http://www.calsec.or.kr/jsebs
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.19, No.3, Aug 2014, pp.1-21
http://dx.doi.org/10.7838/jsebs.2014.19.3.001

금융거래 고객정보 침해사고 보상보험의 구성 및 정책방향

Composition and Policy Direction of Compensation Insurance Against Customer Information Infringements in Financial Transactions

김종환(Jong Hwan Kim)*, 임종인(Jong In Lim)**

초 록

개인정보는 금융거래의 성립조건이며 금융회사의 핵심자산이다. 그러나 정보사회의 부작용으로써 나타난 개인정보 침해사고는 중대한 사회적 위험이 되고 있으며, 이러한 위험은 개인과 회사의 실제적 피해로써 현실화되고 있다. 본 연구는 소비자의 손실 측면에서 개인정보 침해사고로 인해 금융 분야에서 발생한 금전적, 정신적 손해 현황을 분석하고, 이러한 실제 손해를 최소화하기 위한 위험전가의 수단으로써 보험의 유용성을 제시하였다. 그리고 개인 정보 침해사고 보상보험의 구성요소와 보험료의 산정원리를 검토하고 최종적으로 이러한 보험 제도를 활성화하기 위한 정책을 제안하였다. 위험관리의 한 방법으로써 보험은 소비자 보호와 회사의 재무적 건전성을 동시에 확보할 수 있는 유용한 수단이며, IT 리스크의 계량적 측정을 위한 기반을 제공할 수 있다.

ABSTRACT

Personal information is a requisite for financial transactions as well as a core asset of financial companies. However, as a side effect of the information society, personal information infringements have emerged as significant social risks, causing realized loss to individuals and companies. This study analyzes results of financial and emotional loss in terms of consumer loss and also presents usefulness of insurance in order to minimize such actual damages as a means of risk transfer. In addition, this study investigates components and premium calculation principles of compensation insurance against personal information invasion and finally presents policies to activate these insurance product. As a method of risk management, insurance not only is a useful tool to guarantee consumer protection and companies' financial soundness simultaneously but also provides a basis of quantitative measurement of IT risks.

키워드 : 개인정보 침해사고, 정보보호 보험
Personal Information Infringement, Information Security Insurance

* CIST(Center for Information Security and Technologies), Korea University, Seoul, Korea(kiwimyth@empal.com)
** Corresponding Author, CIST(Center for Information Security and Technologies), Korea University, Seoul, Korea (jilim@korea.ac.kr)
2014년 04월 28일 접수, 2014년 05월 29일 심사완료 후 2014년 06월 16일 게재확정.

1. 서 론

경제활동을 하는 거의 모든 개인은 금융거래를 하고 있다. 개인과 금융회사간의 금융거래는 개인정보 제공을 조건으로 성립하므로 금융회사는 우리나라 국민 대부분의 개인정보를 수집하여 이용하고 있다고도 볼 수 있다. 가계에서의 금융이 재산의 가치를 보존하고 부의 증대를 이루는 주요 수단임을 고려하면 금융회사를 통한 개인정보와 금융거래정보의 유·누출 사고에 사회가 민감하게 반응하는 것은 당연한 귀결이다.

2014년 1월 언론에 알려진 국내 3개 신용카드회사의 대규모 개인정보 유출 사건은 개인정보 부실관리의 실태와 문제점을 여실히 보여주었다. 동 사건으로 각 사의 대표이사가 사임하고, 고객이탈로 인해 영업 기반이 훼손되는 등 개인정보 유출 위험은 이미 전사적 위험으로써 회사의 경영 전반을 위협하고 있으나, 이에 대한 대책은 위험의 통제를 기반으로 한 사전 예방적 조치에 집중되고 있다.

개인정보 침해 위험을 상시적인 위험으로 인식하기 위해서는 '정보유출을 완전히 차단할 수 있다'는 가정보다는 '정보는 유출될 수 있다'는 가정 하에 출발해야 한다. 이러한 가정은 보안의 사전 예방적 기능뿐만 아니라 손실 복구의 중요성을 강조한다. 특히, 금융소비자 보호의 강화, 개인정보 보호에 대한 인식 제고, 기업의 책임 강화 등의 사회적 경향으로 인해 개인정보 유출은 기업에 대한 신뢰도 저하, 고객 이탈 및 대규모 소송 등을 촉발하여 기업의 실제적·재무적 손해로 이어질 수 있다.

개인정보 침해사고 보상보험은 고객에 대한 피해를 신속하고 합리적으로 보상함으로써 소비자를 보호하는 실질적 수단이 되며, 고객에 대한 손해배상으로 기업에게 발생하는 재무적 손실을 보전함으로써 기업의 건전성을 확보하기 위한 유효한 수단이 될 수 있다.

본 논문은 이와 관련하여 보상보험의 유용성을 제시하고, 개인정보 침해사고로 인해 금융 분야에서 발생한 손실 현황을 분석한 후, 손실에 대응되는 비용(보험료)을 산출하는 과정과 그 구성요소를 검토한다. 그리고 최종적으로 보험시장이 활성화되기 위한 정책방향을 수요측면, 공급측면, 유효성측면에서 제안하고자 한다.

보험의 구성을 이해하는 과정은 보험료의 산출 과정을 이해하는 것과 같다. 보험료의 산출을 위해서는 위험의 측정 및 손해의 산정이 핵심 요소이다. 따라서 본 논문의 연구 범위는 개인정보 침해로 인한 손실가치 및 위험의 측정과도 관련될 수 있다. 아울러, 기업과 개인 중 개인(금융소비자) 관점에서의 손실을 연구의 범위로 한다.

2. 관련 연구

2.1 정보보호 보험시장

보험개발원(2012)은 개인정보 보호가 국가과제로 대두되고 있으며, 2011년 9월부터 시행된 개인정보보호법에서 '개인정보유출통지제도', '입증책임의 전환', '단체소송' 등의 책임요건을 강화하여 소송 및 보험수요의 증가가 예상된다고 하였다. 개인정보 유출과 관련

된 보험의 활성화를 위해서 담보범위 확대, 중소기업용 단체보험의 개발 등 국내 환경에 맞는 보험상품의 정비, 공공기관의 보험가입 의무화 우선 실시 등 점진적 보험가입 의무화 등을 제시하였다[13].

배병환 외(2013)는 미국, 일본, 우리나라 등의 정보보호 보험 상품을 소개하고, 보험시장 활성화를 위해 단계적인 보험 가입 의무화 제도 도입, 정부차원의 보험 가입 활성화 유도 정책, 정보보호 전문기관과 보험전문기관과의 협력, 기업들의 인식제고를 위한 홍보 활동 강화를 제시하였다[1].

이 연구들은 개인정보 유출 위험을 관리하기 위한 수단으로 보험의 유용성과 필요성을 제기한 거의 유일한 국내 연구자료로서 의의가 있다.

2.2 개인정보 유출 손실가치 측정 : 개인측면

이해춘 외(2008)는 개인들을 대상으로 설문을 통해 개인정보 유출시 손해배상에 대한 수용의사금액(Willingness to Accept, WTA)을 약 756만 원으로 산정하고, 이를 통해 전체 손실가치(2006년 기준 약 32조 원)를 추정하였다[19].

JNSA(Japan Network Security Association)는 2003년부터 매년 개인정보 사고에 대한 조사・분석 자료를 토대로 “Information Security Incident Survey Report”를 작성・배포하고 있다. JNSA에 의한 개인정보 유출에 따른 손해 배상액 산출식은 “기본정보 가치[500엔] × 정보민감도 × 본인식별 용이도 × 정보 유출 조직의 사회적 책임도 × 사후 평가”로 표현된다[2].

권홍 외(2012)는 개인들을 대상으로 직접 질문법과 이중양분선택형 질문형식을 통해 개인정보 침해 시나리오를 3가지로 가정하여 위 자료 수용금액을 조사하였다[18]. 시나리오 1(이름, 전화번호, 이메일주소 유출)의 경우 직접 질문법, 이중양분선택형 질문법에 대해 각각 314천 원, 233천 원, 시나리오 2(시나리오 1 + 주민등록번호, 아이디 유출)의 경우 각각 668천 원, 698천 원, 시나리오 3(시나리오 2+ 계좌번호, 신용카드번호 또는 의료기록 등 유출)의 경우 각각 3,226천 원, 2,595천 원을 위 자료 금액으로 산정하였다.

