www.calsec.or.kr
http://dx.doi.org/10.7838/jsebs.2013.18.1.001

개인정보 유출이 기업의 주가에 미치는 영향

Analyzing Effects on Firms' Market Value of Personal Information Security Breaches

김정연(JeongYeon Kim)*

초 록

온라인 환경에서 개인정보의 사용 빈도가 많아짐과 동시에 제 3자에 의한 개인정보 수집 및 저장의 가능성도 높아지고 있다. 인터넷 서비스 제공에 사용되는 개인정보는 본인이 원하지 않는 용도로 사용되나 타인에게 유출되는 경우 뜻하지 않는 추가피해를 불러올 수 있다. 비록 개인정보 관리 제도의 개선이 이루어지고 있으나 여전히 개인정보의 유출 사례를 주변에서 손쉽게 찾아볼 수 있다. 개인정보보호에 관한 보다 합당한 투자 근거를 제시하기 위해서는 개인정보 유출로 인해 발생될 수 있는 피해의 측정이 선행되어야 한다.

본 논문은 해당 측정 방법의 하나인 개인정보 유출을 겪은 기업의 주가 변화를 측정하여 개인정보보호법 시행 이전보다 개인정보 보안과 관련한 인식이 개선되었는지 검증한다. 실증분석의 결과는 제도적 개선이 이루어지고 있음에도 불구하고 자본시장에서의 개인정보 유출로 인한 피해 인식은 크게 변화되지 않고 있음을 확인해 주고 있다. 여전히 주기적으로 발생하는 정보 보안 사건의 적극적 예방을 위해서는 그 피해액의 산정에 있어 개인의 추가 피해 가능성을 광범위하게 인정하는 전향적인 태도와 함께 피해 배상에 대한 의무를 명확히 인식할 수 있도록 추가적인 개선이 선행되어야 할 것으로 판단된다.

ABSTRACT

With the increases of requirement for user identification in Internet services, we should let the service companies know my personal information. If the shared personal information with them are used in not-allowed area or delivered to un-authorized persons, we may have practical harms in several fields such as financial related operations. Korean Government has introduced new management method for personal information, but it is not hard to find the personal information management issues from Korean news papers. The proper measurement should be delivered to related companies to help them to decide investment for security.

This paper review the indirect measurement method of demages by check the stock prices of related company for personal information management issue. We check the relationship between change of stock price and the information management issue. The result shows there are no changes in stock market. Korean government added strong regulations for personal information management though. To prevent further personal information issues, we should recognize the indirect damages properly and let the company pay higher reparations for any personal information abuse.

키워드 : 개인정보, 보안, 피해 측정, 주가 변동, 배상금, 사건연구
Personal Information, Security, Damage Measurement, Stock Price Change, Reparation, Event Study

본 연구는 2012학년도 상명대학교 교내연구비를 지원받아 수행하였음.

* Corresponding Author, College of Business Administration, Sangmyung University (E-mail : jykim@smu.ac.kr)

2013년 02월 09일 접수, 2013년 02월 14일 심사완료 후 2013년 02월 16일 게재확정.

1. 서 론

2000년대 이후 지속적인 발전을 보인 인터넷 응용 분야로 인해 특정 개인을 식별하기 위한 개인정보의 이용도 증가하고 있다. 행정안전부에서 실시한 2011년 정보화 통계조사에 따르면 홈페이지 보유 사업체 26만 8천여 개 중 홈페이지 방문자의 개인정보를 수집하고 있는 사업체의 비율이 2010년 47.0% 12만 6천여 개로 추정되어 2008년의 35.7%에 비해 11.3% 증가한 것으로 조사되었다. 그러나 온라인 과금이나 기타 정보서비스 제공 목적을 위한 개인정보 이용의 꾸준한 증가는 필연적으로 제 3자에 의한 정보의 수집과 저장을 유도한다.

협의의 개인정보는 생존하는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(개인정보보호법 제2조) 또는 특정한 개인을 알아볼 수 있는 부호, 문자, 음성, 음향 및 영상 등의 정보(정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조)로 정의할 수 있다. 두 조항 모두 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 항목을 포함한다. 그러나 보다 포괄적 의미로는 본인의 의사에 반하거나 본인이 알지 못하는 상황에서 타인에 의해 이용될 경우 당사자의 안전과 이해관계에 영향을 미칠 수 있는 모든 정보는 개인정보에 포함될 수 있다.

