Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.23, NO.6, Dec. 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.6.1207

정보보호 투자와 침해사고의 인과관계에 대한 실증분석

신 일 순,† 장 원 창,‡ 박 희 영
인하대학교

Information Security Investment and Security Breach: Empirical Study on the Reverse Causality

Ilsoon Shin,† Wonchang Jang,‡ Heeyoung Park
Inha University

요 약

본 연구는 2010년 한국인터넷진흥원에서 조사한 "기업의 정보보호 실태조사"의 원자료를 패널데이터로 재구성하여 정보보호 투자와 침해사고의 인과관계를 분석하였다. 이중차분법을 이용하여 분석한 실증결과는 다음과 같다. 첫째, 정보보호투자가 침해사고를 줄인다는 통상적인 인과관계에 대해서는 유의미한 실증적인 근거를 발견하기 어려웠던 반면, 역의 인과관계, 즉 침해사고가 많은 기업이 정보보호 투자를 증가시킨다는 가설은 유의미하게 데이터에 의해 입증되는 것으로 나타났다. 둘째, 정보보호에 매우 민감하기 때문에 다른 업종에 비해 과감한 사전적인 투자를 수행하는 것으로 인식되고 있는 금융/보험업의 경우, 실증분석에 따르면 오히려 침해사고의 발생에 따라 사후적으로 정보보호 투자를 수행하고 있는 대표적인 업종으로 나타났다.

ABSTRACT

This study utilizes raw data from "Research on the actual condition of firms' information security" of KISA (2010) and constructs panel dataset to analyze a causal relationship between information security investment and security breach. Using Difference in Difference estimation method we find the following results. First, while the usual causality that information security investment reduces security breach is not supported, the reverse causality that security breach increases information security investment is well explained. Second, contrary to the conventional wisdom, firms in the finance/insurance business sector show the most significant reverse causality pattern.

Keywords: Information Security Investment, Security Breach, Difference-in-Differences, Reverse Causality

I. 서 론

인터넷의 확산과 네트워킹의 일상화가 진행되면서 사회 전반적으로 정보보호(information security)의 중요성이 증가하고 있다. 특히 치열해지는 경쟁 환경에서 자신의 비즈니스를 지속적이고 안정적으로 수행하는 것이 기업의 경쟁우위 확보의 전제 조건이라는 점을 고려할 때 기업의 위험관리차원에서 정보보호의 필요성이 높아지고 있다[1]. 정보보호와 안정적 비즈니스 수행의 관계에 대한 사례는 수없이 많은데, 국내의 경우 2011년 이후 SK컴스(3,500만 명), 넥슨(1,320만 명), 현대캐피탈(175만 건) 등의 기업에서 해킹을 통한 대규모 개인정보 유출사고가 지속적으로 발생한 바 있으며, 이에 대한 시시비비를 가리기 위한

접수일(2013년 4월 4일), 수정일(2013년 10월 14일), 게재확정일(2013년 10월 15일)
† 주저자, ishin@inha.ac.kr
‡ 교신저자, wjang@inha.ac..kr(Corresponding author)

소송이 현재까지도 진행되고 있는 것을 들 수 있다. 한국의 경우 개인정보 유출 규모는 2011년 5048만 건, 2012년 1293만 건이며, 비금융분야와 금융분야가 각각 6148만 건, 193만 건으로 집계되었다. 해외 정보보안업체인 Symantec과 Ponemon의 분석(2013) 에 따르면, 정보 침해사고 후 고객 이탈비율이 미국의 경우 2.8%, 프랑스는 4.4%에 달하는 것으로 나타났다. 이러한 사례는 정보보호가 기업의 안정적인 비즈니스를 영위하기 위해 필요할 뿐만 아니라 기업의 가치창출 원천이 유형 자산에서 무형 자산 중심으로 변화되는 상황을 고려할 때 그 중요성은 더욱 높아지고 있다. 즉, 기업의 중요한 무형 자산으로 보호되어야 하는 정보의 가치는 날로 증가하고 있으며, 이에 대한 효율적이고 효과적인 정보 자산관리와 정보보호 투자에 대한 중요성이 부각되고 있다. 이에 따라 정보보호 투자에 대한 이해관계자들의 책임과 권한, 그리고 정보보호 투자의 대상 및 투자 기준을 명확히 정의하고, 정보보호 투자에 대한 효과를 분석하여 그 성과를 극대화하는 것이 중요한 이슈가 되고 있다. 그럼에도 불구하고 정보보호 성과 측정을 위한 체계적인 방법이 제시되지 못하고 있으며, 정보보호 투자 효과를 계량적으로 추정하는 연구가 부족하여 효과적이고 적절한 정보보호 투자 수준에 대한 기업의 의사결정에 어려움이 있는 것이 현실이다[2].

특히 정보보호 투자의 정량적 효과를 실증적으로 분석하기 위해서는 정보보호 투자에 대한 데이터 및 침해사고 건수, 피해액 등 정보보호 투자의 효과를 나타내는 데이터의 존재가 필수적이다. 그러나 정보보호 투자 및 침해에 대한 데이터가 필연적으로 가질 수밖에 없는 정보의 민감성 때문에, 외부 연구자가 특정 기업으로부터 데이터를 수집하는 것이 매우 어려운 것이 사실이다. 미국 기업을 대상으로 정보보호 투자의 효과를 추정하는 모델을 설정하고 이를 위해 데이터를 수집하려 시도하였던 연구[3]에서 응답 기업의 불충분한 답변으로 인해 분석을 완료하지 못하였던 경험은 이러한 정보보호 관련 데이터의 민감성과 수집의 어려움을 대변한다고 볼 수 있다. 이를 반영하여, [3]에서는 "정보보호와 관련된 정확한 정보를 주요 기관의 도움 없이 해당 기업 조직으로부터 추출한다는 것은 거의 불가능하다(We conclude that it is nearly impossible to extract information of this nature by mail from business organizations without having a major supporter.)"라고 결론을 내리고 있다. 이러한 정보보호와 관련된 데이터 및 그 수집의 특유한 성격에 따라 기존의 대다수 관련 연구가 정보보호 투자의 효과에 대한 실증적이고 계량적인 연구보다 이론적으로 정보보호 투자의 최적 수준이 어떠한지에 대한 논의에 집중되고 있는 상황이다[4].

데이터의 부족 이외에도 정보보호 투자의 효과를 실증적으로 연구하는 것이 가지는 어려움은 다른 투자 활동과 정보보호 투자 활동과의 차이점을 비교할 때 확연히 드러난다. 일반적으로 기업의 정보보호 투자는 이로 인한 긍정적인 가치나 수익 창조의 기회 제공보다는 투자를 하지 않았을 때 발생하는 부정적인 피해 위험을 감소시키기 위해 그 필요성이 강조되는 분야로 볼 수 있다. 이러한 정보보호 투자의 특유한 특징은 기업의 정보보호 투자가 적절한 수준에 비해 과소하게 수행되고 있는 현실적인 상황에 대한 하나의 이유로 지적되고 있다[5][6].

