

CVM을 이용한 국내 개인정보 침해사과의 위자료 산정*

권 흥,[†] 이 은 주, 김 태 성[‡], 전 효 정
충북대학교 경영정보학과/BK21사업팀

Estimating Compensation for Personal Information Infringement in Korea Using Contingent Valuation Methods*

Hong Kwon,[†] Eun-Ju Lee, Tae-Sung Kim[‡], Hyo-Jung Jun
Department of MIS / BK21 Project Team, Chungbuk National University

요 약

(개인정보 침해사과의 위자료 산정)

개인정보의 상업적 가치가 증대되면서 불법적 거래나 유통, 유·노출사고 등의 개인정보 침해사과가 발생하고 있고 개인정보침해에 대한 위자료 산정이 침해사과에 대한 해결책이 되고 있다. 그러나 개인정보는 비시장재이며 교환가격이 존재하지 않으므로 위자료의 정량적 산정에는 어려움이 있다. 이에 대한 대안으로 본 연구에서는 시장에서 거래되지 않아 가치에 대한 정보를 얻을 수 없는 개인들의 가치평가를 추정하기 위해 CVM을 이용하여 유형별 WTA를 추정하였다. 또한, 일본의 JNSA JO 모델을 적용하여 한국에 부재한 위자료산정의 정형화된 모델에 관한 연구를 시도했다. 본 연구는 단순히 위자료 산정의 접근 방안을 제시한 것에 그치는 것이 아니라 개인정보의 가치를 측정함으로써 기업이나 조직들에게 개인정보의 중요성에 대한 경각심을 일깨워줄 수 있을 것이다.

ABSTRACT

(Estimating Compensation for Personal Information Infringement)

As the value of personal information increases, personal information infringements is more likely to happen. The compensation for personal information infringements needs to be calculated in the process of infringement remedy. However, as personal information is regarded as non-market goods with no exchange price and calculating the remedy for mental sufferings from infringements has no guideline, it is not easy to determine the compensation amount. In this study, we adopt Contingent Valuation Methods (CVM) to analyze Willingness to Accept (WTA) of each type of personal information. Also, this study attempts to examine a standard model for calculating compensation by applying JNSA JO Model of Japan, which is not prepared in Korea. This study does not simply present a plan of estimating compensation. By measuring the value of personal information, it could awaken companies and organizations to the importance of personal information security.

Keywords: Personal Information Infringement, Compensation, Remedy for Mental Sufferings, Contingent Valuation Methods (CVM), Willingness to Accept (WTA)

접수일(2012년 3월 7일), 게재확정일(2012년 4월 7일)

* 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한 국연구재단 기초연구사업의 지원을 받아 수행된 연구임

(2011-0025512)

[†] 주저자, 3czolo@hanmail.net

[‡] 교신저자, kimts@chungbuk.ac.kr

I. 서 론

지난 10여년 간 한국은 인터넷의 광복할만한 발달과 보급으로 정보화 사회의 고도화를 촉진시켰고, 인터넷 등의 네트워크를 통한 개인정보의 수집, 이용, 보관, 가공이 일반화 되었다. 주민등록번호를 비롯한 개인정보는 네트워크상에서 사용자 입장에서의 자신의 신분을 나타내는 본인식별(Identification)과, 기업이나 조직 입장에서의 고객에게 서비스를 제공하기 위한 개인식별 기능 외에도 마케팅 수단으로써 활용되고 있다[1]. 특히 디지털 기술이 가져다 준 방대한 정보처리능력은 개인정보의 이용가치를 극대화시켰다. 이러한 과정에서 개인정보 침해사고가 발생하고 있으며, 실제로 한국인터넷진흥원 개인정보침해신고센터에 접수된 통계자료를 보면 개인정보침해 신고 건수가 지속적으로 증가하고 있다[2].

특히 개인정보를 취급하는 기업이나 조직의 개인정보 유·노출 등의 침해사고가 빈번해지고 있고, 근래에는 천만명 단위의 대규모 개인정보 유·노출사고가 잇달아 발생하는 등 사회적 손실과 더불어 개인의 피해 범위가 확대되고 있다. 이에 따라 많은 이들이 관련법에 의거하여 개인정보 침해사고에 대한 분쟁조정, 손해배상 청구 소송 등의 피해구제¹⁾ 활동을 점차 활발히 진행하고 있다. 하지만 소송과정에서 정신상의 고통을 금전으로 위자하기 위하여 지급되는 금원인 위자료 혹은 정신적 손해배상은 자칫 판단기관의 자의적인 판단이 될 수 있고, 일관성을 잃을 가능성이 있다는 의미가 될 수 있다[3]. 더욱이 최근 수년간 불거진 온라인상의 대규모 개인정보 유·노출 사고는 판단여하에 따라 해당기업의 존폐위기와 더불어 사회적 파장을 불러일으킬 소지가 높다. 표 1을 통해서 최근 개인정보 침해사고의 대형화 특성을 확인할 수 있으며, 피해 당사자의 손해배상 청구액과 실제 배상액간의 적잖은 괴리가 있음도 확인할 수 있다.

본 연구에서는 개인정보 침해사고와 관련한 위자료 산정은 수용자인 개인들의 의사를 반영할 때 타당한 의미를 가질 수 있다는 점에 의거하여 연구를 진행하고자 한다. 구체적으로 본 연구의 목적은 우선 한국 내에 개인정보 침해사고에 대한 정형화된 위자료 산정

[표 1] 소송관련 주요 개인정보침해사고

사고업체	일시	유·노출 인원	청구액 (1인당)	배상액(1인당)
엔씨소프트	2005.5	40~50만명	500만원	10만원 (1심: 50만원)
	2006.2	28만명	100만원	원고 패소
국민은행	2006.3	3만 2277명	100만원	10만원 (1심: 7만원)
			300만원	20만원 (1심: 10만원)
LG전자	2006.9	400명	2000만원	30만원 (1심: 70만원)
옥션	2008.2	1863만명	200만원 (평균 100만원)	원고 패소 (소비자원-분쟁 조정금액: 5~10만원)
하나로텔레콤	2008.4	600만명	100만원	10~20만원
LG텔레콤	2008.4	800만명	100만원	원고 패소
다음	2008.7	55만명	30만원	진행 중
GS칼텍스	2008.9	1151만명	100만원	원고 패소
SK커뮤니케이션즈	2011.6	3500만명	100만원	진행 중

