JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 20, No. 8, pp. 1567-1576, Aug. 2019

기업의 정보보호관리가 영업성과와 기업가치에 미치는 영향 : 정보보호관리체계(ISMS)를 중심으로

최 동 권 · 윤 현 식*
전남대학교 경영학과

A Study on Impact of Information Security Management on Sales Performance and the Value of Corporate: Focusing on Information Security Management System(ISMS)

Dong-Kwon Choi · Yoon, Hyun Shik*
College of Business Administration, Chonnam National University, Gwangju 61186, Korea

[요 약]

본 연구는 코스피 상장기업을 대상으로 정보보호관리 활동의 하나인 ISMS인증 취득이 기업의 영업성과와 기업가치에 어떠한 영향을 미치는가에 대한 실증연구를 하였다. IT 침해사고는 사고 발생 시 규모가 크고 불가역적이며, 기업에게 심각한 재정적 위험, 그리고 기업의 명성에 치명적인 피해를 초래한다. 또한 4차 산업혁명 시대에 들어서면서 세계적으로 각국 정부들의 규제가 강화되는 추세에 있다. 그럼에도 재무적 관점에서 보안과 관련한 연구는 여전히 초기 단계에 머물러 있다. 본 연구의 실증분석 결과, 정보보호관리 활동은 기업의 영업성과와 기업가치에 모두 긍정적인 영향을 미치는 것으로 나타났다. 이러한 분석결과는 침해사고 뿐만 아니라 침해사고에 대응하는 정보보호관리가 기업의 경영성과와 기업가치에 직접적으로 영향을 미칠 수 있음을 시사한다. 따라서 기업가치에 대한 정보보호관리 활동의 긍정적 결과를 주장한 기존의 정성적 연구결과들을 지지하며 기업이 정보보호관리를 적극적으로 고려해야 하는 실증적 근거를 제시하였다.

[Abstract]

This study is an empirical study on how Information Security Management System(ISMS) certification affects business performance and the value of the corporate listed on Korea Composite Stock Price Index(KOSPI). Information security incidents cause serious financial risks to the enterprise and damage to the reputation of the enterprise. Therefore, many countries in the world are tightening regulations for information security. Nonetheless, research on information security with a financial perspective have been still in the begging stages. As a result of the empirical analysis of this study, we found that the company's management on the information security had a positive effect on their performance and corporate value. Therefore, this study supports the research which asserted the positive result of the activity for information protection on the enterprise value, and presents an empirical basis for the company to actively consider the information protection management.

색인어 : 기업가치, 영업성과, 정보보호, 정보보호관리체계, ISMS인증
Key word : Corporate value, Information security, Information Security Management System(ISMS), ISMS certificate, Sales performance

http://dx.doi.org/10.9728/dcs.2019.20.8.1567

Received 29 July 2019; **Revised** 06 August 2019
Accepted 26 August 2019

***Corresponding Author; Yoon, Hyun Shik**
Tel: +82-62-530-1452
E-mail: Dr.Yoon@jnu.ac.kr

Ⅰ. 서 론

한국은 지난 30년간 세계적인 정보화 추세에 발맞춘 중장기 국가정보화 마스터플랜을 통해 세계 최고수준의 정보통신(ICT) 인프라를 보유하게 되었고, 전자정부 세계 1위의 괄목할만한 성과를 이뤄냈다[1]. 그러나 사이버 공격 방어 기술 선도업체인 파이어아이(FireEye)에 따르면 한국은 지난해 아시아 지역 국가들 중 사이버공격을 가장 많이 받았으며, 지능형 사이버 공격 노출률이 아시아 국가 평균인 23.3%보다 두 배 가까이 높은 43.5%로 나타났다. 특히 지난 3년간 랜섬웨어(Ransomware)[1] 피해 접수는 2015년 2,678건에서 2016년 3,255건, 2017년 4,475건으로 총 피해 금액도 2015년 1,090억원에서 2016년 3,000억원, 2017년 7,000억원으로 증가추세를 보이고 있다[2]. 또한 미래창조과학방송통신위원회에 따르면 2008년부터 2016년까지 9년간 개인정보 유출 피해 규모는 1억 7,572 만명으로 국내 인구의 세 배가 넘는 수치를 보였다. 이렇게 유출된 개인정보들에는 주민등록번호를 비롯해서 신용카드번호 등과 같은 민감한 정보들이 포함된 체 국외로 유출되고 있어 국가적 재난에 가깝다고 할 수 있다[3].

사물인터넷(IoT; Internet of Things), 인공지능(AI; Artificial Intelligence), 블록체인 등 4차 산업혁명의 주요 기술이 지향하는 초연결성, 초지능성은 보안 측면에서는 약점으로 부각될 가능성이 높아 선제적인 대응을 필요로 한다. 특히 IoT 기능이 탑재된 기기가 폭발적인 속도로 증가함에 따라 날로 커지는 보안 취약성에 대한 우려가 제기된다. 가트너(Gartner)와 산업연구원의 국내외 IoT 시장 규모 전망에 따르면 글로벌 시장은 2016년 375조원에서 2017년 457조원으로, 국내 시장은 2016년 4조 9,000억원에서 2017년 6조 4,000억원 규모로 확대될 전망이다. 세계적 보안업체 시만텍 측은 "IoT 디바이스는 네트워크 상에 24시간 연결된 상태로 유지되는 경우가 대부분"이라며 "이 같은 IoT 기기가 악성코드에 감염된다면 사용자가 알지 못하는 사이 좀비 IoT 기기로 사이버범죄에 악용될 가능성이 높음을 지적하였다. 이미 2017년에는 CCTV, 네트워크 스토리지(NAS), 공유기 등 IoT 기기 10만대가 악성코드에 감염되어 아마존과 트위터, 넷플릭스 등 주요 웹사이트를 디도스 공격하는 데 동원되어 미국 동부지역의 인터넷 접속 장애를 유발하였다[4].