그런데 이러한 정보보호 투자 효과에 대한 실증 분석의 어려움과 특이성에도 불구하고, 국내의 경우 상당 기간에 걸쳐 한국인터넷진흥원에서 "기업의 정보보호 실태조사"를 수행하여 왔다. 이 조사는 패널데이터(panel data)의 특성을 가지지는 않지만[1], 다른 나라에서 쉽게 조사되지 않는 정보보호에 대한 여러 가지 내용을 설문 방법을 통해 비교적 다수(2010년의 경우 6,000개 이상)의 기업들에 대해 체계적으로 조사한 자료이다. 특히 이 조사의 항목 중에는 정보보호 투자 및 침해 현황에 대한 내용을 포함하고 있고, 매우 흥미롭게도 투자 및 침해 건수의 전년 대비 증가율에 대한 데이터가 있기 때문에 이를 이용하면 두 기간에 걸친 패널데이터로 재구성할 수 있다. 따라서 "기업의 정보보호 실태조사"의 원자료(raw data)를 활용하여 기업 수준(firm-level)에서 정보보호 투자 및 침해의 현황에 대한 데이터와 적절한 패널데이터 분석 방법을 통해 정보보호 투자의 효과를 추정하는 것이 가능해진다.

특히 본 연구에서는 정보보호 투자 효과에 대해, 인과관계를 이중차분법(Difference-in-Differences)을 이용하여 살펴보는 것을 주제로 삼고 있다. 그 이유는 첫째, 위에서 언급한 정보보호 분야의 특이성에 따라 정보보호 투자가 침해사고의 건수를 감소시킬 것이라는 일반적인 인과관계에 대한 믿음이 과연 실제 데이터에 의해 지지되는지를 살펴보고자 함이다. 둘째, 역시 정보보호 데이터의 특이성 때문에 정보보호

1) 다른 말로, 동일한 기업에 대해 다년간 조사를 수행한 것은 아니고, 매년 조사대상 기업이 바뀐다는 의미이다.

투자를 수행하지 않은 기업과 침해사고를 경험하지 않은 기업이 전체 샘플에서 대다수로 나타나고 있어, 일반적인 실증분석 방법과 차별화하여 이러한 특징을 적절히 통제하는 실증적인 방법이 필요하기 때문이다.

본 논문은 다음과 같이 구성되었다. 먼저 Ⅱ장에서는 정보보호 투자 및 침해에 대한 자료를 이용하여 실증분석을 수행할 경우에 발생할 수 있는 내생성의 문제를 제시하고, 이중차분법이 필요한 이유를 서술한다. Ⅲ장에서는 본 연구에서 사용한 데이터 및 주요 변수들을 소개한다. Ⅳ장에서는 과연 정보보호 투자와 침해사고 간의 일반적인 인과관계와 역의 인과관계 중 어떠한 것이 적절한지에 대한 실증분석과 업종별 역의 인과관계 여부를 분석하며, Ⅴ장은 요약 및 결론이다.

Ⅱ. 내생성 문제와 이중차분법

2.1 내생성(endogeneity) 문제

본 장에서는 기업의 정보보호 투자와 정보보안 침해사고에 대한 데이터가 존재하는 경우를 상정하고, 일반적인 실증분석을 행할 경우에 어떠한 문제점이 발생하는지를 살펴보기로 한다. 편의상 정보보호 투자의 정보보안 침해사고에 대한 효과를 분석하기 위해 N개 기업의 데이터가 있는 경우를 상정하자. 이에 부가하여 만일 기업 $i(\in[1, N])$가 정보보호 투자를 수행하였다면 $X_i = 1$로, 투자를 하지 않았으면 $X_i = 0$으로 나타내며, 정보보호 투자를 수행한 기업의 수를 N_1, 그렇지 않은 기업의 수를 N_0이라고 하자. 즉, $N = N_0 + N_1$이다. 한편, Y_i는 기업 i가 경험한 정보보안 침해사고 건수를 나타내는 변수로 상정한다.

일반적인 실증분석의 방법의 경우는 다음과 같은 간단한 회귀식(regression equation)을 추정하여 정보보호 투자의 효과를 분석한다.[2)]

$$Y_i = \alpha + \beta X_i + \epsilon_i \tag{1}$$

여기서 ϵ_i는 오차항이고, 식 (1)의 β에 대한 OLS(Ordinary Least Square) 추정치는 다음과 같이 표현된다.

$$\hat{\beta}_{OLS} = \frac{\sum_{i=1}^{N}(X_i - \overline{X})(Y_i - \overline{Y})}{\sum_{i=1}^{N}(X_i - \overline{X})^2} \tag{2}$$

식 (2)에서 변수 위에 막대(bar)가 있는 것은 해당 변수의 평균값을 의미한다. 식 (2)를 $N = N_0 + N_1$ 및 X_i의 정의를 이용하면 풀어 보면, 다음과 같은 식이 도출된다.

$$\begin{aligned}\hat{\beta}_{OLS} &= \frac{1}{N_1}\sum_{i\in N_1} Y_i - \frac{1}{N_0}\sum_{i\in N_0} Y_i \\ &= (\overline{Y}|X=1) - (\overline{Y}|X=0)\end{aligned} \tag{3}$$

식 (3)이 의미하는 것은 정보보호 투자의 침해사고에 대한 효과를 추정하는 OLS 추정치가 정보보호 투자를 수행한 기업에서 발생한 침해사고 건수의 평균값에서 투자를 하지 않은 기업에서 발생한 침해사고 건수의 평균값을 뺀 값이라는 것이다. 이 추정치가 불편(unbiased) 추정량[3)]인지를 살펴보기 위해 기대값을 취하면,

$$\begin{aligned}E[\hat{\beta}_{OLS}] &= E\left[\frac{1}{N_1}\sum_{i\in N_1} Y_i - \frac{1}{N_0}\sum_{i\in N_0} Y_i\right] \\ &= E\left[\frac{1}{N_1}\sum_{i\in N_1}(\alpha+\beta+\epsilon_i) - \frac{1}{N_0}\sum_{i\in N_0}(\alpha+\epsilon_i)\right] \\ &= \beta + \left[E(\epsilon_i|X_1=1) - E(\epsilon_i|X_1=0)\right]\end{aligned} \tag{4}$$

식 (4)에서 마지막 항의 괄호 안이 0이 되면 OLS 추정치는 불편추정량이 되어 정보보호 투자의 침해사고에 대한 효과를 적절히 측정하게 된다. 그런데 여기서 마지막 항이 0이 된다는 것은 정보보호 투자를 수행한 기업과 그렇지 않은 기업의 관측 불가능한 오차항의 평균값이 같다는 것을 의미한다. 과연 이 두 값이 같을 것으로 생각할 수 있는가? 일반적으로 다른 것으로 보는 것이 합당할 것이다. 즉 정보보호를 수행한 기업과 그렇지 않은 기업으로 구분하여 보면, 두 집단은 정보보호 투자 활동이외의 다른 측면에서 서로 다른 특성을 가지기 때문에 정보보호 투자 행동을 서로 다르게 수행한 것으로 보는 것이 더 정확할 것이다. 예를 들어, 정보보호 투자를 수행하는 기업은 그렇지 않은 기업에 비해 미래의 위험에 대비하는 능력

2) 선형 회귀분석의 경우, 기본 가정으로 정규성, 독립성, 선형성, 등분산성 등이 전제되어야 하며, 독립변수들간 상관관계로 인해 발생하는 다중 공선성(multicollinearity) 문제가 대표적인 한계점으로 지적된다.

