「정보시스템연구」 제27권 제1호
한국정보시스템학회
2018년 3월, pp. 193~224
http://dx.doi.org/10.5859/KAIS.2018.27.1.193

개인정보 유출의 정보전이 효과

박상수* · 이현철**

〈목 차〉

Ⅰ. 서 론

정보통신기술의 급격한 발전과 더불어 인터넷 및 무선통신망의 전 세계적 구축으로 말미암아 다양한 분야의 기업이 자사의 고객정보를 수집·이용하여 고객의 욕구를 사전에 예측하고 이들의 욕구를 충족시킴으로써 더 높은 부가가치를 창출하고자 노력하고 있다(주미진, 김광용, 김진수, 2016). 이를 위해 정보통신 기업뿐만 아니라 각종 유통 및 소매업체, 제조업체 및 금융기관 등 수 많은 영역의 기업이 개인의 정보를 온·오프라인을 통해 취득하고 이를 분석하며, 그들의 마케팅에 활용하고 있는 실정이다.

개인정보란 '개인을 구별할 수 있는 정보'로, 예전에는 주민등록번호처럼 개인을 명확히 구별할 수 있는 정보에 한정되어 그 범위가 좁았으나, 오늘날엔 다양한 수단을 통해 수집·생성된 개인의 자료로 그 범위가 넓어졌다(양재모, 2010; 주미진, 김광용, 김진수, 2016). 예를 들어, 인터넷 기사에 대한 댓글, 휴대폰의 위치인식 소프트에 의해 수집된 개인의 이동반경 및 경로별 빈도, 휴대폰 번호, 계좌번호, SNS에 작성한 글, 각종 상품의 구매내역 및 네트워크에 접속한 IP주소 등 다양한 것들이 개인정보로 간주되고 있다.

비록 기업에 의해 수집·보관되는 개인정보라 하더라도, 이는 해당 기업의 자산이기 이전

* 조선대학교 경영학부, dori@nanoit.kr(주저자)
** 조선대학교 경영학부, chul72@chosun.ac.kr(교신저자)

에 정보제동자 개인의 소중한 재산으로 볼 수 있다. 법적으로 이에 대한 권리는 적극적 의미 및 소극적 의미의 정보통제권으로 분류된다(한귀현, 2005; 김정연, 2013). 소극적 의미의 정보통제권은 본인의 정보가 자신의 의사와는 달리 다른 사람에 의해 수집되지 않도록 하는 권리를 말한다. 반면 적극적 의미의 정보통제권은 자신의 정보에 대한 열람청구권, 잘못 기록된 자신의 정보에 대한 정정 및 보완 청구권, 삭제·사용중지 및 봉쇄청구권, 타인의 이용 및 제공에 대한 동의권 등을 포함하고 있다. 정보통제권에 대한 적극적 의미는 소극적 의미에 비해 그 권리 인정의 범위가 대폭 확대된 경우라 하겠다. 그러나 인터넷이 일반인에게 보급되기 시작한 1990년대 이후부터, 개인의 정보가 침해되고 있는 사례가 빈번히 발생하고 있다. 개인정보 침해란 “해당 정보주체와 관계된 다양한 정보가 잘못 사용(유출, 변경, 도용 및 훼손 등)됨으로써 개인의 자기정보통제권이 침해되는 것”을 말한다. 한국인터넷진흥원 개인정보침해신고센터 접수자료에 따르면 2010년 54,832건, 2011년 122,215건, 2012년 166,801건, 2013년 177,736건, 2014년 158,900건의 개인정보 유출 사고가 발생했던 것으로 알려지고 있다. 이러한 사례의 대표적인 것으로 기업의 개인정보 유출 사건을 들 수 있다.

한국 내 개인정보 유출 사고를 살펴보면, 2008년 1월 중국 해커에 의해 발생된 것으로 추정되는 옥션 약 1,800만 건을 시작으로, 2011년 3월 신세계몰에서 390만 건의 개인정보가 유출되었다. 이 외에도, 2011년 4월 현대캐피탈에서 175만 건의, 2011년 7월 경에는 SK커뮤니케이션에서 350만 건의 개인정보가 각각 유출되었다. 그 어느 기업보다 보안이 철저해야할 금융권에서도 개인정보 유출 사고가 발생하였으며, 이의 대표적인 예로 2014년 KB국민카드 5,300만 건, NH농협카드 2,500만 건 및 롯데카드 2,600만 건 등의 사고를 들 수 있다. 이들 규모를 총 합산하면 약 1억 400만 건의 개인정보가 유출된 셈이다. 단지 이는 보도로 들어난 일부에 불과할 뿐이어서, 실질적 사고의 규모는 우리의 상상을 초월할 것으로 생각된다. 한편, 한국과 인접한 중국의 경우 2011년에 교통은행에서 발생한 7천 만 건을 비롯하여 2014년 중국이동 1만 5천 건 및 차이나 유니콤에서 발생한 1만 5천 건의 개인정보 유출 사고가 있었다(주미진, 김광용, 김진수, 2016). 유출된 개인정보에는 주민등록번호, 이름, 휴대폰 전화번호, 주소, 직장명 및 신용카드의 사용 내역 등 다양한 정보가 포함되어 있는 것으로 보도되고 있다. 유출된 개인정보는 단순한 정보유출에 그치는 것이 아니라 개인명의 도용 및 개인 아이디 해킹 등의 2차 피해를 불러올 수 있다. 실제 유출된 개인정보로 인해 개인명의 및 아이디가 도용되는 사례가 각종 언론매체 상에 보도되고 있다. 이는 개인정보 유출 사고에서 그치는 것이 아니라 정보사회의 발전에 심각한 장애를 불러올 수 있으며, 자칫 인터넷 문화의 붕괴를 가져올 수 있다는 점에서 크나큰 문제라 하겠다. 한국의 경우 2011년부터 개인정보보호법이 제정·시행되고 있어 그나마 개인정보 유출에 따른 피해 보상이 이루어지고 있으나, 많은 국가의 경우 개인정보 유출에 대한 법률의 미비로 인해 피해 보상이 이루어지지 못하고 있는 실정이다.

본 연구는 기업의 개인정보 유출이 해당 기

업 및 정보보안 기업의 주가에 어떤 영향을 미치는지를 살펴보고자 한다. 기존 연구결과는 개인정보 유출 기업은 사건일 주식의 가격이 하락하는 것을 보여준다(주미진, 김광용, 김진수, 2016). 그러나 한국의 상장기업을 대상으로개인정보 유출 시 정보보안 기업의 주가가 어떻게 변하는 가에 대한 사건연구는 거의 보고되지 않고 있는 실정이다. 이는 기업의 개인정보 유출 사고로 인한 정보보안 기업으로의 정보전이 효과를 살펴볼 수 있다는 점에서 매우 흥미로운 연구라 하겠다. 또한 개인정보유출의 사회적 심각성을 고려할 때, 본 연구의 결과는 관련 기업 및 개인에게 매우 큰 의의를 가질 것으로 생각된다. 본 연구는 다음과 같이 구성되어 있다. 제1장의 서론에 이어, 제2장은 개인정보유출에 대한 선행연구들을 살펴본다. 제3장은 연구모형을 제시하고, 제4장은 정보전이 효과를 실증분석을 한다. 마지막으로 제5장에서는 연구결과를 요약하고 연구의 시사점을 제시한다.

Ⅱ. 이론적 배경

2.1 개인정보유출의 경제적 · 사회적 손실

김여라, 이해춘, 유진호(2007)는 개인정보에 대한 가치를 추정하기 위해 가상가치접근법(contingent valuation methods)을 이용하여 개인정보 유출피해라는 사회적 손실을 회피하기 위해 응답자가 지급할 의향이 있다고 답한 금액을 평균하여 평균적 지불의사금액(willingness to pay)을 산출하였다. 분석결과 개인정보 유출에 대한 피해를 예방하기 위한 지불의사는 가구소득이 많을수록, 금융정보에 대한 피해경험이 있을수록, 월 통신요금 지불이 많을수록 높은 것으로 나타났다. 또한 개인이 인식하고 있는 정보유출에 대한 심각성은 금융정보의 유출에 대한 심각성이 가장 높으며, 개인고유정보, 통신정보, 영상정보, 바이오정보, 조직정보, 위치정보 순으로 나타났다.

채승완(2008)은 개인정보의 경제적 가치를 분석하고, 이를 이용하여 개인정보보호의 경제적 필요성을 분석하고자 하였다. 분석결과 개인정보를 이용하는 시장에서의 수요 및 공급은 개인정보 보호수준에 영향을 받으며, 개인정보 보호수준의 강화는 개인정보 시장을 활성화한다고 주장한다. 그러나 개인정보보호체계의 정비로 인해 개인정보 보호수준이 향상된다고 하여도 개인정보 보호 사각지대가 존재하게 되면 개인정보의 이용에 더 많은 비용이 수반된다고 하였다. 그리고 개인정보 유출사고가 발생 하였을 경우 경제적 피해규모가 더 커짐을 주장한다.

이해춘, 안경애(2008)는 기업이 보유하고 있는 개인정보가 유출되어 발생시키는 경제적 손실을 계산하기 위해 우선 정보유출로 피해를 본 개인이 수용 가능한 손해 배상액을 가상가치측정방법을 이용하여 추정하였다. 그리고 이 추정된 값에 언론 매체에 발표되거나 정보보호진흥원에 접수된 개인정보 유출피해에 대한 피해 건수를 곱하여 경제적 손실의 규모를 측정하였다. 우리나라에 발생한 개인정보 유출사건은 50% 이상이 개인 고유정보 유출로 인한 피해이며, 다음이 통신정보, 위치정보, 금융정보의 유출로 피해가 발생한 것으로 나타났다. 손해배상금으로 요구 가능한 금액은 피해건당 756만원으로 추정되었으며, 2006년을 기준으

로 개인정보 유출의 잠재적 손실액 규모는 대략 32조원에 이른다고 보았다. 그들은 기업의 마케팅생산성 향상을 위해 개인정보의 적극적인 활용은 필수적이나, 개인정보 유출로 인한 손실은 오히려 기업의 마케팅 생산성을 저하시킬 수 있을 것으로 보았다. 따라서 그들은 이러한 손실을 최소화하기 위해 개인정보 보호에 투자를 증대시켜야 함을 주장한다.

한창희, 채승완, 유병준, 안대환, 박채희(2011)는 개인정보유출 사고가 발생할 경우 민간기업의 실질적 손실비용과 이를 복구하기 위한 비용을 측정함과 더불어 고객의 손실과 사회적 파급효과 등의 경제적 피해규모를 정량적으로 산출할 수 있는 모형을 우리나라 상황에 맞게 수정하였다. 이들은 연구모형을 이용하여 유출사고의 발생, 사고의 영향, 사고에의 대응 및 복구, 법적보상 및 사회적 파급효과 등을 분석하였다. 이를 위해 직접 산출이 가능한 직접비용을 중심으로 개인정보유출 피해액을 산출하였고, 명시적 직접비용만을 다룬 기존의 연구와 달리 산출이 어려운 간접비용과 잠재적 비용을 고려하였다. 추가적으로 개인정보유출사고의 영향이 클 것으로 예상되는 관련 사업에의 파급효과와 기업의 법적비용, 벌금 및 보상받지 못한 고객의 손실까지 산출의 범위를 확대하여 보다 정확한 피해액을 도출하고자 하였다. 명시적 직접비용은 유출사고에만 명확하게 연계될 수 있는 비중 중 유출사고 기간 동안 발생한 분명한 비용을 말하며, 여기에 해당되는 것에는 사고대응 인건비와 IR 대응비용 및 고객감소로 인한 수익 감소분이 있다. 또한 개인정보 유출사고와는 명확하게 연결되지만 유출사고기간을 넘어 발생 할 수 있는 암묵적 직접비용으로 법적비용과 벌금 보상받지 못한 개인의 정보가치 등을 계산하였다. 그리고 이들은 단일 유출 사고뿐만 아니라 다른 사고에 의해서도 영향을 받을 수 있는 간접비용 역시 유출사고 기간 동안 명백하게 발생하는 명시적 간접비용과 그렇지 않은 잠재적 간접비용으로 분류하였다. 명시적 간접비용은 산업파급효과, 고객신뢰도측정 비용, 시스템보완 및 교체비용 등이 말하며, 잠재적 간접비용은 기업이미지손실 등이 포함된다. 그런데 모형에서는 직접비용은 모두 고려하되 명시적 간접비용은 산업파급효과만 고려하였고 기업의 이미지손실은 측정이 어렵고 명시적 직접비용에서 수익손실에 일부분이 포함되므로 잠재적 간접비용을 산출대상에서 제외하였다. 이를 바탕으로 이들은 다음의 결론을 도출하였다. 개인정보 유출에 따른 기업의 피해액은 대응 인건비, IR(investor relations) 대응비용, 수익손실, 법적보상금, 법적으로 실제 보상한 개인의 정보가치 등의 피해를 입으며 동시에 개인은 유출된 개인 정보가 갖는 가치만큼의 손해를 보게 된다. 기업이 개인에게 보상한 법적보상금은 유출된 개인정보가 가지는 가치의 일부분이기에 산정 시 중복을 피하고자 기업의 손실로 측정하며, 개인의 순손실은 유출된 개인 정보의 가치 중 기업이 보상한 법적보상금을 제외한 그 나머지를 산정한다. 이렇게 산정한 기업 손실과 개인손실은 관련 산업에 파급효과와 더해져 개인정보유출에 따른 전체 피해액으로 계산할 것을 제안하였다.