정보보안사고는 주식시장에서 기업의 재무적 가치에 부정적인 영향을 미친다[5-13]. 특히 이러한 부정적 영향은 E-비지니스 기업에서 더 높게 나타난다는 연구결과[6], [14]가 보고 되었을 뿐만 아니라, 기업의 유형에 관계없이 부정적인 영향을 미친다는 연구 결과도 있다[10-11]. 상기에서 보듯 보안사고는 기업의 운영에 있어서 일차적으로 주가 하락을 유발하는 재무적 위험(Financial Risk)으로 작용한다는 주장이 주류 연구결과이다. 뿐만 아니라 잠재적으로 각종 소송에 휘말리는 법률적 위험(Legal risk), 정부의 규제와 감시가 강화되는 제도적 위험(Regulatory risk), 그리고 기업 이미지에 타격을 주는 평판에 대한 위험(Reputational risk)을 내포하고 있다[15]. 가장 최근의 예로 2018년 네트워크 해킹에 의해 이용자 5,000만명 정보가 유출되었다고 밝힌 페이스북의 주가는 폭락을 했고, 미국에서는 징벌적 손해배상을 위한 재판이 진행 중이다. 또한 유럽 개인정보보호규정(GDPR)을 위반한 혐의로 16억 3000만달러 (약 1조 8125억원)에 달하는 과징금을 낼 위기에 직면하고 있다. 이에 따라 페이스북에 대한 국제적인 소송과 벌금 부과가 잇따를 전망이다[16]. 따라서 기업의 정보보안은 단순한 기술적 문제가 아닌 지속 가능한 경영을 위해 꼭 관리되어야 할 경영 전략적 필수 요소라고 할 수 있다. 마찬가지로 기업과 직간접적으로 이해관계에 있는 투자자, 금융기관, 정부 등은 적극적으로 기업의 정보보안 수준을 평가하고 의사결정에 반영해야 할 필요가 있다.

정보보호활동의 중요성과 사회적 요구가 증가함에 따라 국내에서는 정보보호와 관련한 연구가 점차적으로 증가하고 있다. 정성적 연구에서는 정보보호관리체계(ISMS; Information Security Management System)[2]인증 취득이 조직성과에 긍정적인 영향을 미침으로써 궁극적으로 기업성과를 향상시킬 수 있는 가능성을 제시하였다[17]. 또한 금융기관의 보안대책이 금융리스크를 감소시켜 영업성과에 긍정적인 영향을 미칠 수 있으며[18], 개인정보보호 관리는 재무, 고객, 업무, 지속성장 관점의 성과에 긍정적인 영향을 미친다는 주장이 제기 되었다[19]. 정량적 연구에서는 보안투자는 장기적으로 기업의 매출액을 증가시키는 데 도움을 준다는 연구 결과가 있으며[20], 사건연구를 통해 기업의 정보보안 인증 취득 공시가 단기적으로 기업의 주가에 긍정적인 영향을 미친다는 주장이 제기되었다[21]. 이들 선행 연구들은 정보보호활동이 직·간접적으로 경영성과와 기업가치에 긍정적인 영향을 미칠 수 있음을 시사한다. 따라서 본 연구에서는 제도적으로 의무화 된 정보보호관리 활동으로써 ISMS 인증 취득이 기업가치와 영업성과에 어떠한 영향을 미치는지를 정량적으로 측정하였다. 이를 위해 총 3,003개의 코스피 상장기업을 대상으로 실증 분석을 실시하였다. 분석에는 통합일반회귀분석(Pooled OLS regression)을 실시하였다.

분석결과 ISMS 인증을 대용치로 사용한 기업의 정보보호관리는 기업가치와 영업성과 모두에 긍정적인 영향을 미치는 결과를 확인할 수 있었다. 이러한 연구결과는 ISMS 인증을 통한 기업의 경쟁력 향상을 통해 수익성과 기업가치를 높이는데 도움을 줄 수 있다는 시사점을 제시한다.

본 연구는 정량적 자료들을 바탕으로 ISMS인증과 기업성과와 관련한 기존의 정성적 연구결과를 뒷받침함으로써, 기업의 정보보호관리 활동이 단순히 비용만 발생시키는 행위가

1) 컴퓨터 사용자의 파일들을 암호화하여 금전을 요구하는 악성코드 (TTA 정보통신용어사전)

2) 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(정보통신망 이용촉진 및 정보보호 등에 관한 법률)

아닌 기업의 경쟁력 제고를 통해 영업성과와 기업가치에 영향을 미친다는 것을 실증적으로 규명했다. 이는 기업이 정보보호관리를 적극적으로 고려해야 하는 실증적 근거가 될 수 있다. 또한 투자자와 금융기관에게는 리스크관리 측면에서 의사결정에 필요한 객관적 정보를, 정부에게는 제도의 개선방향을 수립하는데 정책적 시사점을 제공할 것으로 기대된다.

Ⅱ. 선행연구 및 가설설정

2-1 한국의 정보보안 관리제도

국내의 경우 지속적으로 개인정보유출사고가 발생함에 따라 개인정보를 보호하기 위해 2011년에 개인정보보호법을 제정하였고, 정보통신망 이용 촉진 및 정보 보호 등에 관한 법률 제47조에 ISMS 인증과 개인정보보호관리체계 (PIMS; Personal Information Management System)[3] 인증에 대한 근거 조항이 마련되어 있다[22]. ISMS 인증 의무대상은 연간 매출액 또는 세입 등이 1,500억 이상이거나 정보통신서비스 매출액 100억 또는 일일평균이용자 수 100만명 이상인 사업자나 기관을 대상으로 한다. 한편, 투자자들의 의사결정에 반영될 수 있도록 정보보호 공시제도를 통해 최대 인증수수료의 40%를 감면해 주고 있다 (미래창조과학부 정보보호 공시 가이드라인 2016). 또한 한국인터넷진흥원에 의하면 인증제도 취득 시 IT관련 정부과제 입찰 시 인센티브를 부여하고, 한국기업지배구조원의 상장기업대상 ESG(Environmental Social Governance) 평가에 반영 한다[23].

한국인터넷진흥원에 따르면, 2017년 기준으로 ISMS와 PIMS 인증을 유지하고 있는 기업은 각각 532개, 68개로써 저조한 수준이다. 하지만 ISMS의 경우, 2012년에 제도권으로 편입되면서 2012년 152건에서 2017년 532건으로 의무인증 대상은 증가하는 추세에 있다. 한편, 인증에 필요한 비용이 2억원 가량 발생하고 유지하는데 추가적인 비용이 소요되기 때문에, ISMS 의무 인증 대상이 인증을 받지 않고 과태료 3,000만원을 납부하고 마는 경우도 늘고 있어 앞으로 기업의 인식변화와 정부 정책의 보완이 요구된다.

2-2 정보보안사고와 기업가치

우리나라의 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조에서는 침해사고를 “해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태”로 정의하고 있다.

