	296	37%
유형 7) 법적정보: 전과 범죄기록, 납세기록, 과태료 부과내역 등.	800	423	**53%**

사회관계정보, 법적정보 유출 방지를 위하여 금전적 부담의사가 없는 응답자는 전체의 50%를 초과하였다. 이는 상대적 중요도 순위 응답에서와 유사한 결과이며, 이를 통해 사전적으로 사회관계정보 및 법적정보의 WTP는 0으로 판단할 수 있다. WTP에는 음의 값도 존재할 수 있다(Horowitz and McConnell,

2002). 예를 들어 친우회 혹은 동호회 활동은 사람들이 널리 홍보하고자 할 유인이 있기 때문으로 이에 대한 사례에 해당한다. 이는 본 조사에서도 나타난 결과이며, 사전적으로 사회관계정보와 법적정보의 경우 2명 가운데 1명 이상이 금전적 부담의사가 존재하지 않음으로 WTP가 0보다 크다고 말하기 어려울 수 있다. 만일 개인이 자신의 정보가 유출되어 효용을 누린다고 생각하면, 정보의 유출에 대하여 지원을 할 의사가 존재할 수도 있기 때문이다.

(2) 금전적 부담을 할 의사가 없는 이유

금전적으로 부담할 유인이 없다는 응답자 183명 가운데 약 41%인 75명이 개인정보의 유출은 기업에서 발생한 것이므로 기업이 모든 책임을 져야한다고 응답하였다. 개인정보의 유출은 금전적 부담으로 해결할 수 있는 문제가 아니다(24.6%), 경제적으로 부담이 크다(21.9%) 등이 뒤를 이었다. 개인정보의 유출은 기업에서 책임져야 한다는 의견이 많다는 것은 흥미로운 조사결과라고 할 수 있다. 즉 개인의 책임보다는 기업의 책임에 대한 요구가 높은 것이란 것을 확인할 수 있다.

[표 5-27] 개인정보 유출 방지를 위한 금전적 부담 의사가 없는 이유

		빈도	퍼센트	유효 퍼센트
유효	경제적으로 부담이 크다.	40	5.0	21.9
	개인정보 유출에 의한 피해가 크지 않으므로, 금전적 부담까지는 필요없다.	6	0.8	3.3
	개인정보의 유출은 기업에서 발생한 것이므로, 기업이 모든 책임을 져야한다.	75	9.4	41.0
	개인정보의 유출은 개인이 각자 알아서 해결해야 한다.	7	0.9	3.8
	개인정보의 유출은 금전적 부담으로 해결할 수 있는 문제가 아니다.	45	5.6	24.6
	기타	10	1.3	5.5
	합계	183	22.9	100.0
결측	시스템 결측값	617	77.1	
합계		800	100.0	

8. 가구별 개인정보 보호를 위한 WTP 추정

WTP를 산정하기 위해서는 두 가지 방법, 즉 지불의사가 전혀 없는 응답자를 포함하는 방법(Case 1)과 이를 포함하지 않는 방법(Case 2)이 존재(Horowitz and McConnell, 2002)한다. WTP가 없는 응답자를 포함하면 평가금액이 보수적이란 것은 한국해양수산개발원(2001)도 이미 지적한 바가 있다.

(1) (Case 1) 전체 개인정보에 대한 WTP가 1원도 없는 응답자를 포함하여 보수적으로 매월 지불의사액을 추정한 경우에는 4,260원으로 산출되었다. 이를 연간 금액으로 계산하면 WTP는 51,120원이다.

[표 5-28] 개인정보 유출 피해 예방에 대한 지불의사액

(단위: 원, 매월)

구 분		%	지불의사액
전 체		100	4,260
▨ 성 별 ▨	남 성	51.4	5,147
	여 성	48.6	3,352
▨ 결혼여부별 ▨	기 혼	60.8	4,444
	미 혼	39.3	4,026
▨ 학 력 별 ▨	고졸 이하	18.5	2,820
	대 학 교	69.4	4,189
	대학원이상	12.1	6,820
▨ 가구소득별 ▨	299만원 이하	28.5	2,922
	300-499 만원	39.0	4,217
	500만원 이상	32.5	5,511
▨가구통신요금별▨	월10만원 미만	37.9	2,725
	월10-20만원 미만	36.8	4,488
	월20만원 이상	25.4	6,251
▨ 연 령 ▨	20 대	23.8	4,427
	30 대	27.5	4,308
	40 대	26.3	4,189

	50 대	16.3	4,070
	60세 이상	6.3	3,951

주) WTP가 1원도 없는 응답자를 포함

남성이거나 기혼자의 WTP가 여성이거나 미혼자 보다 높게 추정되었으며, 학력이 높을수록, 가구소득이 높을수록, 그리고 가구의 통신료 지불이 많을수록 WTP는 높게 추정되었다. 또한, 연령이 높을수록 WTP가 낮아지는 것을 확인할 수 있다. 남성의 경우 매월 5,147원을 그리고 여성의 경우 매월 3,352원을 지불할 용의가 있는 것으로 나타났다. 기혼인 경우 미혼에 비하여 매월 약 418원을 더 지불할 용의가 있다. 그리고 통신요금을 매월 20만원 이상 납부하는 응답자는 매월 약 6,250원을 개인정보 유출피해 예방을 위해서 지불할 용의가 있는 것으로 조사되었다. 흥미로운 사실은 연령이 증가할수록 WTP가 감소하는 것으로 조사되어 60세 이상의 응답자는 매월 약 4천원 이하의 WTP가 있는 것으로 조사되었다.

(2) (Case 2) 개인정보에 대한 WTP가 1원도 없는 응답자 183명을 제외하는 경우에는 매월 WTP는 7,344원이었으며, 이를 연간 금액으로 계산하면 88,128원이었다. 학력이 높을수록, 가구소득이 높을수록, 그리고 가구의 통신료 지불이 많을수록, 연령이 높을수록 WTP가 높았다. WTP는 Case 1의 경우와 비교할 때 전반적으로 높게 나타났음으로 기존의 믿음 즉 WTP가 없는 응답자를 제외하면 평가금액이 증가할 것을 확인할 수 있었다. 그 외 흥미로운 사실은 응답자의 연령이 증가할수록 WTP가 case 1과 달리 증가하는 것으로 나타났으며, 이는 연령별 WTP가 없는 응답과 밀접한 관계가 있는 것으로 보인다.

[표 5-29] 지불의사액(지불의사가 없는 응답자 제외한 경우)

(단위: 원, 매월)

구 분		%	지불의사액
전 체		100	7,344
☒ 성 별 ☒	남 성	51.4	8,320
	여 성	48.6	6,332

▨ 결혼여부별 ▨	기 혼	60.8	7,548
	미 혼	39.3	7,060
▨ 학 력 별 ▨	고졸 이하	18.5	6,047
	대 학 교	69.4	7,238
	대학원이상	12.1	9,750
▨ 가구소득별 ▨	299만원 이하	28.5	6,681
	300-499 만원	39.0	7,298
	500만원 이상	32.5	7,915
▨가구통신요금별▨	월10만원 미만	37.9	5,937
	월10-20만원 미만	36.8	7,509
	월20만원 이상	25.4	9,081
▨ 연 령 ▨	20 대	23.8	7,343
	30 대	27.5	7,344
	40 대	26.3	7,345
	50 대	16.3	7,346
	60세 이상	6.3	7,347

주) WTP가 1원도 없는 응답자(183명) 제외

(3) 연령에 따른 WTP의 변화

WTP가 1원도 없는 응답자를 포함한 경우와 포함하지 않은 경우가 상이한 결과를 보이고 있다. 40대에 WTP가 1원도 없는 응답자가 비율이 32%로 가장 높고, 20대와 60대는 각각 16%, 18%로 낮았다. 40대를 정점으로 연령이 증가하거나 혹은 감소하거나 WTP는 감소하는 것으로 나타났다.

