【 주간이슈 】

개인정보 유출리스크 증대에 따른 안전망 구축 필요성

산업연구실

□ 개인정보 유출사고가 매년 증가되고 있어 이로 인한 경제적 피해를 보상할 수 있는 안전망 구축에 대한 논의가 필요

o 개인정보 침해건수는 공공부문이 2009년에 423건(전년대비 95.8%p 증가), 민간부문은 약 4만건(53.3%p 증가)이며 이중 약 30~40%가 개인정보 유출사고임.

o 금액기준으로는 연평균 약 3조원의 추정 손해액이 발생하고 있어 개인정보 유출사고의 사회적 리스크 관리는 매우 중요한 과제임을 시사

□ 미국, EU, 일본 등 주요 선진국의 경우 개인정보보호에 따른 관리체계가 상당부분 법제화되어 있음.

o 특히 개인정보유출보험을 통한 리스크 관리가 체계적으로 이루어지고 있는 것으로 평가됨.

□ 우리나라의 개인정보 유출리스크와 관련하여 시장참여자들(국민, 공공기관 및 기업체 개인정보 담당자)의 리스크인식도 매우 높은 수준으로 조사됨.

o 개인정보 유출리스크 측면에서 '막연한 리스크', '경제적 손실리스크', '유출사고 가능성'에 대한 리스크인식 정도가 56.0~73.3% 수준

□ 개인정보 유출리스크 경감을 위한 제도적 대응방안이 강구될 필요가 있음.

o 첫째, 개인정보 관리기관의 개인정보 관리시스템 구축 강화와 더불어 피해자 보호를 위한 경제적 안전망 구축에 대한 논의가 요구됨.

o 둘째, 피해자의 경제적 손실보상 장치 중에서 효율적 범주에 들어가는 보험제도(일명 "개인정보유출사고배상책임보험")의 활성화 조치를 마련

o 셋째, 개인정보유출사고배상책임보험의 활성화를 위한 다양한 상품개발 및 적정 보험료 결정을 위한 보험회사의 합리적 노력 필요

o 넷째, 개인이 개인정보를 제공하는 기관을 확인할 수 있는 장치(안전인증제도 등)마련과 개인의 세심한 확인 노력이 요구됨.

1. 검토배경

□ 개인정보는 국가행정조직 및 공공기관과 민간 영역에서 중요한 핵심인프라로 작용하며 유출사고 발생시 정보제공자에게 정신적 고통과 경제적 손해를 초래할 가능성이 매우 큼.

o 이에 따라 일본, 미국 및 EU 등의 선진 국가에서 개인정보 유출로 인한 경제 주체의 피해를 최소화하기 위한 다양한 제도와 법규들이 마련되고 있음.

□ 개인정보 유출리스크는 사업자나 정보집중기관 등이 집적하고 있는 개인정보가 본인의 사전 동의 없이 유출되고 이로 인하여 발생한 손해를 입을 가능성이라고 정의할 수 있음.

o 개인정보 유출리스크는 재산손해, 우발적 손해, 간접손해를 포함하는 당사자리스크(first party risk)와 법률배상책임인 제3자 리스크(third party risk)로 구분
o 제3자 리스크는 일반적인 불법행위와 비교하여 사고주체, 1사고당 피해자수, 사고의 파급효과 측면에서 다른 특성이 있음.

<표 1> 제3자 리스크의 특징 비교

구분	개인정보유출	자동차사고	제조물책임	일반불법행위
적용법리	개인정보법 등: 조건부과실책임	자배법: 무과실책임	제조물법: 엄격책임	민법: 과실책임
사고주체	내외부 요인 병존	내부요인 (운전자)	내부요인 (제조자)	내부요인 (행위자)
1사고당 피해자	다수	소수	다수	극소수
손해액 규모	중·대규모	중·소규모	중·대규모	소규모
다른 사고로의 연계성	신원도용 등을 통한 금융범죄, 사회질서 문란	없음	화재, 폭발, 파손 등으로 연결	연계가능하나 희박

□ 본고에서는 국내 및 주요국의 개인정보 유출 현황과 이에 따른 리스크 관리 실태를 살펴보고, 향후 과제를 제안하고자 함.