2.2 개인정보유출과 주식가격

Ettredge and Richardson(2002)은 자본 시장

참여자들이 인터넷 기업들 중 전자 상거래 활동이 인터넷 기업 특유의 정보보안 위험을 점차적으로 증가시키는 것으로 보는지 여부를 조사하였다. 이들은 전자 상거래에 대한 위험을 보기위해 위험의 정도를 측정하는 변수를 전자소매상 인터넷 기업과 전자소매상이 아닌 기업으로 구분하였다. 또, 증권 거래위원회 (SEC)에 제출 한 기업의 비즈니스 리스크에 대한 설명에서 많은 통계를 도출하였는데, 특히 IT의존성으로 인해 발생하는 자체 평가 위험, 즉 인터넷 기술 변화로 인한 위험, 부적절한 인프라로 인한 위험, 온라인 보안 침해로 인한 위험 등 여러 가지 지표에 주목했다. 이들은 이전 연구들이 주주가 IT 성과에 관계된 발표가 있을 때 주가 변동으로 인한 이득을 얻는지 여부를 조사하기 위해 비정상적인 주가 수익을 계산한 것과 달리 전자상거래로 인하여 발생한 위험 요소 사건에 대한 투자자들의 반응을 조사하였다. 당시 언론에서는 전사소매상 인터넷 기업이 다른 인터넷기업에 비해 위험이 증가할 것이라는 견해가 있었는데 실제로 증권 거래위원회(SEC)에 제출 한 기업의 비즈니스 리스크에 대한 설명에서 통계적으로 유의미한 결과를 확인 하였다. 실증분석으로 2000년 2월에 유명한 인터넷 회사들에 시작된 분산서비스거부공격(DDoS)에 대한 투자자의 반응을 조사 했다. 이러한 전자상거래 위험 요소 사건은 공격이 갑작스럽고 예기치 않게 발생했기 때문에 투자자의 인터넷 위험 반응에 대한 사건연구에 적합하다고 했으며 공격으로 인해 전자 상거래 관련 위험이 가장 높고 인터넷 회사의 큰 취약점이 드러났다. 특히 인터넷 기술 변화로 인한 위험, 부적절한 인프라로 인한 위험 및 온라인 보안 침해로 인한 위험 등 정보통신기술에 의존하여 발생하는 자체 평가 위험이 있으며, 인터넷 기업의 주가 하락은 이러한 위험 요소들과 관련이 있다고 하였다.

Acquisti et al.(2006)은 경제학 연구가 정보보안 침해 및 취약성에 대한 발표가 주식 시장에 미치는 영향을 조사하기 시작했지만 개인정보 침해 사건에 대한 실증연구는 거의 없기 때문에 기업의 개인 정보 보호가 미치는 영향에 대한 포괄적 인 분석을 제시하였다. 그는 이를 위해 보안 메커니즘(해킹, 도난 또는 분실 된 장비, 불량 데이터 처리 프로세스 등)의 실패로 인하여 개인 정보 유출 사례에 대한 광범위한 데이터를 수집하였다. 분석 결과 개인정보 침해 사건에 대한 발표 일에 기업의 시장 가치가 하락 하는 통계적으로 유의한 영향이 있음을 보여주었다. 구체적으로 실증분석을 위한 세 가지 가설을 세웠는데 첫째, 개인 정보 침해가 발표 될 때마다 기업은 시장 가치의 손실을 입을 것이다. 둘째 지역 또는 산업 분야가 아닌 국가에서 개인 정보 침해가 보고 될 때마다 -CAR(누적 비정상 수익률)의 크기가 커질 것이다. 마지막으로 사적 침해의 영향을 받는 개인의 수에 따라 음수의 CAR의 크기가 커질 것으로 보았다. 분석결과 CAR은 위반 발표 다음날에 규모가 커지며, 수명이 짧지만 통계적으로 유의미하며 음으로 나왔다. 특히 대기업이 시간이 지남에 따라 구축된 신뢰 평판이 개인 정보 보호 관행에 대한 부정적 보고서의 영향을 더 크게 받는다고 하였다.

Ishiguro et al.(2006)은 정보유출사건에 대한 뉴스 보도의 경제적 파급효과가 일본 주식시장의 기업 가치에 미치는 영향을 조사 하였다. 분

석결과 정보유출사건에 대한 뉴스 보도에 대한 반응이 미국 시장에 비해 일본 시장의 반응 속도가 상대적으로 느린 것으로 나왔다. 일본 시장은 뉴스 보도가 있은 지 약 10일 만에 통계적으로 유의미한 반응을 보인 점과 주가순자산비율(price book value ratio, 이하 PBR)이라는 새로운 요인으로 설명할 수 있다. 특히 PBR은 사고요인이나 기업규모 보다 기업의 시장 가치에 더 많은 영향을 미친다. 정보보안에 대한 기업의 투자는 특히 IT 중심 기업의 주식 시장에서 무형 자산으로 높게 평가된다. PBR은 시장에서 순자산(유형자산)과 비교하여 무형 자산을 이 상대적으로 어떻게 평가되는지를 나타내는 지표이다. 무형 자산이 높게 평가되는 기업은 낮게 평가된 기업보다 보안 사고가 기업가치에 더 심각한 영향을 받는다고 하였다.

유진호, 지상호, 임종인(2009)은 개인 정보 유출에 의한 기업의 손실 추정에 관한 연구를 하였다. 이 연구로 개인 정보 유출이 주가에 부정적인 영향을 미칠 수밖에 없는 근거를 제시하였다. 이들은 개인정보 유출로 인한 기업의 직접적이고 정량적인 손실비용의 산출방안을 제시기 위해 개인정보 침해사고에 의해 발생할 수 있는 손실비용을 범주에 따라 분류하고 비용을 구성하는 요소들을 구체적으로 분석하였다. 이를 위해 손실비용을 직접비용(direct costs)과 간접비용(indirect costs), 명시적 비용(explicit costs)과 잠재적 비용(implicit costs)으로 구분하였다. 그리고 상대적으로 연구가 적은 직접비용에 초점을 맞추어 개인정보침해 사고에 의한 직접적인 손실액을 산출하였다. 손실액을 산출하기 위해 개인정보 침해사고 후 발생 피해를 최소화하기 위해 신속히 대응하고 복구하는데 드는 침해사고 대응비용(response cost)과 정상적인상태에서 개인정보 침해사고 발생 후 해당업무의 생산성이 저하되는데 드는 생산성 손실비용(cost of lost productivity) 그리고 침해사고를 당한 피해자들에게 지급해야 하는 손해배상금, 법위반에 따른 과태료를 포함하는 잠재적인 법적 책임비용(legal cost)을 고려하였다. 분석결과 침해사고 대응비용은 2006년도 이후에 800만 건 이상의 대용량 고객자료가 유출되어 개인정보 침해사고 건 1당 피해자 수가 크게 증가하여 대응비용이 증가한 것과 특히 잠재적 법적 책임비용은 모든 피해자에게 손해배상을 한다는 가정 하에 산출되었기 때문에 개인정보 침해사고에 의해 기업이 입게 되는 경제적 손실비용은 잠재적인 손해배상금이 총 손실의 약99% 정도로 대부분을 차지하였고 그 절대 금액도 매우 큰 것으로 나타났다. 따라서 잠재적인 위험을 고려하면 기업은 대용량고객 자료의 유출에 의해 파산에 이를 수 있다는 경각심을 가질 필요가 있다고 주장하였다.

개인 정보 유출이 주가에 미치는 영향에 관한 연구에서 방법론적으로는 개인 정보 유출 이외의 다른 이벤트가 주가에 미치는 영향을 제거하는 것이 중요한데 Patel(2010)의 연구가 그 시사점을 제공해 주고 있다. 예를 들어 M&A, 유·무상증자, 주식 병합 및 분할, 특별이익 등 이벤트가 정보유출 공시 한 달 이내로 발생한 경우 그 주식은 제외함으로써 정보 유출 이외에 다른 요인이 주가에 미치는 효과를 사전에 제거하여야 한다. Patel(2010)의 연구는 3일, 8일, 30일 기간별 CAR을 사용하여 분석하였고, 또한 통제 기업(개인유출이 없는 기업들 중에서 무작위로 샘플링) CAR을 측정하여 비

교하고 있다. 그리고 개별 기업 수준에서 CAR을 측정하여 개별 기업의 차이점을 분석하고 있다. Patel(2010)은 3일 측정치는 유의한 영향력이 없고 8일은 음의 영향을 주고 있다고 밝히고 있다. 그러나 8일의 경우 비 유출기업(통제기업)의 주가에도 부정적인 영향을 주고 있어서 정보 유출이 산업 전반의 모든 기업의 주가에 부정적인 영향을 주고 있음을 밝혀냈다. 그러나 30일의 경우에 주가에 대한 영향력이 다시 유의하지 않게 나타나고 있음을 주장하였다. 이 연구에서는 개인정보 유출이 장단기(3일, 30일) 주가에 미치는 부정적인 영향은 유의하지 않은 것으로 나타났기 때문에 부정적인 영향을 미치는 다른 변수를 찾는 것이 필요하고 향 후 연구에서는 그 변수를 찾기 위해서 다양한 상황적 변수와 개별 기업 변수를 고려하여 통계적으로 유의한 변수를 찾아내는 것이 필요할 것으로 보인다.

김정연(2013)은 개인정보유출을 겪은 기업의 주가변화를 측정하여 개인정보보호에 관한 제도적 보완이 실제 시장 참여자의 개인정보보안과 관련한 인식이 개선되었는지를 살펴보았다. 개인정보가 유출된 기업의 초과수익률을 사건연구방법론으로 기존 연구결과와 비교하여 실제 개인정보유출사고로 인한 기업가치의 변화가 축소 혹은 확대 되었는지 보았다. 이를 위해 두 가지 가설을 세웠는데 첫 번째 가설은 개인정보유출사건은 최근에도 기업가치에 음의 영향을 미친다는 것과 두 번째 가설은 개인정보유출로 인한 기업가치의 감소는 최근 선행연구결과대비 축소되었다는 것이다. 분석결과 반복되는 개인 정보유출사례에도 시장의 반응은 부정적이었는데 이는 기업가치에 부정적 영향을 미치는 것을 말하며 해당사건에 여전히 제도적 개선이 이루어지고 있음에도 불구하고 자본시장에서의 개인정보 유출로 인한 피해인식은 크게 변화되지 않았음을 확인해 주었다. 이에 여전히 주기적으로 발생하는 정보보안사건의 적극적 예방을 위해서는 그 피해액의 산정에 있어 개인의 추가 피해가능성을 광범위하게 인정하는 전향적인 태도와 함께 피해 배상에 대한 의무를 명확히 인식할 수 있도록 추가적인 개선이 선행되어야 한다고 보았다.

김태환, 이해니, 유진(2014)은 개인정보유출사고가 기업가치에 부정적인 영향을 끼친다는 기존연구들을 토대로 개인정보유출사고 발생 직후에 나타나게 되는 기업주가의 변화를 7가지 패턴으로 분류하여 분석하였다. 분석대상으로 주식시장에 상장된 기업의 개인정보 유출사고만을 기준으로 주가분석을 실시하였다. 이들은 주가의 변화를 분석할 7가지 요인을 V1~V7로 분류하였는데 사고이후로 기업의 주가가 다시 상승하기 전까지 소요된 시간을 V1, V2는 V1기간 동안의 하락한 주가수치를 말한다. V3는 V1이후 주가가 다시 하락하기 전까지 상승한 기간, V4는 V3기간 동안 상승한 주가의 수치이며, V5는 사고발생 이전의 주가로 회복하는데 소요된 시간을 말한다. V6는 사고발생 당시 주가와 사고발생 후 2주일 내의 주가 중 최저치간의 등락율을 의미하며 V7은 사고발생 전 일주일 동안의 등락률과 V6간의 차이를 말한다. 분석결과 개인정보유출사고 발생 직후 주가는 평균적으로 2일 동안 1.0%하락하였다, 개인정보유출사고 발생 전의 주가로 회복하는데 드는 시간은 약 5일 정도이고 2주내에 주가를 회복하지 못하는 경우도 발생했다. 또한 주가를

회복한 이후에 다시 10% 이상 주가가 폭락한 경우도 있었는데 이는 사고의 시기나 중요도 등 내외적 요인에 의한 것으로 보았다.