[표 5-30] 연령별 WTP가 없는 응답자 비율

연령	응답자(A)	지불의사 없는 응답자(B)	비율(B/A)
20 대	190	31	16%
30 대	220	52	24%
40 대	210	68	32%
50 대	130	23	18%
60세 이상	50	9	18%

9. 개인정보 보호를 위한 사회적 지불의사 비용 추정

사회적 WTP를 가계기준(2011.11월 행안부 기준)으로 보면 보수적으로 연간 1.0~1.3조원으로 추정된다. 이 금액은 지불의사가 없는 응답자를 고려했는지에 따라 다소 차이가 있다.

1안	월지불액 * 12개월 * 가계수 = 4,260원 * 12월 * 20,019,850 가구 = 1조 234억원
2안 (지불의사가 없는 응답자 고려)	월지불액 * 12개월 * 가계수 * 지불의사 있는 응답자 비중 = 7,3440원 * 12월 * 20,019,850가구 * (1-23%)= 1조 3,585억원

사회적 WTP를 개인기준(2013년 통계청 인구추계)으로 평가하면 연간 2.0~2.6조원으로 추정된다. 이 금액 또한 지불의사가 없는 응답자를 고려했는지에 따라 다소 차이가 있다.

1안	월지불액 * 12개월 * 20세 이상 인구수 = 4,260원 * 12월 * 39,499,131명 = 2조 191억원
2안 (지불의사가 없는 응답자 고려)	월지불액 * 12개월 * 20세 이상 인구수 * 지불의사 있는 응답자 비중 = 7,344원 * 12월 * 39,499,131명 * (1-23%)= 2조 6,804억원

10. 개인정보 유형별 지불의사 비용 추정

유형별 WTP의 경우 고유정보에 대한 지불의사액이 2,948원으로 가장 높은 것으로 조사되었고, 다음으로 기본인적정보, 경제정보로 나타났다. 사회관계정보와 법적정보는 응답자의 과반수 이상이 단 1원도 지불할 의사가 없다고 응답한 것을 반영하여 0원으로 추정하였다.

[표 5-31] 개인정보 유형별 WTP

(단위: 원, 매월)

	WTP
유형 1) 기본인적 정보: 성명, 주소, 아이디 및 패스워드, 가족관계 등.	**2,524**
유형 2) 고유정보: 주민등록번호, 여권번호, 운전면허 등록번호 등.	**2,948**
유형 3) 의료건강정보: 병력, 병원 진료기록, 신체장애 정도, 건강상태 등.	**113**
유형 4) 경제정보: 소득, 신용카드 및 통장계좌번호, 물품 구매내역, 대출 또는 담보설정 등	**2,466**
유형 5) 사회관계정보: 학력 및 학업성적, 친우관계, 동호회 활동 등 사회활동 관련 정보	**0**
유형 6) 통신위치정보: 휴대폰 번호, 이메일주소, GPS 위치정보 등.	**418**
유형 7) 법적정보: 전과 범죄기록, 납세기록, 과태료 부과내역 등.	**0**
총 금액	**8,469**

전체 유형별 WTP의 합은 8,649원으로 전체 개인정보 유출을 방지하기 위한 WTP 값을 훨씬 상회하고 있다. 이는 곽승준 외(2001)이 제기하고 있는 Kahneman and Knetshce의 포함효과(embedding effect) 가운데 합산문제(adding-up problem)와 일치[24]함을 보여준다. 다시 말해 개인정보의 유형별 WTP의 합과 개인정보 전체의 WTP가 동일하지 않은 것을 확인할 수 있었다.

개인정보 유출 피해 예방에 대한 정보 유형별 지불의사액을 살펴보면 다음과 같다.

(단위: 원, 매월)

구 분		기본인적 정보 (유형 1)	고유정보 (유형 2)	의료건강 정보 (유형 3)	경제 정보 (유형 4)	통신위치 정보 (유형 6)
전 체		2,524	2,948	113	2,466	418
▨ 성 별 ▨	남 성	3,174	3,664	676	2,696	859
	여 성	1,856	2,205	0	2,227	0

24) 곽승준 외 (2001)는 지리산 반달곰의 예로 합산문제를 지적한다. 즉 "지리산에 반달곰 10마리가 생존해 있다고 가정하자, CVM을 통해 반달곰의 가치를 평가할 경우 1마리의 가치를 평가하여 이를 10배할 경우 가치는 반달곰 10마리 가치를 한꺼번에 평가할 경우의 가치보다 훨씬 크게 나타난다."

▨ 결혼여부별 ▨	기 혼	3,394	3,485	423	2,779	490
	미 혼	1,346	2,214	0	2,051	335
▨ 학 력 별 ▨	고졸 이하	2,511	2,447	0	2,048	0
	대 학 교	2,427	2,856	33	2,415	620
	대학원이상	3,132	4,285	1,884	3,363	385
▨ 가구소득별 ▨	299만원 이하	1,497	1,705	0	1,452	0
	300-499 만원	2,493	2,915	95	2,442	396
	500만원 이상	3,489	4,126	1,096	3,432	1,148
▨가구통신요금별▨	월10만원 미만	1,686	1,979	0	1,529	0
	월10-20만원 미만	2,647	3,092	286	2,610	520
	월20만원 이상	3,608	4,205	1,523	3,692	1,259
▨ 연 령 ▨	20 대	2,001	2,746	203	2,593	816
	30 대	2,363	2,884	137	2,505	525
	40 대	2,725	3,021	72	2,416	233
	50 대	3,088	3,159	7	2,327	0
	60세 이상	3,450	3,297	0	2,239	0

주) WTP가 1원도 없는 응답자를 포함

제6장 결론 : 정책 제언

제1절 개인정보 침해에 따른 비용최소화를 위한 기업의 대응

2013년 2월 방송통신위원회가 발표한 <2012년 정보보호 실태조사 결과>에 따르면 민간기업들 중 정보보호에 투자하고 있는 기업이 26.1%로서 매우 저조한 것으로 나타났다. 또한 정보보호 지출이 없는 기업들 중 81.8%가 "필요성을 느끼지 못한다."고 답한 것으로 알려져 기업들의 정보보호에 관한 인식수준이 매우 미흡한 것으로 나타났다. 이는 동 보고서에서 인터넷 이용자의 98.7%가 '정보보호'가 중요하며, 99.2%가 '개인정보보호'가 중요하다고 인식하고 있는 것과는 상반된 결과이기도 하다.

이 같은 상황이 벌어진 이유는 기업들이 정보보호에 투자하는 비용이 그로 인해 얻게 되는 실익에 비해 적다고 느끼기 때문으로 생각할 수 있는데 이러한 사고방식은 장기적인 관점에서 볼 때 매우 큰 위험성을 내포하고 있다.

본 보고서에서 계산한 바에 의하면 개인정보 유출로 인해 발생하는 기업 측면의 손실이 매년 약 2,800 ~ 3,750억 원 정도로 추정되고 있다. 이는 한 해 평균 천만 건이 훌쩍 넘어가는 대형 유출사고가 일어나는 것에 비하면 작아 보일수도 있다. 하지만 이러한 결과는 개인정보 유출로 인해 일어나는 피해가 적어서가 아니라 기업들이 그 피해를 온전히 부담하지 못한 채 상당부분을 사회와 개인의 몫으로 전가하고 있는데서 비롯된다. 예를 들어 기업의 책임으로 인해 발생한 피해액을 개인에게 보상하는 법적 보상금을 살펴보자. 지난 몇 년 동안 수천만 건에 이르는 대형 유출사고가 끊임없이 일어났지만 실제 법적 보상이 일어난 경우는 거의 없다. 이는 기업의 책임이 없다기 보다는 비정상적인 대형 유출사고로 인해 기업이 물어야하는 법적 보상금이 실제 배상될 경우 기업의 생존이 위협받을 만큼의 거대규모이기에 법원이 매우 보수적인 판결을 내릴 수밖에 없는 데서 기인한다고도 볼 수 있다. 약 1,125만 건에 이르는 GS 칼텍스의 유출사고만 보더라도 개인정보분쟁조정위원회의 기준인 평균 20만 원 정도의 보상금을 적용했을 시 기업이 개인에게 보상해야 하는 금액이 2조 2,500억 원에 이른다.

이는 한 기업의 생존을 위협할 정도의 거대한 규모이며, 그 결과 법원에서는 기업에 책임이 있음에도 불구하고 보상판결을 내리지 않았다.