이 연구는 개인정보의 가치를 금전적 가치로 환산하여 사회적・잠재적 가치를 추정한 것에 의의를 둘 수 있다. 그러나 이것은 설문조사를 통한 개인 의사를 반영한 결과로써 개인정보 유출사고에 대한 국내 판례상 위자료 금액이 현재 1인당 10만 원 내지 20만 원임을 감안하면 실제 배상기준보다 과대평가된 경향이 있다. 실제로 JNSA의 2010년 보고서에서는 적정 보상액 산정의 경우 판사의 판결에 따라 보상 판결액이 바뀌는 등 추정과 실제가 차이가 발생하는 문제점을 고려해서 유출된 정보의 기본 가치액을 추정하는 원론적 형태로 모델의 방향을 수정하였다[11].

2.3 개인정보 유출 손실가치 측정 : 기업측면

유진호 외(2009)는 Gordon and Loeb(2006)의 손실비용 산출 프레임을 기반으로 기업의 직접적인 손실액을 침해사고 대응비용, 생산

성 손실비용, 잠재적인 법적 책임비용으로 구분하고, 2,800개 사업체에 대한 설문 조사를 통해 파라미터를 추정하였다. 이에 따라 개인정보 침해사고로 인한 총 피해액이 2005년 12,331억 원, 2006년 67,745억 원, 2007년 30,653억 원으로 추정되었다[24].

이 연구는 개인정보 침해사고로 인한 손실규모를 신속하게 파악하기 위한 모형을 제시하였다는 점에서 의의가 있다. 잠재적인 위험을 계량화하기 위해 피해자 전원에 대한 법적 보상금을 계산함으로써 기업의 손실비용 중 약 99%가 법적 손해배상금으로 산출되었으나, 피해자 전원에 의한 소송제기는 실현가능성이 거의 없다는 점에서 기업들의 실무적인 위험관리 기준으로 삼기에는 무리가 있다. 실제로 GS칼텍스 정보유출 사건의 경우 전제 11,517,125명 중 2,200명(0.02%), SK컴즈 사건의 경우 34,954,887명 중 2,882명(0.008%)만이 정보유출 피해자 중 실제 소송에 참여한 당사자 수이다.

3. 개인정보 침해사고 보상보험의 정의 및 기능

3.1 정의

우리나라 상법(제719조)상 책임보험계약이란 피보험자가 보험기간 중에 생긴 사고로 제3자에 대하여 손해배상책임을 짐으로써 입은 손해를 보험자가 보상할 것을 목적으로 하는 손해보험계약을 말한다. 이러한 책임보험의 개념을 인용하면 개인정보 침해사고 보상보험이란 “기업이 보험기간 중에 생긴 개인정보 침해사고로 소비자에게 발생한 손해를 보상할 책임을 짐으로써 입은 손해를 보험자가 보상할 것을 목적으로 하는 손해보험계약”으로 정의할 수 있다. 이는 개인정보 침해사고의 발생으로 인하여 기업에게 생긴 재산상의 직접손해를 보상하는 것이 아니라, 사고의 발생으로 인하여 소비자에게 발생한 손해를 기업이 보상함으로써 입은 간접손해를 보상할 것을 목적으로 하는 점에서 일반손해보험과 다르다[20]. 개인정보 침해는 “원인이나 경로보다는 어떠한 유형이든 마지막 관점에서 각 개인이 겪게 되는 금전적(물리적), 정신적(심리적) 피해”를 의미한다[16].

3.2 보상보험의 기능

첫째, 보험은 기업 및 개인의 재무적 손실을 경감시킬 수 있다. 기업은 존속에 영향을 미칠 수 있는 미래의 거대 손해를 보험료라는 현재의 평균 비용으로 대체함으로써 계속기업으로 성장할 수 있고, 개인은 보험으로 확보된 기업의 배상자력을 통해 실질적인 구제를 받을 수 있다. 곧, 보험은 기업의 재무적 건전성을 확보함과 동시에 소비자를 보호하는 유용한 수단이 될 수 있다.

둘째, 보험은 손실 예방 및 방지의 역할을 한다. 보험료는 과거 사고발생 내역과 그 기업의 정보보호 수준 등에 연계될 수 있으므로 기업은 보험료를 절감하기 위해 보안수준을 제고할 유인을 갖게 된다[7]. 또한 보험회사(이하 ‘보험자’라 한다)는 손실방지, 즉 지급보험금 경감을 위해 여러 면에서 예방 활동을 한다. 중소기업을 대상으로 하는 일본의

개인정보유출보험은 개인정보보호법에 대응한 리스크진단 서비스를 무료로 제공하여 중소기업의 개인정보 유출위험을 줄이는데 기여하고 있다[13]. 보험개발원 보험통계연감에 의하면 우리나라 손해보험회사가 보험사고 예방비로 지출한 비용은 2011년 222억, 2012년 199억 원이다[12]. 이러한 손실 예방 효과는 보험료를 줄이고 사회의 직·간접 손실을 감소시켜 사회의 효용을 증가시키는 역할을 한다.

셋째, 보안산업 시장의 확대 및 기업의 보안 수준 향상에 기여할 수 있다. 보험계약의 체결·인수(underwriting) 및 보험금 지급을 위한 보안사고 조사는 보안 컨설팅 및 전문지식을 필요로 하며 이와 관련한 시장이 확대될 수 있다. 또한, 보험자는 보험계약의 체결·인수 및 보험료의 산정 과정에서 IT 보안표준(Common Criteria, ISO 2700x 등)을 기준으로 삼거나, IT 보안 제품이나 서비스의 인증을 요청할 수 있다[7].

넷째, 보험 계리 데이터의 집적은 IT 리스크 측정 및 관리에 기여할 수 있다. 보험상품 운영을 위해 집적되는 보안 정보는 기업, 산업 또는 우리나라 전체의 IT 리스크 수준을 측정하는데 활용될 수 있으며 이는 궁극적으로 보험료라는 계량화된 지표로 나타나게 된다. 보험료는 과거의 보안사고 경험통계와 미래의 보안사고 발생가능성을 바탕으로 시장에 의해 평가된 실제적 위험 수준이라 할 수 있다.

이하 제 4장과 제 5장에서 개인정보 침해사고로 인한 금융 분야에서의 손해를 보상하는 보험을 구성하고 보험의 유용성을 확인하고자 한다.

4. 손해의 현황 및 보험의 범위

개인정보 침해사고 발생시 소비자의 손실에 대한 보상은 충분한 수준이어야 한다. 따라서 개인정보 침해사고의 손해를 분류하고 그 손실가치를 측정하는 일은 보험이 보상하는 손해 및 담보를 명확히 하는 필수적 과정이다. 본 논문에서는 손실을 금전적 손해와 정신적 손해로 구분하고, 과거 사건의 통계를 이용하여 손실을 집계한다. 이는 그 동안 금융 분야에서 개인정보 침해사고로 발생한 소비자의 손실을 측정하는 일이기도 하다.

4.1 금전적 손해

개인정보 침해로 인한 금전적 손해를 크게 금융사기에 의한 손해와 금융거래를 위한 매체의 침해에 따른 손해로 구분하고 이를 보험의 담보 범위로 한다. 금융사기에 의한 손해는 유·노출된 개인정보를 악용하여 금융소비자를 속여 계좌에서 부당 인출하거나, 신용카드를 부당하게 사용함으로써 발생하는 손해이며, 보이스피싱, 인터넷피싱, 파밍, 카드정보·명의 도용을 통한 신용카드 부정사용 등에 의한 손해가 해당된다. 금융거래를 위한 매체의 침해에 따른 손해는 제 3자가 금융거래에 이용되는 PC, 네트워크, 소프트웨어, 웹사이트 등에 불법으로 접근하여 개인정보·금융거래정보 또는 접근매체의 위·변조를 통해 계좌에서 부당 인출하거나, 신용카드를 부당하게 사용함으로써 발생하는 손해이다. 여기에는 메모리해킹, 카드 위·변조를 통한 신용카드 부정사용 등에 의한 손해가 포함된다.

이와 관련하여 금융 분야에서 발생한 금전적 손해를 <Table 1>에 나타내었다. 2010년부터 2012년까지 3년간 총 피해금액은 2,580억 원(피해건수 : 66,925건)이며, 연평균 피해금액은 860억 원(연평균 피해건수 : 22,308건) 수준이다.