3) 여기서 불편추정량이라 함은 추정계수의 기대값이 모수와 일치하는 경우, 즉 $E[\hat{\beta}_{OLS}] = \beta$가 성립함을 의미한다.

이 우월하거나 과거에 침해사고의 경험이 많은 기업일 가능성이 크다. 그렇다면 두 집단 간에 관측 불가능한 오차항의 평균값이 동일하다고 볼 수 없게 되어 OLS 추정치에 편의(bias)가 발생하게 된다. 이 문제를 해결하기 위해 정보보호 투자이외에 침해사고에 영향을 미칠 것으로 예측되는 다른 통제변수 Z_i 를 식 (1)에 추가하면 다음의 식 (5)로 바뀌게 된다.

$$Y_i = \alpha + \beta X_i + \gamma Z_i + \epsilon_i \quad (5)$$

그런데 이 회귀모형에 대해 OLS를 통해 β 를 추정하는 경우, 추가되는 변수가 정보보호 투자와 오차항 간의 상관관계를 완전히 없애지 못하는 한, 즉 $Cov(X_i, \epsilon_i) \neq 0$ 이 성립하면, OLS 추정치는 계속해서 편향성을 가지게 된다. 만약 $Cov(X_i, \epsilon_i) > 0$ 이면 양(+)의 편의가 발생하고, $Cov(X_i, \epsilon_i) < 0$ 이라면 음(-)의 편의가 발생한다.

일례를 들어 경찰이 늘어나면 범죄가 줄어들 것인지를 분석하기 위해 지역별로 범죄발생 건수(Y_i)와 경찰의 수(X_i) 및 그 지역의 특성을 나타내는 정보(Z_i)를 수집하여 자료로 모았다고 하자. 이 자료를 이용하여 식 (1)과 같이 OLS 추정을 하면 일반적으로 X_i 의 계수값이 양(+)으로 추정된다. 즉 경찰의 숫자가 많을수록 오히려 범죄가 늘어나는 것으로 해석된다. 상식에 어긋나는 결과를 보고 Z_i 를 포함시켜 식 (5)를 추정하여도 결과는 크게 변화하지 않는다. 즉, 통제변수를 늘리는 것이 도움이 되지 않는다. 왜 이러한 결과가 나타나는가? 사실은 경찰이 많을수록 범죄가 늘어나는 것이 아니라 범죄가 많은 지역에 경찰을 많이 투입하였기 때문이다.

정보보호의 측면에서도 이러한 편의가 실제로 발생하는지를 살펴보기 위해 정보보호 투자 및 침해사고에 대한 우리나라의 데이터를 이용하여 간단한 OLS로 추정해 보도록 한다. 실증분석을 위한 회귀식은 식 (1)과 식 (5)이며, 정보보안 침해사고에 대한 정보보호 투자의 효과를 분석하는 회귀식 추정의 결과는 다음과 같다.[4)]

$$Y_i = 0.29 + 1.53 X_i$$
$$(0.047) \quad (0.072)$$
$$Y_i = -0.62 + 1.10 X_i + other\ controls$$
$$(0.104) \quad (0.074)$$

4) 이 결과는 [11]에서 조사된 전체 기업을 대상으로 한 것이다. 보다 자세한 자료의 소개는 이하에서 다루어진다.

여기서 괄호안의 값은 추정오차이다. 처음의 추정식은 정보보호 투자와 침해사고만을 고려한 것이고, 두 번째 식은 침해사고에 영향을 미칠 다른 변수들을 고려한 것이다.[5)] 위의 추정결과에 따르면, 정보보호 투자를 더 많이 할수록 정보보안 침해사고의 건수가 "오히려 유의미하게 증가"한다는 결론이 도출되며, 이러한 양의 관계는 다른 통제변수를 포함시키더라도 큰 변화가 없는 것으로 나타난다. 이러한 추정결과는 정보보호 투자로 인해 그동안 인지하지 못하던 침해사고를 인지하게 된데 기인할 가능성이 있다.[6)]

2.2 이중차분법(Difference-in-Differences)

이와 같이 통상적인 선형회귀모형에서 주요 설명변수(여기서는 정보보호 투자)와 모형의 오차항이 통계적으로 서로 독립적이지 않고 체계적인 양(+) 또는 음(-)의 상관관계가 있는 경우에 내생성(endogeneity)이 존재한다고 말한다. 내생성이 존재할 경우에는 설명변수가 종속변수에 영향을 미치는 정도가 실제의 효과를 과소 또는 과대 추정되게 되며, 극단적인 경우에는 내생성이 통제되지 않은 채 도출된 추정 결과와 실제 인과관계가 반대 방향이 되기도 한다.

이러한 내생성 문제의 완전한 해결은 관측대상이 처리집단(treatment group)과 통제집단(control group)으로 - 위의 예에서는 정보보호 투자를 행하는 기업과 그렇지 않은 기업으로 - 무작위 배정(random assignment)되는 경우에만 가능하게 된다. 일반적으로 실험(experiment)을 통해 무작위 배정이 가능한 자연과학 분야와는 달리 사회과학 분야에서는 무작위 배정이 어렵기 때문에 많은 설명변수를 포함시키거나 복잡한 통계방법을 활용하여 인과효과를 구하는 데 집중해 왔다. 그러나 최근의 여러 실증경제학 연구들은 이러한 문제를 비교적 간단하게 해결하는 방법들을 제시하고 있다.

본 연구에서는 이러한 방법 중에서 이중차분법(Difference-in-Differences)을 이용하여 정보보호 투자의 효과 및 정보보호 투자와 침해사고의 인과관계를 살펴보고자 하였다. 이중차분법을 간단히 설명

5) 구체적으로 기업의 규모, 기업이 속하는 산업, 기업의 사업형태 등을 통제변수로 포함하였다.

6) 이를 고려할 경우 정보보호투자와 침해사고 피해규모간 상관관계에 대한 실증분석이 필요한데, 본 연구가 이용하는 자료에는 피해금액에 대한 내용이 없어 실증적으로 입증하는데 한계가 있다.