문제는 언제까지 이러한 상황이 지속될 수 있느냐다. 미국과는 달리 기업이 개인정보 유출로 인한 피해액을 고스란히 보상해야 하며 정신적 피해보상까지 지급해야 하는 국내의 상황을 볼 때 대형 유출사고로 인한 피해액은 천문학적일 수밖에 없다. 이러한 상황을 기업의 영속성을 지켜주기 위해 책임을 미루는 행위는 정책적으로 지속성을 가질 수 없다. 결국 특정 시점을 기준으로 보상판결은 시작될 것이며, 이는 좋은 운영성과를 내던 기업 하나를 한 순간에 파산시킬 만큼 큰 피해로 다가올 것이다. 결국 기업의 경우 직접적인 피해액뿐만 아니라 직접적으로 드러나지 않는 잠재적인 비용까지 고려해야 하며, 눈앞의 이익에만 집중해서 기업의 영속성을 위협하는 현재의 인식을 바꿔야 한다.

동시에 이러한 노력은 기업뿐만 아니라 정부에서도 동시에 수반되어야 한다. 본 연구에서는 데이터 확보와 관련하여 정부의 법제화 및 강력한 시행에 관해 이야기하고 싶다. 일본의 경우 이미 2004년에 개인정보 유출사고가 일어나면 이를 공식적으로 알려야 하는 법이 제정하였으며 이를 강력하게 시행하고 있다. 그 결과 개인정보 유출 사고를 막기 위한 기업들의 노력이 커졌으며, 여기서 수집된 데이터를 바탕으로 정확한 피해액 집계가 가능하기 때문에 정책결정에 있어 큰 도움이 되고 있다.

한 예로 일본의 JNSA(Japan Network Security Association)는 2009년 기준으로 약 1,500건에 이르는 방대한 기업의 개인정보 유출 데이터를 확보했고 이를 자체 개발한 정보의 기본 가치 추정 모델인 'JO모델'(JNSA Damage Operation Model for Individual Information Leak)에 대입해서 그 피해액을 추정하였다. 이는 한 해 언론을 통해 알려진 개인정보 유출사고에 관한 데이터가 수 십 건 남짓한 국내의 사례와 대조되는 모습이다. 현재 개인정보 유출과 관련된 데이터가 매우 부족하고 기업들이 사고가 일어나도 조용히 넘어가려하는 국내의 상황에 비춰볼 때 일본의 사례는 큰 시사점을 주고 있다.

국내에도 일본과 같이 개인정보 유출사건이 일어나면 이를 공지하도록 하는 법이 시행되고는 있지만 그 실효성에 있어서는 문제가 있어 보이며, 이는 저조한 신고건수를 통해 증명되고 있다. 따라서 이러한 법제를 보다 활성화할 방안

을 찾는 일이 필요해 보인다. 이는 개인정보 보호에 대한 사회적 인식을 높이고 기업들이 개인정보 유출 방지를 위해 노력하게 할 것이며 더 나은 정책을 수립할 수 있는 귀중한 데이터를 확보할 수 있는 좋은 방안이다. 나아가 개인정보 유출로 인한 피해를 줄이는데도 큰 도움이 될 것이다.

마지막으로 정부 차원의 국가적 대응을 제안하고자 한다. 실제 사고가 일어날 경우 피해자들은 기업에 직접 번거로운 소송을 걸어야 보상을 받을 수 있으며, 실제 보상판결도 잘 이루어지지 않고 있다. 수많은 사람들이 정보 유출로 인해 피해를 입고 있는데 이에 대한 보상이 잘 이루어지지 않고 있는 것이며 이러한 사실을 기업들도 인지하고 있기 때문에 정보보호에 관한 투자도 미흡하고, 인식 개선이 되지 않고 있는 실정이다. 실제 미국의 경우 협회를 설립해서 개인정보 유출 사건이 일어난 기업에게 벌금과 과태료를 부과하고 이를 기금으로 만들어 정보보호 관련 사업에 쓴다. 이 경우 잘못한 기업들이 지불하는 비용이 똑같은 사건이 재발하지 않도록 하는데 쓰이기 때문에 사회 전체에 혜택이 돌아가며, 기업의 경우 경각심을 가질 여지가 충분하다. 국내에서도 국가적으로 벌금이나 과태료를 부과하고 이를 기금 등의 형태로 만들어 정보보호와 관련된 사업에 사용한다면 사회 전체가 혜택을 받을 수 있으며, 부족한 정보보호 관련 예산도 확충할 수 있다. 또한 기업의 경우 더 이상 개인정보 유출에 미온적으로 대처하지 못할 것이며, 사회적인 인식도 크게 개선될 것으로 판단된다.

제2절 정책적 시사점

본 연구에서는 우리나라 전체가계가 매년 개인정보 보호를 위해 지불하고자 하는 WTP를 추정하였다. 기존문헌에서 한걸음 나아가서 보수적으로 WTP를 추정하기 위하여 노력하였다. 즉 개인정보 유·노출에 대한 객관적 정보를 제공하고, 가구소득이 제한되어 있음으로 개인정보 지불은 지출감소와 이어진다는 것을 명시적으로 설명하였다. 본 연구를 통해 얻을 수 있는 정책적 시사점은 다음과 같다.

첫째, 정부와 민간 기업에서는 개인정보보호 측면에서 국민의 기대 수준에 맞는 투자를 해야 한다는 것이다. 본 연구에서는 기존 문헌과 달리 가구기준으로 우리나라 전체가구가 개인정보 보호를 위하여 지불하고자 하는 금액을 이중양분선택법을 이용하여 WTP를 2013년 현재 연간 최소 1조원으로 추정하였다. 이는 우리나라 국민들은 개인정보 보호를 통해 얻는 편익을 위해서 연간 최소 1조원 정도를 투자해서라도 개인정보를 보호하겠다는 의미이다. 즉, 개인정보보호를 지키기 위해 울타리 비용으로 연간 1조원 정도를 투자하겠다는 것이다.

이해춘 외(2008)는 개인정보 유출로 피해 가능성이 있는 응답자가 기업이 제시하는 손해 배상을 수용하는 WTA(Willingness to Accept)를 화폐액으로 추정하여 개인정보 유출의 잠재적 손실액을 추정하였다. 이 연구의 결과에서 이용자는 자신의 명의가 도용되어 특정 온라인 게임사이트에 가입된 사실을 알고, 1인당 약 750만원의 배상금을 받기를 원하는 것으로 나타났다. 이러한 결과를 통해 이용자는 개인정보가 침해당할 경우 기업이 제시하는 배상금액을 받아들이기는 쉽지 않는 성향에 의해 WTA에 의한 추정값은 상대적으로 과추정(over-estimate)될 수 있는 여지가 많다는 것을 알 수 있다.

앞서 밝힌 것 처럼 본 연구는 개인정보 침해가 발생한 경우 정보보유자들이 요구하는 WTA를 추정하는 것과는 달리 본 연구에서는 개인정보 유출과 노출을 예방하기 위해 투자를 하고자 하는 WTP를 추정하였다. 또한 WTP를 최대한 보수적으로 도출하기 위해서 개인정보 유·노출에 대한 객관적인 정보를 제공하고, 설문조사시 응답자의 소득이 제한되어 있으며, 그 소득은 다른 여러 용도로

도 지출되어야 함을 명시적으로 설명하고, 가구기준으로 WTP를 질의하였다. 이러한 과정을 통해 도출된 금액, 즉 연간 지불가능한 WTP 금액이 1조원이라는 것은 당장 국민들로부터 확보할 수 있는 비용이나 마찬가지기 때문에 적은 비용이 아니라고 판단된다.