본질적으로 기업이 수집, 보관하고 있는 개인정보는 기업의 자산이기 이전에 정보제공자의 사적 재산이다. 개인정보에 대한 개인의 권리는 자신의 정보가 타인에 의하여 수집되지 않도록 하는 소극적 의미의 정보통제권과 자기정보 열람청구권, 자기정보 정정 및 보완 청구권과 같은 적극적 의미의 정보통제권을 함께 포함한다. 이를 고려하면 기업의 대규모 개인정보 수집 현상은 정보 소유 기업에 의해 본인이 허용하지 않은 부정적 용도로의 사용을 규제하는 문제나 소유권의 허용 문제와 같은 논쟁을 일으킬 수 있다. 또한 개인의 정보를 위탁 받은 기업으로부터 해당 정보가 유출된 경우에는 관리 기업의 경제적 손실 뿐 아니라 해당 개인의 유무형의 피해를 함께 야기할 수 있다. 특히 전자 상거래와 같이 사이버 공간 상에서의 경제활동의 경우에는 상거래 업체에 대한 신뢰가 고객 확보에 매우 중요한 요인으로 작용한다. 정보 보안에 취약한 인터넷 기반의 전자상거래에 대한 소비자의 우려를 불식시키고 해당 서비스 제공 기업의 신뢰도를 제고하기 위한 공적 관리가 반드시 필요하다[9]. 개인화 서비스 혹은 마케팅 기법의 발달로 인해 개인정보의 수집 노력이 광범위하게 이루어지고 있는 현실에 비추어 개인정보의 관리 문제는 정보제공자와 관리 기업의 사적 재화이면서도 사회전체가 관리 보호해야 하는 공공재이기도 하다[17].

이러한 맥락에서 2011년 개정 시행된 개인정보보호법은 기존의 '공공기관의 개인정보보호에 관한 법률'을 넘어 공공, 민간 통합 규율로 법적용 대상이 확대 되었으며, 개인정보 수집, 이용, 제공, 파기 등 처리단계별 공통된 보호기준과 원칙을 제시하고 있다. 더불어 개인정보 유출이나 오·남용시 국민의 권리 구제도 크게 확대되게 되어 개인정보피해를 구제하기 위한 개인정보 침해 신고센터와 개인정보분쟁 조정위원회를 운영하고 있다.

이와 같이 개인정보보호를 위한 제도적인 보완이 대폭 이뤄졌지만 여전히 유사시 피해자들의 적절하게 피해를 구제받는 장치가 마련됐는지에 대해서는 논란이 많다.

본 논문은 개인정보보호에 관한 제도적 보완이 실제 시장 참여자의 개인정보보호 인식에 영향을 미치고 있는지를 살피기 위해 개인정보가 유출된 기업의 초과 수익률을 사건연구방법론을 이용하여 관측한다. 또한 이를 기존 연구 결과와 비교하여 실제 개인정보 유출 사고로 인한 기업 가치의 변화가 축소 혹은 확대되는지를 살핀다.

2. 선행연구

개인의 사적 정보 보호와 관련하여 우선 국내의 실제 개인정보 유출 및 피해구제 사례를 살펴보면 다음과 같다. 대통령 소속 개인정보보호위원회에 따르면 개인정보 침해 신고는 2007년 847건에서 2011년 2556건으로 급증하고 있고 상담 건수도 2007년 2만 5118건에서 2011년 11만 9659건으로 5배 이상 증가했다. 개인정보보호법 시행에 따라 정보 주체들의 권리보호를 위한 의식은 높아지고 있다. 그럼에도 불구하고 방송통신위원회에서 실시한 2011년 정보보호 실태조사에 따르면 사업체의 62.6%가 2010년 1년간 정보보호에 대한 지출이 없었던 것으로 조사되어 기업의 내부 보안대책 마련, 보안투자 등은 상대적으로 소홀한 것으로 나타났다.

