http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.21, No.2, May 2016, pp.81-96
http://dx.doi.org/10.7838/jsebs.2016.21.2.081

정보유출이 기업가치에 미치는 효과분석: 원천 및 장기성과

Empirical Investigation on Information Breach Effect on the Market Value of the Firm: Focused on Source and Long Term Performance

권순만(Sun Man Kwon)*, 한창희(Chang Hee Han)**

초 록

본 연구는 정보유출에 따른 주가반응을 측정함으로 정보유출이 기업가치에 주는 효과를 분석한다. 정보유출기업은 사건발생 2일 이내에 평균 1.3%의 시장가치를 상실하여 98.9백만원의 손실액이 추산된다. 우리는 원천, 유형, 크기 등 다양한 정보유출 유형에 대한 비정상수익율을 분석하였다. 시장은 외부원천의 정보유출에 유의미한 반응을 하지 않지만, 내부원천의 정보유출에는 통계적으로 유의미한 반응을 보였다. 우리는 60일간의 장기 비정상수익율을 추정하였다. 60일 평균 누적비정상수익율과 매입보유 비정상수익율 모두 유의미한 시장반응을 보인다. 이로써 우리는 정보유출사건 이후 일관된 시장반응이 있다고 결말지을 수 있다. IT기업과 비IT기업의 시장반응 차이는 통계적으로 유의미하다. 그러나 유출규모, 기업크기, 발생시점 등은 유의미한 시장반응을 보이지 않는다.

ABSTRACT

This paper analyzes the impact of information breach on shareholder value by measuring the stock price reaction associated with the announcements of data breach. The breach firms in the sample lost, on average, 1.3% of their market value, amounting to 98.9 million won of loss within two-day of the event period after the announcement. We examine the abnormal returns in various categories (i.e., source, type, size, etc.) of information breach. Although the market does not react significantly to the announcements of outside breach, we find statistically significant market reactions to inside breach. We estimate abnormal returns over the following 60 days. The mean 60-day cumulative abnormal return and BHAR (buy-and-hold abnormal returns) are both significantly far from zero. We conclude that there is a coherent market reaction following the announcement. The difference between the market reactions to IT firms and Non-IT firms is statistically significant. But breach amount, firm size, and the year the breach occurred do not show to be significant variables.

키워드 : 시장가치, 정보유출, 원천, 유형, 장기 성과
Market Value, Information Breach, Source, Type, Long-Term Performance

* Hanyang University(sunman86@hanmail.net)
** Corresponding Author, Hanyang University(chan@hanyang.ac.kr)
Received: 2016-04-22, Review completed: 2016-05-17, Accepted: 2016-05-24

1. 서 론

ICT 시스템, 인터넷의 발달과 개인 모바일 기기의 업무사용 증가 등으로 정보의 수집, 처리 등이 빠르고 용이해진 반면 보안위험 및 정보유출로 인한 개인, 기업, 국가적 손실의 피해가 커지고 있다[7]. 개인정보뿐 아니라 사용자의 서비스이용 및 거래 정보 등을 활용하는 데이터산업의 발전은 정보보호의 필요성을 높이고 있다.

본 연구는 개인정보유출에 관련한 기업 주가의 반응을 측정함으로 정보유출이 기업가치에 주는 영향을 분석한다. 또한 개인정보유출의 원천이 내부 혹은 외부공격에 따라 시장반응이 유의한 차이를 보이는지, 정보유출이 기업의 장기성과에 의미 있는 영향을 주는지를 검증한다.

우리가 다루고 있는 이슈는 다음과 같은 중요한 의미를 보여준다. 첫째, 2014년 1월 발생한 국내 최대의 신용카드사고 이후에도 개인정보유출은 지속되고 있다. 정보유출에 따른 기업의 사과와 사후대책 발표에도 유사한 사고가 재발하고 있다. 유출사고 후 기업의 사후대책 또한 중요하지만, 정보유출이 주는 피해규모와 기업가치에 주는 영향은 적잖은 논란이 있다. 선행연구를 살펴보면 인터넷 보안사고가 평균 2.1%의 시장가치 하락으로 사건 당 16.5억 달러의 손실을 보인다는 주장이 있는 반면[4], 투자자들이 정보유출 이후 진행되는 과정을 보고 그 영향을 판단하기 때문에 정보유출에 따른 기업가치의 영향은 유의미하지 않다[17]는 주장도 있다. 정보유출의 결과가 기업가치에 장기적으로 미치는 영향이 없다고 주장한 반면, 국내의 경우 사건발생인 이후 25사건일에 부정적 효과를 보였다[13]. 본 연구에서는 국내 기업들을 대상으로 정보유출이 기업가치에 미치는 영향 정도와 장기영향을 검증함으로 기업 정보보호와 정보유출 재발 방지를 위한 사후대책의 중요성에 대한 증거를 제시한다.

둘째, 지금까지 개인정보유출은 사회적 피해를 주고 기업가치에 음(-)의 재무적 영향을 준다는 견해가 다수이나, 실증분석에 필요한 데이터의 부족으로 피해규모를 측정하는데 어려움을 보여주고 있다. 미국의 Ponemon에서는 2005년을 시작으로 개인정보유출에 따른 비용추정 보고서를 출간하고 있다. 산업별 설문을 통해 총체적 피해규모를 조사하고 있으며 2007년 정보유출 사건 당 평균비용 손실은 약 630만 달러였던 것으로 나타났다[24]. 정보유출의 피해를 측정하는 방법에는 비용편익 분석방법론[8], 사건연구방법론[5], 가상가치접근법(CVM), 회귀분석 등을 통해 연구가 진행되었다. 비용편익분석은 개인정보유출로 인해 발생될 기업이미지 손상과 주가하락 등과 같은 간접적 손실의 측정이 어렵다는 한계가 있다. Yoo et al.[25]은 기업의 손실비용 산출을 위해 손실 범주를 분류하고 개인정보유출 사고 손실을 일본 사례와 비교 분석하였다. Han et al.[9]은 데이터 부족으로 인한 모델 확립과 적용에 어려움이 있었고, 피해규모 수치보다는 설문과 상대적 비교분석 등의 기법을 이용한 방법론 제시에 의미를 부여하였다. 가상가치접근법은 정보유출피해라는 손실을 회피하기 위한 응답자의 지불의사금액을 산출하여 사회적 손실가치를 추정하였다[21]. 지불의사금액으로 정보유출의 보상액을 산정하는 이 방법은 실제 개인이 자신의

