情報保護學會論文誌
第19卷 第4號, 2009. 8

# 개인정보 유·노출 사고로 인한 기업의 손실비용 추정

유 진 호,[1†‡] 지 상 호,[1] 임 종 인[2]
[1]한국인터넷진흥원, [2]고려대학교 정보경영공학전문대학원

# Estimating Direct Costs of Enterprises by Personal Information Security Breaches

Jinho Yoo,[1†‡] Sangho Jie,[1] Jongin Lim[2]
[1]Korea Internet & Security Agency,
[2]Graduate School of Information Management and Security, Korea University

요 약

해킹에 의한 개인정보의 유출 또는 기업의 관리 소홀로 인한 개인정보 유·노출 등의 침해사고가 다양한 형태로 발생하고 있으며, 이로 인한 피해범위도 확대되고 있다. 개인정보 유·노출 사고의 발생시 기업의 손실비용을 산출하는 일은 정보보호 투자에 대한 의사결정을 위해 필요하다. 본고는 개인정보 유·노출 사고로 인한 기업의 직접적이고 정량적인 손실비용 산출방안을 제시하고자 한다. 먼저 개인정보 침해사고에 의해 발생할 수 있는 손실비용을 범주에 따라 분류하고, 비용을 구성하는 요소들을 구체적으로 분석하였다. 또한 제시된 모형으로 2005~2007년 동안 국내에서 발생한 개인정보 유·노출 사고의 손실을 추정하였고, 이를 일본의 사례와 비교 분석하여 시사점을 도출하였다.

ABSTRACT

Recently personal information security breaches by unauthorised access, mistakenly disclosure or stolen become more frequent and the scale of the economic loss of such incidents is growing. Assessing economic loss of personal information security breaches is needed for decision making of information security investment. This paper presents a framework to analyze economic impact of personal information security breaches and develops formula for each element to empirically calculate the economic loss. We also compared annual economic loss of Korea with that of Japan to develop some implications.

**Keywords:** Personal information security breaches, Information security incidents, Economic loss

## I. 서 론

정보화의 빠른 진전과 더불어 그의 역기능 역시 확산되고 있다. 특히 기업의 마케팅 기법이 고도화됨에 따라 개인에 대한 정보가 기업의 마케팅 전략에 적극 이용되고 있다. 이와 같은 현상이 역기능 측면에서는 개인정보를 수집, 저장 및 관리, 이용 및 제공, 파기의 과정에서 임의로 혹은 관리소홀로 개인정보가 유출 또는 노출로 이어지고 있다. 한국정보보호진흥원(2008)에 의하면 2007년 한 해 동안 주민번호 노출 등 개인정보 침해로 인한 상담 및 피해구제 신청 건수가 총 25,965건으로, 2005년도에 18,206건, 2006년도에 23,333건에 비해 꾸준히 증가하는 추세이다[1].

기업이 보유하고 있는 개인정보는 기업의 자산일 뿐만 아니라 정보제공자의 사적 재산이다. 따라서 어떠한 이유에서든지 기업이 보유하고 있는 개인정보의 유출이 발생한 경우에는 피해자 개인에게 정신적·경제적 피해를 야기하고, 기업에게는 사고대응비용, 피해자 보상비용, 기업의 이미지 하락 등으로 인한 경제적 손실로 연결되어 진다. 또한 개인정보의 유·노출은 피해 당사자

접수일(2008년 10월 22일), 수정일(2009년 4월 16일), 게재확정일(2009년 6월 26일)
† 주저자, jhyoo@kisa.or.kr
‡ 교신저자, jhyoo@kisa.or.kr

들인 개인과 기업의 문제 뿐만 아니라 사회적 문제로 발전하고 있는 것처럼, 이제 개인정보는 정보제공자 개인의 사적재화 뿐만 아니라 제도적 차원에서 사회전체가 관리 보호해야 하는 공공재이기도 하다.

개인정보를 보호하는 것이 중요함에도 불구하고 개인정보 침해사고에 의한 기업의 손실비용에 대한 연구와 자료가 미흡한 실정이기 때문에 이에 대한 국가적 손실규모를 계량화하는 작업에 많은 현실적 어려움이 존재하고 있다. 손실규모를 제대로 평가하면 경제적으로나 사회적으로 미치는 사고 영향의 심각성을 제대로 파악할 수 있고, 결과적으로 개인정보 침해사고 대응책에 필요한 노력과 비용의 크기에 대한 의사결정을 할 수 있기 때문에 체계적인 경제적 손실규모를 파악하는 일은 선행적으로 반드시 필요한 과제이다.

본고는 개인정보 침해사고가 발생하는 경우 조직내에서 경제적 손실규모를 산출할 수 있는 모형을 수립하여, 개인정보보호의 중요성에 대한 기업의 인식수준을 제고하고 국가 차원에서의 개인정보보호 수준을 높이기 위한 기초자료로 활용하고자 한다. 이를 통해 향후 유사한 상황이 발생할 시 그 경제적 손실을 측정하고 이를 예방하기 위한 대책 수립에 활용하는 것을 목적으로 하고 있다.

2장에서는 개인정보에 대한 정의, 개인정보 침해사고에 대한 정의 및 관련 연구들을 살펴본다. 3장에서는 본고에서 제시하는 개인정보 침해사고에 의한 손실비용 산출 모형을 소개하고, 구체적인 산출 방식을 제시하고자 한다. 4장에서는 본고에서 제시한 모형을 2005년도부터 2007년도까지 국내 기업에서 발생한 개인정보 침해사고에 적용하여 실제 측정값을 산출하였으며, 일본의 사례와 비교 분석하고자 한다. 최종적으로 5장에서는 본고의 연구결과에 대한 평가와 이를 통한 시사점 분석 및 향후 연구방향에 대해 정리하고자 한다.

## II. 선행 연구

정보통신망이용촉진및정보보호등에관한법률 제2조에 의하면 개인정보는 "생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명, 주민등록번호 등의 사항에 의하여 당해 개인을 알아볼 수 있는 정보(당해 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함)"로 정의된다[2].

정부혁신지방분권위원회(2004)는 개인정보를 크게 속성정보, 활동정보, 민감정보 3가지로 구분하였다[3]. 속성정보는 개인을 타인으로부터 식별하고 특성을 규정하는 정보로서 이름, 성별, 주민등록번호, 지문 등이 해당한다. 활동정보는 개인의 일상생활과 관련된 정보로서 가족·출신 및 생활환경, 학력 및 교육, 고용 및 경력, 재산·신용·납세, 사회보장 및 행정서비스 정보 등이 포함된다. 민감정보는 개인의 기본적 인권을 현저하게 침해할 우려가 있는 정보로서 인종, 민족, 정치적 성향, 보건, 의료정보 등이 해당한다.

Weible(1993)은 개인정보를 일반정보, 가족정보, 교육 및 훈련정보, 병역정보, 부동산정보, 동산정보, 소득정보, 기타 수익정보, 신용정보, 고용정보, 법적 정보, 의료정보, 조직정보, 습관 및 취미정보 등 총 14개의 유형으로 상세하게 분류하여 개인정보에 대한 이해를 용이하도록 하였다[4].

김여라 외(2007)는 디지털 기술의 발전과 더불어 최근에는 개인의 통신정보, 위치정보, 영상정보 등과 같은 기록도 개인의 활동을 반영하는 정보로서 중요하게 다루어질 필요가 증가함에 따라, 개인정보에 대한 분류체계를 제시하고 개인정보의 가치 분석에 활용하였다[5].

일반적으로 개인정보 침해사고는 "본인 동의 없는 개인정보 수집 및 제3자 제공 또는 정보통신망에 의하여 처리되는 개인정보의 분실, 도난, 유출 변조 등으로 개인이 물리적, 심리적 피해를 입게 되는 사태"로 정의된다. 따라서 개인정보 침해는 원인이나 경로보다는 어떠한 유형이든 마지막 관점에서 각 개인이 겪게 되는 물리적, 심리적 피해를 의미한다.

Gordon & Loeb(2006)은 정보보호 침해사고에 의한 비용 산출에 활용하기 위해 손실비용 구조모형(Cost Grid)을 제시하였다[6]. 이 연구는 특히 여러 가지 다양한 침해사고로부터 발생하는 손실비용을 직접비용(Direct Costs)과 간접비용(Indirect Costs), 명시적 비용(Explicit Costs)과 잠재적 비용(Implicit Costs)으로 구분하여 침해사고로 인한 손실비용을 산출할 수 있는 개념적인 분석 틀을 제시하였다.