보안사고와 관련한 초창기 연구들은 사건연구방법론을 통한 보안사고의 주가반응에 초점을 두었으며 대다수의 연구들에서 부정적인 영향을 미친다는 결과를 제시하였다[6], [24-26]. 뿐만 아니라 동일 산업 내의 다른 기업들의 주가에서도 부정적인 영향을 미치는 것으로 나타났다[27]. 최근의 연구에서는 보안사고에 따른 기업가치 하락에 대응하기 위한 연구가 활발히 진행되고 있다. 가장 최근의 연구로 [28]는 얘기치 않은 정보보안사고는 기업 명성에 악영향을 미쳐 단기뿐만 아니라 장기적으로도 기업가치를 하락시키지만, CSR(Corporate Social Responsibility) 점수가 높은 기업들에서 부정적인 영향이 낮게 나타남을 확인하였다. 따라서 CSR 투자 활동을 강화하는 것이 부정적인 충격에 대응하는 방안이라고 주장하였다. 논문[29]는 기존의 연구들과 마찬가지로 정보유출은 기업가치에 악영향을 미치는 연구결과를 보고하였으며, 특히 명성이 낮은 기업일수록 부정적 영향이 더 크다는 결과를 제시하였다. 또한 정보유출 이후 기업들의 대응전략 유형에 따른 효과를 분석한 결과 이미지쇄신과 완화전략 만이 기업 명성이 낮은 기업들에서 효과적임을 도출하였다. 따라서 기업의 명성은 보안사고로 발생하는 기업가치를 방어하는데 중요한 자산이라고 주장하였다. 그 외 침해 사고와 관련한 재무적 성과 측면의 연구에서는 침해 사고 직후 단기적으로는 재무적 성과에 영향을 미치지 않았지만 중장기적으로 수익성이 감소하는 것으로 나타났다[7].

국내의 연구에서도 침해 사고와 기업의 주가 반응에 관한 연구가 주류를 이루고 있으며 주가에 부정적인 영향을 미친다는 일관된 결론을 보고하고 있다. 논문[12]는 2003년부터 2013년까지 농협, 에스케이텔레콤, 다음 등 국내 11개 기업의 정보보안 사고 사례를 바탕으로 사건연구를 실시한 결과 보안사고 발생 하루 뒤의 주가에 직접적으로 부정적인 영향을 확인하였다. 논문[30]은 2000년부터 2015년까지 21건의 개인정보 유출사고가 발생한 상장기업을 대상으로 주가에 미치는 영향을 분석하여 개인정보 유출은 해당기업의 주가에 부정적인 영향을 미친다는 결론을 내렸으며, 투자 주체별 투자성과를 분석한 결과 외국인 및 기관투자자와는 달리 개인투자자는 순매도 매매 패턴을 보여 상대적으로 불리한 위치에 있음을 확인하였다. 논문[31]은 2011년부터 2014년까지 24개의 코스피, 코스닥 상장기업을 대상으로 한 연구에서 개인정보 유출사고 발생 시 IT서비스 및 소프트웨어와 관련한 정보보호 업체의 주가 상승을 근거로 침해사고는 관련 산업의 기업에게 까지 영향을 미친다고 주장하였다.

한편 일부 연구에서는 보안사고에 대한 주식시장의 차별적 반응에 대한 연구결과가 보고 되었다. 논문[11]은 2001년에서 2011년까지의 정보보안사고를 대상으로 조사한 결과 정보보안 사고의 발표는 전자상거래 기업에게만 장·단기간에 걸쳐 주가에 부정적인 영향을 미치는 것으로 나타났다. 논문[13]은 2005년부터 2014년까지 국내 보안사고 52건을 대상으로 사건연구를 실시하여 보안사고가 주가에 부정적인 영향을 미치는 결과를 확인하였다. 또한 기업가치를 나타내는 토빈의 큐(Tobin’s Q. 이하 토빈큐)[4]가 1보다 크거나 0보다

3) 정보통신망에서 개인정보보호 활동을 체계적이고 지속적으로 수행하기 위하여 필요한 관리적 · 기술적 · 물리적 보호조치를 포함한 종합적 관리체계 (정보통신망 이용촉진 및 정보보호 등에 관한 법률)

작은 기업에서 더 높은 평균기대손실이 발생하는 것을 평판 손실 때문이라고 주장하였다.

2-3 정보보호관리와 기업가치

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제42조에서는 정보보호(Information security)란 정당한 권한이 없는 자가 정보통신망에 접근·침입하는 것을 방지하거나 대응하고 정보의 불법 유출·변조·삭제 등을 방지하기 위한 기술적·물리적 보호조치 등으로 정의하고 있다. 국내에서는 정보보안이 정보유출, 징벌적 손해배상, 기업이미지 저하 등과 같이 기업의 안정성과 재무적 상태에 중대한 영향을 미칠 수 있기 때문에 2016년부터 정보보호 공시제도를 시행하고 있다. 이로써 정보보호는 기업에 대한 주주의 알권리 보장과 경영능력 요소로도 인정받기 시작하였다.

정보보안에 관련된 연구로 논문[32]는 대리인문제는 경영자의 재임기간동안 지나친 IT보안투자를 유발하기 때문에 장기적으로 기업의 재무구조를 약화시키는 부정적 결과를 가져온다고 주장하였다. 논문[33]은 영국, 미국, 독일과 스페인 기업들을 대상으로 ISO 27001(정보보안경영체계)인증이 기업의 주가에 미치는 영향을 사건연구를 통해 분석한 결과 의미 있는 영향을 발견하지 못하였다. 따라서 정보보호관리는 기업의 경쟁력 높이는 요소가 아닌 의무라고 주장하였다. 그러나 논문[34]는 118개의 사례를 대상으로 IT 보안에 대한 투자를 상업적 목적과 순수 보안 개선목적으로 분류하여 주가에 미치는 영향을 분석한 결과 선재적인 IT 보안투자는 상업적 이용이 목적일 때 더 높은 주가상승을 확인하였다. 또한 보안침해에 대한 대응으로써 보안투자는 순수 IT 보안개선을 목적으로 할 때 더 높은 주가상승결과를 가져왔다.