2. 국내 개인정보 유출사고 실태 및 대응 현황

가. 개인정보 유출사고 실태

□ 개인정보 유출사고의 발생원인은 부적절한 접근과 수집, 부적절한 이전, 원하지 않은 영업행위, 부적절한 저장 등임.

o 「정보통신망법」에 의한 개인정보 유출사고 유형은 “고지·명시한 범위를 초과한 목적외 이용 또는 제3자 제공(§24, §24의2)”, “개인정보취급자에 의한 훼손·침해 또는 누설(§28의2)”, “타인정보의 훼손·침해·도용(§49)” 등임.

□ 2008년 발생한 GS칼텍스의 개인정보 유출사고는 그 규모(유출정보건수)가 약 1,100만 건으로 세계적으로도 대형사건으로 기록됨[1].

o 침해건수를 기준으로 할 때 공공부문의 경우 2009년 423건(전년대비 95.8% 증가)으로 최근 급증하고 있으며 이중 약 40%가 개인정보 유출사고임.
o 민간부문의 경우는 2008년 약 4만건(전년대비 53.3% 증가)이 침해사고이며, 이중 개인정보 유출사고 유형은 약 30%임.

<표 2> 정보통신망법상 개인정보 유출사고 현황

(단위: 건)

	2000	2005	2008
목적 외 이용 또는 제3자 제공관련	108	916	1,037
개인정보 취급자에 의한 훼손·침해 등	28	186	125
주민등록번호 등 타인 정보의 훼손·침해·도용	956	9,810	10,148
소계	1,092	10,912	11,310
침해사고 전체	2,035	18,206	39,811
유출건수 비율(%)	53.7	59.9	28.4

자료: 한국인터넷진흥원; 송훈석 의원 정책자료집(2009) 재인용

□ 유진호 외 3인(2009)[2]의 연구에 의하면 개인정보 유출사고로 인한 피해규모는 추정 손해배상금이 2007년 기준 약 3조원, 2005~07년의 누적 피해자수는 7천 만명, 누적 손해배상금 추정액도 약 11조원에 달하는 것으로 분석

1) 오픈 시큐리티 파운데이션(Open Security Foundation(http://www.datalossdb.org)에 따르면 GS칼텍스 사건은 약 1,100만 건으로 전세계 개인정보 유출규모에서 12위를 차지한 것으로 나타남(2010.5월 기준).
2) 자료: 유진호·지상호·임종인, 「개인정보 유·노출 사고로 인한 기업의 손실비용 추정」, 『정보보호학회논문지』, 제19권 4호, 2009, p.72.

o 2007년의 손해배상금 추정액 3조원은 현재 의무보험인 자동차보험의 대인배상 보험금 2.3조원(FY2008)보다도 큰 금액으로 개인정보 유출사고의 사회적 리스크가 매우 중요한 과제가 될 것임을 시사

나. 개인정보 유출사고 관련 법규

□ **우리나라의 개인정보보호와 관련된 법적 규제는 분야별로 독립적인 법률이 존재하는 분산형 체계**

o 공공분야의 경우 「공공기관의 개인정보보호에 관한 법률」, 민간부문은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 주요 법률임.
o 이 외 관련법률로서 「전자금융거래법」, 「통신비밀보호법」, 「신용정보의 이용 및 보호에 관한 법률」,「전자상거래 등에서의 소비자 보호에 관한 법률」 등 개별 관련분야에서 독립적으로 적용되고 있음.

□ **2010년 6월 현재 국회에 계류중인 「개인정보보호법안」은 개인정보보호를 포괄적으로 적용하는 법률안으로 「공공기관의 개인정보보호에 관한 법률」을 폐지하고 이를 대체하는 것임.**

o 「개인정보보호법안」에서는 기존의 타 법률에서 규정하고 있지 않은 개인정보 유출사고 방지대책과 유출사고시 피해자 구제대책도 체계적으로 포함하고 있음.