유진호 외(2008)는 정보보호 침해사고 중에서 가용성 상실에 의해 나타나는 손실비용을 Gordon & Loeb(2006)의 분석틀을 이용하여 측정하였다[7]. 이 때 계량경제학적인 접근방법 보다는 피해비용 항목을 분할한 다음 표본조사를 통해 필요한 파라미터를 추정하여 전체 규모를 파악하는 원단위(原單位, basic unit) 접근법을 사용하였고, 이론적인 배경 보다는 실무 연구자 관점에서 이해하기 쉽게 접근한 것이 특징이다.

김여라 외(2007), 유진호(2007)는 가상가치접근법(CVM)을 활용하여 이용자가 개인정보 유출방지를 위해 금전적으로 지불할 수 있는 금액(WTP: Willingness to Pay)을 추정하였다[5,8]. 유승훈 외(2003) 또한 CVM을 이용하여 스팸메일의 불편회피를 위한 지불의사액을 추정하였다[9]. 그러나 이용자는 자신의 개인정보를 보호하기 위해 직접 지불해야 하기 때문에 WTP 추정금액은 상대적으로 낮게 추정되는 특징이 있다.

이해춘 외(2008)는 CVM 방법론을 이용하여 개인정보 유출의 손실가치를 분석하였다[10]. 이 연구는 개인정보 유출로 피해 가능성이 있는 응답자가, 기업이 제시하는 손해 배상을 수용하는 WTA(Willingness to Accept)를 화폐액으로 추정하여 개인정보 유출의 잠재적 손실액을 추정하였다. 그러나 이용자는 개인 정보가 침해당할 경우 기업이 제시하는 배상금액을 받아들이기는 쉽지 않는 성향에 의해 WTA에 의한 추정값은 상대적으로 과추정(over-estimate)되는 특징이 있다. 이 연구의 결과에서 알 수 있듯이 이용자는 자신의 명의가 도용되어 특정 온라인 게임사이트에 가입된 사실을 알고, 1인당 약 750만원의 배상금을 받기를 원하는 것으로 나타났다.

반면 김여라 외(2007)의 연구 결과에서 이용자는 자신의 개인정보 보호를 위해 부가적인 통신서비스 요금을 낼 경우, 1개월에 약 3,900원을 지불할 의사가 있는 것으로 나타나 이용자의 양면적인 태도를 알 수 있다[5]. 따라서 WTA에 의한 추정치는 과추정의 우려가 있고, WTP에 의한 추정치는 상대적으로 낮게 추정될 우려가 있다는 것을 입증한다.

CVM 방법론은 이론적인 배경은 강점을 가지고 있으나, 실제 기업의 업무 환경을 직접적으로 반영하는 것 보다는 간접적인 측정방법으로서 한계점을 가진다. 특히 CVM 방법론은 이용자에게 제시하는 초기금액이나 가상시나리오에 의해 크게 영향을 받거나 조사자에 의한 편의(bias)가 발생할 수 있기 때문에 관련분야 전문가들의 면밀한 검토가 없으면 조사 시점마다 크게 달라질 수 있는 한계가 있다[11].

일본 JNSA(2007)는 2002년도부터 뉴스 미디어, 인터넷 뉴스 등을 통해 공식 보도된 개인정보 누출 사고에 대한 조사 및 분석을 매년 실시하고 있다[12-14]. 이 조사에서는 개인정보 누출과 관련된 자료를 수집하고, 누출이 발생한 기업 또는 조직의 유형, 개인정보 누출에 영향을 받은 개인 피해자의 수, 정보누출의 원인 및 경로, 누출된 정보의 유형 분석, 비용 산출 등을 수행하고 있다. 특히 비용 산출방식은 계량경제학 방법 보다는 간단한 원단위 접근법을 사용하였다. 이 연구는 기업이 보유한 개인정보의 유출을 보험사의 손해사정 관점에서 배상금을 추정하고 전체 손실규모를 산정하였다.

미국 PGP Corporation & Vontu(2007)는 2005년도부터 미국내 약 35개의 기업에서 발생한 개인정보 침해사고로부터의 손실비용을 그룹의 대푯값을 통해 전체규모를 추정하는 원단위 접근법을 사용하였다[15,16]. 이는 기업들로 하여금 개인정보 침해사고에 의한 손실을 산출하는데 적용할 수 있도록 한 것이다. 미국에서는 2002년에 California Senate Bill 1386을 통해 개인정보 유출시 공지에 대한 의무 규정이 발효된 이후, 개인정보 유출로 인한 손실비용은 꾸준히 증가하고 있는 현실이다. 실제로 2005년도 이후에 미국에서 유출된 개인정보건수는 2억 1천 5백만건 이상이 되는 것으로 나타났고, 2007년도에는 미국 35개 이상의 주에서 개인정보 유출에 의한 의무고지 조항이 지켜지고 있다[17].

개인정보 침해사고 피해액을 산출하기 위해 시도한 JNSA와 PGP Corporation & Vontu의 연구는 개인정보 침해사고로 인한 직접적인 손실을 산출하기 위한 방법이고, 계량경제학적으로 접근하기 보다는 개괄적이고 실무자 관점에서 접근한 방법론이라는 점에서 공통점을 가진다.

본고에서도 국내에서 발생한 개인정보 침해사고에 대해 기업의 직접적인 손실규모를 실무자 관점에서 파악하는데 초점을 맞추었으며, 침해사고 발생시 신속하게 적용할 수 있고 현실적으로 여러 조직 내에서도 활용할 수 있도록 하기 위해 논리적인 사고로 접근할 수 있는 원단위(原單位, basic unit) 접근법을 사용하였다. 또한 기존 문헌에서 사용된 변수들의 장단점을 분석하여, 국내에서 실질적으로 적용하는 데 보다 타당성을 갖도록 하였으며, 일반기업 뿐만 아니라 공공부문 등에도 포괄적으로 적용될 수 있도록 하였다.

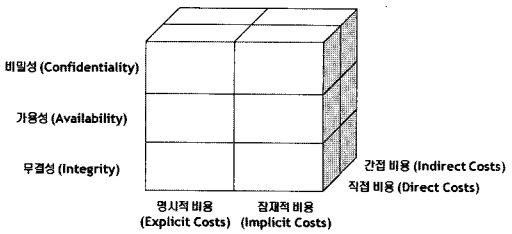
## III. 개인정보 침해사고로 인한 손실비용 산출모형

### 3.1 손실비용 산출 Framework

개인정보 침해사고로 인한 손실비용을 산출하기 위해서는 유출된 개인정보로 인해 조직 내에서 어떠한 비용이 발생했는지를 요소별로 파악할 수 있어야 한다. 본고는 이러한 비용 구조 파악을 위해 Gordon &

Loeb(2006)이 개념적으로 정의한 침해사고 비용 구조를 활용하고자 한다[6]. Gordon & Loeb(2006)은 [그림 1]과 같이 침해사고 피해유형을 크게 비밀성, 가용성, 무결성이 상실된 것으로 나누고, 이에 따른 손실비용을 직접비용(Direct Costs)과 간접비용(Indirect Costs), 명시적 비용(Explicit Costs)과 잠재적 비용(Implicit Costs)으로 구분하여 정의하였다[6]. 개인정보 침해사고는 기업의 비밀성 정보가 상실된 경우이므로, Gordon & Loeb(2006)의 손실비용 산출모형을 적용할 수가 있다.

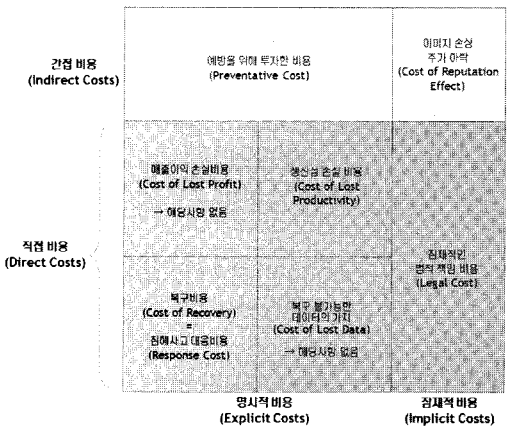
Gordon & Loeb(2006)의 모형에 따르면 직접비용은 특정 침해사고에 명확하게 연계(link)될 수 있는 비용을 의미하는 것으로 해당사고에 의해 발생하는 인력손실, H/W 손실, S/W 손실 등을 의미한다[6]. 반면에 간접비용은 특정 침해사고와 직접적으로 연계되어지지 않는 비용으로서, 다른 사고에 의해서도 영향을 받을 수 있는 피해비용을 의미한다[6]. 예를 들어 침해사고 예방을 위해 투입된 보안장비 구입비용은 특정사고만을 위한 비용이 아니라, 여러 가지의 사고 예방을 위해 투자한 비용이므로 보안장비 구입 후 침해사고에 의해 손실이 발생되었다면 간접비용의 손실이 발생한 것이다.