※자료: 주요 사고 기사검색(2005.1.1.~2012.2.29)

모델이 없는 것에 착안하여 해외 사례를 탐색해 보고, 정형화된 위자료 산정모델의 필요성에 대한 논의와 더불어 해외에서 실무적으로 사용되는 모델을 분석하여 한국에서의 적용 가능성을 타진해 보고, 수용자인 개인들의 시각에서 평가한 개인정보 침해사고에 대한 정신적 손해배상액인 위자료의 수준은 어느 정도인지 측정해 보고자 한다. 더불어 개인들을 대상으로 개인정보 침해사고에 대한 인식 및 위자료 문제에 관한 인지도는 어떠한지, 각 주체별 위자료 수준은 어떠한 경향을 보이는지를 연구하고자 한다. 나아가 개인정보를 취급하는 기업이나 조직 입장에서 위자료 경감에 미치는 요인 분석을 통해 개인정보보호에 대한 중점 사안을 도출해 내고자 한다.

II. 관련 연구 고찰

기존 문헌들 가운데 개인정보의 금전적 가치산정에 대한 연구는 많지 않다. 더욱이 본 연구에서 하고자

1) (광의의) 개인정보 피해구제: 민사, 형사, 행정적 피해구제를 모두 포괄, 피해구제라 함은 민사적 피해구제를 의미하는 것이 일반적. 구제방법으로는 손해배상, 원상회복, 강제조치, 확인판결 등이 있으며 강제조치에는 금지명령이나 이행명령 등이 포함.

하는 수용자 관점에서의 위자료 산정에 초점을 둔 연구는 더욱 접하기 어려웠다. 이에 대한 이유는 정보보호라는 큰 틀 안에서 개인정보 분야에 대한 연구가 본격적으로 시작된 것은 근래의 일이고, 더욱이 위자료라는 세부적인 주제에 관해서는 온라인상에서 대규모 개인정보 유·노출 사고가 발생하여 많은 사람들이 공동소송에 참여함에 따라 주목을 받게 된 것이 불과 2~3년 전의 일이기 때문으로 보여진다. 이에 본 연구에서는 위자료라는 것이 개인정보의 가치를 반영하는 것과 상호연관성이 깊기 때문에 개인정보의 중요성 인식 및 개인정보의 가치를 추정한 문헌들을 위주로 고찰하였다.

2.1 개인정보의 중요성 및 관리에 관한 연구

이기혁 외(2008)는 개인정보의 중요도 분석을 통해 위험분석을 수행하고 이에 따른 위험 수준을 산출함으로 인해 개인정보 흐름을 분석하여 궁극적으로는 전사적으로 개인정보보호 위험에 대한 통합 모니터링을 가능하게 하는 방향을 제시하였다(4). 이 연구에서는 개인정보를 취급하는 민간기업들이 개인정보 유출을 사전에 방지할 수 있도록 하는 일환으로써 개인정보영향평가를 수행할 수 있으며, 이러한 일련의 프로세스를 이용한 개인정보 유출에 대한 위험 측정 방안과 위험평가 결과를 토대로 위험에 효율적으로 대응할 수 있는 방안을 제시하였다.

Xin (Luna) Dong (2005)는 디지털화에 따른 정보의 다량화로 인한 개인정보의 중요성에 대해 인식하고 개인정보관리시스템(Personal Information System (PIM))의 올바른 방향성을 제시하였다(5). 이 연구에서는 개인정보를 논리적 시각으로 구체화하여 의미 있는 구성과 구성요소들 간의 적절한 조합을 PIM의 주요 요건으로 제안하였다.

David L. Monthersbaugh 외 (2011)는 온라인상의 개인정보제공과 관련하여 온라인 마케터의 관점에서 기업의 이익과 개인정보의 제공에 관한 상관관계를 분석하였다(6). 이 연구에서는 개인정보제공의 민감도에 따라 이익에 영향을 미치는 정도를 파악한 결과, 정보제공의 민감도가 클수록 이익은 작아지고 정보의 통제와 온라인 프라이버시의 고려사항이 높을수록 이익에 미치는 영향이 많은 것을 밝혀냈다.

2.2 개인정보의 가치 산정에 관한 연구

김여라 외 (2007)는 조건부가치측정법(Contin-

gent Valuation Methods, CVM)을 이용하여 개인정보보호의 가치를 산출했다(7). 이 연구는 개인정보 유출 피해라는 사회적 손실을 막기 위한 응답자의 평균적 지불의사금액(Willingness to Pay, WTP)을 산출하여 개인정보의 사회적 가치를 추정하였다.

이해춘 외 (2008)는 CVM을 이용하여 개인정보 유출의 손실 가치를 분석했다(8). 이 연구는 개인들을 대상으로 한 설문을 통해 손해배상에 대한 수용의사금액(Willingness to Accept, WTA)을 측정하여 건당 평균 WTA(약 756만원)를 계산하고, 이를 통해 전체 손실가치(2006년 기준 약 32조원)를 추정하였다. 그러나 유출된 개인정보의 유형에 따라 개인들이 생각하는 피해정도 역시 다르기 때문에, 이점을 고려하지 않은 것은 한계점이라 볼 수 있다. 따라서 본 연구에서는 JNSA(Japan Network Security Association) JO(JNSA Damage Operation Model for Individual Information Leak) 모델을 적용하여 유출된 정보의 유형에 따라 피해에 대한 WTA를 산정하였다.

