기업의 개인정보 유출로 인한 경제적 피해규모 산출방법

A Quantitative Assessment Model of Private Information Breach

한창희(Chang Hee Han)*, 채승완(Seung Wan Chai)**, 유병준(Byung Joon Yoo)***, 안대환(Dae Hwan Ahn)****, 박채희(Chae Hee Park)*****

초 록

정보화의 빠른 진전과 더불어 정보화의 역기능 역시 비례하여 확산되고 있으며 그 피해는 막대한 것으로 추정되고 있다. 하지만 현재까지 개인정보 유출의 피해규모에 대한 연구와 자료가 미흡한 실정이기 때문에 이로 인한 국가적 피해규모를 계량화하는 작업에 많은 현실적 어려움이 존재하고 있다. 만약 피해액의 규모를 제대로 산출하여 보안정책 수립에 참고한다면 경제적으로나 사회적으로 미치는 사고 영향의 심각성을 정확히 파악할 수 있으며, 결과적으로 유출사고 대응에 필요한 기업 그리고 정부의 노력과 비용의 크기~에 대한 의사결정을 할 수 있기 때문에 체계적인 경제적 피해규모를 파악하는 일은 매우 필요한 과제라고 판단된다. 이에 본 연구는 일본 네트워크 보안협회 등 해외 유수 연구들의 방법론과 새로운 접근법들을 참고하여, 개인정보 유출사고의 피해실태를 파악하기 위한 정보의 수집과 이의 정량적 분석의 개념적 틀을 제시하고자 한다. 또한 비교적 데이터가 부족한 국내의 환경에서도 정책적 지표로서 의미 있는 피해액을 측정함으로써 개인정보 유출 피해를 막기 위한 다양한 정책기획의 기반자료로 활용될 수 있기를 기대한다.

ABSTRACT

Damage caused by private information breach causes serious problems and huge social losses. In order to make a better policy that prevents society from suffering from the damage, we have to know about the actual size of damage. So it is needed to develop a quantitative model of private information breach that helps catching the more accurate size of damage.

In our study, we suggest a method which calculate not only the costs of damage from firms' perspective but also those from individual and social perspectives. In this process, we refer to methods adopted by JNSA(Japan Network Security Association) and Ponemon Research Institue and modify it with considering our current situation. Also we try to make a new model by using new methods(web traffic analysis, survey, indirect comparison, etc.) and

* 한양대학교 경영학부 부교수
** 한국인터넷진흥원 아카데미팀 팀장
*** 교신저자, 서울대학교 경영전문대학원 부교수
**** 서울대학교 경영전문대학원 석사과정
***** 한양대학교 경영컨설팅학과 석사과정
2011년 10월 17일 접수, 2011년 10월 28일 심사완료 후 2011년 11월 12일 게재확정.

verify it with theories and methods from econometrics, cost accounting and theory of producer.

키워드 : 보안정책, 개인정보, 개인정보의 유출, 피해규모의 산출, 정량적 평가모델
Security Policy, Private Information, Private Information Breach, Calculating Damage, Quantitative Assessment Model

1. 서 론

1990년의 IP기반 인터넷 연결 이후 우리나라의 정보화 이용 및 환경 수준은 비약적으로 진전되었다. 기업과 개인 등의 인터넷 이·활용의 증가에 따라 특정 개인을 식별하기 위한 개인정보의 이용도 증가하여 2011년 현재 홈페이지를 통해 개인정보를 수집하고 있는 기업은 47%에 이르고 있다.

하지만, 개인정보의 이용 증가는 과금, 서비스 제공 목적 달성 등 순기능을 활성화하는 양의 효과를 가지는 반면, 제 3자에 의한 정보 시스템 침해를 통한 개인정보의 유출과 이의 부정적 용도로의 사용이나 정보 소유기업 자체에 의한 정보 소유권의 남용으로 인해 심각한 부의 효과를 발생시키고 있다.

예를 들어, 2008년 중국 해커에 의해 발생한 옥션 개인정보 유출 사건으로 약 1,800만 명의 개인 정보가 유출되었으며, 2010년에는 신세계를 비롯한 25개 사이트의 약 2,500만 명의 개인 정보가 유출되는 등 엄청난 규모의 개인정보 유출 사건이 계속해서 발생하고 있다. 이렇게 유출된 정보는 스팸, 보이스 피싱, 텔레마케팅 등에 이용되고 있으며 이로 인해 수많은 소비자들이 피해를 겪고 있는 실정이다.

