정보유출배상책임보험의 가입 의무화에 관한 연구

박영준(단국대 법대 교수)

Ⅰ. 서론

2011년 7월 SK커뮤니케이션즈가 운영하는 서버가 중국에 거주하는 해커에게 해킹당하여 네이트 또는 싸이월드의 회원 중 3495만여명의 개인정보가 유출되었다. 유출된 개인정보에는 아이디, 비밀번호, 주민등록번호, 성명, 생년월일, 이메일 주소, 전화번호, 주소가 포함되어 있고, 가입 당시 혈액형, 닉네임 등을 입력한 일부 회원들의 경우 혈액형, 닉네임 등도 포함되어 있었다. 이에 대하여 개인정보가 유출된 회원들 중 일부는 SK커뮤니케이션즈 등을 상대로 손해배상을 청구하는 소송을 다수 제기하였다. 이 중 일부 하급심 판례는 원고들의 청구를 기각한 반면, 일부 하급심 판례는 원고들의 청구를 일부 인용하여[1] 상반된 결론을 내렸고, 현재 모두 서울고등법원에서 소송 계속 중이다.[2]

2011년 11월 넥슨의 온라인 게임 '메이플스토리' 이용자 1320만여명의 개인정보가 해킹으로 유출되었다. 이는 전체 메이플스토리 회원의 약 3분의 2의 개인정보가 유출된 사건이다. 이에 메이플스토리 운영 회사인 넥슨 측은 이를 사과하고, 비밀번호를 변경하는 이벤트를 열어 비밀번호를 변경한 회원들에게 2700원 세트 캐시 아이템을 교환할 수 있는 쿠폰을 지급했다.

2012년 KT한국통신은 전산시스템의 해킹으로 870만건의 고객정보가 유출되었다. 이에 대해 피해자 중 28,715명에 대해 1인당 10만원을 손해배상금으로 지급하라는 판결이 선고되었고 이는 현재 KT한국통신의 항소로 서울고등법원에서 소송계속 중이다.

2014년 1월에는 KB국민, NH농협, 롯데카드 등 3개 신용카드사에서 1억 580만건의 고객정보가 유출되었다.

같은 해 3월에는 KT 한국통신의 홈페이지가 해킹당하는 사건이 벌어지며 1200만명의 고객정보가 유출됐다.

이와 같이 인터넷의 발달과 그 이용의 확대는 생활에 많은 편리를 가지고 왔지만 정보통신기술의 악용으로 대량의 개인정보가 유출되는 사고도 빈번하게 발생하

1) 개인정보유출 피해자 2,882명에게 1인당 20만원의 위자료를 지급하라는 판결을 내렸음. (서울서부지방법원 2013.2.15. 선고 2011가합11733 등 판결)
2) 관련판례에 대하여 자세한 것은 최호진, "해킹에 의한 개인정보유출과 정보통신서비스 제공자에 대한 손해배상책임에 관한 고찰 -SK컴즈 사건을 중심으로-", 법조 63권 2호, 법조협회, 2014, 123~159면 참조.

고 있다. 2001년 이후 국내 주요 개인정보 유출 사고를 정리한 아래 <표 1>을 보면 개인정보가 유출된 기업은 통신사, 온라인게임회사, 온라인컨텐츠 제공업자 등 정보통신서비스업체에 국한 된 것이 아니라 금융회사, 일반 사업회사 등 개인정보를 수집하고 있는 모든 영역의 기업들에게서 발생하고 있다. 또한 시간의 경과와 함께 유출규모가 점차 대규모화 되고 있다.

<표 1> 2001년 이후 국내 주요 개인정보 유출 사고

사고사례		정보 유출 규모
2001년	SK텔레콤	관리소홀로 휴대전화 가입자 신상정보 유출
2002년	하나로통신	e메일 입력 실수로 3,000명의 신용카드 정보 등 유출
2007년	KT하나로텔레콤	고객 730만명의 개인정보가 위탁업체 등에 유출
2008년	옥션	해킹으로 고객 1,081만명 개인정보 유출
	GS칼텍스	고객 1,119만명의 개인정보가 담긴 컴퓨터용 디스크 유출
2009년	SK커뮤니케이션즈	해킹으로 싸이월드 미니홈피 방문자 200만명 정보 유출
2011년	현대캐피탈	해킹으로 고객 42만명 정보 유출
	SK커뮤니케이션즈	3,500만명의 주민등록번호 및 휴대전화번호 등 유출
	넥슨	메이플스토리 이용자 1320만여명의 개인정보가 해킹으로 유출
2012년	KT	고객 870만명 정보 유출
	진학정보사이트	고교 3학년생 68만명 정보 유출
2014년	KB국민, 농협, 롯데카드	1억 580만건 신용정보 유출
	KT	홈페이지 해킹으로 1,170만건 정보 유출

이러한 개인정보유출은 비단 우리나라만의 일은 아니다. 전세계적으로 매년 수천만에서 수억 건의 정보유출이 이루어지고 있으며 정보유출건수와 유출된 정보수는 급증하는 추세를 보이고 있다.[3] 그리고 과거에는 금융기관, 정부 그리고 일반 대기업 등 개인정보를 다수 취급하는 기관·기업이 해킹의 주요대상이었으니 최근 들어서는 항공우주, 전기, 가스 등의 업체에 대한 해킹이 증가하는 추세를 보이고 있다.[4]

3) http://www.datalossdb.org 참조
4) 최창희·김혜란, "해외 사이버 배상책임보험시장 성장의 시사점," kiri Weekly 제298호, 보험연구원,

개인정보유출 사건이 발생하는 경우 자신의 개인정보가 침해된 피해자들은 피해액을 입증하기가 쉽지 않고 소송절차가 번거로워 배상이 용이하지 않고 그 배상액 또한 낮은 문제점이 있다. 반면 개인정보유출을 당한 기업체는 유출로 인한 손해배상의 범위가 확정되어 있지 않아서 이로 인한 손해배상액의 예측이 어려워 위험관리측면에서 어려움을 겪고 있다. 이러한 위험을 관리하기 위하여 미국 등에서는 "사이버 배상책임보험"(Cyber Liability Insurance: CLI)이 사용되고 있다. 사이버 배상책임보험(CLI)은 e-비지니스, 인터넷 네트워크 및 정보 자산 등 사이버 리스크와 관련하여 계약당사자의 위험과 제3자에 대한 손해배상 위험을 모두 담보하는 보험으로서 뮌헨 재보험사는 이 시장이 2013년 현재 13억 달러 규모이며 7년 안에 50억 달러 이상의 규모로 성장할 것을 예상하고 있다.[5)]

현재까지 우리나라에서도 개인정보유출에 따른 피해자에 대한 배상책임을 담보하는 보험이 사이버 배상책임보험(CLI)의 일종으로 몇몇 손해보험사에서 "개인정보보호배상책임보험"이라는 명칭으로 보험상품으로서 제공하여 왔으나 그 이용실적은 미미하였다.

그러나 2014년 1월, 3개 신용카드사의 고객정보 유출사건을 계기로 사회전반에서 개인정보 유출의 심각성이 대두되고 그 배상방법의 불확실성에 대한 우려가 커지면서 최근에는 개인정보유출시의 배상에 관한 보험가입을 의무화하기 위한 법률개정안들이 국회에 의원입법으로 상정되어 있다.

본고에서는 입법에 의한 정보유출배상책임보험의 가입 의무화가 과연 적절한 것인지, 그리고 가입 의무화시 고려할 법적 쟁점은 어떠한 것이 있는지에 관하여 고찰하고자 한다.

Ⅱ. 정보유출배상책임보험의 가입 의무화와 관련된 입법안

1. 개인정보 등의 보호에 관한 현행 법률체계

현재 우리나라에서는 개인정보에 대하여 다수의 법률에 의한 중첩적인 규제를 취하고 있다.

(1) 「개인정보 보호법」에 의하여 개인정보의 처리 및 보호에 관한 일반적인 사항을 규제하고 있다. 이 법에 따라 정보주체는 개인정보처리자가 이 법을 위반한 행

214.9.1. 4면 참조.

5) 최창희·김혜란, 전게논문, 2면 참조

위로 손해를 입으면 개인정보처리자에게 손해배상을 청구할 수 있다. 이 경우 그 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다(개인정보보호법 제39조 제1항). 즉, “개인정보처리자”는 개인정보의 유출에 대한 손해배상책임을 부담한다.

(2) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(약칭: 정보통신망법)」에 따라 “정보통신서비스 제공자”에 의한 개인정보의 처리 및 보호에 관한 사항을 규제하고 있다. 이 법에 따라 이용자는 정보통신서비스 제공자등이 개인정보의 보호에 관한 규정을 위반한 행위로 손해를 입으면 그 정보통신서비스 제공자등에게 손해배상을 청구할 수 있다. 이 경우 해당 정보통신서비스 제공자등은 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다(정보통신망법 제32조). 즉, “정보통신서비스 제공자”는 개인정보의 유출에 대한 손해배상책임을 부담한다.

(3) 「신용정보의 이용 및 보호에 관한 법률(약칭: 신용정보법)」에 따라 “신용정보회사 등”에 대한 신용정보의 이용 및 관리에 관한 사항을 규제하고 있다. 이 법에 따라 신용정보회사 등과 그 밖의 신용정보 이용자가 법을 위반하여 신용정보주체에게 피해를 입힌 경우에는 해당 신용정보주체에 대하여 손해배상의 책임을 진다. 다만, 신용정보회사등과 그 밖의 신용정보 이용자가 고의 또는 과실이 없음을 증명한 경우에는 그러하지 아니하다(신용정보법 제43조 제1항). 즉, “신용정보회사 등”은 신용정보의 유출에 대한 손해배상책임을 부담한다.

위와 같은 개인정보에 관한 규제를 도표로 표시하면 아래 <표 2>와 같다.

<표 2> 개인정보관련 법률의 적용대상[6)]

6) 정종일, “개인정보보호 정상화 대책,” 개인정보 제도변경 관련 설명회 발표자료, 손해보험협회, 2014.9.3. 8면 및 12면의 표를 이용하여 작성함.

법명	분야	적용대상	대상 수	관할청
개인정보보호법	총괄	모든 개인정보처리자	약 380만개 사업자	안전행정부
정보통신망법	정보통신분야	정보통신서비스 제공자 등	약 273만개 사업자 + 160만개 스마트폰 앱	방송통신위원회
신용정보법	금융·신용분야	신용정보회사 등	약 7만개 사업자	금융위원회

사업자는 개별 개인정보의 분야에 따라 위와 같이 다양한 규제를 받는 것 이외에 사업자의 사업내용에 따른 규제를 추가적으로 받게 된다. 예컨대 금융회사가 전자금융거래를 하는 경우에는 「전자금융거래법」에 의한 규제를 추가적으로 받게 된다. 즉, “금융회사 또는 전자금융업자”는 전자금융거래법 제9조 제1항 각호의 어느 하나에 해당하는 사고로 인하여 이용자에게 손해가 발생한 경우에는 그 손해를 배상할 책임을 진다(전자금융거래법 제9조 제1항).

2. 정보유출배상책임보험의 가입 의무화 관련 법률개정안

위에서 언급한 여러 법률에서 개인정보의 유출과 관련된 개인정보처리자 등의 손해배상책임을 명기하였음에도 불구하고 실제로는 피해를 입은 정보주체가 손해배상청구의 소를 제기하더라도 해당 기업 등의 배상능력이 부족한 경우에는 피해구제에 한계가 있게 된다.

이러한 문제를 제거하기 위하여 개인정보처리자 등에게 손해배상책임이 발생한 경우 그 손해의 배상을 보장하기 위하여 보험에 가입하거나 금융회사에 자산을 예탁하게 함으로써 정보주체를 위한 피해보상 체계를 구축하고자 하는 법률 개정안이 발의되었다. 각 법률개정안의 실제 내용은 아래와 같다.

(1) 개인정보 보호법

개인정보 보호법 일부개정법률안은 2014년 2월 14일에 박대동 의원을 대표로 발의되었다. 그 내용은 아래와 같다.

현 행	개 정 안 (박대동 의원안)
<신 설>	제39조의2(손해배상의 보장) ①개인정보처리자는 제39조 제1항에 따른 손해배상책임의 이행을 위하여 보험에 가입하거나 「금융위원회의 설치 등에 관한 법률」 제38조 제1호부터 제8호까지의 기관에 자산을 예탁하여야 한다. ② 제1항에 따른 보험가입 및 자산예탁의 기준, 절차 등 그밖에 필요한 사항은 대통령령으로 정한다.
제75조(과태료) ① (생 략)	제75조(과태료) ① (현행과 같음)
② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.	② ----------.
<신 설>	14. 제39조의2제1항에 따른 보험가입 또는 자산의 예탁을 하지 아니한 자

(2) 정보통신망법

정보통신망법 일부개정법률안은 2014년 2월 14일에 박대동 의원을 대표로 발의되었다. 그 내용은 아래와 같다.

현 행	개 정 안 (박대동 의원안)
<신 설>	제32조의2(보험가입 등) ① 정보통신서비스 제공자 등은 제32조에 따른 손해배상책임의 이행을 위하여 보험에 가입하거나 「금융위원회의 설치 등에 관한 법률」 제38조 제1호 내지 제8호의 기관에 자산을 예탁하여야 한다. ② 제1항에 따른 보험가입 및 자산예탁의 기준, 절차 등 그밖에 필요한 사항은 대통령령으로 정한다.
제76조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자와 제7호부터 제11호까지의 경우에 해당하는 행위를 하도록 한 자에게는 3천만원 이하의 과태료를 부과한다.	제76조(과태료) ① ---------- ---------- ---------- ---------- ----------.
<신 설>	13. 제32조의2 제1항에 따른 보험가입 또는 자산의 예탁을 하지 아니한 자

(3) 신용정보법

신용정보법 일부개정법률안은 2014년 2월 14일에 박대동 의원을 대표로 발의되었다. 그 내용은 아래와 같다.

현 행	개 정 안 (박대동 의원안)
<신 설>	**제43조의2(**손해배상의 보장**)** ① 신용정보회사 등과 그 밖의 신용정보 이용자는 제43조 제1항에 따른 손해배상책임의 이행을 위하여 보험에 가입하거나 「금융위원회의 설치 등에 관한 법률」 제38조 제1호 내지 제8호의 기관에 자산을 예탁하여야 한다. ② 제1항에 따른 보험가입 및 자산예탁의 기준, 절차 등 그 밖에 필요한 사항은 대통령령으로 정한다.
제52조(과태료) ① 제32조 제7항을 위반하여 개인신용정보를 제공받는 자의 신원과 이용 목적을 확인하지 아니한 자에게는 3천만원 이하의 과태료를 부과한다.	**제52조(과태료)** ① 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다. 1. 제32조 제7항을 위반하여 개인신용정보를 제공받는 자의 신원과 이용 목적을 확인하지 아니한 자
<신 설>	2. 제43조의2 제1항에 따른 보험가입 또는 자산의 예탁을 하지 아니한 자

그러나 신용카드 3사의 개인정보유출 사건과 관련하여 신용정보법에 관한 총 16건의 법률안이 각각 발의되어 2014년 4월 30일 국회 법안심사소위원회에서는 각 법률안의 내용을 통합·조정하여 대안을 위원회안으로 제안하기로 하였고 이에 따라 2014년 5월 1일 아래와 같은 내용이 정무위원회안으로 제안되었다.

정무위원회안은 전자금융거래법 제9조 제4항을 모델로 한 입법으로서, 기존 박대동 의원안과는 달리 과태료의 부과가 제외되었다.

현 행	개 정 안 (정무위원장 대안)
<신 설>	**제43조의2(손해배상의 보장)** 대통령령으로 정하는 신용정보회사등은 제43조에 따른 손해배상책임의 이행을 위하여 금융위원회가 정하는 기준에 따라 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 하여야 한다.

(4) 참고: 전자금융거래법

참고로 전자금융거래법은 2006년 4월 28일 법제정시부터 금융기관 또는 전자금융업자가 접근매체의 위조나 변조로 발생한 사고, 계약체결 또는 거래지시의 전자적 전송이나 처리과정에서 발생한 사고로 인하여 이용자에게 손해가 발생한 경우에 그 손해를 배상할 책임을 이행하기 위하여 금융위원회가 정하는 기준에 따라 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 하여야 하도록 규정하여(전자금융거래법 제9조 4항) 배상책임을 담보하는 보험 등의 가입을 의무화 하고 있었다.

전자금융거래법에는 보험 등 가입의무 위반시에 대한 과태료의 부과가 규정되어 있지 않다.