본 연구에서 추정한 개인정보 보호를 위한 지불의사 금액은 일반인을 대상으로한 설문에 근거한다. 이에 반해 우리나라 중앙행정기관의 개인정보 보호예산은 2013년 현재 578억원에 불과한 상황이다. 다행인 것은 2012년에 비하여 31%가 증가한 것이지만 우리나라 가계가 지불의사를 가지고 보호하고자 하는 가치(WTP)에 턱없이 미달하고 있다는 것을 확인할 수 있다. 물론 본 연구에서 계산한 WTP의 경우 개인과 공공부문이 아닌 기업측면에서도 부담할 수 있다는 것을 인식할 필요가 있다. 금전적으로 부담할 의지가 없다는 이용자의 약 41%가 개인정보 유출에 대하여 기업의 책임을 강조하였다는 점에서 기업의 역할도 크다. 결론적으로, 국민들이 생각하고 있는 개인정보 보호를 위한 투자가치 수준과 정부와 민간 기업에서 이를 보호하기 위해 투자하고 있는 수준과는 크게 차이가 있는 것으로 나타났다. 따라서 정부와 민간기업에서는 국민의 개인정보 보호를 위하여 국민들의 기대 수준에 맞도록 추가적인 투자와 지속적인 사업추진이 필요할 것으로 판단된다.

< 정부 개인정보 보호예산 및 사업규모 >

연도	사업 수	예산 (단위: 백만원)			
		합계	정책·제도 개선	시스템 운영	교육·홍보
2012	323개	44,114	5,000	37,058	2,056
2013	323개	57,862	2,771	52,927	2,164

계획 작성대상 : 17부, 3처, 17청, 6위원회(방통위, 원자력위, 금융위, 공정위, 권익위, 인권위), 국정원, 감사원, 총리실 등 46개 중앙행정기관

둘째, 국민들은 주민번호, 여권번호 등 기본적인 고유정보에 가장 민감하기 때문에 이를 우선적으로 보호할 필요가 있다는 것이다. 국민들은 개인정보 유형별 상대적 중요도에 있어서 뿐만 아니라 개별 WTP 금액에서도 고유정보, 기본인적

정보, 그리고 경제정보 순서로 중요하다고 인식함을 알 수 있었다. 물론 법적정보와 의료건강정보의 경우 해당정보에 민감한 개인들의 경우 그 정보에 대한 중요성을 강조할 수 있다. 그러나 일반인의 경우 상대적으로 법적정보와 의료건강정보 보다는 기본인적정보, 고유정보, 그리고 경제정보에 대한 보호에 관심이 높다는 것을 알 수 있었다. 특히 고유정보 즉 주민등록번호, 여권번호, 운전면허등록번호 등에 대한 WTP가 기본인적정보와 경제정보에 대한 WTP 보다 높다는 것은 결국 이를 보호하기 위한 투자를 중요하게 인식하고 있다는 것을 간접적으로 보여준다고 볼 수 있다.

뿐만 아니라 본론에서 지적한 것처럼 개별 정보에 대한 WTP의 합이 전체 개인정보의 WTP로 직결된다는 해석에 대한 경계도 필요하다. 그리고 법적정보와 의료건강정보에 대한 투자를 기본인적정보, 고유정보, 그리고 경제정보에 대한 투자보다 줄여야 한다고 해석될 수는 없을 것이다. 관련 정보에 대한 이슈가 존재하는 개인정보 보유자들은 그렇지 않는 개인정보 보유자에 비해서 관련 정보의 보호의 중요성을 더 높게 평가할 수 있기 때문이다.

셋째, 사회적 약자들을 대상으로 개인정보 보호의 중요성에 대해 홍보를 강화할 필요가 있다. 개인정보 보호를 위한 WTP는 통신요금이 높을수록 그리고 소득이 높으면 증가하였다. 또한 남성이 여성에 비하여 개인정보 보호에 대한 WTP를 높게 평가하는 것으로 나타났다. 연령대가 낮은 20~30대가 60대 보다 WTP를 높게 평가하였다. 학력이 높은 사람도 낮은 사람에 비해 WTP를 높게 평가하였다.

본 연구결과에서 나온 것처럼 여성, 노인, 저소득층의 국민들이 상대적으로 개인정보 보호를 통해 얻는 편익을 낮게 판단하고 있다는 것은 지불능력이 상대적으로 낮기 때문이기도 하고, 개인정보 침해로 인한 피해를 간과하고 있을 수도 있기 때문이다. 따라서 개인정보의 가치가 개인의 특성과 별개로 모든 개인에게 동등하다고 가정하면, 이러한 사회적 약자들을 대상으로 개인정보 보호에 대해 쉽게 이해할 수 있도록 홍보하고 스스로 지킬 수 있는 자기정보통제력을 키워주는 정책이 필요하다고 판단된다.

넷째, 정부・공공기관과 민간기업에서는 보유하고 있는 개인정보량에 비례해서 투자 규모를 차별화할 필요가 있다는 것이다. 현재 정보통신망에서는 개인정

보보호관리체계(PIMS) 인증에 대해 권고하고 있고, 개인정보보호법에서도 “개인정보보호 인증마크 제도”를 권고하고 있다. 그러나 이제는 보유한 개인정보량에 따라 개인정보량이 많은 기업이나 정부・공공기관에 대해서는 보유한 개인정보의 가치에 적합한 보호조치를 취하도록 의무사항으로 한다거나, 일정 수준 이상의 투자를 하도록 할 필요가 있다. 이제는 국민들도 자신의 개인정보를 보호하기 위한 적극적 의지가 강해진 상황이다. 따라서 이러한 국민들의 눈높이에 맞도록 개인정보를 보호하기 위한 차별화된 조치는 필요하다고 판단된다.

< Appendix >

1. 개인정보 침해에 따른 사회적 비용분석을 위한 설문조사

2. Ponemon 보고서 (2013)

3. 일본 JSNA 보고서 (2008)

개인정보 침해에 따른 사회적 비용분석을 위한 설문조사

안녕하십니까?

디지털 경제에 핵심자원으로 개인정보의 활용이 증가하고 있습니다. 그러나 이에 따른 부작용인 개인정보침해가 지속적으로 발생하고 있습니다.

개인정보 유출에 따른 사회적 비용을 수량적으로 **추정**하고, 이를 통하여 개인정보 유출에 따른 피해의 심각성, 개인정보 보호의 중요성 그리고 개인정보 보호를 위한 정책제언을 위하여 **상명대학교,** 개인정보보호위원회, 그리고 개인정보보호협회에서는 공동으로 **본 설문을 실시**하고 있습니다. 본 설문은 만 20세 이상 75세 이하를 대상으로 하고 있습니다.

조사결과는 학술적 목적으로만 사용되며, **반드시 조사와 연구에 관련된 목적에만 사용**될 것이며, **비밀은 철저히 보장**될 것임을 약속드립니다. 설문조사에 응해 주셔서 감사드리며, 귀하의 평안과 번창하심을 기원합니다.

2013년 8 월

☎ 문의전화 (02)

1. 개인정보에 대한 인지도 조사

개인정보는 지식정보사회에서 우리가 편리한 서비스를 제공받기 위해 기업이나 공공기관에 최소한으로 제공해야 하는 정보입니다. 이름, 주민등록번호, 주소 등과 같은 개인정보를 이용하여 기업이나 공공기관은 우리가 요청한 사항을 신속히 처리해 주고 다양한 서비스를 제공해 주고 있습니다.

예를 들어 은행에서는 우리가 거래한 내역이나 잔고를 보고, 우리에게 가장 적합한 금융상품을 추천해 주기도 합니다. 병원에서는 지금까지의 진료기록을 보고, 현재 질병이 어떤 상태인지를 진단해 줍니다. 경찰청과 소방센터에서는 위급한 상황 시 우리의 위치 정보를 보고 긴급지원서비스를 제공하기도 합니다.

본 설문에서는 우리가 기업이나 공공기관에 제공하는 개인정보를 다음과 같이 분류하고자 합니다.