홍일유, 이재훈, 강성민(2015)은 정보보안 사고에 대한 공시가 시장에서 기업의 주식가치에 미치는 영향을 분석하였다. 이 연구는 주식시장에서 개별 기업의 비정상수익률을 바탕으로 보안사고가 기업의 주가 수익률에 어떻게 영향을 미치는지를 알아보았다. 이들은 보안사고가 일어난 후 +1일에 기업의 주가에 부정적 영향을 미친다는 것을 도출하였다. 또한 정보보안 사고, 개인정보유출, 전산망 마비는 기업의 주가에 부정적 영향을 미쳐 투자자들뿐만 아니라 기업의 이해관계자들에게 손해를 입히게 된다는 점을 밝혔다. 이로 인해 기업이 정보보안에 적극적이고 체계적인 투자를 해야 한다는 점과 기업의 최고 경영자들이 정보보안에 대한 투자 의사결정을 위한 정량적인 요인으로 고려할 수 있는 객관적인 내용을 제시하였다.

주미진, 김광용, 김진수(2016)는 2006년부터 2014년까지 9년 동안 한국 및 중국에서 발생한 개인정보 유출 사건(총 104개)이 해당 기업의 주가에 미치는 영향에 대한 사건연구를 실시하였다. 이들은 유출 기업을 대상으로 한 사건일 전 170일부터 사건일 후 5일 동안의 주가자료를 이용하여 비정상 수익률과 기간별 CAR을 측정하고 이의 통계적 유의성을 검증하였다. 분석 결과 한국의 경우 개인정보 유출이 주가에 유의한 영향을 미치나, 중국의 경우 유의한 영향이 없음을 확인하였다. 이들은 한국과 중국의 상이한 연구결과에 대해 한국의 경우 개인정보보호에 관한 법률이 있어 정보유출에 따른 개인적 피해를 법률적으로 보호받을 수 있으나, 중국의 경우 이러한 개인정보보호에 대한 법률의 부재로 인해 개인정보 유출에 따른 피해를 법률적으로 구제받을 수 없기 때문에 양국 간 상이한 결과가 나타남을 주장한다.

2.3 개인정보유출과 정보보안 기업의 주가반응

일반적으로 정보보안 기업은 정보보안 관련된 사건이 일어나도 법적인 책임이 없기 때문에 주가에 큰 타격을 받지 않는 경우가 많았다. 오히려 새로운 소프트웨어 개발 때문에 기업가치 상승을 예상하고 투자자들이 더 많이 주식을 매입하는 경우도 발생할 수 있을 것이다. Cavusoglu, Mishra, Raghunathan(2004)는 정보보안 관련 사고는 주가 수익률에 부정적인 효과를 미치는 것을 밝혀냈다. 그리고 이러한 비정상적인 주가 변동은 해당 기업의 규모, 업종, 발생 년도 등에 따라서 다르게 나타난다고 주장하였다.

권영옥, 김병도(2007)는 정보보안 사고에 따른 기업의 손실과 보안 투자로 인한 수익을 기업 시장가치의 변화를 이용하여 정량적으로 측정하였다. 이들은 정보보호 또는 정보보안을 일반적으로 고의, 과실, 재해 등에 의해 정보시스템이 고장 및 파괴되는 등의 위해를 막기 위한 물리적·논리적 대응으로 보고 고의적으로 발생하는 사고만을 대상으로 하였다. 이들의 사건연구방법론을 통해 정량적으로 측정 결과 정보보안 사고는 해당 기업의 주가에 부정적인 영향을 미치지만 보안 관련된 투자는 기업 가치 상승에 별다른 영향을 주지 않는 것으로 나타났다. 또한 국내 기업은 해외 기업에 비해서 정

보보안 사고가 주가에 미치는 영향이 미비한 것으로 나타나 아직까지 기업의 보안 사고의 심각성이 인식되지 못하고 있는 점을 시사한다.

Telang and Wattal(2007)은 정보보안 사건이 보안 소프트웨어 개발 업체들의 주가에 미치는 영향을 분석하였다. 분석 결과 정보의 유출 사건은 정보보안 개발 업체들의 주가에 부정적인 영향을 미치고 있는 것으로 나타났다. 이러한 현상은 시장 경쟁이 심할수록 개발 업체의 규모가 작을수록 더 커지는 것으로 나타났다. 또한 정보 유출 사건의 유형에 따라서 손실 규모에 차이가 발생하며, 보완 프로그램 개발이 늦어질 경우 손실 규모가 더 증가함을 확인하였다.

김민정, 허남길, 유진호(2016)은 개인정보 유출 사고가 정보보호업체의 주가에 미치는 영향에 대해 실증 분석하여 보안사고가 정보보호업체에 미치는 영향을 연구하였다. 이들은 정보보호업체의 업태별 분석을 위해 기업들을 IT서비스, 소프트웨어, 장비의 세가지 업태로 구분하였다. 분석 결과 개인 정보의 유출 사건은 정보보안 업체의 주가에 긍정적인 영향을 미치는 것으로 나타났다. 또, 정보 유출 기업의 규모와 업종에는 유의한 차이가 없었지만 정보보호 업체의 업태 구분에 따른 차이는 발생하였다.

Ⅲ. 연구모형

3.1 사건연구모형

Brown and Warner(1985)는 시장조정수익률 모형, 평균조정수익률모형 및 OLS 시장모형을 이용하여 초과 수익률을 측정하는 통계적 모형을 제시하였다. 이는 Brown and Warner(1985)의 결과와 거의 일치하며, 본 연구는 사건의 공시에 따른 주식 수익률 반응의 분석을 위해 일별 주식 수익률 자료를 이용함으로 Brown and Warner(1985)가 제시한 방법을 중심으로 논하고자 한다. 이들 연구의 핵심은 셋째 단계에서 제시된 AR 추정 시 이용되는 정상성과모형 중 과연 어느 모형의 검정력(power)이 우수한가이며, 이는 시뮬레이션 방법을 통해 실시되었다. Brown and Warner(1985)는 “비정상 수익률은 ‘0’ 이다”라는 귀무가설이 진실임에도 불구하고 이를 기각하는 것을 제1종 오류라 하며, 귀무가설이 참이 아님에도 불구하고 이를 제대로 기각하지 못하는 것을 제2종 오류라 하였다. 여기서, 제2종 오류의 확률을 검정력이라 하며, 이는 비정상 수익을 정확하게 추정할 수 있는 가능성을 의미한다. Brown and Warner(1980, 1985)는 간단한 시장모형에 기반 한 것이 다른 복잡한 통계적 방법에 비해 다양한 조건 하에서 가장 검정력이 큰 것으로 분석되었다. 더불어, 월별 주식 수익률 자료를 이용하기보다 일별 주식 수익률 자료를 사용할 때 검정력이 훨씬 큰 것으로 나타났음을 확인하였다. 따라서 본 연구는 Brown and Warner(1980, 1985)와 같이 일별 자료를 이용하여 사건연구를 실시한다. 이들은 사건연구를 실시함에 있어 시장모형을 중심으로 평균비정상수익률(average abnormal return, 이하 AAR)과 누적평균비정상수익률(cumulative average abnormal return, 이하 CAAR)의 측정과 이의 통계적 유의성 검정을 위한 검정통계량 측정방법을 제시하였다. 다음은 이들이 제시한 측정방법에 대한 설명이

다. 시장모형을 이용한 AAR과 CAAR의 추정을 위해, 우선적으로 표본 개별주식의 일별 주식가격자료를 이용하여 아래 식 (1)과 같이 일별 주식수익률을 계산한다.

$$R_{i,t} = \frac{P_t - P_{t-1}}{P_{t-1}} \quad (1)$$

$R_{i,t}$: 주식 i의 t일 주식수익률

P_t : 주식 i의 t일 종가

P_{t-1} : 주식 i의 t-1일 종가

시장모형을 이용하여 기업별 비정상수익률(abnormal return, 이하 AR)을 추정하고 이것을 표본의 자료 수로 나누어 AAR을 산출한다. 그리고 이 AAR을 누적하여 CAAR을 도출한다 (Brown and Warner, 1980; 정형찬, 1997).

본 연구는 AR의 추정을 위해 사건 공시 전 170일부터 사건 공시 후 5일까지(공시일 포함) 총 176일 자료를 이용 한다. 여기서 사건기간은 사건공시일과 사건공시일 전 5일 및 후 5일(-5일에서 +5일까지 총 11일)로 설정한다. 사건 일 전 170일에서 사건일 전 21일까지 총 150일을 시장모형의 추정기간으로 한다. 추정 시 식 (2)를 이용하여 사건일 전 170일에서 사건일 전 21일까지 기업별 일별 주식 수익률과 시장포트폴리오 수익률 간의 회귀분석을 통해 절편($\hat{\alpha}_i$)과 기울기($\hat{\beta}_i$)을 추정한다. 그리고 추정된 절편과 기울기를 이용하여 기업별로 일별 AR을 도출한다.

$$AR_{i,t} = R_{i,t} - \hat{\alpha}_i - \hat{\beta}_i R_{mt} \quad (2)$$

여기서, $\hat{\alpha}_i, \hat{\beta}_i$: 표본기업(i)의 절편과 기울기

$R_{i,t}$: t일의 표본기업(i)의 주식수익률

R_{mt} : t일의 시장포트폴리오 수익률

$AR_{i,t}$: t일의 표본기업(i)의 비정상수익률

식 (2)의 $\hat{\alpha}_i$ 및 $\hat{\beta}_i$은 개별주식 및 종합주가지수의 일별수익률을 자료를 회귀분석하여 추정한다.[1] 상기 식 (2)의 과정을 통해 도출한 기업별 일별 비정상수익률의 합을 t일의 표본기업수로 나누어 AAR을 도출하며, 이는 식 (3)과 같다.

$$AAR_{i,t} = \frac{1}{N}\sum_{i=1}^{N} AR_{i,t} \quad (3)$$

여기서, t : -170에서 5의 값을 가지는 정수

N : 표본기업의 수

$AAR_{i,t}$: 평균비정상수익률

아래의 식 (4)를 통해 CAAR를 도출하며, 이는 AAR을 누적한 것이다.

$$CAAR_t = \sum_{t_1}^{t_2} AAR_{t_1,t_2} \quad (4)$$

여기서, $CAAR_t$: 누적평균비정상수익률

아래의 식(5)와 식 (6)은 AAR과 CAAR에 대한 통계적 유의성 검정을 위한 t통계량을 계산하는 방법을 보여준다. 이는 횡단면 독립성을 가정한 Brown and Warner(1985)와 동일한 방

1) 종합주가지수의 일별수익률 측정은 사건 기업이 한국유가증권시장에 상장된 경우 KOSPI지수의, 코스닥에 등록된 경우 KOSDAQ지수의 일별자료를 각각 사용한다.