다. 피해자 구제제도

□ **개인정보 유출사고 피해자의 구제를 위하여 공공기관에서는 행정안전부가 개인정보침해신고센터를 운영하고 있으며 또한 한국소비자원의 분쟁처리절차를 이용할 수도 있음.**

□ **보험을 통한 피해자 구제는 「전자금융거래법」과 「정보통신망법」에서 보험가입을 의무화하고 있으나, 공공기관과 대부분의 민간업체는 보험 가입이 의무화되어 있지 않은 실정임.**

o 금융기관 또는 전자금융업자, 집적정보통신시설업자[3]의 경우 보험가입을 하고

3) 집적통신시설업자란 타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자를 말함.

는 있으나 현실적으로 담보금액이 낮음[4].

o 기타 대부분의 개인정보취급 공공기관 및 기업체는 임의보험으로 개인정보유출 배상책임보험, 이비즈배상책임보험을 가입할 수 있으나 가입률은 극히 저조한 실정임.

<표 3> 국내 개인정보유출 관련 주요 보험상품

구분	상품명	주요 보상 내용	가입대상
의무보험	전자금융거래배상책임보험	해킹 또는 전산장애 등으로 금융거래 피해를 본 고객이 입은 손해를 보상	금융기관 및 전자금융업자
	공인전자문서 보관소 배상책임보험	전자문서보관 등의 업무수행과 관련하여 위법한 행위로 이용자에게 손해를 입힌 경우 손해를 보상	공인전자문서보관소
	집적정보통신 시설사업자 배상책임보험	집적정보통신시설의 멸실, 훼손, 그 외 운영장애로 발생한 피해를 보상	집적정보통신시설 사업자
임의보험	개인정보유출 배상책임보험	보험에 가입한 기업이 개인정보 유출을 당한 가입 고객으로부터 손해배상청구 소송을 당했을 때 발생하는 손해를 보상	온라인 쇼핑몰 등 고객정보를 다루는 업종
	이비즈 배상책임보험	피보험자의 인터넷 및 네트워크 활동에 기인하여 타인에게 손해를 가함으로써 피보험자가 제3자에게 부담하여야 할 법률상의 손해를 보상	온라인 쇼핑몰 및 인터넷 개발업자 등

3. 주요국의 개인정보 관리체계

가. 일본

□ **일본은 개인정보보호와 관련하여 민관을 통합하는 「개인정보보호에 관한 법률」이 2003년 5월에 제정되어 동 년 4월에 전면적으로 시행되었음.**

o 동 법의 구체적인 시행방안으로 “개인정보보호에 관한 기본방침”을 정하고 22개 분야에 대한 35개의 개인정보보호 가이드라인을 제정(2006년 현재)
- 민간영역에서 프라이버시마크제도, JIS Q 15001(개인정보보호관리시스템-요구사항) 등이 자율적으로 운용

o 동 법에서는 피해자 구제를 위한 손해배상책임 등의 명시적 조항은 없으나 기본방침에서 개인정보보호 조치에 관한 기본사항을 규정

4) 은행권역의 보험가입금액은 10억원에서 20억원으로 차등화되어있고, 증권회사 등은 5억원, 보험 등 기타 금융기관은 1억원이다. 금융기관전자금융업의 경우 전자자금이체업무와 직불전자지급수단의 발행 및 관리업무를 수행하는 기관은 2억원, 기타 전자금융업자는 1억원임.

□ 개인정보유출보험은 일본상공회의소의 회원을 대상으로 미쯔이스미토모(三井住友海上)를 사무간사사로 하여 13개 손해보험회사가 공동인수하는 형태임.

o 2005년 미쓰비시종합연구소(三菱總合研究所)의 조사에 따르면 개인정보보호법 시행에 따른 보험가입에 대한 의향이 매우 높으며 사후적인 개인정보유출 리스크관리 측면에서 매우 중요하게 인식하고 있어 향후 보험가입이 활발할 것으로 예상

나. 미국

□ 미국은 포괄적인 개인정보보호법제가 제정되어 있지 않으며 다양한 개별법과 자율규제를 중심으로 법적대응이 이루어짐.