[그림 1] 사이버 침해사고 비용 구조
(출처: Gordon & Loeb(2006))

한편 명시적 비용은 특정 침해사고를 예방하고, 탐지하고, 복구하기 위해서 침해사고 기간 동안 발생한 명백한 비용을 의미한다. 예를 들어 복구인력 비용, 매출손실 비용 등이 해당한다. 반면에 잠재적 비용은 기회손실과 연관된 묵시적, 파생적 비용을 의미하는 것으로 침해사고에 의한 기업의 이미지 손실, 잠재적 법적 책임비용 등이 해당된다.

본고는 개인정보 침해로 인한 손실비용을 산출하기 위해 Gordon & Loeb(2006)이 정의한 것을 바탕으로, [그림 2]와 같이 개인정보 침해사고에 의해 발생되는 비용을 상세하게 구분하고자 한다. 유진호 외(2008)의 연구에서도 이와 같은 방식에 의해 인터넷의 가용성 상실로 인한 침해사고 손실비용을 산출하였다[7]. 서승우(2008)도 직접비용과 간접비용, 명시적인 비용과 잠재적인 비용으로 구분하고, 이를 구성하는 비용항목들을 설명하였다[18]. 이는 김정덕, 최광희(2000)가 제시한 Spreedsheet를 이용한 비용산정 방법에 해당한다[19]. 김정덕, 최광희(2000)는 계량적 위험모형(QRM 모형, Quantitative Risk Model)이나 일반화된 비용결과모형(GCC 모형, Generalized Cost Consequence Model)에 비해 현실적인 활용가능성 측면에서 Spreedsheet 방법론이 가장 유용하다고 하였다[19].




[그림 2] 침해사고 손실비용 산출 모형 Framework

개인정보 침해사고는 현재의 상태 $I_0$가 개인정보가 노출 또는 유출된 상태 $I_1$로 변환된 행위로 정의할 수 있으며, 여기서 손실비용이란 특정 침해사고 s와 직접적으로 연계된 직접비용과, 침해사고 s라고 단정할 수는 없지만 여러 요인에 의해 파생적으로 발생할 수 있는 간접비용으로 구분된다. 직접비용 자체도 사고 전후의 변화에 따라 기업의 내부적인 조치를 위해 소요되는 명시적 비용과 외부적인 영향에 의해 발생되어지는 잠재적 비용으로 구분되고, 간접비용도 마찬가지로 명시적 비용과 잠재적 비용으로 구분된다.

$$
\begin{aligned}
&\text{침해사고 피해액 } \mathrm{TotalCost}(I_1)\\
&\quad \equiv \mathrm{DirectCost}(s|I_1) + \mathrm{IndirectCost}(I_1)\\
&\quad \equiv \{\mathrm{DirectExplicitCost}(s|I_1) +\\
&\qquad \mathrm{DirectImplicitCost}(s|I_1)\} +\\
&\qquad \{\mathrm{IndirectExplicitCost}(I_1) +\\
&\qquad \mathrm{IndirectImplicitCost}(I_1)\}
\end{aligned}
$$

여기서, DirectExplicitCost(s|$I_1$)은 개인정보가 유·노출된 $I_1$상태에서 특정사고 s와 직접적으로 연계된 직접비용 중 내부적인 조치를 위해 소요되는 명시적 비용이고, DirectImplicitCost(s|$I_1$)은 개인정보가 유·노출된 $I_1$상태에서 특정사고 s와 직접적으로 연계된 직접비용 중 외부적인 영향에 의해 발생되는 잠재적 비용이다. 또한 IndirectExplicitCost($I_1$)은 여러 가지 다양한 사고를 예방하기 위해 내부적으로 명백히 투입하였으나 개인정보가 유·노출된 $I_1$상태가 됨에 따라 손실된 명시적 비용이고, IndirectImplicitCost($I_1$)은 개인정보가 유·노출된 $I_1$상태에서 특정 침해사고 s를 포함한 다양한 외부 환경에 의해 영향을 받아 손실된 잠재적 비용이다.

DirectExplicitCost(s|$I_1$)은 사고 발생 전 $I_0$ 상태에서 기대되는 매출이익과 업무 생산성이 손실되어 발생한 비용과 개인정보가 유출 또는 노출된 상태 $I_1$을 원래 상태 $I_0$로 복원시키기 위해 추가적으로 발생한 비용으로 구분할 수 있다.

고객의 개인정보 유·노출로 인한 기업 내 매출이익손실은 사고 당시 발생하는 것이 아니라 사고 공지 후 기업 이미지 실추에 의한 효과(Reputation Effect)이다. 따라서 사고 당시 시점에서의 직접적인 손실 보다는 2차적으로 발생하는 손실 비용, 즉 간접비용에 해당한다. 그러나 사고가 발생하면 조직 내 생산인력이 복구과정 또는 내부 조치 과정에 투입되기 되기 때문에 기존 업무 생산성의 손실비용(Cost of Lost Productivity)은 직접비용에 해당한다.

침해사고 발생상태 $I_1$을 사고 발생전 상태 $I_0$로 복원하기 위해 투입되는 추가적인 복구 비용(Cost of Recovery)은 침해사고 발생 후 파생적 피해를 최소화하기 위해 고객들에게 알리고 콜센터를 운영하는 등 내부조치 뿐만 아니라 여러 가지 조사 및 법적 대응준비 등에 사용되는 침해사고 대응비용(Response Cost)이다. 그리고 개인정보가 유·노출된 것은 조직 내부의 데이터가 외부로 유출된 것으로 데이터 원본 자체가 변조되거나 복구 불가능한 상태가 아니므로 복구 불가능한 데이터의 가치는 해당사항이 없다.

DirectImplicitCost(s|$I_1$)은 비밀성 유지가 필요한 개인정보가 유출됨으로 인해 파생되는 손실이다. 피해 당사자인 개인의 소송에 의해 발생하는 법적 책임비용(Legal Cost)이 여기에 해당된다. 즉, 침해사고를 당한 피해자들에게 지급되어야 하는 손해배상금과 법령 위반에 의해 부과되는 과태료 등이다.

IndirectExplicitCost($I_1$)은 여러 가지 침해사고를 사전에 예방하기 위해 내부적으로 투입한 침해사고 예방비용(Preventative Cost)이다. 침해사고 예방을 위해 투입된 보안장비 구입비용은 특정사고 s만을 위한 비용이 아니라, 여러 가지의 사고 예방을 위해 투자한 비용이므로 이에 해당한다.

IndirectImplicitCost($I_1$)은 침해사고로 인한 기업의 이미지 하락, 주가 하락, 고객이탈로 인한 매출 손실 등으로 일정기간 이후에 나타나는 이미지 손실비용(Cost of Reputation Effect)이다. 간접비용을 산출하기 위한 방식으로는 사고 후 주가변동률을 분석하는 것이 일반적이다. Campbell et al.(2003), Cavusoglu et al.(2004)는 사이버 공격을 당한 기업의 주가 변동률을 분석하였다[20][21]. 국내에서는 남상훈(2005)이 보안 Event가 주식가격에 미치는 영향을 실증적으로 검증하였다[22]. 권영옥, 김병도(2007)에서도 정보보안 사고가 기업가치에 부정적 영향을 미치는 것으로 주식 변화를 분석하여 입증하였다[23]. 간접비용은 사고 발생 시점이 아닌, 사고가 공지된 시점 이후에 발생할 수 있는 비용이기 때문에 반드시 특정사고 s에 의한 것이라고 단정할 수는 없다. 사고가 공지된 시점에서의 매출과 주가 등은 외부 경제적 환경요인에 의해서도 영향을 받을 수 있기 때문에 이에 대한 편의(bias)를 제거하는 세심한 주의가 필요하다.