제정당시	현행
제9조(금융기관 또는 전자금융업자의 책임) ④금융기관 또는 전자금융업자는 제1항의 규정에 따른 책임을 이행하기 위하여 금융감독위원회가 정하는 기준에 따라 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 하여야 한다.	**제9조(금융회사 또는 전자금융업자의 책임)** ④금융회사 또는 전자금융업자는 제1항의 규정에 따른 책임을 이행하기 위하여 금융위원회가 정하는 기준에 따라 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 하여야 한다.

Ⅲ. 가입의무화 여부

1. 사회·경제적 필요성

앞서 본바와 같은 정보유출사고의 빈번한 발생위험성과 정보유출시의 정보주체 및 개인정보처리자 등(정보유출기업)에 대한 심각한 경제적 위험성을 고려하여 볼 때 정보유출배상책임보험의 가입을 법에 의하여 의무화하는 것은 사회·경제적으로 필요성이 있다고 보인다. 정보주체, 개인정보처리자 등(정보유출기업) 그리고 보험회사 등 관련당사자 등의 측면에서 살펴보면 다음과 같다.

(1) 정보주체(피해자) 측면

정보주체의 측면에서 보면 개인정보처리자 등에게 맡겨놓은 본인의 개인정보가

유출될 경우 손해를 입는 것은 물론이나 현실적으로 그 손해의 발생 및 손해배상액의 입증에는 대단한 어려움이 따른다. 이를 고려하여 우리나라의 개인정보보호법, 정보통신망법, 신용정보법에서는 그 입증책임을 전환하여 개인정보처리자 등이 위법사실에 대한 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없도록 규정하고 있다.

그런데 입증책임이 전환되었다 하더라도 정보를 유출한 개인정보처리자 등의 배상자력이 불충분한 경우에는 정보주체의 피해를 보상받기 어렵게 된다. 실제로 최근 정보유출사고는 대규모로 행하여지는 경우가 많아서 사고 1건 별로 개인정보처리자 등이 부담하는 배상책임액이 커질 수 밖에 없다.

따라서 개인정보처리자 등(정보유출기업)이 의무적으로 정보유출배상책임보험을 가입한 경우 피해자인 정보주체의 측면에서는 자력있는 보험회사 등에게 피해보상을 받을 수 있으므로 실질적인 손해보상이 될 수 있을 것이다.
또한 정보유출배상책임보험은 그 법적 성질이 “책임보험”이므로 보험사고의 발생시 피해자인 정보주체는 상법 제724조 제2항에 의하여 보험회사에 대해 직접청구권을 행사할 수 있으므로 보다 원할한 손해보상이 가능해지는 이점 또한 있게 된다.

(2) 개인정보처리자 등(정보유출기업)의 측면

우리나라의 개인정보보호법, 정보통신망법, 신용정보법에서는 그 입증책임을 전환하여 개인정보처리자 등이 위법사실에 대한 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없도록 규정하고 있다. 그런데 최근의 정보유출사고는 대규모로 행하여지는 경우가 많아서 사고 1건 별로 개인정보처리자 등이 부담하는 배상책임액이 커질 수 밖에 없다. 즉, 정보유출시 1인당 피해배상액은 소액일지라도 다수의 피해자가 발생하여 총 배상액은 기업이 감당하기 어려운 수준이 될 가능성이 크다.

실제로 2011년 7월 SK커뮤니케이션즈의 네이트 또는 싸이월드의 회원 중 3495만여명의 개인정보가 유출된 사건에 대하여 2013년 서울서부지방법원은 1인당 20만원의 위자료를 2882명의 원고에게 지급하라는 판결을 내렸는데[7] 이 사건에서 만약 3495만명이나 되는 피해자 전부가 소송을 제기하였다면 6조 9900억원이라는 천문학적인 액수의 배상금이 지급되게 된다.

참고로 <표3>에서 볼 수 있듯이 세계 주요국가의 개인정보 유출 사고당 평균비용은 2009년 기준 약 343만 달러로 중소기업에게는 경영에 타격을 줄 수 있을 정도의

7) 개인정보유출 피해자 2,882명에게 1인당 20만원의 위자료를 지급하라는 판결을 내렸음. (서울서부지방법원 2013.2.15. 선고 2011가합11733 등 판결)

고액이다.

<표3> 주요국 정보유출 사고당 평균비용[8)]

[단위 : 달러]

국가	미국	영국	독일	프랑스	호주	평균
평균비용	675만	256만	344만	253만	183만	343만

최근에는 징벌적 손해배상제나 법정손해배상제의 도입[9)]이 개인정보 관련 논의에서 쟁점화 되어 있고, 관련 규정이 곧 입법에 반영될 것으로 생각되어 개인정보처리자 등이 부담하는 경제적인 위험은 보다 커진 것으로 생각된다. 따라서 정보유출배상책임보험 가입을 통한 위험의 분산이 필요할 것으로 생각된다.

(3) 보험회사의 측면

위에서 본바와 같이 정보유출배상책임보험 가입을 통하여 정보주체는 자신이 받은 피해에 대한 확실한 보상이 가능하고, 개인정보처리자 등은 위험의 분산을 통하여 정보유출사고 발생시 경제적 위험을 피할 수 있게 된다.

그런데 만약 정보유출배상책임보험의 가입을 의무화하지 않을 경우 보험회사에 이 보험을 가입하는 개인정보처리자 등은 대부분이 사고발생의 확률이 높은 자일 가능성이 크다. 그렇게 되면 보험회사로서는 정보유출가능성이 높은 소위 불량물건만 보험가입을 받도록 되어 있어 정상적인 위험률에 따른 보험료의 부과가 어렵게 될 것이다. 즉, 개인정보처리자 등의 위험의 역선택이 발생할 가능성이 높다.

따라서 보험가입을 의무화하여 가능한한 보험집단의 크기를 키우는 것이 정보유출배상책임보험의 위험률계산을 쉽게하고 실제 보험료를 적절하게 유지할 수 있도록 할 것으로 생각된다.

---

8) 자료 : 보험연구원 2012.2 (원 자료 PGP/Ponemon, 2009)

9) 정보통신망법은 2014.5.28.개정시에 이미 법정손해배상제도를 도입하여 2014.11.29.부터 시행하고 있다.

제32조의2(법정손해배상의 청구)

① 이용자는 다음 각 호의 모두에 해당하는 경우에는 대통령령으로 정하는 기간 내에 정보통신서비스 제공자등에게 제32조에 따른 손해배상을 청구하는 대신 300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다. 이 경우 해당 정보통신서비스 제공자등은 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

1. 정보통신서비스 제공자등이 고의 또는 과실로 이 장의 규정을 위반한 경우
2. 개인정보가 분실·도난·누출된 경우

② 법원은 제1항에 따른 청구가 있는 경우에 변론 전체의 취지와 증거조사의 결과를 고려하여 제1항의 범위에서 상당한 손해액을 인정할 수 있다.

2. 법적 가능성(위헌여부의 평가)

우리 헌법에서는 국민의 모든 자유와 권리는 본질적인 내용을 침해하지 않는 범위 내에서 국가안전보장·질서유지 또는 공공복리를 위하여 필요한 경우에 한하여 법률로써 제한할 수 있다(헌법 제37조 제1항)고 되어있으므로 입법자의 판단에 따라 헌법상 국민의 기본권의 본질적인 내용을 침해하지 않는 범위 내에서 특정보험의 가입을 의무화하도록 입법하는 것은 가능하다고 생각된다.

현재 우리나라에서는 공공의 이익 등을 위하여 여러 가지 의무보험제도를 실시하고 있다. 대표적인 것은 아래와 같다(보험업법 시행령 제80조 참조).

① 「자동차손해배상 보장법」 제5조에 따른 책임보험계약
② 「화재로 인한 재해보상과 보험가입에 관한 법률」 제5조에 따른 신체손해배상특약부화재보험계약
③ 「도시가스사업법」 제43조, 「고압가스 안전관리법」 제25조 및 「액화석유가스의 안전관리 및 사업법」 제33조에 따라 가입이 강제되는 손해보험계약
④ 「선원법」 제98조에 따라 가입이 강제되는 손해보험계약
⑤ 「체육시설의 설치·이용에 관한 법률」 제26조에 따라 가입이 강제되는 손해보험계약
⑥ 「유선 및 도선사업법」 제33조에 따라 가입이 강제되는 손해보험계약
⑦ 「승강기시설 안전관리법」 제11조의3에 따라 가입이 강제되는 손해보험계약
⑧ 「수상레저안전법」 제34조 및 제44조에 따라 가입이 강제되는 손해보험계약
⑨ 「청소년활동 진흥법」 제25조에 따라 가입이 강제되는 손해보험계약
⑩ 「유류오염손해배상 보장법」 제14조에 따라 가입이 강제되는 유류오염손해배상 보장계약
⑪ 「항공운송사업 진흥법」 제7조에 따라 가입이 강제되는 항공보험계약
⑫ 「낚시 관리 및 육성법」 제48조에 따라 가입이 강제되는 손해보험계약
⑬ 「도로교통법 시행령」 제63조 제1항, 제67조 제2항 및 별표 5 제9호에 따라 가입이 강제되는 손해보험계약
⑭ 「국가를 당사자로 하는 계약에 관한 법률 시행령」 제53조에 따라 가입

이 강제되는 손해보험계약

⑮ 「야생생물 보호 및 관리에 관한 법률」 제51조에 따라 가입이 강제되는 손해보험계약

과거의 예를 보면 4층 이상의 건물을 특수건물로 규정하여 손해보험회사가 영위하는 신체손해배상특약부화재보험에 강제가입하도록 규정한 화재로 인한 재해보상과 보험가입에 관한 법률 제5조는 헌법재판소에서 “개인의 경제상의 자유와 창의의 존중을 기본으로 하는 경제질서와 과잉금지의 원칙에 합치되지 아니한다”고 하여 위헌으로 결정되었다.[10] 그렇지만 사실 이 경우에도 헌법재판소가 보험의 가입강제 자체를 위헌으로 본 것은 아니었다. 단지 “지나치게 과도한” 보험가입강제가 위헌이라는 것이었다고 해석되므로, 정보유출배상책임보험의 가입의무화 규정을 입법할때는 “지나치게 과도한” 보험가입강제가 되지 않도록 주의해야 할 것으로 보인다.

헌법재판소는 구 신체손해배상특약부화재보험이 “보험금액에 관하여 배상책임보험의 경우에는 사망 500만원, 부상 400만원을 상한으로 한 부분보험임에 대하여, 화재보험의 경우에는 건물시가에 해당하는 금액 전액으로 하여 전부 보험으로 하고 있어서 대인배상책임에 대한 책임보험이라는 그 공공적인 주된 목적은 뒤쪽으로 물러나고 (물건보험인) 화재보험이 오히려 주된 자리를 차지하게 하였다“고 하면서 이는 “주된 입법목적을 일탈하여 배상책임보험은 뒷전으로 돌려 부수적인 것으로 하고 화재보험만을 완벽하게 한 본말전도의 체계부조화의 입법이라 아니 할 수 없다”라고 평가하면서 국민의 일반행동자유권 내지 경제활동의 자유를 제한하고 있다고 하였다.

정보유출배상책임보험은 신체손해배상특약부화재보험과는 달리 자신의 이익을 위한 물건보험을 가입강제하는 것이 아니고 경제적으로는 타인을 위한 보험을 가입강제하는 것이라고 할 수 있다. 때문에 국민의 일반행동자유권 내지 경제활동의 자유를 제한한다는 것에서는 비교적 자유롭다고 할 수 있을 것이다.

Ⅳ. 가입의무 입법시 문제점

1. 의무가입자의 범위

10) 헌법재판소 1991. 6. 3, 89헌마204 사건. 당시 이는 정책판단의 문제이지 헌법판단의 문제는 아니라고 한 소수의견도 있었다.

정보유출배상책임보험의 가입을 의무화 하는 경우 개인정보 보호법, 정보통신망법 및 신용정보법의 적용대상이 되는 개인 또는 기업의 모두에게 가입을 의무화할 것인가? 헌법재판소의 판단[11]에 비추어보면 “개인의 경제상의 자유와 창의의 존중을 기본으로 하는 경제질서와 과잉금지의 원칙에 합치되는 한도”에서의 가입 의무화를 규정해야 할 것으로 생각한다.

이미 보험 등의 가입의무화를 규정하고 있는 전자금융거래법 제9조 제4항에서도 “금융위원회가 정하는 기준에 따라” 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 하도록 규정하고 있다. 이에 따라 전자금융거래감독규정 제5조[12]에서는 기업 규모에 따른 가입의무를 규정하고 있다.

이러한 면에서 개인정보 보호법, 정보통신망법 및 신용정보법 개정안은 “보험가입 및 자산예탁의 기준, 절차 등 그밖에 필요한 사항은 대통령령으로” 정하도록 하고 있기 때문에 향후 시행령에서의 적절한 가입기준의 제시가 있어야 할 것으로 생각한다.

2. 보상범위의 제한

정보유출배상책임보험의 가입을 의무화 하는 경우 그 보험의 보상범위를 어디까지 할 것인지가 문제가 된다. 개인정보 보호법, 정보통신망법 및 신용정보법 개정안은 “각 법에 따른 손해배상책임의 이행을 위하여” 보험에 가입할 것을 규정하고 있다.[13] 이 경우 각 법률에서 규정한 의무의 범위가 매우 다양하기 때문에 개인정보

11) 헌법재판소 1991. 6. 3, 89헌마204 사건.

12) 전자금융거래감독규정 제5조(전자금융사고 책임이행을 위한 보험 등의 가입에 관한 기준)
① 금융회사 또는 전자금융업자가 법 제9조제4항에 따라 전자금융사고 책임이행을 위한 보험 또는 공제에 가입하는 경우 보상한도는 다음 각 호에서 정하는 금액 이상이어야 한다. <개정 2013.12.3>
1. 「금융위원회의 설치 등에 관한 법률」 제38조제1호(다만, 「은행법」에 의한 지방금융회사 및 같은 법 제58조에 의해 인가를 받은 외국금융회사의 국내지점은 제외한다) 및 제7호의 회사, 「전자금융거래법 시행령」 제2조제2호의 회사 : 20억원
2. 「금융위원회의 설치 등에 관한 법률」 제38조제8호의 회사, 「전자금융거래법」 제2조제3호나목(신용카드업자에 한한다) 및 다목의 회사, 「전자금융거래법 시행령」 제2조제1호의 회사, 「은행법」에 따른 지방금융회사 및 같은 법 제58조에 의해 인가를 받은 외국금융회사의 국내지점 : 10억원
3. 「금융위원회의 설치 등에 관한 법률」 제38조제2호(다만, 명의개서대행업무를 수행하는 회사는 제외)의 회사 : 5억원
4. 제1호 부터 제3호 이외의 금융회사 : 1억원. 다만, 제1호 부터 제3호 이외의 금융회사들이 관련 법령에 의해 당해 금융회사를 구성원으로 하는 금융회사를 통해 전자금융거래 관련 정보기술부문의 주요부분을 공동으로 이용하는 경우, 정보기술부문의 주요부문을 제공하는 금융회사가 공동 이용 금융회사 전체의 사고를 보장하는 내용으로 제2호의 금액(시행령 제2조제5호의 금융회사는 제1호의 금액) 이상의 보험 또는 공제에 가입하면 공동 이용 금융회사는 본호의 보험 또는 공제에 가입한 것으로 본다.
5. 법 제28조제2항제1호 및 제2호의 전자금융업자 : 2억원
6. 제5호 이외의 전자금융업자 : 1억원

처리자 등이 손해를 배상해야 할 경우의 수도 상당히 광범위할 것으로 예상된다.

따라서 의무가입해야 하는 정보유출배상책임보험의 보상범위를 각 법이 규정하는 핵심적인 범위에 제한 할 수 있도록 향후 시행령에서의 적절한 규정이 있어야 할 것으로 생각된다.

3. 보상한도의 제한

개인정보유출 사고의 경우는 한 번의 사고로도 대량의 정보가 유출되는 경우가 많고, 1인당 피해액은 소액에 불과하더라도 총 배상액의 규모는 다액인 경우가 많이 있다. 때문에 보상한도의 제한을 두지 않는 경우 보험료 부담이 너무 커서 헌법재판소가 위헌의 기준으로 제시하는 "지나치게 과도한" 보험가입강제가 될 여지가 있다. 따라서 정보유출배상책임보험의 가입을 의무화 하는 경우 의무가입해야하는 보상한도를 제한할 필요성이 있다고 본다.

보상한도의 제한에 있어서는 (1) 자동차손해배상보장법 제5조처럼 의무보험에 가입해야 하는 보상금액의 상한을 정하는 방식, (2) 전자금융거래법에 따라 전자금융거래감독규정 제5조처럼 의무가입할 보상금액의 하한을 정하는 방식 2가지 모두 검토 가능할 것이다.

