한국경영과학회지
제38권 제4호
2013년 12월
http://dx.doi.org/10.7737/JKORMS.2013.38.4.095

금융기업의 보안대책이 금융 IT 보안책임과 위험감소 그리고 기업성과에 미치는 영향 : 변혁적 리더십의 조절효과

김근아[1] · 김상현[1†] · 박근재[2]
[1]경북대학교 경영학부, [2]오레곤대학교 란드퀘스트 경영대학

The Study on Financial Firm's Performance Resulting from Security Countermeasures and the Moderating Effect of Transformational Leadership

Geuna Kim[1] · Sanghyun Kim[1] · Keunjae Park[2]
[1]School of Business Administration, Kyungpook National University
[2]Lundquist College of Business, University of Oregon

■ Abstract ■

Information system (IS) security continues to present a challenge for firms. Especially, IT security accident is recently taking place successively in the financial sector. Thus, a comprehensive measure on this is demanded. A large part of a research on security relies upon technical design in nature and is restrictive in a consideration of person and organizational issue. To achieve a goal of firm security, it is possible with an effort of organizational management and supervision for maintaining the technical and procedural status. Based on a theory of accountability, we propose that the security countermeasures of organization lead to an increase in accountability and reduction in risk of IT security in a financial firm and further to firm performance like promotion in firm reliability. In addition, we investigate which difference a theoretical model shows by comparison between South Korean and American financial firms. As a result of analysis, it found that South Korea and America have significant difference, but that a measure on the financing IT security is important for both countries. We aim to enhance interpretability of a research on security by comparatively analysis between countries and conducting a study focus on specific firm called financial business. Our study suggest new theoretical framework to a research of security and provide guideline on design of security to financial firm.

Keyword : Financial Firm, Firm Performance, Accountability, Security Countermeasures, Transformational Leadership, Cross-National Research

논문접수일 : 2013년 09월 29일 논문게재확정일 : 2013년 12월 09일
논문수정일(1차 : 2013년 11월 30일)
† 교신저자 ksh@knu.ac.kr

1. 서 론

정보기술(Information Technology : IT) 보안의 지속적인 문제는 악의적인 내부자의 위협, 사소한 실수 및 무의식적 행동, 혹은 정보자원 접근 위임에 있어서의 조직 구성원에 대한 신뢰의 남용으로부터 비롯된다[37]. 특히, 외부 공격자에 비해 조직 내부자는 꽤 높은 수준의 지식, 자원, 그리고 접근성을 보유하고 있는데, 모두가 상당한 조직 위험을 나타낸다고 할 수 있다[26] 일반적으로 내부자의 위협은 그들이 조직의 방침에 반하는 방법으로 민감하거나 중요한 정보에 접근하는 것으로부터 발생된다[39]. 이러한 보안 사고는 그들 자신에게 심각한 사안일 뿐 아니라 크게는 피해사례로 인한 민사소송, 규제 제재조치, 그리고 홍보 손상과 같은 것에 노출된다[39]. 더욱이 내부 보안 약화는 외부의 침해에도 안전할 수 없다. 기업의 보안 실패는 외적요인보다 내적요인에 따른 발생빈도가 높게 나타나고 이는 관리, 감시의 부족 때문인 것으로 평가되고 있다[35].

특히, 최근 금융 산업의 IT 환경은 인터넷과 모바일 뱅킹 등의 전자금융거래가 급격하게 증가하면서 각종 개인정보 유출, 해킹과 같은 보안위협이 끊이지 않는 등, 보안 문제는 일상적인 일이 되어가고 있다[36]. 금융기관들이 경쟁우위 확보의 한 방안으로 IT 사용을 늘려가고 있지만 이로 발생되는 보안사고 및 피해의 역기능 또한 증대되고 있는 것이 현실이다[16]. 이와 같은 금융기관의 보안 목표 달성을 위해서는 보안통제 영역을 구분하고 금융 IT의 지속가능한 우수한 보안 솔루션을 만들어 기업의 보안인식 수준을 향상시킴으로써 가능하다[36].

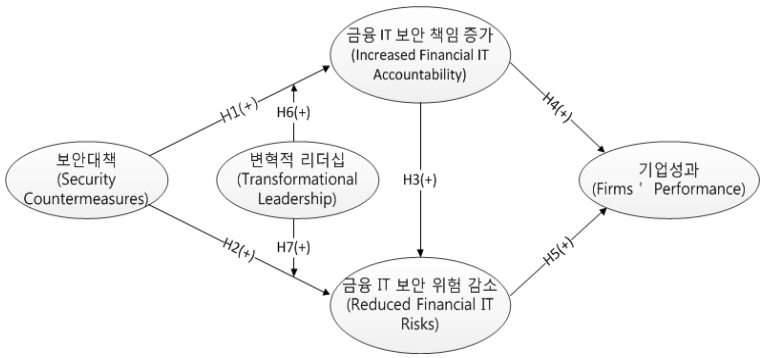
하나의 기대할 수 있는 수단으로는 다른 시선으로부터 그들의 신념과 행동을 정당화하기 위한 무언의 혹은 명시적인 압력인 책임을 통해 조직의 보안 프로세스 전반을 변경하는 것이다[31]. 책임의 구조는 심리학 및 조직 행동에서 상당한 주목을 받고 있다[22]. 이전의 연구는 책임은 사회적으로 받아들일 수 없는 방식으로의 행동을 감소시킬 가능성이 있다는 것을 일관되게 발견했다[28]. 따라서 본 연구는 다음의 연구 질문(Research Question : RQ)을 제안하였다.