주식 변화 데이터를 통해 간접적인 손실을 입증한 국내외의 학술적 연구에 비해, 상대적으로 개인정보 유·노출을 통해 기업이 입은 직접적인 손실규모를 산출한 사례는 드물다. 특히 계량경제학적인 학술적인 접근 방식이 아닌 실무적인 관점에서 이해하기 쉽게 접근한 국내사례는 없기 때문에, 본고는 개인정보 침해사고에 의해 기업이 입게 되는 직접적인 손실규모를 파악하는데 초점을 맞추어, 이를 상세하게 계산하는 산출식과 적용사례를 제시하고자 한다.

## 3.2 개인정보 침해사고에 의한 직접적인 손실액 산출

### 3.2.1 침해사고 대응비용(Response Cost, 복구비용)

침해사고 대응비용(Response Cost)은 조직 내에서 침해사고 발생 후 피해를 최소화하기 위해 신속히 대응하고 이를 정상상태로 복구하는 과정에서 소요되는 비용이다. 기업은 개인정보 유출 또는 노출 등에 의한 침해사고가 발생하면 신속히 고객들에게 공지 또는 사죄광고를 하고, 전문가의 자문을 받아 법적 분쟁에 대비하게 된다. 또한 고객들의 확인전화에 응대하

기 위한 콜센터를 운영하고 필요에 따라서는 피해를 당한 고객들에게 미리 보상서비스를 제공하기도 한다.

2004년 6월 일본 야후 BB는 인터넷 서비스 이용자 450만 명의 개인정보가 유출되었을 때, 가입자 전체에게 개인정보 유출에 관계없이 500엔 상당의 상품권을 지급하였다. 이와 같은 보상서비스 비용도 침해사고 대응을 위해 소요되는 비용이므로 이를 포함한 침해사고 대응비용(Response Cost)을 다음과 같이 정의하고자 한다.

$C_R = C_{Announce} + C_{Consulting} + C_{Callcenter} + C_{Service}$

$C_{Announce}$ : 이메일 공지, 웹사이트 공지, 신문 공지 등을 포함한 사고공지 비용

$C_{Consulting}$ : 사고에 대한 법적 대응 준비를 위해 지불한 법률 자문(컨설팅) 및 포렌식 자문(컨설팅) 비용

$C_{Callcenter}$ : 사고응대를 위해 상담센터를 운영한 비용

$C_{Service}$ : 피해자에게 사고에 대한 보상차원에서 지불한 서비스 비용

PGP Corporation & Vontu(2007)도 직접적인 비용(Direct Incremental Costs)에 보상서비스 제공비용, 사고 공지비용, 법률·감사·회계 자문비용, 콜센터 운영비용 등을 포함하여 산출하였다. 여기서는 특히 서베이를 통해 침해당한 개인정보 1건당 평균 소요비용, 기업당 평균 소요비용을 추정하여 전체 피해비용을 산출하였다.

### 3.2.2 생산성 손실비용(Cost of Lost Productivity)

개인정보 침해사고 발생 후, 일부 직원들은 침해사고 대응을 위해 신속히 대응업무에 투입되어 이를 처리하게 된다. 따라서 정상적인 상태에서 진행되고 있던 해당 업무의 생산성은 저하될 수 밖에 없으며, 이로 인한 손실이 발생하게 된다. 즉, 기존 인력이 긴급업무에 투입됨으로 인해 기존에 수행되는 업무의 생산성은 정상적인 상태보다 저하된다. 따라서 '생산성 손실비용'을 다음과 같이 정의하고자 한다.

$C_{LP} = N_{Affected} \cdot P_{Employee} \cdot T_{Response}$

$N_{Affected}$ : 침해사고로 영향 받은 직원 수

$P_{Employee}$ : 사고로 영향받은 직원의 시간당 생산성

$T_{Response}$ : 긴급 대응업무 투입시간

'긴급 대응업무 투입시간'은 기존 업무 대신에 개인정보 침해사고 대응을 위해 투입된 시간이다. '침해사고로 영향을 받은 직원 수'는 사고로 인해 기존 업무 대신에 침해사고 대응업무를 수행한 직원 수를 말하며, '시간당 생산성'은 침해사고로 영향받은 직원 1인이 시간당 생산에 기여한 것을 화폐가치로 환산한 금액이다. 직원 1인당 '시간당 생산성'을 측정하기 위한 방법으로는 생산을 위해 투입된 금액 즉, 직원의 '시간당 인건비 단가'로 간접 추정할 수 있다. 이는 생산과 지출은 이론적으로 등액이라는 경제학적인 원칙에 따른 것이다.

Weaver & Paxson(2004)은 웜에 의한 침해사고 손실을 측정할 때, '시간당 생산성'을 측정하는 변수로 미국 근로자 1인당 GDP 값을 사용하였다[24]. 그러나 1인당 GDP 값은 경제 주체가 생산하는 총 부가가치의 합을 나타내므로, 앞부분에서 언급한 '매출이익손실' 부분을 포함하는 개념이다. 앞서 설명한 바와 같이 개인정보 침해사고에 의한 '매출이익 손실'은 사고 직후에 발행되는 것이 아니라 사고가 공지된 후, 2차적으로 발생되는 간접피해비용에 해당하므로 직접적인 피해비용 산출에 1인당 GDP 값을 적용하는 것은 사고로 인한 직접적인 생산효율 저하 측면에서는 과추정(over-estimate)될 수 있을 것으로 판단된다.

Weaver & Paxson(2004)의 연구와 같이 시스템과 네트워크의 가용성(Availability)이 상실된 경우에는 사고가 발생하는 시점부터 매출이익손실을 포함한 직원의 생산성에 직접적인 영향을 미치나, 개인정보 침해사고와 같은 비밀성(Confidentiality)이 상실된 사고시점에는 직원들이 복구를 위해 투입되므로 업무생산성에는 영향을 미치나, 매출은 사고가 공지된 이후 고객들의 이탈에 의해 영향을 받으므로 이를 별도로 분리하여 관리할 필요가 있다. 따라서 본고에서는 '시간당 생산성'을 측정하는 변수로 직원의 시간당 인건비를 사용하고자 한다. 이와 같이 '시간당 생산성'을 측정하는 변수로 인건비를 사용할 것인지, 1인당 GDP값을 사용할 것인지는 피해액을 측정하고자 하는 범위 또는 상황여건에 따라 결정되는 것이 필요하다.

### 3.2.3 잠재적인 법적 책임비용(Legal Cost)

잠재적인 법적 책임비용은 침해사고를 당한 피해자들에게 지급해야 하는 손해배상금, 법 위반에 따라 지불해야 하는 과태료 또는 과징금 등을 포함하는 비용

으로 다음과 같이 정의하고자 한다.

$C_I = C_{Compensation} + C_{Penalty} + C_{Surcharge}$
$C_{Compensation}$ : 유·노출 사고 피해자에 대한 손해배상금
$C_{Penalty}$ : 법 기준 위반 행위에 의한 과태료(벌금액)
$C_{Surcharge}$ : 규약 위반에 대한 제재로 징수하는 과징금 (이익 환수 금액 등)

대량의 개인정보가 유·노출되어 피해자 수가 많을 경우에, 침해사고에 대한 일인당 피해보상금은 전체 손실비용에 가장 큰 영향을 주기 때문에 이를 합리적으로 산출하는 것이 가장 중요하다. 손해배상금을 합리적으로 산출하기 위해서는 법원의 판결에 의해서 배상이 이루어진 판례 또는 개인정보분쟁조정위원회에서 조정이 이루어진 과거 사례를 활용하는 것이 바람직할 것이다.

본고에서는 최근 법원의 판결사례가 있는 경우에는 판결사례를 우선적으로 사용하고, 판결사례가 없는 경우에는 개인정보침해분쟁조정위원회에서 조정한 사례를 사용하고자 한다. 법원 판결은 시대적 상황에 따라 법의 해석이 달라질 수 있는 특성상, 가장 최근의 판례가 현실을 가장 잘 반영하는 것이라고 판단되기 때문에 최근에 나온 결과를 대푯값으로 사용하고자 한다.