유형 1) 기본인적 정보: 성명, 생년월일, 주소, 가족관계 등
유형 2) 고유식별 정보: 주민등록번호, 여권번호, 운전면허번호 등
유형 3) 의료·건강 정보: 병력, 진료기록, 신체장애, 건강상태 등
유형 4) 경제 정보: 소득, 신용카드 및 통장계좌번호, 물품구매내역, 대출 또는 담보설정 등
유형 5) 사회·관계 정보: 학력 및 학업성적, 친우관계, 종교, 동호회 등 모임 가입·활동 직장 등
유형 6) 통신·위치 정보: 휴대폰번호, 이메일주소, GPS 위치정보 등
유형 7) 법적 정보: 전과·범죄기록, 납세기록, 과태료 내역 등
유형 8) 바이오 정보: DNA, 지문, 얼굴, 홍체 등

그러나 은행, 병원, 경찰청 등 기업이나 공공기관 제공한 개인정보를 '**본인의 동의 없이** 수집하거나 제3자에게 제공하여' **개인정보 및 프라이버시 침해**가 발생하기도 합니다. ' 정보통신망에 의하여 처리되는 개인정보의 분실, 도난, 유출, 변조 등으로 인하여 개인의 사생활이 침해'되는 것을 **개인정보 및 프라이버시 침해**라 지칭하기도 합니다.

개인정보 및 프라이버시 침해가 발생하는 경우 개인정보를 제공한 해당 당사자는 상당 수준의 정신적 물질적 손해를 볼 수 있습니다. 또한 일부에서는 개인정보 침해의 심각성은 이제 개인의 문제가 아니라 사회적 문제로 이슈화되기 시작하였다고 주장하기도 합니다.

문 1. 귀하는 '개인정보침해'의 의미에 대해서 얼마나 잘 알고 있습니까?

1. 전혀 모른다　2. 잘 모른다　3. 보통이다
4. 잘 아는 편이다　5. 매우 잘 알고 있다

문 2. 귀하는 현재 우리 사회에서의 개인정보 침해가 얼마나 위험하다고(위협적이라고) 생각하십니까?

1. 전혀 위험하지 않다　2. 별로 위험하지 않다　3. 보통이다
4. 위험한 편이다　5. 매우 위험하다

문 3) 지난 1년 간 귀하는 온라인을 포함한 일상생황에서 개인정보 또는 프라이버시 침해로 인한 피해를 입으신 경험이 있으십니까?

1. 예 => 문 3-1)로
2. 아니오 => 문 4)으로

문 3-1) **(문 3)에서 1로 답한 경우에 한하여)** 귀하는 어떤 유형의 개인정보/프라이버시 침해를 경험하셨습니까?

피해 내용	피해 유무
① 사업자의 관리 소홀로 개인정보가 유출된 경우	1. 있음 2. 없음
② 사업자가 귀하의 동의 없이 개인정보를 본래 목적 이외의 용도로 이용하거나 제3자에게 제공한 경우	1. 있음 2. 없음
③ 사업자가 귀하의 개인정보를 무단 수집하여 텔레마케팅 목적으로 이용하였거나 무단으로 회원으로 가입시킨 경우	1. 있음 2. 없음
④ 주민번호 도용으로 웹사이트 회원가입이 되지 않았거나 경제적인 피해를 입은 경우	1. 있음 2. 없음
⑤ ID 및 비밀번호 도용으로 게임 아이템, 사이버머니, 캐릭터 등을 도난 당한 경우	1. 있음 2. 없음
⑥ 기타 (적을것)	1. 있음 2. 없음

2. 개인정보보호에 대한 중요도 조사

문 4) 귀하는 다음에 대하여 얼마나 중요하다고 생각하십니까? 중요한 정도에 대해 하나씩만 ○표 표시해 주십시오.

	매우 그렇지 않다	그렇지 않다	보통이다	그렇다	매우 그렇다
개인정보 보호는 중요하다.	1	2	3	4	5
해킹 및 바이러스로 인한 사회 전반의 피해는 심각하다.	1	2	3	4	5
개인정보 및 프라이버시 침해로 인한 사회 전반의 피해는 심각하다.	1	2	3	4	5
휴대전화 스팸, 스마트폰 스팸, 스팸메일로 인한 사회 전반의 피해는 심각하다.	1	2	3	4	5

보이스 피싱으로 인한 사회 전반의 피해는 심각하다.	1	2	3	4	5
웹사이트에 회원가입, 경품응모, 물품구입 등을 위해 개인정보를 제공하실 때, 해당 사이트의 개인정보 관리 수준을 확인한다.	1	2	3	4	5
특정 웹사이트의 회원을 해지할 때 개인정보 파기여부를 확인한다.	1	2	3	4	5
웹사이트에 게시되어 있는 '이용약관'이나 '개인정보 보호정책' 등은 나의 개인정보보호에 도움이 된다	1	2	3	4	5

문 5) 여러분들이 제공하는 개인정보는 가치를 가질 수 있습니다. 귀하께서는 각각의 가치들이 얼마나 중요하다고 생각하십니까? 중요한 정도에 대해 하나씩만 ○표 표시해 주십시오.

	가치가 없다	거의 가치가 없다	가치가 있다	가치가 높다	매우 가치가 높다
유형 1) 기본인적 정보: 성명, 생년월일, 주소, 가족관계 등	1	2	3	4	5
유형 2) 고유식별 정보: 주민등록번호, 여권번호, 운전면허번호 등	1	2	3	4	5
유형 3) 의료·건강 정보: 병력, 진료기록, 신체장애, 건강상태 등	1	2	3	4	5
유형 4) 경제 정보: 소득, 신용카드 및 통장계좌번호, 물품구매내역, 대출 또는 담보설정 등	1	2	3	4	5
유형 5) 사회·관계 정보: 학력 및 학업성적, 친우관계, 종교, 동호회 등 모임 가입·활동 직장 등	1	2	3	4	5
유형 6) 통신·위치 정보: 휴대폰번호, 이메일주소, GPS 위치정보 등	1	2	3	4	5
유형 7) 법적 정보: 전과·범죄기록, 납세기록, 과태료 내역 등	1	2	3	4	5
유형 8) 바이오 정보: DNA, 지문, 얼굴, 홍체 등	1	2	3	4	5

3. 개인정보보호를 위한 지불의사액에 관한 질문

인터넷 등을 통해 개인정보가 침해되면 해당 당사자는 상당 수준의 정신적 물질적 손해를 볼 수 있습니다. 이러한 개인정보 침해의 심각성은 이제 개인의 문제가 아니라 사회적 문제로 이슈화되기 시작했습니다.

예를 들어 안전행정부에 따르면 개인정보침해신고센터로 접수된 개인정보 침해 신고 및 상담건수는 2012년 약 17만 건으로 이는 2011년과 비교하여 36%가 증가하였습니다.

개인정보를 보호하고 관리하기 위해서는 투자가 필요하며 많은 사람들이 이에 동의하는 경우 개인정보 유출 및 누출을 효과적으로 예방할 수 있다고 가정하십시오. 또한 귀하의 소득은 제한되어 있으며, 그 소득은 다른 여러 용도에 지출되어야 합니다. **향후 10년 동안 매달** 개인정보의 유출과 누출을 예방하기 위하여 얼마를 매달 지불하실 의사가 있으신지 여쭙고자 합니다.

제시금액은 1,000원, 2,000원, 3,000원, 4,000원, 5,000원, 6,000원, 7,000원, 8,000원, 9,000원, 10,000원으로 각 구간은 동일한 비중이 유지

문 8) 귀하의 가구는 개인정보 유출을 완전히 차단하기 위하여 향후 10년간 매월 부담해야 한다고 가정해 보십시오. 매월 <제시금액>을 추가적으로 지불하실 의사가 있습니까? 만약 귀하의 가구가 이 금액을 지불하시지 않는다면 개인정보는 완전히 보호되기 어렵습니다.
(1) 있다 - - - - - - - - > [문 9로]
(2) 없다 - - - - - - - - > [문 10로]

문 9). 그렇다면 귀하의 가구는 개인정보 유출을 완전히 차단하기 위하여 매월 <2 배가격>을 지불하실
의사가 있습니까? 이 역시 귀하의 가구가 이 금액을 지불하시지 않는다면 개인정보는 완전히 보호되기 어렵습니다.
(1) 있다 - - - - - - - - > [문 12로]
(2) 없다 - - - - - - - - > [문 12로]

문 10) 그렇다면 귀하의 가구는 개인정보 유출을 완전히 차단하기 위하여 매월 <1/2 가격>을 지불하실 의사가 있습니까? 이 역시 귀하의 가구가 이 금액을 지불하시지 않는다면 개인정보는 완전히 보호되기 어렵습니다.
(1) 있다 - - - - - - - - > [문 12로]
(2) 없다 - - - - - - - - > [문 11로]

문 11) 그렇다면 귀하의 가구는 단 1원도 지불하실 의사가 없습니까?
(1) 지불할 의사가 있다 - - - - - - - - > [문 12로]

(2) 지불할 의사가 없다 - - - - - - - - > [문 13로]

문 12). 그렇다면 귀하의 가구가 개인정보보호를 매월 지불하시고자 하는 최대 금액은 얼마입니까?
(　　)원

문 13). 귀하가 앞에서 개인정보보호를 일정 금액을 기꺼이 내고자 하신 목적 중 다음의 항목들에 대해 순위를 매겨 주십시오. 그런 다음 각 항목에 대한 점수를 매기시되 귀하의 가구 입장에서 생각해 주십시오. 가장 중요하다고 생각하는 항목의 점수는 100점입니다.