국내의 경우 논문[10]은 2001년부터 2005년 사이에 발생한 59건의 정보보안사고와 정보보안 투자 발표가 기업의 가치에 미치는 영향을 사건연구를 통해 분석하였다. 분석결과 정보보안사고는 주가에 부정적인 영향을 미치는 결과를 확인하였으나 정보보안 투자가 주가 미치는 영향을 발견할 수 없었다. 그러나 논문[18]은 한국과 미국의 금융기관을 대상으로 총 2,000개의 설문을 통해 한국금융기관에서 보안대책이 금융IT보안책임을 증가시키고, 금융IT 보안위험을 감소시켜 궁극적으로 기업성과에 긍정적인 영향을 미치는 것을 확인하였다. 반면에 미국의 경우 보안대책이 금융IT 보안책임증가에 유의한 영향을 주지는 않지만, 금융IT 보안위험감소에는 긍정적인 영향을 미쳐 기업성과를 높이는 것으로 나타났다. 논문[20]은 2009년부터 2013년까지 총 125개의 중소 · 중견기업을 대상으로 설문을 통해 수집한 400개의 표본을 바탕으로 기업의 보안투자는 단기적으로 기업의 매출에 부정적인 영향을 미치지만 장기적으로는 긍정적인 영향을 미친다는 결과를 보고하였다. 논문[19]는 정보통신기업을 대상으로 실시한 315개의 설문조사 표본을 분석한 결과 개인정보보호 이행이 균형성과지표(Balanced Scorecard)의 재무, 고객, 업무, 지속성장 관점의 기업 성과에 긍정적인 영향을 미친다고 주장하였다. 정보보호관리와 관련한 인증 측면에서는 논문[17]은 정보보호관리체계 인증을 취득함으로써 기업 이미지 제고와 홍보효과로 인해 매출액 증가와 침해사고 예방에 따른 비용절감 효과가 있다고 주장하였다. 논문[21]은 2002년부터 2015까지의 90개 표본을 대상으로 사건연구를 통해 기업의 정보보안인증 취득 관련한 언론보도가 기업의 주가에 단기적으로 긍정적인 영향을 미치고 있음을 확인하였다.

2-4 가설설정: 정보보호관리와 기업가치

이 절은 침해사고가 야기하는 법률 리스크(Legal risk), 정부의 규제와 감시가 강화되는 제도 리스크(Regulatory risk), 그리고 기업 이미지에 타격을 주는 평판 리스크(Reputational risk)[15]에 대한 선재적 대응의 하나로써 ISMS 인증 취득이 기업가치 및 영업성과에 어떠한 영향을 주는지를 분석하는데 필요한 가설을 설정한다.

다수의 선행연구들은 정보침해 사고는 즉시, 직접적으로 시장에서 기업가치에 부정적인 영향을 미친다는 실증 분석 근거를 제시하고 있다[9, 10, 11], [13], [27-29]. 따라서 정보보호관리활동은 기업의 잠재적 보안 리스크를 줄일 뿐만 아니라[34] 비용절감과 매출액 증가 [17], [20]와 공공부문 사업자 선정 시 가산점 부여 등을 통해 기업의 영업성과를 높일 수 있을 것으로 예상된다. 또한 한국지배구조원에서 상장기업을 대상으로 한 지배구조, 사회책임경영, 환경경영의 수준(ESG) 평가에 반영하는 등의 다양한 정책적 혜택들을 고려해 볼 때 기업가치에 긍정적인 효과를 기대해 볼 수 있다. 이러한 논리를 바탕으로 다음과 같은 가설1과 가설2를 설정한다.

가설 1. 기업의 정보보호관리 활동은 기업의 영업성과를 높이는데 기여한다.

가설 2. 기업의 정보보호관리 활동은 기업가치를 높이는데 기여한다.

III 선행연구 및 가설설정

3-1 표본선정 및 자료수집

본 연구의 자료는 다음의 기준을 만족하는 기업을 표본으로 선정 하였다.

4) Tobin(1969)이 제시한 기업가치를 측정하는 척도로 재무제표 상의 회계자료와 시장가치를 결합한 식(시장가치 / 총자산가치의 대체비용)으로 나타낸다. 따라서 기업의 무형자산, 시장지배력, 상표권, 성장잠재력 등 가치 추정치를 제시한다.

표 1. 변수의 정의 및 측정
Table 1. Variable definition and measurement

Variable name	Code	Expected signs	Measurement method
Tobin's Q	TOBINQ		(Market value of common stock + Book value of preference stock and debt) / Book value of total asset
Return on asset	ROA	+	Net-income$_t$ / Total assets$_{t-1}$
ISMS certification	ISMS	+	1 if companies is ISMS certified, else 0
Debt ratio	LEV	+/-	Total debt$_t$ / Total equity$_t$
Growth rate	GRW	+	(Sales$_t$ - Sales$_{t-1}$) / Sales$_{t-1}$
Foreign ownership	FORE	+	Proportion of foreign stockholder ownership
Firm age	AGE	-	The number of years(plus one) since the company was legally founded
Firm size	SIZE	-	Natural logarithm of the total assets
Year	YEAR	·	1 if year is, else 0
Industry	IND	·	1 if industry is, else 0

1) 2013년부터 2017년까지 유가증권시장에 상장된 비금융 기업

2) 2013년부터 2017년까지 한국 인터넷 진흥원으로부터 ISMS 인증을 취득 또는 유지하는 기업

3) 한국신용정보주식회사의 KIS-VALUE를 통해 재무제표 자료수집이 가능한 기업

표본은 2013년부터 2017년 사이 금융업종을 제외한 한국 상장기업이다. 금융업종은 업무의 특수성으로 인해서 상장법인 등의 회계처리에 관한 규정 제7조에 따라 이자 및 배당금 수익이 영업수익으로 구분되고 매출총손익을 구분하지 않는 등 일반 기업과 회계기준 및 재무제표 등에서 차이가 있기 때문에 제외하였다. 그리고 회귀모형에 포함된 모든 변수의 극단치 영향을 통제하면서 표본 손실을 최소화하기 위해 논문[35]가 제시한 상하위 1%의 값 조정(Winsorizing)을 실시하였다. 재무제표 결측치가 존재하는 기업을 제외하고 총 3,003개 표본의 패널 자료를 구축하였다. 이들 중 92개는 ISMS인증 취득 또는 유지하는 기업의 표본에 해당한다.

3-2 변수의 조작적 정의 및 측정

종속변수: 기업가치는 토빈큐(Tobin'Q)를 이용하여 측정한다. 자산의 대체원가 대비 시장가치를 나타내는 비율로서 무형자산 비중이 높은 IT기업의 기업가치를 나타내는데 적합한 측정방법이다[36]. 일반적으로 토빈큐의 값이 클수록 기업가치가 높게 평가되는 것으로 해석할 수 있다. 또 다른 종속변수인 기업의 영업성과 대용치는 당기순이익을 총자산으로 나눈 비율인 자산순이익률(ROA)을 사용한다[37].

관심변수: 기업의 정보보호관리를 나타내는 대용치로는 ISMS인증의 취득 또는 유지 여부로 측정한다. 2013년부터 정보통신망법에 따라 ISMS인증제도가 의무화되었다. 그에 따라 ISMS 인증 취득 기업은 급격히 증가하고 있다.