현재까지 우리나라에는 개인정보 유출의 피해규모에 대한 연구와 자료가 미흡한 실정이기 때문에 국가적 피해규모를 계량화하는 작업에 많은 현실적 어려움이 존재하고 있다. 그러나 피해의 규모를 제대로 평가하면 경제적으로나 사회적으로 미치는 사고 영향의 심각성을 제대로 파악할 수 있고, 결과적으로 유출사고 대응책에 필요한 노력과 비용의 크기에 대한 의사결정을 할 수 있기 때문에 체계적인 경제적 피해규모를 파악하는 일은 반드시 필요한 과제라 판단된다.

본 연구는 이러한 맥락에서 개인정보 유출사고가 발생하는 경우 민간 기업의 실질적 손실비용과 이를 복구하기 위한 비용을 측정하는데 그치지 않고, 나아가 고객의 손실과 사회적 파급 효과 등의 경제적 피해규모를 정량적으로 산출할 수 있는 모형을 수립함으로써, 향후 유사한 상황이 발생할 시 그 피해를 정량화하여 경제적 손실을 측정하고 이를 예방하기 위한 대책 수립에 활용하는 것을 목적으로 하고 있다. 여기서 말하는 모형이란 유출 사고의 발생으로부터 시스템 복구 및 업무 정상화와 법적 보상에 이르기까지 사태의 흐름을 현실에 입각해 재현함으로써, 그 과정에서 발생할 수 있는 각종 손실을 다면적으로 파악·산출하는 구조를 말한다. 즉, 모형의 구축은 유출사고의 발생, 사고의 영향, 사고에의 대응 및 복구, 법적 보상 그리고 사회적 파급 효과 등을 분석하여 전체적인 피해를 간결하게 표현하는 것이다. 이러한 작업을 통하여 유출사고의 피해실태를 정확

하게 파악하기 위한 착안점을 찾고, 유출사고 위기관리에 필요한 정보를 체계적으로 수집할 수 있는 틀을 확보하고자 한다.

2. 선행연구 분석

2.1 국내 연구

2008년 발표된 '인터넷 침해사고에 의한 피해손실 측정'에서는 인터넷 침해사고가 발생하였을 때 민간 기업의 실질적 손실비용과 이를 복구하기 위한 비용 등 경제적 피해규모를 산출할 수 있는 모형을 수립하였다[5]. 비록 유출사고를 포함하지 않고 침해사고에 한정된 연구라는 한계가 있지만 향후 유사한 상황이 발생할 시 그 피해를 정량화하여 경제적 손실을 측정하고 이를 예방하기 위한 대책 수립에 활용할 수 있게 되었다는 점에서 의미가 있다. 또한 보안사고의 피해실태를 정확하게 파악하기 위한 착안점을 찾고, 보안사고 위기관리에 필요한 정보를 체계적으로 수집할 수 있는 틀을 확보하였다.

2.2 일본 JNSA

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

섹션 1은 정보 유출 환경에 관한 다양한 자료 조사를 토대로 유출에 따른 피해액 추정과 그 대응비용에 관한 논의를 다루고 있으며, 섹션 2는 정보 유출과 관련된 법적 보상비용을 산정하고 여기에 주가 변화를 통해 단기·중기적 피해액을 산정하는 방법을 추가적으로 논의하고 있다[27].

그러나 2010년 보고서에서는 그 타당성에 관한 의문이 제기되고 산정이 어렵다고 평가되는 직접 복구비용, 기회비용 등의 사고비용과 관련된(과거 보고서의 섹션 1에 해당) 부분을 제외하였다. 그리고 섹션 2의 적정 법정 보상액 산정에 관한 부분의 경우 판사의 판결에 따라 보상 판결액이 바뀌는 등 추정과 실제가 차이가 발생하는 문제점이 있다는 점 등을 고려해서 유출된 정보의 기본 가치액을 추정하는 원론적 형태로 모델의 방향을 수정하였다[28]. 또한 2003년도 보고서에서 잠시 시도되었던 주가를 이용한 피해액 산출 방법은 그 예측의 타당성 여부에 대한 문제점으로 현재는 사용하지 않고 있다.