법이다.

$$t_{AAR_t} = \sqrt{N_t} \cdot \sum_{i=1}^{N_t} \frac{AR}{\hat{S}(AAR)} \quad (5)$$

$$\hat{S}(AAR_{i,t}) = \sqrt{(\sum_{t=-170}^{-21} (AR_{i,t} - AR_i^*))/N_t - 1}$$

$$AR_i^* = \frac{1}{N_t} \sum_{t=-170}^{-21} AR_{i,t}$$

여기서, t_{AAR_t} : AAR에 대한 t통계량

$\hat{S}(\bullet)$: 해당 변수의 표준편차

$$t_{CAAR}(t_1,t_2) = \sum_{t=t_1}^{t_2} AR_t / \sqrt{\sum_{t=t_1}^{t_2} \widehat{S^2}(AAR_t)} \quad (6)$$

$$\widehat{S^2}(AAR_t) = \frac{1}{N_i - 1} \sum_{t=170}^{-21} (AR_t - AR^*)^2$$

$$AR^* = \frac{1}{N_t} \sum_{t=-170}^{-21} AR_t$$

여기서, $t_{CAAR}(t_1,t_2)$: t_1일 부터 t_2일까지의 누적평균비정상수익률에 대한 t통계량

3.2 횡단면 회귀분석모형

개인정보유출의 공시에 따른 기업가치 변화의 결정요인을 살펴보기 위해 횡단면 회귀분석모형을 설정한다. 본 연구는 설정된 모형을 최소자승법으로 추정하며, 추정 시 사건일 및 사건일 이후 1일에 발생하는 개별 기업의 비정상수익률 및 누적비정상수익률을 종속변수로 한다. 개별 기업의 주가에 긍정적 영향을 미치는 정보는 대개 공시 전 사전유출로 인해 사건 일 전에 비정상 수익률이 양(+)의 유의한 결과를 보인다. 반면 주가에 부정적 영향을 미치는 정보의 경우 기업이 외부로 유출되는 것을 극도로 차단함과 더불어 주식시장이 개장할 때 공시하기보다 시장이 마감할 무렵 또는 마감 이후 공시하는 경향이 있다. 이로 인해 비정상수익률이 지연반응을 보이기도 한다. 아마도 이는 부정적 정보에 대한 투자자의 과민반응에 따른 주식가격의 극심한 하락을 피하고자 하는 경영자의 심리에 기인한 것으로 생각된다.

개인정보유출은 유출 기업에게는 부정적 정보로 작용하기 때문에 본 연구는 아래의 식 (4) 및 식 (5)와 같이 횡단면 회귀분석모형을 설정한다. 식 (4)의 기업규모인 $LN(ASSET)$은 사건일 직전 연도 말 기업의 총자산에 자연로그를 취하여 계산한다. 이는 개인정보 유출에 따른 기업규모의 효과를 살펴보기 위한 것이다 (Szewczyk et al., 1996; Chan et al., 1997; Acquisti et al., 2006; Lee et al., 2012). 기업의 규모가 클수록 외부의 부정적 충격을 흡수할 수 있는 능력이 크기 때문에, 기업규모 $LN(ASSET)$은 양(+)의 부호를 가질 것으로 생각된다(Acquisti et al., 2006). 성장기회인 ME/BE는 사건일 직전 연도 말 자기자본의 시장가치를 장부가치로 나누어 측정한다. 전략적 제휴, 개방형 혁신(Open Innovation) 등과 같이 기업에 긍정적인 영향을 주는 사건의 경우, 많은 실증연구는 성장기회가 비정상수익률에 양(+)의 유의한 영향을 미침을 확인하였다 (Szewczyk et al., 1996; Chan et al., 1997; Das et al., 1998; Kwon, 2006; Lee et al., 2012). 반면 개인정보 유출과 같이 부정적 정보는 성장기회가 큰 기업에게 더욱 큰 영향을 줄 것으로 생각된다. 따라서, 성장기회 ME/BE는 음(-)의 부호를 가질 것이다. Acquisti et al.(2006)과 같이 기업유형 $FIRM\ TYPE$을 추가하였다.

기업유형 $FIRM\ TYPE$은 인터넷 기업이면 1, 아니면 0의 값을 갖는 더미변수이다. 인터넷 기반의 사업을 영위하는 기업일수록 보안이 더욱 중요한 것으로 생각된다. 따라서 이는 음(-)의 부호를 가질 것으로 기대된다.

$$AR_i = \alpha + \beta_1 LN(ASSET) + \beta_2 (ME/BE) + \beta_3 FIRM\ TYPE_i + \epsilon_i \quad (4)$$

여기서, $LN(ASSET)_i$: i기업의 직전년도 말 총자산액의 자연로그 값

$(ME/BE)_i$: i기업의 직전년도 말 자기자본의 시장가치를 장부가치로 나눈 값

$FIRM\ TYPE_i$: 사건일 i기업이 인터넷 기업이면 1, 아니면 0

$$CAR_i = \alpha + \beta_1 LN(ASSET) + \beta_2 (ME/BE) + \beta_3 FIRM\ TYPE_i + \epsilon_i \quad (5)$$

정보전이로 인한 정보보안관련 기업의 비정상수익률 및 누적비정상수익률이 어떠한 요인에 의하여 영향을 받는지를 확인하기 위하여 아래의 식 (6) 및 식 (7)의 회귀분석모형을 설정한다. 기업규모가 작을수록 외부의 긍정적 영향에 따른 주식 가격의 변화가 클 것으로 생각된다. 따라서, 기업규모 $LN(ASSET)$은 음(-)의 부호를 가질 것으로 생각된다. 많은 연구는 긍정적인 사건의 공시에 따른 비정상수익률이 기업규모와 음(-)의 관계임을 보여준다(Szewczyk et al., 1996; Chan et al., 1997; Acquisti et al., 2006; Lee et al., 2012). 성장기회 ME/BE가 클수록 주어진 기회에 보다 적극적으로 반응할 수 있을 것으로 생각할 수 있다. 그러나 본 연구에서 다루는 개인정보 유출은 정보보안 기업에게 소위 반사적 이익에 가까운 것이다. 반사적 이익은 성장기회가 큰 기업보다는 이것이 적은 기업에게 보다 큰 영향을 미칠 것으로 생각된다. 따라서, 성장기회 ME/BE는 음(-)의 부호를 가질 것이다. 더미변수 PHY(물리적 보안 기업의 더미변수), NS(네트워크 및 시스템 보안 기업의 더미변수), SOL(보안 응용 소프트웨어 기업의 더미변수), CER(암호·인증 기업의 더미변수) 및 SI(시스템 통합 기업의 더미변수)는 정보보안 기업을 그 성격에 따라 분류하기 위한 것이다. 이는 과연 어떠한 분야의 정보보안 기업에 정보전이 효과가 크게 나타나는가를 확인하기 위한 것이다.

$$AR_i = \alpha + \beta_1 \ln(ASSET)_i + \beta_2 (ME/BE)_i + \beta_3 PHY_i + \beta_4 NS_i + \beta_5 SOL_i + \beta_6 CER_i + \beta_7 SI_i + \epsilon_i \quad (6)$$

여기서, PHY_i : i기업이 물리적 보안 기업이면 1, 아니면 0

NS_i : i기업이 네트워크 및 시스템 보안 기업이면 1, 아니면 0

SOL_i : i기업이 보안 응용 소프트웨어 기업이면 1, 아니면 0

CER_i : i기업이 암호·인증 기업이면 1, 아니면 0

SI_i : i기업이 시스템 통합 기업이면 1, 아니면 0

$$CAR_i = \alpha + \beta_1 \ln(ASSET)_i + \beta_2 (ME/BE)_i + \beta_3 PHY_i + \beta_4 NS_i + \beta_5 SOL_i + \beta_6 CER_i + \beta_7 SI_i + \epsilon_i \quad (6)$$

정보보안은 기밀성(confidentiality), 무결성(integrity), 가용성(availability) 3요소로 구분할 수 있다. 그러나 이들 요소는 서로 결합하여 사용되기 때문에 정보보안 기업의 분류 기준으로 적합하지 않다. 또한 한국산업표준분류는 정보보호 관련 업종으로 컴퓨터 보안프로그램 개발업, 보안시스템 운영업 및 보안시스템 서비스업을 구분하고 있다. 이 분류 방식은 보안업종을 너무도 단순하게 다루고 있어, 이는 보안업종에 따른 차별적 주가반응을 분석하고자 하는 본 연구의 목적에 적합하지 않다. 정보보호산업 실태와 기술개발 동향(데이코산업연구소, 2013)은 정보보호산업을 산업현황에 따라 정보보안산업과 물리보안산업으로 분류하고 있다. 그리고 이 보고서는 정보보안산업을 네트워크 보안 제품, 시스템 보안 제품, 컨텐츠·정보유출방지보안 제품, 암호·인증 제품, 보안관리 제품, 보안 컨설팅 서비스, 기타 제품 및 서비스로 세분화하고 있다. 이러한 이유로 인해 본 연구는 정보보안 기업을 물리적 보안 기업, 네트워크 및 시스템 보안 기업, 보안 응용 소프트웨어 기업, 암호·인증 기업, 보안 시스템 통합 기업으로 분류하였다.[2)]

물리적 보안 기업은 절도, 파괴, 화재 등과 같은 각종 물리적 위협으로부터 정보 시스템 자산을 보호하는 것이며, 대표적인 한국의 기업으로 에스원, 미래아이앤지 등을 들 수 있다. 네트워크 및 시스템 보안 기업은 비인가자가 인터넷 또는 네트워크로 접속 가능한 자원에 접근하려 할 때 관리자가 사용하는 컴퓨터 네트워크 및 하부구조를 보호하고, 시스템에 대한 접근 제어를 통한 보안 서비스를 전문으로 제공하는 회사로, 이의 대표적인 한국의 기업에는 넥스지, 안랩, 파수닷컴 등이 있다. 보안 응용 소프트웨어 기업은 컨텐츠 보호, 안티 바이러스 및 유해사이트 차단 등 특수한 목적의 정보보호를 제공하는 것을 말한다. 이에 포함되는 대표적인 한국의 기업에는 수산아이앤티, 이스트소프트, SBI핀테크솔루션즈가 있다. 암호·인증 기업은 권한 증명을 위하여, 암호 및 생체인식 기술 등을 이용하여 권한자를 식별하는 서비스를 제공하는 것을 말한다. 미래테크놀로지, 시큐브, 삼성SDS 등이 대표적인 한국의 기업이다. 보안 시스템 통합 기업은 보안 컨설팅 및 보안 시스템 통합 구축 용역을 제공하는 회사이며, 이에는 다우기술, 케이엘넷, 현대정보기술을 대표적인 한국의 기업으로 들 수 있다.

Ⅳ. 실증분석

4.1 연구자료

본 연구는 개인정보 유출에 따른 정보전이

2) 본 연구는 정보보안 기업을 물리적 보안 기업, 네트워크 및 시스템 보안 기업, 보안 응용 소프트웨어 기업, 암호·인증 기업, 보안 시스템 통합 기업으로 분류하였으나, 이는 연구자의 경험에 기초한 것이다. 향후 보다 정확한 분류기준을 이용하여 이 부분에 대한 추가적인 연구가 진행될 필요가 있겠다.

효과를 살펴보기 위해 한국유가증권시장 및 코스닥시장에 상장된 기업을 대상으로 개인정보 유출 사건을 조사하였다. 조사기간은 2006년부터 2017년까지 총 12년이다. 개인정보 유출기업의 검색은 우선 네이버 및 구글 뉴스를 이용하였으며, 다음으로 정보보안 전문 인터넷뉴스에서 제공되는 보안뉴스의 기획기사 중 연간 중요 개인정보유출 사건 정보를 활용하였다. 그리고 행정자치부의 “개인정보보호법 위반 행정처분”에 포함된 기업을 네이버 및 구글 뉴스를 통해 추가 검색하였다. 마지막으로 한국인터넷진흥원의 개인정보유출 신고 접수현황 및 방송통신위원회 개인정보유출 관련 시정조치 고지를 받은 기업에 대하여 상기 검색엔진을 이용하여 보완하였다. 이를 통해 표본기간 동안 30개 기업에 대해 총 47건의 개인정보 유출 사고 표본을 확보하였다. 물론 이 기간 중 개인정보 유출 사건은 100건 이상이었으나, 유출 기업이 한국유가증권시장 및 코스닥시장에 상장되지 않아 표본에서 제외하였다. <표 1>은 최종적으로 선택된 연도별 개인정보 유출 사건 및 관련 기업 수를 보여준다. 개인정보 유출 사건은 2014년 23건 발생하였으며, 이는 전체의 48.9%에 해당한다. 특이한 사실 중 하나는 2007년의 경우 개인정보 유출이 3건 발생하였으며, 이는 KT에서 모두 발생한 것이다. 개인정보 보호에 무엇보다도 신중을 기해야할 이동통신사에서 이와 같은 일이 발생했다는 것은 정보통신업의 강국임을 주장하는 한국에게는 더 없이 부끄러운 일이라 하겠다. 개인정보 유출 기업 수는 총 30개 사이나, 연도별로 기업 수를 계산하다보니 <표 1>의 전체 기업 수가 40개 사로 기록되

<표 1> 연도별 개인정보 유출 사건 및 관련 기업 수

(단위 : 건, 사)

구분	사건 수	기업 수
2006년	1	1
2007년	3	1
2008년	0	0
2009년	0	0
2010년	2	2
2011년	3	3
2012년	4	3
2013년	3	3
2014년	23	19
2015년	0	0
2016년	7	7
2017년	1	1
합계	47	40

었다.