4. 면책사유의 문제

현행 개인정보 보호법, 정보통신망법 및 신용정보법 등에 따를 때 개인정보처리자 등의 고의에 의한 위법행위로 인한 정보주체의 손해에 대하여도 배상할 책임이 있으므로 정보유출배상책임보험의 보상범위에 고의에 의한 사고도 포함될 가능성이 있다.

기존의 의무가입보험의 경우, 자동차손해배상보장법에 의한 대인배상I은 고의에 대해서도 보상하고 있지만, 유류오염손해배상보장법에 의한 보험가입의 경우에는 유조선 선박소유자의 고의로 손해가 발생한 경우 보험자 등에 대하여 직접 손해배상의 지급을 청구할 수 없다고 규정하고 있다(유배법 제16조 제1항). 즉 의무가입보험의 경우 고의를 면책으로 할 것인가는 입법자의 재량으로 맡겨져 있다고 보아야 할 것이다.

---

13) 신용정보법 제43조: "신용정보회사등이 이 법을 위반하여 신용정보주체에게 피해를 입힌 경우"
개인정보보호법 제39조: "개인정보처리자가 이 법을 위반한 행위로 정보주체에게 손해를 입힌 경우"
정보통신망법 제32조: "정보통신서비스 제공자등이 개인정보보호 관련 규정을 위반한 행위로 손해를 입힌 경우"

생각건대 현재 보험계약법상 고의사고는 면책이 일반적인 점(상법 제659조), 현재 임의보험으로 운영 중인 정보유출배상책임보험에서도 고의를 면책으로 하고 있는 점, 정보유출배상책임보험의 보험사고가 자동차손해배상보장법에 의한 대인사망사고와 비교할 때에는 그 피해의 정도가 약할 것으로 생각되는 점, 보험이 기업의 도덕적 해이를 조장하는 수단으로 악용될 우려를 없애야 한다는 점을 고려한다면 고의로 인한 사고의 경우에는 면책으로 하는 것이 타당할 것으로 생각된다.

5. 가입강제방법

개인정보 보호법, 정보통신망법 개정안 및 신용정보법 개정초안은 정보유출배상책임보험의 의무가입을 강제하기 위하여 "미가입시 3천만원 이하 과태료를 부과"하는 제재 수단을 규정하고 있다.

보험가입 의무화에도 불구하고 제재 수단 불비시 가입의무를 이행하지 아니한 자와 이행한 자에 대한 형평성의 문제가 발생하고, 정보주체 보호라는 제도의 취지가 퇴색될 우려가 있어서 미가입자에 대한 제재 도입은 필요하다고 보여진다.

다만, 우리 헌법재판소는 구 화재로 인한 재해보상과 보험가입에 관한 법률에서 보험계약의 체결강제를 위하여 제23조에서 특수건물의 소유자가 가입의무를 어기는 경우에는 500만원 이하의 벌금에 처하게 하였고, 제7조는 이에 더 나아가 재무부장관이 관계 행정기관에 대하여 가입의무자에 대한 인·허가의 취소, 영업의 정지, 건물사용의 제한 등 필요한 조치를 취할 것을 요청할 수 있고 행정기관은 이 요청에 정당한 이유가 없으면 응하여야 하도록 규정하고 있는 것에 대하여 이러한 조항을 "보험가입 의무자인 특수건물소유자가 의무이행을 하지 않을 때에는 그 직업선택의 자유와 재산권행사의 제한이 따르게 함으로써 기본적 생존, 인간다운 생활에 위협을 받게 하는 등 그 간접강제의 수단으로서는 지나치게 가혹하다"고 평가하였다.[14] 반면 자동차손해배상보장법에 의한 자동차손해배상 책임보험과 고압가스안전관리법에 의한 손해배상 책임보험에 대해서는 "일종의 강제보험이지만 그 가입강제를 위하여 인·허가의 취소, 영업의 정치처분 등의 제재까지를 과하게 되어 있지는 않다"고 평가하였다.

정보유출배상책임보험의 의무가입을 강제하기 위하여 미가입시 과태료를 부과하도록 규정한 것은 헌법재판소 판결에 비추어 보았을 경우 지나치게 가혹한 제재수단으로는 생각되지 아니한다. 다만 과태료 액수 "3천만원"이 적절한 것인가는 입법적인

14) 헌법재판소 1991. 6. 3, 89헌마204 사건. 당시 이는 정책판단의 문제이지 헌법판단의 문제는 아니라고 한 소수의견도 있었다.

판단을 필요로 한다고 보인다.

6. 3개 법률에 의한 보험가입 의무의 중복문제

개인정보 보호법, 정보통신망법 및 신용정보법 개정안에 따라 정보유출배상책임보험의 가입의무가 부과되는 경우 3개 법률의 적용범위가 중첩됨에 따라서 1개 사업자가 각각의 법률에 의하여 보험가입의무가 중복되는 문제가 발생하게 된다. 예컨대 어떠한 사업자가 개인정보보호법과 정보통신망법에 의하여 별도인 2건의 보험가입의무가 발생하는 경우이다.

이 경우 법이론적으로는 개별 법령은 각각 그 규율대상이 상이하기 때문에 각각 보험을 가입해야 한다고 생각할 수 있으나, 실무적으로는 유사한 보험 상품에 중복하여 가입하는 셈이 될 수 있다. 따라서 이러한 문제를 해결하기 위해서는 향후 의무보험관련 보험상품을 만들 때에 개별 법률에서 보호하는 부분이 중복되는 것을 기본약관으로 하고 개별 법률이 특별히 규율하는 부분은 특별약관으로 하여 하나의 보험계약으로 포괄적으로 보험보상이 가능하도록 보험상품을 설계해야 할 것으로 생각된다.

Ⅴ. 결론

이상에서 개인정보 보호법, 정보통신망법 및 신용정보법에 정보유출배상책임보험에의 가입 의무조항을 신설해야 하는 지에 대해서 살펴보고, 가입의무조항의 신설시에 유념해야할 관련 법률문제에 관하여 연구하였다.

정보유출배상책임보험을 의무 가입하도록 하는 방안은 정보주체에 대한 실질적인 손해보상, 기업의 위험 분산 등의 측면에서 바람직하다고 생각된다.

정보유출배상책임보험의 가입기준, 보상범위, 보상한도 등은 향후 시행령에서 적절하게 제한할 필요가 있을 것으로 보여진다. 다만, 고의에 의한 사고의 경우는 현행 법률과의 균형 및 보험의 선의성 유지를 위한 고의사고 면책 방안, 정보주체 보호라는 제도 취지 제고를 방지하기 위한 적절한 수준의 제재수단 도입 방안에 대하여는 적극적으로 검토할 필요가 있다고 생각된다.

(끝)

개인정보유출 배상책임보험
제도개선 토론회

국내외 사이버 배상책임보험 시장 현황

2014. 12. 1

보험연구원 최창희 연구위원

발표 내용 요약

- 사이버 배상책임보험(CLI)*은 개인정보 유출 배상책임보험을 포함하는 종합보험입니다.
- 현재 사이버 위험에 의한 손해는 대재해에 의한 손해의 5배 수준으로 추정됩니다.
- 미국에서는 연간 수천만에서 수억 건의 개인정보 유출이 일어나고 있으며 미국 CLI 시장 규모는 연간 13억 달러, CLI 시장 침투도는 0.0077%입니다.
- 최근 한국에서 미국과 유사한 수준의 대규모 개인정보 유출 사고가 일어나고 있음에도 불구하고 한국 CLI 시장 규모는 연간 42.9억 원이고 침투도는 0.00031%로 미국의 1/25 수준입니다.
- 이렇게 활성화되지 않은 CLI 시장은 한국 기업의 사이버 위험에 대한 의식 수준이 높지 않다는 것을 보여줍니다.
- 현재 외국의 보험회사들은 다양한 담보를 포함하는 CLI 상품을 판매하고 정보 유출 사고 방지를 위한 다양한 부가 서비스를 함께 제공하여 정보 유출사고 방지에 기여하고 있습니다.
- 개인정보 유출 보험의 의무화는 국내 CLI 시장을 활성화시켜 개인정보 유출 피해자의 권리를 보호하고 기업을 사이버 위험으로 부터 지킬 뿐 아니라 더 나아가 보험회사들이 개인정보 유출 사고를 방지하는 부가 서비스를 제공하는데 기여할 것으로 예상됩니다.

*** 사이버 배상책임보험을 CLI (Cyber Liability Insurance) 라 함.**

Contents

I CLI 보험과 사이버 위험

KiRi 보험연구원

1. 사이버 배상책임보험이란?

✓ 피보험자의 사이버 상의 행위로 인하여 제3자 또는 피보험자 자신에게 발생하는 손해를 담보하는 보험을 사이버 배상책임보험(CLI)이라 함
⇒사이버 배상책임보험은 개인정보 유출 배상책임보험을 포함하는 보험임

사이버 배상책임보험 상품

제3자 손해 보상

1) 정보 유출·훼손·유실에 의한 손해
2) 1)로 발생한 2차적 재산 손해(금융·의료 정보 유출)
3) 업무 차질로 발생한 매출 감소 및 휴업 손해 (시스템 정지·오류)

피보험자 손해 보상

1) 정보유출·훼손·유실에 의한 소득 손실 또는 비용 증가
2) 시스템 복구 비용 및 업무 중단으로 발생하는 비용
3) 사이버 갈취, 명성훼손, 법적 대응 비용
4) 피해자 공지 비용, 벌금 및 과징금, 카드 재발급 비용

부가 서비스

1) 사이버 위험 평가 서비스
2) 사이버 위험 관련 교육 서비스
3) 사이버 위험 관리 컨설팅
4) 사고 발생 실시간 대응 서비스

2. 사이버 손해의 규모

✓ 사이버 보안 회사인 매카피(McAfee)의 2013년 보고서에 따르면 전세계적으로 사이버 상의 불법행위에 의해 발생하는 비용은 연간 3천억~1조 달러 규모임(대재해 손해의 5배 규모)

⇒ 사이버 범죄는 개인, 기업, 국가에 큰 피해를 가져와 경제발전을 위협하므로 사이버 위험은 철저히 관리될 필요가 있음

<각종 불법행위에 의한 연간 발생 비용>

세계	비용(Billion 달러, 조 원)	GDP 대비 비율(%)	출처
해적 약탈 행위	1~16	0.008~0.02	IMB
마약	600	0.50%	UNOCD
사이버 범죄	300~1,000	0.4~1.4%	Various

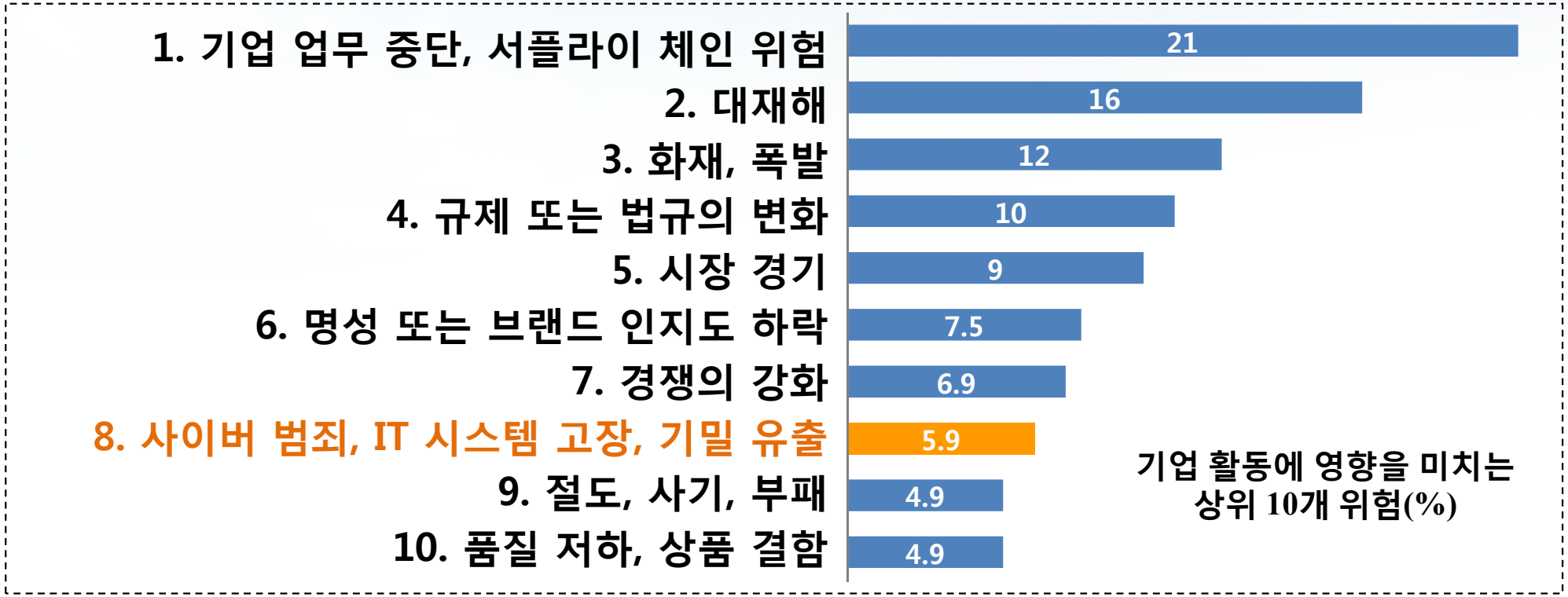
미국	비용(Billion 달러, 조 원)	GDP 대비 비율(%)	출처
자동차 사고	99~168	0.7~1.2	CDC, AAA
기업 도난 사고	70~280	0.5~2	NRF
사이버 범죄	24~120	0.2~0.8	Various

출처: "The Economic Impact of Cybercrime and Cyber Espionage", McAfee, 2013, pp. 5.
http://www.mcafee.com/sg/resources/reports/게-economic-impact-cybercrime.pdf
주: 1 달러를 천 원으로 환산함.

3. 글로벌 기업의 경제 활동에 영향을 미치는 10대 위험

✓ 사이버 위험은 기업활동에 영향을 미치는 10대 위험 중 8번째로 현재 기업의 경제활동에 심각한 위협이 되는 위험임

<글로벌 기업의 10대 위험 서베이 결과>

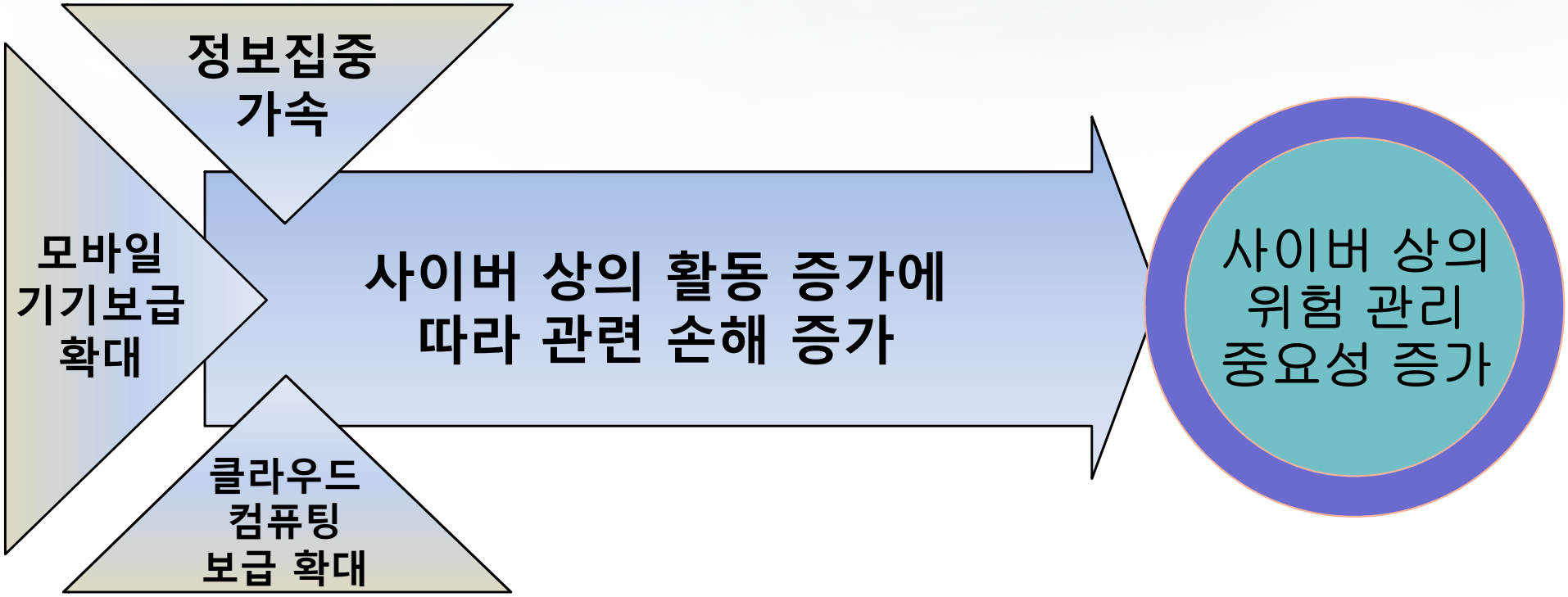


출처: 알리안츠 보험, Top 10 global business risks for 2014

주: 알리안츠의 서베이에 의한 10대 기업 위험, 각 항목은 보험분야에서 557명의 위험관리 컨설턴트, 언더라이터, 임원, 보험금 청구 전문가 등이 선정한 기업활동에 영향을 미치는 위험의 비중. 중복 답변 가능, 합이 100%가 되도록 재합산