2.3 미국 Ponemon

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

포네몬 연구소는 미국뿐만 아니라 영국, 독

일, 오스트레일리아, 프랑스를 조사 대상으로 삼고 있으며, 매 년 관련국가의 개인 정보 유출 보고서를 발표하고 있다. 또한 이 보고서들을 하나로 모아 비교 분석한 'Global Cost of Data Breach'라는 보고서도 함께 내놓고 있는데 이는 보안 환경과 경제 규모에 따른 국가들의 피해액을 체계적으로 비교·분석하는 자료로 활용되고 있다. 이들이 조사하는 대상은 2009년 기준으로 전 세계 18개 산업에 걸친 130여 개의 기업에 이른다.

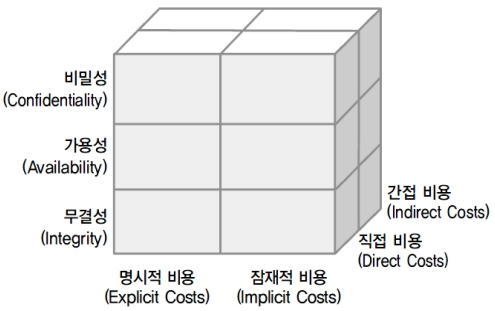
포네몬 보고서의 주요 내용은 연간 개인정보 유출 사건의 건당 소요비용과 이를 이루는 직·간접비용, 연간 총 피해비용, 산업별·단계별 피해비용, 세부 항목별 소요비용 등으로 이루어져 있다[29].

3. 개발 모델의 프레임워크

3.1 프레임워크 구성

개인정보 유출사고의 피해유형과 발생된 피해요소에 대한 개념적인 정의 및 구분은 Gordon and Loeb의 연구를 활용한다[24]. Gordon and Loeb은 피해유형인 비밀성, 가용성, 무결성의 상실에 따른 피해 발생 비용을 직접비용(Direct Costs)과 간접비용(Indirect Costs), 명시적 비용(Explicit Costs)과 잠재적 비용(Implicit Costs)으로 구분하여 정의하였다<그림 1>.

여기서 비밀성(기밀성), 무결성, 가용성은 정보보안의 3요소로 불린다. 비밀성은 정보가 비인가된 개인, 프로그램 및 프로세스에 공개되지 않음을 보장하는 것이며, 무결성은 정보가 변경되지 않음을 보장하는 것으로 정



〈그림 1〉 정보보호 침해사고 피해비용 구조[5]

보의 정확성 및 완전성을 보호하는 것이다. 또한 가용성은 인가된 사용자가 요구하는 정보, 시스템 및 자원의 접근이 적시에 제공되는 것을 의미한다.

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

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

본 연구에서는 비밀성과 완결성이 상실된

개인정보 유출사고 피해액을 산출하기 위해 Gordon and Loeb의 개념적인 정의 중 비용적인 부분만을 고려한 선행연구의 방법을 정량적 모델 개발의 시작점으로 활용한다[5]. 이에 따라 개인정보 유출사고로 인해 발생할 수 있는 모든 가시적인 비용과 비가시적인 비용을 명시적/잠재적/간접/직접의 기준에 따라 분류했으며 그 결과는 아래의 <표 1>과 같다.

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

이러한 결과가 일어난 이유는 각 기관들이 결과 산출 시 서로 다른 요소들을 뽑아냈거나 아니면 각 요소에 대한 구체적인 추정 과정이 달랐기 때문으로 추측해 볼 수 있다. 따라서 실제와의 오차를 줄이고 정교한 산출액을 도출하기 위해서는 가장 먼저 서로 겹치지 않으면서도 실제 요소들의 전 범위를 커버할 수 있는 예상 목록 도출이 이뤄져야 한다. 이를 위해 <표 1>에서 제시한 변형된 Gordon and Loeb의 프레임워크를 다양한 요소들을 도출하고 분류하기 위한 기준으로 활용하고자 한다.

3.2 신규개발 모델에의 적용

위에서 언급한 예상 목록 도출을 위해 본 연구에서는 포네몬 연구소, 인포메이션 쉴드(Information Shield Inc.) 등의 보안 전문 연구소와 기업에서 발행한 보고서를 수집·정리함으로써 예상 요소들을 도출하였다. 그 중 본 연구의 목적과 가장 잘 맞는다고 판단한 인포메이션 쉴드 사의 예상 요소를 기준점으로 사용하게 되었다. 이를 위에서 도출한 '개인정보 유출사고 피해액 산출 모형' 프레임워크에 적용함으로써 보다 체계적이고 정교한 산출이 가능해졌다.