이와 같이 국내기업이 개인정보보호 관련 투자에 소홀한 원인은 개인정보 유출과 관련된 집단소송의 결과에서도 쉽게 찾을 수 있다. 최근 해킹에 의한 개인정보 대규모 유출 사례로는 2008년 1월 옥션(1,800만 건), 2011년 3월 신세계몰(390만 건), 2011년 4월 현대캐피탈(175만 건), 2011년 7월 SK커뮤니케이션즈(3,500만 건), 2011년 8월 한국엡손(35만 건), 2011년 11월 넥슨(1,320만 건) 등을 들 수 있다. 개인정보 유출의 피해 규모를 산정하기 위해서는 민간 기업의 실질적 손실비용과 복구비용을 측정하는데 그치지 않고, 나아가 고객의 손실과 사회적 파급 효과 등의 경제적 피해 규모를 함께 고려하여야 한다.

그러나 현재까지 종업원에 의해 의도적으로 관련정보를 사외로 빼돌린 경우를 제외하면 개인정보 유출과 관련된 국내의 집단소송에서 원고가 승소한 판례는 없다. 제기된 사용자들의 집단소송은 피고인 기업의 과실이라고 볼 수 없어 손해배상의 책임이 없다는 판결로 마무리되었다. 지난 몇 년간의 개인정보 유출 관련 집단소송 판결은 대부분, 사업자가 해킹 방지 의무를 다하였으며, 유출된 개인정보가 원고들에게 어떤 피해를 입혔는지 입증하기 어렵다는 이유로 원고 패소했다. 또한 옥션, GS칼텍스, SK컴즈, 넥슨 등의 경우에는 모두 법에서 규정하는 조치를 모두 취했기 때문에 해당 기업은 형사 처분 역시 받지 않았다.

2006년 미국의 신용정보제공회사인 초이스포인트사가 16만 3천 명의 개인재무정보 유출과 함께 해당 정보가 위조신용카드 제작 등에 사용된 점이 인정되어 미국 연방거래위원회(FTC)로부터 1000만 달러의 벌금과 500만 달러에 달하는 관련자 배상 지불을 합의한 내용과는 사뭇 다른 결과이다. 일본의 경우에도 소프트뱅크의 800만 명의 개인정보

유출로 인해 개인당 500엔, 총 40억 엔의 손해배상금을 지불한 사례가 있다.

이와 같이 개인정보의 오용, 유출과 같은 상황에 대해 사회 구성원들이 자신의 권리를 인정받기 위해 많은 문제를 제기하고 있지만 재발 방지를 위한 투자가 미진하고 이에 대한 피해구제가 어렵다. 그 이유로는 우선 1차적인 개인정보의 유출로 인해 발생될 수 있는 2차적 피해가 입증되기 어렵다는 점을 들 수 있다. 개인정보 유출 피해의 측정 문제와 정보보호 투자의 효과 측정 문제와 관련한 선행 연구는 아래와 같다.

일본 IPA(2001)는 '정보보안 사고에 관한 조사'에서 인터넷 침해사고로부터 보호해야 할 대상과 그 사고로 인한 피해의 구성요소로 침해사고를 정의하였다. 보안 사고에 의한 피해의 구성요소를 컴퓨터 바이러스에 의한 피해, 제3자에 의한 부정 액세스, 내부 범죄 등에 의한 정보유출 등으로 구분하였다. 이에 따르면 개인정보 유출은 기업이 보유하고 있는 개인정보를 허가받지 않은 내/외부인의 액세스를 통해 기업 외부로 빠져나가는 것으로 정의될 수 있다. 보안 사고 피해 측정 관련 연구들은 정보보안 사고를 보유하고 있는 자료의 손상 혹은 파괴를 동반한 물리적 1차 피해와 자료의 손실이나 유출로 인한 2차적 피해로 구분하고, 간접적 피해가 파급효과가 큼에도 불구하고 비가시적이고 측정이 쉽지 않다는 점으로 인해 중요성이 간과되고 있다고 지적하고 있다.