JNSA(2007)는 개인정보 유·노출에 의한 법적 배상금을 산출하기 위해 개인정보 침해의 피해 정도를 침해된 개인정보 항목별로 경제적 피해 수준(Economic Distress Level)과 정신적 피해 수준(Emotional Distress Level)의 두 가지 측면에서 평가하여 산출하였다. 그러나 배상금 산출에 대한 계산식을 보면, 보험사의 손해사정 관점에서 지수함수를 적용한 구체적인 근거와 합리적인 타당성을 제시하지 않고 있기 때문에 객관적으로 쉽게 납득하기가 어려운 점이 있다.

본고에서는 손해배상금을 산출하기 위해서 새로운 계산식을 개발하는 것 보다는 법적 기준에 의해 결정된 최근 판례가 현실을 가장 적절히 반영하는 것이라 판단하여, 국내 판례 결과를 활용하고자 한다.

## IV. 적용 및 비교

### 4.1 연간 개인정보 침해사고에 의한 기업의 직접적인 손실액 추정

앞서 제시된 모형으로 국내 기업에서 연간 발생한 개인정보 침해사고의 손실비용 규모를 산출하고자, 2005년도에서 2007년도까지 3년 동안 국내 언론에 보도된 개인정보 침해사고 내용을 분석하였다. [표 1]과 같이 2005년도에는 41건, 2006년도에는 57건, 2007년도에는 46건이 언론에 보도되었다. 언론에 보도된 사건들에 대한 조사는 웹사이트 뉴스검색을 통해 조사하였으며, 동일 사고에 대해 여러 매체에서 보도된 사건은 1건으로 계산하고, 서로 다른 사고에 의해 피해당한 피해자 수는 중복을 확인할 방법이 없기 때문에 단순합계로 집계하였다.

[표 1] 연간 개인정보 침해사고 발생 내역

| 구분 | 2005년 | 2006년 | 2007년 |
|---|---|---|---|
| 총 피해 인원 | 6,849,088명 | 46,187,814명 | 17,341,887 |
| 사고 발생 건수 | 41건 | 57건 | 46건 |
| 사고당 피해자 수 | 167,051명 | 810,313명 | 376,998명 |
| 유·노출 건수 기준 Top 5 | -홈쇼핑업체 (260만건)<br>-홈쇼핑업체 (200만건)<br>-졸업앨범 제작업체 (100만여건)<br>-통신사(75만건)<br>-졸업앨범정보 사이트 (33만여건) | -포팅업체 (842만건)<br>-통신사(837만건)<br>-통신사(771만건)<br>-홈쇼핑업체 (570여만건)<br>-통신사(300만건) | -통신사(730만건)<br>-통신사(400만건)<br>-대출사이트 (231만건)<br>-통신사(190만건)<br>-통신판매업체 (74만건) |
| 주요 이슈 사건 | -리니지 사용자 id/ 비밀번호 유출<br>-개인정보 빼내 인터넷 뱅킹으로 5천만원 인출<br>-은행 피싱사이트 국내 첫 발견 | -리니지 명의도용<br>-국민은행 고객정보 첨부 이메일 발송<br>-초고속인터넷 가입자 정보 매매<br>-LG전자 입사지원서 유출 | -국민은행/농협 피싱사이트 발견<br>-엔씨소프트, 국민은행 소송 배상판결 |

※조사방법 : 2005~2007년 동안 언론에 보도된 사건들을 웹사이트 뉴스 검색을 통해 조사하였으며, 동일 사고는 1건으로 계산하고, 피해인원은 서로 다른 사고에 의해 피해당한 인원수를 합한 수치

과거 2000년대 초까지는 디스켓 등 저장매체를 통한 바이러스 전파에 의해 시스템 보호가 주요 이슈였으나, 2003년 1.25 인터넷 침해사고 이후에는 네트워크를 통한 웜 자동전파, 악성 봇을 통한 통신망 공격이 주를 이룸에 따라 네트워크 보호가 주된 관심사항이었다. 2005년 이후에는 금전적 목적의 개인정보

를 탈취하고 도용하는 범죄 성향의 공격이 주가 됨에 따라 개인정보보호 이슈가 크게 대두되었고 특히 국내에서는 2006년 2월 리니지 명의도용 사건 이후 개인정보보호에 대한 관심이 크게 증가하여 개인정보 침해사고에 대한 내용들이 언론에 자주 보도되었다. [표 1]과 같이 2006년도 이후에는 800만건 이상의 대용량 고객 DB가 유·노출 되어 개인정보 침해사고 1건당 피해자 수가 크게 증가한 것이 특징이다.

[표 2] '침해사고 대응비용' 산출을 위한 파라미터

| 구분 | 파라미터 | | 기준값 | 출처 및 근거 |
|---|---|---|---|---|
| 사고 공지 비용 | 이메일 공지 비용 | 담당자 시간당 평균임금 | 19,227원 | 컴퓨터 전문가 시간당 평균임금: 임금구조 기본통계 (노동부 2005, 2006). |
| | | 작업시간 | 6.43시간 | 표본에 의한 설문조사 결과 |
| | 웹 사이트 공지 비용 | 담당자 시간당 평균임금 | 19,227원 | 컴퓨터 전문가 시간당 평균임금: 임금구조 기본통계 (노동부 2005, 2006). |
| | | 작업시간 | 10.9시간 | 표본에 의한 설문조사 결과 |
| | 신문 공지 비용 | 건당 신문사 공지비 | 36,630천원 | 주요 신문사에 5단, 12칼럼 사죄광고를 1일 게재하는 비용 - 5단(1단: 3.4cm) ×12컬럼(1컬럼: 3.08cm) 크기 |
| | | 매체 수 | 3.48개 | 표본에 의한 설문조사 결과 |
| | | 기간 | 4.56일 | 표본에 의한 설문조사 결과 |
| 법률/ 포렌식 자문 비용 | 법률 자문료 | 변호사 시간당 자문료 | 400천원 | 서울지법 "로펌 1시간 자문료 40만원 정당" (한국경제신문, 2006.5.15) |
| | | 자문기간 | 14일 | 표본에 의한 설문조사 결과 |
| | | 변호사 수 | 2.18명 | 표본에 의한 설문조사 결과 |
| | 포렌식 자문료 | 컨설턴트 1일 임금 | 500천원 | 컴퓨터 포렌식 전문기관의 자문 |
| | | 자문기간 | 12.45일 | 표본에 의한 설문조사 결과 |
| | | 전문가 수 | 12.62명 | 표본에 의한 설문조사 결과 |
| 콜센터 운용 비용 | 상담원 투입 인원수 | | 18.9명 | 표본에 의한 설문조사 결과 |
| | 투입기간 | | 20.54일 | 표본에 의한 설문조사 결과 |
| | 상담원의 시간당 임금 | | 7,194원 | 텔레마케터가 속한 그룹인 산업지원 서비스업의 시간당 평균임금 사용 (노동부, 2005, 2006) |
| 보상 서비스 제공 비용 | 개인보상금 | | 5,000원 | 피해자에게 5,000원권 문화상품권을 지급하는 것으로 가정 (2004년도에 일본 야후 BB는 피해자 전원에게 500엔권 상품권과 사과문 발송) |
| | 우편 발송 비용 | | 360원 | 우체국의 대량 우편물 재작 발송비 (www.epost.go.kr) |

[표 3] '생산성 손실비용' 산출을 위한 파라미터

| 구분 | 파라미터 | 기준값 | 출처 및 근거 |
|---|---|---|---|
| 생산성 손실 비용 | 침해사고로 영향받은 직원수 | 10.8명 | 표본에 의한 설문조사 결과 |
| | 직원의 시간당 인건비 | 19,227원 | 컴퓨터 전문가 시간당 평균임금: 임금구조 기본통계 (노동부 2005, 2006). |
| | 긴급 대응업무 투입일 | 11.7일 | 표본에 의한 설문조사 결과 |

[표 2]~[표 3]은 기업의 손실비용 산출에 사용된 측정 항목들과 자료의 출처를 기입한 내용이다. 데이터로서 존재하는 값들은 출처를 밝힌 바와 같이 관련 자료를 참조하였고, 이메일 공지비율 등과 같이 데이터로서 존재하지 않는 값들은 주로 설문조사를 통해 확보되었다. 설문대상 기관은 종사자수 5인 이상이고 네트워크에 연결된 컴퓨터를 1대 이상 보유하고 있으며 개인정보를 수집하고 있는 전국의 모든 사업체를 대상으로 하였다. 업종별 규모별로 층을 나누어 2,800개의 사업체가 표본으로 선정되었고, '08년 11~12월 기간 동안 사업체 방문면접조사와 구조화된 웹 설문지를 이용한 온라인조사 방법이 병행되었다.