정보유출로 인해 느끼는 피해가치를 정확히 반영하지 못할 수 있다는 한계가 있다. 회귀분석방법은 정보유출에 영향을 주는 변수와 비정상 수익률간의 장기적 관계를 분석한다. 이 방법은 연구기간 동안 비정상 수익율에 영향을 미치는 다양한 설명 요인간의 다중공선성의 이슈 등이 있어 선정된 요인에 따라 결과가 민감하게 반응하곤 한다. 본 연구는 정보유출사건이 시장가치에 주는 영향을 측정하는 방법으로 '사건연구방법'이 적용된다. 사건연구는 특정 사건으로 인해 기업의 수익성에 변화를 주는 시장반응이 있는지를 측정하여 이들 간에 연관관계가 있는지를 측정한다. 개인정보유출이 기업가치에 주는 영향을 분석함으로 우리는 정보유출이 기업가치에 주는 손실규모를 파악할 수 있다.

우리는 선행연구를 확장하면서 다음과 같은 상이한 관점에서 분석을 수행했다. 첫째, 정보유출이 기업가치에 미치는 장기효과에 대해 연구결과는 지금까지 미흡하다. Hovav and Han[13]이 제시한 장기의 '누적 비정상수익율'을 이용한 장기효과는 부정확한 추론을 가져올 수 있는 문제가 있다[1, 20]. 우리는 사건일을 확장해 '60일간'의 사건기간에 대한 '누적 비정상수익률'과 '매입보유 비정상수익율(Buy and Hold Abnormal Return, BHAR)'을 사용해 정보유출이 기업가치에 미치는 장기적 효과를 검증한다. 둘째, 개인정보유출은 발생원천에 따라 해킹 등 외부공격에 의한 것과 내부직원 등에 의한 내부의 원천이 있다. Hovav and D'Arcy[12]는 바이러스 공격에 따른 사고보도가 기업가치에 영향을 주지 않음을 보였다. 국내에서도 정보유출에 대해 법원은 회사의 관리부실에 책임을 묻는 추세이다. 예컨대 인터넷 복권구매 안내 메일을 발송하면서 고객명단과 신상정보파일을 함께 첨부한 국민은행에 개인정보유출 피해를 입은 고객들에게 각 20만 원씩 손해를 배상하라는 판결을 내렸다(서울고법 민사9부, 2007. 11. 27). KT는 이동전화 이용약관에 '회사의 귀책사유'인 경우 위약금을 면제한다고 명시해 기업의 내부적 원인에 의한 개인정보유출이 발생할 경우 고객이탈 등으로 기업가치에 직접적인 영향을 주게 된다. 즉 정보유출의 원인이 내부적 요인에 의한 경우 외부요인에 의한 경우보다 기업가치에 더 큰 영향을 줄 수 있음을 추론할 수 있다. 우리는 정보유출의 원천에 따른 시장반응을 검증함으로써 내부적 원인에 의한 정보유출을 통제하기 위한 시스템 마련이 우선적으로 필요함을 제시한다.

우리는 2001년~2014년의 기간 동안 일간기사에 나타난 총 38건의 개인정보유출과 관련한 주식시장 반응을 측정함으로써 기업의 개인정보유출이 주주가치에 미치는 영향을 분석한다. 먼저 정보유출관련 연구현황을 살펴보고, 연구방법론과 가설, 실증분석 결과 및 결론의 순서로 정리한다.

2. 문헌연구 및 가설

2.1 개인정보유출

'개인정보의 유출'이라 함은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대해 개인정보처리자가 통제를 상실하거나 또는 권한 없는 자의

접근을 허용한 것을 뜻한다(표준개인정보보호지침 제26조). 개인정보의 유출사고 피해를 파악하기 위해 Han et al.[9]은 악성코드 감염, 해킹 등의 외부의 공격으로 인한 '개인정보유출'과 조직 내부를 통한 '개인정보누출'을 구분하기도 하였다. 본 연구에서 개인정보유출은 외부공격이나 조직 내부 등의 사고원천을 포괄하여 발생한 사고를 연구대상으로 하였다.

정보유출사고로 인한 피해규모를 산정하기 위해 비용편익 분석, 가상가치접근법, 사건연구 등의 방법이 시도되고 있다. 비용편익분석의 경우, 개인정보유출로 인해 발생되는 간접적 손실의 측정이 어렵다는 한계가 있으나, 피해요소의 측정 및 실무차원의 활용을 위해 연구가 진행되었다. 기업의 직접적이고 정량적인 손실비용 산출을 위해 2005년~2007년 국내에서 발생한 개인정보 사고의 손실을 추정하였다[25]. 한 번의 설문조사 및 판례 등을 통해 직접적 손실비용을 산출한 이 연구는 장기간에 걸친 기업의 피해 정도를 제시하는 데는 한계를 보여 주었다. Han et al.[9]은 개인정보유출 사고의 피해실태 파악을 위한 정보수집과 정량적 분석의 개념적 틀로 피해액을 측정함으로써 개인정보유출 피해를 막기 위한 기반자료를 제안하였다. 이 연구는 사고내용과 발생건수 파악 등 데이터의 부족으로 정확한 모델을 확립하는데 어려움을 제시하면서 정보사고의 심각성에 대한 공감으로 국가적 차원의 개인정보유출 관련 데이터 수집과 질 향상을 제언하였다. JNSA는 2002년부터 개인정보사고에 대한 조사분석을 매년 실시하고 있다. 2003년에 니케이주식 평균을 기준으로 하여 주가를 이용한 피해산출이 있었으나, 예측의 타당성 이슈로 사용되지 않고 있다. 이 조사는 사고가 발생한 기업의 유형, 피해자수, 유출원인 등을 산출 발표하고 있다.

가상가치접근법은 개인정보유출의 피해자가 기업이 제시하는 손해배상액을 추정하여 잠재손실액을 추정하는 방법이다[21]. 직접적 보상액이 아닌 지불의사금액을 통해 산정하는 방법으로 개인정보유출 피해자가 기업이 제시하는 배상액을 수용하지 않으려는 성향으로 과추정되는 특징을 보여준다.