한편, 우리 민법 제750조는 "고의 또는 과실로 인한 위법행위로 타인에게 손해를 가한 자는 그 손해를 배상할 책임이 있다."고 규정하고 있다. 따라서 기본적으로 "과실이 없으면 책임이 없다"는 원칙이 적용되어 있으나, 본 논문에서는 금전적 피해에 대해 무과실책임을 적용(제안)한다. 그 이유는 금전적 피해에 대한 보상이 피해자의 가계경제를 복구하기 위해 우선적으로 필요한 보상이므로 책임여부의 공방으로 인해 비용과 시간을 낭비하지 않고, 신속하고 실질적인 구제를 보장함으로써 실효성 있는 보험의 목적(유용성)을 달성하기 위함이다. 개인의 권리의식이 높아지고 소비자 보호를 강화하면서 불법행위제도가 점차 과실이 없음에도 책임을 인정하는 무과실책임주의로 나아가고 있고, 아울러 입증책임도 피해자로부터 가해자에게 전환되어 기업의 책임이 점점 더 엄격해 지고 있는 추세이다[14].

〈Table 1〉 Financial Loss from Personal Information Infringements in the Financial Section

(unit : record, 100million won)

Classification			2010	2011	2012	Total	Annual Average
Phishing		Record	5,455	8,244	5,709	19,408	6,469
		Amount	554	1,019	595	2,168	723
Illegal Use of Credit Card		Record	10,532	13,857	23,021	47,410	15,803
		Amount	121	133	146	400	133
	Information Theft	Record	675	1,370	6,359	8,404	2,801
		Amount	5	3	9	17	6
	Identity Theft	Record	772	776	843	2,391	797
		Amount	29	35	36	100	33
	Forgery, Falsification	Record	9,085	11,711	15,819	36,615	12,205
		Amount	87	95	101	283	94
Internet Banking Hacking		Record	22	26	59	107	36
		Amount	2.5	2.1	7.2	11.8	4
	Bank	Record	20	26	51	97	32
		Amount	1.7	2.1	4.9	8.7	3
	Non-Bank	Record	2	-	8	10	3
		Amount	0.8	-	2.3	3.1	1
Total		Record	16,009	22,127	28,789	66,925	22,308
		Amount	678	1,154	748	2,580	860

Source : Financial Services Commission, Financial Supervisory Service([10], [8]), Lee, J. K.(a member of the National Assembly, [21]).

또한, 금전적 손해에 대한 무과실책임 보상은 개인정보의 악용에 따른 재산상 침해에 대한 불안감을 상당 부분 해소하여 정신적 손해의 정도를 완화할 수 있는 요건이 될 수도 있다.

4.2 정신적 손해

일반적으로 타인의 불법행위로 인하여 재산권이 침해된 경우에는 그 재산적 손해의 배상에 의하여 정신적 고통도 회복된다고 보아야 하지만, 재산상의 손해 이외에 명예나 신용의 훼손 등으로 재산적 손해의 배상만으로는 회복할 수 없는 정신적 손해가 있는 경우에는 그로 인한 정신적 고통에 대하여 위자료를 지급하여야 한다(대법원 1997. 2. 14. 선고 96다36159판결). 이는 곧, 개인정보 침해로 인한 금전적 손해에 대한 보상이 있더라도 개인정보자기결정권을 침해당한 것만으로 정신적 손해에 대한 청구가 별도로 이루어 질 수 있음을 의미한다.

본 논문에서는 정신적 손해에 대해서는 과실책임(배상책임보험)을 적용한다. 그 이유는 정신적 손해에 따른 손실액을 산정하기가 어렵기 때문인데, 관련 판례가 부족하여 실제 사건의 위자료 집계가 과거 경험통계를 전혀 반영할 수 없고, 현재 정신적 손해의 통상손해 인정여부는 사건에 따라 재판부의 재량에 의해 좌우되므로 재판부의 기준을 예측할 수 없기 때문이다. 또한 정신적 손해에 대한 보상, 즉 위자료의 적정수준에 대한 사회적 합의도 미흡하다. 정신적 손해는 일반 물건을 담보로 하는 보험과 달리 가치측정이 매우 어려우며, 실제로 일본 아이오이손보사의 개인정보유출 배상책임보험의 경우에는 법원에 의해 결정된 위자료를 지급하는 것이 아니라 개인정보가 유출된 개인에게 1건당 500엔을 한도로 위로금을 보상하는 등 계약 당사자 간의 약정에 의해 보상한도를 정해 놓는다[1].

2014년 3월 금융감독원 전자공시시스템에 공시된 사업보고서에 의하면 2014년 1월 카드 3사 사태의 정보유출 규모는 K카드사 4,300만 명, N카드사 2,427만 명, L카드사 1,760만 명으로 총 8,487만 명(중복포함)이며, K카드사의 경우에는 성명, 주민등록번호, 연락처 등 개인정보가, N카드사와 L카드사는 추가적으로 카드번호, 유효기간 등 신용정보까지 유출된 것으로 알려져 있다.

이에 대한 손실 가치를 그 간의 연구결과를 이용하여 측정하고 실제 회사들이 인식하고 있는 위험 수준과 비교해보기로 한다.

권홍 외(2012)의 연구결과에 의하면 K카드사의 경우는 시나리오 2, N카드사 및 L카드사는 시나리오 3에 해당하며, 개인들에 대한 설문조사결과 이중양분선택형법을 통한 수용의사금액은 각각 698천 원, 2,595천 원이다[18]. 이 금액을 카드 3사의 피해인원과 곱하면 위자료 금액은 K카드사 30조 140억 원, N카드사 62조 9,807억 원, L카드사 45조 6,720억 원 등 총 138조 6,667억 원에 달한다. 유진호 외(2009)는 손해배상금 산출을 위한 파라미터로 주민등록번호 등 ID 정보 침해의 경우 20만원(판례), 카드번호 등 금융정보 침해의 경우 30만 원(개인정보분쟁조정사례)을 기준 값으로 사용하였으며, 잠재적인 위험을 계량화하기 위해 반드시 피해자 전원에 대한 법적 보상금이 계산될 필요가 있다고 하였다[24]. 이에 따르면 추정 손실비용은 K카드사 8조

6,000억 원, N카드사 7조 2,810억 원, L카드사 5조 2,800억 원 등 총 21조 1,610억 원이다.

이와 대조적으로 K카드사는 투자설명서(2014. 2. 10.)에서 SK컴즈사건의 실제 소송에 참여한 당사자수가 0.008%에 불과하였으나, 본 사건의 경우 보수적으로 판단하여 실제 소송에 참여할 당사자수를 1%로 산정하고 20만 원의 정신적 손해를 인정한 판례를 적용하여 최대 약 860억 원(43만 명×20만 원)의 보상액이 발생할 것으로 추정하였다[9]. 같은 논리로 N카드사는 약 485억 원(24.3만 명×20만 원), L카드사는 약 352억 원(17.6만 명×20만 원)을 추정하는 등 카드 3사는 정신적 피해에 대한 손해배상액으로 최대 총 1,697억 원을 추정하였으며, 이에 대해서도 실제로 발생할 가능성은 낮을 것으로 보고 있다. 이 금액이 모두 실현되려면 약 85만 명이 소송에 참여하고 모두 승소하여 1인당 20만 원의 위자료를 지급받아야 한다.

예상 손실을 측정하는 기준을 결정하는 것은 중요하다. 이 기준을 통해 기업은 보안 투자의 수준을 결정하기도 하고, 손실에 대비한 충당금을 적립할 수도 있다. 아울러 이 기준은 보험가액을 결정하는 중요한 요인이 된다.

상기 사례에서 보상의 수요자(개인, 보상을 요구하는 측)와 보상의 공급자(기업, 보상을 제공하는 측)가 모두 '최대 손실'을 강조하면서도 그 추정 값이 크게 다른 것은 최대 손실에 대한 개념적 차이에서 비롯된다. 본 논문에서는 이를 MPL(Maximum Possible Loss)과 PML(Probable Maximum Loss)로 구분하고자 한다. MPL은 최악의 상태에서 발생할 수 있는 최대의 손실액을 말하며, PML은 정상적인 상태에서(있을 수 있는 환경 하에서) 발생 가능한 최대손실액을 말한다[14]. 곧, 기존 연구결과[18], [24]에 의한 추정 손실액은 MPL, 카드 3사의 추정 손실액은 PML로 이해할 수 있다.