유진호 외 (2009)는 Gordon과 Loeb(2006)이 개념적으로 정의한 침해사고 비용 구조를 바탕으로 개인정보 침해사고로 인한 기업의 직접적이고 정량적인 손실비용 산출방안을 제시하였다(9). 이 연구에서는 개인정보 침해사고로 인한 기업의 손실비용에 대해 침해사고 대응비용, 생산성 손실비용, 잠재적인 손해배상금으로 각각 산출하여 전체적인 관점에서 분석하였다. 이 연구에서 손해배상금 산출은 한국내 실제 사고의 배상 판결 사례와 개인정보침해분쟁조정위원회의 조정 사례를 통한 기준 값을 근거로 하였다. 하지만 아직까지 한국내 판례가 많지 않아 유형에 따라 다양한 사례에 적용하기에 미흡한 부분이 있으며, 연구자가 밝힌 것처럼 판례 적용에 대한 객관적인 타당성 입증 필요하다.

김철완 외 (2001)는 개인정보보호 수준을 비보호, 강보호, 약보호 상태로 차별화하여 각 수준에서 응답자들이 구간별로 나눠진 금액을 선택하도록 하여 개인정보의 가치를 평가했다(10). 그 결과는 표 2와 같이 각 수준별로 123천원에서 169천원 수준을 나타냈다. 이외에도 동일한 방식으로 구간별로 나눠진 금액을 선택하도록 하여 지불의사금액과 기업들을 대상으로 개인정보 5만명, 20만명의 가치를 설문을 통해 조사하였다. 이를 통해 개인정보 시장의 수요독점적 성격으로 인해 시장 왜곡이 발생하고 있는 것을 보여주었다.

(표 2) 개인정보보호수준별 개인정보 가치

	평균값 (원)	표준 편차(원)
비보호(개인정보가 어떤 형태로든 보호된다는 확신이 없는 경우)	169,000	52,300
강보호(개인정보가 사전에 명시된 대상 및 용도에만 사용되도록 보호된다는 확신이 있는 경우)	123,000	64,800
약보호(개인정보가 사전에 명시된 대상 및 용도와 함께 대상과 용도가 추가적으로 발생한다면 이를 반드시 사전에 허락받을 경우에만 사용되도록 보호된다는 확신이 있는 경우)	135,100	60,800

PGP(2009)는 2005년²⁾부터 연간보고서를 통해 기업의 데이터 침해사고에 대한 비용을 산출해내고 있다. 2008년에는 미국내 43개 기업을 대상으로 손실 비용을 산출했는데 레코드(Record)당 총202달러의 비용 손실이 있는 것으로 산출되었다[11]. 이는 2005년 138달러, 2006년 182달러, 2007년 197달러로 산출된 것과 비교하여 매년 지속적으로 비용이 증가하는 것으로 나타난 수치이다.

한창희 외(2011)는 미국 포네몬 연구소와 일본 JNSA의 방식을 참고하여 개인정보 유출과 누출로 인한 피해를 기업뿐만 아니라 사용자의 피해까지도 고려해 산출하는 방법을 제시하였다[12]. 이 연구에서는 개인정보 유출의 총 피해규모에 관한 비용 산출 방법론 제시를 하였지만 유출된 정보의 가치를 판례나 개인정보분쟁조정위원회의 손해배상금 관련 자료를 이용해 추정함으로써 개인적 차원에서의 개인정보 가치의 산정에는 한계가 있다.

김정은 외(2010)는 소비자의 개인정보 관련 소비자행동과 소비자의 개인정보 가치평가간의 인과적 관계를 알아본 결과, 소비자의 행동이 가치평가에 유의한 영향을 주며 가치평가는 행동에 유의한 영향을 주지 않음을 발견하였다[13]. 이 연구에서는 소비자집단별 특성에 따른 개인정보 관련 정책의 집행이 요구되며, 이를 위해서는 관심대상인 변수의 수준별로 소비자 집단을 세분화시켜 분석할 수 있는 새로운 연구방법의 도입의 필요성을 제기하였다.

III. 위자료 산정모델

위자료는 정신적·비재산적 손해에 대한 금전적 배상이기 때문에 손해를 산술적으로 계량하기가 곤란하다는 특성이 있다. 위자료를 산정하기 위해서는 먼저 개인정보 침해로 발생한 정신적 손해에 대하여 금전적 평가가 이루어져야 하는데, 문제는 바로 정신적 손해에 대한 금전적 평가를 객관적으로 할 수 있는 구체적인 기준이 없다는 점이다.

따라서 개인정보 침해로 인한 정신적 손해배상액인 위자료를 합리적이고 적정하게 산정하기 위한 방법과 기준이 필요하다. 이에 대한 대안으로 위자료 산정 모델 내지는 위자료 산정 프레임워크를 적용하는 방안이 될 수 있다.

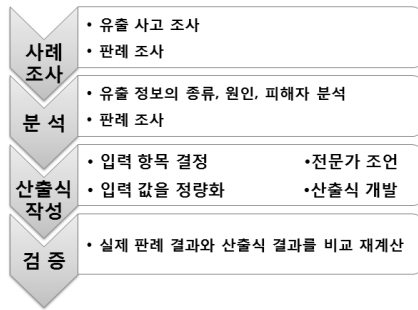
상기한대로 실무적으로 활용할 수 있는 위자료 산정모델의 필요성에도 불구하고 한국에는 아직 실제 적용되고 있는 모델이 없기에 본 연구에서는 일본에서 실무적 모델로 활용되고 있는 JNSA JO모델에 대해 구체적으로 논의해 보고, 한국에서의 적용가능성 및 개선방안을 모색하고자 한다.

JNSA JO모델은 일본 네트워크 보안 협회의 보안 피해 조사 그룹이 제시한 모델로 피해 대상을 각 항목별로 분할하고, 표본조사를 통한 단위 비용을 추정하여 전체 규모를 산출하는 원단위(Basic Unit) 접근법을 통한 정형화된 실무적 모델이다. 조사는 신문과 인터넷 뉴스 등에서 보도된 개인정보 유출 사고를 집계 분석하여 이루어지며, JO모델을 통해 추정 손해배상액을 산출한다[14].