[표 4]~[표 5]는 설문에 응답한 표본의 업종별 구성 비율이다. 표본은 통계청에서 조사한 "사업체기초

[표 4] 업종별 표본 구성비율

| 구분 | 표본수 | 비율 |
|---|---|---|
| 농림수산업 | 80 | 2.9% |
| 제조업 | 388 | 13.9% |
| 건설업 | 281 | 10.0% |
| 도매업 | 276 | 9.9% |
| 소매업 | 298 | 10.6% |
| 숙박 및 음식업 | 199 | 7.1% |
| 운수 및 통신업 | 253 | 9.0% |
| 금융 및 보험업 | 255 | 9.1% |
| 부동산 및 임대업 | 341 | 12.2% |
| 기타 서비스업 | 429 | 15.3% |
| 계 | 2,800 | 100% |

〔표 5〕 규모별 표본 구성비율

| 구분 | 표본수 | 비율 |
|---|---|---|
| 5~9명 | 991 | 35.4% |
| 10~49명 | 1,068 | 38.1% |
| 50~249명 | 565 | 20.2% |
| 250명 이상 | 176 | 6.3% |
| 계 | 2,800 | 100% |

통계조사"와 한국정보사회진흥원에서 실시한 "2007년 정보화통계조사"를 바탕으로 업종별 규모별로 구분하였다. 특히 표본이 모집단의 특성을 잘 반영하도록 "2007년 정보화통계조사"에 있는 모집단의 업종별 규모별 분포 가중치를 각 표본에 적용하여 최종결과를 산출하였다[26].

잠재적인 법적 책임비용에는 손해배상금과 법령 위반에 의한 과태료의 계산이 필요하다. 2008년 6월에 개정된 정보통신망이용촉진및정보보호등에관한법률에 의하면 서비스 제공자가 적절한 조치를 하지 아니하여 이용자의 개인정보를 분실·도난·누출·변조 또는 훼손한 경우에 최고 3천만원까지 과태료를 부과할 수 있도록 되어, 개정 전 최고 1천만원에 비해 상향조정되었다. 또한 개정된 법률에는 과징금에 대한 내용이 추가되었기 때문에 향후에는 과징금 부분에 대한 내용도 고려될 필요가 있다. 그러나 과태료나 과징금은 과실여부에 대한 최종 결정에 따라 기업이 지불해야 하는 금액이고, 사고건당 지불하기 때문에 모든 피해자에게 지불해야 하는 손해배상금에 비해 상대적으로 미미하다. 따라서 본고에서는 손해배상금만을 잠재적인 법적 책임비용으로 추정하고자 한다.

현재 미국에서는 개인정보 침해사고 발생시 집단소송제가 적용되어 피해자 대표가 소송을 하면, 별도로 제외신고(Opt-out)를 하지 않는 한, 판결의 효력이 피해자 전체에 미치는 일괄구제 제도이다. 아직 우리나라에서는 재판을 받은 대표들만이 피해구제를 받는 선정당사자 제도로, 판결의 직접적인 효력이 이해당사자 전체에 미치지 않는다. 그러나 개인정보 침해사고 피해는 피해자 전원의 개인정보 가치가 손실된 것이므로 잠재적인 위험을 계량화하기 위해서는 반드시 피해자 전원에 대한 법적 보상금이 계산될 필요가 있다.

본고는 표면적으로는 나타나지 않는 잠재적인 위험에 대한 정량적 이해를 위해 피해자 전원에게 보상금을 지급하는 것을 가정하여 기업의 손실비용을 산출하였다. 기업에서 개인정보 유·노출 사고가 발생하면, 피해자 개인 모두가 잠재적인 2차 피해자가 될 수 있고 이에 따라 기업에서는 최대 모든 피해자에게 손해배상금을 지급할 가능성도 있다. 따라서 기업 입장에서는 최악의 상황을 고려해야 하기 때문에 피해자 전원에게 지급한다는 가정이 잠재적인 위험에 대한 손실의 총량을 산출하는 방법이다. 일본에서도 아직 집단소송제가 적용되고 있지는 않으나 JNSA(2007)의 연구에서도 위험의 정량적인 총량을 파악하기 위해 피해자 전원에게 손해배상금을 지급하는 것을 가정하여 산출하였다.

집단소송으로 인한 손해배상금을 추정하기 위해 〔표 6〕과 같이 대량의 DB가 유출된 사고의 판례에 초점을 맞추어 기준값을 정하고, 피해자 1인당 배상금액을 파라미터로 사용하였다. 〔표 2〕~〔표 3〕의 데이터를 기반으로 개인정보 침해사고로 인한 국내 기업의 연간 손실비용을 산출한 결과, 〔표 7〕와 같이 '05년도에는 약 1조 2천억원, '06년도는 약 6조 8천억원, '07년도에는 약 3조 1천억원으로 추정되었다.

〔표 6〕 '손해배상금' 산출을 위한 파라미터

| 구분 | | 기준값 | 근거 |
|---|---|---|---|
| 1인당 손해 배상금 | 주소, 전화번호, 이메일 등 주소정보 침해 | 100천원 | 서울고법 민사9부 (2007.11.27): 이메일 유출에 대한 판결 |
| | 주민등록번호 등 ID 정보 침해 | 200천원 | 서울고법 민사9부 (2007.11.27): 주민번호 유출에 대한 판결 |
| | 결제 내역, 거래 내역, 카드번호, 신용정보 등 금융정보 침해 | 300천원 | 개인정보분쟁조정 사례(2007): 금융정보 도용에 대한 조정결과 |
| | 자기소개서, 이력서, 일기장, 범죄사실, 의료기록 등 민감성 정보 침해 | 700천원 | 서울중앙지법 민사합의10부 (2008.1.3): 입사지원서 노출에 대한 판결 |

모든 피해자에게 손해배상을 한다는 가정하에 산출되었기 때문에 개인정보 침해사고에 의해 기업이 입게 되는 경제적 손실비용은 잠재적인 손해배상금이 총 손실의 약 99% 정도로 대부분을 차지하였고, 그 절대금액도 매우 큰 것으로 나타났다. 따라서 잠재적인 위험을 고려하면 기업은 대용량 고객 DB의 유·노출에 의해 파산에 이를 수 있다는 경각심을 가질 필요가 있다. 또한 최근 추진 움직임이 있는 집단소송제에 대한 대비를 위해서라도 기업은 고객 개인정보에 대한 철저

〔표 7〕 개인정보 침해사고로 인한 손실비용

(단위 : 억원)

| 구분 | | 2005년 | 2006년 | 2007년 |
|---|---|---|---|---|
| 1) 침해사고 대응비용 | 사고 공지비용 | 63 | 88 | 71 |
| | 법률/포렌식 자문비용 | 15 | 21 | 17 |
| | 콜센터 운영비용 | 3 | 5 | 4 |
| | 보상서비스 제공비용 | 49 | 328 | 123 |
| | 소계 | 130 | 442 | 215 |
| 2) 생산성 손실 비용 | | 7 | 11 | 9 |
| 3) 잠재적인 손해배상금 | | 12,194 (98.9%) | 67,292 (99.3%) | 30,429 (99.3%) |
| 총 피해액 | | 12,331 | 67,745 | 30,653 |

한 관리 대책을 마련하는 것이 필요하다.

〔표 8〕은 잠재적인 손해배상금에 대한 상세내역을 분석한 결과이다. '05년도 대비 '06년도 비용이 큰 폭으로 증가한 이유는 대용량 고객DB가 유출된 건수가 많아 사고 1건당 피해 인원수가 크게 증가하였기 때문인 것으로 분석된다. '07년도는 '05~'06년도에 비해 상대적으로 금융결제내역, 카드번호 등과 같은 개인 금융정보와 자기소개서, 이력서, 범죄사실 등과 같은 민감성 정보의 유출이 많아진 것이 특징이다. 그러나 '07년도 전체 피해인원은 '06년도에 비해 상대적으로 감소하여 전체 손실비용은 감소한 것으로 분석된다. '07년도에 금융정보, 민감성 정보 등과 같은 개인정보의 유·노출이 상대적으로 증가하는 것을 보면, 향후에는 민감도가 높은 개인정보의 유·노출에 의한 기업의 손실비용은 더 크게 증가할 것으로 예상된다.