보험은 현실에서 발생 가능한 실제적 손해를 기준으로 위험을 측정한다. 따라서 본 논문에서는 MPL이 아닌 PML로 정신적 손해의 손실액을 추정한다. PML은 항상 고정적인 것이 아니며 위험 환경의 변화와 함께 변동할 수 있다. 즉, 향후 소송참여자의 비율이 증가할수록 판례의 위자료 금액이 증가할수록 PML은 MPL에 근접하게 된다.

2008년부터 2013년까지 5년간 금융감독원에 집계된 금융회사의 고객정보 유출사고는 총 17건으로 총 3백 30여 만 건의 고객정보가 유출되었다[15]. 연평균 3.4건의 개인정보 유출사고가 발생하였으며, 연평균 유출규모는 약 67만 건 수준이다. 이를 PML로 환산하기 위하여 ① 소송에 참가할 당사자의 규모와 법원의 판결금액을 상기 사례에서의 1%와 20만원으로 특정하여 추정한 결과와 ② 실제 일본 아이오이손보사의 개인정보유출 배상책임보험에서 1건당 5,000원(100엔 = 1,000원 가정)의 위자료를 지급하는 경우로 구분하여 산출한 결과 값을 <Table 2>에 나타내었다.

즉, 'PML(①) = 유출건수 × 소송참가율 × 소송승소자 1건당 위자료', 'PML(②) = 유출건수 × 유출 1건당 위자료'로 나타낼 수 있다. 이 때 개인정보 유출 피해자 중 소송참가율을 1%로 가정할 경우, PML(②)에서처럼 소송 전에 유출 1건당 5,000원의 위자료를 일괄 지급하는 것은 소송 후에 소송참가자당 50만 원의 금액을 위자료로 지급하는 것과 같은

〈Table 2〉 Emotional Loss(PML) from Personal Information Security Breaches of Financial Companies

(unit : record, 100 million won)

Year	2009	2010	2011	2012	2013	Total	Average
Incident(Company)	3	2	9	1	2	17	3.4
Leaked Data Records	180,109	815,000	2,032,698	104,000	198,000	3,329,807	665,961
PML(①)	3.6	16.3	40.7	2.1	4.0	66.7	13.3
PML(②)	9.0	40.8	101.6	5.2	9.9	166.5	33.3

가치(소송참가율 × 소송승소자 1건당 위자료 = 유출 1건당 위자료)이다. 이와 같은 비교를 통해 일본의 보험상품(50만 원)이 우리나라 법원의 판례(20만 원)보다 한 사건에 대한 총 보상금 수준이 다소 높음을 추정할 수 있다. 이와 같은 정신적 위자료에 대한 지급조건은 보험자와 보험가입 회사 간의 계약에 의해 결정된다.

5. 보험의 구성

보험료는 기본적으로 보험자의 수입과 예상 지출이 같아지도록 결정하는 수지상등의 원칙에 따른다. 보험계약자가 납입하는 보험료 총액과 보험자가 예상하는 보험금 지급액 및 관련 비용의 총액을 동일한 금액이 되도록 하는 것이다[14]. 본 장에서는 제 4장에서의 손해현황을 토대로 보상보험의 보험료를 결정하는 과정을 전체 시장의 관점에서 예시하고 보험료 산정의 요소와 유용성을 고찰하고자 한다.

5.1 금전적 피해에 대한 보험의 구성

보험은 회사의 위험을 보험자에게 전가하는 유용한 수단이지만, 이러한 기능으로 인해 방관적 위험 내지 정신적 위험상황(morale hazard)이라는 부작용을 초래한다. 보험계약이 체결되었기 때문에 보안사고에 대한 주의력이 이완될 수 있는 것이다. 따라서 공제조항(Deductible clause)을 설정하여 손해액에서 일정액을 기업이 부담하게 함으로써 부작용을 차단할 필요가 있다. 또한, 공제액과 보험료는 서로 반비례하여 공제액이 크면 클수록 보험료는 적어지는 효과를 가진다[14].

현재의 침해정도는 가장 최근의 보안수준에 더 영향을 받는다고 가정하여 2010년 및 2011년 피해금액의 가중이동평균(WMA : Weighted Moving Average)을 2012년 피해액으로 단순 추정하면 995억 원(1,154억 원 × 2/3 + 678억 원 × 1/3)이 산출된다. 공제율을 20%로 가정하면 2012년도의 보험금 예상액은 총 796억 원(995억 원 × 0.8)이 된다. 보험자의 총 보험료는 위험에 충당하기 위한 순보험료와 사업비 등에 충당하기 위한 부가보험료로 구성되는 데, 위의 796억 원이 순보험료를 구성하게 된다. 부가보험료는 보험종목별로 회사별로 자율적으로 결정되는 부분으로 여기서는 고려하지 않기로 한다.

2012년도에는 실제 748억 원의 금전적 피해액이 발생하였으므로 20%의 공제율을 가

정하면 실제 보상액은 598억 원이 되고 이에 따른 손해율은 75.1%(=598억 원/796억 원)가 된다. 만일 이 보험에 가입한 회사가 10개(동일한 위험집단)이고 748억 원의 피해액이 1개 회사에서만 발생했다고 가정하면 이 회사는 보험료 79.6억 원(796억 원/10개사)과 자기부담금 149.6억 원(748억 원×0.2)의 합인 229.2억 원으로 실제 피해액 748억 원에 대응한 효과를 갖는다.

한편, 보험료는 기업이 보안사고 예방에 대해 적극적으로 참여할 수 있도록 위험의 수준을 탄력적으로 반영하여야 한다. 즉 위험의 증가에는 할증을 위험의 감소에는 할인을 해주어야 한다. 2013년의 보험금 예상액(=순보험료)을 위와 동일한 방법으로 계산하면 예상피해액×(1-공제율) = 872억 원(748억 원×3/6+1,154억 원×2/6+678억 원×1/6)×0.8 = 697억 원이 된다. 여기에 전년도(2012년) 손해율 75.1%를 감안하여 보험료를 할인하면 최종(순)보험료 수준은 523억 원이 된다.

2012년 보험료 796억 원, 2013년 보험료 523억 원은 위험 수준을 금전적 가치로 표현한 것으로 이해할 수 있다. 위의 예시에서는 전체 시장을 대상으로 산출하였으나, 이를 개별 회사로 세분하여 산출한다면 보험료를 해당 회사에 대한 위험의 측정치로 이해 가능하다. 위의 사례는 '위험수준 = 예상 위험액 × 신뢰도'라는 식을 정의한 것이며, 예상 위험액 산출에 과거 손해액에 대한 가중이동평균방법을 신뢰도에 전년도 실제 손해율을 적용한 것이다. 이러한 과정은 위험평가자의 가정과 투입변수에 따라 달라질 수 있으며 실무적으로는 더욱 정교해질 필요가 있다.

5.2 정신적 피해에 대한 보험의 구성

금융회사의 개인정보 유출사고는 연간 사고건수가 경험통계로서의 역할을 하기에는 상당히 부족하므로 정신적 피해에 따른 예상 위험액 산출에 단순평균을 사용한다. 금융회사의 개인정보 유출사고의 빈도는 연간 3.4건(17사고건/5년)이며, 심도는 1사고당 195,871건(3,329,807건/17사고건), 연간 665,961건(3,329,807/5년)으로 나타난다. 제 4.2절의 PML을 가정하여 소송참여율을 1%, 건당 판결금액을 20만 원이라 가정하면 2014년도의 예상 피해액은 13.3억 원(= 665,961건×1%×20만 원)으로 추정할 수 있다.

〈Table 3〉 Composition of Insurance Against Financial Loss from Personal Information Infringements

(unit : 100 million won, %)

Year	(1) Real Loss	(2) Expected Loss	(3) Expected Insured Amount	(4) Premium	(5) Real Insured Amount	(6) Loss Ratio(%)
2010	678 (①)	-	-	-	-	-
2011	1,154 (②)	-	-	-	-	-
2012	748 (③)	995 (④)	796	796	598	75.1
2013	-	872 (⑤)	697	523	-	-

Calculation : ④ = ②×2/3+①×1/3, ⑤ = ③×3/6+②×2/6+①×1/6, (3) = (2)×(1-deductible ratio(0.2)), (4) = (3)×loss ratio(6) of last year, (5) = (1)×(1-deductible ratio(0.2)), (6) = (5)/(4).