사건연구는 정보유출로 인한 기업의 이미지 하락, 고객이탈 등의 간접비용을 고려한 방식으로 주가변동을 분석한다. 사건연구방법은 시장가치를 측정할 수 있는 기업들을 대상으로 사건발생이 주식가치의 변동에 유의한 영향을 주는 지를 검증한다. 기업유형에 따른 영향으로 전자상거래 기업이 더 큰 손실을 경험한다고 주장[4]도 있으나, Kwon and Kim[22]는 보안사고에 따른 손실과 보안투자의 수익을 측정하면서, 정보유출의 피해가 기업유형에 따라 유의한 영향을 주지 않는다고 주장하였다. Kim[19]은 시점에 따른 정보유출의 피해로 기업가치가 일시적으로 하락했으며, 피해인식이 크게 변화되지 않았다고 언급했다.

우리는 개인정보유출이 기업가치에 미치는 영향이 원천에 따라 차이가 있는지, 또한 장기적으로 견고하게 유의미한 영향을 주는지를 검증한다. 이를 위해 국내에서 발생한 정보유출이 기업가치에 미치는 영향을 2001년부터 2014년까지 확대하고 원천, 업종, 규모, 시점 등 다양한 관점에서 정보유출이 기업가치에 주는 영향을 분석한다.

〈Table 1〉 Literature Review on Information Breach

Studies	Source	Samples	Methodology and results
Han et al. [9]	Web traffic Survey Indirect comparison	Individual, Firm	'Cost-Benefit analysis'_ adopted by JNSA and Ponemon, measuring damage cost from firm, individual, and social perspectives
Yoo et al. [25]	Survey Judicial precedent	Firm (2,800)	'Cost-Benefit analysis': develop formula to calculate economic loss (practical method for measuring damage cost)
JNSA[16]	Survey Interview	IT Firm (1,000)	'Security incident survey and damage calculation model': Estimated damages
Kwon et al. [21]	Survey	Students, etc. (552)	'CVM(Contingent Valuation Methods)'_adopted by JNSA, analyze Willingness to Accept and measure the value of personal information
Kannan et al. [17]	News, Stock price (1997~2003)	60 Firms	'Event study'; security announcements have no negative returns over long-term.
Cavusoglu et al. [4]	News, Stock price (1996~2001)	40 Firms (66 events)	'Even-study': assessing the value of IT security; lost 2.1% of market value within 2 days of the announcement.
Kwon and Kim [22]	News, Stock price (2001~2005)	59 events	'Event-study': lost 0.86% of market value, security-related investments have no impact on firm value
Kim [19]	News, Stock price (2010~2012)	12 events	'Event-study': No change in stock market after the information management issue.

2.2 연구방법론: 사건연구(Event study)

우리는 효율적 시장가설에 기반한 사건연구 방법론을 이용하여 정보유출사건에 대한 시장 반응을 측정한다. 사건연구를 위해서는 먼저 비정상수익률(Abnormal Return)을 측정할 사건기간(event period)을 결정한다. 사건일로의 전환을 위해 사건 발생일을 "0일(Day 0)"로 설정하고, 발생일의 하루 전 거래일은 "-1일(Day -1)"로 한다. 사건연구 모델 중 비정상수익률을 측정하는데 가장 유용한 '시장모델(Market Model)' 을 사용한다[3]. 이 모델은 시장수익률과 주식주익률 간에 선형관계를 가정한다.

$$R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it}$$

R_{it} : 주식 i의 t시점 수익률 {= $(P_t - P_{t-1})/P_{t-1}$}, P_t: t일의 거래종가

R_{mt} : t시점 시장(포트폴리오) 수익률(예, 종합주가지수, 코스닥지수, *업종대표지수)*

α_i : 주식 i에 대한 절편(주식 i의 고유위험)

$\beta_i R_{mt}$: 시장전체 변화에 따른 주식 i의 수익율 변화

ε_{it} : 주식 i의 t시점 오차항(error term)~ i.i.d. $N(0, \sigma^2)$

표본 기업의 기대수익률 산출을 위해 추정거래기간 동안의 최소자승회귀를 이용하여 모수를 추정한다. Hendricks and Singhal[10]에 의하면 특정 사건에 대한 시장 반응은 -1일과 0일에 관측될 가능성이 높다고 하였다. 그러나, 정

보유출사건의 경우 일반적으로 예측이 불가능하므로 사건 전일은 포함하지 않았다. 따라서 사건기간으로 사건일(Day 0)과 사건다음거래일(Day+1)로 구성되는 '2일 사건기간'의 비정상수익률을 분석하였다. 그리고, 모수 추정에 일반적으로 사용되는 -11일(Day -11)에서 -210일(Day -210)을 추정기간으로 적용하였다. 사건발생 전 2주간(10거래일)을 추정기간에서 제외함으로써 사건공표효과가 개별주가추정에 미치는 영향을 배제하고 모수 추정치의 비정태성(non-stationarity)이슈를 최소화하였다[2].

비정상수익률(A_{it})은 실제 수익률과 예상수익률간의 차이로 도출된다.

$$A_{it} = R_{it}-(a_i+b_i R_{mt}) \ (i = 1, 2, \cdots, N)$$

a_i, b_i는 추정기간동안 OLS 회귀분석에 의한 추정치

t일의 평균비정상수익율(abnormal mean returns; $\bar{A}_t$)은 다음과 같이 주어진다.

$$\bar{A}_t = \sum A_{it}/N \ (i = 1, 2, \cdots, N),$$

N; 연구에 포함된 표본의 수

평균비정상수익률의 통계적 유의성을 검정하기 위해 비정상수익률(A_{it})을 추정표준편차로 나누어 표준화를 시킨다. 비정상수익률이 기업간 독립적이라는 가정하에 N개의 표준화 비정상수익률의 합은 중심극한정리에 의해 정규분포에 근사한다. 정규분포가정하 사건은 수익율에 영향을 주지 못한다는 귀무가설을 검정한다. 이때 검정통계량 TS_t는 다음과 같다[3].

$$TS_t = \Sigma(A_{it}/S)/\sqrt{N}(S_i;\ \text{오차항의 추정표준편차})$$

누적비정상수익률(CAR)은 평균 비정상수익률의 기간 내 누적값을 의미하며 아래와 같다.