인포메이션 쉴드사의 개인정보 피해액 산출을 위한 예상 요소는 다음과 같다[26].

〈표 1〉 개인정보 유출사고 피해액 산출 프레임[5]

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

〈표 2〉 Information Shield Inc.의 피해액 산출 요소

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

본 연구에서는 Information Shield Inc.의 예상 요소들을 앞서 변형한 Gordon and Loeb 프레임워크에 적용하여 다음과 같은 프레임워크를 제안한다.

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

이때 명시적 간접비용인 고객의 신뢰도 측정비용과 시스템 보완 & 교체비용은 현재보다는 미래 대응적 가치이기에 고려 대상에서 제외했으며, 산업 파급효과는 그 영향이 크고 비교적 즉각적인 반응이 나타날 것으로 예상되는 1차 파급효과만을 다루기로 했다. 또한

〈표 3〉 개인정보 유출사고 피해액 산출 범위

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

주) 법적비용 + 벌금 + 보상받지 못한 개인의 정보가치 = 유출된 정보의 가치.

기업의 이미지 손실 역시 측정이 어렵고 명시적 직접비용에서 수익 손실에 일부분이 포함되기에 역시 산출 대상에서 제외했다.

추가적으로 용어에 대한 설명을 하면 명시적 직접비용은 유출사고에만 명확하게 연계될 수 있는 비용 중 유출사고 기간 동안 발생한 명백한 비용을 말한다. 여기에 해당하는 요소로는 사고 대응 인건비와 IR 대응비용 그리고 고객 감소로 인한 수익 손실이 있다. 또한 유출 사고와는 명확하게 연결되지만 유출사고 기간을 넘어 발생할 수 있는 암묵적 비용인 직접적 잠재비용으로는 법적비용과 벌금, 보상받지 못한 개인의 정보가치 등이 있다.

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

4. 개인정보 유출사고 분석 및 피해액 산출 요소

4.1 개인정보 및 개인정보 유출사고의 정의

개인정보 유출사고 피해규모의 파악을 위해서 선행되어야 할 일은 개인정보 유출사고의 범위를 정의하는 일이다.

본 연구에서는 자신에 관한 정보의 수집・이용・공개・제공 등을 본인이 통제할 수 있는 권리인 자기정보통제권이 침해되었을 경우를 의미하는 개인정보 침해사고 중에서 악성코드 감염, 해킹, 서비스 방해 등의 공격행위에 의해 개인정보가 외부로 내보내지는 개인정보 유출과 조직내부에서 개인정보가 새어나가는 개인정보 누출을 논의의 범위로 한정한다. 여기서 유출과 누출은 법률용어가 아니며, 사전적 의미로 볼 때 유출은 특정주체가 개인정보를 의도적으로 밖으로 내보내는 것을 말하며 누출은 기밀・정보 등이 밖으로 새어나가는 것을 의미한다.

4.2 피해요소의 구성

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

〈표 4〉 개인정보 유출사고 피해액 다이어그램

<table>
<tr><th><기업 손실></th><th><개인 손실></th></tr>
<tr><td>대응 인건비</td><td rowspan="4">보상받지 못한
개인 정보 가치</td></tr>
<tr><td>IR 대응비용</td></tr>
<tr><td>수익 손실</td></tr>
<tr><td>(실제 보상한) 법적보상금</td></tr>
</table>

관련 산업 파급 효과

위의 다이어그램에서 제안한 피해요소를 구성하기 위해 본 연구에서는 미국의 포네몬 보고서[29]와 일본 JNSA의 연구[28]를 참고했다.