13.3억 원은 약 6,660명에게 20만 원의 보상이 가능한 수준이다. 2014년 1월 카드 3사 정보유출사고에서 소송참여율 1%가 모두 실현된다면(즉, 약 85만 명이 소송에 참여하고 모두 승소하여 1인당 20만 원의 위자료를 지급 받는다면) 카드 3사의 위자료는 총 1,697억 원이므로 이것이 모두 보험금으로 지급되면 보험자는 거대 위험에 노출 된다.

다만, 배상책임보험에서는 일반적으로 보험가액의 관념이 존재하지 않아 보험사고의 발생으로 인한 손해 예측이 곤란하므로 보험자는 보상한도액(Limits of liability)을 설정할 수 있다. 이를 통해 보험자는 재무능력의 범위 안에서 평균 손해액을 추정하고 경영상의 안정을 꾀하게 된다[14]. 위 사례에서 보험자가 보상한도액을 예상 피해액 수준으로 설정하였다면, 이를 초과하는 위험은 다시 카드 3사에게 이전된다.

정신적 피해를 보상하는 보험을 가정한다면 2014년 카드 3사의 정보유출사고는 2015년 보험료를 크게 인상시킨다. 만약 이 보험이 법에 의한 강제적 가입의 성격을 가진다면 보험료 절감은 회사들의 정보보호 투자에 대한 유인을 제공할 수도 있다.

5.3 개별 기업의 보험료 산정

언더라이팅(Underwriting)이란 보험자가 위험을 인수하거나 거절하는 일련의 과정으로[14] 개별 기업의 보안 상황과 보안 사고의 빈도(frequency) 및 심도(severity)를 측정하여 개별 기업의 보험료를 산정함으로써 보안 리스크를 계량화할 수 있는 중요한 과정이다. 그러나 현재 개별 기업의 보안수준 및 보안사고로 인한 실제 손실금액에 대한 경험 통계나 자료(계리 데이터)는 거의 없는 실정이다. ENISA(European Network and Information Security Agency)는 손실에 대한 계리데이터의 부족과 이로 인한 위험 측정의 불확실성을 사이버 보험(cyber insurance)에 대한 주요 장애요인으로 언급하고 있다[7]. 본 절에서는 개인정보 침해사고와 관련하여 보험료에 영향을 미칠 수 있는 개별 기업의 요인을 이론적 수준에서 고찰하고자 한다.

5.3.1 심도(Severity)의 요인

개인정보 침해사고에 영향을 미칠 수 있는 첫 번째 요인은 그 회사의 업종이라 할 수 있다. 이는 생명보험에 있어서 개인의 직업을 언더라이팅 요소로 보는 것과 유사하다. 업종은 해당 기업의 영업과 위험의 범위를 결정하고, 기업이 준수해야 할 개인정보 관련 법률을 결정한다. 이러한 업종의 구분은 위험의 구분이 통계적 유의성을 가질 수 있는 수준까지 분류되어야 한다. 가령, 제 4.2절의 금융회사의 개인정보 유출사고를 단순히 금융업종으로 분류하면 심도는 1사고당 195,871건(3,329,807건/17사고)이라 할 수 있으나, 이를 좀 더 세분화하면 1사고당 은행업은 46,036건(138,109건/3사고), 금융투자업(증권업)은 9,344건(28,032건/3사고), 보험업은 160,950건(321,900건/2사고), 비은행(카드사, 캐피탈사, 저축은행 등)은 315,752건(2,841,766건/9사고)으로 사고의 심도가 구분됨을 알 수 있다.

두 번째 요인은 회사의 규모와 IT 의존도이다. 금융회사의 금융거래 규모가 클수록 그리고 그 거래가 온라인에 더 많이 노출될수록 사고발생시 더 큰 규모의 피해가 발생하는

〈Table 4〉 Severity of Personal Information Infringements by Financial Company Type

(year : 2009~2013, unit : record)

Classification	Bank	Securities	Insurance	Non-Bank	Total
Leaked Data Records	138,109	28,032	321,900	2,841,766	3,329,807
Incident (Company)	3	3	2	9	17
Severity per Incident	46,036	9,344	160,950	315,752	195,871

것은 자명하다. 일본 손보재팬사의 개인정보 취급사업자보험의 경우 IT 사업자는 연간 매출액 5천만 엔을 기준으로 보장한도를 1억 엔으로 할 때 연간보험료가 508,400엔이고, 제조・건설・소매업은 연간 매출액 5억 엔을 기준으로 보장한도를 5천만 엔으로 할 때 183,000엔 수준의 보험료를 산정하고 있다[1]. 이를 통해 매출액 규모와 IT 사업 유무가 보험료 결정 요인 중 하나임을 확인할 수 있다.

세 번째 요인은 회사가 보유하는 정보의 양과 질이다. 보험산업의 경우는 보험계약의 일회성과 장기성, 보장내용 및 보험료 체계의 복잡성 등으로 인해 인터넷뱅킹, 사이버증권 거래와 같은 인터넷기반 영업이 활성화되지 못하였다. 따라서 인터넷 보험가입을 통해 보유한 개인정보의 양은 많지 않을 수 있으나, 문제는 개인정보의 질이다. 보험회사는 보험가입 및 보험금 지급과 관련하여 개인의 질병 및 진료내역 등을 보유하고 있으며, 이와 같은 정보가 유출될 경우에는 금전적 피해, 개인정보자기결정권의 침해를 포함하여 프라이버시 침해 및 명예훼손 등의 결과로 이어져 그 피해는 은행산업이나 금융투자(증권)산업보다 더욱 크게 나타날 수 있다.

5.3.2 빈도(Frequency)의 요인

침해사고의 발생가능성에 가장 큰 영향을 미치는 요인은 그 회사의 정보보호 수준이라고 할 수 있다. 포네몬사의 보고서(2010)에 의하면 미국 기업의 경우 정보보호최고책임자(CISO)의 역할이 존재할 경우 데이터유출 1건당 평균 비용은 193달러, 존재하지 않을 경우의 평균 비용은 232달러로 39달러의 차이를 보이고 있다[22]. 이는 체계적인 정보보호에 대한 대처, 즉 정보보호의 수준이 보안사고의 결과에 영향을 미친다는 사실을 시사하고 있다.

2008년 이후 우리나라 금융회사 개인정보 유출사고 17건(제 4.2절 참조)을 유출 경위별로 분석하면 내부자에 의한 유출이 9건(52.9%), 해킹에 의한 사고가 7건(41.2%), 기타 프로그램 실수에 의한 사고가 1건으로 나타났다. 이 중 조치 완료되어 금융감독원의 제재공시 내용으로 확인 가능한 12건의 원인을 분석해보면 다음과 같다. 테스트 프로그램의 공개용 서버 노출(I캐피탈, H캐피탈), 특정 문자열에 대한 필터링 취약(I캐피탈, S카드), 인터넷주소 변경을 통한 고객 인증번호 임의 수령(L캐피탈), 프로그램 실수(N증권) 등 프로그램의 보안 취약성에 기인한 사건이 5건이었다. 또한, 관리자 비밀번호의 평문노출(I캐피탈, H캐피탈), 퇴직자의 시스템 계정 유지(H캐피탈) 등 정보시스템 관리자의 계정관리 불철저에 기인한 사건은 3건이었다. 한편, 내부직

원에게 업무목적 외의 과도한 권한을 부여한 경우(S은행, S카드, S캐피탈, H카드, I캐피탈, M화재)가 6건으로 가장 많았으며, 이러한 과도한 권한 부여는 파일 반·출입 통제의 미흡(H카드, I캐피탈, M화재)과 결합되어 고객정보가 이메일, USB, 웹하드 등으로 유출되는 결과가 발생하였다. 또한 I캐피탈은 해킹 사고 발생 후 해킹 프로그램 4개 중 3개만 제거하고 나머지 1개를 제거하지 않음으로써 고객정보가 추가 유출되고, H보험, N증권은 시스템 가동기록을 제대로 보관하지 않는 등 개인정보 유출사고 이후의 사후대처도 미흡한 것으로 나타났다.