JNSA JO모델은 개인정보 침해사고에 대한 손해배상액을 추정하는데 있어서 정형화된 모델로서 실무적 관점에서 의미가 크다고 볼 수 있다. 특히 손해배상액 산정 요소를 체계화하고 객관화하여, 금액으로 정량화하는 방법을 제시함에 따라 개인정보를 취급하는 기업이나 조직의 잠재적 위험을 파악하는데 충분히 활용할 만한 가치가 있다고 판단된다.

JO모델의 국내 적용은 가능하다고 보여지되 2003년에 수립된 모델임을 감안하여 물가상승과 환율변동 등에 따른 기본정보 가치 조정, 한국 실정에 보다 적합한 EP다이어그램 개선 등의 보완 절차가 필요하다고 본다. JO모델 역시 기존 판례와 전문가들의 합의로 개발된 모델이기에 피해자인 개인들의 의사는 반영되었다고 보기 어렵다.

2) 2007년 보고서까지는 PGP사와 Vontu사가 공동으로 조사



(그림 1) JNSA JO 모델의 추정 손해배상 산출식 개발 프로세스

따라서 이를 기본정보 가치 조정 또는 정보민감도의 가중치 부가 등의 개선을 통해 시장 내에서 통용될 보편타당한 위자료 수준을 형성해 나가는 작업이 필요하다. 다음 장부터는 이를 위한 제반사항의 연구를 위해 논의하였다.

IV. 자료 조사 개요 및 주요 결과

설문을 통한 실증연구를 진행하기 위해 사전조사, 전문가설문, 본조사의 단계를 거쳤다. 사전조사는 일반인 50명을 대상으로 조사내용을 설명하고 응답을 받아 양분선택형 질문을 두 번 제시하는 이중양분선택형법(Double-bounded Dichotomous Choice)의 초기제시액 구간을 설정하였으며 개별 인터뷰를 통해 응답편의성, 설문문항 이해 용이도 등의 의견을 수렴하여 설문을 수정·보완하였다. 그리고 전문가 의견수렴과 더불어 시나리오 설정, 질문 구성 등의 내용타당성을 검토하기 위해 전문가설문을 의뢰하였다.

본조사는 2010년 10월 4일 부터 11월 5일까지 대학·대학원생 및 일반인을 대상으로 실시하였다. 한국인터넷진흥원의 '2010년 인터넷이용실태조사'에 따르면 연령별 인터넷 이용률이 20대가 99.9%, 30대가 99.3%로 타 연령층에 비해 월등히 높았다(50대: 55.2%, 60대 이상: 21.8%). 또한 개인정보 제공이 필수적으로 요구되는 인터넷쇼핑 이용률은 20대가 90.1%, 30대가 77.4%로 각각 1위와 2위이다. 인터넷뱅킹 역시 20대가 61.1%로 가장 높고, 다음으로 30대가 59.4%를 나타내고 있다[15]. 즉 2·30대가 인터넷 정보서비스를 가장 활발히 이용하고 있는 연령대이고 개인정보 침해사고에 민감하게 반응하며 유경험자가 가장 많고, 설문의 제반 환경을 쉽게 이해할 것으로 판단했다. 따라서 본 연구에서 하고자 하는 온

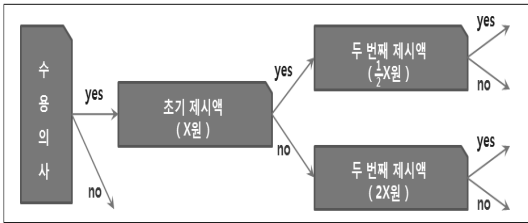
라인상의 개인정보 문제를 다루는데 있어서 대표성을 가질 것이라 가정했다. 물론 본 연구에서 표본설계 및 추출의 한계가 있었기에 이후 산출되는 WTA 값이 인터넷 이용자들의 가장 타당한 대푯값이 되기에는 무리가 있음을 밝힌다. 이를 해결하기 위해서는 추후 연구에서 다단계층화집락추출 등의 표본추출이 필요하다. 배포한 설문지는 총 564부이며, 이 중 응답설문은 559부였다. 결과 분석에서는 이중양분선택형 질문에 대한 응답이 서로 모순되거나 개방형 질문의 응답과 극명한 차이를 보이는 경우, 그리고 기타 불량응답을 제외하여 총 552명에 대한 자료를 분석하였다.

설문조사에 포함되는 주요 내용은 첫째, 온라인상의 개인정보 침해사고 대표 사례 소개, 둘째, 개인정보 침해사고에 대한 인식 및 위자료 문제에 관한 사전 정보 등의 인지도, 셋째, 개인정보 침해사고 경험 유무, 넷째, 개인정보 침해사고 개요 설명, 다섯째, 시나리오별 수용의사 여부 질문, 여섯째, 위자료 경감 요인에 대한 수용 여부 등으로 구성하였다.

다섯째 단계의 시나리오는 유·노출 개인정보의 내역에 따라 시나리오①, ②, ③으로 단계화하고 각각에 대해 직접질문법과 이중양분선택형법을 병행하여 적용하였다. 시나리오는 유·노출 개인정보의 조합에 따라 수많은 유형이 있지만 한국내 인터넷 정보서비스 이용시 발생할 수 있는 대표유형을 선택하였다. 또한 이 세가지 유형은 기존 판례와 직접 비교가 가능하고, JNSA JO모델의 유형 분류에도 부합된다[표 3].

[표 3] 시나리오 구성

	시나리오①	시나리오②	시나리오③
유·노출 개인정보 내역	이름, (휴대)전화번호, (이메일)주소	이름, (휴대)전화번호, (이메일)주소 + 주민등록번호, 아이디	이름, (휴대)전화번호, (이메일)주소 + 주민등록번호, 아이디 + 계좌번호, 신용카드번호, 구매내역 (또는) 의뢰기록, 신체정보, 소득, 직장, 경력, 사적인 이메일 내용



(그림 2) 이중양분선택형법 질문방식

본 연구에서 적용한 이중양분선택형법 질문형식은 그림 2와 같다. 우선 개인정보 침해사고에 대한 위자료를 수용할 의사가 있는 개인들을 대상으로 초기 제시액(X원)을 수용하겠는가에 대해 질문한다. 이에 동의할 경우는 두 번째 제시액을 $\frac{1}{2}X$ 원으로 제시하여 동의 여부를 질문하고, 비동의할 경우는 두 번째 제시액을 2X원으로 제시하여 동의 여부를 질문한다.