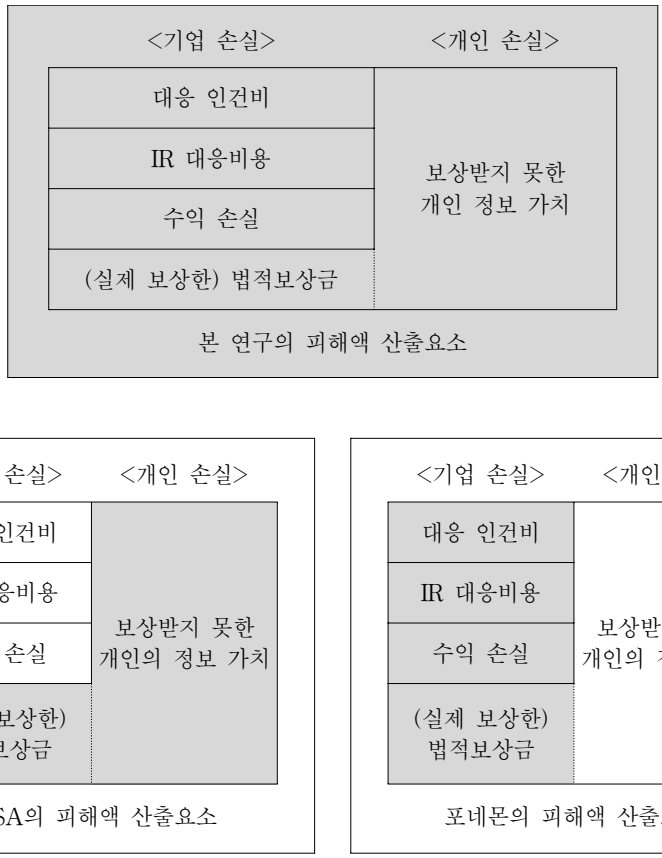
미국의 포네몬 보고서와 일본의 JNSA는 정보 유출에 따른 비용을 각각 기업의 입장과 유출된 정보 자체의 가치에 기반 한 관점에서 산출했다. 하지만 포괄적인 사회적 파급효과를 측정하기 위해서는 정보 유출로 인해 기업과 개인이 겪는 양쪽 모두의 피해액을 동시에 고려하는 것이 필수적이다.

실제 포네몬의 연구는 기업의 손실분을 대상으로 하고 있으며, JNSA가 측정한 정보 가치는 유출로 인해 개인이 받는 피해라고 볼 수 있다. 따라서 기업과 개인 모두의 피해를 동시에 측정할 때 두 사례를 참고하고 적절히 통합하는 방법을 사용하였다. 이를 위에서 제시한 손실액 다이어그램을 이용해 요소별로 비교해서 정리하면 <표 5>와 같다.

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

결과적으로 본 연구에서 측정하는 피해액은 포네몬 보고서에서 산출한 기업 중심의 피해액과 JNSA 보고서에서 산출한 유출된 정보 자체의 가치를 모두 고려한 후 이러한 피해가 관련 산업에 미치는 파급효과까지 측정하였다고 볼 수 있다.

〈표 5〉 측정요소와 선행연구와의 비교 다이어그램



4.3 피해요소의 측정

피해액 산출을 위한 요소들을 도출했으면 이를 측정할 수 있는 자료 수집을 위한 각 요소별 세부식이 필요하다. 이를 위해 실제 측정이 이루어지고 있는 포네몬 연구소[29], 인포메이션 쉴드(Information Shield Inc.)[26] 등의 보안 전문 연구소와 기업에서 발행한 보고서를 참고했다.

먼저 대응 인건비는 시간당 인력비용과 수행 시간을 단위로 사용 하며 여기에는 개인정보 유출이 일어났는지 판단하는 시간, 상황해결을 위해 논의하는 시간, 정보가 유출된 고객을 구분해내는 시간, 메일과 안내문을 쓰고 보내는 시간 그리고 그 외의 부수적인 시간이 포함된다.

IR 대응비용은 유출사고로 인해 실추된 이미지를 회복하고 고객의 이탈을 막기 위한 홍보비용과 고객에게 유출 관련 소식을 알리고 사과를 하는 고객접촉비용을 포함한다.

고객 감소로 인한 수익 손실은 고객 1인당 수익 발생 측면의 가치와 이탈한 고객수로 산출하는데 여기서 고객 1인당 수익 발생 측면의 가치는 고객 1인당 발생하는 수익을 의

〈표 6〉 피해액 산출식

총 피해액 = 1 + 2 + 3 + 4 + 5

1. 대응 인건비 = 시간당 인건비 × 총 인력 투입시간
2. IR 대응비용 = 브랜드 보호를 위한 광고비
3. 고객 감소로 인한 수익 손실 = 고객 1인당 수익 발생 측면 가치 × 이탈한 고객수
4. 유출된 정보의 가치 = 법적 비용 + 보상받지 못한 개인의 정보가치 = [(1인당 보상금 × 소송참여 피해자수) + 소송 비용 + 벌금납부 비용] + 보상받지 못한 개인의 정보가치
5. 관련 산업 파급효과 = 산업 연관표 중 유발계수를 이용해 산출

미한다. 법적 손실 비용과 벌금은 소송비용과 소송을 통해 고객에게 배상해야 하는 보상금 그리고 벌금 납부 비용으로 구성되어 있다.