위와 같이 금융회사의 개인정보 유출사고는 내부통제의 불철저 및 안전성 확보의무의 미 이행에 영향을 받고 있다. 따라서 회사의 정보보호수준은 사고 발생의 척도가 될 수 있다.

위의 내용을 정리하면 '개별 회사의 보험료 수준 = Severity(업종, 규모, IT 의존도, 정보의 양, 정보의 질) × Frequency(정보보호 체계; 접근제어, 파일 반출입통제, 계정관리, 프로그램 취약성, 기타)'로 표현할 수 있으며, 이러한 개별 회사의 보험료 수준은 곧, 그 회사의 정보보호 수준으로 볼 수 있다.

보험자에게 언더라이팅을 위해 정보보호 수준 분석 능력을 직접 갖출 것을 요구할 수도 있지만 이보다는 전문적인 보안회사의 컨설팅 및 지식을 이용하는 것이 더 현실적이다. 다만, 이 경우에도 시간과 경비가 지나치게 많이 소요될 수 있다. 따라서 직접적인 방법보다는 사회가 공감하고 동의할 수 있는 정보보호지수 내지 정보보호등급의 활용이 효율적일 수 있다. 채승완 외(2007)는 개인정보 보호수준과 침해는 상호 불가분의 관계로 개인정보보호지수(개인정보의 보호수준을 객관적으로 측정하여 개인정보가 침해당하지 않는 정도)에 대한 개발이 개인정보보호 정책의 일환으로 수행되어야 하며, 개인정보보호 수준의 제공은 개인정보 제공에 대한 우려도를 불식시켜 시장에서 개인정보의 가격을 낮추고 거래량을 증진시키는 효과가 있다고 하였다[3].

6. 정책 방향

개인정보 침해사고 보상보험의 활성화를 위해 직접적으로 취할 수 있는 정책은 보험가입을 의무화하는 것이다. 그러나 정보보호의 필요성에 대한 인식이 수반되지 않는 의무보험 도입은 정보보호 수준의 향상은 가져오지 못한 채 자칫 기업의 부담만 초래할 수 있고, 기업은 보험료를 위험관리의 수단이 아닌 불필요한 비용으로만 인식할 우려가 있다. 본 장에서는 보험의 수요를 확대하고 이에 대응하는 공급의 확대를 위한 정책 방향을 검토하고자 한다.

6.1 수요의 확대

6.1.1 제재의 강화 및 소비자에게 유리한 소송환경의 조성

보험에 대한 수요를 유발하기 위해서는 정보보호에 대한 투자 및 고객에 대한 즉각적 보상이 회사에 이익(또는 더 적은 손해)이 될 수 있는 정책을 시행하여야 한다. 이를 위해

서는 개인정보 유출사고 발생시 강력한 제재를 부과함으로써 회사에 법규 준수 및 내부통제 강화의 유인을 제공해야 한다. 또한, 소송이 제기되면 패소의 가능성이 높아져 회사의 손실 발생이 확실하다는 인식이 확산되어야 한다. 이를 위해서는 다음과 같은 현행 법제도의 개선이 필요하다.

현행「개인정보보호법」제39조(손해배상책임) 1항은 "정보주체는 개인정보처리자가 이 법을 위반한 행위로 손해를 입으면 개인정보처리자에게 손해배상을 청구할 수 있다. 이 경우 그 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다."고 규정하고 있다. 이러한 논리는「신용정보의이용및보호에관한법률」제43조(손해배상의 책임)에도 동일하게 적용된다. 이것은 일반적으로 개인이 손해를 입은 경우 개인정보처리자의 고의·과실을 입증하는 것이 현실적으로 어려운 측면이 많다는 점에서 입증책임을 개인정보처리자에게 전환시킴으로써 개인정보처리자의 법규준수를 유도하고 정보주체의 권익보호를 강화하고 있는 것으로 해석된다[2]. 그러나 이는 소송을 제기하는 소비자의 입장에서 보면 여전히 개인에게 불리한 조항이다. 실제적 손해가 발생한 정보주체에 대한 배상여부를 기업(개인정보처리자)의 입장에서 생각하고 있는 것이다. 즉, 정보유출 사고에 대해 개인과 기업이 모두 과실이 없는 경우에 기업이 자기에게 과실이 없음을 입증하면 기업의 배상책임은 면제된다. 이 경우 사고로 인한 사회적 손실을 선의의 개인이 모두 떠안게 된다. 소비자보호를 위해서는 기업이 자기의 고의 또는 과실이 없음을 입증하면 면책되는 것이 아니라 정보주체의 고의나 중과실을 입증하는 경우에만 면책되는 것으로 법을 개선할 필요가 있다.

이러한 입법례의 경향은「전자금융거래법」에서도 확인할 수 있는데, 현행「전자금융거래법」제9조는 "접근매체의 위조나 변조로 발생한 사고, 전자적 장치 또는 정보통신망에 침입하여 거짓이나 부정한 방법으로 획득한 접근매체의 이용으로 발생한 사고"로 인하여 이용자에게 손해가 발생한 경우 금융회사 등이 그 손해를 배상할 책임을 진다고 규정하고 있다. 다만, 이용자의 고의나 중대한 과실이 있는 경우는 예외로 한다. 즉, 이용자에게 경과실이 있거나 이용자에게 과실이 없는 무권한거래 기타의 사고가 발생한 경우 회사는 자신에게 과실이 없더라도 그 사고에서 발생한 손해를 배상할 책임을 진다[23].

한편,「개인정보보호법」제39조(손해배상책임) 1항에 의해 정보주체가 손해배상을 청구하기 위해서는 개인정보처리자가 이 법을 위반하여야 하며(법 위반사실 입증), 정보주체가 손해를 입어야 하며(손해사실 입증), 법을 위반한 행위로 손해를 입어야 한다(법 위반사실과 손해의 인과관계의 입증). 정보주체의 손해사실의 입증과 관련하여 정신적 피해의 경우에는 정보유출 사실만으로 권리를 침해받은 사실을 입증 가능하며, 금전적 피해의 경우에는 계좌 이체 및 카드 부정결제 내역 등으로 입증이 가능하다. 또한 법 위반사실의 입증은 개인으로서는 현실적으로 어려우며, 이는 금융당국의 행정적 검사·제재내용과 수사기관의 수사내용 등에 의존할 수 있다. 가장 어려운 것은 바로 정보유출과 손해의 인과관계를 입증하는 것이다. 즉, 이번에 이용자에게 발생한 피해가 이번 정보유출 사건의

결과에 의한 것인지 과거 다른 정보유출 사건의 결과에 의한 것인지를 구분하는 것은 매우 어려운 일이다.

이러한 인과관계 입증책임의 부담을 개선하기 위해서 손해배상 청구를 위한 요건으로 정보주체에게 손해사실의 입증 책임만을 부과하고 개인정보처리자의 법 위반사실 입증, 법 위반사실과 손해의 인과관계의 입증은 제외할 필요가 있다. 또는 인과관계 입증책임의 부담을 덜어주기 위해 정보주체의 피해 발생에 원인이 되었던 개인정보 항목을 유출한 회사들에게 모두 공동의 책임을 부과하는 제도도 검토해 볼 수 있다. 이렇게 되면 정보주체는 개인정보 오·남용으로 인한 피해가 어느 회사의 정보유출 사고에 기인한 것인지를 증명할 책임이 없게 된다. 다만, 회사의 무한책임에 따른 부담을 완화하기 위해 책임의 범위를 정보유출 사고 발생 후 특정기간 내로 한정할 필요는 있다.

6.1.2 침해사고 및 보상에 대비한 회사 내부의 준비금 적립

정보보호를 위한 지출이 투자가 아닌 단순 비용으로 인식되는 경향이 있다. 이는 위험관리 수단으로 보험을 가입하는 회사의 경우에도 마찬가지이다. 보험을 가입함으로써 정보보호에 대한 주의가 이완될 수 있으며, 보험료는 손익계산서 상 비용처리 됨으로써 원가의 상승을 초래하고, 그러한 가격의 인상은 다시 소비자에게 전가될 수 있다. 따라서 회사가 보안사고를 상시적 위험으로 인식하기 위해서는 보험에 의한 위험전가와 회사 내부의 준비금 적립이 병행될 필요가 있다.