하면 다음과 같다. 특정한 처리(treatment) - 여기서는 정보보호 투자 - 가 시간이 지남에 따른 가지는 효과를 측정하려는 연구에서 중요한 방법론적 쟁점은 해당 처리의 순효과(net effect)를 어떻게 측정하는가 하는 것이다. 예를 들어, 정보보호 투자를 수행한 기업이 침해 사고를 감소시키는 효과를 가지더라도, 이 차이가 정보보호 투자 자체의 효과로 인한 것이 아니라 정보보호 투자를 수행한 기업 자체의 속성에 의한 것일 수 있다는 것이다. 이 경우 정보보호 투자 여부와 기타 기업의 (측정되지 않는) 속성들 간에 내생성이 존재할 수 있다. 그러므로 단순하게 정보보호 투자를 수행한 기업과 그렇지 않은 기업을 비교하는 것(위에서 제시한 것처럼 단순 OLS로 분석하는 것)으로는 신뢰성 있는 결과를 얻지 못할 가능성이 존재한다. 이 문제를 해결하기 위해서는 정보보호 투자를 수행한 기업이 이를 수행하지 않았을 경우라는 反사실(counterfactual)과 비교했을 때, 일정 시점 경과 후 나타날 효과의 차이를 추정하는 것이 필요하다.

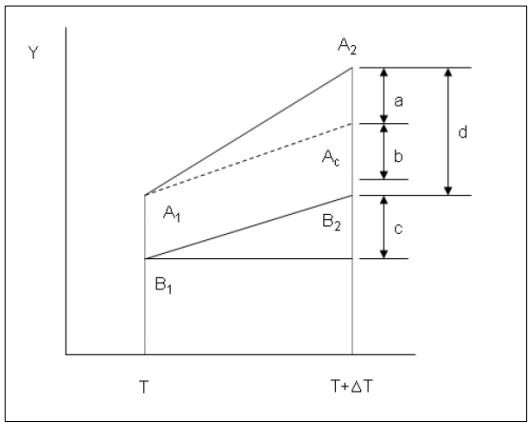

Fig.1. The Outline of Difference-in-Differences
자료) K. W. Kim(2008)

이중차분법에서는 특정 시점에서의 처리집단(여기서는 정보보호 투자를 수행한 기업들)과 통제집단(여기서는 정보보호 투자를 수행하지 않은 기업들)을 식별하고 일정 시간 경과 후 이들 간의 피측정치의 차이를 이중 차감함으로써, 앞서 언급한 기업의 실제 효과와 정보보호 투자를 수행하지 않았을 경우라는 反사실에서의 성과 간의 차이를 추정한다. 이중차분법의 기본 골격을 도식화해 보면 위 Fig. 1.과 같다[7]. Fig. 1.과 같이 처방집단(A_1)과 통제집단(B_1) 간의 $\triangle T$ 기간 이후의 효과의 차이를 측정하고자 할 경우를 고려해 보자. 처방집단과 통제집단 간의 초기 시점의 차이가 없다고 가정할 경우에는 $T+\triangle T$ 시점에서 A_2와 B_2 간의 차이(d)를 단순 측정하게 된다. 그러나 만약 측정하고자 하는 변수에 관해 초기 시점에서 A_1이 B_1에 비해 체계적으로 높은 값을 지니고 있다면, 측정하고자 하는 특정 처리의 효과를 보기 위해서는 A_1이 처리를 받지 않았을 경우 가상의 변화(A_C)와의 차이, 즉 a를 측정해야 한다. 이는 처방집단의 $\triangle T$ 기간 동안의 Y의 변화량($a+b$)에서 처리집단이 처리를 받지 않았을 경우, 즉 정보보호 투자를 수행한 기업이 정보보호 투자를 수행하지 않았을 경우의 변화량(a)을 차감함으로써 측정할 수 있다. 그런데 현실적으로 처리집단이 특정 처리를 받지 않았다는 反사실의 변화량을 측정하는 것은 불가능하기 때문에, 여기서는 처리집단이 처리를 받지 않았을 경우 통제집단과 동일하게 변화할 것이라는 가정(즉, $b=c$) 하에 비교집단의 $\triangle T$ 기간 동안의 변화량(c)을 측정하고 이를 사용하여 a를 추정하게 된다.

이러한 이중차분 모형은 일반적으로 특정 처리(treatment) 더미와 이후 연도 더미 및 이들 간의 교호항을 포함한 회귀모형을 통해 분석될 수 있다[8]. 본 연구의 경우, 정보보호 투자를 통한 순효과는 정보보호 투자 여부 더미(D_X)와 시간 더미(D_T) 및 이들 간의 교호항(D_XD_T)을 포함한 다음과 같은 회귀식을 통해 추정할 수 있다.

$$Y_{i,t}=\alpha+\beta_1 D_X+\beta_2 D_T+\beta_3 D_X D_T+\epsilon_{i,t} \quad (6)$$

위 식 (6)에서 피설명변수인 $Y_{i,t}$는 i 기업의 t 시점에서의 정보보안 침해사고이며, α는 상수항, D_X는 특정 처리 더미(본 연구의 경우 정보보호 투자 여부), D_T는 연도 더미이며, $\epsilon_{i,t}$는 오차항이다. 식 (6)에서 정보보호 투자의 순효과를 알려 주는 계수를 알기 위해 조건부 기대값(conditional expectation)을 계산하면 다음과 같다.

$$E_{11}=E(Y|D_X=1,D_T=1)=\alpha+\beta_1+\beta_2+\beta_3$$
$$E_{10}=E(Y|D_X=1,D_T=0)=\alpha+\beta_1$$
$$E_{01}=E(Y|D_X=0,D_T=1)=\alpha+\beta_2$$
$$E_{00}=E(Y|D_X=0,D_T=0)=\alpha$$

여기서 추정하고자 하는 효과는 Fig. 1.에서 $(a+b)$로 표현되는 처리집단의 시간 효과($E_{11}-E_{10}$)

에서 Fig. 1.에서 (c)로 표현되는 통제집단의 시간 효과($E_{01}-E_{00}$)를 차감한 것이다. 이는 가정($c=b$)에 따라 $(E_{11}-E_{10})-(E_{01}-E_{00})=\beta_3$ 이라는 것을 알 수 있으며, 처리의 순효과는 정보보호 투자 여부 더미(D_X)와 시간 더미(D_T)의 교호항의 계수임을 알 수 있다. 이렇듯 처리집단의 순효과를 추정하는 방법은 차분을 이중으로 하여 도출된다는 의미에서 이중차분법(Difference-in-Differences)라는 이름을 갖게 된다. 식 (6)에 다른 설명변수들(Z_i)을 추가할 수 있으며, 이는 식 (7)로 표현할 수 있다.

$$Y_{i,t}=\alpha+\beta_1 D_X+\beta_2 D_T+\beta_3 D_X D_T+\gamma Z_i+\epsilon_{i,t} \qquad (7)$$

여기서 주의하여야 할 점은 설명변수들을 추가하거나 빼더라도 β_3 의 해석이 달라지지 않아야 한다는 것이다. 식 (6)과 식 (7)을 따로 추정했을 때 β_3 의 추정계수의 값이 크게 다르지 않으면 이중차분법이 잘 적용되었다고 판단할 수 있다.