본 연구에서는 [표 3]의 시나리오 ①, ②, ③에 대하여 각각 JNSA JO모델의 산출값을 기준으로 하여 구간별로 초기제시액을 설정하였다. CVM에서 초기 제시액이 상당히 중요한 것을 감안하면 이는 기존 연구들이 단지 사전조사 또는 연구자의 판단에 의해 초기제시액을 결정한 것에 비하여 타당성을 높였다.

개인정보 침해사고에 따른 위자료청구사례를 마스크를 통해 접한 경험을 나타내는데 85.7%가 있는 것으로 응답했다[표 4]. 이것은 한국에서 지난 2008년부터 천만명 단위의 대형 사고가 연이어 발생함에 따라 마스크를 통해 대대적으로 보도된 것이 영향을 미친 것으로 판단된다. 이 결과는 많은 개인들이 개인정보 침해사고가 발생한다면 자신도 동일하게 손해배상(위자료)청구소송 등의 피해구제활동에 참여할 수 있다는 인식을 갖춘 것이라 해석할 수 있다.

개인정보보호의 중요성에 대한 인식은 대다수(93.0%)가 매우 중요하거나 중요하다고 응답해 높은 수준을 나타냈다[표 5]. 이는 정보화 사회를 살아가면서 수많은 개인정보가 노출되고 있고, 이에 대해 많은 응답자들이 위험성을 지각하고 있다는 반증이다. 즉 자신의 개인정보가 안전하게 보호되길 바라는 것으로

(표 4) 개인정보 침해사고에 따른 위자료 청구 사례의 마스크를 통한 노출 경험

	빈도	상대빈도
없다	79	.143
있다	473	.857
합계	552	1.000

(표 5) 개인정보보호의 중요성 인식

	빈도(상대빈도)	축적빈도(상대축적빈도)
전혀 중요하지 않다	-	-
별로 중요하지 않다	6 (.011)	6 (.011)
보통이다	33 (.060)	39 (.071)
중요하다	188 (.341)	227 (.411)
매우 중요하다	325 (.589)	552 (1.000)

추후 개인정보 침해사고에 대한 대응이 적극적으로 이루어질 개연성을 내포하고 있다.

표4 에서 개인정보 침해사고에 따른 위자료청구사례를 마스크를 통해 접한 경험(85.7%)에 비해 이와 관련한 구체적인 위자료 액수에 대해서는 상대적으로 잘 모르는 것으로 나타났다[표 6]. 이는 개인정보 침해사고 사실과 소송 참여에 대한 보도는 많았지만 정작 판결이나 피해보상 등의 결과에 대한 사실 보도는 적었던 점과 아직까지 판례가 극소수였던 것이 원인이라 볼 수 있다. 이러한 위자료 수준에 대한 사전 정보는 행동의 귀결이 불확실한 상황에서 합리적인 경제주체의 판단은 결과에 관한 효용의 기대치에 입각하여 이루어진다는 개인들의 기대효용이론에 입각하여 피해구제활동 참여 여부에 지대한 영향을 미칠 것으로 예상된다. 또한 위자료 수준에 대한 사전 정보가 없다는 것은 그만큼 개인정보의 가치를 평가하는데 있어서 준거점이 없다고 볼 수 있다.

조사결과 응답자의 28.6%에 해당하는 158명이 개인정보 침해사고 경험이 있는 것으로 나타났다[표 7]. 이 가운데 피해 횟수는 69.0%에 해당하는 109명이 1회로 응답하여 가장 많이 차지했다[표 8]. 이는 실제 개인정보 침해사고 발생 통계치에 비해 낮은 수준으로 사고 발생시 해당 기업이나 조직의 사고 공지가 제대로 이루어지지 않고 있음을 방증하는 것이다. 근본적으로 개인정보 시장은 수요자(기업·조직)와 공급자(개인)간의 정보 비대칭성으로 인하여 유발되는 문제가 많으며 이는 감독기관의 법률적·정책적 역할이 중요함

(표 6) 개인정보 침해사고에 대한 위자료의 사전 정보

	빈도(상대빈도)	축적빈도(상대축적빈도)
전혀 모른다	212 (.384)	212 (.384)
잘 모른다	273 (.495)	485 (.879)
보통이다	61 (.111)	546 (.989)
잘 안다	5 (.009)	551 (.998)
매우 잘 안다	1 (.002)	552 (1.000)

을 일깨워주는 사실이다.

(표 7) 개인정보 침해사고 경험

	빈도	상대빈도
없다	186	.337
모른다	208	.377
있다	158	.286
합계	552	1.000

(표 8) 개인정보 침해사고 경험 횟수

	빈도(상대빈도)	축적빈도(상대축적빈도)
1회	109 (.690)	109 (.690)
2회	28 (.177)	137 (.867)
3회	12 (.076)	149 (.943)
4회	5 (.032)	154 (.975)
5회	2 (.013)	156 (.987)
10회	2 (.013)	158 (1.000)

한편 개인정보 침해사고 유경험자 158명 가운데 손해배상청구 소송 또는 분쟁조정 신청 경험이 있는 사람은 4명으로 나타났다. 4명의 각 1회별 청구액과 배상액은 표 9와 같다.

(표 9) 실제 손해배상청구 소송 또는 분쟁조정 금액

청구액(만원)	배상액(만원)
25	25
50	0
50	20
100	0

위자료 수준을 측정하기에 앞서 개인정보 유·노출로 인한 정신적인 피해에 대하여 위자료 지급을 요구할 의사가 있는지 여부가 중요하다. 이에 대하여 유·노출된 개인정보의 내역에 따라 차이를 나타냈다. 구체적으로 시나리오①에 대해서는 50.2%가 시나리오②는 85.0%, 시나리오③은 88.8%가 위자료 청구 의사를 보였다(표 10). 시나리오②와 시나리오③의 경우 개인정보의 민감도가 높기 때문에 당연한 결과로 보여진다.