정보보안 기업은 2000년대 들어와 정보통신 기술의 발전으로 인한 새로운 업종의 기업이다. 이는 기존의 컴퓨터관련업에 속한 기업이 사업영역을 확장한 경우, 기존 사업영역에 정보통신 기술을 융합하는 과정에서 새로 진입한 경우, 정보보안이라는 세분된 영역을 사업모델로 창업한 경우 등으로 인해 생성되었다. 이로 인해 한국의 표준산업분류 상에는 정보보안이 별도의 산업영역으로 분류되어 있지 못한 실정이다. 이러한 이유로 본 연구는 우선 금융감독원 전자공시시스템의 기업개황 데이터베이스를 이용하여 한국 표준산업분류 대분류 상 “출판, 영상, 방송, 우편통신, 컴퓨터 및 정보서비스업”을 영위하고 있는 상장기업 500여개를 확보하였다. 기업의 전자공시시스템 내 개황정보에서 제공하는 사업내용을 바탕으로 정보보안 기업으로 볼 수 있는 업체를 선별하였다. 선별 시 각 기업이 공시한 사업내용 및 제품을 홈페이지를 통해 모두 검토함과 더불어 2017년 국내 정보보호산업 및 실태조사에서 정보보안 기업으로 분류된 업체와 일치성 여부를 추가적으로 확인하였다.[3] 이러한 과정을 통해 본 연구는 최종적으로 65개의 정보보안 표본기업을 확보하였다.[4] <표 2>는 본 연구에서 사용된 연도별 정보보안 기업 수이다. 정보보안 기업 수는 2006년 26개 사에서 2017년 63개 사로 매년 증가하는 추세이다. 시스템 통합 기업을 제외한 나머지 영역의 모든 부문에서 2006년에 비해 2017년 기준 약 3배의 증가를 보인다. 암호・인증 기업의 경우 2006년 0개 사에서 2017년 4개 사로 증가하였다. 이는 공인인증서 사용에 대한 법률적 규제로 인한 것으로 생각된다. 그러나 향후 생체인식 기술의 발전과 현재 의무적으로 사용되고 있는 공인인증서에 대한 규제가 완화될 경우, 암호・인증 기업의 미래가 지금과 같은 성장세를 보일 것이라 생각하기 어렵다. 기업의 수적 측면에서 판단할 때, 정보보안 기업 중 가장 미약한 성장세를 보이는 분야는 시스템 통합이다. 시스템 통합 기업은 2006년 기준 10개 사에서 2016년 13개 사로 증가하였다. 한국 내 대부분의 시스템 통합 기업은 자체적으로 개발한 플랫폼에다 외부에서 개발된 솔루션을 포함하여 수요 기업에 납품하는 형태를 취한다. 이러한 사업 방식이다 보니 기업의 주 수입원은 용역비가 주를 이룬다. 이 분야는 인건비를 어떻게 줄일 수 있는가와 얼마나 빠른 시간 내 용역을 완수할 수 있느냐가 핵심이다. 적은 인력을 이용하여 고 수익을 창출은 네트워크 및 시스템보안과 보안 응용 소프트웨어 기

3) 국내 정보보호산업 실태조사는 창조과학부와 한국정보보호산업협회가 공동으로 발행한 것으로 개별 기업의 자료, 인터뷰 등의 방식으로 정보를 취합・분석하였기에 국내 정보보안 기업 현황을 광범위하게 포함하고 있다.

4) KISVALUE는 한국표준산업분류에 따른 KISC산업분류와 GICS의 분류에 따른 KIS-IC산업분류 두 가지를 제공한다. 정보보안산업은 기존의 산업형태에 ICT기술이 융합되면서 다양한 형태의 제품과 서비스가 제공되며, 지금 현재도 새로운 사업영역과 제품이 창조되고 있다. 이로 인해 정보보안 기업 목록 작성 시 KIS-IC에 분류된 세분류를 기준으로 판단하기보다 한국표준산업분류 대분류 기준으로 기업목록을 작성하고, 여기서 비 정보보안 기업을 삭제하는 것이 표본기업의 누락을 방지 할 수 있는 보다 효과적인 방법으로 생각하였다. 이에 본 연구는 본문에 기술한 조사방법을 사용하여 정보보안 기업을 선별하였다.

<표 2> 연도별 정보보안 기업 현황

(단위 : 사)

구분	정보보안 기업 수					
	물리적 보안 기업	네트워크 및 시스템 보안 기업	보안 응용 소프트웨어 기업	암호·인증 기업	시스템 통합 기업	합계
2006년	6	8	2	0	10	26
2007년	8	9	2	0	11	30
2008년	0	0	0	0	0	0
2009년	0	0	0	0	0	0
2010년	9	12	3	0	12	36
2011년	9	13	4	1	12	36
2012년	12	15	4	1	12	44
2013년	11	15	5	1	12	44
2014년	12	17	7	2	12	50
2015년	0	0	0	0	0	0
2016년	15	20	9	4	13	61
2017년	15	22	9	4	13	63

업과 같이 연구개발을 통한 자체 상품의 발굴을 필요로 한다. 향후 이 부분은 한국 내 시스템 통합 기업의 도전과제로 생각된다. 물리적 보안 기업 영역은 2006년 6개 사에서 2017년 15개사로 약 2.5배의 성장 추세를 보인다. 4차 산업혁명의 도래는 많은 영역에 있어 무인화와 각종 사물이 단일 통신망 내에서 연결됨과 더불어 기기 간 통신을 통한 자동화를 불러올 것이다. 이러한 시대의 도래는 일상생활 및 각종 물건의 생산에 있어 편리함과 효율화를 가져올 것이다. 그러나 여기서 우려해야할 사실 중 하나는 해킹에 의한 보안사고의 발생이다. 예를 들어 공장에서 생산된 물건이 주인도 모르는 사이에 다른 곳으로 배송되어 불법적으로 거래될 수 있다. 또한 경쟁 사의 생산 시스템을 마비시켜 자사의 이익을 향상시킬 수 있다. 이외에도 다양한 방법으로 보안사고의 피해가 발생할 수 있다. 따라서 향후 많은 기업가는 자체적으로 보안인력을 확보하기 보다는 외부에 자사의 보안을 의뢰할 것으로 생각된다. 이는 물리적 보안 영영에 대해 현재보다 더욱 많은 수요를 창출할 것이다.

4.2 실증분석 결과

4.2.1 개인정보 유출 기업에 대한 실증분석 결과

<표 3>은 개인정보 유출 기업에 대한 사건

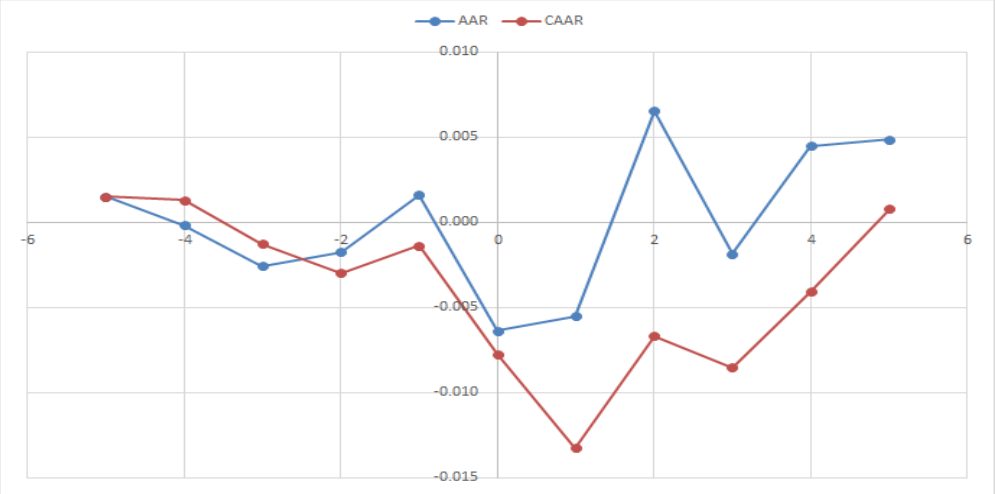
<표 3> 개인정보 유출 기업에 대한 AAR 및 CAAR

사건일	AAR	AAR의 t값	CAAR	CAAR의 t값
-5	0.001	0.519	0.001	0.519
-4	0.000	-0.061	0.001	0.324
-3	-0.003	-0.894	-0.001	-0.252
-2	-0.002	-0.603	-0.003	-0.520
-1	0.002	0.565	-0.001	-0.212
0	-0.006*	-2.215	-0.008	-1.098
1	-0.006	-1.920	-0.013	-1.742
2	0.007*	2.283	-0.007	-0.822
3	-0.002	-0.645	-0.009	-0.991
4	0.004	1.557	-0.004	-0.447
5	0.005	1.693	0.001	0.084

주 1) **, *는 각각 1%, 5% 수준에서 유의함.
2) 관측수(n)는 47개임.

전 -5일에서 사건 후 5일 간의 AAR 및 이의 t값 그리고 CAAR 및 CAAR의 t값을 보여준다. 개인정보 유출 기업에 대한 사건공시는 사건일(0일)에 -0.6%의 음(-)의 비정상수익률을 보이며, 이는 5% 유의수준에서 유의하였다. 즉, 개인정보 유출이 기업의 주가에 부정적인 영향을 미침을 알 수 있었다. 비록 5% 수준에서 유의하지 않으나 사건일 이후 첫날(1일)의 주식가격이 음(-)의 AAR값을 보이고 있다. 이는 개인정보 유출의 부정적 정보에 대한 시장의 지연반응으로 생각할 수 있다. 또는 일부 사건의 공시가 주식시장 마감에 근접하여 또는 이후에 이루어짐으로써 사건 일에 정보가 주식가격에 반영되지 못하고 사건일 다음 일(1일)에 반영된 결과로 볼 수 있다. 부정적 정보를 가급적 감추고자하는 인간의 심리를 고려할 때, 사건일 다음 날 음(-)의 주가반응은 아마도 후자의 경우로 생각된다. 사건일 다음 날 CAAR의 t값이 통계적으로 유의한 수준에 매우 근접하고 있다. 다소 특이한 사실은 사건공시 이후 2일차에 5% 수준에서 유의한 양(+)의 AAR이며, 이로 인해 개인정보 유출에 대한 부정적 주가반응이 모두 사라지고 있음을 알 수 있다. 표본수가 47개로 다소 충분하지 않은 측면이 있어, 이것이 무엇이라 쉽게 단정하기 어렵다. <그림 1>은 -5일부터 +5일까지의 AAR 및 CAAR을 도식화한 것이다. 사건일과 사건일 다음날에 주식가격이 떨어짐을 알 수 있다.

<표 4>는 개인정보 유출 기업에 대한 기간별 CAAR을 보여준다. 사건일과 사건일 다음날의 CAAR은 -0.012로 1% 수준에서 유의하다. 결과적으로 개인정보 유출 시 기업의 주가가 약 1.2% 내려감을 알 수 있다. 사건일 이전 1일과 이후 1일의 AAR을 누적한 CAAR은 -0.010으



<그림 1> 개인정보 유출 기업의 AAR 및 CAAR

<표 4> 개인정보 유출 기업에 대한 기간별 CAAR

기간	CAAR	CAAR의 t값	기간	CAAR	CAAR의 t값
-1일 ~ 0일	-0.005	-1.167	-3일 ~ 3일	-0.010	-1.296
-1일 ~ 1일	-0.010*	-2.061	-5일 ~ 5일	0.001	0.084
-1일 ~ 2일	-0.004	-0.643	0일 ~ 1일	-0.012**	-2.924
-2일 ~ 2일	-0.005	-0.845			

주 1) **, *는 각각 1%, 5% 수준에서 유의함.
2) 관측수(n)는 47개임.

로 5% 수준에서 유의하였다. 0일에서 1일에 대한 CAAR이 -1일에서 1일에 대한 CAAR보다 더욱 유의하다.

<표 5>는 개인정보 유출 기업에 대한 횡단면 회귀분석 결과이다. 모형 1-a는 AAR의 값이 통계적으로 유의한 사건일의 AR값을 종속변수로, 모형 1-b는 AAR의 값이 유의수준에 매우 근접하는 사건일 이후 1일의 AR값을 종속변수로 설정한 것이다. 모형 2는 기간별 CAAR값이 가장 유의하게 나오는 0일에서 1일까지의 값을 이용하였다. 모형 1 및 2의 기업규모변수 $LN(ASSET)$은 5% 수준에서 유의하지 않았다. 기업규모가 비정상수익률 및 누적비정상수익률에 영향을 미치지 않았다. 성장기회의 대용변수 ME/BE는 모형 1-b의 경우 5% 수준에서 유의하다. 이는 성장기회가 클수록 더 많은 음의 AR이 발생함을 의미한다. 기업유형의 더미변수 $FIRM\,TYPE$은 5% 수준에서 유의하지 않았다. 조정된(adjusted) R^2값은 0.1 이하이며, 모형의 적합도를 나타내는 F값은 5% 수준에서 유의하지 않았다.