또한 보상받지 못한 개인의 정보가치는 실제 법적 보상을 받지 못한 개인들의 피해액의 총합으로 추정하고자 하며, 산업파급효과는 산업 연관표의 유발계수를 이용하여 측정한다.

이를 표로 정리하면 <표 6>과 같다.

이렇게 도출된 산출식을 직접 계산하기 위해서는 기본적으로 개인과 기업을 대상으로 한 설문결과를 활용한다. 보안관련 개인과 기업 대상의 설문에서 설문 문항들을 제시, 수집한 결과를 위의 산출식에 대입하면 설문기업들의 피해액을 산출할 수 있다.

4.4 측정값의 검증

본 연구에서는 단순히 설문조사를 통해 얻은 결과를 그대로 가져다 피해액을 산출하는 것만으로는 정확도가 떨어질 위험이 있기에 이를 검증하고자 각 항목마다 다양한 방식의 산출 대안을 마련한 후 이를 설문 결과와 비교・조정함으로써 보다 정확한 값을 얻을 수 있도록 몇 가지 방법을 제안하고자 한다.

먼저 대응 인건비와 IR 대응비용의 경우 포네몬 연구소의 조사결과와 간접비교를 통해 검증하는 방법이 있다.

포네몬 연구소의 보고서에는 유출 기록 1건당 피해액과 각 세부 항목별 비율이 제시되어 있는데[29], 국가별 차이를 고려해서 조사결과를 국내 실정에 맞게 조정한다면 간접적인 비교 기준으로 활용할 수 있게 된다. 예를 들어 대응 인건비와 IR 대응비용의 경우 주로 사람의 힘을 이용한 활동이기 때문에 각 국가 간의 인건비 차이를 조정 요인으로 두고 값을 변환시키면 되는데 이 경우 각 국가별 사무직 평균 임금 등을 파라미터로 활용할 수 있다.

또한 유출 기업 당 피해비용을 비교하고자 하는 경우 국가별 기업의 평균 규모 차이를 이용할 수 있는데 이는 각 국 증권거래소의 총 규모를 상장된 회사의 숫자로 나눠 상장사의 평균 규모의 차이를 유추하는 방법을 이용할 수도 있다.

고객 감소로 인한 수익 손실의 경우 인터넷 기업과 그렇지 않은 기업으로 케이스를 나눠 생각할 수 있다.

인터넷 기업의 경우 매출과 수익이 트래픽에 비례한다는 가정 하에 개인정보 유출 후 급격히 감소한 트래픽량을 측정한 다음 이 값이 1년간 총 트래픽의 몇 %나 되는지를 계산하면 기업의 연수익에서 유출로 인해 약 몇 %의 손해를 보았는지 추정할 수 있다.

인터넷 기업이 아닌 경우엔 포네몬 보고서에 나타난 유출 기록 1건당 수익 감소[29]를 간접 비교하면 된다. 이 경우 국가 간 소비자의 구매력 차이를 조정 요인으로 둘 수 있으며, 이를 위해 구매력은 GDP에 비례한다는 가정 하에 국가별 GDP를 비교 파라미터로 활용할 수 있다.

유출된 정보의 가치는 판례나 개인정보분쟁조정위원회의 손해배상금 관련 자료[1]를 이용해 추정해 볼 수 있다. 이 경우 정보의 성격에 따라 서로 다른 가치가 추정되는데 이를 고려하여 정보를 몇 단계로 분류하는 작업을 수행할 필요성이 있다. 정보의 분류는 오래전부터 체계적인 분류작업을 진행해 온 일본 JNSA의 기준[28]을 참고하여 경제적・정신적 피해 정도에 따라 구분하는 것이 좋은 방법이 될 수 있다. 이렇게 분류된 정보의 종류에 판례나 손해배상금 자료를 참고하여 가치를 부여하면 좋은 기준을 만들 수 있다.

마지막으로 관련 항목과 관련된 각계 전문가와의 심층 인터뷰를 통해 결과값의 타당성을 한 번 더 검증・조정하는 작업을 추가로 수행하여 정확성을 더 높일 수 있다.