본 연구에서는 2회에 걸쳐 개방형 질문인 직접질문법을 통해 WTA를 추정하였다(표11). 1차 응답을 기준으로 보면 시나리오①은 314,400원, 시나리오②는 668,100원, 시나리오③은 3,226,900원으로 추정되었다. 또한 시나리오①에서 시나리오③으로 갈수록 표준편차가 크게 증가하였는데 이는 개인정보의 민감도가 높아질수록 개인별로 생각하는 가치 수준의 변화폭

(표 10) 위자료 청구 의사

	위자료 청구 의사		
	전체	있음	없음
시나리오①	552	277 (.502)	275 (.498)
시나리오②	552	469 (.850)	83 (.150)
시나리오③	552	490 (.888)	62 (.112)

이 커지는 것으로 나타났다. 그리고 2차 추정 금액의 경우 1차에 비해 다소 감소한 경향을 보이는데 이는 위자료의 기준값이 공개된 후의 응답이므로 일종의 준거점 역할이 영향을 미친 것으로 예상된다. 결과에 대한 구체적인 논의는 다음 장의 '위자료 산정에 대한 논의'에서 통합적으로 후술하였다.

(표 11) 직접질문법을 통한 WTA

(단위: 만원)

	N	응답 순서	평균	S.D.	중앙값	최빈값
시나리오①	277	1차	31.44	67.4	10	10
		2차	25.97	63.2	15	10
시나리오②	469	1차	66.81	130.7	40	100
		2차	61.39	123.7	45	50
시나리오③	490	1차	322.69	783.1	100	100
		2차	324.16	769.7	171	100

앞서 제시한 이중양분선택형법에 대한 WTA 추정모형을 토대로 계산한 결과 대표적 응답자의 수용의 사금액은 시나리오①이 233,366원, 시나리오②가 698,881원, 시나리오③이 2,595,845원으로 추정되었다(표12).

(표 12) 시나리오별 이중양분선택형법을 통한 WTA

(단위: 원)

시나리오	①	②	③
Median WTA	206,897	614,561	2,320,615
Mean WTA	233,366	698,881	2,595,845

[표 13] 사후 대처에 따른 영향

영향 요인	위자료 경감 용의 (N=552)
자발적인 사고공지	408 (73.9%)
사후조치의 신속성, 적절성, 보완성	460 (83.3%)
사고고지 및 피해회복조치 이행	473 (85.7%)

개인정보 침해사고가 발생하면 대다수의 기업은 사고 자체를 은폐하려는 경향이 있다. 이로 인하여 2차, 3차 피해 발생의 위험성을 가중시키는 결과를 불러오기도 하고, 발각되지 않고 넘어갈 경우 여타 기업들이 개인정보보호 노력에 소홀히 하는 풍토를 조장할 우려도 있다. 환언하면 신속하고 적절한 사후 대처는 정보주체인 개인들은 물론 기업의 입장에서도 피해 확산을 막고, 최소화할 수 있는 최선의 방안이다. 이에 대하여 응답자들도 해당 기업이 적극적인 사후 대처를 할 경우 기업의 책임 경감 용의가 있는 것으로 나타났다 [표 13]. 결과적으로 기업의 입장에서는 법적 책임과 더불어 도의적 책임을 다하는 것이 손실을 최소화 하는 방안이 될 것이다.

V. 위자료 산정에 대한 논의

판례상 위자료, JNSA JO모델 산출값, 기존 연구, 본 연구의 결과를 종합하여 보면 표 14와 같다. 판례상 위자료는 10~30만원 수준을 보이고 있는데 이 금액 역시 1심과 2심을 거치며 반복된 것이다. 또한 위자료 산정의 명확한 기준이나 객관적인 근거 제시가 불투명하다. 한편 JNSA JO모델의 산출값과는 유사한 경향을 보인다. 하지만 JNSA JO모델은 앞서 언급한대로 실무적 위자료 산정 모델로서 필요성과 활용성 측면에서는 우수하지만 JO모델 역시 일본 내 기존 판례와 전문가들의 합의로 개발된 모델이기에 피해자인 개인들의 의사는 충분히 반영되지 못한 점을 지적할 수 있다. 위자료 산정은 원고와 피고간의 공방과 합의의 과정을 거쳐 법원의 판단을 통해 도출된다. 그리고 실제로 위자료를 수용하는 것은 피해 당사자인 개인들임을 고려할 때 위자료 산정에 이들의 가치평가가 반영되어야 함은 당연하다. 판례상의 금액과 본 연구를 통해 산출된 개인들의 위자료 수용의 사금액 수준을 비교해 보면 괴리가 있음을 분명히 확인할 수 있다.

[표 14] 주체별 위자료 수준의 경향

(단위: 천원)

구분	개인정보 내역	판례	JNSA JO 모델	기존 연구	본 연구	
					직접 질문을 통한 수용 사금액	이중 양분 선택을 통한 수용 의사 금액
시나리오 ①	이름, (휴대)전화번호, (이메일)주소	100	78	7,563	314	233
시나리오 ②	①+주민등록번호, 아이디	200	234		668	698
시나리오 ③	②+계좌번호, 신용카드번호, 구매내역(또는)의료기록, 신체정보, 소득, 직장, 경력, 이메일 내용	300 (1심 700)	859		3,226	2,595

한편 본 연구의 산출값 역시 타당성이 있는지 검토할 필요가 있다. 우선 기존 연구와 비교를 해보면 기존 연구에서는 유·노출 개인정보의 유형에 따른 상황을 분류하지 않고 단순히 개인정보 침해사고로 접근하여 개인들의 수용의사금액을 추정하였다. CVM의 특성상 WTA는 과추정(Overestimate)될 우려가 있다. 특히 조건 오설정 편익(Misspecification Bias)³⁾가 극복되지 않은 상태에서 도출된 756만원이라는 추정치는 상당히 과추정되었다고 판단된다. 또한 개인정보의 민감도에 따라 개인들이 입는 정신적 피해정도가 확연히 다름이 분명한데 이를 간과한 것은 한계점으로 지적할 수 있다. 본 연구에서는 이를 보완하기 위해 인터넷 정보서비스를 이용하는데 발생할 수

3) 응답자가 해당 가상시장과 평가대상을 적절하게 이해하고 현실성을 느낄 수 있도록 설문은 가상적 시장의 성격과 조건을 응답자에게 적절히 주지시켜야 한다. 그러나 이과정에서 응답자가 시장의 조건을 오해하게 되면 조건 오설정 편익이 나타난다[16].