<표 5> 개인정보 유출 기업에 대한 회귀분석 결과

모형 1 : $AR_i = \alpha + \beta_1 LN(ASSET) + \beta_2 (ME/BE) + \beta_3 FIRM TYPE_i + \epsilon_i$
모형 2 : $CAR_i = \alpha + \beta_1 LN(ASSET) + \beta_2 (ME/BE) + \beta_3 FIRM TYPE_i + \epsilon_i$

변수	모형 1-a (AR_0)	모형 1-b (AR_1)	모형 2 ($CAR_{0\sim1}$)
상수	-0.025 (-0.735)	-0.027 (-0.836)	-0.053 (-1.005)
$LN(ASSET)$	0.001 (0.581)	0.001 (0.817)	0.002 (0.893)
ME/BE	-0.000 (-0.308)	-0.003* (-2.286)	-0.003 (-1.632)
$FIRM TYPE$	-0.001 (-0.149)	-0.001 (-0.173)	-0.002 (-0.206)
$Adjusted\text{-}R^2$	-0.055	0.092	0.036
$F\text{-}value$	0.195	2.547	1.569
관측수(n)	47		

주) **, *는 각각 1%, 5% 수준에서 유의함. ( )안은 t값임.

4.2.1 정보보안 기업의 실증분석 결과

<표 6>은 개인정보 유출 기업의 사건공시가 정보보안 기업의 주가에 미치는 영향을 보여준다. <표 6> 내 수치는 정보보안 기업의 사건공시 일 전 -5일에서 사건공시 일 이후 5일 간의 AAR 및 이의 t값과 CAAR 및 CAAR의 t값이다. 정보 유출 기업에 대한 사건공시는 전체 정보보안 기업의 주가에 사건일(0일)에 -0.001, 0.000의 유의하지 않은 AAR 및 CAAR을 보인다. 사건일 이후 1일차 역시 AAR 및 CAAR은 0.001 및 0.001의 5% 수준에서 유의하지 못하다. 이에 본 연구는 정보보안 기업을 물리적 보안, 네트워크 및 시스템 보안, 보안 응용 소프트웨어, 암호·인증, 시스템 통합으로 분류하여 AAR 및 CAAR을 살펴보았으며, 그 결과 역시 <표 6> 내에 제시되어 있다. 사건일 다음 날인 1일에 네트워크 및 시스템 보안 기업의 AAR은 0.005로 5% 수준에서 유의한 양(+)의 값을 보였다. 반면, 물리적 보안, 보안 응용 소프트웨어, 암호·인증 및 시스템 통합 기업의 AAR 및 CAAR은 어떠한 날에서도 유의한 결과를 보이지 않았다. 이는 개인정보 유출에 따른 정보전이 효과는 정보보안 기업 중 네트워크 및 시스템 보안 기업에서 발생한다는 것을 보여준다. <그림 2>는 정보보안 기업에 대한 -5일부터 +5일까지의 AAR 및 CAAR을 도식화한 것이다. 네트워크 및 시스템 보안 기업의 AAR이 사건일 다음날 올라감을 알 수 있다.[5] <표 7>은 정보보안 기업에 대한 기간별 CAAR을 보여준다. 사건일과 사건일 다음날 전체 정보보안 기업의

5) 사건 당일 정보보안 기업의 수익률에 영향을 미칠 수 있는 개별 사건들이 있을 수 있다. 향후 이 부분을 통제하여 보다 엄밀한 연구를 진행할 필요가 있다.

CAAR은 0.004로 5% 수준에서 유의하다. 결과적으로 이는 개인정보 유출 시 정보보안 기업으로의 정보전이 효과가 존재함을 거듭 보여주는 것이라 하겠다. 네트워크 및 시스템 보안 기업의 CAAR이 0.004로 다소 유의하지 못했다. 이는 개인정보 유출의 사건공시 일에 네트워크 및 시스템 보안 기업의 AAR이 양(+)의 유의한 값을 보이지 못한 것에 기인한 것이다. 결과적으로 이는 정보전이에 시간이 소요됨을 보여주는 것이다. 다시 말해 어떤 사건에 대한 정보가 주식시장으로 전달될 때 1차적으로 이 정보와 직접적으로 관계된 주식의 가격이 변화하며, 시간적 간격을 두고 2차적으로 이 정보와 관련된 기업의 주식 가격에 반응이 일어나게 된다.

<표 8>은 정보보안 기업에 대한 횡단면 회귀분석 결과이다. 모형 3-a는 사건일의 AR값을 종속변수로, 모형 3-b는 네트워크 및 시스템보안 기업의 AAR 값이 통계적으로 유의한 사건일 이후 1일의 AR값을 종속변수로 설정한 것이다. 모형 4는 모형 2와 같이 기간별 CAAR값이 가장 유의하게 나오는 0일에서 1일까지의 값을 이용하였다. 모형 3 및 4의 기업규모변수 $LN(ASSET)$은 5% 수준에서 유의하지 않았다. 정보유출 기업에 대한 횡단면 회귀분석결과와 같이 기업규모가 비정상수익률 및 누적비정상수익률에 영향을 미치지 않았다. 성장기회의 대용변수 ME/BE는 모든 모형에 있어 5% 수준에서 유의한 음(-)의 값을 보였다. 이는 성장기회가 클수록 더 많은 음의 AR이 발생함을 의미한다. 기업유형의 더미변수 PHY(물리적 보안 기업의 더미변수), NS(네트워크 및 시스템 보안 기업의 더미변수), SOL(보안 응용 소프트웨어 기업의 더미변수), CER(암호・인증 기업의 더미변수) 및 SI(시스템 통합 기업의 더미변수) 중 NS가 모형 3-b에서 5% 수준에서 유의한 양(+)의 값을 보였으며, 나머지 더미변수는 모두 유의하지 않았다. 모형 4의 NS는 비록 5% 수준에서 유의하지 않지만, 5% 수준에서 유의한 양(+)의 t값에 근접하고 있다. 이는 상기에서 언급한 정보전이 효과의 속도에 기인한 것으로 생각된다. 조정된(adjusted) R^2값은 최소 0.02에서 최대 0.014의 범위에 있다. 모형 3-a를 제외한 모든 모형의 F값은 1% 수준에서, 모형 3-a의 첫째 열 F값은 5% 수준에서 각각 유의하다.

<표 6> 정보보안 기업에 대한 AAR 및 CAAR

사건일	AAR	AAR의 t값	CAAR	CAAR의 t값
a. 전체(n=1,535)				
-5	-0.001	-0.609	-0.001	-0.609
-4	0.001	0.583	0.000	-0.018
-3	0.001	0.529	0.001	0.291
-2	0.000	0.222	0.001	0.363
-1	-0.000	-0.129	0.001	0.267
0	-0.001	-0.470	0.000	0.052

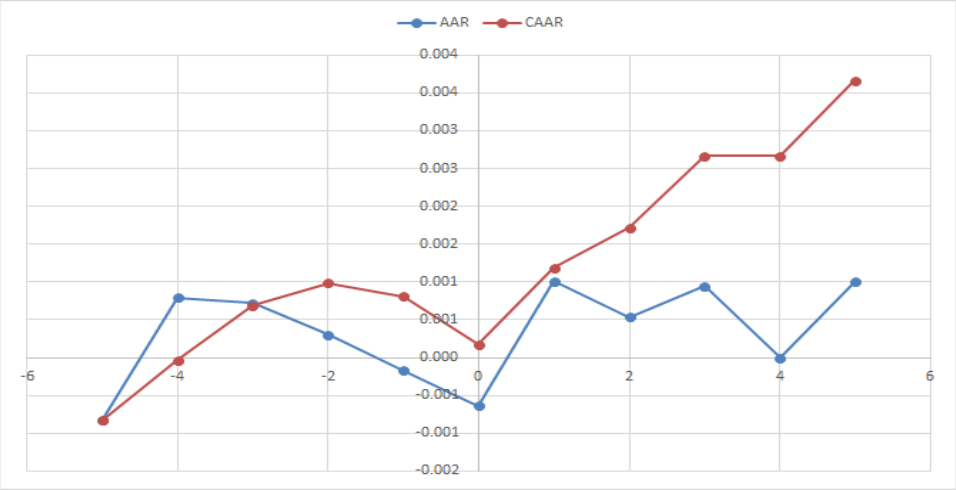
표 계속

사건일	AAR	AAR의 t값	CAAR	CAAR의 t값
1	0.001	0.743	0.001	0.329
2	0.001	0.391	0.002	0.446
3	0.001	0.696	0.003	0.652
4	0.000	0.000	0.003	0.619
5	0.001	0.735	0.004	0.812
b. 물리적 보안(n=384)				
-5	-0.001	-0.479	-0.001	-0.479
-4	0.001	0.435	0.000	-0.031
-3	-0.001	-0.414	-0.001	-0.264
-2	0.001	0.540	0.000	0.041
-1	0.001	0.460	0.001	0.242
0	0.000	0.153	0.001	0.284
1	-0.001	-0.347	0.001	0.131
2	0.002	0.930	0.002	0.452
3	0.003	1.382	0.005	0.887
4	-0.001	-0.390	0.004	0.718
5	0.003	1.401	0.007	1.107
c. 네트워크 및 시스템 보안(n=518)				
-5	-0.001	-0.324	-0.001	-0.324
-4	0.000	0.144	0.000	-0.127
-3	0.004	1.797	0.004	0.934
-2	0.000	0.115	0.004	0.866
-1	0.000	0.123	0.004	0.829
0	-0.001	-0.222	0.004	0.667
1	0.005*	2.022	0.008	1.381
2	-0.002	-0.792	0.007	1.012
3	-0.001	-0.523	0.005	0.780
4	0.001	0.311	0.006	0.838
5	0.002	0.665	0.008	1.000
d. 보안 응용 소프트웨어(n=173)				
-5	-0.001	-0.268	-0.001	-0.268
-4	-0.001	-0.246	-0.001	-0.363
-3	0.001	0.454	0.000	-0.034
-2	-0.003	-1.671	-0.004	-0.865

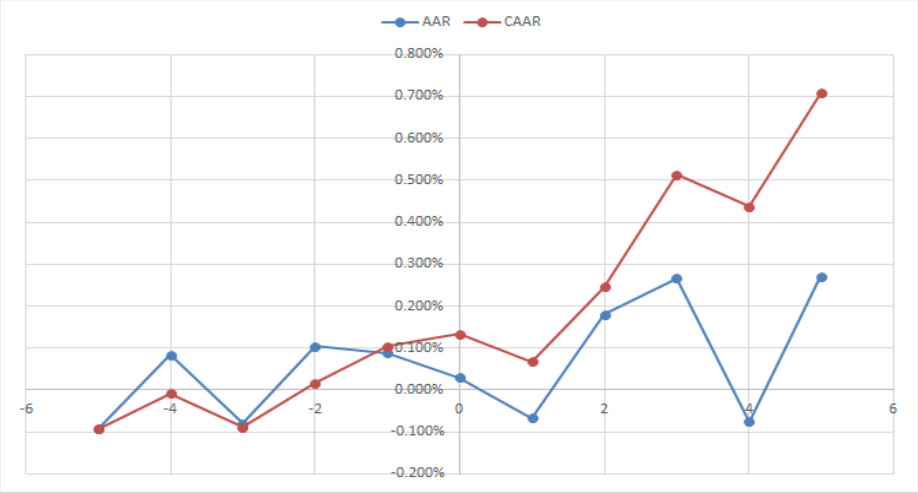
표 계속

사건일	AAR	AAR의 t값	CAAR	CAAR의 t값
-1	0.001	0.686	-0.002	-0.467
0	-0.001	-0.429	-0.003	-0.601
1	0.002	1.154	-0.001	-0.121
2	0.002	1.008	0.001	0.243
3	0.000	-0.212	0.001	0.159
4	0.000	-0.170	0.001	0.097
5	0.002	1.058	0.003	0.412
e. 암호・인증(n=45)				
-5	0.001	0.159	0.001	0.159
-4	0.003	0.514	0.003	0.476
-3	0.002	0.336	0.005	0.583
-2	0.008	1.667	0.013	1.338
-1	0.001	0.166	0.014	1.271
0	-0.002	-0.339	0.012	1.022
1	-0.009	-1.823	0.003	0.257
2	0.007	1.461	0.011	0.757
3	0.009	1.839	0.020	1.327
4	0.007	1.421	0.027	1.708
5	0.000	0.044	0.027	1.642
f. 시스템 통합(n=416)				
-5	-0.001	-0.604	-0.001	-0.604
-4	0.002	0.903	0.001	0.211
-3	-0.002	-1.256	-0.002	-0.553
-2	0.000	0.213	-0.001	-0.372
-1	-0.003	-1.345	-0.004	-0.934
0	-0.001	-0.775	-0.005	-1.169
1	-0.001	-0.803	-0.007	-1.386
2	0.001	0.501	-0.006	-1.119
3	0.002	0.939	-0.004	-0.742
4	-0.001	-0.430	-0.005	-0.840
5	-0.002	-0.891	-0.007	-1.069