통제변수: 두 모형의 통제변수로는 공통적으로 기업의 특성을 나타내는 부채비율(LEV), 매출액성장율(GRW), 외국인지분율(FORE), 기업업력(AGE), 연도더미(YEAR), 산업더미(IND)를 선정하였다. 그리고 기업가치의 대용치인 토빈큐(TOBINQ)를 종속변수로 설정한 가설 2의 모형에 기업의 수익성을 나타내는 통제변수로써 자산순이익률(ROA)을 포함시켰다.

부채비율(LEV)은 자본조달순위이론[38]에 따르면 기업은 외부에서 자본을 조달하기보다는 기업 내부의 자본 사용을 선호하기 때문에 기업가치와 음(-)의 관계가 예상되지만, 신호이론[39]에 의하면 기업의 부채발행은 채권자들에게 투자에 대한 긍정적인 신호로 해석될 수 있어 기업가치와 양(+)의 관계 또한 예상되었다. 자산순이익률(ROA)과 매출액성장율(GRW)은 기업의 미래성장 가능성을 나타내기 때문에 기업가치와 양(+)의 관계가 예상하였다[40]. 외국인지분율(FORE)은 경영투명성을 나타내는 지표로써 기업가치를 높일 수 있어 기업가치와 양(+)의 관계가 예상하였다[41]. 기업업력(AGE)은 기업의 수명주기에 따라 수익성 및 가치 관련성이 차별적으로 작용할 수 있고[42], 기업의 나이와 성장 간에는 음(-)의 관계를 보인다는 연구결과[43]를 바탕으로 기업가치와 음(-)의 관계가 예상되었다. 기업규모(SIZE)의 증가에 따른 대리인 문제와 정보불균형은 비용을 증가시키는 요인으로 작용하기 때문에 기업가치와 음(-)의 관계가 예상되었다 [44]. 마지막으로 산업간 차이를 통제하기 위해 한국표준산업분류[5] 중분류를 따르는 산업더미(IND)와 연도에 따른 경기변동영향을 통제하기 위해 연도더미(YEAR)를 모형에 포함하였다.

3-3 연구모형의 설정

본 연구는 기업의 정보보호관리 활동이 기업가치 및 영업성과에 영향을 미치는지를 분석하기 위해 패널자료를 바탕으로 통합회귀분석을 실시하였다. 식(1)은 영업성과(ROA)를 종속변수로 설정한 회귀모형이고, 식(2)는 기업가치(TOBINQ)를

5) 생산단위(사업체단위, 기업체단위 등)가 주로 수행하는 산업 활동을 그 유사성에 따라 체계적으로 유형화 한 분류체계로서 순차적으로 대분류, 중분류, 소분류, 세분류, 세세분류 단계 항목으로 구분된다. (통계청)

표 2. 기초통계량 및 차이검증(T-test)
Table 2. Descriptive statistics and difference test(T-test)

Dependent variable	Total sample (N=3,003)					ISMS certified firms (N=89)	Non-ISMS certified firms (N=2,914)	Difference	T-statistic
	Mean	Median	Max	Min	Std. dev	Mean			
TOBINQ	1.283	1.017	5.717	0.440	0.882	1.854	1.266	0.589	3.893***
ROA	0.015	0.024	0.233	−0.420	0.085	0.057	0.014	0.043	7.990***
ISMS	0.030	0.000	1.000	0.000	0.170	-	-	-	-
GRW	0.034	0.012	1.487	−0.655	0.258	0.085	0.032	0.053	2.196**
FORE	0.094	0.041	0.650	0.000	0.126	0.271	0.089	0.182	9.675***
LEV	1.051	0.665	9.233	0.002	1.358	1.037	1.051	−0.014	−0.093
SIZE	11.620	11.519	13.420	10.385	0.629	12.409	11.596	0.813	12.305***
AGE	39.287	41.000	84.000	3.000	18.099	31.865	39.513	−7.648	−3.936***

1) *, ** and *** denotes significance at the 10%, 5% and 1% levels, respectively.
2) TOBINQ=Tobin's Q, ROA=return on asset, ISMS=ISMS certification, GRW=sales growth ratio, LEV=debt ratio, FORE=foreign stockholder ownership, SIZE=firm size. AGE=firm age.

종속변수로 하는 회귀모형이다.

$$ROA_{i,t} = \beta_0 + \beta_1 ISMS_{i,t} + \beta_2 LEV_{i,t} + \beta_3 GRW_{i,t} + \beta_4 FORE_{i,t} + \beta_5 AGE_{i,t} + \beta_6 SIZE_{i,t} + \sum YEAR + \sum IND + \varepsilon_{i,t} \quad (1)$$

$$TOBINQ_{i,t} = \beta_0 + \beta_1 ISMS_{i,t} + \beta_2 ROA_{i,t} + \beta_3 LEV_{i,t} + \beta_4 GRW_{i,t} + \beta_5 FORE_{i,t} + \beta_6 AGE_{i,t} + \beta_7 SIZE_{i,t} + \sum YEAR + \sum IND + \varepsilon_{i,t} \quad (2)$$

Ⅳ. 실증분석 결과

4-1 기초통계량 및 평균비교(T-test) 분석

표 2는 주요변수들의 기술통계량과 관심변수인 정보보호관리체계(ISMS)의 인증 취득 기업과 일반 기업 간의 평균의 차이를 분석한 T-test 결과를 보여주고 있다. 종속변수인 기업가치(TOBINQ)와 영업성과(ROA)는 정보보호관리체계(ISMS)인증 취득 기업의 평균이 일반 기업에 비해 유의수준 1%에서 각각 0.589와 0.043 만큼 높게 나타나 본 연구의 가설을 지지하는 결과를 보여준다. 그 외 변수들로는 성장률(GRW), 외국인지분율(FORE)과 기업규모(SIZE)는 정보보호인증 취득 기업에서 통계적으로 유의하게 높은 결과를 보였다. 또한 기업업력(AGE)은 정보보호인증 취득 기업의 평균(31.865)이 비인증기업의 평균(39.513)에 비해 7.648만큼 유의수준 1% 수준에서 낮게 나타났다. 다시 말해서 정보보호인증을 취득한 기업의 기업가치와 성장성은 높고 기업규모(SIZE)가 큰 반면에 기업업력(AGE)은 짧은 것으로 나타났다.