있는 대표적 유형을 세 가지 시나리오로 구분하여 설계하였으며, 초기 제시액에 따른 시작점 편의를 최대한 줄이고 타당성을 높이기 위해 JNSA JO 모델 산출값을 기준으로 하였다. 또한 응답자들이 상황을 정확하게 이해하고 현실적이고 신중한 판단을 하도록 설문문을 구성하고 주의사항을 강조하였다. 이를 통해 응답자들이 현실적인 증거 기준을 가지고 응답하도록 통제하였다. 특히 시나리오①의 경우 응답자의 49.8%가 위자료 청구 의사가 없다고 하는 것을 보면 아래의 산출값이 비현실적이거나 맹목적인 금액은 아님을 간접 확인 할 수 있다. 그리고 참고적으로 전문가(총 20명) 설문문에 의한 결과에 따르면 시나리오①의 경우 135천원, 시나리오②는 611천원, 시나리오③은 6,394천원으로 나타났다. 이는 전문가 집단이 개인정보 침해 사고 발생시 배상책임이 있는 즉 개인정보를 취급하는 기업이나 조직의 인원으로 구성된 것에 비추어 매우 고무적인 결과이다.

VI. 결론

5.1 결론 및 시사점

정보화의 역기능과 마찬가지로 개인정보도 상업적 가치가 증대되면서 불법적 거래나 유통, 유·노출 사고 등의 개인정보 침해사고가 발생하고 있다. 이에 따라 관련법에 의거하여 손해배상청구소송 또는 분쟁조정 등의 피해구제 활동이 증가하고 있다. 이 과정에서 손해배상액을 산정하게 되는데 이 가운데 정신적 피해에 대한 배상인 위자료의 경우 가상의 가치로서 비시장재이며 교환가격이 존재하지 않으므로 정량적 산정의 어려움이 있다. 이러한 연유로 기존의 판례들을 살펴보면 위자료 산정에 대한 명확한 기준이나 객관적인 근거 제시가 불투명하며 일관성이 낮을 뿐 아니라 피해 당사자인 개인들의 가치평가는 제대로 반영되지 못하고 있다. 과거 개인정보보호를 위한 지불의사금액을 추정하는 등의 개인정보의 가치를 측정하고자 하는 연구는 소수 있었으나, 이는 피해보상에 상응하는 위자료와는 부합되지 않는다. 이에 대한 대안으로 본 연구에서는 시장에서 거래되지 않아 가치에 대한 정보를 얻을 수 없는 재화에 대한 개인들의 가치평가를 추정하기 위해 CVM을 이용하여 유형별 WTA를 추정하였다. 이 과정에서 개인정보의 피해 유형에 따라 시나리오를 구분하고, 초기 제시액에 따른 시작점 편의를 최대한 줄이고 타당성을 높이기 위해 JNSA JO 모델

산출값을 기준으로 결과를 도출하였으며, 이를 통해 시사점을 제시하였다.

더불어 개인정보 침해사고에 대한 위자료 청구의 제도적 개선과 정형화된 위자료 산정모델의 필요성, 활용가치 및 적용방안에 대해 모색하였으며 개인들의 인식을 바탕으로 기업의 책임영향 요인과 대처방안을 분석하였다. 특히 위자료 문제를 다양한 접근을 통해 수용자 관점에서 조명했다는 점과 한국에 부재한 위자료 산정의 정형화된 모델에 관한 연구를 시도했다는 점이 차별화 된다고 본다. 이러한 연구는 단순히 위자료 산정의 접근 방안을 제시한 것에 그치는 것이 아니라 개인정보의 가치를 측정함으로써 개인정보를 안전하게 관리해야 할 책임이 있는 기업이나 조직들에게 경각심을 인식시켜 개인정보보호 인식을 제고할 수 있고, 한편으로는 관련 보험 상품 개발 및 보험 투자 등의 개인정보보호 투자에 대한 의사결정에 도움을 줄 수 있을 것이라 기대한다.

요컨대, 과다한 피해보상은 거시적인 측면에서 사회적 비효율성을 높이지만 이러한 피해보상이 개인정보 제공자(정보주체인 개인)와 수요자(기업이나 조직)간에 적절히 조정되고 타협될 경우, 즉 적절하고 보편타당한 위자료가 형성될 경우 제공자와 수요자 간의 정보 비대칭성에서 유발되는 문제를 상쇄할 수 있으며 개인정보보호가 중요함에도 불구하고 기업이나 조직이 책임을 회피하거나 의무를 소홀히 하는 근본적인 왜곡을 피할 수 있다. 그리고 개인정보보호의 불확실성에 따른 사회적 비효율성과 개인정보 시장의 왜곡을 방지하기 위해서는 정부의 개입을 보다 적극적으로 수행해야 할 필요성이 있다. 앞서 기술한바와 같이 개인들은 민감도가 낮은 개인정보 침해사고의 경우 위자료 청구 의사가 없다는 점, 적절한 사후대처가 주요하게 영향을 미친다는 점 등을 미루어보아 관련법 개정이나 제도적 장치 보완이 필요하다.

5.2 연구 한계점 및 향후 연구

본 연구를 진행하면서 연구 주제와 관련하여 기존 연구들이 많지 않아 어려움이 있었다. 그만큼 새롭게 부각될 수 있는 연구 분야라고도 볼 수 있다. 본 연구의 한계점임과 동시에 향후 연구의 방향은 다음과 같다.