## 4.2 일본의 피해액 산출값과의 비교

JNSA(2007)의 연구자료에 의하면 〔표 9〕와 같이 개인정보 침해사고로 인한 일본 기업의 연간 손실비용은 '05년도 약 6조 5천억원, '06년도 3조 7천억원으로 추정되었다[7-9].

일본에서는 2003년 5월에 참의원 본회의에서 '개인정보의 보호에 관한 법률'이 가결되었고, 2004년도 '개인정보보호의 기본방침'이 실행되어 국가, 자치단체 및 개인정보 취급사업자가 개인정보보호를 위한 조치를 강구하도록 하였으며, 2005년 4월에는 '개인정보의 보호에 관한 법률'이 전면적으로 시행되었다[25]. 이러한 제도적 조치에 의해 개인정보 침해 사안에 대한 명백한 단속 근거가 확립되고, 사고에 대한 공지를

〔표 8〕 잠재적인 손해배상금 상세분석

| 침해정보 구분 | | 주소 정보 | 주민번호 | 금융 정보 | 민감성 정보 | 합계 |
|---|---|---|---|---|---|---|
| '05 | 사고 수 (건) | 11 | 20 | 8 | 2 | 41건 |
| | 피해인원 (명) | 4,108,662 | 136,057 | 2,603,667 | 702 | 6,849,088명 |
| | 비용 (억원) | 4,106 | 272 | 7,811 | 5 | 12,194억원 |
| '06 | 사고 수 (건) | 10 | 39 | 6 | 2 | 57건 |
| | 피해인원 (명) | 26,230,203 | 18,825,306 | 1,128,704 | 3,601 | 46,187,814명 |
| | 비용 (억원) | 26,230 | 37,651 | 3,386 | 25 | 67,292억원 |
| '07 | 사고 수 (건) | 7 | 14 | 14 | 11 | 46건 |
| | 피해인원 (명) | 6,712,103 | 8,188,553 | 2,437,113 | 4,118 | 17,341,887명 |
| | 비용 (억원) | 6,712 | 16,377 | 7,311 | 29 | 30,429억원 |

〔표 9〕 일본 개인정보 침해사고의 손해배상금 추이

| 구 분 | 2002년 | 2003년 | 2004년 | 2005년 | 2006년 |
|---|---|---|---|---|---|
| 총 피해액 (연평균 환율적용) | 18,922백만¥ (1,891억원) | 28,069백만¥ (2,890억원) | 466,693백만¥ (4조 9,412억원) | 700,179백만¥ (6조 5,163억원) | 456,584백만¥ (3조 7,508억원) |
| 총 피해 인원 | 419천명 | 1,555천명 | 10,435천명 | 8,815천명 | 22,237천명 |
| 사고 발생 수 | 62건 | 57건 | 366건 | 1,032건 | 993건 |
| 1인당 평균 피해액 | 452천원 | 186천원 | 474천원 | 739천원 | 170천원 |

〔표 10〕 연도별 개인정보 침해사고 관련 한일 법적 보상금 비교

| 구분 | 2005년 | | | 2006년 | | |
|---|---|---|---|---|---|---|
| | 한국 | 일본 | 비율(한국/일본) | 한국 | 일본 | 비율(한국/일본) |
| 총 피해액 | 1조 2천억원 | 6조 5천억원 | 19% | 6조 7천억원 | 3조 8천억원 | 179% |
| 총 피해 인원 | 6,849천명 | 8,815천명 | 78% | 46,188천명 | 22,237천명 | 208% |
| 사고 발생 건수 | 41건 | 1,032건 | 4% | 57건 | 993건 | 6% |
| 일인당 피해액 | 178천원 | 739천원 | 45% | 146천원 | 169천원 | 86% |

제도적으로 의무화함에 따라 2004년 이후에 사고발생 건수가 크게 증가한 것으로 판단된다. 이와 같이 개인정보보호 법률 제정 및 시행은 연도별 개인정보 침해사고 피해 발생 추이에도 영향을 주고 있는 것으로 분석된다.

특히 '05년도 대비 '06년에는 대형 DB 유·노출 사고 발생에 의해 피해 인원이 크게 증가하였음에도 불구하고, 민감한 정보의 침해사고가 줄고 상대적으로 단순한 정보의 침해사고 증가로 인해 손실비용이 크게 감소한 것으로 JNSA(2007)의 연구는 분석하였다〔12-14〕. 이러한 점에 볼 때 일본에서는 개인정보보호법에 의해 기업이 지켜야할 의무사항이 제도화됨에 따라, 초기에는 사고 공지의무로 인해 사고발생건수가 증가하여 손실규모도 증가하였으나, 점차 기업내 개인정보에 대한 관리가 보다 엄격해짐에 따라 민감하고 중요한 개인정보의 유·노출의 감소로 이어져 전체 손실규모는 감소하는 것으로 분석된다.

〔표 10〕은 연도별 개인정보 침해사고 관련 기업의 연간 손해배상금 비용을 일본의 사례와 비교한 자료이다. '05년도 국내 기업의 비용은 일본의 1/5 수준이나 '06년도는 일본의 1.8배 수준으로 상대적으로 크게 증가하였다. 또한 '05년도는 국내 피해자 수는 일본의 78% 수준이나, '06년도에는 총 피해자수가 일본의 2배에 이른다. 사고 발생 건수가 일본에 비해 현저히 낮은데도 이러한 현상을 보이는 것은 우리나라가 한 번의 사고로 인해 많은 피해자가 양산되는 대용량 고객 DB 유·노출이 상대적으로 많았다는 것을 보여준다.

일본은 2003년에 개인정보보호법이 제도화되어 사고 발생시 공지 의무사항으로 인해 사고발생 건수는 증가하고 있으나, 기업의 손실비용은 상대적으로 감소하는 현상을 볼 때, 2004~2006년도를 거쳐 개인정보보호에 대한 제도가 점차 정착화되고 있다고 판단된다. 이에 반해 우리나라는 2006년도 이후에 개인정보보호 문제가 크게 대두되었으나 아직 제도적 뒷받침이 미흡하다. 이러한 사실은 2008년도에 들어와 쇼핑몰, 정유사 등에서 이전보다 더 방대한 대용량 DB 유출사고로 이어지고 있는 우리의 현실을 볼 때 우리에게 시사하는 바가 크다고 할 것이다.

## V. 결 론

본고에서는 기업에서 발생하는 개인정보 유·노출 사고로 인한 기업의 손실비용을 다각도로 분석하고, 그의 규모를 산출할 수 있는 방법을 제시하였다. 지금까지 계량경제학적인 방법에 의한 시도가 있었으나 국내에서는 처음으로 실무자 관점에서 쉽게 활용할 수 있는 방법론을 제시했다는 점에서 의미가 크다고 할 수 있다. 특히, 개인정보 침해사고로 인한 손실을 정의하고 단순화하여 객관적으로 추정할 수 있는 방법론을 제시함을 통해 기업체 뿐만 아니라 공공기관 등에서도 내부 자체적으로 충분히 활용될 수 있을 것으로 보인다.

그러나 본고에서 제시한 방법론은 조직 내에서 객관적으로 활용될 수 있는 장점이외에도 몇 가지 한계점을 가지고 있다. 첫째, 산출된 모형은 개인정보 침해사고로 인한 직접적인 손실비용만을 다루고 있어, 사고로 인한 기업의 이미지 손상과 주가하락 등과 같은 간접적인 비용은 고려하고 있지 않다는 점이다. 기업에게는 직접적인 손실에 비해 간접적이고 파생적으로 나타나는 2차 손실도 중요하다. 따라서 향후에는 기업의 이미지 손상, 주가하락, 고객이탈에 의한 매출하락 등과 같은 2차적인 손실에 대해서도 원단위 접근법을 통해 측정할 수 있는 방법론 연구를 통해 이를 보완하고자 한다.

둘째, 침해사고 대응비용과 생산성 손실 비용을 산출하기 위해 단 한 번의 설문조사 결과를 활용하고, 손해배상금 산출을 위해 최근 판례를 적용하였으나, 이에 대한 객관적인 타당성을 입증하는 것이 필요하다는 점이다. 따라서 향후에는 오랜 기간 동안 설문조사 결과를 주기적으로 측정하고 다양한 판례 사례를 조사

함으로써 연구에 대한 타당성을 증명하는 시도를 진행할 예정이다.