III. 본 연구의 자료

본 연구에서 사용한 데이터는 Korea Internet and Security Agency(2010)의 "A Survey of 2010's Information Security(Firm)"의 원자료(raw data)이다. Korea Internet and Security Agency는 민간부문의 정보보호 인식 제고를 위한 각종 정책 활동의 성과지표 산출, 국내 정보보호 수준 측정을 위한 각종 지수 산출, 민간부문의 정보보호 통계자료 제공 등을 목적으로 2001년부터(2005년 이후에는 매년) 기업부문의 정보보호에 대한 조사를 실시하고 있다. 2010년 조사의 경우 종업원 5인 이상의 사업체 가운데 네트워크에 연결된 컴퓨터를 1대 이상 보유하고 있는 총 30만개의 사업체를 모집단으로 하고, 11개 업종과 4개 규모(종업원 기준)로 할당한 6,529개의 기업을 표본으로 하여 2010년 9월에서 10월까지 조사하였다.

조사 내용은 시점에 따라 약간의 차이는 있지만, 2010년의 경우 정보보호 정책 수립 및 정보보호 조직 구성 현황, 정보보안 환경 평가 및 위험 요소 평가, 임직원 대상 정보보호 교육 실시 및 정보보호에 대한 투자 현황, 정보보호 제품 사용 현황 및 정보보호 업무 수행 방식, IT관련 신규 서비스 도입 및 보안정책 수립, 보안패치 적용 방식 및 정보시스템 사용자 인증 기법, 웹사이트를 통하여 수집한 개인정보의 유/노출 방지를 위한 대응 현황, 개인정보처리시스템 및 보안서버 구축 현황, 인터넷 침해사고 대응을 위한 활동 및 복구계획 수립/운영 현황, 인터넷 침해사고 및 개인정보 유/노출 피해 경험 및 현황 파악 등으로 이루어져 있다.

본 연구에서는 위의 원자료를 이용하여 한 가지 추가적인 과정을 거쳐서 필요 변수를 추출하였다. 이미 설명한 것처럼 본 연구에서는 정보보호 투자 및 정보보안 침해사고를 두 가지 주요한 변수로 삼고, 통상적인 인과관계 및 역의 인과관계를 이중차분법으로 살펴보고자 한다. 그런데 [9]에 따르면, 이중차분법을 이용하는 경우 처리변수(treatment variable)와 누락변수(omitted variable)간 상관관계(correlation)로 인해 추정결과가 왜곡될 가능성을 고려하여 처리변수의 선택에 유의하여야 한다는 점을 지적하고 있다. 본 연구의 경우 처리변수가 정보보호 투자와 침해사고 여부라는 점에서 누락변수와 상관관계가 높을 가능성이 존재한다. 또한, 기업 자체의 특징에 대한 변수가 소수에 불과하다는 데이터의 한계로 인해 중요하지만 누락되는 변수가 존재할 가능성이 있다. 이러한 문제를 우회하기 위해 본 연구에서는 [10]의 방법과 같이 처리변수 이외의 측면에서 처리집단과 통제집단의 표본을 유사하게 조정하는 방법을 선택하였다. 이를 좀 더 자세히 살펴보기 위해 정보보호 투자 및 정보보안 침해사고에 대한 기본적인 통계치를 소개하면 다음과 같다.

Table 1.에서 나타나는 특징은 먼저 전체 6,529개 기업 중에서 정보보호 투자를 전혀 하지 않은 기업

Table 1. Firms' Characteristics by Information Security Investment and Breach

변수		평균	표준편차	최소값	최대값	관측치수
기업분류	정보보호 투자를 미수행 기업	1.83	0.89	1	5	3,611
	정보보호 투자를 수행 기업	2.61	1.25	1	5	2,918
	정보보안 침해사고 미경험 기업	2.05	1.05	1	5	5,399
	정보보안 침해사고 경험 기업	2.80	1.31	1	5	1,130

(주) 종업원 수를 범주화하여 5-9명인 경우는 1, 10-49명인 경우는 2, 50-249명인 경우는 3, 250-999명인 경우는 4, 1000명이상인 경우는 5의 값을 부여한다.

의 비중이 절반을 초과하는 55.3%이고, 정보보안 침해사고를 경험하지 않은 기업이 무려 82.7%나 된다는 것이다.[7] 이러한 데이터의 특징은 많은 기업이 0의 데이터 값(투자하지 않거나 경험하지 않은 경우)을 가지기 때문에 통상적인 실증분석을 하는 경우에 문제가 발생할 가능성이 있음을 의미한다. 두 번째 특징은 종업원 수를 기준으로 할 때, 기업 규모가 큰 기업이 정보보호 투자를 수행할 가능성이 높고, 동시에 정보보안 침해사고를 경험할 가능성이 높다는 것이다. 즉 전체 기업을 대상으로 분석할 경우에는 [9]에서 제기된 것처럼 처리집단과 통제집단에 처리 변수이외의 내생적인 차이가 존재할 가능성이 높게 된다.

이에 따라 본 연구에서는 민간 기업만을 대상으로 (전체 기업 중에는 회사외 법인 및 국가기관/지방자치단체도 포함되어 있음) 하고, 서비스업만을 대상으로 (전체 기업 중에는 농수산업, 제조업, 건설업 등이 포함되어 있음) 하며, 기업 규모를 종업원 수 기준으로 10~250명인 경우로 제한하여 분석하고자 한다. 이렇게 데이터를 한정지으면 유의할 개연성이 있는 표본을 제외하는 단점이 존재하지만, 이중차분법 이용의 적절성이 증가하는 장점이 존재하게 된다. 위와 같이 샘플을 재구성할 경우 기업 수는 1,845개로 감소하게 되며, 이들 기업을 대상으로 본 연구에서 주요하게 다루고 있는 변수들을 설명하면 다음과 같다.

Table 2. Basic Statistic of Key Variables

변수	평균	표준편차	최소값	최대값	관측치수
정보보호 투자 여부 (itsinv_bin)	0.46	0.49	0	1	1,845
정보보안 침해사고 여부 (dam_bin)	0.17	0.38	0	1	1,845
2009년 정보보호 투자 (itsinv2009)	1.57	2.54	0	25.7	1,845
2010년 정보보호 투자 (itsinv2010)	1,64	2.67	0	20	1,845
2009년 침해사고 건수 (dam2009)	0.87	2.50	0	12	1,845
2010년 침해사고 건수 (dam2010)	0.89	2.57	0	25	1,845

(주) 정보보호 투자 여부 및 정보보안 침해사고 여부는 더미 변수, 연도별 정보보로 투자 변수는 정보화 지출 대비 정보보호 지출 금액의 백분위수, 연도별 침해사고 건수는 컴퓨터 바이러스 공격, 해킹, DoS, DDoS, 애드웨어 및 스파이웨어 감염 등에 대한 기업의 피해빈도를 합산한 것임

7) 특히 침해사고의 경우 기업이 잘못된 보고(false reporting)를 하거나 실제로 침해를 당했지만 인지하지 못했을 가능성도 존재할 것으로 예상된다.