정보유출의 직간접 폐해의 측정을 위해 다양한 방법론이 제시되고 있지만[3, 4, 8, 16, 17] 가장 보편적인 방법론으로는 Gordon, Loeb[6]가 제시한 정보보호 침해사고와 관계된 비용(Cost)과 편익(Benefit) 분석 방법론이 있다. 특히 침해사고 피해유형을 크게 비밀성, 가용성, 무결성이 상실된 것으로 나누고, 침해사고 피해로부터 발생하는 비용을 직접비용(Direct Costs)과 간접비용(Indirect Costs), 명시적 비용(Explicit Costs)과 잠재적 비용(Implicit Costs)으로 구분하여 침해사고 피해액을 산출할 것을 제시하고 있어 다양한 정보 유출 피해를 일관성 있게 정의할 수 있는 점이 특징이다[12]. 개인정보 침해사고는 기업의 비밀성 정보가 상실된 경우로 손실비용 산출모형을 적용할 수가 있다. 다만 개인정보 유출로 인해 발생될 수 있는 간접적 피해의 양상이 너무도 다양하고 정보 기술의 추가와 더불어 새로운 내용이 추가되고 있어 그 세부적인 내용까지 일반화하는 것은 무리가 따를 것으로 예측된다.

마지막으로 정보보안사고로 인해 발생되는 직간접적 피해를 산출하기 보다는 자본시장에서의 시장가치 변경을 통해 추정하기 위한 연구도 진행되었다. Ettredge, Richardson[5]는 사건 연구 방법론을 통해 DoS 공격이 자본시장에서 기업 가치에 영향을 미치는 지를 검증하였다. 이를 통해 보안사고가 인터넷 관련 기업에 미치는 영향이 전통 산업보다 크게 나타남을 실증하였다. Cavusoglu, Mishra, Raghunathan[2]는 1996~2001 동안의 보안사고에 대해 사건 연구 방법론을 적용하여 사건 발생 이틀 동안 평균적으로 해당 기업의 주가에 -2.1%에 이르는 초과수익률을 나타내고 있음을 보였다.

국내의 연구로는 권영옥, 김병도[11]이 동일한 방식의 시장가치의 변화를 2001~2005 Q1 기간 동안 측정하고, 그 영향력이 사건발

표 시점에 시장가치 대비 -0.86%의 영향에 그치고 있다고 하였다. 남상훈[7]은 기업의 보안 이벤트가 주식가격에 미치는 영향으로 정보보호 투자효과를 대체함으로써 정보보호 투자로 인한 가치 창출 효과를 측정, 투자 기준으로 삼을 것을 제안하였다.

3. 연구 설계

3.1 연구가설의 설정

선행연구에서 언급한 바와 같이 국내의 자본시장은 정보 보안 사고에도 미국의 사례에 배해 비교적 미미한 반응을 나타내고 있다[11]. 이와 같은 현상은 국내 기업의 보안사고 방지를 위한 투자 현황이나 보안사고 이후의 집단소송 결과에서도 그 중요성을 상대적으로 인정받고 있지 못하는 현상과 일맥상통한다. 국내의 경우 인터넷 사용이 급격히 늘어난 2000년대 이후 개인정보 유출사건이 지속적으로 반복되고 있으며 이에 대한 대비책 역시 사회적인 관심이 늘어났다. 개인정보보호법의 시행과 홍보로 인터넷 사용자의 개인정보에 대한 권리 의식이 크게 향상되고 기업의 의무가 크게 강화되고 있음을 감안하면 추후 개인정보 유출 사건은 국내 기업의 시장가치에 여전히 부정적인 영향을 미칠 것으로 예상할 수 있다.

가설 1 : 개인정보 유출사건은 최근에도 기업가치에 음의 영향을 미친다.

그러나 개인정보보호법의 시행 이후 변화가 예상되고는 있지만, 여전히 개인정보 유출로 인한 2차 피해에 대한 입증 의무를 피해자가 갖는 국내 현실과 개인정보 유출 사고가 반복되고 있는 상황을 고려하면, 관련 위험이 이미 자본시장에 반영되어 추가적인 시장의 반응을 기대하기 어려운 측면도 있다. 국내 사용자의 개인정보가 이미 공공연한 매매의 대상이 되고 있는 시점에서 단순한 개인정보의 1차 유출만으로 기업 가치에 심각한 타격이 나타나리라고 기대하는 것은 무리가 따른다. 특히나 최근에 나타나고 있는 개인정보 유출 사고는 많은 정보를 축적해 놓은 대기업에서도 자주 발생하고 있는 점과 동일한 기업이 반복적으로 개인정보를 노출시키는 경우에도 추가적인 제재가 뒤따르고 있지 않은 점은 시사하는 바가 크다. 이는 최근 2000년대 중반에 유사한 사건이 주로 소규모 인터넷 기업에 미치는 영향[1]에 비하여 개별 기업의 가치에 미치는 영향을 오히려 축소시키게 될 것이다.