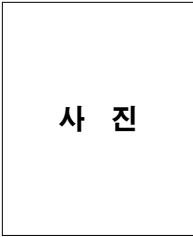
우선 표본 추출의 한계를 지적할 수 있는데 이는 추후 다단계층화집락추출(Stratified Multi-stage Cluster Sampling) 등의 통계적 가치를 높이는 방

식이 필요하다. 또한 개인들의 특성을 반영하여 집단을 세분화하여 조사하는 것이 필요하다. 그리고 보다 다양한 기법을 통해 위자료 수준을 분석하고 비교하여 실제 가치평가에 보다 근접한 값으로 수렴하도록 하는 노력이 요구된다. 또한 손해배상의 기준을 법률화하여 정착시키는 방향의 연구가 필요하다고 판단된다. 그리고 정보통신기술의 발달에 따라 위치정보, 바이오정보, 영상정보 등 새로운 형태의 개인정보들이 창출되는 것에 발맞춰 연구 범위를 넓힐 필요가 있다. 이와 더불어 위자료 문제와 관련하여 조사내용을 추가한 개인정보 관련 실태조사가 지속적으로 이루어지고, 체계성도 강화될 필요성이 있다고 본다. 특히 개인정보침해사고의 발생 트렌드(빈도, 규모, 유형 등)와 위자료 금액간의 관계 분석과 추이분석도 유용할 것이다. 나아가 한국 실정에 적합한 개인정보 침해사고에 대한 위자료 산정 모델을 개발하는 연구가 필요하다고 판단된다.

참고문헌

- [1] 장종인, “개인정보시장에서 주민등록번호의 이용”, 정보통신정책, 17(18), pp. 26-50, 2005년 10월.
- [2] 한국인터넷진흥원 인터넷통계정보검색시스템, <<http://isis.kisa.or.kr/>>, 2012년 2월
- [3] 권홍, 김태성, “개인정보 침해사고에 대한 정량적 위자료 산정 모델 고찰”, 한국경영정보학회 춘계학술대회, 10(1), pp. 432-436, 2010년 6월.
- [4] 이기혁, 윤재동, “민간 기업의 개인정보 유출 위험에 따른 측정 방법과 그 사례에 대한 연구”, 정보보호학회지, 18(3), pp. 92-100, 2008년 6월
- [5] Xin (Luna) Dong, “A Platform for Information Management and Integration”, Proceedings of VLDB 2005 PhD Workshop, pp. 26-30, August 2005
- [6] David L. Mothersbaugh, William K. Foxx II, Sharon E. Beatty, “Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information”, Journal of Service Research, 15(1), pp. 76-98, December 2011
- [7] 김여라, 이해춘, 유진호, “가상가치접근법(CVM)을 활용한 개인정보보호의 가치 산출 방법론 고찰”, 정보보호 Issue Report, 한국정보보호진흥원, 2007년 2월.
- [8] 이해춘, 안경애, “CVM을 이용한 개인정보 유출의 손실가치 분석”, 생산성논집, 22(2), pp. 1-24, 2008년 6월.
- [9] 유진호, 지상호, 임종인, “개인정보 유·노출 사고로 인한 기업의 손실비용 추정”, 정보보호학회논문지, 19(4), pp. 63-75, 2009년 8월.
- [10] 김철완, 정준현, 이상원, 오영석, 개인정보보호제도 시행의 경제·사회적 파급효과 분석연구, 정보통신정책연구원, 정책연구 01-05, 2001년 12월.
- [11] PGP Corporation, 2008 Annual Study: Cost of a Data Breach, Ponemon Institute LLC, April 2009.
- [12] 한창희, 채승완, 유병준, 안대환, 박채희, “기업의 개인정보 유출로 인한 경제적 피해규모 산출방법”, 한국전자거래학회지, 16(4), pp. 17-31, 2011년 11월
- [13] 김정은, 여정성, “소비자의 개인정보보호 가치평가에 영향을 미치는 요인에 관한 연구”, 소비자학연구, 21(2), pp. 341-366, 2010년 6월
- [14] JNSA, 2009年 情報セキュリティインシデントに關する 調査報告書, JPO Japan Network Security Association, September 2010.
- [15] 한국인터넷진흥원, 2010년 인터넷이용 실태조사, 연간보고서, 방송통신위원회, 2010년 12월.
- [16] 김태운, 김상봉, 비용·편익분석의 이론과 실제: 공기업평가와 규제영향분석, 박영사, 2004년 8월.

〈著者紹介〉



권 홍 (Hong Kwom) 학생회원
 2011년 2월: 충북대학교 경영정보학과 석사
 <관심분야> 개인정보보호, 정보보호



이 은 주 (Eun-Ju Lee) 학생회원
 2005년 2월: 충북대학교 경영정보학과 학사
 2009년 3월~2012년 2월: 충북대학교 경영정보학과 조교
 2011년 9월~현재: 충북대학교 경영정보학과 석사과정
 <관심분야> 정보보호, 개인정보보호 정책



김 태 성 (Tae-Sung Kim) 종신회원
 1997년 2월: KAIST 산업경영학과 박사
 1997년 2월~2000년 8월: 한국전자통신연구원 정보통신기술경영연구소 선임연구원
 2005년 1월~2006년 2월: Univ. of North Carolina at Charlotte 방문교수
 2010년 7월~현재: Arizona State University 방문연구원
 2000년 9월~현재: 충북대학교 경영정보학과 교수
 <관심분야> 정보보호 분야의 경영 및 정책 의사결정



전 효 정 (Hyo-Jung Jun) 학생회원
 2001년 2월: 충북대학교 경영정보학과 학사
 2003년 8월: 충북대학교 경영정보학과 석사
 2003년 9월~2007년 5월: 한국전자통신연구원 사업기획팀 기술원
 2006년 9월~현재: 충북대학교 경영정보학과 박사과정
 <관심분야> 정보시스템 정보보안, 보안감사, 정보보호정책