먼저 2010년 정보보호 투자(itsinv2010)는 기업의 연간 정보화 지출 총액 중 정보보호 분야에 지출한 금액의 백분위수이다. 여기서 정보화 지출은 기업의 정보화를 위한 하드웨어, 소프트웨어, 네트워크 등과 관련한 구입, 유지, 보수비용이고, 정보보호 지출은 그 중 방화벽, 침입탐지 시스템, 바이러스 백신, 보안서비스 등과 관련한 구입, 유지, 보수비용이다[11]. 2009년 정보보호 투자(itsinv2009)는 조사에서 직접 설문하고 있지는 않지만, 2010년 정보보호 투자가 전년 대비 어느 정도 증감하였는지를 묻는 항목이 있어 이를 이용하여 역산하였다. 다음으로 2010년 침해사고 건수(dam2010)는 컴퓨터 바이러스 공격, 해킹, DoS(Denial of Service), DDoS(Distributed Denial of Service), 애드웨어/스파이웨어 감염 등에 대해 기업의 피해빈도의 수를 모두 합친 것이다. 2009년 침해사고 건수(dam2009) 역시 정보보호 투자와 마찬가지로 전년 대비 증감의 정도를 묻는 항목을 이용하여 역산하였다. 정보보호 투자 여부(itsinv_bin)와 정보보안 침해사고 여부(dam_bin)는 2009년을 기준으로 정보보호 투자를 수행한 기업과 그렇지 않은 기업, 침해사고를 경험한 기업과 그렇지 않은 기업으로 구분한 더미변수이다.

Table 2.에 따르면 종업원 수가 10~250명인 민간 서비스업을 대상으로 하는 경우, 46%가 정보보호 투자를 수행하였으며, 17%만이 정보보안 침해사고를 경험한 것으로 나타난다. 또한 정보화 지출 대비 정보

Table 3. Basic Statistic of Firm Specific Variables

변수	내용	비율(%)	전체 관측치수
업종 (num2)	도매업	12.79	1,845
	소매업	14.74	
	숙박/음식업	9.38	
	운수업	13.88	
	통신업	9.97	
	금융/보험업	12.95	
	부동산임대업	10.41	
	기타 서비스업	15.88	
규모 (num3)	10-49명	64.72	
	50-250명	35.28	
사업형태 (type1)	단독사업체	49.65	
	본사/본점 등	20.00	
	공장/지사/영업소 등	28.78	
	무응답	1.57	
조직형태 (type2)	개인사업체	24.23	
	회사법인	75.77	

보호 지출은 평균 1.6% 수준으로 매우 적은 것으로 나타나며, 평균 침해건수도 연간 1건 미만인 것으로 나타난다.

주요 변수 이외에 기업의 특성을 나타내는 변수들은 Table 3.과 같다. 여기서 한 가지 유의하여야 할 점은 Table 3.의 변수 내용에서 나타나는 것처럼, 기업 특징에 대한 변수들이 순서에는 의미가 없는 비순서질(non-ordered qualitative) 변수라는 점이다. 따라서 이하의 실증분석에서 비순서질 변수들은 통제(control) 변수의 역할만을 수행하며, 그 추정계수들에 대해서는 특별한 경제적인 의미를 부여하지 않았다.

IV. 실증분석

먼저 통상적인 인과관계의 분석에 대해 살펴보자. 이중차분법을 이용하는 경우 위의 식 (7)과 같은 회귀식을 구성하는데, 만일 사용되는 데이터가 본 연구의 경우와 같이 균형 패널(balanced panel)이면 이를 차분하여 다음과 같이 회귀식을 설정할 수 있다.

$$\triangle Y_i = \tau_0 + \tau_1 D_X + \gamma Z_i + \epsilon_i \quad (8)$$

식 (8)은 두 기간에 걸친 식 (7)을 차분하여 도출된 것으로, 식 (7)을 2010년과 2009년에 대해 구성한 후 차분하면 상수항과 연도 더미는 없어지게 되며, 식 (7)에서 정보보호 투자 여부 더미(D_X)와 시간 더미(D_T)의 교호항의 계수 β_3는 식 (8)에서는 τ_1이 되어 이를 이중차분 추정량으로 간주할 수 있다.

이중차분법의 추정 결과를 통상적인 실증방법과 비교하기 위해 먼저 특정 연도의 정보보안 침해 건수를 피설명변수로 하고 정보보호 투자를 주요한 설명변수로 하는 통상적인 회귀식의 추정 결과를 살펴보면 다음과 같다 (Table 4. 참고).

$$Y_{i,2010} = a_0 + a_1 D_X + a_2 Z_{i,2010} + \epsilon_{i,2010} \quad (9)$$

여기서 $Y_{i,2010}$은 기업 i의 2010년도 침해사고 건수(dam2010)이며, D_X은 기업 i가 2009년도에 정보보호 투자를 수행하였는지 여부(itsinv_bin)를 나타내는 더미변수이며, $Z_{i,2010}$은 업종, 규모, 사업형태, 조직형태 등 기업 i의 특성 변수이다.

Table 4.에서 모형 (1)은 독립변수로 정보보호 투자만을 사용한 경우이며, 모형 (2)는 기타 기업 특성변수를 통제변수로 추가한 것이다. 추정 결과에 따르면, 정보보호 투자를 수행한 기업에서 오히려 유의미하게 정보보안 침해사고 건수가 증가하는 것으로 나타난다. 즉, 연구자가 실증분석 방법의 선택에 있어 충분한 주의를 기울이지 않고 통상적인 방법을 사용하는 경우 정보보호 투자의 효과가 예상과는 반대의 방향으로 나타남을 알 수 있다. 통상적인 분석에서 드러나는 결과가 내생성 문제에 기인하는 것으로 예측할 수 있기 때문에 보다 적절한 추정방법인 이중차분법을 사용하여 식 (8)을 추정한 결과는 Table 5.에 제시되어 있다.