5. 결 론

본 연구에서는 개인정보 침해사고 중 개인정보 유출과 누출로 인한 피해를 기업뿐만 아니라 사용자의 피해까지도 고려해 산출하는 방법을 제시하였다. 이 과정에서 미국 포네몬 연구소와 일본 JNSA의 방식을 참고했지만 이를 국내 여건에 맞게 수정하고 나아가 트래픽 분석과 설문 조사 결과, 다양한 지표를 이용한 간접비교 등의 방식을 추가적으로 시도했다. 이는 기존 모델이나 다른 연구 논문들과 비교하여 우리 실정에 적합한 피해규모의 측정을 시도하였다는 점에서 큰 특징을 가진다고 할 수 있으며, 이로 인해 개인정보 유출사고로 인한 피해를 더욱 객관적으로 측정할 수 있도록 기존의 방법을 개선하였다고 판단된다.

실제 엄청난 규모의 피해가 매년 개인정보 유출로 인해 발생하고 있어도 아직 국내의 보안인식은 미국과 일본 같은 나라를 따라가지 못하고 있음을 각종 통계자료를 통해 알 수 있다. 결국 정부를 비롯해 산업을 이끄는 기업과 국민 개개인에 이르기까지 개인정보 보호에 관한 보안 의식이 확립되어야 할 것이며, 이를 위해 더 많은 노력이 필요하다.

본 연구를 수행하는 도중 데이터의 부족으로 인해 보다 정확한 모델을 확립하고, 국내 적용 가능성을 생각해 보는데 어려움이 있었다. 예를 들어, 상당수의 유출사고에 대하여 유출 내용과 유출 건수를 파악할 수 없는 경우가 매우 많았다. 가까운 일본의 경우 개인정보 유출 사고가 일어나면, 이를 미디어를 통해 공표하는 것이 법제화되어 있어 실제 어떤 정보가 유출되었는지 매우 세세한 부분까지 JNSA가 데이터화하여 보유하고 있음에 비해, 국내의 경우 피해액 산출에 이용할 데이터를 찾기가 매우 어려운데다 실제 일어난

사건들이 알려지지 않고 간과되는 일이 빈번하게 현재도 일어나고 있는 것으로 예상된다. 이에 본 연구에서는 일과성으로의 이번 추정에 그치지 않고, 앞으로 데이터를 모으고, 유출사고에 관한 정보와 그 심각성을 보다 많은 사람에게 알림으로써 사회적 공감대를 형성하고 모두의 인식을 개선해야함을 주장하고자 한다. 또한, 국가수준의 적극적 실행을 위한 보안정책 상의 관련 내용 제정의 필요성도 제기한다.

본 연구는 피해규모 수치 그 자체보다는 설문과 상대적 비교 분석 등의 기법을 이용한 산출 방법론을 제시했다는데 의의를 두고 있으며, 이를 적용한 개인정보 유출관련 피해액 산출 작업을 통하여 향후 체계적인 개인정보 유출관련 피해액 산출 모델을 더욱 확립해 나갈 수 있을 것으로 기대한다. 향후 제도적 보완과 이에 의한 데이터 질의 향상과 함께 산출 피해액은 더욱 정확하고 정교하게 추정될 수 있을 것으로 예상된다.

참 고 문 헌

[1] 강달천, 김동환, 오은천, “개인정보분쟁조정사례집”, 한국인터넷진흥원・개인정보분쟁조정위원회, 2010.

[2] 국가보안기술연구소, “정보보호의 경제적 동향분석에 관한 연구”, 국가보안기술연구소, 2006.

[3] 김본미, “개인정보피해구제 및 배상기준에 관한 연구”, 한국정보보호진흥원・개인정보분쟁조정위원회, 2004.

[4] 민경식, 송혜인, “정보보호의 경제적 분석 연구 동향”, 정보보호 이슈보고서 2008-8호, 2008.

[5] 유진호, 지상호, 송혜인, 정경호, 임종인, “인터넷 침해사고에 의한 피해손실 측정”, 정보화정책, 제15권, 제1호, 2008.

[6] 정보통신부, “정보통신망 침해사고 조사결과”, 2003.

[7] 정연수, 김동우, 이재종, “2005년 민간부문 개인정보보호 관리현황 및 보호방안에 관한 연구”, 한국정보보호진흥원, 2005.

[8] 주덕규, 강달천, 정연수, “개인정보 침해와 대처방안”, 정보통신윤리, 통권39호, 2002.

[9] 채승완, “개인정보보호의 경제적 효과”, 소비자문제연구, 제33호, 2008.

[10] 한국인터넷진흥원, “개인정보 영향평가 방법론과 구축사례”, 2009.