$$CAR[t_1, t_2] = \sum \bar{A}_t$$

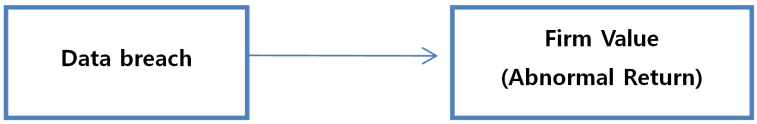
모수검정 결과에 대한 점검을 위해 수익분포 가정에 대해 자유로운 비모수검정을 수행하였다. 이상치(outlier)의 영향을 점검하기 위해, 'Wilcoxon signed-rank test'를 사용하여 중간치(median) 비정상수익률의 통계적 유의성을 검증하였고, 사건기간 동안 비정상수익률이 추정기간 동안의 값보다 유의적으로 높은지를 '일반화된 sign test'를 사용하였다. 우리는 세 방법 모두에서 비정상수익율이 음(-)이라는 가설을 단측검정(One-tailed p-value)으로 검증하였다.

2.3 연구가설

정보유출에 따라 기업은 유출확인을 위한 콜센터 인건비, IR 대응비용, 고객신뢰 상실, 법적비용, 고객감소로 인한 수익감소 등의 손실이 발생한다[14]. 우리는 기업의 개인정보유출이 기업에 비용을 발생시키고 수익의 감소를 가져와 비정상수익율, 즉 기업가치에 부정적 영향을 준다는 개념모델을 사용한다. 따라서 우리는 시장이 기업의 정보유출에 단기간에 부정적으로 반응한다는 연구가설을 수립할 수 있다.

H1-1: 시장은 기업의 정보유출에 대해 단기간에 부정적(negatively)으로 반응한다.

개인정보 침해사고는 정보유출의 원천(source)에 따라 해킹 등의 외부의 공격행위에 의한 경우와 조직 내부 관계자에 의한 정보유출로 구분할 수 있다. 내부직원이 고의로 정보를 유출한 경



〈Figure 1〉 Conceptual Model

우 법원은 회사의 관리부실에 책임을 묻는 판결을 내리고 있는 반면, 기업이 사업자의 주의 의무를 다하였다고 판단될 경우 기업의 책임 없음을 인정하고 있다. 통신업계 정보유출의 경우, 기업의 기술관리적 조치가 미흡하여 발생한 '내부 귀책'의 사건이면 위약금 없는 해지도 가능하도록 되어있다. 이는 정보유출의 원천이 내부인 경우 시장이 보다 부정적으로 반응할 수 있음을 보여준다. 따라서 정보유출사건을 내부원천에 의한 경우와 외부공격에 의한 경우의 하부유형을 구분하여 다음 가설을 수립한다.

H1-2: 시장은 정보유출원천이 '내부'인 경우 '외부'인 경우보다 부정적으로 반응한다.

선행연구에서 개인정보유출은 일시적으로 기업성과에 부정적 영향을 주나[19], 장기간에는 기업가치에 영향을 주지 않는 것으로 나타났다[17]. 국내는 인터넷 보급율이 높고, 주가에 대한 인터넷 주식게시판 내 집단적 투자의견이 전체 주식시장에 유의한 상관관계가 있음[23]을 볼 때, 다른 결과를 보일 수 있다. 따라서 다음 연구가설을 수립한다.

H2: 시장은 기업의 정보유출에 대해 장기간에 부정적(negatively)으로 반응한다.

대규모 정보유출로 인해 개인에게 영향을 미치는 정보의 수가 늘어나고 집단소송으로 까지 확산되는 것은 지속적이고 대규모적인 정보유출에 기인한다. Kim[19]은 정보유출에 대한 시장의 반응이 개인정보보호 인식의 확대뿐 아니라 지속적으로 늘어나는 개인정보유출 현상의 규모 때문인지 추가 검증이 필요하다고 언급했다. 따라서 우리는 정보유출 규모에 따라 시장반응의 차이가 있는지를 연구가설로 수립한다.

H3: 정보유출 규모에 따라 시장 반응이 차이가 날 것이다.

Cavusoglu et al.[4]은 인터넷 기업의 보안사고에 대한 비정상수익율이 전통적 기업보다 크다고 밝힌 바 있다. 컴퓨터, 게임, 포털, 유무선통신 등 IT기업의 경우 정보수집, 가공, 보관, 재생, 전달 등의 정보관련 활동이 기업의 본업과 밀접하게 연관되어 있다. 특히 금융 등 非 IT(Non-IT) 기업에 비해 경쟁이 활성화 되어 보안사고 등이 발생하면 고객이탈이라는 영업기반이 흔들리는 상황을 맞게 된다. 반면, 금융 등 비IT기업의 경우 과점화되어 보안사고가 기업가치에 주는 영향은 크지 않을 것으로 본다. 따라서 정보유출이라는 사건이 기업의 유형(Type)에 따라 주식 변동 값에 차이가 있을 것으로 보고 다음 가설을 검증한다.

H4: IT기업의 정보유출이 Non-IT기업의 경우보다 부정적 시장의 반응이 클 것이다.

기업 크기는 몇몇 사건 연구에서 영향력이 있음이 발견되었다[11]. 일반적으로 기업이 작을수록 기업이윤에 한 사건이 주는 상대적 영향이 크기 때문에 큰 기업보다 강한 시장반응

을 보인다[6]. 큰 기업은 낮은 자본비용, 다양한 소득원천, 다양화된 상품, 브랜드네임 인지도 등으로 인해 소규모 기업보다 부정적인 경제적 충격을 보다 쉽게 흡수할 수 있다. 반면 소규모 기업은 기업 분석가에 의해 면밀히 검토가 되지 않는 경향도 있어 대 기업의 사건발생에 비교하여 예상치 못한 요소를 갖고 있을 수 있다. 이러한 기업 크기의 효과를 검증하기 위해 총 자산기준으로 크기에 따라 4개 그룹으로 구분한다. 상위집단과 하위집단의 평균분석을 통해 기업규모에 따른 정보유출 영향의 차이를 검증한다.

H5: 대기업보다 소규모기업의 정보유출이 기업가치에 미치는 영향이 클 것이다.