o 공공부문은 「프라이버시법(Privacy Act, 1974)」이 대표적이며, 민간부문은 「공정신용조사법(1970)」, 「의료보험의 상호운용성 및 설명책임에 관한 법률(1996)」, 「아동온라인프라이버시보호법1999)」, 「금융서비스현대화법(1999)」등이 제정
o 또한 각 주별로 독자적인 제도가 있으며, 민간기업에서는 자율규제와 가이드라인 운영
  -「개인정보유출고지법(2003)」은 캘리포니아주가 2003년 최초로 도입한 이후 2010년 현재 46개주가 채택하였으며 연방법화를 추진

□ 미국의 보험시장은 유출사고시 본인에 직접 고지하여야 하는 「개인정보유출고지법」에 있는 의무조항 때문에 성장하게 되는 계기 마련

o 법 시행이후 유출사고 통계가 급격히 증가하였으며, Garg et al.(2003)의 연구에 의하면 실제 사고발생 기업의 주가는 크게 하락하는 실증적 결과를 얻음.
o 미국의 관련 보험시장은 2010년 연간 6억달러로 추산되었으며 이에 많은 보험사가 100% 이상의 고 성장세 기록

다. 유럽

□ EU가맹국은 1995년에 공공부문과 민간부문을 포괄적으로 규제하는 「EU 정보보호 지침」을 제정함으로써 국내법을 정비함.

o 영국은 「개인정보보호법(1998)」, 독일은 「연방정보호호법(2001)」, 프랑스는 「정보처리, 정보파일 및 개인의 자유에 관한 1978년 1월 6일의 법률 78-17호, 1978(2004년 법률 제2004-801호에 의해 개정)」등이 있음.

□ **유럽각국의 개인정보보호 관련 보험은 국내법의 재정비와 정보보안전문기관의 설립 등을 계기로 판매가 활성화되기 시작**

o 최근 유럽은 개인정보 유출사고에 대한 체계적인 대책마련을 위한 유럽네트워크 정보보안 전문기관인 ENISA(Europe Network and Information Security Agency)를 출범하여 범국가적인 노력을 기울임.
o ENISA는 미국의 「개인정보유출고지법」의 효과성에 주목하며 유럽에서 개인정보유출보험시장의 범위를 확대하기 위한 정부의 역할을 언급
- 정부의 역할로는 개인정보유출보험의 의무화, 개인정보유출리스크에 대한 국가재보험 필요성, 금융시장에서 사이버리스크 전가수단 확충, 부보가능한 인프라구조의 설계로 보험가입 유도 등임.

4. 개인정보 유출리스크 경감을 위한 안전망 확보 필요성

□ **현행 개인정보 유출사고 피해자 보상체계를 보면, 중소기업은 피해자 보호측면에서, 공공기관은 개인정보 담당자가 개인적 파산에 노출될 개연성 측면에서 취약한 점이 있다고 판단됨.**

o 대기업의 경우 개인정보유출 사고 피해자를 보호할 수 있는 배상자력을 사내유보를 통해 확보할 수는 있으나, 이러한 방법은 비효율적이라고 판단됨.
o 중소기업의 경우 대기업이나 국가 및 지방자치단체와 달리 개인정보 유출로 인한 피해자의 경제적 손실을 보상할 수 있는 배상자력이 취약함.
o 공공기관(국가 및 지방자차단체)의 경우 국가배상법(제2조)에서 따라 공공기관이 피해자에게 직접 배상할 수 있으나 사전에 준비하기 보다는 사고가 발생할 경우 특별예산을 편성하기 때문에 일시에 큰 재원을 마련해야 하는 부담과 자원배분의 비효율이 나타날 수 있음.

□ **개인정보와 관련하여 당사자들은 개인정보가 유출될 리스크, 개인정보 유출로 인한 경제적 손실 리스크에 대한 우려가 큰 것으로 조사됨.**

o 시장의 개인정보와 관련한 당사자의 리스크인식을 알아보기 위하여 국민, 공공기관 및 기업체의 개인정보 담당자에게 '막연한 리스크', '경제적 손실', '유출사고'에 대한 리스크인식을 설문으로 조사하였음.

o 그 결과 개인정보 유출사고와 관련하여 '막연한 리스크'의 경우 모든 시장참여자가 가능성을 높게 평가(약 70%수준)하였으며, '경제적 손실리스크' 및 '유출사고 가능성'도 국민 및 공공기관 담당자는 높게(65%이상), 기업체 담당자는 상대적으로 낮게(약 56%~ 58%) 인식함.