[11] 한국정보보호진흥원 전략기획팀, “개인정보의 경제적 가치 분석 고찰”, 정보보호 Issue Report, 2007.

[12] 한국정보보호진흥원, “컴퓨터 해킹, 바이러스 피해액 산출방법 연구”, 2002.

[13] 한국정보보호진흥원, “인터넷 침해사고 피해액 산출모형 개발에 관한 연구”, 2006.

[14] 한국정보보호진흥원, “2007년 정보보호실태조사”, 2007.

[15] 한국정보보호진흥원, “2008년 정보보호실태조사”, 2008.

[16] 한국정보보호진흥원, “2009년 정보보호실태조사”, 2009.

[17] 한국정보보호진흥원, “2003년도 개인 인터넷 이용자의 정보화 역기능 실태조사 보고서”, 2003.

[18] Anita, D. and Amico, D., “What does a Computer Security Breach Really Cost?,” Secure Decision, a division of Applied Visions, Inc., 2000.

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

[20] CIC Security Working Group, “Incident Cost Analysis and Modeling Project,” 1998.

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

[22] Congressional Research Service, “The Economic Impact of Cyber-Attacks,” 2004.

[23] Farahmand, F., Navathe, S. B., Sharp, G. P., and Enslow, P. H., “Assessing Damages of Information Security Incidents and Selecting Control Measures, a Case Study Approach,” Workshop on the Economics of Information Security, 2005.

[24] Gordon, L. A. and Loeb, M. P., “Managing Cybersecurity Resources : A Cost-Benifit Analysis,” 2006.

[25] Howard, J. D., “An Analysis of Security Incidents On the Internet 1989~1995,” 1997.

[26] Information Shield Inc., “Privacy Breach Impact caculator,” (hhttp://www.informationshield.com/privacybreachcalc.html)

[27] JNSA, “情報セキュリティインシデントに關する 調査報告書,” 2003.

[28] JNSA, “情報セキュリティインシデントに關する 調査報告書,” 2010.

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

[30] Smith, D. M., “The Cost of Lost Data,” The George L. Graziadio School of Business and Management Report, Pepperdine University, 2003.

[31] Tech//404, “Data Loss Cost Calculator,” http://www.tech-404.com/calculator.html).

[32] USENIX Association, “Incident Cost Analysis and Modeling Project Ⅱ,” 2000.

저 자 소 개

한창희 (E-mail : chan@hanyang.ac.kr)
1992년 한양대 산업공학 (학사)
1994년 KAIST 산업공학 (석사)
1999년 KAIST 경영공학 (박사)
Georgia Tech 초청연구원
현대정보기술 연구원
오픈타이드 코리아컨설턴트
현재 한양대학교 경상대학 부교수
관심분야 융합비즈니스, 온라인 사업전략, 의사결정 분석

채승완 (E-mail : chaisw@kisa.or.kr)
1990년 수원대학교 경제학 (학사)
1992년 단국대학교 경제학 (석사)
2001년 일본 니아가타(新潟) 대학 경제학 (박사)
일본 ERINA(동북아경제연구소) 연구원
한양대학교 연구조교수
현재 한국인터넷진흥원(KISA) 책임연구원
관심분야 인터넷 및 정보보호 정책, 동 산업전략 및 경제성 분석, 동 인력양성 및 교육 등

유병준 (E-mail : byoo@snu.ac.kr)
1994년 서울대학교 경영학 (학사)
1999년 미국 아리조나 주립대학교 경영정보 (석사)
2003년 미국 카네기멜론 경영대학원 경영학 경영정보전공 (박사)
고려대학교 경영대학 조교수
현재 서울대학교 경영대학원 부교수
관심분야 온라인 비즈니스 전략, 디지털컨텐츠산업 전략 및 경제성 분석, 전자보안 등 IT 투자효과 분석

안대환 (E-mail : Ahndaehwan@gmail.com)
2011년 서울대학교 건축학 및 경영학 (학사)
현재 서울대학교 경영대학원 석사과정
관심분야 소셜네트워크, 소셜필터링, 디지털컨텐츠 산업 전략, 온라인 게임, 컨텐츠 가격설정, 전자상거래

박채희 (E-mail : gogepao@naver.com)
2010년 한양대학교 신문방송학 및 경영학 (학사)
현재 한양대학교 경영컨설팅학과 석사과정
관심분야 온라인 비즈니스, 인터넷 정보보호, 온라인 게임 비즈니스, 디지털 자산