4. CLI의 중요성이 부각되고 있는 이유

✓ 경제활동과 실생활에서 컴퓨터 사용과 인터넷의 보급이 확대되면서 개인정보의 집중도가 높아지고 사이버 상의 활동에 수반되는 손해도 함께 증가하는 추세가 나타나고 있음
⇒ 이러한 위험을 관리하기 위해 CLI에 대한 수요가 세계적으로 빠르게 증가하고 있음



5. 사이버 위험의 특징

✓ 아래의 특징을 고려한 효과적인 사이버 위험 관리가 필요함

대재해와 유사한 통계적 특징을 가짐

- 발생 빈도가 높지 않으나 발생 시 피해 규모가 큼
- 발생 시 피해 규모가 매우 클 수 있어 자가 보험이 효과적이지 않음
- 금융시장과의 상관관계가 낮아 금융 시장을 통한 위험관리가 어려움

새로운 손해 유형이 지속적으로 발생

- 잠재 피해자가 과거 유형에 대응하므로 끊임없이 새로운 유형의 불법행위가 발생함
  - 예: 새로운 해킹 기법, 사기 유형
- 새로운 불법행위 유형을 빠르게 인지하고 대응해야 하는 어려움이 있음

업체 간 위험 노출 수준에 차이가 큼

- 동종 업체 간에도 위험 관리 체계, 교육 수준, 보안 시스템 등에 편차가 커 이를 고려한 맞춤형 위험관리가 필요함

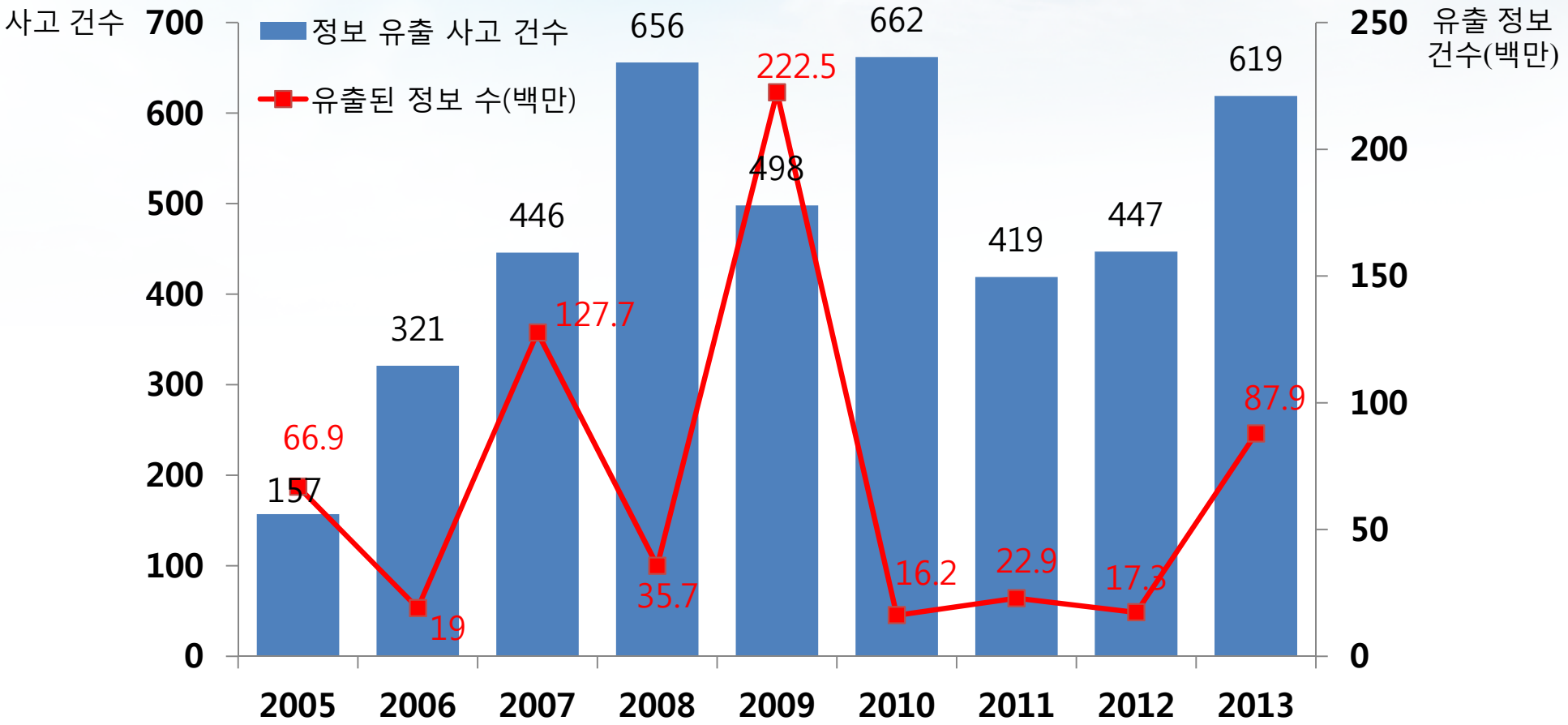
정보집중 가속화로 피해액 증가 추세

- 컴퓨터 및 모바일 기기 보급의 확대로 정보의 집중도가 높아지고 있으며 피해의 규모도 커지는 양상을 보임

6. 미국의 정보 유출 사고 발생 추이

✓ 미국에서는 매년 수천만 건에서 수억 건의 정보 유출 사고가 발생하여 정보 유출이 심각한 사회적 문제로 대두되었음

<미국의 개인정보 유출 사고 건수와 유출 건수 추이>



출처: Identify Theft Resource Center.

주: 2013년 자료는 2014년 1월 1일 자료로서 2014년 1월에 공개된 3천만 건의 유출된 정보 수를 포함, 왼쪽 축은 사고 건수, 오른쪽 축은 사고에 따른 정보 유출 건수.

7. 세계 정보 유출 사고 사례

✓ 세계적으로 대규모 정보 유출 사고가 꾸준히 발생하고 있고 국내에서도 외국과 유사한 규모의 대형 정보 유출 사고가 발생하고 있어 최근 관련 사회적 비용이 크게 증가하였음

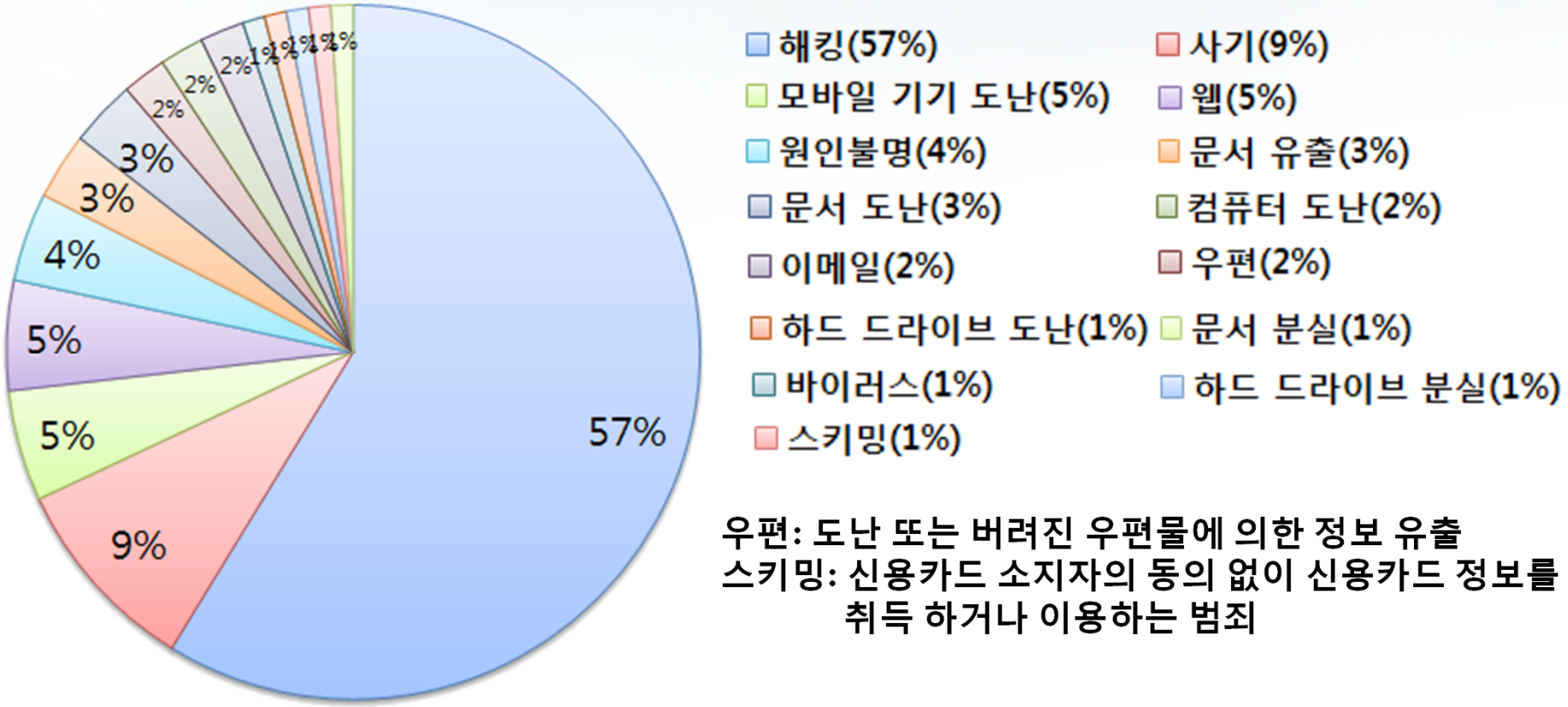
- 2013: 6월 한국 카드3사가 1억 580만 건의 개인정보 유출
  10월 Adobe가 1,300만 건의 사용자 정보 유출
  11월 Target이 4,000만 건의 고객 정보 유출
- 2012: 7월 KT 870만 명의 개인정보 유출
- 2011: 3월 RSA가 SecureID 토큰 유출
  4월 소니가 770만 사용자 정보 유출
  6월 Citi 그룹이 21만 건의 고객 신용카드 정보 유출
- 2009: 1월 Heartland가 1억 건의 신용카드 정보 유출
  5월 영국 의회 비용 영수증 스캔 파일 유출
  12월 RockYou! 가 3,200만 건의 사용자 정보 유출
- 2008: 1월 GE Money가 15만 건의 개인식별번호와 65만 건의 신용카드 정보 유출
  1월 뉴저지 Blue Cross & Blue Shield가 30만 건의 고객 정보 유출
  1월 British National Party가 당원 목록 유출
  1월 Countrywide Financial이 250만 개인식별 번호를 포함한 개인정보 유출
  2월 Lifeblood가 32만 건의 헌혈자 목록 유출

외국 사례 출처: http://en.Wikipedia.org/wiki/Data_breach

8. 정보 유출 원인

✓ 정보 유출 원인은 해킹에 의한 것이 57%로 가장 많았고 그 뒤를 사기, 모바일 기기 도난 등이 따르고 있음. 다양한 경로를 통해 정보가 유출되므로 이러한 부분에 대한 관리가 필요함

<미국의 정보 유출 원인>



우편: 도난 또는 버려진 우편물에 의한 정보 유출
스키밍: 신용카드 소지자의 동의 없이 신용카드 정보를 취득 하거나 이용하는 범죄

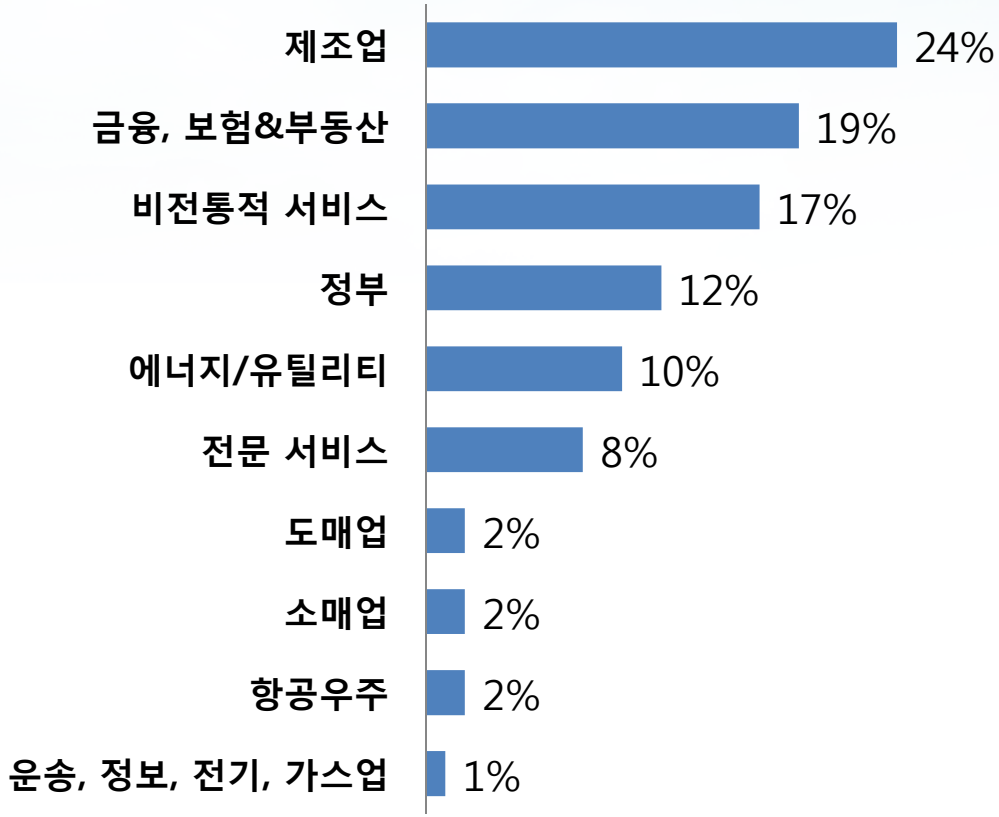
출처: www.datalossdb.org

9. 사이버 공격 대상과 업종별 정보 유출 비용

✓ 현재 미국에서는 다양한 업종의 기업들이 해킹 공격의 대상이 되고 있고 특히 근로자 250인 이하인 중소 기업에 대한 해킹 시도가 빠르게 증가하고 있는 추세를 보임(전체 공격의 31%)