가설 2 : 개인정보 유출로 인한 기업가치의 감소는 최근 선행 연구 결과 대비 축소되었다.

3.2 연구가설의 검증 모형

언급한 바와 같이 본 논문은 개인정보 유출 사건이 기업 가치에 미치는 영향을 측정하기 위해 사건 연구 방법론을 활용한다. 사건 연구란 개별 기업과 관련된 정보가 공표된 후 시장에서의 기업가치에 어떠한 변화를 가져오는 지를 측정하는 방법이다. 시장에서의 기업가치를 측정하는 방법으로는 일반적

으로 초과 수익률을 사용한다.

$$A_{it}^{*} = R_{it} - E[R_{it}] \quad (1)$$

단, A_{it} : 기업 i의 시간 t의 초과 수익률
R_{it} : 기업 i의 시간 t의 실제 수익률 (사건 Xt가 발생하기 전후)
$E[R_{it}]$: 사건 Xt가 없다고 가정한 기업 i의 기대 수익률

식 (1)에서 사용되는 기대 수익률은 일정 기간 동안의 시장 평균 수익률과 기업 i의 실제 수익률 사이의 회귀분석을 통해 예측한다. 이를 위해 아래 식 (2)를 사용한다.

$$R_{it} = \alpha + \beta_i \times R_m + \epsilon_{it} \quad (2)$$

단, R_{it} : 기업 i 의 시간 t의 실제 수익률
R_m : 시간 t 의 시장 평균 수익률

본 연구는 시장평균수익률과 기업 i의 수익률간은 회귀관계를 확인하기 위해 사건발생일로부터 영업일 10일 이전의 1년간의 데이터를 사용한다. 분석 기간 동안에 발생하였을지 모를 다른 사건들의 영향을 배제하기 위해서는 1년간의 자료를 각 기업별로 회귀분석한다.

3.3 자료의 선정

2010년 이후 발생한 개인정보 유출 사례는 <Table 1>에 정리되어 있다. 이전 개인정보 유출 사건과 비교하면 규모가 1000만 건을 넘는 사례가 다수 있을 정도로 대규모 자료 유출이 빈번하였으며 주로 대기업, 특히 KT의 경우에는 반복적인 개인정보 유출이 일어났음을 알 수 있다. 본 논문은 KisValue 시스템의 주가 자료를 이용하여 해당 개인정보

〈Table 1〉 Leak of Personally Identifiable Information After 2010 in Korea

Date	Company Name	Listed	Size of Information
2010/3	Shinsegae Department Store	O	20,000,000 records (including shinsegae.com membership record - 3,300,000)
2010/3	DaeMyong Resort	X	800,000 records
2010/7	National Pension Services	X	100,000 records
2010/10	KT	O	records of Apartment residents
2011/4	Honda Korea	X	2,200,000 records
2011/4	Hyundai Capital Co.	X	1,750,000 records
2011/7	SK Communications	O	35,000,000 records
2011/7~9	Samsung Card Co.	O	200,000 records (internal employee)
2011/11	Nexon Co.	X	13,200,000 records
2012/3	SK_Tel/kt	O	200,000 records (cooperative company's employee)
2012/5	EBS	X	4,000,000 records
2012/7	KT	O	8,000,000 records

cf) we count the last information leakage from KT in 2012/July with largest number of records.

유출 사건으로 인한 상장회사의 주가 변동을 확인한다.