항목	순위	점수
유형 1) 기본인적 정보: 성명, 생년월일, 주소, 가족관계 등		
유형 2) 고유식별 정보: 주민등록번호, 여권번호, 운전면허번호 등		
유형 3) 의료·건강 정보: 병력, 진료기록, 신체장애, 건강상태 등		
유형 4) 경제 정보: 소득, 신용카드 및 통장계좌번호, 물품구매내역, 대출 또는 담보설정 등		
유형 5) 사회·관계 정보: 학력 및 학업성적, 친우관계, 종교, 동호회 등 모임 가입·활동 직장 등		
유형 6) 통신·위치 정보: 휴대폰번호, 이메일주소, GPS 위치정보 등		
유형 7) 법적 정보: 전과·범죄기록, 납세기록, 과태료 내역 등		
유형 8) 바이오 정보: DNA, 지문, 얼굴, 홍체 등		

문 13).귀하가 개인정보 보호를 위하여 단 1원도 지불하실 의사가 없는 가장 중요한 이유는 무엇입니까 ?
1. 경제적으로 부담이 크다.
2. 개인정보 유출에 의한 피해가 크지 않으므로, 금전적 부담까지는 필요 없다.
3. 개인정보의 유출은 기업에서 발생한 것이므로, 기업이 모든 책임을 져야한다.
4. 개인정보의 유출은 개인이 각자 알아서 해결해야 한다.
5. 개인정보의 유출은 금전적 부담으로 해결할 수 있는 문제가 아니다.
6. 기타 (　　)

4. 수용의사액에 관한 질문

다음의 경우를 가정하여 보십시오. 귀하의 개인정보를 보유하고 있는 기업이, 개인정보를 잘못 관리하여 귀하의 개인정보가 인터넷에 유노출 되었습니다. 이로 인하여 귀하는 앞으로 정신적 피해뿐만 아니라 재산적 손해를 볼 수도 있습니다.

앞에서 문 8에서 제시금액은 1,000원인 경우 10만원, 2,000원 경우 20만원, 3,000원인 경우 30만원, 4,000원인 경우 40만원, 5,000원인 경우 50만원, 6,000원인 경우 60만원, 7,000원인 경우 70만원, 8,000원인 경우 80만원, 9,000원인 경우 90만원, 10,000원인 경우 100만원으로 제시

유형 1) 기본인적 정보(성명, 생년월일, 주소, 가족관계 등)가 유출되었을 때,
문 14) 개인정보 유·노출과 관련하여 귀하가 당할 수 있는 정신적·재산적 손해에 대하여 개인정보를 유출한 기업이 위자료로 <제시금액>을 제공한다고 하면, 이를 수용할 의사가 있습니까?

(1) 있다 - - - - - - - - > [문 15로]
(2) 없다 - - - - - - - - > [문 16로]

문 15). 그렇다면 귀하의 개인정보를 유출한 기업이 동 사건과 관련하여 귀하가 당할 수 있는 정신적·재산적 손해에 대하여 위자료로 <1/2 가격>을 제공하고자 합니다. 이를 수용할 의사가 있습니까?

(1) 있다 - - - - - - - - > [문 17로]
(2) 없다 - - - - - - - - > [문 18로]

문 16)그렇다면 귀하의 개인정보를 유출한 기업이 동 사건과 관련하여 귀하가 당할 수 있는 정신적·재산적 손해에 대하여 위자료로 <2배 가격>을 제공하고자 합니다. 이를 수용할 의사가 있습니까?

(1) 있다 - - - - - - - - > [문 18로]
(2) 없다 - - - - - - - - > [문 18로]

문 17). 귀하는 기업이 위자료를 지불하지 않아도 되겠습니까 ?
(1) 그렇다 - - - - - - - - > [문 19로]
(2) 아니다 - - - - - - - - > [문 18로]

문 18). 귀하는 수용할 의사가 있는 위자료의 최소금액은 얼마 입니까 ?
( )만원

유형 2) 고유식별 정보(주민등록번호, 여권번호, 운전면허번호 등)가 유출되었을 때,
유형 3) 의료·건강 정보(병력, 진료기록, 신체장애, 건강상태 등)가 유출되었을 때,
유형 4) 경제 정보(소득, 신용카드 및 통장계좌번호, 물품구매내역, 대출 또는 담보설정 등)가 유출되었을 때,
유형 5) 사회·관계 정보(학력 및 학업성적, 친우관계, 종교, 동호회 등 모임 가입·활동 직장 등)가 유출되었을 때,
유형 6) 통신·위치 정보(휴대폰번호, 이메일주소, GPS 위치정보 등)가 유출되었을 때,
유형 7) 법적 정보(전과·범죄기록, 납세기록, 과태료 내역 등) 가 유출되었을 때,
유형 8) 바이오 정보(DNA, 지문, 얼굴, 홍체 등)가 유출되었을 때,

5. 사회경제적 사항에 대한 질문

문 19) 기본사항 질문

연령	성별	거주지	세대주 여부	결혼 여부	수입있는 가족수	자녀수	취업여무	총가족수
만( )세	□남성 □여성	시/도	□그렇다 □아니다	□그렇다 □아니다	명	명	□취 업 □미취업	명

19-1) 가족 중 인터넷을 이용하는 사람은 몇 명입니까?

인터넷 이용자수 ( )명

※ 문14 에서의 응답 결과보다 작거나 같아야 함

문 20) 귀하의 직업은 무엇입니까?

1. 자영업 2. 판매/서비스/영업직 3. 기술/노무직
4. 사무/전문직 5. 경영/관리직 6. 중고등학생
7. 대학(원)생 8. 주부 9.기타( )

문 21) 귀하의 학력은 어떻게 되십니까?(교육 년수를 아래 숫자에 표 해주십시오)

무학	초등학교						중학교			고등학교			대학교				대학원			
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

문 22) **귀댁의** 월 평균 소득은 어떻게 되십니까?

가구소득(월 평균) : _____

1. 100만원 이하
2. 101만원-200만원
3. 201만원-300만원
4. 301만원-400만원
5. 401만원-500만원
6. 501만원-600만원
7. 601만원-800만원
8. 801만원-1,000만원
9. 1,000만원 이상

문 23) **귀댁의** 월 평균 통신요금(집전화, 휴대전화, 인터넷 등 포함)은 얼마입니까?