Table 4. Estimation Results of Usual Method

변수	종속변수: 2010년 정보보안 침해 건수(dam2010)	
	모형 (1)	모형 (2)
상수항	0.4949** (0.0217)	-0.5231 (0.3859)
정보보호 투자 (itsinv2010)	0.2467** (0.0679)	0.2297** (0.0244)
업종 (num2)		0.0146 (0.0244)
규모 (num3)		0.3061* (0.1243)
사업형태 (type1)		-0.0945* (0.0477)
조직형태 (type2)		0.2221 (0.1425)
No. obs.	1,845	1,845
R^2	0.064	0.071

(주) 괄호속의 숫자는 추정 오차이며, *, ** 는 각각 통계적 유의수준으로 5%, 1% 내에서 추정계수가 유의미함.

Table 5. Estimation Results of Difference-in-Differences Method (Investment ⇒ Breaches)

변수	종속변수: 2010년 정보보안 침해 건수의 차분 (△dam)	
	모형 (1)	모형 (2)
상수항	0.0202 (0.0156)	-0.0201 (0.0758)
정보보호 투자 여부 (itsinv_bin)	0.0026 (0.0229)	0.0022 (0.0234)
업종 (num2)		-0.0009 (0.0048)
규모 (num3)		0.0017 (0.0246)
사업형태 (type1)		-0.0047 (0.0094)
조직형태 (type2)		0.0310 (0.0283)
No. obs.	1,845	1,845
R^2	0.000	0.001

(주) 괄호속의 숫자는 추정 오차이며, *, ** 는 각각 통계적 유의수준 5%, 1% 내에서 추정계수가 유의미함.

Table 5. 역시 Table 4.와 동일하게 모형 (1)은 독립변수로 정보보호 투자 여부만을 사용한 경우이며, 모형 (2)는 기타 기업 특성 변수를 통제변수로 추가하여 추정한 결과이다. Table 5.의 결과에 따르면 이중차분법을 이용한 추정량의 경우 더 이상 정보보호 투자가 정보보안 침해사고 건수에 유의한 영향을 미치지 못하는 것으로 나타난다. 이러한 결과는 기타 통제변수를 포함한 모형 (2)에서도 유사하게 나타나고 있으므로 비교적 강건한 결과로 해석할 수 있다. 이 결과를 Table 4.와 비교하면, 내생성을 적절하게 다루어 추정한 회귀분석의 결과 그렇지 않은 경우에 정보보호 투자가 오히려 유의미하게 정보보안 침해사고 건수를 증가시키는 것으로 분석되었던 것에 비해 정보보호 투자가 정보보안 침해사고 건수에 유의미한 영향을 미치지 않는 것으로 분석되고 있는 것으로 변화하는 것을 알 수 있다. 따라서 자연스럽게 생각할 수 있는 다음 문제는 과연 정보보호 투자가 정보보안 침해사고에 영향을 미친다는 통상적인 인과관계가 아니라, 이와 반대의 방향으로 정보보안 침해사고가 정보보호 투자에 영향을 미치는지에 대한 것이며, 이에 따라 역의 인과관계에 대한 실증분석의 필요성이 대두된다. 이러한 분석을 위한 회귀식은 식 (8)에서 피설명변수와 설명변수를 서로 교체한 것으로 다음 식 (10)의 형태가 된다.

$$\triangle X_i = \tau_0 + \tau_1 D_Y + \gamma Z_i + \epsilon_i \quad (10)$$

여기서 X_i 는 기업의 정보보호 투자를 나타내는 변수이고, D_Y 는 정보보안 침해사고 여부를 나타내는 더미변수이며, 추정 결과는 다음과 같다.

Table 6. Estimation Results of Difference-in-Differences Method (Breaches ⇒ Investment)

변수	종속변수: 2010년 정보보호 투자의 차분 (△itsinv)	
	모형 (1)	모형 (2)
상수항	0.0613** (0.1197)	-0.2119** (0.0718)
정보보안 침해사고 여부 (dam_bin)	0.0765** (0.0284)	0.0685* (0.0285)
업종 (num2)		0.0075 (0.0046)
규모 (num3)		0.0597** (0.0232)
사업형태 (type1)		0.0096 (0.0089)
조직형태 (type2)		0.0339 (0.0265)
No. obs.	1,845	1,845
R^2	0.004	0.012

(주) 괄호속의 숫자는 추정 오차이며, *, ** 는 각각 통계적 유의수준 5%, 1% 내에서 추정계수가 유의미함.

Table 6.에서 특정적으로 나타나는 것은 모형 (1) 및 모형 (2)에서 공통적으로 정보보안 침해사고를 경험한 기업이 유의미하게 정보보호 투자를 증가시키는 것으로 분석된다는 점이다. 이에 대한 추정계수를 해석하면, 정보보안 침해사고를 경험한 기업이 그렇지 않은 기업에 비해 평균적으로 0.07%p 정도 정보화 지출 대비 정보보호 지출을 더 수행한다는 의미이고, 이를 다시 환산하면 정보보안 침해사고를 경험한 기업의 경우 그렇지 않은 기업에 비해 정보화 지출 대비 정보보호 지출이 4.4% 정도 더 높다는 의미이다. 다시 말해 내생성을 통제한 이후에 유의미한 분석 결과를 기준으로 판단하면, 정보보호 투자가 정보보안 침해사고를 줄이는 효과를 가지는 것보다 침해사고를 경험한 기업이 사후적으로 정보보호 투자 비율을 증가시키는 것으로 보는 것이 적절한 해석인 것으로 판단할 수 있다. 이러한 결과는 모형 (1)과 모형 (2)에서도 일관적으로 나타나고 있으며, 모형 (2)의 추정 결과에서 규모가 큰 기업에서 정보보안 침해사고가 더 많이 증가하는 것으로 추정되었다는 점에서 직관에 부합하는 것으로 볼 수 있다. 이상의 실증분석의 결과를 요약하면, 정보보호관련 기업 활동의 특징 및 내생성을 적절히 고려하여 이중차분법으로 분석할 경우에 통상적인 인과관계로 볼 수 있는 정보보호 투자가 침해사고를 줄인다는 효과에 대해서는 실증적인 근거를 발견하기 어려웠던 반면, 그 역의 인과관계, 즉 침해사고를 경험한 기업이 정보보호 투자에 적극적이라는 가설이 어느 정도 데이터에 의해 입증되는 것으로 해석할 수 있다.

마지막으로, 역의 인과관계, 즉 정보보안 침해사고에 대한 경험이 사후적으로 정보보호 투자비율을 증가시키는 성향이 어떠한 업종에서 현저하게 나타나는지를 살펴보도록 한다. 통제변수를 제외하고 총 8개 서비스업의 업종별로 식 (10)을 추정한 결과는 Table 7.에서 제시되어 있다.

Table 7.에서 제시되는 결과를 통해 판단하면, 전체 서비스업 중에서 숙박/음식업 및 금융/보험업에서 역의 인과관계가 매우 유의미하고 현저하게 나타나고 있는 것을 발견할 수 있다. 특히 금융/보험업의 경우 정보보호에 매우 민감하기 때문에 다른 업종에 비해 과감한 사전적인 투자를 수행하는 것으로 인식되고 있음에도 불구하고, 본 연구의 분석에 따르면 침해사고에 따라 가장 사후적으로 정보보호 투자를 수행하고

있는 업종으로 나타나고 있어 기존의 통상적인 인식과는 매우 다른 결과를 보여주고 있다.