<표 4> 개인정보 유출리스크에 대한 불안정도

(단위: 점)

구분	막연한 리스크		경제적 손실		유출사고	
	점수	비율	점수	비율	점수	비율
국민	4.87	69.5%	5.13	73.3%	5.09	72.7%
공공기관	4.64	66.2%	4.67	66.7%	4.91	70.1%
기업체	4.81	68.7%	3.92	56.0%	4.08	58.3%

주: 1) 점수는 7점이 기준임. 2) 비율은 전체 리스크(=7) 중에서 해당 리스크(=점수)의 비율(=리스크 점수 ÷ 전체 리스크(7점))을 의미함.

□ **시장참여자들이 개인정보가 유출될 경우 리스크, 특히 경제적 손실리스크를 걱정하는 이유는 피해자(국민)의 경제적 손실을 보상해주는 장치가 미흡하다고 믿기 때문으로 판단됨.**

o 개인정보 유출사고로 인한 경제적 리스크인식의 원인으로 국민은 '경제적 피해보상체계 미흡', 공공기관 담당자는 '공공기관의 책임회피', '피해자 보상체계 미비', 기업체는 '피해자 보상체계 미비' 및 '회사의 책임회피' 때문으로 인식

- 국민은 개인정보를 제공하고 개인정보가 유출되었을 때 피해를 입는 당사자이므로 경제적 보상체계의 미흡만을 주요 원인으로 생각하는 것으로 판단됨.
- 그러나 공공기관 및 기업체의 개인정보 담당자의 경우에는 개인정보가 유출되었을 경우에 그 책임을 개인정보관리 담당자가 질 수 있다는 우려가 반영되어 '피해자 보상체계 미비'를 리스크인식의 원인으로 생각하는 것으로 판단됨.

<표 5> 각 주체별 리스크인식 원인

국 민	공공기관	기업체
경제적 보상체계 미흡	공공기관의 책임회피	회사의 책임회피
	피해자 보상체계 미비	피해자 보상체계 미흡

5. 개인정보 유출리스크 안전망으로서 보험제도 필요

□ **개인정보 유출사고에 대비한 개인정보 관리기관의 배상자력 확보방법 중에서 보험(일명 “개인정보유출사고배상책임보험”)이 효율적인 방법의 범주에 속함.**

o 개인정보유출사고에 대비한 배상자력 확보 방법으로는 크게 1) 기업체 내부 유보금액(공공기관의 경우 예산)을 보유하는 방법과 2) 보험을 이용하는 방법이 있음.

o 보험은 다수의 가입자(사고발생자 및 미발생자 포함)가 사고발생자를 보조해주는 제도이므로, 적은 보험료로 큰 사고를 담보하는 데 유용한 금융제도임.

o 따라서 다량의 개인정보를 관리하는 기관 또는 기업체의 경우 매년 적은 보험료를 납입하고 개인정보유출 사고가 발생하는 시점에는 납입한 보험료 이상의 큰 금액(보험금)을 지급받을 수 있는 레버리지 효과를 얻을 수 있음.

□ **보험제도는 보험회사가 피보험자인 개인정보취급기관(또는 기업체)에게 효율적으로 개인정보보호를 하도록 감시하는 기능이 있으므로, 시장 전체의 안정성 제고를 통해 개인정보의 관리수준 향상에 기여할 수 있음.**

o Shavell(1982)[5]에 따르면, 보험시장이 없는 경우 배상책임법률만으로는 사회전체 차원에서 최적 예방수준을 달성할 수 없다고 주장함.

- 보험시장이 존재하는 경우 보험회사는 개인정보관리기관에서 개인정보를 효율적으로 관리하는지를 주시하고, 개인정보 유출방지 노력과 연계한 보험상품을 공급함으로써 개인정보보호를 강화하는 사회적 시스템 구축에 기여

□ **설문조사 결과 보험제도는 개인정보 유출사고시 피해자의 경제적 손실을 보장해주는 제도 중 시장참여자(국민, 공공기관 및 기업체 담당자)들이 가장 선호하는 제도임.**

o 설문대상이 국민(개인)인 경우 개인정보 유출사고시 경제적 리스크 경감 방법으로 ‘보험처리’를 가장 선호함.

o 공공기관의 경우 ‘보험처리“를 가장 선호하며, 기업체의 경우 ’회사부담‘ 다음으로 ’보험처리‘를 선호하는 것으로 나타남.