개인정보 침해사고로 인한 손실액을 정량적으로 산출하는 연구는 개인정보가 갖는 가치를 간접적으로 측정하는 방안으로서, 개인정보를 안전하게 관리하기 하기 위해 적절한 보안 조치를 해야 한다는 경각심을 기업들에게 인식시켜 줄 수 있을 뿐만 아니라, 개인정보 침해사고 예방을 위한 합리적인 투자규모를 도출하기 위한 기초자료로 활용될 수 있을 것으로 기대된다. 특히, 조직 내에서 침해사고로 인한 손실규모를 정량적으로 산출하는 일은 위험관리 측면에서 정보보호 투자대비 효과(ROI) 분석의 기초자료로 활용되어 조직의 내부 보안전략수립에 활용될 수 있을 것으로 기대된다.

일본은 이미 2005년 4월부터 개인정보보호법의 전면적인 시행을 통해 기업의 개인정보 유출 금지 및 2차적인 피해를 방지하기 위한 관련 정보의 공개 등을 의무화하였다. 이에 따라 기업은 정보유출 사실을 숨기기보다 공개하는 것이 소비자의 신뢰를 얻는데 도움이 된다는 인식을 갖게 되었고, 그 결과 개인정보 침해사고의 보도 건수는 증가하였다. 그러나 기업내 개인정보 관리가 보다 철저해짐에 따라 민감하고 중요한 개인정보의 유·노출이 줄어 전체적인 손실비용은 감소하고 있는 것으로 나타났다.

우리나라도 이러한 제도적 장치를 신속히 마련하여 조직의 운영 리스크 중에서 대단히 중요한 요소로서 기업이 개인정보 침해사고를 관리하도록 할 필요가 있다. 이를 통해 기업 내에서 개인정보 유출을 막을 수 있는 방안들이 마련되어야 하며, 개인정보보호를 위한 다양한 활동들이 활발히 이루어지도록 해야 할 것이다.

## 참 고 문 헌


[1] 한국정보보호진흥원, 정보보호 포털 사이트, http://www.securenet.or.kr

[2] 한국정보보호진흥원, "정보통신망 이용촉진 및 정보보호 등에 관한 법률," 정보통신·정보보호 법령집, pp. 2-3, 2006년 9월.

[3] 정부혁신지방분권위원회, "개인정보관리현황조사계획," 2004년 1월.

[4] R.J. Weible, Privacy and Data, doctoral dissertation, Mississippi State Univ., 1993.

[5] 김여라, 이해춘, 유진호, "가상가치접근법(CVM)을 활용한 개인정보보호의 가치 산출 방법론 고찰," 정보보호 이슈리포트, 한국정보보호진흥원, pp. 1-22, 2007년 2월.

[6] L.A. Gordon and M.P. Loeb, Managing Cybersecurity Resources: A Cost-Benefit Analysis, McGraw-Hill Companies, Inc., Sep. 2005.

[7] 유진호, 지상호, 송혜인, 정경호, 임종인, "인터넷 침해사고에 의한 피해손실 측정," 정보화정책, 15(1), pp. 3-18, 2008년.

[8] 유진호, "개인정보 유출 회피를 위한 지불의사액 추정," 한국정보보호진흥원 정보보호심포지움 발표자료, 2007년 6월.

[9] 유승훈, 곽승준, 신철오, "스팸메일의 불편 비용 추정," 정보통신정책연구, 정보통신정책학회, 10(1), pp. 71-93, 2003년 6월.

[10] 이해춘, 안경애, "CVM을 이용한 개인정보 유출의 손실 가치 분석," 생산성 논문집, 22(2), pp. 1-24, 2008년 1월.

[11] 김상봉, 공공투자분석, 세창출판사, 2009년 3월.

[12] JNSA(일본네트워크시큐리티협회), "2006년 정보보안사고에 관한 조사보고서," pp. 1-50, 2007년 10월.

[13] JNSA(일본네트워크시큐리티협회), "2006년 개인정보유출사고 조사결과," pp. 1-15, 2007년 6월.

[14] JNSA(일본네트워크시큐리티협회), "2005 Information Security Incident Survey Report, Information Leakage: Projected Damages and Observations," pp. 4-50, July 2006.

[15] PGP Corporation and Vontu, Inc., 2007 Annual Study: Cost of a Data Breach, Nov. 2007.

[16] PGP Corporation and Vontu, Inc., 2006 Annual Study: Cost of a Data Breach, Oct. 2006.

[17] Privacy Rights Clearinghouse, http://www. privac yrights.org

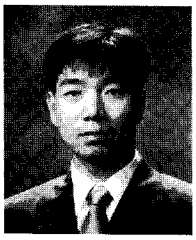
[18] 서승우, 보안경제학, 서울대학교 출판부, 2008년 5월.

[19] 김정덕, 최광희, "정보보안사고 비용산정을 위한 개념적 모델," 산업경영연구, 9(1), pp. 23-44, 2000년.

[20] K. Campbell, L. Gordon, M. Loeb, and L. Zhou, "The Economic Cost of Publicly Announced Information Security Breaches:

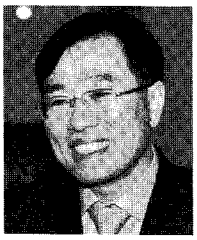
Empirical Evidence from the Stock Market," Journal of Computer Security, vol. 11, no. 3, pp. 431-448, 2003.
[21] H. Cavusoglu, B. Mishra, and S. Raghunathan, "The effect of Internet security breach announcements on market value: capital market reactions for breached firms and Internet security developers," International Journal of Electronic Commerce, vol. 9, no. 1, pp. 69-104, 2004.
[22] 남상훈, "기업 정보보호 투자효과 분석방법에서 보안 Event 가 주식가격에 미치는 영향 실증연구," 박사학위논문, 고려대학교, 2005년 12월.
[23] 권영옥, 김병도, "정보보안 사고와 사고방지 관련 투자가 기업가치에 미치는 영향," Information System Review, 9(1), pp. 105-120, 2007년 4월.
[24] N. Weaver and V. Paxson, "A Worst-Case Worm," Third Annual Workshop on Economics and Information Security (WEIS), pp. 1-12, May 2004.
[25] 채승완, "일본의 개인정보보호체계와 개인정보의 경제적 가치," 한일경상논문집 38권, pp. 1-25, 2007년 10월.
[26] 한국정보보호진흥원, "2008 정보보호 실태조사-기업편," pp. 10-20, 2008년 12월.

## 〈著者紹介〉



유 진 호 (Jinho Yoo) 종신회원
1992년 2월: 고려대학교 수학과 학사
1994년 2월: 고려대학교 통계학과 석사
2006년 3월 ~ 2008년 2월: 고려대학교 정보경영공학전문대학원 박사수료
1993년 11월 ~ 1999년 12월: 한국전자통신연구원 기술조사팀 연구원
2000년 1월 ~ 2004년 9월: 한국IBM 차장
2004년 10월 ~ 현재: KISA 홍보전략팀장
〈관심분야〉 정보보호정책, 정보보호경제성 분석, 정보보호관리

지 상 호 (Sangho Jie) 정회원
1991년 2월: 고려대학교 통계학과 학사
1993년 6월: Univ. of Minnesota at Twin Cities 수학과 석사
1995년 11월: Univ. of Minnesota at Twin Cities 통계학과 박사 수료
1998년 9월 ~ 2002년 12월: Statistical Clinic 컨설턴트(U of MN, TC)
2003년 8월 ~ 현재: KISA 조사분석팀장
〈관심분야〉 정보보호정책, 정보보호경제성 분석, 정보보호관리 인력양성



임 종 인 (Jongin Lim) 종신회원
1986년 2월: 고려대학교 대학원 수학과 박사(암호학)
2000년 8월: 고려대학교 정보보호대학원/CIST 원장(센터장)
2004년 1월: 국가정보원 정보보호정책 자문위원
2005년 7월: 대통령 자문 전자정부 특별위원
2005년 12월: 국회 과기정위원회 정보통신정책 자문위원
〈관심분야〉 정보보호기술, 정보보호정책, PET, 컴퓨터 포렌식