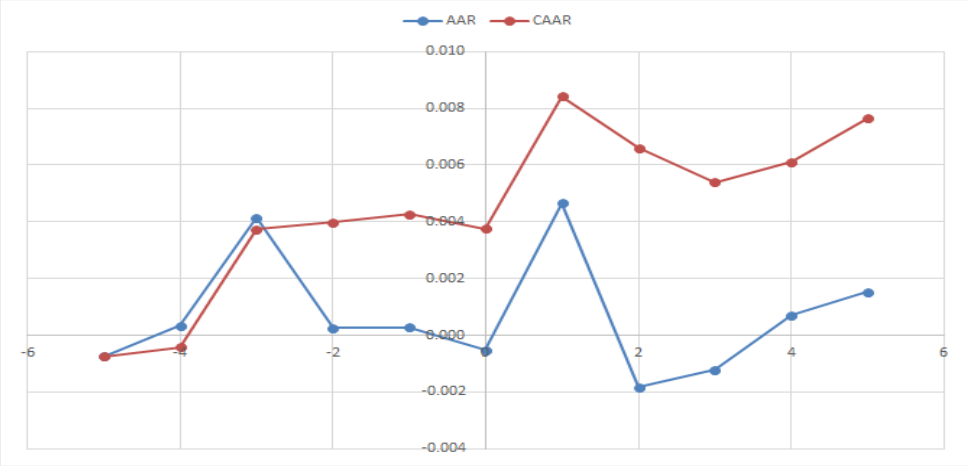
주 1) **, **는 각각 1%, 5% 수준에서 유의함.
2) n은 표본의 관측수임.



a. 전체

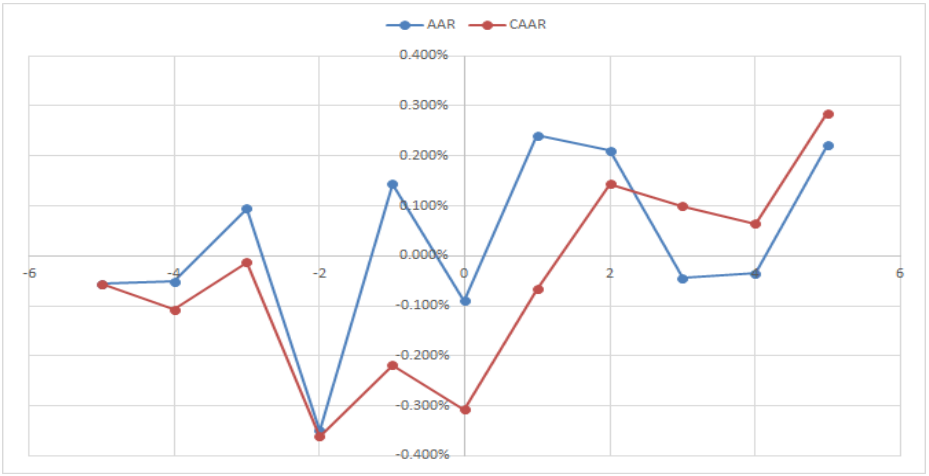


b. 물리적 보안

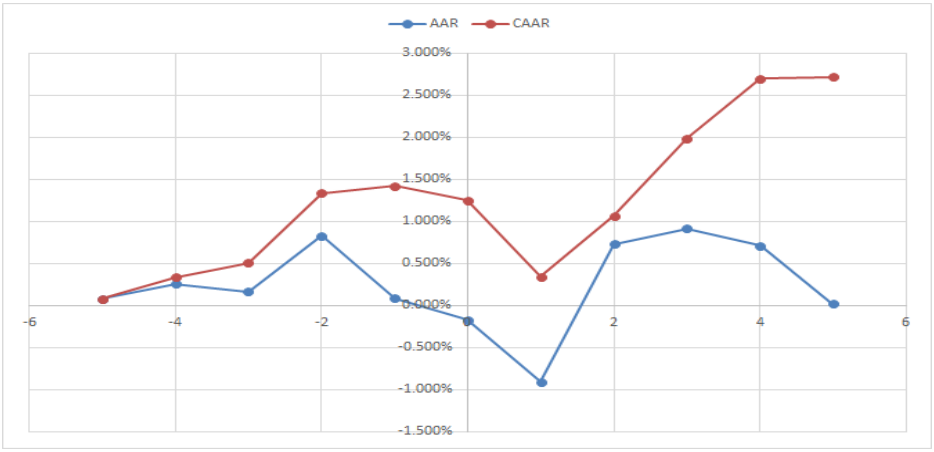


c. 네트워크 및 시스템 보안 기업

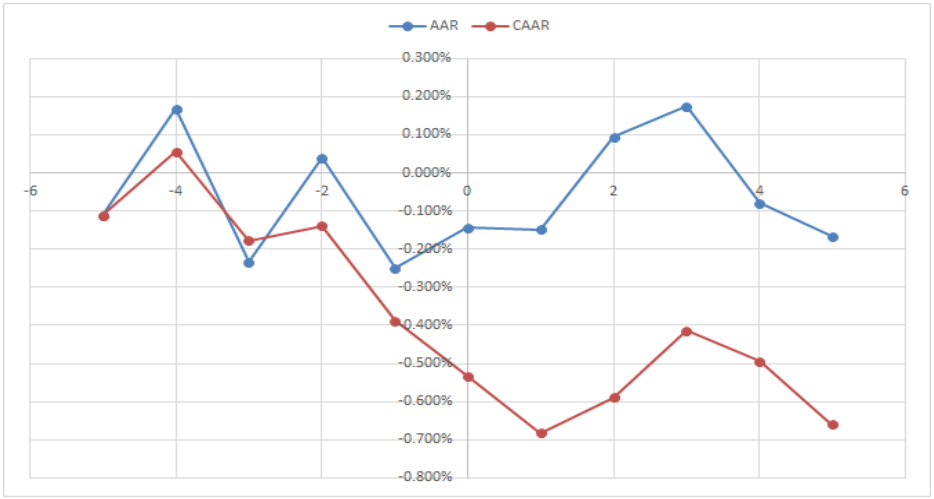
그림 계속



d. 보안 응용 소프트웨어



e. 암호·인증



f. 시스템 통합

<그림 2> 정보보안 기업의 AAR 및 CAAR

<표 7> 정보보안 기업에 대한 기간별 CAAR

기간	CAAR	CAAR의 t값	기간	CAAR	CAAR의 t값
a. 전체(n=1,535)					
-1일 ~ 0일	-0.001	-0.424	-3일 ~ 3일	0.003	0.749
-1일 ~ 1일	0.000	0.083	-5일 ~ 5일	0.004	0.812
-1일 ~ 2일	0.001	0.268	0일 ~ 1일	0.0004*	0.196
-2일 ~ 2일	0.001	0.339			
b. 물리적 보안(n=384)					
-1일 ~ 0일	0.001	0.433	-3일 ~ 3일	0.005	1.022
-1일 ~ 1일	0.001	0.153	-5일 ~ 5일	0.007	1.107
-1일 ~ 2일	0.002	0.598	0일 ~ 1일	0.000	-0.138
-2일 ~ 2일	0.003	0.776			
c. 네트워크 및 시스템 보안(n=518)					
-1일 ~ 0일	0.000	-0.070	-3일 ~ 3일	0.006	0.952
-1일 ~ 1일	0.004	1.110	-5일 ~ 5일	0.008	1.000
-1일 ~ 2일	0.003	0.565	0일 ~ 1일	0.004	1.272
-2일 ~ 2일	0.003	0.557			
d. 보안 응용 소프트웨어(n=173)					
-1일 ~ 0일	0.001	0.182	-3일 ~ 3일	0.002	0.374
-1일 ~ 1일	0.003	0.815	-5일 ~ 5일	0.003	0.412
-1일 ~ 2일	0.005	1.209	0일 ~ 1일	0.002	0.512
-2일 ~ 2일	0.002	0.334			
e. 암호·인증(n=45)					
-1일 ~ 0일	-0.001	-0.122	-3일 ~ 3일	0.016	1.250
-1일 ~ 1일	-0.010	-1.152	-5일 ~ 5일	0.027	1.642
-1일 ~ 2일	-0.003	-0.267	0일 ~ 1일	-0.011	-1.529
-2일 ~ 2일	0.006	0.506			
f. 시스템 통합(n=416)					
-1일 ~ 0일	-0.004	-1.499	-3일 ~ 3일	-0.005	-0.954
-1일 ~ 1일	-0.005	-1.688	-5일 ~ 5일	-0.007	-1.069
-1일 ~ 2일	-0.005	-1.211	0일 ~ 1일	-0.003	-1.116
-2일 ~ 2일	-0.004	-0.988			

주 1) **, *는 각각 1%, 5% 수준에서 유의함.
2) n은 표본의 관측수임.

<표 8> 정보보안 기업에 대한 회귀분석 결과

모형 3 : $AR_i = \alpha + \beta_1 \ln(ASSET)_i + \beta_2 (ME/BE)_i + \beta_3 PHY_i + \beta_4 NS_i + \beta_5 SOL_i + \beta_6 CER_i + \beta_7 SI_i + \epsilon_i$
모형 4 : $CAR_i = \alpha + \beta_1 \ln(ASSET)_i + \beta_2 (ME/BE)_i + \beta_3 PHY_i + \beta_4 NS_i + \beta_5 SOL_i + \beta_6 CER_i + \beta_7 SI_i + \epsilon_i$

변수	모형3-a (AR_0)		모형3-b (AR_1)		모형 4 ($CAR_{0\sim1}$)	
상수	-0.005 (0.219)	0.003 (0.127)	0.007 (0.296)	-0.008 (-0.329)	0.012 (0.380)	-0.005 (-0.158)
LN(ASSET)	-0.000 (-0.115)	0.000 (0.012)	-0.000 (-0.0049)	0.000 (13.278)	-0.000 (-0.119)	0.000 (0.349)
ME/BE	-0.002** (2.753)	-0.002** (-2.765)	-0.002** (-3.501)	-0.002** (-3.345)	-0.004** (-4.604)	-0.004** (-4.496)
PHY	0.001 (0.492)		-0.003 (-1.298)		-0.002 (-0.062)	
NS		-0.000 (-0.212)		0.006* (2.518)		0.006 (1.747)
SOL		-0.001 (-0.394)		0.003 (0.952)		0.002 (0.436)
CER		0.000 (0.008)		-0.005 (-0.945)		-0.005 (-0.707)
SI		-0.001 (-0.627)		0.000 (-0.161)		-0.002 (-0.569)
Adjusted-R^2	0.003	0.002	0.007	0.012	0.012	0.014
F-value	2.705*	1.389	4.518**	3.969**	7.176**	4.746**
관측수(n)	1,530					

주) **, *는 각각 1%, 5% 수준에서 유의함. ( )안은 t값임.

Ⅴ. 결 론

인터넷을 통한 각종 거래가 활성화되면서 기업에 의해 수집된 개인정보가 무단으로 거래되거나 부주의하게 제3자에게 유출되는 각종 사고 및 이에 따른 다양한 문제가 발생하고 있다. 이에 본 연구는 한국의 기업을 대상으로 기업의 개인정보 유출의 공시가 해당 기업 및 정보보안 기업의 주가에 어떠한 영향을 미치는 지를 살펴보았다. 정보보안 기업의 주가반응을 살펴보는 것은 개인정보 유출에 따른 정보전이 효과를 검증하는 것이며, 이는 한국에서 실시된 바 없다. 이를 위해 본 연구는 한국유가증권시장 및 코스닥시장에 상장된 기업을 대상으로 개인정보 유출 사건을 조사하였다. 조사기간은 2006년부터 2017년까지 총 12년이며, 표본기간 동안 총 47건(30개 사)의 개인정보 유출 사고 및 65개의 정보보안 표본기업을 확보하였다.