⇒ 국내에서도 유사한 패턴이 나타날 수 있으므로 이에 대한 대비책이 필요함

<해커의 공격 대상 기관(비율)>



<업종별 정보유출 건당 평균 발생 비용(달러)>

출처: Symantec Internet Security Report 2013
기업에 대한 해킹 공격 통계는 2011년 기준

Ⅱ 국내외 CLI 시장 현황

1. 한·미 CLI 시장 비교

✓ 국내에서 미국과 유사한 규모의 개인정보 유출 사고가 발생하고 있으나 국내 기업들의 의식 수준이 높지 않아 CLI 시장이 활성화되어 있지 않음

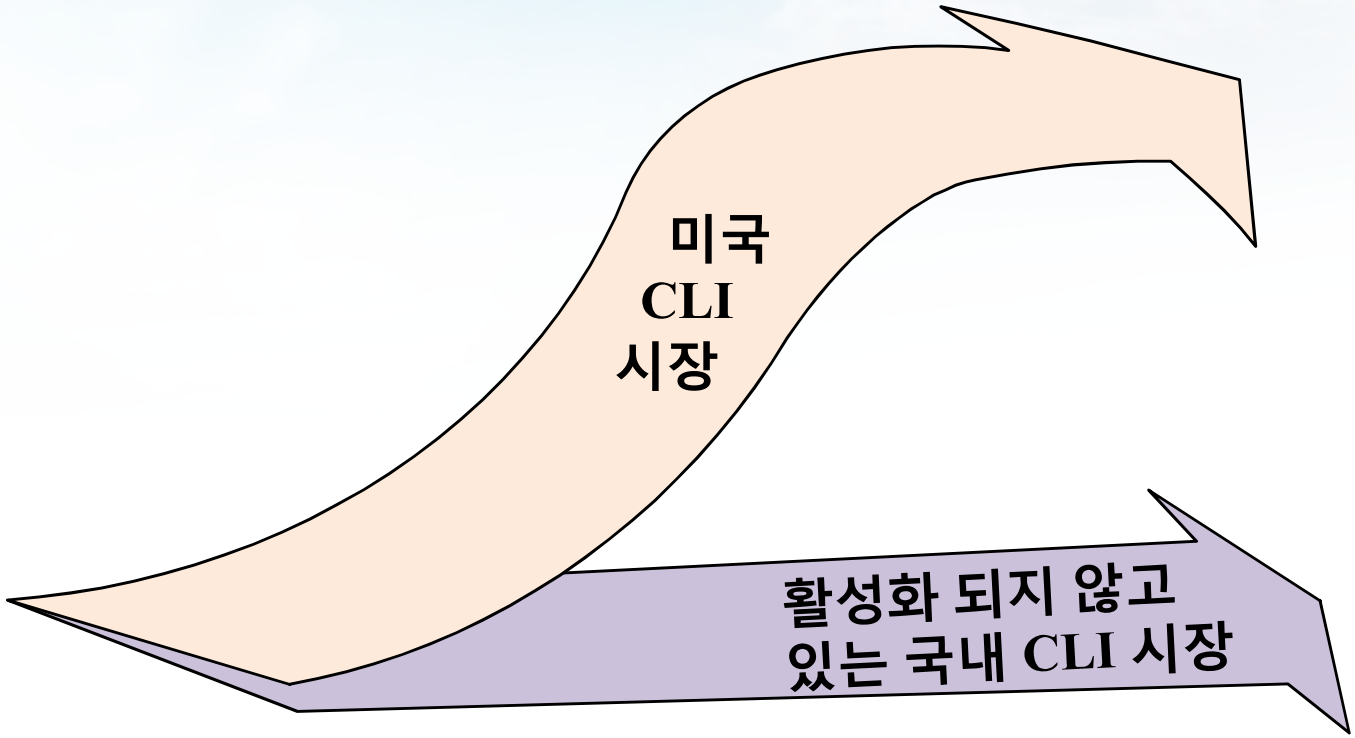
⇒ 보험회사들은 활성화되지 않은 CLI 시장에서 다양한 상품을 개발하고 사고 방지를 지원하기 위한 서비스를 제공하는데 어려움을 가짐

	미국	한국
CLI 보험 보험료	13억 달러	42.9억 원
GDP	16조 8천억 달러	1,376조 원
CLI 침투도 (GDP 대비 보험료)	0.0077%	0.00031%
상품	다양한 상품·담보	상품·담보의 수가 적음
부가 서비스	위험관리 컨설팅, 위험관리 교육, 실시간 사고 대응 지원	없음

출처: 미국 CLI 보험료(https://www.advisen.com/market.html),
한국 CLI 보험료(http://www.kiri.or.kr/pdf/전문자료/KIRI_20140829_175939.pdf),
미국 GDP(World Bank), 한국 GDP(한국 통계청),
한국 보험상품(전자금융거래 배상책임보험, 개인정보 유출 배상책임보험, e-Biz 배상책임보험,
공인전자문서 보관소 배상책임보험, 집적정보통신시설 사업자 배상책임보험), 2013년 기준

2. 미국 CLI 시장 규모 및 추이

✓ 뮌헨재보험의 발표 자료에 따르면 현재 미국 CLI 시장은 13억 달러 규모이고 향후 7년간 50억 달러 규모의 시장으로 현재의 3배 이상 발전할 것으로 예상되나 국내 시장은 저조한 실정임



출처: http://www.asiainsurancereview.com/aircyber/
https://www.advisen.com/market.html

3. 한·미·일 CLI 상품 담보 비교

✓ 한국의 CLI 상품은 7개의 손해만을 담보하고 있어 미국(20개)과 일본(19개) 보다 담보하는 손해의 종류의 수가 적어 CLI 상품이 다양하지 않음

특약의 내용	한국	미국	일본
데이터 재건, 대체 비용	O	O	O
개인정보 유출로 인한 손해배상 비용	O	O	O
네트워크 안전 확보 실패로 인한 손해배상 비용	O	O	O
도난당한 정보가 공적으로 노출되었을 때 손해배상 비용	O	O	O
해킹, 바이러스 관련 손해배상 비용	O	O	O
사이버 범죄 유죄 판결 시의 위자료 비용	O	O	O
기술적인 오류나 부주의로 일어난 손해배상 비용	O	O	O
도난당한 정보의 사용과 관련된 협박처리 비용		O	
정보 유출 시 그 정보의 소유자에게 고지하라는 법률 비용		O	
서비스 중단으로 인한 외부비용과 수입 감소분		O	O
적절한 서비스를 제공했음에도 불구하고 생긴 외부 비용과 수입 감소분		O	O
정보도난, 유출에 대한 위기관리 비용		O	O
정보도난처리비용		O	O
벌금		O	
기업평판 관련 비용		O	
사이버 공공기물 파손 시 처리 비용		O	O
네트워크 파괴 및 침입 시 대처 비용		O	O
유럽의 개인정보보호법과 관련된 비용		O	
포괄적인 접근에 대한 보호 비용(오프라인매개체포함)		O	O
사이버 테러리즘에 대한 보상		O	O
내부 직원에 의한 데이터 유출			O
개인정보 위탁처의 사업자의 누설로 인한 피해보상 시 구상권 불행사			O
피보험자의 부주의, 실수로 인해 생긴 데이터 손실 보상			O
클라우드 컴퓨팅 이용 기업을 대상으로 일반 사이버보험 보장 제공			O

출처: 김소연, 차윤주, 김창기, 최양호(2014), 국내 사이버 위험과 사이버 보험에 관한 연구, 보험학회 하계 학술대회, 2014

4.1 외국 보험회사의 CLI 상품 (1): AIG

✓ AIG는 손해 예방, 보험을 통한 사후 관리, 사고 발생 시 실시간 대응 지원 등으로 피보험자가 능동적으로 사이버 위험에 대비할 수 있도록 다각적인 지원을 제공하는 CLI 상품 판매

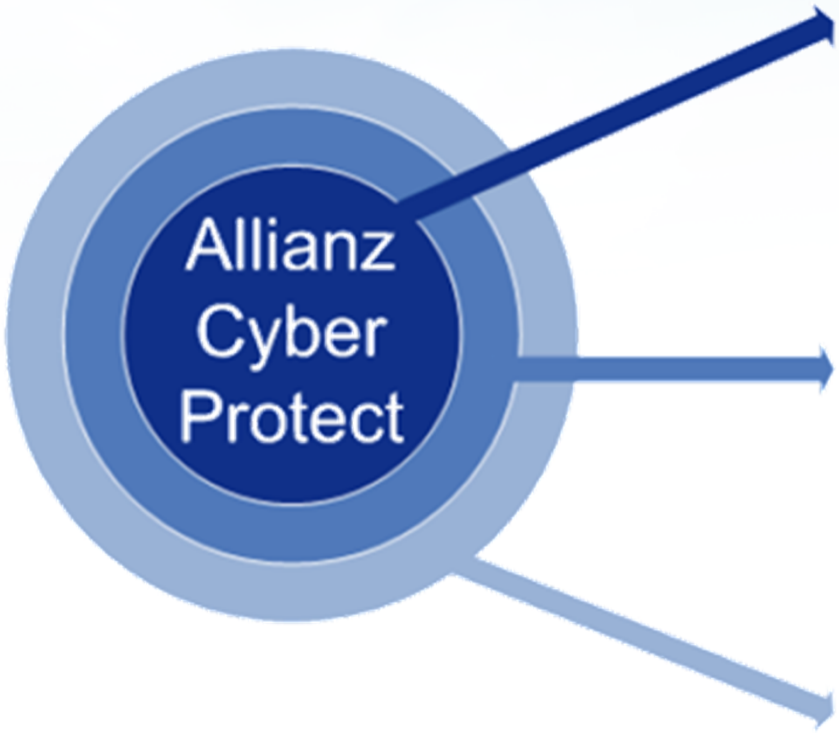
<AIG의 CLI 상품 CyberEdge 개관>

손해 예방	보험 담보	사고 관리 팀
관련 지식	제3자 손해 배상	24시간 지원 서비스(IBM)
연수 및 교육 RiskAnalytics	피보험자에게 발생한 손해	법률 지원
정보보안 평가 서비스(IBM)	휴업 복구 비용	휴업 복구 비용
사이버 리스크 관리 컨설팅	해커 협박 비용	대중매체 전문가 지원
사이버 리스크 예방 서비스 RiskAnalytics	명성 피해 및 저작권 침해	15년간의 사고 관리 지식 공유

4.2 외국 보험회사의 CLI 상품 (2): 알리안츠

✓ 알리안츠도 AIG와 유사하게 피보험자의 사이버 위험을 평가하고 사고를 방지하는데 도움을 주는 부가 서비스를 CLI와 함께 제공

<알리안츠의 사이버 프로텍트 개관>



표준 상품: CLI 보험

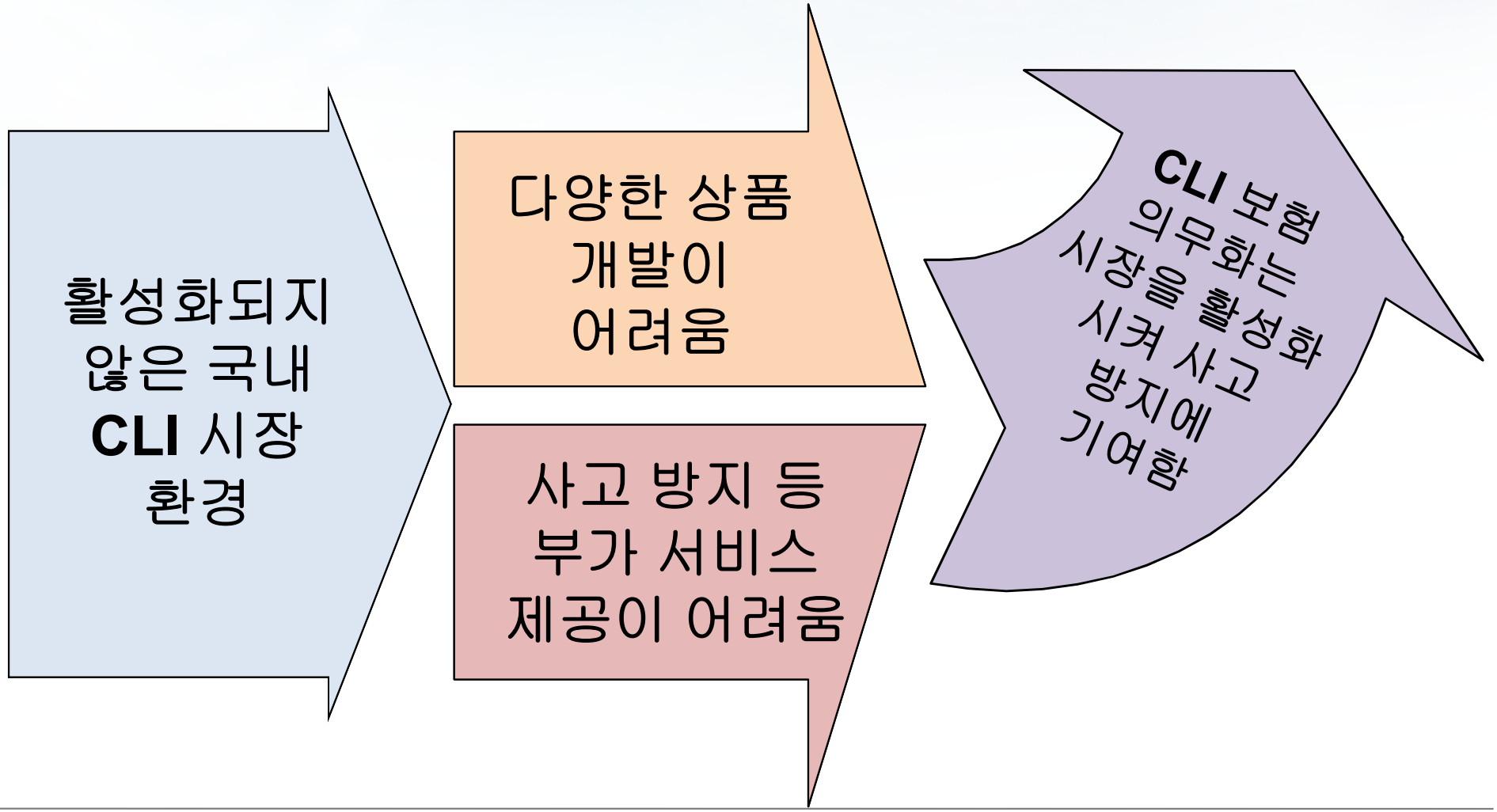
프리미엄: CLI 보험
+CLI 위험 진단 및 컨설팅
(알리안츠 자체 컨설팅)

플러스: CLI 보험
+CLI 위험 진단 및 컨설팅
(외부 파트너 협업)

Ⅲ 제도개선의 기대 효과와 보험회사에 주어진 과제

1. 개인정보 유출 배상책임보험 의무화의 기대 효과

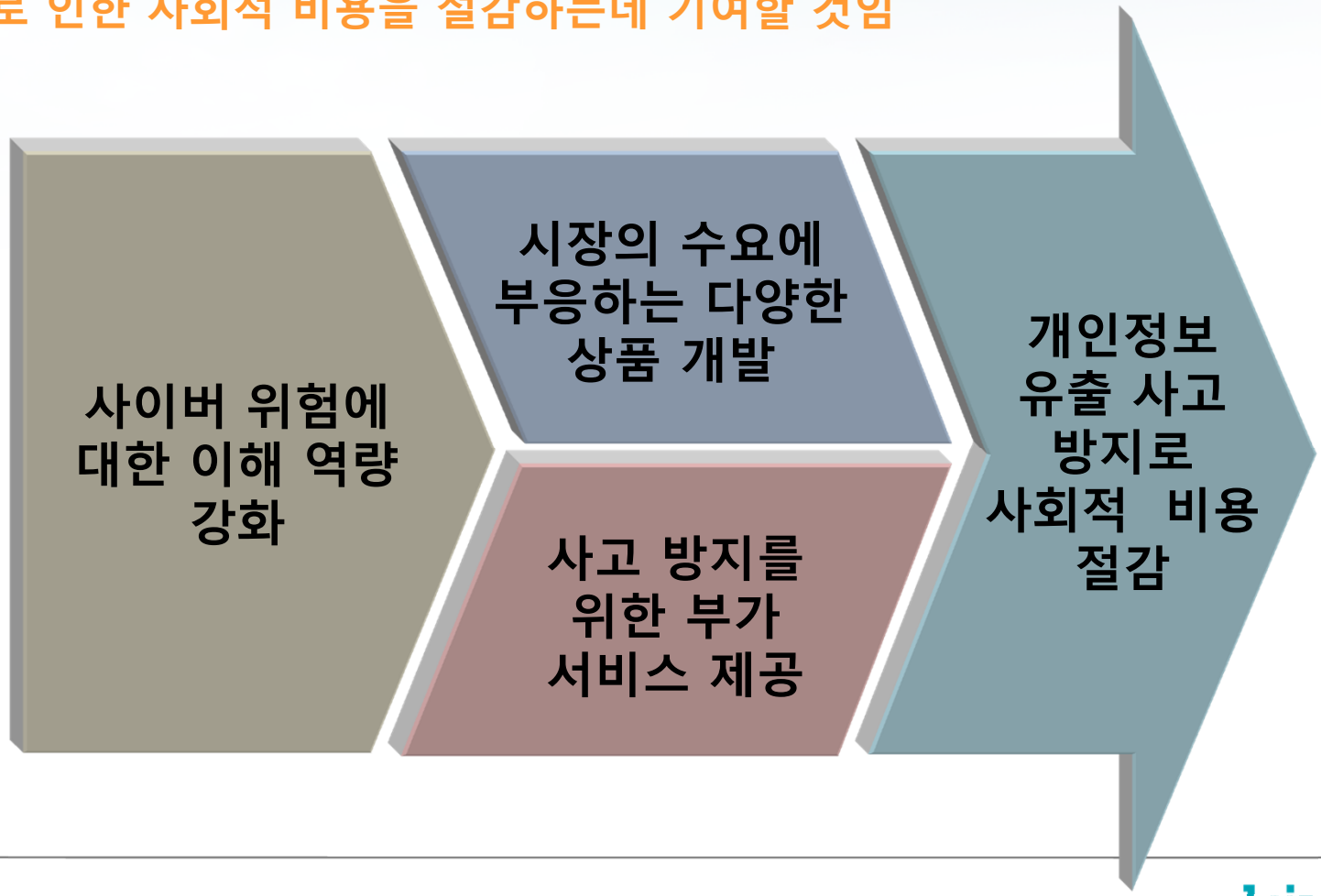
✓ 개인정보 유출 배상책임보험의 의무화는 피해자의 권리를 보호하고 피보험자를 개인정보 유출에 의한 손해로 부터 지키고 더 나아가 국내 CLI 시장을 활성화시켜 보험회사들이 기업이 필요로 하는 CLI 상품을 개발하고 개인정보 유출 방지를 위한 서비스를 제공할 수 환경을 조성하여 개인정보 유출 사고를 줄이는데 기여할 것임



2. 국내 보험회사들에게 주어진 과제

✓ 보험회사들은 ① 사이버 위험 진단, ② 사이버 사고 방지 지원, ③ 사고 발생 시 대응 지원, ④ 시장의 수요에 부응하는 상품을 개발하기 위해 사이버 위험에 대한 역량(IT 시스템, 해킹 대응 기법, 사이버 리스크 관리 체계 구축 및 운영, 관련 법규, 사고 대응 전략 구축 및 실행, 24시간 사고 대응 지원 시스템)을 강화할 필요가 있음

⇒ 궁극적으로 이러한 노력은 개인정보 유출 사고를 방지하여 사이버 상에서 발생하는 사고로 인한 사회적 비용을 절감하는데 기여할 것임



감사합니다.