보험료와 다르게 준비금의 부담이 소비자에게 전가되지 않게 하려면 이를 회사의 비용이 아니라 배당재원 등에 사용할 수 있는 이익잉여금(당기순이익 등)의 처분으로 적립해야 한다. 이는 경영진, 주주, 채권자 등 경제적 이해관계자에게 보안사고를 상시적 위험으로 인식시키는데 효과적일 수 있다. 이러한 준비금은 제 5.1절의 공제액(자기부담금)에 충당할 수 있으며 준비금이 많을수록 보험료는 절감되고 보상한도는 확대될 수 있게 된다. 이러한 입법례는 자본의 충실을 기하기 위하여 결손보전 등의 목적에 사용하기 위해 「상법」 제458조에 따라 적립하는 이익준비금 등에서 찾아볼 수 있다. 이익준비금은 매 결산기에 이익배당액의 10분의 1 이상을 자본금의 2분의 1에 달할 때까지 적립한다.

6.2 공급의 확대

6.2.1 국내 IT 환경에 맞는 보험상품의 정비

기존에 국내에도 개인정보 유출관련 보험상품이 존재하였음에도 이것이 활성화되지 않은 원인을 먼저 분석해야 한다. 이것은 기업 내 위험관리자가 개인정보 유출위험에 대한 인식이 부족했기 때문일 수 있으며, 위험관리의 수단으로서 보험을 고려하지 않고 있기 때문이기도 하다. 또한, 이는 기존 상품이 가입자의 기대에 부응하는 보상을 제공하지 않기 때문이다. 즉, 보상 조건에 과도한 보험금 불지급사유 즉, 면책조항(내부자 정보유출, 미폐기 정보의 유출, 위탁업체의 정보유출, 계좌번호 유출 등)을 설정함으로써 실효성 있는 보험의 역할을 기대할 수 없었기 때

문이다. 따라서 보험회사는 보상범위를 확대하고 종합형 상품, 가입대상별 세분화 상품(공공기관용/대기업용/중소기업용), 개인가입형 상품 등으로 상품성을 강화하려는 노력을 해야 한다[13].

6.2.2 보험자의 위험전가 장치 마련

보험자는 위험의 동질성과 다수성을 확보함으로써 위험으로 인한 손실의 규모와 발생확률을 정확히 예측하게 되고(대수의 법칙) 이에 따른 보험료를 산출한다[17]. 보험가입자는 보험료를 보험자에게 납부하고 반대급부로 위험을 전가하게 되는데, 계리데이터가 부족하여 손실의 빈도와 심도를 잘못 예측하게 되면 보험자는 거대 위험에 노출되게 된다. 즉 보안사고에 대한 계리데이터의 부족 및 보험자의 위험 헤지(hedge) 수단의 부재가 보험상품의 공급을 제한하는 요인이 된다.

ENISA(2008)는 보험자의 위험 전가를 위해 국가 재보험(re-insurance)을 제안하기도 하였으나[6], 시장에 대한 국가의 개입이라는 측면에서 다소 부정적인 측면이 있기도 하다.

이 보다는 위험의 분산을 위해 단체보험 형태로 상품을 운용하는 것이 더 현실적이다. 일본의 경우 일본상공회의소 및 지방상공회의소의 회원을 대상으로 개인정보유출보험을 단체보험으로 판매하고 있다[13]. 이를 우리나라의 은행산업에 적용한다면, 은행연합회가 회원사, 즉 은행들을 대상으로 하여 단체보험에 가입하고 이 단체보험을 1개 보험사가 아닌 여러 보험사가 공동으로 인수함으로써 은행이라는 위험집단의 동질화를 확보하면서 위험을 여러 보험사들이 공유하게 되는 효과를 기대할 수 있다.

6.3 보험의 실효성 제고

보험이 정상적인 기능을 수행하려면 정확한 위험 측정에 따른 보험료의 산출이 필요하다. 따라서 계리데이터의 정합성 확보는 보험의 실효성을 제고하기 위한 선결조건이라 할 수 있다.

6.3.1 정보보호등급제 도입 및 활용

제 5.3절에서 정보보호 수준이 침해사고로 인한 손실과 보험료 수준에 영향을 미칠 수 있으며, 이러한 정보보호 수준에 대한 객관적 지표로서 정보보호등급의 활용 가능성을 언급하였다. 이러한 정보보호등급제도는 예측 가치와 피드백 가치(feedback value)를 갖는다. 즉, 소비자, 보험자 등의 정보이용자는 정보보호등급을 통해 해당 기업의 정보보호 수준을 예측하고 자신이 기대하는 수준에 부합하는 기업을 취사선택할 수 있다. 또한, 정보보호등급과 사고발생 및 손실의 관계에 대한 통계는 다시 정보보호등급의 산정 과정에 영향을 미쳐 각 등급별 구분을 정교화하는 도구로 활용될 수 있다. 정보보호등급의 활용을 통해 소비자는 안전한 정보제공을 위한 탐색비용을 절감할 수 있고, 보험자는 회사의 위험수준을 파악하기 위한 언더라이팅 비용을 절감할 수 있으며, 정부는 정보보호등급을 해당 기업의 감독 목적에 직접 활용함으로써 행정비용을 절감할 수 있다. 이러한 정보보호등급제의 도입 및 공시는 결과적으로 기업의 정보보호 수준을 향상시킬 유인을 제공한다. 정보보호등급제 도입의 중간 단계로 인증제 적용을 고려해 볼 수 있으나, 보험에 있어서는 등급제 도입이 더 효율적이다. 즉, 인증제

는 위험집단을 단순히 인증회사와 미인증회사로 구분하므로 위험의 세분화가 미흡하기 때문이다.

6.3.2 계리데이터의 집적 및 활용 제고

정확한 계리데이터의 측정을 위해서는 침해사고가 누락 없이 집계·측정되어야 하고 이를 위해서는 회사가 침해사고의 발생사실을 정확히 당국에 알리고 공표해야 한다. 그러나 영리를 목적으로 하는 기업의 특성상 침해사고의 발생사실을 은폐할 유인이 존재한다. 미국 CSI(Computer Security Institute)의 조사결과(2010)에 의하면 138개 조사대상 업체 중 25.4%가 침해사실을 외부에 전혀 알리지 않은 것으로 나타났다[4]. 따라서 신고의 누락 및 부실을 막기 위해서는 미신고로 인한 불이익이 신고 이후의 불이익 수준과 동일해지거나 그 이상이 되도록 제재를 강화할 필요가 있다.

또한, 정부 당국은 침해사고가 발생할 경우 피해 확산 방지 등의 조치와 더불어 사후적으로 정확한 사고의 원인과 과정, 물리적·재무적 피해상황 등을 집계·정리하여 보험요율기관, 연구기관, 정보보호전문기관 등에 투명하게 공개함으로써 정보독점에서 벗어나 데이터의 불확실성을 줄여줘야 한다.

7. 결 론

개인정보는 금융거래의 성립조건이며 금융회사의 핵심 자산이다. 본 논문에서는 이러한 개인정보 침해사고로 발생하는 위험을 관리하기 위한 실효성 있는 수단으로 보험을 제시하였다. 개인정보 침해사고 보상보험은 고객에 대한 손해배상에 있어서 법적 절차에 따른 시간과 비용을 절감하고, 법적 요건보다 완화된 조건으로 보상을 제공함으로써 소비자 보호에 기여할 수 있으며, 동시에 정보유출 사고로 인한 미래의 불확실한 거대 손해를 보험료라는 확실한 현재의 평균비용으로 대체함으로써 기업의 재무건전성을 확보하여 준다. 또한, 보험계약의 체결, 보험료 산정, 보험금 지급 등의 일련의 과정에서 기업의 정보보호 수준과 보안사고 발생가능성을 측정·평가함으로써 보안산업 시장의 확대 및 기업의 보안 수준 향상 유도, IT 리스크 측정 기반 마련에 기여할 수 있다.