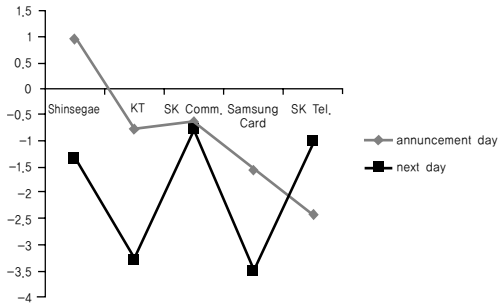
4. 분석 결과

4.1 회귀분석과 기대수익률

먼저 각 종목의 기대수익률을 구하기 위해 사건이 일어나기 영업일 10일 전까지의 1년간 식 (2)를 이용하여 평균 수익률과 실제 수익률 간의 회귀분석 결과를 산출한다. 시장의 평균 수익률은 KOSPI 지수를 이용하여 산출하였으며 개별 종목의 회귀 분석 결과는 <Table 2>에 정리되어 있다.

해당 회귀분석을 이용하여 개인정보 유출 사건이 발생한 날을 기준으로 5일 전후의 초과수익률을 구한다. 특히 발표 당일 혹은 발표 다음날의 초과 수익률은 <Figure 1>에 정리되어 있다. SK 컴즈의 사례를 제외하고는 대부분 발표 당일 혹은 발표 다음날에는 음의 초과 수익률을 보인다. 더불어 t-검정을 통해 초과 수익률이 0이라는 귀무가설을 기각할 수 있다.

또한 당일날의 영향이 -0.8779%로 나타나는 결과는 선행 연구[11]의 결과와 상당히 유사한 흐름을 나타내고 있다. 다만 선행 연구에서는 음의 초과 수익률이 당일 하루에 그쳤지만 본 연구의 결과는 이틀 후에도 음의 평균 초과수익률을 나타내고 있다. 특히나 발표 당일 보다는 발표 다음날에 더 큰 음의 영향을 받고 있는 것은 신뢰가 기본인 금융업종에서 나타난 현상이라는 점과 영향을 받은 개인정보의 수가 선행 사례들보다 많은 경우에 해당하기 때문으로 풀이된다.



〈Figure 1〉 Abnormal Returns on the Announcement Day and 1st Day

〈Table 2〉 The Result of Regression for Equation (2)

	Shinsegae Department Store	SK Communications	Samsung Card Co.	SK Tel.	KT
α (p-value)	-0.0013 (0.9905)	-0.0882 (0.7249)	0.0012 (0.9909)	-0.0390 (0.7316)	-0.0500 (0.5465)
β (p-value)	0.7083 (0.0000***)	1.2555 (0.0000***)	0.8189 (0.0000***)	0.3661 (0.0000***)	0.3713 (0.0000***)
F-value	75.4251	66.9637	79.3998	28.3968	53.6361
Adj R^2	0.2273	0.2094	0.2402	0.0991	0.1745

cf) ( ) p-value, */**/*** : statistically signifiant in 10%/5%/1% level.

4.2 가설의 검증

먼저 검증할 가설 1은 여전히 개인정보 유출 사건은 관련 기업의 주가에 음의 영향을 미친다는 것이다. <Table 3>에 나타난 개인정보 유출 기업의 사건연구 결과로 발표 당일 나타난 초과 수익률 평균은 0.8779%의 시세 하락을 나타낸다. 발표 다음날의 경우에는 2%에 이르는 시세하락을 나타내고 있으며 두 경우 모두 초과수익률이 0이라는 귀무가설을 기각할 수 있는 t-검정 결과를 나타내고 있다. 따라서 가설 1은 2010년 이후에도 성립한다고 결론 내릴 수 있다.

검증할 두 번째 가설은 실제 개인정보 유출 사건으로 영향을 받는 주가의 변동 폭이 줄어들 것으로 예상한 부분이다. 이미 사례분석에서 언급한 바와 같이 개인정보보호법의 시행에도 불구하고 기존 사례의 피해 측정과 책임에 대한 분명한 결론이 나지 않고 있는 상황에서 반복적으로 개인정보 유출 사건이 발생하고 있다. 심지어 동일한 기업에서 수차례 정보 유출 사건이 발생하는 경우도 있어 오히려 자본시장에서 이미 이전 내용을 주가에 반영하고 있다면 추가적인 정보 유출에 의한 주가 변동은 줄어들 수 있다고 가정하였다.