토론문

정보유출배상책임보험 도입방안

김 은 경 (한국외국어대학교 법학전문대학원 교수)

토론문1

정보유출배상책임보험 도입방안

김은경(한국외국어대학교 법학전문대학원 교수)

Ⅰ 개요

개인정보 유출 사태가 빈번히 발생하고 있다. 게임사, 통신사, 포털사이트, 카드사, 증권사, 보험사 등 업종을 가리지 않고 고객정보를 다루는 회사라면 어디는 상관없이 개인정보가 유출되고 있는 실정이다. 개인정보가 유출되어 국민경제에 악영향을 미치는 시점에서 개인정보를 보호하고 그 유출에 대하여 제재를 강화하기 위하여 2011년 3월 29 개인정보보호법이 제정되었고, 현재까지 지속적인 개정을 해 왔으나 개인정보 유출은 줄어들지 않고, 오히려 계속 증가하고 있다. 또한 그 유출의 건수, 유출정보의 내용, 방법 등이 갈수록 심각하고 민감한 수준에 이르고 있다.

최근 농협의 예금자의 예금에서 거액인출사건이 발생했다. 거액인출사건이 신종해킹이나 피싱 또는 파밍에 해당하는 전자금융사기의 경우에는 그 손해액을 보험사가 보상하는 보험[1]이 가동되고 있다. 그러나 해당 은행의 관리부실이나 보안시스템 허점 또는 예금자의 과실로 사고가 발생한 것으로 밝혀질 경우에는 보험자는 면책이 되어 책임보험자는 보험금을 지급할 필요가 없다. 이때 예금자가 텔레뱅킹 또는 인테넷뱅킹이체시 고객 계좌번호, 통장 비밀번호, 자금이체 비밀번호, 보안카드번호, 주민등록번호의 정보 등의 관리나 전화번호가 연동하여 보안의 대상에 대하여 관리소홀 등의 책임이 있는 경우라면 보험자는 면책이 된다. 즉 예금자의 고의 또는 중과실로 유출되는 경우는 보험자의 면책이다. 또한 은행의 정보관리부실의 경우도 더불어 보험자 면책사유가 된다.

정보유출이 원인인지에 대하여는 아직까지 밝혀지지 않은 상태이지만 전자적 방법으로 거래되

1) 전자금융거래법 제9조 제4항에 따르면 "금융회사 또는 전자금융업자는 접근매체의 위조나 변조로 발생한 사고, 계약체결 또는 거래지시의 전자적 전송이나 처리 과정에서 발생한 사고 또는 전자금융거래를 위한 전자적 장치 또는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 제1항 제1호에 따른 정보통신망에 침입하여 거짓이나 그 밖의 부정한 방법으로 획득한 접근매체의 이용으로 발생한 사고에 따른 책임을 이행하기 위하여 금융위원회가 정하는 기준에 따라 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 하여야 할" 보험가입 등의 의무가 있다.

는 은행업무는 정보 등의 보안이 매우 중요한 사항이다. 이는 기업의 존립과도 연관되는 것일 수 있다. 이와 같이 최근에 발생한 사고 이외에도 빈발하는 개인정보 유출사태는 간과할 수 없는 기업의 물적 손해요인이며 기업이미지에도 타격이 될 수밖에 없는 것이다. 그러한 측면에서 이에 관한 제도적 안전망의 존재를 확인하고 이를 제도적으로 정착시킬 수 있는지를 고찰해봐야 할 다급한 시점인 것은 분명하다.

Ⅱ 정보유출의 대상인 정보의 의미

보호대상이 되는 정보란 자연인을 중심으로 한 개인정보일 수도 있고 개인정보를 기반으로 한 기업정보가 포함될 수도 있다. 사이버배상책임보험의 대상이 될 수 있는 정보에는 개인정보를 중심으로 한 기업정보를 포함한 것으로 판단된다. 그러므로 자연인, 법인, 사자, 부재자 등의 개인정보도 포함되는 총체적 개인정보를 의미하며 인적정보 일체를 말한다고 본다.

보호대상이 되는 정보와 관련한 관련법규에는 개인정보보호법[2], 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정보통신망법)[3], 신용정보의 이용 및 보호에 관한 법률(이하 신용정보법)[4] 및 전자금융거래법 등이 있다.[5] 이에 따라 보호대상이 되는 정보라 함은 "개인정보"란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)[6] 또는 살아 있는 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)[7]를 말한다.

이상을 종합하면 개인정보란 개인의 정신, 신체, 재산, 사회적 지위, 신분 등에 관한 사실·판

2) 2011년 9월 30일 법 제10465호 제정 후 최근 2014년 3월 24일 개정으로 2016년 1월 1일 시행이 예정되어 있다.

3) 1986년 전신법인 '전산망 보급 확장과 이용촉진에 관한 법률으로 제정된 후 법명을 바꾸어 오늘에 이른다.

4) 1995년 1월 5일 법률 제4866호 제정 후 최근 2014년 11월 19일에 개정된 바 있다. 이 법에 따른 보호대상 정보는 동법 제2조 1호 및 2호에 따라 신용정보 및 개인신용정보를 의미하는데 신용정보 중 개인의 신용도와 신용거래능력 등을 판단할 때 필요한 정보를 말한다.

5) 법의 적용순서를 보면 개인정보 보호법은 일반법으로서 전체를 포괄하므로 특별법 중 전자금융거래법, 신용정보법이 우선 적용되고, 관련사항이 해당 적용대상이 아닌 경우 정보통신망법 등의 특별법이 우선 적용된다. 이 특별법에 규정이 미비하거나 다시금 해당법위가 아닌 경우 개인정보보호법이 적용된다.

6) 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조 6호.

7) 개인정보보호법 제2조 1호.

단·평가를 나타내는 개인에 관한 정보를 말한다. 뿐만 아니라 개인정보에 포함되어 있는 성명, 주민번호 등의 사항에 의하여 개인을 식별할 수 있는 정보까지도 개인정보라고 본다[8]. 헌법재판소는 개인정보에 대하여 "개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격 주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보라고 할 수 있고, 반드시 개인의 내밀한 영역이나 사사(私事)의 영역에 속하는 정보에 국한하지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함한다."라고 판시한바[9] 있다.

〈개인정보보호위원회의 개인정보 분류표〉

유형 구분	개인정보 항목
일반정보	이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 생년월일, 출생지, 본적지, 성별, 국적
가족정보	가족구성원 이름, 출생지, 생년월일, 주민등록번호, 직업, 전화번호
교육 및 훈련정보	학교출석사항, 최종학력, 학교성적, 기술자격증 및 전문 면허증, 이수한 훈련 프로그램, 동아리 활동, 상벌사항
병역정보	군번 및 계급, 제대유형, 주특기, 근무부대
부동산정보	소유주택, 토지, 자동차, 기타 소유차량, 상 및 건물 등
소득정보	현재 봉급액, 봉급경력, 보너스 및 수수료, 기타소득의 원천, 이자소득, 사업소득
기타 수익정보	보험(건강, 생명 등) 가입현황, 외사의 판공비, 투자프로그램, 퇴직프로그램, 휴가·병가
신용정보	대부잔액 및 지불상황, 저당, 신용카드, 지불연기 및 미납의 수, 임금 압류 통보에 대한 기록
고용정보	현재의 고용주, 회사주소, 상급자의 이름, 직무수행평가기록, 훈련기록, 출석기록, 상벌기록, 성격테스트결과, 직무태도
법적정보	전과기록, 자동차교통 위반기록, 파산 및 담보기록, 구속기록, 이혼기록, 납세기록
의료정보	가족병력기록, 과거의 의료기록, 정신질환기록, 신체장애, 혈액형, IQ, 약물테스트 등 각종 체테스트 정보
조직정보	노조가입, 종교단체가입, 정당가입, 클럽회원
통신정보	전자우편(e-mail), 전화통화내용, 로그파일, 쿠키(cookies)
위치정보	GPS나 휴대폰에 의한 개인의 위치정보
신체정보	지문, 홍체, DNA, 신장, 가슴둘레 등
습관 및 취미정보	흡연, 음주량, 선호하는 스포츠 및 오락, 여가활동, 비디오 대여기록, 도박성향

〈출처: 개인정보보호위원회[10]〉

〈관련법상 개인정보의 정의〉

구분	내용
개인정보보호법	(제2조 1) "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하

8) 다만 이 경우 개인정보 이외의 행태정보를 수집, 가공, 양도하는 경우는 정보통신망 이용촉진 및 정보보호 등에 관한 법률에 따른 정보에는 해당하지 않는다.

9) 헌법재판소 2005.5.26.선고 99헌마513 결정.

10) http://www.pipc.go.kr/

구분	내용
	여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.
정보통신망 이용촉진 및 정보보호 등에 관한 법률	(제2조 6) "개인정보"란 생존하는 개인에 관한 정보로서 성명 · 주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호 · 문자 · 음성 · 음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.
신용정보의 이용 및 보호에 관한 법률	(제2조 1) "신용정보"란 금융거래 등 상거래에 있어서 거래 상대방의 신용을 판단할 때 필요한 다음 각 목의 정보로서 대통령령으로 정하는 정보를 말한다. 가. 특정 신용정보주체를 식별할 수 있는 정보 나. 신용정보주체의 거래내용을 판단할 수 있는 정보 다. 신용정보주체의 신용도를 판단할 수 있는 정보 라. 신용정보주체의 신용거래능력을 판단할 수 있는 정보 마. 그 밖에 가목부터 라목까지와 유사한 정보
위치정보의 보호 및 이용 등에 관한 법률	(제2조 2) "개인위치정보"라 함은 특정 개인의 위치정보(위치정보만으로는 특정 개인의 위치를 알 수 없는 경우에도 다른 정보와 용이하게 결합하여 특정 개인의 위치를 알 수 있는 것을 포함한다)를 말한다.

〈출처: 국가법령정보센터〉

정보통신망을 통하여 정보가 유출되는 과정에서의 "침해사고"란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말하고(정보통신망법 제2조 7호), 전자금융거래상의 "전자적 침해행위"란 해킹, 컴퓨터 바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 전자금융기반시설을 공격하는 행위를 말한다(전자금융거래법 제2조 22호).

정보유출을 방지하는 보안기술에는 암호 알고리즘을 사용한 인증, 방화벽, 바이러스 방지 시스템, 비밀번호 관리가 핵심적인데 이에 덧붙여 이를 실제로 관리하는 보안정보책임자(Admin)의 인적관리가 매우 중요한 핵심적인 요소이다. 이러한 것의 구비여부가 정보유출과 관련한 사업자의 책임성을 판단하는 기준이 될 수 있다.

Ⅲ 정보유출과 배상책임의 문제

1. 개요

피보험자의 사이버상에서의 행위로 인하여 정보유출이 됨으로써 피보험자가 제3자에게 손해를 일으켜 배상책임에 근거하여 부담하여 손해배상으로 생기는 피보험자의 재산상의 손실을 전보하는 보험이 곧 정보유출배상보험일 것이다. 정보가 유출되는 이유는 다양하겠지만 주로 해킹이나 DOS공격 등에 의한 경우도 있고 산업스파이에 의한 정보에의 접근과 침해가 있을 수 있다. 어떠

한 형식으로든지 이 정보 등을 관리하고 관련 정보에 근간하여 기업을 운영하는 자는 정보유출로 인한 정보제공자에의 손해를 배상할 책임이 있다. 그런데 이 책임을 기업의 개별책임으로 수인하기에는 기업운영이나 기업지속가능성 측면에서 큰 부담이 되므로 이를 사회책임의 전환하여 위험을 분산하는 방식으로 보험제도를 이용하고자 하는 것이 곧 정보유출책임보험의 제도적 필요성일 것이다.

2. 해외사례

1) 미국

미국의 경우는 사이버책임보험(Cyber Liability Insurance; CLI)을 판매하고 있다. 그 담보범위가 상당히 광범위하다. 사이버상의 행위로 인하여 제3자 또는 기업을 운용하는 피보험자에게 발생한 손해를 담보하는 것이 이 보험의 특징이다.[11]

2) 독일

① IT-책임보험

독일에서의 IT-책임보험이란 IT관련 전문가와 서비스제공자가 영업과정에서 생기는 배상책임, 즉 인적 손해, 물적 손해 및 재산적 손해에 대하여 전문적인 담보를 해야 하는 경우에 이를 전보하는 보험이다. IT 분야와 관련하여 발생하는 전형적인 위험을 인수하여 재산상의 손해를 담보범위로 한다. 즉 이 보험은 사실상 독일에서 기업이 가입하는 보편적인 영업책임보험(Betriebshaftpflichtversicherung)으로 전보하지 못하는 위험이나 영업행위와 관련한 업무로 인해 생겨난 손해를 전보하는 데 충분하지 못한 여타의 손해를 추가적으로 전보시켜주는 것이다.[12]

② Cyber 보험(Cyber Versicherung)[13]

Cyber 보험은 개인정보를 관리하는 차원에서 발생한 정보보호위반에 기인하여 발생한 제3자에 대한 손해를 전보해주는 보험으로서 책임보험의 형식으로 확장되어 제공된다. 이는 개인정보와

---

11) 이에 관한 구체적인 것은 최창희 박사님의 연구자료에 의존한다.

12) Mit unserer speziellen IT-Haftpflichtversicherung für IT-Experten und IT-Dienstleister genügen wir höchsten Ansprüchen und bieten unseren Kunden damit eine professionelle Absicherung vor Personenschäden sowie Sach- und Vermögensschäden. Wir bieten Ihnen den Nachweis hoher Deckungssummen für Vermögensschäden, die in der IT-Branche typischerweise auftreten. Leider ist dies keine Selbstverständlichkeit in der IT-Branche, da selbst eine übliche Betriebshaftpflichtversicherung die Risiken und Tätigkeiten eines IT-Experten nicht genügend abdeckt; https://www.was-ist-datenschutz.de/unternehmen/it-haftpflichtversicherung.html.

13) Der Versicherungsschutz unserer CyberEdge-Police erstreckt sich auf die Haftpflichtversicherung von Unternehmen und versichert Sie bei Schäden, die aufgrund von Datenschutzverletzungen bei der Verwaltung von personenbezogenen Daten entstehen können. Das Produkt bietet Versicherungsschutz für Ansprüche Dritter gegen den Versicherten, sowohl für die Verletzung personenbezogener Daten (Mitarbeiter- und Kundendaten), als auch für die Verletzung von Unternehmensdaten; http://www.aig.de/cyberedge_3194_435521.html.

관련한 종업원과 고객의 정보뿐만 아니라 기업정보와 관련한 정보유출 등으로 인한 손해에 대하여 피보험자(기업)에 대하여 피해당사자인 제3자가 행사하는 손해배상청구에 대하여 보험상의 보호를 하는 것이다.