1. 월 3만원 미만
2. 월 3-5만원 미만
3. 월 5-10만원 미만
4. 월 10-20만원 미만
5. 월 20만원 이상

문 24) 정보화기기 이용여부 질문

일반 메일로 뉴스레터, 문화정보 등을 받아보십니까?	□예 □ 아니오
온라인에서 벗어난 동아리, 커뮤니티 등에 가입하고 있으십니까 ?	□예 □ 아니오
인터넷(이메일 포함)을 이용하십니까?	□예 (문 18로 이동) □ 아니오
TV, 인터넷, 모바일 등을 이용한 쇼핑을 이용하십니까 ?	□예 (문 19로 이동) □ 아니오
소셜커머스를 이용하십니까? 소셜커머스(Social Commerce)란 정해진 기간 동안 일정 수 이상의 구매자가 모이면 할인된 가격으로 상품이나 서비스를 구매(할인쿠폰·티켓 등)할 수 있는 인터넷 쇼핑서비스 예) 티켓몬스터, 쿠팡, 위메이크프라이스, 그루폰, 슈팡, 해피바이러스, 위폰, 데일리픽, 다음 소셜 쇼핑 등	□예 (문 20로 이동) □ 아니오
인터넷/모바일 뱅킹을 이용하십니까 ?	□예 (문 21로 이동) □ 아니오
휴대폰 SMS 문자서비스를 이용하십니까?	□예 (문 22로 이동) □ 아니오
소셜네트워킹 서비스를 이용하십니까? SNS(소셜 네트워킹 서비스)란 친구, 동료 등 지인고의 인간관계를 강화하거나 새로운 인맥을 형성함으로써 폭넓은 인적 네트워크 형성을 할 수 있게 해주는 서비스입니다. 예) 트위터, 페이스북, 카톡, 미니홈피, 블로그, 마이크로블로그, 커뮤니티(가페클럽) 등	□예 (문 23로 이동) □ 아니오

문 25) 인터넷(이메일 포함) 이용에 대한 질의

문 25-1) 귀하께서 월1회 이상 인터넷을 이용하고 계십니까?

1. 예 2. 아니오

문 25-2) 귀하의 **1주일 평균** 인터넷 사용시간(이메일 사용 시간 포함)은 얼마나 되십니까?

1. 2시간 미만 2. 2시간 이상 4시간 미만
3. 4시간 이상 10시간 미만 4. 10시간 이상 20시간 미만
5. 20시간 이상(적을 것 : _____ 시간)

문 25-3) 귀하가 인터넷에 **접속하는 장소의 비율**을 구분하여 답하여 주십시오.

접속장소	비 율
① 집	(%)
② 회사/학교	(%)
③ 기타	(%)
합 계	(100 %)

※ 합계가 반드시 100%로 되도록 함

문 25-4) 귀하가 온라인(인터넷)으로 아래의 표와 같은 세부 활동을 하는 시간 전체를 100%로 하였을 때, **각 영역별 활동이 차지하는 비중**은 얼마나 되는지 답하여 주십시오.

예) 귀하의 평상시 인터넷 이용 시간이 하루 평균 4시간이고, 그 중“ 경제활동”과 관련된 활동 시간이 1시간이라고 하면, 인터넷 활동 중 “경제활동”이 차지하는 비중은 25%가 됩니다.

구분	세부활동	비율
① 경제활동	정보수집, 구매, 인터넷 뱅킹/주식거래 등	(%)
② 학습활동	자료수집, 사이버 강좌 수강 등	(%)
③ 의사소통	메신저, 이메일, 트위터, 페북, 카톡 등 SNS 활동	(%)
④ 여가활동	문화정보 수집, 예약, 웹진/뉴스, 게임 등	(%)
⑤ 전자정부	정부정책 관련 자료 수집, 정책에 관한 의견 개진, 민원서비스 등	(%)
⑥ 기타(사회참여 등)	선거관련 정보 검색, 지역모임 참가, 시민단체/정당 활동 등	(%)
합 계		(100 %)

※ 합계가 반드시 100%로 되도록 함

문 26) TV, 인터넷, 모바일 등을 이용한 쇼핑에 대한 질의

문 26-1) TV, 인터넷, 모바일 등을 이용한 쇼핑을 얼마나 자주 이용하십니까?

1. 1주일에 1회 이상
2. 한 달에 1회 이상
3. 1년에 1회 이상
4. 1년에 1회 미만
5. 이용안함

문 26-2) 개인적으로 TV, 인터넷, 모바일 등을 이용한 상품이나 서비스를 구매(예약·예매 포함)한 금액은 월 평균 어느 정도 입니까? 2012년 8월부터 2013년 7월까지(지난 1년) 구매 경험을 기반으로 월평균 금액을 기재해 주십시오. 인

월 평균 _____ 원

문 26-3) 쇼핑 및 상품의 구매할 때 판매자가 개인정보를 제공하고 회원 혹은 맴버쉽(membership)에 가입을 권유하는 경우 이에 따르십니까 ?

1. 가입하지 않는다
2. 대체로 가입한다
3. 가입한다

문 26-4) 쇼핑 및 상품의 구매와 관련하여 소식지(백화점, TV 홈쇼핑 등)를 받아보시고 계십니까?

1. 예
2. 아니오

문 27) 소셜커머스에 대한 질의

문 27-1) 소셜커머스를 얼마나 자주 이용하십니까?

1. 1주일에 1회 이상
2. 한 달에 1회 이상
3. 1년에 1회 이상
4. 1년에 1회 미만
5. 이용안함

문 28) 인터넷/모바일 뱅킹에 대한 질의

문 28-1) 인터넷/모바일 뱅킹을 얼마나 자주 이용하십니까?

1. 1주일에 1회 이상　　2. 한 달에 1회 이상
3. 1년에 1회 이상　　4. 1년에 1회 미만
5. 이용안함

문 28-2) 시중은행 이외에 비은행권(저축은행, 신협, 및 우체국 등)에 금융거래를 하십니까?

1. 예　　2. 아니오

문 29) 휴대폰 SMS 문자 서비스에 대한 질의

문 29-1) 휴대폰 SMS 문자서비스를 얼마나 자주 이용하십니까?

1. 하루 1회 이상　　2. 1주일에 1회 이상
3. 한 달에 1회 이상　　4. 한 달에 1회 미만
5. 이용안함

문 29-2) 귀하의 **1주일 평균** SMS 문자서비스 이용시간은 얼마나 되십니까?

1. 1시간 미만　　2. 1시간 이상 2시간 미만
3. 2시간 이상 4시간 미만　　4. 4시간 이상 10시간 미만
5. 10시간 이상(적을 것 : _____ 시간)

문 30) SNS이용에 대한 질의

문 30-1) 귀하는 SNS를 얼마나 자주 이용하십니까?

1. 하루 1회 이상　　2. 1주일에 1회 이상
3. 한 달에 1회 이상　　4. 한 달에 1회 미만
5. 이용안함

문 30-2) 귀하의 **1주일 평균** SNS 이용시간은 얼마나 되십니까?

1. 1시간 미만　　2. 1시간 이상 2시간 미만
3. 2시간 이상 4시간 미만　　4. 4시간 이상 10시간 미만
5. 10시간 이상(적을 것 : _____ 시간)

문 30-3) 귀하는 SNS를 운영하고 계십니까 ?

1. 예　　2. 아니오

응답해 주셔서 감사합니다

참 고 문 헌

1. 국내 자료

[1] 강달천, 김민섭, 김현철(2005), “개인정보 피해구제 및 상담 사례분석”, 한국정보보호진흥원 단행본.

[2] 강달천(2007), “정보통신망등에서의 개인정보보호에 관한 법률 제정 및 발전방안”, 정보보호법 발전방안 마련을 위한 공청회, 정보통신부.

[3] 곽승준(2001), 자연자산의 경제적 가치측정 방안 연구, 환경부 연구과제 참조

[4] 국가보안기술연구소(2006), "정보보호의 경제적 동향분석에 관한 연구", 국가보안기술연구소.

[5] 금융감독위원회(2004), “금감원 2004 국정감사보도자료”.

[6] 김동노, 하승창, 김영홍, 최인욱(2003), “금융기관과 인터넷에서의 개인정보 공유 현황 실태조사”, 2003년도 인권상황 실태조사 연구용역 보고서, 국가인권위원회.

[7] 김여라, 이해춘, 유진호, 개인정보보호의 가치 산출, KISA 정보보호정책동향, 2007

[8] 김정덕, 신수정, 홍기향(2004), “정보시스템 생명주기 및 구성요소별 정보보호 고려사항과 세부 평가항목 개발”, KISA 연구보고서.

[9] 김정은 외 (2010), 소비자의 개인정보 가치평가에 영향을 미치는 요인에 대한 연구, 소비자학연구

[10] 김재홍(2010), 태화산 생태공원의 경제적 가치추정에 관한 연구, 환경정책연구 9(1), 109-135

[11] 민경식, 송혜인(2008), “정보보호의 경제적 분석 연구 동향”, 『정보보호 이슈보고서』 2008-8호.

[12] 서혜석(2006), "개인정보 이용의 해외사례와 시사점", 서혜석 의원실.