정보유출은 시점에 따라서 시장에 미치는 효과가 다를 수 있다. Kim[19]은 2010년 이후 발생한 개인정보유출사례를 기반으로 '개인정보보호법'시행에 따른 기업가치에 미치는 영향이 없다고 밝혔다. 최근 개인정보가치 및 보안의 인식 증대로 동일한 정보유출에 대해서도 시장의 반응이 다를 수 있다고 가정하고 개인정보보호법 시행시점('12. 3. 30)을 기준으로 사건을 나누어 분석함으로 다음 가설을 검증한다.

H6: 정보유출 발생시점에 따라 기업가치에 미치는 영향이 다를 것이다.

3. 실증분석 결과

3.1 표본과 데이터

우리는 표본을 생성하기 위해 '개인정보유출, 집단소송, 주가' 등의 핵심단어를 사용하여 사건관련 기사를 선별하였다[15]. 정보유출관련 기사는 종합일간지, 경제일간지, TV 방송뉴스 등을 포함한 최대 규모의 기사 DB를 보유한 KINDS(Korea Integrated News Database System) 뿐 아니라, 추가로 조선미디어, 네이버뉴스 등에 실린 사건을 조사하였다. 사건 발생 기업 중 Fnguide.com에서 제공하는 개별종목 일별 시계열 자료를 사용하여 주가를 산출하였다. 사건표본 중 다음의 유형은 제외되었다.

- 사건발생일 2주 전부터 1년 동안 주가를 얻을 수 없는 경우
- 동일 사건이 다수 기사에 나타난 경우(이 경우에는 최초 발생일에 포함하였다.)
- 일주일 내(5일) 동일기업에 대해 연속적으로 발생한 경우

2001년에서 2014년 사이에 개인정보유출 검색을 통해 도출된 총 사건은 68건이었으나, 주가를 얻을 수 없는 정부기관, 비영리기관, 비상장기업 등이 제외되는 등 조건을 만족하는 최종 사건은 38건으로 조사되었다. 우리는 개별주식에 대한 기준지수(Benchmark index)로 종합주가지수, 코스닥지수 외에 업종별수익률이 사건연구에 보다 타당하다는 주장에 따라 업종지수를 분석에 활용하였다[18].

<Table 2>는 사건기업 표본의 기술통계량을 나타낸다. 시가총액은 사건일에 해당하는 값을, 그 외의 데이터는 사건 발생시점의 이전 년도 값을 구하였다. 사건기업 표본은 기업특성의 편차 값이 크나, 평균값이 중앙값보다 크게 나타나고 있다.

〈Table 2〉 Descriptive Statistics for the Sample of Events

	Market value (₩M)	Total assets (₩M)	Sales (₩M)	Net income (₩M)	Employees
Mean	7,608,325	29,056,686	8,875,092	637,097	9,849
Median	5,054,147	11,464,346	4,298,007	277,375	2,660
Std Dev	7,267,477	66,711,788	9,916,509	706,908	13,983
Max	26,271,255	311,296,843	39,425,960	2,059,570	46,100
Min	38,922	57,952	50,827	-88,842	23

〈Table 3〉 Security Breach Announcements(2001~2014)

Year	Announcement	Final sample	Rate (%)
2001	1	1	100%
2002	4	0	0%
2003	4	1	25%
2004	3	1	33%
2005	3	2	67%
2006	5	2	40%
2007	3	3	100%
2008	7	5	71%
2009	1	1	100%
2010	2	1	50%
2011	11	4	36%
2012	4	3	75%
2013	5	3	60%
2014	15	11	73%
Total	68	38	56%

3.2 분석 결과

전체 38개 표본에 대하여 [4-A]은 사건발생일(0일)과 사건다음일(1일)에 대한 시장반응을 나타낸다. 2일 사건기간(Day 0&1)은 5% 수준에서 평균(중앙값)비정상수익률, 음의 비정상수익율% 모두 0과 유의미하게 통계적으로 다른 값을 나타내고 있다.

정보유출기업은 평균적으로 '2일 사건기간' 동안 시가의 1.3%를 상실했다. 이는 기업평균 시장가치를 기초로 할 때 평균적으로 98,908백만 원의 손실로 해석할 수 있다. 이 결과는 해외 사례[4]보다 상대적으로 시장의 반응이 작은 것으로, 국내의 경우 정보유출 사고에 대한 미흡한 기업의 사후조처와 법원판결 사례 등에서 그 원인을 추정해 볼 수 있다.

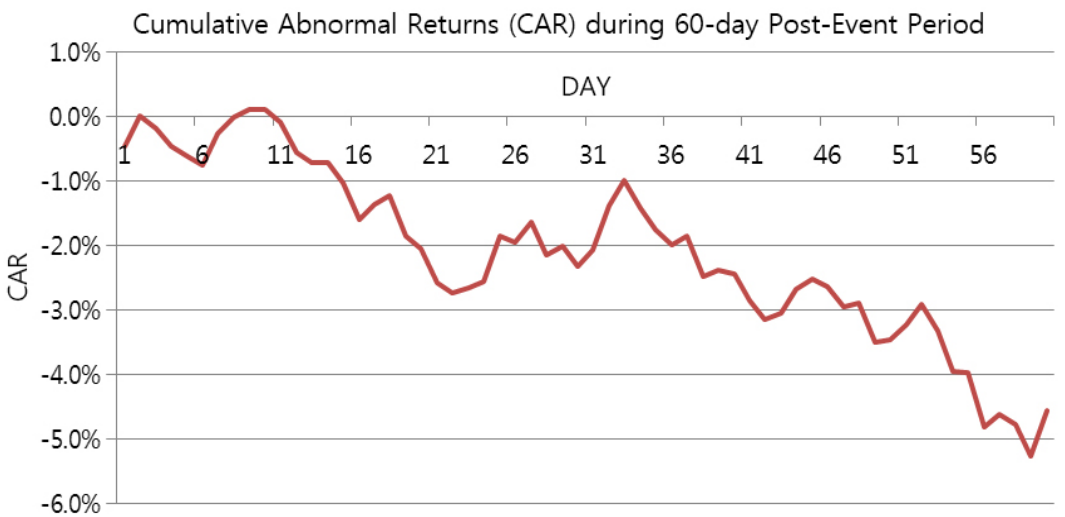
[4-B]에서는 정보유출 원천에 따른 비정상수익율의 분석결과를 제시하였다. 해킹 등 외부 원천의 2일 사건기간 동안의 평균(중앙값) 비정상수익율은 -0.857%(-0.357%)로 통계적으로 유의미하게 0과 다르다고 할 수 없었다. 해외사례[12]와 유사하게 해킹 등에 의한 외부 정보유출에는 시장이 통계적으로 유의미하게 반응하지 않았음을 나타낸다.