본 연구의 결과를 선행 연구와 비교하면 선행 연구에서는 개인정보 유출에 따른 주가 변동이 발표 당일에 한정적으로 부정적 결과를 나타낸 반면에 본 연구의 결과는 발표 당일과 함께 발표 다음날까지도 부정적 영향이 남아 있는 것을 볼 수 있다. 오히려 변동 폭은 발표 다음날이 더 확실한 음의 영향을 보여준다. 선행연구에서는 모든 보안 사고를 포함한 사건연구 결과를 제시하였지만 본 연구에서는 지속적으로 반복되는 개인정보 유출 사건만을 한정하여 사건연구 방식의 분석 결과를 제시한다는 점을 감안하면 선행 연구의 결과 보다 오히려 주가 변동의 폭이 늘어난 것으로 판단한다면 이는 개인정보의 중요성

〈Table 3〉 Average Abnormal Returns with T-test for Equation (1)

day count	mean abnormal returns	t-statistics	p-value	cumulative mean abnormal returns
-5	-0.9753	-5.47389	0.0633*	-0.9753
-4	0.2838	-13.6251	0.0000***	-0.6915
-3	0.7390	-0.63664	0.2128	0.0475
-2	-0.4595	2.700881	0.7592	-0.412
-1	0.4588	0.456822	0.1555	0.0468
0	-0.8779	4.149098	0.0460**	-0.8311
1	-1.9860	-8.08289	0.0000***	-2.8171
2	-0.3146	-2.73405	0.7122	-3.1317
3	0.3912	4.696409	0.0416**	-2.7405
4	0.4962	1.417515	0.9494	-2.2443
5	0.6648	1.624428	0.8354	-1.5795

cf) */**/*** : statistically significant in 10%/5%/1%.

을 시장이 반영한다고 볼 수 있다. 다만 언급한 바와 같이 2010년 이후 발생한 개인정보 유출의 경우는 영향을 미치는 개인정보의 수가 크게 증가하고 집단 소송으로까지 연결되는 등 사회적으로 큰 관심을 끌 사례가 더욱 많아진 정황을 고려하여야 할 것이다. 이를 함께 반영하다면 시장이 보다 분명한 반응을 나타낸 것은 개인정보 보호에 대한 인식의 확대 뿐 아니라 지속적이고 보다 확대된 개인정보 유출 현상 규모의 차이 때문이라고도 해석할 수 있다. 향후 보다 자세한 자료 분석을 통해 보안 문제의 종류 뿐 아니라 규모나 업종에 따라서도 시장의 반응이 달라질 수 있는지 추가 검증할 필요가 있다.

5. 결 론

본 연구는 개인정보 유출에 의한 피해 규모를 산출하기 위한 방법의 하나로 재무학의 사건연구 방식을 이용하여 주가의 변화폭을 검증한다. 완전시장 가설을 받아들인다면 이와 같은 주가의 변동을 개인정보 유출에 의한 피해 규모의 대용치로 활용이 가능할 것이다.

기존의 개인정보 유출로 인한 주가 변동 결과를 바탕으로 2010년 이후 발생한 개인정보 유출 사례가 기존의 주가 변동과 유사한 반응을 나타내었는지 혹은 개인정보보호법의 시행으로 보다 강화된 보안 의식이 작용하여 시장의 반응이 보다 확대 되었는지를 실증적으로 분석하는 것이 본 연구의 목적이다. 2010년 이후 발생한 사례에 대한 분석을 통해 얻은 결론은 아래와 같이 정리할 수 있다.

첫째, 반복되는 개인정보 유출 사례에도 불구하고 시장의 반응은 해당 사건에 여전히 부정적인 것을 확인할 수 있다. 즉 개인정보 유출 사례로 인해 일시적이나마 기업의 가치에 음의 영향을 미치는 결과는 이전과 변함이 없다.

둘째, 반복되는 개인정보 유출과 관대한 처분, 이에 반해 법적으로 보다 강화된 개인정보보호법의 시행 등과 같이 상반된 효과를 기대할 수 있는 요소들이 혼재되어 있는 상황이지만, 최근 대용량화 되어가는 사용자 정보 유출 추세나 금융기관까지 해킹 당하는 사태에 대해서는 시장의 반응도 보다 명확한 결과를 나타내고 있다. 다만 이와 같은 결과가 법적 혹은 제도적 정비를 통한 효과인지 혹은 보다 대형화되어가고 있는 보안사건 자체 때문이지는 아직 분명하지 않다.