그러나, 보험은 실제 손실을 최소화하기 위한 위험관리의 한 수단일 뿐이다. 위험을 타인에게 전가하지만 위험을 예방, 통제하지는 못한다. 이는 보험이 정보보호의 영역 중 복구(recovery) 부문에 해당하기 때문이다. 따라서 보험에 대한 지출은 사고 예방을 위한 투자의 개념이 아닌 사고처리를 위한 비용의 개념으로 인식되기 쉬우며, 보험계약이 체결되었기 때문에 보안사고에 대한 주의력이 이완될 수 있는 방관적 위험(morale hazard)을 초래할 수 있다. 그리고 계리적 정합성이 확보되지 않은 보험의 설계는 보험계약자나 보험자의 위험을 완전히 헤지하지 못하고 여전히 한 쪽에 거대한 위험으로 존재할 수 있다. 본 논문에서는 이에 대한 정책적 제언으로 침해사고 및 보상에 대비한 회사 내부의 준비금 적립, 보험 구성시 공제조항의 적용, 단체보험 활용을 통한 보험자의 위험전가 장치 마련, 정확한 위험 측정을 위한 정보보호등급제

도입 및 계리데이터의 집적·활용 등을 제안하였다.

예상 손실액(위험액)은 사고에 영향을 미치는 요인과 그 요인에 대한 민감도의 결합으로 산출할 수 있다. 본 논문에서는 보험을 구성할 때 시장 전체의 예상 손실액을 산정함에 있어 과거 개인정보 침해사건들의 결과만을 이용하였다. 이는 과거의 손실경험을 바탕으로 다음 기간의 보험료를 조정함으로써, 기업에게 보험료를 낮추기 위한 개인정보 보호노력을 장려하는 효과를 갖고 있지만 위험의 요인으로서 현재 기업의 보안수준, 외부의 보안위협 상황 등의 요인을 반영하지 못하는 한계가 있다. 향후 연구에서는 과거의 경험통계와 미래의 사고 발생가능성을 정확히 반영할 수 있는 이론적 모형의 개발이 필요하다. 또한, 개별 회사의 보험료(정보보호 수준)를 Severity(업종, 규모, IT 의존도, 정보의 양, 정보의 질) × Frequency(정보보호 체계; 접근제어, 파일 반출입통제, 계정관리, 프로그램 취약성, 기타)로 표현하였으나, 이는 과거 사건을 바탕으로 분석하여 관계를 표현한 것이며 실제 보험료를 산출하기 위한 정량적 식은 아니다. 향후 연구에서는 시장 전체의 위험을 개별 회사에 안분하는 기법, 또는 개별 기업의 보안요소에 가중치를 부여하여 이를 금액으로 환산하는 모형 등이 필요하다.

한편, 본 논문에서는 개인의 관점에서 손실을 고려하였으나, 개인정보 침해사고의 위자료에 대한 과거 경험이 충분히 확보되지 않은 현재의 상황에서는 고객이탈로 인한 영업 손실 등 기업 관점에서의 손실에 대한 연구가 기업의 위험관리 기준으로 유용할 수 있다. 향후에는 개인 관점에서의 가치, 기업 관점에서의 가치를 결합하여 개인정보의 경제적 가치를 산출하고 다시 권리적 가치와 결합하여 종합적인 개인정보보호의 방향으로 연구가 지속되어야 할 것이다.

보험은 소비자보호와 회사의 건전성 확보를 동시에 달성할 수 있는 유용한 수단이며, IT리스크의 계량적 측정을 위한 기반이 될 수 있다. 보안과 보험은 모두 사회적 안전망을 확보하기 위한 체계이다. 두 영역이 결합하여 시너지 효과를 발생시킨다면 개인정보의 보호 및 신용사회의 정착에 크게 기여할 수 있을 것이다.

References

[1] Bae, B. H. and Min, K. S., “Policy recommendations on the activation plan of domestic information security insurance market,” Internet and Security Focus 2013 July, pp. 6-26, 2013.

[2] Cha, G. S., “A Study on the Criteria to Estimate the Compensation from the Infringement of Personal Information,” Soongsil University, p. 22, p. 56, 2011.

[3] Chai, S. W., Min, K. S., Hwang, S. W., and Won, S. J., “A study on the analysis of the economic value of private information,” Information Security Issue Report 2007-03, pp. 1-20, KISA, 2007.

[4] CSI(Computer Security Institute), “15TH ANNUAL 2010/2011 COMPUTER CRIME AND SECURITY SURVEY,” p. 23, 2011.

[5] Dieter Gollmann, COMPUTER SECURITY Third Edition, pp. 32-33, WILEY, 2011.

[6] ENISA(European Network and Information Security Agency), Security Economics and The Internal Market, http:// www.enisa.europa.eu/, p. 85, 2008.

[7] ENISA, Incentives and barriers of the cyber insurance market in Europe, http:// www.enisa.europa.eu/, pp. 19-20, p. 27, 2012.

[8] FSC(Financial Services Commission), FSS, "Press release : Damage prevention comprehensive plan for new and variant telecommunications fraud," 2013.

[9] FSS(Financial Supervisory Service), DART (Data Analysis, Retrieval and Transfer System), http://dart.fss.or.kr.

[10] FSS, "Press release : Analysis of the damage caused by phishing and notes on financial transactions," 2013.

[11] Han, C. H., Chai, S. W., Yoo, B. J., Ahn, D. H., and Park, C. H., "A Quantitative Assessment Model of Private Information Breach," The Journal of Society for e-Business Studies, Vol. 16, No. 4, pp. 17-31, 2011.

[12] KIDI(Korea Insurance Development Institute), Insurance statistics information services, http://www.insis.or.kr.

[13] KIDI, "Activation plan of the liability insurance for personal information security breaches," CEO REPORT KIDI 2012-04, pp. 1-18, KIDI, 2012.

[14] Kim, H. S., Theory of damage assessment, p. 83, 113, 119, pp. 145-149, p. 169, p. 306, LLOYDS, 2008.

[15] Kim, K. S.(member of the National Assembly), Breaches of customer information of financial companies since 2008, http:// www.dreamk.kr, 2014.

[16] Kim, Y. R., Lee, H. C., and Yoo, J. H., "A study on the methodology to estimate the personal information value using the Contingent Valuation Methods(CVM)," Information Security Issue Report 2007-02, pp. 1-22, KISA, 2007.

[17] Kim. D. H. PRINCIPLES OF INSURANCE, p. 16, p. 40, HAKHYUNSA, 2002.

[18] Kwon, H., Lee, E. J., Kim, T. S., and Jun, H. J., "Estimating Compensation for Personal Information Infringement in Korea Using Contingent Valuation Methods," Journal of The Korea Institute of Information Security and Cryptology, Vol. 22, No. 7, pp. 367-377, 2012.

[19] Lee, H. C. and Ahn, K. A., "The evaluation of Personal Information Leakage Loss using the Contingent Valuation Methods," Productivity Review, Vol. 22, No. 2, pp. 1-24, 2008.

[20] Lee, J. B., Theory of damage assessment, p. 156, p. 398, DOOYANGSA, 2008.

[21] Lee, J. K.(member of the National Assembly), Status of the illegal use of credit card, http://www.ljk.co.kr/, 2013.

[22] Ponemon Institute, LLC, 2010 Annual Study : U.S. Cost of a data Breach, p. 32, 2011.

[23] Son, J. H., Electronic Financial Transaction Act, p. 62, BOBMUNSA, 2008.
[24] Yoo, J. H., Jie, S. H., and Lim, J. I., “Estimating Direct Costs of Enterprises by Personal Information Security Breaches,” Journal of The Korea Institute of Information Security and Cryptology, Vol. 19, No. 4, pp. 63-75, 2009.

저 자 소 개

김종환	(E-mail : kiwimyth@empal.com)
2002년	서울대학교 컴퓨터공학부 (학사)
2013년~현재	고려대학교 정보보호대학원 정보보호학과 (석사과정)
2002년~현재	금융감독원 선임조사역
관심분야	정보보호정책, 금융보안

임종인	(E-mail : jilim@korea.ac.kr)
1980년	고려대학교 수학과 (학사)
1982년	고려대학교 수학과 (이학석사)
1986년	고려대학교 수학과 (이학박사)
1986년~2001년	고려대학교 자연과학대학 정교수
2001년~현재	고려대학교 정보보호대학원 원장
	대검찰청 디지털수사자문위원회 위원장
	금융보안연구원 보안전문기술위원회 위원장
	안전행정부 정책자문위원회 위원
	방송통신위원회 인터넷협의회 운영위원 등
관심분야	정보법학, 디지털포렌식, 개인정보보호, 전자정부보안, 융합기술보안 등