이 책임보험에 따른 보상범위는 기본형과 계약 내용의 선택에 따른 부가형이 있다. [14] 기본형은 일명 데이터책임(Data Haftpflicht)을 담보하는 것으로 개인정보, 기업정보, 아웃소싱계약 및 네트워크안정망에 관한 책임문제를 담보한다. 선택형I은 DOS공격이나 보안위반에 따른 보험계약자의 네트워크차단, 또는 네트워크상 심각한 장애의 결과 생겨난 손해로서 일종의 영업중단으로 인한 손해를 전보하고, 선택형 II는 일종의 복합네트워크책임(Multimedia-Haftpflicht)으로서 전자적인 내용을 통한 지적재산의 침해 또는 인격권의 침해의 경우 제3자의 부당한 배상청구의 방어 또는 정당한 손해배상에 대한 이행에 대한 것이다. 그 외 기타 재판상 조사비용 및 안전침해에 대한 방어비용도 부보된다.[15]

독일의 경우 이 사이버책임보험의 가입비율은 2014년을 기준으로 3.6%에 불과한 실정이고, 현재 이 보험에 가입을 준비하는 회사가 7.9%, 장래에 고려해볼 것이라고 답변한 회사는 24.2%이며, 기타 64.3%는 무관심을 나타냈다.[16][17] 현재로서는 이 보험의 가입에 대한 필요성을 체감하지 못한다는 의미로 읽혀진다.

일반적인 기업이 이 보험에 가입을 하기 위해서는 보험료가 약 100.000 ~200.000유로 정도로 고액으로 알려진다. 독일의 경우 이 보험에 대하여 보상범위와 보험사고의 경우 보험자의 급부를 정확하게 산정하는 것이 어렵다는 것과 중소기업에게는 지나치게 고액의 보험료로 인한 부담으로 현재로서는 기업에 설득력을 얻지는 못하고 있다. 그러나 헤커의 공격으로 희생자가 되고 과실로 정보(데이터)를 분실할 개연성이 건물에 화재가 발생하여 소실된 개연성보다 더 높다고 판단하고 있기는 하다. 그러나 이 경우 화재보험에 가입하며 피보험목적물이나 건물에 대하여 그 보험가액을 판단하기 비교적 쉽기 때문에 기업측면에서는 화재보험에의 계약체결의 요인을 더 가진다는 것이다. 사이버공격을 통하여 얼마만큼의 손해액을 산정할 수 있을 지에 대하여 기업 스스로가 명백하게 인지할 수 없기 때문에 근본적으로 이 보험에 대하여 회의적이라고 한다.[18]

---

14) Deckungsumfang
- Daten-Haftpflicht – versichert personenbezogene Daten, Unternehmensdaten, Outsourcingverträge und Netzwerksicherheit
- Optional: Netzwerk-/Betriebsunterbrechung – versichert sind entgangene Gewinne infolge einer maßgeblichen Unterbrechung des Netzwerkes des Versicherungsnehmers nach einer DOS-Attacke oder einer Sicherheitsverletzung
- Optional: Multimedia-Haftpflicht – versichert sind die Befriedigung berechtigter und die Abwehr unberechtigter Schadenersatzansprüche Dritter wegen der Verletzung geistigen Eigentums, Persönlichkeitsrechtsverletzungen oder anderer Sorgfaltspflichtverletzungen durch elektronische Inhalte
- Erstattung der Kosten für forensische Untersuchung und Abwehrkosten wegen angedrohter Sicherheitsbeeinträchtigungen

15) 기타

16) Quelle: Corporate Trust 2014; http://www.corporate-trust.de/pdf/CT-Studie-2014_DE.pdf.

17) 동일한 내용으로 오스트리아기업에 조사한 바로는 각각 3.4%, 5.1%, 22%, 69.5%에 달한다.

사이버책임보험의 장래 필요성에 대한 설문에서 독일의 경우는 매우 중요함(3.3%), 중요함(12.3%), 중요하지 아니함(10.1%) 그리고 선택적임(74.3%)으로 나왔고 오스트리아의 경우는 각각 5.1%, 14.4%, 8.5%, 72% 가 나왔다.[19]

③ 신용보증보험

기업에 고용된 종업원이 불법행위 또는 범죄행위 등으로 제3자에게 손해를 입힌 경우 이를 전보해 주는 보험이 신용보증보험이다. 즉 기업의 종업원이나 기타 기업에서 신뢰하는 인물이나 관재인에 의하여 일으켜진 불법행위로부터 생긴 재산상손해를 전보해주는 보험으로서 주로 상업신용보험이라고 한다. 이러한 신용보증보험은 기업의 IT를 관리하는 과정에서 기업의 종업원이 제3자에게 일으킨 손해에 대하여도 배상책임을 부담한다. 이때 기업의 IT를 관리하는 과정에서 제3자의 정보를 유출한 경우가 해당사례가 될 것이다. 물론 불법행위의 유형은 매우 광범위한데 그 유형으로는 사기, 횡령, 절도, 배임, 물건손괴, 태업 또는 독일민법 제823조(우리 민법 제750조)에 따라 손해배상의무가 발생하는 기타 고의에 의한 불법행위가 여기에 속한다. 일반적으로 기업 자체에 생겨난 손해뿐만 아니라 제3자에게 가해진 손해를 포함하여 보상하여 준다. 상업보증보험은 일종의 신용보험의 일종으로 다룬다.

Ⅳ 문제점

1. 가입기준

정보유출배상책임보험의 대상이 사이버상 행위로 인한 정보유출인데 과연 사이버상의 행위에 포함되는 것이 무엇인지를 확인할 필요가 있다. 최근에 발생한 농협에서의 예금인출 사건이 일반적인 사이버상의 행위에 구체적으로 해당되는지의 여부를 아직 확인할 길이 없다. 예금자의 경우는 인터넷뱅킹이나 텔레뱅킹을 이용한 바가 없는 경우라고 하므로 이에 대한 사실관계에 대한 확정이 필요한 부분이다.

개인정보가 유출된 사건 중 손해배상청구가 있었던 사례는 아래의 표와 같다. 사실상 정보를 관리하는 회사가 소비자의 정보가 유출되어 해당 소비자에게 손해가 발생하여 이를 기준으로 손

18) Die Wahrscheinlichkeit, Opfer eines Hackerangriffes1 zu werden oder durch Fahrlassigkeit Daten zu verlieren, ist zwar wesentlich hoher als zum Beispiel ein Brand eines Fabrikgebaudes –. der Wert einer Feuerversicherung lasst sich jedoch relativ leicht am Wert der zu versichernden Gebaude und Gegenstande beurteilen; Industriesponage 2014, Corporate & Trust, S. 63.

19) Industriesponage 2014, a.a.O., S. 65.

해배상청구를 하여도 현재로서는 기업보호 차원상 소비자의 손을 들어주는 편은 아니고, 설령 손을 들어준다 하여도 손해로 인한 배상금액이 그다지 의미있는 수준은 아닌 편이었다. 그러나 최근 빈발하는 정보유출사고에 대한 인식이 제고되는 측면도 있고 그 피해규모도 커지는 측면에서 정보를 관리 또는 이용하는 회사에게 손해에 대한 배상을 묻고자 하는 분위기로 전환되고 있는 추세이다. 다만 해당 기업이 정보처리나 관리에 대하여 관련 법규에서 요구하는 기술적 안전조치를 다하는 등의 주의의무를 기울인 경우 그 책임을 전부 면책해 주고는 있지만, 최근 그 면책 조건을 보다 엄격하게 적용하여 정보유출 그 자체만으로 해당 기업이 일정 수준의 책임을 부담하여야 한다는 엄격책임의 원리적용의 취지의 의견도 있어 관련법규의 정비가 차후에 필요할 수도 있을 것이고 정보처리나 관리와 관련한 위험을 보험의 대상으로 하는 보험의 필요성이 끊임없이 요구될 것이다.

〈유출 경위별 주요 손해배상청구 사례〉

유출 경위	회사(피고)	사건번호	결과	진행
내부과실	GS칼텍스	대법원2011다59834	원고패	확정
	엔씨소프트	대법원2007다17888	원고승 (각 10만원)	확정
	국민은행	서울고법2007나33059, 33066	원고승 (각 20/10만원)	확정
	LG전자	대법원2008다96826	원고승 (각 30만원)	확정
외부침입	옥션	서울고등법원2010나31510	원고패	상고심
	SK컴즈	서울중앙지법2011가합90267	원고패	항소심
		서울서부지법2011가합11733	원고승 (각 20만원)	항소심
기타	SK브로드밴드	서울고등법원2011나67493	원고승 (각20만원)	확정

(2014.8월말 기준)

문제는 위와 같은 정보유출로 인한 위험을 담보해주는 보험의 가입기준을 어떻게 설정하는 지의 문제이다. 현실적으로 그간 정보유출로 인하여 기업지속의 위기를 느낀 기업은 보험가입에의 필요성이 있을 것이라고 판단할 것이지만, 정보관리를 철저히 하기 위하여 각종 인프라를 구축하고 위험에 대비하는 등의 역량을 강화하고 있는 기업의 입장에서는 이러한 보험에 대한 수요나 긴급성을 그다지 인식하지 않고 있을 것이다. 결국 리스크 수준이 상대적으로 높은 잠재 보험수요자가 해당 리스크를 관리하기 위하여 보험상품에 가입할 경향(propensity)이 높거나 더 높은 담보범위(insuracnce coverage) 또는 보장률을 설정하려는 경향이 높기 때문에 이러한 현상을 보험자가 감안하지 않을 수 없는 것이다. 결국 이는 보험에 대한 역선택(Adverse Selection)의 문제가 되는 것이다. 이러한 상황이라고 하면 정보유출관련 배상책임보험을 상품으로 시장에 출

시하여 보험을 인수할 보험자에게는 보험사고의 위험도가 높은 기업과 보험계약을 체결해야 하는 또 다른 위험을 감수하여야 하는 데 과연 기업차원에서 위험을 대비하는 기업이 아닌 사고의 개연성이 높은 기업과 흔쾌히 보험계약을 체결할 것인지는 의문이다. 이는 결국 정보유출배상책임보험의 시장의 크기의 문제이며 IT와 유관한 가입대상 기업의 보험에 대한 계약체결 요인 등에 관한 문제이다.

이를 해결하기 위해서는 배상책임보험을 의무보험화 해야 하는데 정보유출 등의 사회적인 안전망을 넘는 사건에 대하여 수지상등의 원칙을 기반으로 한 영리보험사가 이러한 사회적 위험을 과연 전적으로 인수할 것인지 도 판단해보아야 할 부분이다. 결국 이러한 상황에서 의무보험으로 시행하려면 보험사에게 그에 대한 인센티브가 있어야 하거나 제도적인 장치를 통하여 보상한도를 기술적으로 정하여야 할 것이다.

2. 보상범위

사이버상에서의 정보유출로 인한 보험자의 보상범위도 또한 그 범위를 확정하는 것이 쉬운 문제가 아니다. 보상범위는 보험자가 인수한 보상의 범위가 중요한 기준이다. 보험자가 주계약을 통해서 정한 보상범위와 추가적으로 부보를 약정한 특약의 범위는 무엇인지에 따라 다르다. 이러한 보상범위를 확정하기 위하여는 무엇을 손해사고로 하고 그에 따라 어디까지를 보험사고로 하는 지를 확정하여야 한다.

-① 사이버상에서 생겨난 손해사고라고 한다면 손해를 일으킨 원인이나 방법은 불문하는지,
-② 보호범위를 개인정보유출에 한정한다 하더라도 그 손해사고를 어디까지로 한정할 것인지
-③ 그렇다고 한다면 피해액의 산출은 어떻게 해야 하는 것이지가 문제된다.

여기에서 ①과 ②와 관련해서 손해사고의 원인이나 방법과 연동하여 그 범위는 앞선 정보관련 법규범에서 한정하고 있는 원인 및 범위로 한정하는 것이 제안될 수 있다. 즉 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생한 사태, 즉 침해사고로 한정하면 될 것이다. 그러나 최근에 그 범위를 넘어서는 신종의 방법들이 양산되고 있으므로 본질적인 해결책에 해당하는 범위 설정은 되지 못한다.

특히 이러한 류의 책임보험은 보험계약 당시에 보험가액을 정할 수 없는 미평가보험에 해당하므로 보험금액의 범위를 계약상 우선 정하여야 한다. 또한 사이버를 영업무대로 하는 사업자의 범위를 확정하여야 하고 사업자별로 주의의무 정도를 일률적으로 정할 수 없어서 이를 구체화할 수 있는 기준설정이 중요한 문제이다. 사업자가 보안시스템을 유지하고 관리하는 정도가 다르므로 이에 대한 위험계산을 위한 기술적인 것이 확정되어야 한다.

위와 같은 손해사고를 기준으로 발생한 보험사고를 확정하여야 하여야 한다. 보험사고가 확정되면 그 다음은 보험에서 보상하게 될 손해산정 및 확정이 문제이다. 이는 ③ 피해액의 산출에 대한 문제인데 과연 어느 범위까지를 피해액으로 확정할 것인가가 의문이다. 재물보험, 예컨대 화재보험에서는 화재로 인한 유형의 자산을 기준으로 그 가액을 정하는 것이 일반화되어 교환가치로 그것을 정할 수 있는 것이지만 과연 정보유출피해에서의 피해액에서의 인과관계문제는 무형자산과의 관련성이 있으므로 매우 추상적인 문제이다.[20] 궁극적으로 사이버상에서의 정보유출로 인한 손해산정을 위한 전제조건은 이를 산정한 손해사정인의 전문성이 확보되어야 한다. 또 일반적으로 손해발생 당시라고 판단되는 때에 외부로 출현되지 아니한 추가손해의 문제는 어느 범위에서 수인을 할 것인지도 문제이다. 이는 후술할 보상한도와 연동하는 부분일 것이다.

3. 보상한도

정보유출배상책임보험의 손해사고를 확정하고 이에 따라 보험사고를 명확하게 설정하는 것이 다른 보험에 비하여 난해한 측면이 있고 보험가액을 처음부터 정하는 게 기술적으로 어렵기 때문에 이 보험을 활성화하기 위해서는 보험자가 인수할 보상한도를 보험기술적으로 정하는 것이 좋을 것 같다. 보상한도는 당연 유한보상의 방법을 취하겠지만 이를 건별로 할 것인지 총액을 기본으로 할 것인지는 정책적인 측면이 있다고 본다. 직접적인 연관관계는 없으나 최근 자동차보험이 손해율을 낮추고 가입자의 도덕적 해이현상을 억제하기 위한 방법으로 보험요율을 정함에 있어서 자동차보험 건수제로 전환한 바 있다. 금액제로 할 것이지 건수제로 할 것인지는 제도적인 선택의 문제이다.

독일의 자동차보험의 경우는 우리와는 다른 일원적 책임보험체계인데 여기에서 보상한도는 건별과 총액제[21]를 연동하여 하는데 이러한 것이 보험자의 유한책임을 근거로 한 보험정책에 해당하는 것이다. 그러므로 정보유출배상책임보험에서 이를 건별로 할 것인지 총액제로 할 것인지의 문제는 보험을 인수하는 보험자가 결정할 문제이다. 다만 정보유출배상책임보험은 기업보험의 성질을 가지므로 보험자와 보험계약자 사이의 유한배상책임의 범위에서 상호 계약적 합의를 할 수도 있다.

---

20) 경우에 따라서는 의료정보 등의 민감정보 등이 포함될 수도 있어 손해를 산정하는 것이 곤란할 것이다.

21) 현재 전자금융거래법에 근거하여 금융거래업자가 가입하여야 하는 보험의 경우는 총액제로 운용되고 있다.

Ⅴ 제언

정보관련 기술이 발달하면 할수록 역설적으로 보호해야할 정보의 양도 많아진다. 특히 정보가 산업상 거래적인 요소가 되는 경우라면 그 보호의 필요성은 더욱더 대두된다. 그런데 최근 그러한 보호필요성에도 불구하고 잦은 정보유출로 인하여 산업에 막대한 피해가 드러나고 있으며 사회적인 불신도 만만치 않다. 기업이 안심하고 기업활동을 할 수 있도록 제도적으로 부조할 수 있는 것 중의 하나가 보험제도이다. 특히 기업을 영위하는 과정에서 생기는 제3자에 대한 손해배상과 관련한 책임문제에서 비교적 자유롭기 위해서는 보험제도를 잘 이용하여야 할 것으로 보인다. 그중 영업책임과 관련하여 정보유출로 인한 제3자의 피해를 전보하는 정보유출배상책임보험의 도입은 긴급하다. 다만 보험기술적인 보완이 필요하고 전제조건적인 인프라가 동시에 구축되어야 한다. 더욱이 이 보험을 운용함에 있어서 관련기업의 가입 의무화가 바람직한지는 원활한 기업활동을 위해서 필요한 부분인 것으로 판단된다. 다만 사회적 안정망을 제도적으로 확보하는 측면에서는 의무화가 가지는 의미가 크지만 그럼에도 불구하고 가입의무화에 대한 저항을 있을 수밖에 없다. 결국은 가입이 강제되는 것에 대한 제도적인 유인책은 분명하여야 한다. 경제학의 주요원칙 중의 하나인 '인간은 유인체계에 반응한다'는 것에 있고, 이러한 경제학적 원칙은 보험분야에도 적용되기 때문이다.