이상과 같은 결과와 함께, 향후 추가로 발생되는 개인정보 유출 사건에 대해서는 보다 명확한 피해 규모 산정과 이에 상응하는 보상 체계가 명확히 제시되어야 반복되는 개인정보 유출 사고를 최소화 할 수 있을 것으로 판단된다. 비록 개인정보 유출로 인한 2차 피해의 책임 소재가 불분명할 수 있지만 반복적으로 발생하는 유사한 사건을 미연에 방지하기 위해서는 개인정보를 수집하는 기업이나 단체가 이에 대한 책임을 보다 명확히 인식할 필요가 있다.

References

[1] Ahn, H. G., “Trend and Forecast for the Confidential Information Leakage Pre-

vention of Industries and Personal Privacy Protection," Korean Institute of Information Scientists and Engineers, Vol. 25, No. 8, pp. 42-47, 2007.

[2] Cavusoglu, H., Mishra, B., and Raghunathan, S., "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. 70-104, 2004.

[3] CIC Security Working Group, "Incident Cost Analysis and Modeling Project," 1998.

[4] Congressional Research Service, "The Economic Impact of Cyber-Attacks," 2004.

[5] Ettredge, M. and Richardson, V. J., "Assessing the risk in e-commerce," 2002. IEEE.

[6] Gordon, L. A. and Loeb, M. P., "Managing cyber-security resources : A cost-benefit analysis," McGraw-Hill New York, Vol. 1. 2006.

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

[8] Kang, H., Park, K. C., Park, W. H., and Kuk, K. H., "A Study on Model for Assessment of Economic Damages Due to Cyber Terror," Journal of Infoamtion and Security, Vol. 9, No. 3, pp. 25-33, 2009.

[9] Kim, J. K. and Lee, D. H., "A Research on Information Security Risk-based Antecedents Influencing Electronic Commerce User's Trust," Asia Pacific Journal of Information Systems, Vol. 15, No. 2, pp. 65-96, 2005.

[10] Kong, H. K. and Kim, T. S., "Research trend on the effects of invest on information security," Review of Korea Institute of Information Security and Cryptology, Vol. 17, No. 4, pp. 26-33, 2007.

[11] Kwon, Y. O. and Kim, B. D., "The Effect of Information Security Breach and Security Investment Announcement on the Market Value of Korean Firms," Information Systems Review, Vol. 9, No. 1, pp. 105-120, 2007.

[12] Nam, K. H., Park, S. J., Kang, H. S., Nam, K. H., and Kim, S. I., "The latest technology trends and future prospects on personal data protection," Review of Korea Institute of Information Security and Cryptology, Vol. 18, No. 6, pp. 11-19, 2008.

[13] Nam, S. H., "Empirical Study on the Impact of Security events to the Stock Price in the Analysis method of Enterprise Security Investment Effect," Ph.D thesis, Korea University, 2006.

[14] Ryu, I. and Choi, H. R., "Factors Influencing the Consumer Trust and Mediating Roles of Trust on Purchasing Intention

in B2C Electronic Commerce," Asia Pacific Journal of Information Systems, Vol. 13, No. 4, pp. 49-72, 2003.

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

[16] Yoo, J. H., Jie, S. H., and Lim, J. I., "Estimating Direct Costs of Enterprises by Personal Information Security Breaches," Journal of Korea Institute of Information Security and Cryptology, Vol. 19, No. 4, pp. 63-75, 2009.

[17] Yoo, J. H., Gee, S. H., Song, H. I., Chung, K. H., and Lim, J. I., "Estimating Economic Damages from Internet Incidents," National Information Society Agency, Vol. 15, No. 1, pp. 3-18, 2008.

저 자 소 개

김정연	(E-mail : jykim@smu.ac.kr)
2002년	University of Michigan (석사)
2003년	University of Minnesota (박사과정)
2008년~2011년	(주)세린 경영자문이사
2010년	상명대학교 경영학 (박사)
2011년~현재	상명대학교 경영대학 경영학부 조교수
관심분야	이익예측, 정보보안, 기업분석