반면 내부원천에 의한 정보유출의 비정상수익율의 평균(중앙값)은 -1.487%(-1.122%)로 5% 수준에서 통계적으로 유의미한 값을 나타내었다. 게다가 73.1%의 비정상수익율이 음(-)이었고 추정기간보다 5% 수준에서 통계적으로 유의미한 결과를 보였다. 내부원천에 의한 정보유출이 음(-)의 시장반응을 나타내는 것은 기업 내부의 부주의와 주의감독 소홀로 인한 정보유출이 고객의 불신을 야기시켜 기업의 명성을 훼손하고 궁극적으로 기업가치에 부정적 영향을 미치기 때문이라고 추정할 수 있다. 국내의 소송사례에서도 기업이 정보유출 사고에 대한 주의의무를 다했느냐의 여부에 따라 기업의 책임여부를 판단하고 있다.

〈Table 4〉 Event Period Abnormal Returns for the Information Breach

[4-A]			
	Day 1	Day0	Day 0 and 1
Mean abnormal return	-0.454%	-0.834%	-1.288%
t-statistic	-1.241	-2.048**	-2.321**
Median abnormal return	-0.657%	-0.130%	-0.803%
Wilcoxon signed-rank Z-statistics	-1.936**	-1.646**	-2.212**
% abnormal return negative	68.4%	57.9%	68.4%
Sign test Z-statistic	-2.109**	-0.811	-2.109**
[4-B] source(sub category) results for event period(Day 0 and 1)			
	outside	inside	Total
Sample number(N)	12	26	38
Mean abnormal return	-0.857%	-1.487%	
t-statistic	0.726	-2.418**	
Median abnormal return	-0.357%	-1.122%	
Wilcoxon signed-rank Z-statistics	-0.706	-2.273**	
% abnormal return negative	58.3%	73.1%	
Sign test Z-statistic	–1)	-2.157**	

1) Binomial distribution used.
2) All tests are one-tailed: *p < 0.10; **p < 0.05; ***p < 0.01.



〈Figure 2〉 Average Cumulative Abnormal Return Trend when ARs are Cumulated on a Daily Basis(starting on the day after the event day, to 60 days after the event day)

우리는 '사건기간' 후에 의미있는 시장반응이 있었는지를 알아보기 위해 표본 기업의 정보유출사건이후 비정상수익율을 분석하였다. 사건일 이후 60일간의 사건기간에 대한 비정상수익율을 추정하였다. 일반적으로 한 달에 20일의 거래기간이 있으므로 사건일 이후 3달간의 비정상 수익율을 추정한 것이 된다. 60일 평균 누적비정상누익율(CAR)은 -4.57%이고, 단측검정(5% 유의수준)에서 0과 유의미하게 다름을 나타내었다.

장기의 '누적 비정상수익률(CAR)'은 부정확한 추론을 도출할 수 있는 방법론적 문제가 있다. 우리는 추가적으로 '매입보유 비정상수익률(Buy-and-Hold Abnormal Return; BHAR)'을 사용하여 정보유출의 장기효과를 검증하였다[1, 20].

$$R_{i,t} = \Pi_k(1+r_{i,t+k})-1,\ R_{m,t} = \Pi_k(1+r_{m,t+k})-1$$
$$BHAR^i_{t,t+K} = \Pi_k(1+r_{i,t+k})-\Pi_k(1+r_{m,t+k})$$

결과의 견고성(robustness)를 검증하기 위해, 대응표본(KOSPI 등 시장지수)과 표본 기업간의 보유기간 수익율을 비교함으로 60일 '매입보유비정상수익율'을 추정하였다. 평균 60일 매입보유 비정상수익률은 -3.23%이고 단측검정(10% 유의수준)에서 0과 유의미하게 다름을 나타내었다(p-value = 0.057).

우리는 고객 정보유출 규모에 따른 효과를 측정하기 위해 표본을 유출규모에 따라 사분위수(quartile)로 나누었다. 1사분위(중앙값 13,442건)안의 사건을 4사분위(중앙값 11,595,000건)안의 사건의 시장반응과 비교하였다. 정보유출 규모에 따른 시장반응을 살펴보기 위해 각 집단을 t-검정과 비모수 통계기법인 Mann-Whitney Z 검정을 사용해 평균과 중앙값의 차이를 분석하였다. 분석결과 통계적으로 유의미한 차이가 나타나지 않았다. 이는 정보유출규모가 시장반응에 통계적으로 유의미한 영향을 미치지 못함을 제시한다.

개인정보유출사고는 고객의 개인정보를 이용해 판촉에 사용하는 등 정보가 직접 돈으로 연결되는 통신 등 IT 업계에서 자주 발생했다. 이는 개인정보유출 사건의 처벌보다 금전적 이득이 더 커서 보안사건이 자주 일어난다고 볼 수 있다. 우리는 업종기준으로 산업을 IT기업과 Non-IT기업으로 구분하여 사건일 비정상수익율의 그룹 간 평균과 중앙값의 차이를 검정하였다. IT기업의 평균(중앙값) 비정상수익율은 -1.41%(-1.24%)이고 Non-IT기업의 평균(중앙값) 비정상수익율은 0.06%(0.18%)이다. 비정상수익율의 평균(중앙값)차이가 -1.47%(-1.42%)로 나타났다. 5%수준에서 두 개의 기업유형간 비정상수익율에 통계적으로 유의미한 차이가 있다고 할 수 있다.