5) Shavell,Steven."On Liability and Insurance", 13, *Bell J.of Econ.* 120, 1982

<표 6> 개인정보유출로 인한 경제적 리스크 경감방법 선호

(단위: %)

설문대상	회사처리	보험처리	법원소송	개인처리
국민	36.5	42.7	16.9	3.9

주: 점수는 7점 기준이며 비율은 1순위 기준의 비율임.

<표 7> 개인정보유출로 인한 경제적 리스크 경감방법 선호

(단위: %)

설문대상	기관(회사)부담	개인정보담당자	보험처리	기타
공공기관	34.2	2.6	61.7	1.5
기업체	53.4	1.7	43.1	1.7

주: 비율은 1순위 기준의 비율임.

6. 시사점

□ 시장참여자(국민, 공공기관 및 기업체 담당자) 모두가 개인정보 유출사고 리스크에 불안해하고 있다는 점을 고려할 때 시장 전체의 개인정보 유출리스크가 높아질 개연성이 있으므로 이에 대비한 안전망 구축이 필요함.

- o 시장 전체적으로 축적되는 개인정보량이 증가되고 있고, 해킹 등 개인정보 유출 범죄 가능성이 줄어들지 않는 점을 볼 때, 시장참여자들의 개인정보 유출리스크에 대한 걱정은 줄어들지 않을 가능성이 크고, 개인정보 유출사고가 발생한다면 시장참여자들의 커다란 피해가 예상됨.
- o 따라서 개인정보를 관리하는 기관(또는 회사)들이 효과적인 개인정보유출 방지 시스템을 구축하도록 유도하는 정책이 지속적으로 이루어져야 하며, 실제 개인정보 유출사고의 발생에 대비하여 피해자 보호를 위한 안전망 구축이 동시에 이루어질 필요가 있음.

□ 개인정보유출 사고시 피해자의 경제적 손실을 보상해줄 수 있는 장치 중 효율적 범주에 속하는 보험제도(개인정보유출사고배상책임보험)를 활성화할 수 있도록 구체적 대응조치가 필요한 시점임.

o 보험제도를 이용할 경우 개인정보를 관리하는 기관이 효율적으로 개인정보 유출사고 관리 시스템을 구축하도록 유도할 수 있고, 적은 보험료로 높은 배상자력을 확보할 수 있는 장점이 있음.

o 따라서 개인정보유출사고배상책임보험이 활성화될 수 있도록 법적·제도적 장치 마련이 필요함.

□ **보험회사는 공공기관 및 기업체가 보험을 통해 개인정보 유출사고로 인한 경제적 손실을 효과적으로 대비할 수 있도록 시장의 요구에 부합한 상품 개발 및 적정요율의 제시가 필요함.**

o 현행 보험제도 외에도, 법원의 배상판결에 추가하여 보상범위를 확대하는 상품 개발, 개인정보관리 회사에서 요구하는 다양한 상품을 개발하는 등 시장의 요구에 부합한 상품을 개발하여 제공할 필요가 있음.

o 이와 더불어 개인정보유출사고배상책임보험이 활성화되기 위해서는 시장에서 수용 가능한 보험료 수준이 되어야 하므로, 합리적 보험료 산출을 통해 시장에 부합한 보험료를 제공할 필요가 있음.

□ **일반국민(개인)의 입장에서는 개인정보 유출사고가 발생하지 않도록 자신의 개인정보를 잘 관리하는 것이 필요함.**

o 인터넷을 통해 특정 사이트의 회원에 가입할 때 정부기관에서 인정하는 개인정보 관리시스템을 구축하고 있는지 여부, 개인정보 유출사고가 발생하는 경우 피해를 보상해주는 시스템을 갖추고 있는지 여부 등을 종합적으로 판단하여 안전한 사이트라는 것을 철저히 확인해야 할 것임.KiRi