Table 7. Analysis of Reverse Causality (Classified by Industry)

변수	종속변수: 2010년 정보보호 투자의 차분 (△itsinv)			
	도매업	소매업	숙박/음식업	운수업
상수항	0.0271 (0.141)	0.0415* (0.0184)	0.263 (0.0145)	0.0163 (0.0123)
정보보안 침해사고 여부 (dam_bin)	0.0583 (0.0338)	-0.0374 (0.0499)	0.1609** (0.0493)	0.0252 (0.0320)
No. obs.	236	272	173	256
R^2	0.013	0.002	0.059	0.002

변수	종속변수: 2010년 정보보호 투자의 차분 (△itsinv)			
	통신업	금융/보험업	부동산 임대업	기타 서비스업
상수항	0.2598** (0.0846)	0.0811 (0.0512)	0.0505 (0.0303)	0.0678* (0.0248)
정보보안 침해사고 여부 (dam_bin)	-0.0473 (0.1392)	0.3617** (0.1220)	-0.0243 (0.081)	-0.124 (0.0552)
No. obs.	184	239	192	293
R^2	0.001	0.036	0.001	0.001

(주) 괄호속의 숫자는 추정 오차이며, *, ** 는 각각 통계적 유의수준 5%, 1% 내에서 추정계수가 유의미함.

V. 요약 및 결론

일반적으로 기업의 정보보호 투자는 다른 투자와 구별되는 두 가지 특징을 가진다. 첫째, 정보보호관련 기업 정보의 민감성 때문에 정보보호 투자 및 정보보안 침해 사고에 대한 데이터를 입수하기가 매우 어려우며, 둘째, 수익 창출의 수단이 되는 일반적인 투자와 달리 정보보호 투자는 기본적으로 위험 감소의 효과를 가진다. 이러한 특징에 따라 현실적으로 정보보호 투자의 실증적, 계량적 연구가 매우 드물게 이루어져 왔으며, 정보보호 투자를 선제적으로 늘리는 것이 어려울 것이라는 예측을 할 수 있다.

본 연구에서는 첫 번째 문제를 우리나라에서 지속적으로 이루어지고 있는 정보보호 관련 기업조사, 즉 한국인터넷진흥원의 "기업의 정보보호 실태조사"의 원자료를 이용하여 해결하고자 하였고, 두 번째 문제는 원자료를 패널데이터로 재구성하여 인과관계 분석에 적절한 이중차분법을 이용하여 분석하고자 하였다.

실증 분석의 결과는 다음과 같다. 첫째, 실증연구자들이 행하기 쉬운 통상적인 실증분석을 사용하여 정보보호 투자의 효과를 분석하면, 정보보호 투자를 많이 한 기업이 오히려 정보보안 침해건수가 유의미하게 더 높은 것으로 나타나 상식에 위배되는 결론이 도출되는 것을 알 수 있었다.

둘째, 이러한 결과가 나타나는 이유인 내생성을 보정하기 위해 패널 데이터를 구성하고 분석의 대상이 되는 표본을 제약하였으며, 이중차분법을 이용하여 분석한 결과는 통상적인 분석결과와 상당히 다른 것으로 나타났다. 즉, 통상적인 인과관계인 정보보호 투자가 정보보안 침해사고에 미치는 영향은 더 이상 유의미하지 않은 것으로 분석되었고, 반대로 역의 인과관계, 즉 침해사고를 경험한 기업이 정보보호 투자를 증가시킨다는 가설은 유의미하게 데이터에 의해 입증되는 것으로 나타났다.

셋째, 업종별로 역의 인과관계를 분석한 결과, 정보보호에 매우 민감하기 때문에 다른 업종에 비해 과감한 사전적인 투자를 수행하는 것으로 인식되고 있는 금융/보험업의 경우, 오히려 침해사고의 발생에 따라 사후적으로 정보보호 투자를 수행하고 있는 대표적인 업종으로 나타났다.

References

[1] Parker, D. B. "The Strategic Values of Information Security in Business," Computers & Security, Vol. 16, No. 7, pp. 572-582, 1997.

[2] H. K. Kong and T. S. Kim, "Research Trends in the Effect of Information Security Investment," Review of KIISC, Vol. 17 No. 4, pp. 26-33, 2007.

[3] Kotulic, A. G. and J. G. Clark "Why there aren't more information security research studies," Information & Management, Vol. 41, Issue 5, pp. 597-607, 2004.

[4] Gordon, L. A. and Loeb, M. P., "The Economics of Information Security Investment," ACM Transactions on Information and System Security, Vol. 5, No. 4, pp. 438- 457, 2002.

[5] Whitman, Michael E., "Enemy at the

gate: Threats to information security," Communications of the ACM, Vol. 46, No. 8, pp. 91-95, 2003.
〔6〕 Boss, Scott, "Control, Risk, and Information Security Precautions," PhD Dissertation, Katz Graduate School of Business, University of Pittsburgh, 2007.
〔7〕 K. W. Kim, "A Study on the Effect of Government R&D Subsidy on Firm-level Performance," Korea Development Institute, 2008-07, 2008.
〔8〕 S. W. Ko and N. H. Kwon, "The Effect of Government Subsidy on Private IT R&D Investment," Korea Information Society Development Institute, 2005.
〔9〕 DellaVigna, Stefano "Psychology and Economics: Evidence from the Field," Journal of Economic Literature, Vol. 47, No. 2, pp. 315-372, 2009.
〔10〕 Madrian, Brigitte C. and Dennis F. Shea. "The Power of Suggestion: Inertia in 401(k) Participation and Savings Behavior," Quarterly Journal of Economics, Vol. 116, No. 4, pp. 1149-1187, 2001.
〔11〕 Korea Internet and Security Agency, "2010 Survey on Information Security (Business)," Korea Internet and Security Agency, 2011.

〈저자소개〉

신 일 순 (Ilsoon Shin) 정회원
1983년 2월: 서울대학교 경제학과 졸업
1995년 5월: University of Rochester 경제학박사
2003년 3월~현재: 인하대학교 경제학부 교수
〈관심분야〉 인터넷경제, 기술경제, 정보보호

장 원 창 (Wonchang Jang) 정회원
1983년 2월: 서울대학교 경제학과 졸업
1998년 5월: Purdue University 경제학박사
2005년 3월~현재: 인하대학교 경제학부 부교수
〈관심분야〉 금융경제, 계량경제

박 희 영 (Heeyoung Park) 정회원
2012년 2월: 인하대학교 경제학과 졸업
2012년 3월~현재: 인하대학교 경제학부 대학원 석사과정
〈관심분야〉 인터넷경제, 산업조직