기업크기에 따른 차이는 이론적 방향에 부합하나 통계적으로 유의미하지는 않았다. 소규모기업은 평균(중앙값) 비정상수익율이 -2.46%(-1.26%)이고 대규모 기업은 -0.89%(-0.64%)

〈Table 5〉 Industry Descriptions of Information Breach Firm

Industry Type(sample)	Mean(Median) Abnormal Return	Examples
IT(23)	-1.41%(-1.24%)	Telecom, Game, Internet
Non-IT(15)	0.06%(0.18%)	Finance, Education
total(38)		

〈Table 6〉 Event Period Abnormal Returns for the Variables (Day 0)

	Breach Size	Industry Type	Firm Size	Breach Time
Mean difference	-0.294%	-1.472%	-1.574%	-0.215%
t-statistic	-0.226	-1.822**	-1.271	-0.254
Median difference	0.771%	-1.417%	-0.622%	-0.347%
Z-statistic1)	-0.076	-2.105**	-1.058	-0.971

1) Mann-Whitney test Z-statistic.
2) *p < 0.10; **p < 0.05 ; ***p < 0.01.

이었다. 비정상수익율의 평균(중앙값)차이는 -1.57%(-0.62%)가 있으나 통계적으로 유의미한 값을 나타내지는 않았다. 이는 기업의 크기가 정보유출 사건 발생에 따른 시장반응에 영향을 주지 못하였음을 제시한다.

국내 '개인정보보호법' 시행전의 평균(중앙값) 비정상 수익률은 -0.92%(-0.33%)인 반면 시행 후는 -0.70% (0.02%)이었다. 평균(중앙값) 차이는 통계적으로 유의미하지는 않지만 -0.22% (-0.35%)를 보여 법 시행 이후 오히려 시장에 미치는 영향이 줄어들었다.

4. 결론 및 요약

우리의 연구결과는 다음과 같은 흥미로운 함의를 가지고 있다. 첫째, 시장은 정보유출의 원천이 내부이냐 외부이냐에 따라 상이한 반응을 보이고 있다. 내부 원천에 의한 정보유출은 시장반응에는 완전히 반영되지 않았겠지만 브랜드로열티, 고객만족 등 비유형적 형태로 기업가치에 부정적 영향을 주었을 가능성이 외부원천의 경우보다도 크다고 볼 수 있다. 다양한 정보유출 사고가 있지만, 기업은 관리소홀 혹은 악의적 내부에 의한 정보유출 방지를 위한 내부정보관리에 우선적으로 관심을 기울일 필요가 있음을 알 수 있다.

둘째, 정보유출 사건 이후 기업의 주가는 장기적으로 부정적 영향을 받고 있다. 사건일 이후 60일간의 '누적비정상수익률(CAR)'뿐 아니라 '매입보유 비정상수익률(BHAR)'을 통한 주가 분석에서 정보유출이 시장에 장기적으로 부정적 영향을 주고 있었다. 이는 기업이 정보유출사고의 예방이 중요하지만 유출사고가 발생할 경우 임시방편적 대책을 세울 것이 아니라 즉각적이고도 근본적인 사후 대책을 수립하는 것이 매우 중요함을 보여준다.

셋째, 정보유출은 기업유형에 따라 시장반응이 상이하다. 통신, 게임, 인터넷 등으로 대표되는 IT기업의 비정상수익율이 Non-IT기업보다 유의미하게 높게 나타났다. IT기업의 경우 많은 개인정보를 취급 보유하고 있어 이에 맞는 기술관리적 보호조치를 갖추어야 함에도 불구하고 미비한 보호조치로 개인정보가 누출되었고 이는 보다 높은 고객불만요소로 작용해 기업가치에 더 큰 피해를 주었다고 볼 수 있다.

4.1 연구의 요약

이 논문은 국내에서 발생한 정보유출이 기업가치에 미치는 영향을 사건연구방법론을 이

용하여 분석한 의의가 있다. 기업의 정보유출은 기업가치에 유의미하게 부정적인 영향을 미치고 있고 특히 내부원천에 의한 정보유출이 의미 있는 영향을 주고 있었다. 또한 정보유출은 기업의 장기성과에 부정적인 영향을 미치고 있음이 검증되었다. 정보유출 규모와 유출시점은 모두 시장에 영향을 주지 못하고 있었다. 기업크기가 시장반응에 주는 영향은 이론적 방향에는 부합하였으나 시장에 통계적으로 유의미한 영향을 미치지는 못하였다. 한편 기업을 IT와 Non-IT 유형으로 구분하여 비정상수익률을 통계적으로 검정한 결과 유형간 유의미한 차이가 있었다.

4.2 연구 한계 및 추후 연구방향

본 연구는 '정보유출이 시장에 미친 피해'를 측정하는 변수로 '유출사건에 따른 시장반응'을 대리변수(proxy)로 사용하였다. 정보유출이 발생했을 때 이를 공표하지 않거나 기사화되지 않는 경우도 상당히 있어 분석대상의 선정에 한계점을 갖고 있다. 사건연구방법이 기업의 재무성과를 연구하는데 잘 적용되는 방법론이나, 이는 상장기업에만 제한되고 시장데이터의 내재적 오류가 주가변화 측정에 영향을 줄 수 있다. 대안으로 정보유출피해가 '비용상승과 수익감소'를 통해 '기업가치(재무성과)'에 미치는 영향을 회계기반의 측도를 도입해 평가하는 방안을 검토할 수 있겠다. 본 연구가 기업가치에 초점을 맞추고 있으나, 향후 고객만족, 유지율, 추천율 등으로 측정된 고객로열티를 가치척도로 살펴볼 수 있겠다.

향후 연구대상은 첫째, 공공기관을 통한 정보유출 분야이다. 행정전산망이나 관공서 보유의 개인정보는 예산이 없으면 보안투자가 안되어 정부기관의 개인정보유출 또한 심각한 상황이다. 둘째, 개인 스마트폰을 통한 기업정보 접근이 점차 증가하면서 기기의 분실과 도난에 따른 정보유출의 가능성이 증가하고 있다. 스마트폰 보안에 대한 통제시스템과 신속한 사후 대응의 차이에 따른 영향 연구도 흥미로울 것이다. 셋째, 일반적으로 경영자는 기업가치에 큰 영향을 미치는 내부요인에 따른 손실을 간과하기 쉽다. 외부원천에 의한 가치손실뿐 아니라 내부직원 관련한 정보유출을 최소화하기 위해 경영자는 어떻게 내적 통제를

〈Table 7〉 Results for the Hypothesis

Hypothesis	Results	Significance
H1-1: The market reacts negatively to information breach of the firm.	Accepted	$p < 0.05$
H1-2: The market reaction to inside source is greater than that for outside source.	Accepted	$p < 0.05$
H2: The market reacts negatively to information breach over long period.	Accepted	CAR: $p < 0.05$ BHAR: $p < 0.1$
H3: The market reactions will differ by the size of the data breach.	Rejected	$p > 0.1$
H4: The market reaction of IT firm is greater than that of Non-IT firm	Accepted	$p < 0.05$
H5: The market reaction is greater for small firms than for large firms.	Rejected	$p > 0.1$
H6: The market reactions will differ by the time.	Rejected	$p > 0.1$

효과적으로 할 것인가에 대한 연구가 필요하다.