4-2 Pearson 상관관계분석

표 3은 분석에 사용된 주요 변수들 간의 방향성과 강도를 보여주는 상관계수 값을 표시하고 있다. 본 연구의 종속변수인 토빈큐(TOBINQ)와 영업성과(ROA)는 관심변수인 정보보호인증(ISMS)변수와 양(+)의 상관관계를 나타낸다. 따라서 본 연구의 가설과 일치하는 결과를 보여준다. 또한 종속변수

표 3. 상관관계 분석
Table 3. Correlation analysis

	TOBINQ	ROA	ISMS	GRW	LEV	FORE	SIZE
ROA	0.141***						
	(7.809)						
ISMS	0.113***	0.086***					
	(6.242)	(4.756)					
GRW	0.150***	0.173***	0.035*				
	(8.304)	(9.629)	(1.903)				
LEV	−0.082***	−0.284***	−0.002	−0.041**			
	(−4.482)	(−16.203)	(−0.093)	(−2.224)			
FORE	0.168***	0.241***	0.244***	0.012	−0.140***		
	(9.311)	(13.589)	(13.804)	(0.673)	(−7.742)		
SIZE	−0.073***	0.135***	0.219***	−0.044**	0.141***	0.462***	
	(−4.013)	(7.463)	(12.305)	(−2.409)	(7.774)	28.543	
AGE	−0.112***	−0.030	−0.072***	−0.032*	−0.038**	−0.039**	0.034*
	(−6.177)	(−1.636)	(−3.936)	(−1.743)	(−2.085)	(−2.155)	(1.860)

1) *, ** and *** denotes significance at the 10%, 5% and 1% levels, respectively.
2) TOBINQ=Tobin's Q, ROA=return on asset, ISMS=ISMS certification, GRW=sales growth ratio, LEV=debt ratio, FORE=foreign stockholder ownership, SIZE=firm size. AGE=firm age.
3) t-statistics in parentheses.

들 모두 매출액성장율(GRW), 외국인지분율(FORE)과도 양(+)의 상관성을 보인 반면에 부채비율(LEV) 음(-)의 상관관계를 보여준다. 그러나 기업규모(SIZE)는 토빈큐(TOBINQ)와 음(-)의 상관관계를, 영업성과와는 양(+)의 상관성을 나타내 서로 다른 결과를 보여 주었다. 이는 기업의 규모는 규모의 경제와 우월적 시장 지위로 수익성에 긍정적인 영향을 미치지만 투자자들에게는 상대적으로 저평가 받을 수 있음을 시사한다. 기업업력(AGE)은 토빈큐(TOBINQ)에서만 통계적으로 유의한 음(-)의 상관계수(-0.112)값을 나타내 선행연구를 지지하는 결과를 보였다.

4-3 다중회귀분석

표 4의 패널A는 가설1(기업의 정보보호관리 활동은 기업의 영업성과를 높이는데 기여한다)을 검정하기 위한 통합회귀분석 결과를 보여준다. 관심변수인 정보보안인증(ISMS)은 모든 모형에서 유의수준 1% 내의 양(+)의 회귀계수 값(0.056, 0.034)을 나타내 가설1을 지지하는 결과를 보여준다. 따라서 정보보호관리 활동은 기업의 영업성과에 긍정적인 영향을 미치는 것을 확인할 수 있다. 주요통제변수들은 모두 통계적으로 유의한 회귀계수 값을 가지며 부채비율(LEV)과 기업업력(AGE)은 음의 회귀계수 값을 나타낸다. 두 회귀모형 모두에서 F값은 1% 이내에서 통계적으로 유의하기 때문에 모형은 적합하다고 할 수 있다.

표 4의 패널B는 가설2(기업의 정보보호관리 활동은 기업가치를 높이는데 기여한다)를 검정하기 위한 통합회귀분석 결과를 제시한다. 모형1과 모형2로 나누어 분석하는 이유는 주요 통제변수를 제외할 때와 모두 포함시켰을 때 주요변수의 통계분석결과의 일관성을 살펴보기 위함이다. 관심변수인 정보보안인증(ISMS)은 통제변수를 제외할 때(모형1)와 모두 포함할 때 (모형2)각각 유의수준 1%와 10% 수준에서 통계적으로 유의한 양(+)의 회귀계수 값(0.280, 0.171)을 나타냈다. 따라서 본 연구의 가설1을 지지하는 결과를 보여주었다. 주요 통제변수들은 유의한 회귀계수 값을 나타내고 있으며 기업업력(AGE)과 기업규모(SIZE)만 음(-)의 회귀계수 값(-0.005, -0.219)을 나타냈다. 이 결과는 기업수명주기 이론과 대리인 이론을 지지하는 결과로서 기업의 성장율은 성장기와 성숙기를 거쳐 점차 둔화되고 기업규모가 커짐에 따라 정보비대칭의 수준이 높아져 기업가치에 부정적인 영향을 미치게 됨을 시사한다. 두 회귀모형 모두에서 F값은 1% 이내에서 통계적으로 유의하기 때문에 모형은 적합하다고 할 수 있다.

Ⅴ. 결 론

본 연구는 2013년부터 2017년까지 코스피 상장기업을 대상으로 정보보호관리 활동의 하나인 ISMS인증 취득이 기업의 영업성과와 기업가치에 어떠한 영향을 미치는가에 대한 연구를 하였다. 관련 선행연구에서는 침해사고에 대한 기업의 피해 정도를 추정하거나 정보보안관리가 기업에게 미치는 영향을 정성적 분석방법을 통해 접근하였다.

본 연구의 실증분석 결과, 정보보호관리 활동은 기업의 영업성과와 기업가치에 모두 긍정적인 영향을 미치는 것으로 나타났다. 이러한 분석결과는 침해사고 뿐만 아니라 침해사고에 대응하는 정보보호관리가 기업의 경영성과와 기업가치에 직접적으로 영향을 미칠 수 있음을 시사한다. 따라서 기업가

표 4. 횡단면 회귀분석
Table 4. Cross-sectional regression analysis

Panel A
(Dependent variable: sales profit)

$ROA_{i,t} = \beta_0 + \beta_1 ISMS_{i,t} + \beta_2 LEV_{i,t} + \beta_3 GRW_{i,t} + \beta_4 FORE_{i,t} + \beta_5 AGE_{i,t} + \beta_6 SIZE_{i,t} + \sum YEAR + \sum IND + \varepsilon_{i,t}$

	Model 1		Model 2	
Dependent variable	Coefficient	t-statistic	Coefficient	t-statistic
Intercept	0.009	0.481	-0.133	-3.658***
ISMS	0.056	5.678***	0.034	3.576***
LEV			-0.017	-14.195***
GRW			0.056	10.279***
FORE			0.094	6.764***
AGE			0.000	-1.863*
SIZE			0.014	5.058***
IND	Included			
YEAR	Included			
Adjusted R^2	0.086		0.211	
F-statistic	6.234		14.611	

Panel B
(Dependent variable: firm value)