[13] 유진호, 지상호, 송혜인, 정경호, 임종인(2008), "인터넷 침해사고에 의한 피해손실 측정", 『정보화정책』 제15권 제1호.

[14] 유진호, 지상호, 임종인, "개인정보 유노출 사고로 인한 기업의 손실비용 추정”, 정보보호학회논문지 제19권 제4호 pp.63-75, 2009.8.

[15] 윤주연(2003), "각국의 개인정보피해구제제도 비교연구", 한국정보보호진흥원·개인정보분쟁조정위원회.

[16] 이민영(2004), “주민등록번호 남용억제에 관한 법제적 고찰”, 『정보통신정책』 제16권 8호 통권 346호.

[17] 이창범, 김본미(2004), "개인정보피해구제 및 배상기준에 관한 연구", 한국정보보호진흥원・개인정보분쟁조정위원회.

[18] 장종인(2005), “개인정보시장에서 주민등록번호의 이용”, 『정보통신정책』 제17권 18호.

[19] _____(2005), 『개인 감시의 확장: 주민등록번호의 상업적 이용』, 서울대학교 대학원 석사학위 논문. (http://library.snu.ac.kr/DetailView.jsp?uid=11&cid=0001198869)

[20] 정보통신부(2003), “정보통신망 침해사고 조사결과”

[21] 정석균(2012), 인터넷 개인정보보호의 시장자체해결가능성에 대한 연구, 한국디지털정책학회

[22] 정연수, 김동우, 이재종(2005), "2005년 민간부문 개인정보보호 관리현황 및 보호방안에 관한 연구", 한국정보보호진흥원

[23] 주덕규, 강달천, 정연수(2002), “개인정보 침해와 대처방안”, 『정보통신윤리』 통권39호 (http://boho.or.kr/dataroom/data_01_dtl.jsp?board_id=1&page_id=1&u_id=11&page=9&tempidx=11&gubun=0)

[24] 채승완(2008), “개인정보보호의 경제적 효과”, 『소비자문제연구』 제33호.

[25] 채승완, 민경식, 황성원, 원순재 (2007), “개인정보의 경제적 가치분석에 관한 고찰”, 한국정보보호진흥원

[26] 한국개발연구원(2004), 문화시설의 가치추정 연구

[27] 한국인터넷진흥원(2009), "개인정보 영향평가 방법론과 구축사례“

[28] 한국정보보호진흥원 전략기획팀(2007), “개인정보의 경제적 가치 분석 고찰”, 『정보보호 Issue Report』 2007-03.

[29] 한국정보보호진흥원(2002), “컴퓨터 해킹, 바이러스 피해액 산출방법 연구”

[30] _____(2006), “인터넷 침해사고 피해액 산출모형 개발에 관한 연구”

[31] _____(2007), “2007년 정보보호실태조사”

[32] _____(2008), “2008년 정보보호실태조사”

[33] _____(2009), “2009년 정보보호실태조사”

[34] 한국정보보호진흥원(2003), "2003년도 개인 인터넷 이용자의 정보화 역기능 실태조사 보고서"

[35] 행정안전부 (2011), 개인정보 보호법령 및 지침·고시 해설

2. 국외 자료

[1] Acquisiti, Alessandro (2010), Privacy and Security of Personal Information, Carnegie Mellon University working paper.

[2] Agre, Philip E. & Rotenberg, Marc(1998), 『Technology and Privacy: The New Landscape.』, Cambridge, MA: The MIT Press.

[3] Anderson, R. and T. Moore (2006), The Economics of Information Security, *Science* 314, 610-613

[4] Anderson, R.(2001), "Why Information Security is Hard - An Economic Perspective." 17th Annual Computer Security Applications Conference, 2001

[5] Andrew Wong(2008), "Estimating the cost of a Security Breach", (http://www.innovar.com.sg/Archives/Calculating%20the%20Cost%20of%20a%20Security%20 Breach_23Feb08.pdf)

[6] Anita D.D'Amico(2000), "What does a Computer Security Breach Really Cost?", 『Secure Decision』, a division of Applied Visions, Inc.

[7] Branscomb, Anne W.(1994), "Who Owns Information?: From Privacy to Public Access", NY: Basic Books.

[8] Brunk, B.D.(2002), Understanding the Privacy Space, First Monday 7(10).

[9] Butler, S. A.(2002), " Security Attribute Evaluation Method: A Cost-Benefit Approach." Proceedings of the 24th International Conference on Software Engineering, ACM.

[10] Charles T. Horngren, George Foster, Srikant M. Datar, Madhav Rajan, Chris Ittner(2008), 『Cost Accounting: A Managerial Emphasis, 13th Edition』, Prentice Hall.

[11] CIC Security Working Group(1998), "Incident Cost Analysis and Modeling Project"

[12] CnetNews.com(2003), "Counting the cost of Slammer", (www.news.com/2100-1001-982955.html)

[13] Congressional Research Service(2004), "The Economic Impact of Cyber-Attacks".

[14] Dobson, J.(1994), "Messages, Communication, Information Security and Value" Proceeding of the New Security Paradigms Workshop.

[15] Farahmand, F., Navathe, S. B., Sharp, G. P., Enslow, P. H.(2005), "Assessing Damages of Information Security Incidents and Selecting Control Measures,

a Case Study Approach". Workshop on the Economics of Information Security.

[16] Garden, J.(2003), " Large scale Network incidents - what can we do?"

[17] Gordon, L. A and Loeb, M. P.(2006), 『Managing Cybersecurity Resources : A Cost-Benifit Analysis』

[18] Gorden L.A. and M. P. Leob (2002), The Economics of Information Security Investment, ACM Transaction on Information and System Security 5(4), 438-457

[19] Hal R. Varian(1992), 『Microeconomic Analysis, Third Edition』, W. W. Norton & Company.

[20] Horowitz and McConnell, 2002, A Review of WTA/WTA Studies, *Journal of Environmental Economics and Management* 44, 426-447.

[21] Howard, J. D.(1997), "An Analysis of Security Incidents On the Internet 1989-1995."

[22] Information Shield Inc., "Privacy Breach Impact caculator", (http://www.informationshield.com/privacybreachcalc.html)

[23] IPA(2006), "コンピュ_タ_ウイルス被害_況調査報告書"

[24] ____(2006), "情報セキュリティ_連被害等の_況調査票"

[25] ____(2006),『情報セキュリティ讀本　改訂版』

[26] JNSA(2010), "情報セキュリティインシデントに關する 調査報告書"

[27] John Rose and Carl Kalapesi (2012), Rethinking Personal Data: Strengthening Trust, Boston Consulting Group

[28] Meglena Kuneva (2010), Keynote Speech, Roundtable on Online Data Collection, Targeting and Profiling

[29] OECD (2011), Exploring the Economics of Personal Data: A Survey of Methodologies for Monetary Value, OECD Digital Economy Papers No. 220.

[30] Ponemon Institute(2010), "Fifth Annual US Cost of Data Breach, January 2010", (http://www.ponemon.org/data-security).

[31] Posener, R. A. (1980), The Economics of Privacy, *American Economics Review* 71(2), 405-409

[32] Smith, D. M.(2003), "The Cost of Lost Data". The George L. Graziadio School of Business & Management Report, Pepperdine University.

[33] Tech//404, "Data Loss Cost Calculator",

(http://www.tech-404.com/calculator.html)

[34] The Economist (2010), Data, data everywhere, A special report on managing information

[35] USENIX Association(2000), "Incident Cost Analysis and Modeling Project Ⅱ"

[36] Varian H.R.(1996), Economic Aspects of Personal Privacy, http://people.ischool.berkeley.edu/~hal/Papers/privacy/

[37] Varian H.R.(1998), Economics of Information and Intellectual Property Right, 고려대학교 경제연구소

[38] Weaver, N. & Paxson V.(2004), "A Worst-Case Worm". Third annual Workshop on Economics and Information Security.

[39] William H. Greene(2007), 『Econometric Analysis 6th edition』, Prentice Hall.

[40] World Economic Forum (2011), Personal Data: The Emergence of a New Asset Class, An Initiative of the World Economic Forum January 2011