기업들이 개인정보 데이터를 다양하게 활용하는 사례가 늘고 있다. 데이터를 어떻게 수집, 관리 분석하고 활용할 것인가가 중요한 전략 과제로 대두되고 있다. 이때 고려되어야 할 요소가 정보보호이다. 관련 법의 통합 정비 등 사회 안전망 마련이 필요하며, 기업은 개인정보 유출의 사전예방 및 효과적인 사후대책의 중요성을 인식해야 할 것이다.

References

[1] Barber, B. M. and Lyon, J. D., "Detecting long-run abnormal stock returns: the empirical power and specification of test-statistics," Journal of Financial Economics, Vol. 43, pp. 341-372, 1997.

[2] Beaver, W. H., "The Information Content of Annual Earnings Announcements," Journal of Accounting Research, Vol. 6, pp. 67-92, 1968.

[3] Brown, S. J. and Warner, J. B., "Using Daily Stock Returns : The Case of Event Studies," Journal of Financial Economics, Vol. 14, pp. 3-31, 1985.

[4] 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. 69-104, 2004.

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

[6] Fama, E. and French, K., "The cross-section of expected stock returns," Journal of Finance, Vol. 47, No.2, pp. 427-465, 1992.

[7] Garba, A. B., Armarego, J., Murray, D., and Kenworthy, W., "Review of the information security and privacy challenges in BYOD environments," Journal of Information privacy and security, pp. 38-54, 2015.

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

[9] 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.

[10] Hendricks, K. B. and Singhal, V. R., "Does Implementing an Effective TQM Program Actually Improve Operating Performance?: Empirical Evidence from Firms that Have Won Quality," Management Science, Vol. 43, No. 9, pp. 1258-1274, 1997.

[11] Hendricks, K. B. and Singhal, V. R., "The effect of supply chain glitches on shareholder wealth," Journal of Operations Management, Vol. 21, No. 5, pp. 501-522, 2003.

[12] Hovav, A. and D'Arcy, J., "The impact of virus attack announcements on the market value of firms," Information System Security, Vol. 13, No. 3, pp. 46-156, 2004.

[13] Hovav, A. and Han, J. Y., "The Impact of Security Breach Announcements on the Stock Value of Companies in South Korea," The Journal of Internet Electronic Commerce Research, Vol. 13, No. 3, pp. 43-67, 2013.

[14] Information Shield Inc., "Privacy Breach Impact calculator,"(http://www.informationshield.com/privacybreachcalc.html).

[15] Jeong, S. H. and Cho, H. S., "A study on frame transition of personal information leakage, 1984~2014: social network analysis approach," Journal of Digital Convergence, 2014.

[16] JNSA, "Information Security Incident Survey Report," 2004.

[17] Kannan, K., Rees, J., and Sridhar, S., "Market Reactions to Information Security Breach Announcements: An Empirical Analysis," International Journal of Electronic Commerce, Vol. 12, No. 1, pp. 69-91, 2007.

[18] Kim, C. W. and Kim, K. Y., "Measuring Security Price Performance in Event Studies," Korean Journal of Financial Studies, Vol. 20, No. 1, pp. 301-327, 1997.

[19] Kim, J. Y., "Analyzing Effects on Firms' Market Value of Personal Information Security Breach," The Journal of Society for e-Business Studies, Vol. 18, No. 1, pp. 1-12, 2013.

[20] Kothari, S. P. and Warner, J. B., "Measuring long-horizon security price performance," Journal of Financial Economics, Vol. 43, pp. 301-339, 1997.

[21] Kwon, H., Lee, E. J., Kim, T. S., and Jun, H. J., "Estimating Compensation for Personal Information Infringement in Korea Using Contingent Valuation Methods," Journal of The Korea Institute of Information Security and Cryptology, Vol. 22, No. 2, pp. 367-377, 2012.

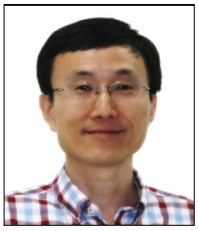
[22] Kwon, Y. O. and Kim, B. D., "The Effect of Information Security Breach and Security Investment Announcement on the Market Value of Korean Firms," Information Systems Review, Vol. 9, No. 1, pp. 105-120, 2007.

[23] Nam, D. W., Park, J. W., Kim, M. K., Jo, H., and Kim, S. H., "A Study about Correlation Between Collective Intelligence On The Internet Stock Message Board And Stock Market," Korea Internet Electronic Commerce Association, Vol. 12, No. 2, pp. 149-164, 2012.

[24] Ponemon Institute, "Cost of Data Breach Study: Global Analysis," 2005~2014.

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

저 자 소 개



권순만 (E-mail: sunman86@hanmail.net)
1990년 연세대학교 경제학 (학사)
2005년 Helsinki School of Economics MBA
현재 한양대학교 경영컨설팅학과 (박사과정)
kt 재직
관심분야 ICT/디지털마케팅, 프로젝트관리, 혁신&변화관리, 전략의사결정 등

한창희 (E-mail: chan@hanyang.ac.kr)
1992년 한양대 산업공학과 (학사)
1994년 한국과학기술원 산업공학과 (석사)
1999년 한국과학기술원 경영공학과 (박사)
Georgia Institute of Technology 초청연구원
Rutgers Univ. 교환교수
현대정보기술, 오픈타이드 컨설팅 수행
현재 한양대학교 ERICA 캠퍼스 경영학부 교수
관심분야 ICT융합서비스, 전략의사결정분석, 기술혁신