$TOBINQ_{i,t} = \beta_0 + \beta_1 ISMS_{i,t} + \beta_2 ROA_{i,t} + \beta_3 LEV_{i,t} + \beta_4 GRW_{i,t} + \beta_5 FORE_{i,t} + \beta_6 AGE_{i,t} + \beta_7 SIZE_{i,t} + \sum YEAR + \sum IND + \varepsilon_{i,t}$

	Model 1		Model 2	
Dependent variable	Coefficient	t-statistic	Coefficient	t-statistic
Intercept	0.927	5.074***	3.577	9.477***
ISMS	0.280	2.825***	0.171	1.745*
ROA			1.266	6.620***
LEV			0.037	2.910***
GRW			0.295	5.143***
FORE			1.109	7.634***
AGE			-0.005	-5.295***
SIZE			-0.219	-7.511***
IND	Included			
YEAR	Included			
Adjusted R^2	0.165		0.220	
F-statistic	11.980		15.071	

1) *, ** and *** denotes significance at the 10%, 5% and 1% levels, respectively.
2) TOBINQ=Tobin's Q, ROA=return on asset, ISMS=ISMS certification, GRW=sales growth ratio, LEV=debt ratio, FORE=foreign stockholder ownership, SIZE=firm size. AGE=firm age.

치에 대한 정보보호관리 활동의 긍정적 결과를 주장한 기존의 정성적 연구결과들을 지지하며 기업이 정보보호관리를 적극적으로 고려해야 하는 실증적 근거를 제시하였다. 그리고 투자자와 금융기관에게는 리스크관리 측면에서 의사결정에 필요한 객관적 자료를 제공하였다. 정부에게는 기업의 정보보호관리 활동의 중요성을 적극적으로 홍보하고 장려하는 한편, 지속적인 모니터링을 통해 기업이 인증을 받지 않을 경우, 1회의 과태료 부과가 아닌 주기적인 과태료 납부(분기별, 반기별 또는 매년) 체계로 전환하는 등의 제도의 개선방향을 수립하는데 정책적 시사점을 제공할 것으로 기대된다.

본 연구의 한계점은 재무정보의 신뢰성을 고려하여 비상장기업과 코스닥 기업은 제외하였기 때문에 실질적으로 많은 표본들이 제외 되었다. 이로 인해 발생할 수 있는 표본 편향(Sampling bias) 문제와 OLS모형이 갖는 내생성(Endogeneity) 문제를 안고 있다. 또한 비교적 짧은 5년 간의 자료를 활용한 점은 본 연구의 한계점이며, 지속적으로 자료를 축적하여 차후 연구를 진행해야 할 것이다. 그럼에도 불구하고 본 연구는 재무적 관점에서 정보보호관리가 기업에게 미치는 영향을 연구한 국내 최초의 정량적 연구라는데 공헌점이 있다.

IT 침해사고는 사고 발생 시 규모가 크고 불가역적이며, 기업에게 심각한 재정적 위험, 그리고 기업의 명성에 치명적인 피해를 초래한다. 또한 4차 산업혁명 시대에 들어서면서 세계적으로 각국 정부들의 규제가 강화되는 추세에 있다. 그럼에도 재무적 관점에서 정보보안과 관련한 연구는 여전히 초기단계에 머물러 있다. 향후 연구에서는 보다 실증적으로 정보보호인증취득이 기업성과에 미치는 인과관계를 규명하기 위해 구조방정식(Structural Equation Modeling) 모형을 사용할 필요가 있다. 또한 투자자, 채권자, 금융기관, 정부와 같은 기업의 다양한 이해관계자에게 침해사고나 정보보호관리가 어떠한 영향을 미치는 지에 대한 연구가 필요하다. 앞으로 관련 연구들이 활발히 수행되기를 기대한다.

참고문헌

[1] Government of the Republic of Korea, 2017 National Informatization White Paper, National Information Society Agency.

[2] 2017 Ransomware data breach Investigations Report , Ransomware Computer Emergency Response Team Coordination Center.

[3] H. J. Moon and H. S. Cho, “Risk based policy at big data era: Case study of privacy invasion,” Information Policy, Vol.19, No.4, 2012.

[4] The Guardian, 2017 Cyber attack: hackers 'weaponised' everyday devices with malware.

[5] L. A. Gordon, M. P. Loeb & L. Zhou, “The impact of information security breaches: Has there been a downward shift in costs?,” *Journal of Computer Security*, Vol. 19, No. 1, pp.33-56, 2011.

[6] H. Cavusoglu, B. Mishra, and S. Raghunathan, “The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers,” *International Journal of Electronic Commerce*, Vol. 9, No.1, pp. 70-104, 2004

[7] M. Ko, K. M. Osei-Bryson and C. Dorantes, “Investigating the impact of publicly announced information security breaches on three performance indicators of the breached firms,” *Information Resources Management Journal*, Vol. 22, No. 2, pp.1, 2009

[8] R. Telang and S. Wattal, “Impact of software vulnerability announcements on the market value of software vendors-an empirical investigation,” 2005.

[9] J. Y. Kim, “Analyzing Effects on Firms’ Market Value of Personal Information Security Breaches,” *The Journal of Internet Electronic Commerce Research*, Vol. 18, pp.1-12, 2013.

[10] Y. O. Kwon and B. D. Kim, “The Effect of Information Security Breach and Security Investment Announcement on the Market Value of Korean Firms,” *Information Systems Review* ,Vol. 9, pp.105-120, 2007.

[11] A. Hovav and J. Han, “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.

[12] I. Y. Hong, J. H. Lee and S. M. Kang, “The Effect of Official Announcement about Information Security Breach on Corporate Stock Value in the Market,” *Entrue Journal of Information Technology*, Vol. 14, pp.33-56, 2015.

[13] H. H. Hwang and H. S. Lee “The relationship between security incidents and value of companies: Case of listed companies in Korea,” *Journal of the Korea Institute of Information Security and Cryptology*, Vol. 25, No.3, pp. 649-664, 2015.

[14] A. A. Yayla and Q. Hu, “The impact of information security events on the stock value of firms: The effect of contingency factors,” *Journal of Information Technology*, Vol. 26, No.1, pp. 60-77, 2011.

[15] R. Sen and S. Borle. “Estimating the contextual risk of data breach: An empirical approach,” *Journal of Management Information Systems*, Vol. 32, No. 2, pp. 314-341, 2015.

[16] The Guardian(2018). Facebook faces $1.6bn fine and formal investigation over massive data breach. Available: https://www.theguardian.com/technology/2018/oct/03/facebook-data-breach-latest-fine-investigation.