이렇게 확보한 표본을 이용하여 사건연구를 진행하였으며, 이의 주요 실증분석 결과는 다음과 같다.

첫째, 사건 일 개인정보 유출 기업의 AAR은 5% 수준에서 유의한 음(-)의 값을 보였다. 비록 5% 수준에서 유의하지 않으나 사건일 이후 1일차 주식가격이 음(-)의 AAR값을 보였으며, CAAR의 값 또한 통계적으로 유의한 수준에 매우 근접하였다. 사건일과 사건일 다음날의 CAAR은 1% 수준에서 유의한 음(-)의 값을 보였다. 개인정보 유출 시 기업의 주가가 약 1.2% 감소하였다. 또한 사건일 이전 1일과 이후 1일의 AAR을 누적한 CAAR은 5% 수준에서 유의한 음(-)의 값을 보였다. 결과적으로 개인정보 유출이 기업가치를 감소시킴을 확인하였다.

둘째, 개인정보 유출 기업에 대한 횡단면 회귀분석 결과 모형 1 및 2의 기업규모변수 $LN(ASSET)$은 5% 유의수준에서 의미 있는 결과를 보이지 못했다. 기업규모가 비정상수익률 및 누적비정상수익률에 영향을 미치지 못했다. 모형 1-b의 성장기회의 대용변수 ME/BE는 5% 수준에서 유의한 음(-)의 값을 보였다. 성장기회가 클수록 기업가치가 더욱 크게 하락함을 확인할 수 있었다. 기업유형의 더미변수 $FIRM\,TYPE$은 5% 수준에서 유의하지 않았다.

셋째, 정보 유출 기업에 대한 사건공시는 전체 정보보안 기업의 AAR 및 CAAR에 유의한 영향을 미치지 못했다. 정보보안 기업을 물리적 보안, 네트워크 및 시스템 보안, 보안 응용 소프트웨어, 암호・인증, 시스템 통합으로 분류하여 분석한 결과 사건일 다음 날(1일) 네트워크 및 시스템 보안 기업의 AAR은 5% 수준에서 유의한 양(+)의 값을 보였다. 반면, 물리적 보안, 보안 응용 소프트웨어, 암호·인증 및 시스템 통합 기업의 AAR 및 CAAR은 어떠한 날에서도 유의한 결과를 보이지 않았다. 개인정보 유출에 따른 정보전이 효과가 정보보안 기업 중 네트워크 및 시스템 보안 기업에서 발생함과 더불어 이 효과가 시간적 간격을 두고 나타남을 확인할 수 있었다.

넷째, 정보보안 기업에 대한 횡단면 회귀분석 결과, 모형 3 및 4의 기업규모변수 $LN(ASSET)$은 5% 수준에서 유의하지 않았다. 성장기회의 대용변수 ME/BE는 모든 모형에 있어 5% 수준에서 유의한 음(-)의 값을 보였다. 결과적으로 성장기회가 클수록 주식가격이 적제 올라감을 알 수 있었다. 기업유형의 더미변수 PHY(물리적 보안 기업의 더미변수), NS(네트워크 및 시스템 보안 기업의 더미변수), SOL(보안 응용 소프트웨어 기업의 더미변수), CER(암호·인증 기업의 더미변수) 및 SI(시스템 통합 기업의 더미변수) 중 NS가 모형 3-b에서 5% 수준에서 유의한 양(+)의 값을 보였으며, 나머지 더미변수는 모두 유의하지 않았다. 개인정보 유출 기업에서 정보보안 기업으로의 정보전이 효과가 나타나기 위해선 일정한 전이 시간이 요구됨을 거듭 확인할 수 있었다.

본 연구는 개인정보 유출이 해당 기업의 주가에 미치는 영향과 더불어 정보보안 기업으로의 정보전이 효과를 살펴보았다. 한국과 미국은 유의한 결과를 보이나, 중국은 유의한 결과를 보이지 않는 것으로 보고되고 있다. 향후 어떠한 요인이 국가별로 상이한 결과를 제시하는지에 대해 보다 엄밀한 연구가 진행될 필요가 있겠다.

개인정보 보호에 대한 중요성이 날로 증가되고 있는 오늘날에 있어, 본 연구의 결과는 개인정보를 수집·활용하고 있는 기업에게는 이에 대한 철저한 보안이 필요함을 말한다. 향후 우리의 삶에 다가올 4차 산업혁명은 무엇보다도 보안의 중요성을 강조한다. 무인화 자동차, 공장 등 자동화 부문에 있어 정보유출사고는 심각한 사회적·경제적 문제를 가지고 올 수 있다. 따라서, 이는 정보보안 기업에게 새로운 사업모델을 요구할 것이다. 고객의 정보유출 및 더 나아가 각종 사업 영역에 있어 해킹으로 인한 피해가 발생하지 않도록 지속적인 기술혁신이 정보보안 기업에게 요구되고 있다. 또한 국가는 개인정보가 부당하게 유출되어 활용되지 않도록 하는 수단으로 정보보안 기업의 육성을 모색할 필요가 있겠다.

참고문헌

권영옥, 김병도, “정보보안 사고와 사고방지 관련 투자가 기업가치에 미치는 영향,” Information Systems Review, 제9권, 제1호, 2007, pp. 105-120.

김민정, 허남길, 유진호, “개인정보 유출 사고시 정보보호 기업의 주가 변동에 관한 연구,” 정보보호학회논문지, 제26권, 제1호, 2016, pp. 275-283.

김정연, “개인정보 유출이 기업의 주가에 미치는 영향,” 한국전자거래학회지, 제18권, 제1호, 2013, pp. 1-12.

김여라, 이해춘, 유진호, 「가상가치접근법(CVM)을 활용한 개인정보보호의 가치산출 방법론 고찰」, 한국정보보호진흥원, 2007.

김태환, 이해니, 유진호, “개인정보 유출사고 이후 기업의 주가변동 패턴에 대한 고찰,” 한국경영정보학회 춘계공동학술대회, 2014, pp. 89-92.

데이코산업연구소, 「정보보호산업 실태와 기술개발 동향」, 2013.

양재모, “전자거래상 개인정보보호에 대한 민사적 접근”, 상이버커뮤니케이션 학보, 제 27권, 제 2호, 2010, pp. 91-119.

이해춘, 안경애, “CVM을 이용한 개인정보 유출의 손실가치 분석,” 생산성논집, 제22권, 제2호, 2008, pp. 1-24.

유진호, 지상호, 임종인, “개인정보 유·노출 사고로 인한 기업의 손실비용 추정,” 정보보호학회논문지, 제19권 제4호, 2009, pp. 63-75.

정형찬, “한국주식시장에 적합한 사건연구 방법론의 고안,” 재무관리연구, 제14권, 제2호, 1997, pp. 273-312.

주미진, 김광용, 김진수, “개인정보 유출이 기업의 주가에 미치는 영향 : 한국 및 중국의 기업을 대상으로,” 인터넷전자상거래연구, 제16권, 제3호, 2016, pp. 53-65.

채승완, “개인정보보호의 경제적 효과,” 소비자문제연구, 제33호, 2008, pp. 43-64.

한귀현, “개인정보보호법제의 동향과 개선방안 -개인정보보호기본법안을 중심으로” 공법학연구, 제6권, 제2호, pp. 82-107.

한창희, 채승완, 유병준, 안대환, 박채희, “기업의 개인정보 유출로 인한 경제적 피해

규모 산출방법," 한국전자거래학회지, 제16권, 제4호, 2011, pp. 17-31.

홍일유, 이재훈, 강성민, "정보보안 사고에 대한 공시가 시장에서 기업의 주식가치에 미치는 영향," Entrue Journal, 제14권, 제2호, 2015, pp. 33-56.

Acquisti, A., A. Friedman, and R. Telang, "Is There Cost Privacy Breaches? An Event Study," *Working Paper*, 2006, pp. 1563-1580.

Brown, S. and S. Warner, "Measuring Security Price Performance," *Journal of Financial Economics*, Vol. 8, No. 3, 1980, pp. 205-258.

Brown, S. and S. Warner, "Using Daily Stock Returns: The Case of Event Studies," *Journal of Financial Economics*, Vol. 14, No. 1, 1985, pp. 3-31.

Cavusoglu, H., B. Mishra, and S. Raghunathan, "The Effect of Internet Security Breach Announcement on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers," *International Journal of Electronic Commerce*, Vol. 9, No. 1 2004, pp. 69-104.

Chan, S. H., J. W. Kensinger, A. J. Keown, and J. D. Martin, "Do strategic alliances create value?," *Journal of Financial Economics*, Vol. 46, 1997, pp. 199-221.

Das, P., K. Sen, and S. Sengupta, "Impact of strategic alliances on firm valuation." *The Academy of Management Journal*, Vol. 41, 1998, pp. 27-41.

Ettredge, M., and V. J. Richardson, "Assessing the Risk in e-Commerce," *Proceedings of the Thirty fifth Hawaii International Conference on Systems Sciences*, Los ALamitos, CA: IEEE Computer Society Press, 2002.

Ishiguro, M., H. Tanaka, K. Matsuura, and I. Murase, "The Effect of Information Security Incidents on Corporate Values in the Japanese Stock Market," *In Workshop on the Economics of Securing the Information Infrastructure*, 2006, pp. 1-15.

Lee, H., S. Kim, and J. Kim, "Open technology innovation activity and firm value: evidence from Korean firms," *Applied Economics*, Vol. 44, 2012, pp. 3351-3561.

Patel, N., "The Effect of IT Hack Announcements on the Market Value of Publicly Traded Corporations," *Working Paper*, 2010, pp. 1-24.

Szewczyk, S. H., G. P. Tsetsekos, and. Zantout, "The valuation of corporate R&D expenditures: evidence from investment opportunities and free cash flow," *Financial Management*, Vol. 25, 1996, pp. 105-110.

Telang, R., and S. Wattal, "An Empirical Analysis of the Impact of Software Vulnerability Announcements on the Firm Stock Price," *IEEE Transactions*

on Software Engineering, Vol. 33, No. 8, 2007. pp. 544-557.

박 상 수 (Park, Sang-Soo)

현재 조선대학교에서 경영학 박사과정 중에 있으며, 주요 관심분야는 정보보안, 네트워크 통신, 메시지 서비스 등이다.

이 현 철 (Lee, Hyun-Chul)

영국 ESSEX 대학교에서 재무학 박사학위를 취득하였다. 현재 조선대학교 경영학부 부교수로 재직 중이며, 주요 관심분야는 기술금융, 자본시장통합 등이다.

<Abstract>

The Effects of Information Transfer of Personal Information Security Breaches

Park, Sang-Soo · Lee, Hyun-Chul

Purpose

Targeting Korean companies listed on Korean securities markets (i.e., KOSPI and KOSDAQ markets), this study aims to shed lights the effects of personal information security breaches on stock prices of information security companies. Interestingly, this study is, to the best of our knowledge, the first to examine the information transfer effect on personal information security breaches of companies.

Design / Methodology /Approach

To examine the information transfer effect of personal information security breaches, our study employs the event study commonly used in financial studies. To this end, we investigate a variety of events of personal information security breaches of companies listed on the KOPSI stock market and the KOSDAQ market. We collect the total samples of one hundred and twelve with forty seven of events of personal information security breaches by thirty companies and sixty five of information security companies.

Findings

The principal findings from the empirical study are as follows. First, for companies of personal information security breaches, our event study presents the significantly negative AAR (averaged abnormal return) value on the event day at the 5 % level and the highly significant negative CAAR(cumulative averaged abnormal return) value on the event day and the day after the event day at the 1 % level. The results suggest that personal information breaches significantly contribute to an decrease in value of the information breached companies. The cross sectional regressions in this study estimate the significantly negative coefficient for the ME/BE variable, the proxy for a growth opportunity at the 5 % level. This suggests a reverse relation between the growth

opportunity of companies and their value.

As for the various samples of the information security companies categorized by physical security, network and system security, security application software, code authentication, system integration, we find the significantly positive AAR on the day after the event day at the 5% level, only for the network and system security-companies. This addresses that the information transfer effect followed by personal information breaches is uniquely observable for companies categorized into network and system companies. The regressions for the network and system companies estimate the significantly positive coefficient for the NS dummy variable (i.e., the dummy of the network and system security companies) at the standard level. This allows us to identify appropriate times needed to make the information transfer effect realized from personal information breached companies to information security companies.

Keyword : Personal information breaches, Information transfer, Event study, Value of company

* 이 논문은 2018년 2월 28일 접수, 2018년 3월 22일 1차 심사, 2018년 3월 29일 게재 확정되었습니다.