토론문

정보유출배상책임보험의 가입 의무화에 관한 연구

신 영 수 (법무법인(유) 율촌 변호사)

토론문2

정보유출배상책임보험의 가입 의무화에 관한 연구

신영수(법무법인(유) 율촌 변호사)

1. 서론

개인정보 보호와 관련해서는 사전적으로 개인정보가 불법적으로 유출되지 않도록 하는 것이 매우 중요하다고 할 것이다. 또한, 개인정보가 유출되었을 경우 그로 인한 개인정보주체의 피해를 보상하는 것 또한 개인정보 보호제도의 중요한 축이 되어야 할 것이다. 이러한 점에서, 최근 활발히 논의되고 있는 개인정보 유출사고 관련 집단소송제도, 징벌적 손해배상제도 및 법정손해배상책임제도 등은 매우 시의 적절하다고 본다.

그러나, 이와 같은 개인정보 유출로 인한 손해배상제도가 보완된다고 하더라도, 개인정보보호법상의 "개인정보처리자", 신용정보의 이용 및 보호에 관한 법률(이하 "신용정보법")상의 "신용정보회사 등", 그리고 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 "정보통신망법") 상의 "정보통신서비스제공자 등"은 개인정보 유출에 대하여 손해배상책임을 부담하는 자에게 경제적 배상능력, 즉 책임재산이 충분하지 않는 경우에는 실질적으로 피해자들이 충분한 구제를 받을 수 없게 되는 문제가 발생하게 된다. 그런데, 정보유출배상책임보험의 가입을 의무화하는 것은 그와 같은 문제를 해결할 수 있는 효과적인 수단이라는 점에서, 정보유출배상책임보험의 의무화를 주장하는 발표자의 견해에 찬성한다.

다만, 다음에서는 정보유출배상책임보험의 가입을 의무화하는 구체적인 방안과 관련하여 고려할 필요가 있다고 생각되는 몇 가지 사항들에 대하여 간략히 살피도록 하겠다.

2. 헌법상 기본권 및 과잉금지의 원칙

헌법상의 기본권을 제한함에 있어서는 이른바 '과잉금지의 원칙'이 적용되는데, 이와 관련하여 우리 헌법재판소는 국민의 기본권을 제한하려는 경우에는, (i) 국민의 기본권을 제한하려는 입법의 목적이 헌법 및 법률의 체제상 그 정당성이 인정되어야 하고(목적의 정당성), (ii) 그 목적의 달성을 위하여 그 방법이 효과적이고 적절하여야 하며(방법의 적절성), (iii) 입법권자가 선택한

기본권 제한의 조치가 입법목적달성을 위하여 설사 적절하다 할지라도 보다 완화된 형태나 방법을 모색함으로써 기본권의 제한은 필요한 최소한도에 그치도록 하여야 하며(피해의 최소성), (iv) 그 입법에 의하여 보호하려는 공익과 침해되는 사익을 비교형량할 때 보호되는 공익이 더 커야 한다(법익의 균형성)고 판시하고 있다(헌법재판소 1990. 9. 3.자 89헌가95 결정 등 참조).

그런데, 정보유출배상책임보험 가입의 의무화는 (i) 개인정보 침해사고가 발생할 경우 그 피해가 심각하므로 그에 대하여 선제적으로 대응할 필요가 있다는 점, 개인정보처리자 등 기업의 입장에서도 개인정보유출사고와 관련된 집단소송제도, 징벌적 손해배상제도 및 법정손해배상책임제도 등에 대비할 필요가 있다는 점, 개인정보 침해로 인한 피해보상을 위해서는 개인정보처리자 등의 경제적 배상능력의 확보가 필수적이라는 점 등에서 "목적의 정당성"이 인정되고, (ii) 개인정보처리자 등으로 하여금 의무적으로 정보유출배상책임보험에 가입하도록 함으로써 피해자들이 실질적으로 효율적인 보상받을 수 있게 한다는 점에서는 "방법의 적절성"도 충족되며, (iii) 개인정보 보호법, 신용정보법 및 정보통신망법 등에 대한 개정법률안들에서 가입의무자의 범위, 보험가입 및 자산예탁의 기준 등을 합리적으로 정하거나 시행령에 위임할 경우에는 "피해의 최소성"도 인정되고, (iv) 개인정보처리자 등의 배상책임보험의 가입강제는 정보주체의 피해를 신속하고 효과적으로 구제하고, 개인정보 처리의 신뢰와 안전성을 확보하여 정보통신산업의 선진화를 제고함으로써 공공복리를 증진하는 중요한 역할을 한다는 공익과 보험가입 강제에 따라 침해되는 영업의 자유 내지 재산권에 대한 제한이라는 사익을 비교할 때, 전자가 훨씬 크다고 할 것이므로 "법익의 균형성"도 충족되며, 따라서 이와 같은 배상책임보험의 의무화는 과잉금지의 원칙에 위반되지 않는 것으로 보인다.

이와 관련하여, 각 개정법률에는 정보유출배상책임보험의 가입의무자를 "개인정보처리자", "신용정보회사등[1]" 및 "정보통신서비스제공자등"으로 되어 규정되어 있어 모든 "개인정보처리자", "신용정보회사등" 및 "정보통신서비스제공자등"에게 정보유출배상책임보험의 가입이 강제되고 있으나, 이를 "대통령령이 정하는 개인정보처리자", "대통령령이 정하는 신용정보회사등" 및 "대통령령이 정하는 정보통신서비스제공자등"으로 수정함으로써 의무가입대상자를 합리적인 범위로 한정할 필요가 있다고 생각한다.

3. 의무보험가입의 강제수단 확보 필요

우리 나라는 현재 약 수십 개의 의무보험제도가 도입되어 시행되고 있으나, 실제로 의무보험에 가입한 비율은 극히 저조하다고 한다. 정보유출배상책임보험의 경우에도 이를 의무화한다도 하더라도 이를 강제할 수 있는 수단이 없으면, 실제로 위 의무보험에 가입하는 비율을 극히 저조할 수밖에 없을 것으로 예상된다. 따라서, 의무보험에 가입하지 않은 경우에는 과태료, 영업정지 등 행

1) 다만, 정무위원회안에는 "대통령령으로 정하는 신용정보회사등"으로 변경되어 있다.

정제재나 벌금 등 형사제재 등을 부과하는 방안을 고려할 필요가 있다. 의무보험가입 강제의 효율성 측면에서는 벌금 등 형사제재, 영업정지 등 행정제재 및 과태료의 순서로 효율적일 것이나, 헌법상의 과잉금지의 원칙과의 관계에서는 "과태료"의 경우에는 별 문제가 없을 것으로 생각되나 "영업정지 등 행정제재나 벌금 등 형사제재"는 위헌의 가능성이 좀 더 높아질 것으로 보인다. 따라서, 정보유출배상책임보험에 가입하지 않는 경우에는 "과태료" 정도의 제재를 부과하는 것이 적절한 것으로 생각된다. 이 점에서, 신용정보법 개정안(정무위원회안)에서 과태료 제재가 제외된 것은 문제가 있다고 본다.

4. 신용정보법 개정안(정무위원회안)에서의 "준비금 적립"에 대하여

신용정보법 개정안(정무위원회안)에서는 "보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 취하여야 한다"라고 규정하고 있습니다. 그러나, 보험이나 자산의 예탁과 달리, 기업이 단순히 회계상으로 "준비금"을 적립하도록 할 경우에는 기업은 해당 준비금을 금융기관에의 예치 등의 방법으로 확보하지 아니하고 단순히 회계장부상으로만 계상할 위험이 있다. 그렇게 되면, 피해가 발행했을 때에 해당 준비금에 상당하는 금전(또는 그에 상응하는 유동성 자산)이 존재하지 않을 수 있어, 피해자가 현실적으로 손해보상을 받지 못할 위험이 있습니다. 따라서, 신용정보법 개정안(정무위원회안)에 포함된 "보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 취하여야 한다"는 부분을, 당초 원안과 비슷하게 "보험 또는 공제에 가입하거나 『금융위원회의 설치 등에 관한 법률』 제38조 제1호 내지 제8호의 기관에 자산을 예탁하여야 한다"와 같이 수정하는 것이 타당하다고 생각한다."

5. 면책사유 관련

개인정보처리자등의 "고의에 의한 사고"를 보상 범위에서 제외할 것인지와 관련해서는, (i) 보험계약은 최대선의(utmost good faith)에 기초한 계약으로, 계약당사자에게 일반 계약에서보다 더 많은 보호의무를 요구하며, 이와 같은 선의성은 보험계약의 해석원칙으로도 기능한다는 점, (ii) 상법은 위와 같은 보험계약의 선의성을 유지하기 위하여 제659조에서 "보험사고가 보험계약자 또는 피보험자나 보험수익자의 고의 또는 중대한 과실로 인하여 생긴 때에는 보험자는 보험금액을 지급할 책임이 없다"고 규정하고 있는 점, (iii) 배상책임보험의 보상 범위를 고의사고까지 확장할 경우 이는 곧바로 보험료 인상으로 이어져 기업들의 경제적 부담을 가중시키게 될 뿐만 아니라, 기업들이 사고를 방지하기 위한 노력을 소홀이 할 인센티브 또는 도덕적 해이(moral hazard)을 유발할 우려가 있다는 점에서, 발표자의 견해와 같이, 개인정보처리자등의 "고의에 의한 사고"는 배상책임보험의 보상 범위에서 제외하는 것이 타당하다고 생각한다.

또한, 현재 판매되고 있는 전자금융거래 배상책임보험에서는 "피보험자가 고의 또는 중과실로

법령을 위반한 경우"에도 면책사유로 규정하고 있는바, 위에 기술한 것과 같은 이유에서 "피보험자가 고의 또는 중과실로 법령을 위반한 경우"에도 면책사유로 규정함으로써 개인정보처리자 등으로 하여금 정보유출을 방지하기 위하여 적절한 조치를 취하도록 할 필요가 있다고 본다.

6. 부가서비스 관련

AIG나 Allianz 등 외국보험사들이 판매하는 사이버배상책임보험(Cyber Liability Insurance, CLI)의 경우에는 보험회사가 보험계약자에게 "사이버위험 평가 서비스, 사이버 위험 관련 교육서비스, 사이버 위험 관리 컨설팅 및 사고 발생시 실시간 대응서비스" 등과 같은 부가서비스를 제공하고 있다. 우리 나라 보험회사들의 경우에는 정보유출배상책임보험상품에 그와 같은 부가서비스가 포함되도록 함으로써, 개인정보 유출사고를 예상하고, 보험사고의 발생율을 낮추며, 또한 보험사고 발생시 신속하고 효율적으로 대응할 수 있도록 할 필요가 있다. 다만, 이와 같은 부가서비스의 제공과 관련해서는 보험업법 제98조 규정의 "특별이익 제공 금지"가 문제될 수 있는데, 이는 자동차보험에서의 부가서비스와 마찬가지로 금융감독당국이 적극적으로 허용할 필요가 있다고 생각한다.

7. 보험의 중복 문제

개인정보법, 신용정보법 및 정보통신망법 등에서 각각 개별적으로 정보유출배상책임보험의 가입을 강제할 경우에는 하나의 사업자가 동일하거나 유사한 하나의 정보유출위험에 대하여 2개 또는 3개의 정보유출책임보험에 의무적으로 가입해야 하는 문제가 발생할 수 있다. 이와 같은 문제를 해소하기 위해서는, 신용정보법에 따른 의무보험의 담보내용에 "신용정보법상의 손해배상책임뿐만 아니라 개인정보법 및 정보통신망법상의 손해배상책임"까지 포함하도록 하고, 대신에 신용정보법에 따른 의무보험에 가입하게 되면 개인정보법 및 정보통신망법에 따른 책임보험에는 가입하지 않아도 되도록 입법적으로 규정할 필요가 있다. 마찬가지로, 정보통신망법에 따른 의무보험의 담보내용에 "정보통신망법상의 손해배상책임뿐만 아니라 개인정보법 및 신용정보법상의 손해배상책임"까지 포함하도록 하고, 대신에 정보통신망법에 따른 의무보험에 가입하게 되면 개인정보법 및 신용정보법에 따른 책임보험에는 가입하지 않아도 되도록 입법적으로 규정할 필요가 있다.

토론문

정보유출에 따른 배상책임보험 도입과 관련하여

조 남 희 (금융소비자원 대표)

토론문3

정보유출에 따른 배상책임보험 도입과 관련하여

조남희(금융소비자원 대표)

최근 대규모 정보유출을 계기로 개인정보의 문제는 금융사만의 문제가 아닌 국가적 문제가 되고 있다고 할 수 있다. 경제 활동자 대부분의 개별정보가 일반정보가 되었다고 해도 과언이 아니다. 정보유출 사태를 계기로 정보의 공유, 교환이나 법적제도의 개선 등이 이루어지고 있다고 하지만, 여전히 금융소비자 측면에서의 실질적인 구제수단으로서의 대책은 크게 진전되고 있지 못한 것이 현실이다. 이러한 상황에서 오늘 논의하는 정보유출에 따른 배상책임보험의 제도 도입은 금융소비자 피해에 대한 실질적인 구제 수단의 하나가 될 수 있다는 점에서 의의가 있다 하겠다.

정보유출배상책임보험의 제도의 도입이 된다면, 긍정적인 부분을 5가지로 요약해 볼 수 있을 것이다.

1. 금융소비자의 손해배상청구가 용이

기존의 방법으로는 약자인 피해자, 금융소비자가 손해배상을 받기 위해서는 상당한 제약이 있었으나 제한된 범위에서 보다 쉽고 빠르게 보상받을 수 있다는 것이다.

2. 금융사의 무조건적 책임회피 인식 변화

금융사고에서 금융사는 대부분 책임을 회피하거나 법을 내세워 피해구제에 대해 소극적이었다고 본다. 책임보험 도입을 통해 일정부분 책임부분에 대해서는 명확히 보상을 제시한 다는 점에서 과거 보다는 진전된 책임의식을 갖게 할 것으로 기대할 수 있다는 점이다.

3. 금융당국의 개입 축소와 금융사의 자율 제고

금융사고시마다 금융당국의 개입이 필연적이었고 그 상황에서 항상 금융당국의 규제와 간섭은 증가해왔다. 하지만 보험도입으로 인해 자율적 조정과 해결의 방법이 도입되어 당국의 간섭을 줄

이면서 업계의 자율성을 제고시킬 수 있을 것이다.

4. 보험사의 구상권을 강화를 통한 정보유출 관련 불법행위 단절

피해보상을 해준 보험사가 구상권을 적극적으로 행사하게 됨으로서 정보유출자나 판매자, 유통업자 등에 대한 강력한 구상권 행사는 불법 정보 관련자들의 재산의 압박이

5. 전자금융사고 확대 시행 및 사고 예방 기대

개인정보유출형 전자금융사기행위에 대하여 피해자의 정보유출 행위를 이유로 하여 금융회사의 면책 주장과 법원의 수용 등으로 인해 금융소비자 피해가 제대로 보상되지 않으나, 이에 대한 구제도 확대될 수 있을 것으로 보인다.

정보유출관련 소송의 경우만 보더라도 일부 하급심에서 소비자에게 유리한 결과도 있었지만 대부분은 피해자인 금융소비자 입장에서는 구제가 되었다고 보기 어려운 것이 현실이다. 정보유출로 인한 금융소비자 피해에 대한 다양한 사례의 검토를 통하여 합리적이고 명확한 기준이 설정되고 손해배상의 청구 등 구제방안이 미비한 현시점에서 오늘 논의되는 정보유출배상책임보험제도는 이를 보완하는 것이고, 이를 바탕으로 정보주체자인 금융사, 금융당국 등이 지금 보다 확연하게 진전된 소비자 정보보호 및 구제 제도가 도입하고 시행, 정착시키는데 노력해야 할 것이다.