[17] Y. S. Bae, “A study of effect of information security management system [ISMS] certification on organization performance,” *Journal of the Korea Academia-Industrial cooperation Society*, Vol. 13, No. 9 , pp. 4224-4233, 2012.

[18] K. A. Kim, S. H. Kim and K. J. Park.. “The Study on Financial Firm's Performance Resulting from Security Countermeasures and the Moderating Effect of Transformational Leadership,” *Journal of the Korean Operations Research and Management*

Science Society, Vol. 38, No.4, pp. 95-112, 2013.

[19] C. S. Moon and S. H. Kim, "An Empirical Study on the Impact of Enterprise's Performance on Personal Information Protection Execution," *Journal of Korean Institute of Information Technology*, Vol. 14, No.3, pp. 97-106, 2016.

[20] K. B. Lee, T. H. Kim and S. Y. Lee, *"A Study on the Influence of Security Investment on Firm's Performance,"* The Korea Society of Management information Systems, pp. 354-359, August 2015.

[21] J. Y. Park, W. J. Jung and B. S. Kim, "The Effect of Information Security Certification Announcement on the Market Value of Firms," *Journal of Information Technology Services*, Vol. 15, No. 3, pp. 51-69, 2016.

[22] D. H. Shin, "Home and foreign Security accident case involved the FinTech," Communications of the Korean Institute of Information Scientists and Engineers, Vol. 34 No. 4, pp. 25-28, 2016.

[23] Korea Internet & Security Agency, Available : https://isms.kisa.or.kr/main/isms/intro/

[24] M. Ettredge and V. J. Richardson. "Assessing the risk in e-commerce," *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*. IEEE, 2002.

[25] K. M. Gatzlaff and K. A. McCullough. "The effect of data breaches on shareholder wealth," *Risk Management and Insurance Review*, Vol. 13, No. 1, pp. 61-83. 2010.

[26] J. Cardenas, A. Coronado, A, Donald, F. Parra and M. A. Mahmood, "The economic impact of security breaches on publicly traded corporations: An empirical investigation," *Eighteenth Americas Conference on Information Systems*, August 2012.

[27] O. Hinz, M. Nofer, D. Schiereck and J. Trillig, "The influence of data theft on the share prices and systematic risk of consumer electronics companies," *Information & Management*, Vol. 52, No. 3, pp. 337-347, 2015.

[28] P. Akey, S. Lewellen and I. Liskovich. "Hacking corporate reputations," *SSRN Electronic Journal,* 2018.

[29] K. L. Gwebu, J. Wang and L. Wang, "The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management," *Journal of Management Information Systems*, Vol. 35, No. 2, pp. 683-714, 2018

[30] J. H. Eom and M. J. Kim, "Effect of Information Security Incident on Outcome of Investment by Type of Investors: Case of Personal Information Leakage Incident," *Journal of the Korea Institute of Information Security and Cryptology*, Vol. 26, No. 2, pp. 463-474, 2016.

[31] M. J. Kim, N. Heo and J. Yoo, "A Study on the Stock Price Fluctuation of Information Security Companies in Personal Information Leakage," *Journal of the Korea Institute of Information Security and Cryptology*, Vol. 26, No.1, pp. 275-283, 2016.

[32] B. Srinidhi, J. Yan and G. K. Tayi, "Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors," Decision Support Systems, Vol. 75, pp. 49-62, 2015.

[33] C. Hsu, T. Wang and A. Lu,, "The Impact of ISO 27001 Certification on Firm Performance," *In System Sciences (HICSS), 2016 49th Hawaii International Conference* pp. 4842-4848. IEEE, January 2016.

[34] F. Xu, X. R. Luo, H. Zhang, S. Liu and W. W. Huang, "Do Strategy and Timing in IT Security Investments Matter? An Empirical Investigation of the Alignment Effect," Information Systems Frontiers, pp. 1-15, 2017.

[35] D. Kennedy, J. Lakonishok and W. Shaw, "Accomodating outliers and nonlinearity in decision models." *Journal of Accounting, Auditing and Finance* Vol. 7, No. 2, pp. 161–190, 1992.

[36] A. S. Bharadwaj, S. G. Bharadwaj and B. R. Konsynski, " Information technology effects on firm performance as measured by Tobin's q," *Management science*, Vol. 45. No. 7, pp. 1008-1024. 1999.

[37] K. C. Chen, and C. J. Lee, "Accounting measures of business performance and Tobin's q theory," *Journal of Accounting, Auditing & Finance*, Vol. 10, No. 3, pp. 587-609, 1995.

[38] S. C. Myers and N. S. Majluf, "Corporate financing and investment decisions when firms have information that investors do not have," *Journal of financial economics*, Vol. 13, No. 2, pp. 187-221, 1984.

[39] S. A. Ross, "The determination of financial structure: the incentive-signalling approach," *The bell journal of economics*, pp. 23-40, 1977.

[40] R. Morck, A. Shleifer and R. W. Vishny, "Management ownership and market valuation: An empirical analysis. Journal of financial economics," Vol. 20, pp. 293-315, 1988.

[41] H. J. Park H. H. Shin and W. S. Choi, "The Korean Firms` Agency Costs and Firm Value: Role of Foreign Investors` Equity Ownership," *Korean Management Review*, vol. 33, pp.655-682, 2004.

[42] S. Y. Kwon and B. Y. Moon "Decomposed Return on Equity, Future Profitability, and Value Relevance over the Firm Life Cycle," *Korean Management Review*, vol. 38, pp. 1213-1249, 2009.

[43] B. Jovanovic, "Selection and the Evolution of Industry," *Econometrica: Journal of the Econometric Society*, pp. 649-670, 1982.

[44] P. G. Berger and E. Ofek, " Diversification's effect on firm value," *Journal of financial economics*, Vol. 37, No. 1, pp. 39-65, 1995.

최동권(Dong-Kwon Choi)

2017년 2월: 전남대학교 대학원 경영학과 (경영학석사)
2017년 3월 ~ 현재: 전남대학교 일반대학원 경영학과 박사과정

※관심분야 : 기업재무, 기업의 사회적 책임(CSR) 등

윤현식(Hyun Shik Yoon)

2009년: University of Missouri(Columbia) (공학석사)
2015년: University of Missouri(Columbia) (공학박사-경영정보시스템)

2010년~2011년: University of Texas(San Antonio) 강사
2015년~2016년: University of Missouri(Columbia) 겸임교수
2016년~2017년: Oklahoma State University(Stillwater) 교수
2017년~현 재: 전남대학교 경영대학 경영학부 조교수
※관심분야: 정보보호, 머신러닝기반 소비자행태분석, IT adoption