RQ : 어떠한 요인에 의해 금융 IT 보안의 책임 인식 증가와 위험 감소, 그리고 나아가 기업의 성과를 만들 수 있는가?

이와 같은 연구 질문에 대한 답을 제시하기 위해 본 연구는 우선 책임과 보안 문헌에 대한 이론적 배경을 살펴본 후, 책임이론을 소개하고 본 연구에서 주장하고자 하는 맥락과 일치되는 가설을 제안하였다. 다음으로 방법론을 설명하고 연구의 분석 결과를 제시하였다. 그리고 본 연구의 결과, 시사점, 그리고 한계점에 대해 논하고 미래 연구 방향에 대해 설명하였다.

2. 연구모형 및 가설개발

본 연구는 보안을 실행하는 최종 단위인 해당 기업들이 이를 효과적으로 해결할 수 있는 실증적 증거를 제공하고자 한다. 특히, 최근 금융권의 잇따른 IT 보안 사고의 발생은 보안의 종합적인 조치를 필요로 한다. 이와 같은 배경으로부터, 본 연구는 책임이론을 바탕으로 보안대책이 금융 IT 보안의 책임증가와 위험감소를 이끌고 나아가 기업의 우수한 성과에도 영향을 미칠 것이라고 제안한다. 또한, 금융보안에 대한 조직 전체의 변화를 추구하기 위해 변혁적 리더십을 조절변수로 제안하여 그 중요성을 살펴보고자 한다. 뿐만 아니라 전 세계적으로 금융보안의 심각성이 증가하고 있다는 점에서 나라별로도 금융보안에 대한 조치가 동일하게 적용되어 질 수 있는지에 대해 알아보고자 금융기관의 한국과 미국의 비교분석을 통해 이론적 모델이 어떠한 차이를 나타내는지에 대해서도 조사하였다. 이러한 논리에 기초한 본 연구는 [그림 1]의 연구모형을 개발하였다.



[그림 1] 연구모형 및 가설

2.1 정보보안 대책 모델

정보보안 대책(information security countermeasures)은 정보시스템 위협에 저항하기 위하여 채택하는 다양한 방법들을 포함한다(예, 물리적 절차, 하드웨어, 소프트웨어, 인적 수단). 이러한 보안대책 모델들은 모두 명시적 혹은 암묵적으로 기술과 사람을 함께 포함하고 있다[38]. 본 연구는 기존 연구의 의미를 포괄하는 개념의 기술적 수단의 보호와 내부 절차적 행동에 대한 두 가지 구분되는 보안대책을 집중적으로 다루었다. 보안 보호에 대한 체계는 내부 보안 프로세스의 존재와 효과에 대한 조직의 인식능력이다[38]. 높은 보안대책 하에서, 조직은 그들이 필요한 자원을 가지고 있고, 요구되는 보안 관리(예, 책임 인지)가 더 가능하다고 믿는다. 보안책임의 상승작용을 위해서는 최종적으로 기업은 내부의 자원(resources)과 기술(skills)을 필요로 한다[35].

절차적 대책은 사회법칙과 같은 기본 체계에 의존적이라고 할 수 있는데, 이는 곧 조직에서 행동을 허용하는 범위의 지식을 전달하는 것과 같다[17]. 다시 말하면, 절차적 대책은 조직의 규정으로 이는 조직의 보안에 대한 의무감을 형성하고 나쁘고 불필요한 방향성을 제거하는데 효과적이다. 한편, 억제(deterrence)에 관한 연구에서는 보안에 대한 감시활동이 불법적 행동에 대한 제재를 증가시킨다고 주장하였다[18]. 컴퓨터 모니터링은 비록 그들을 지켜보고 활동을 기록하는 상대를 볼 수 없어 추상적이지만[22] 기술적 방법에 의한 상시 경계는 보안에 대한 책임을 유인할 수 있다. Vance et al.[35]은 책임 인식 증가를 위해서는 몇 가지 구별되는 하위 요소들, 식별 가능성(identifiability), 모니터링 인식(monitoring awareness), 평가 인식(evaluation awareness), 사회적 존재 인식(social presence awareness)이 반드시 관여되어야 하며, 이러한 메커니즘에 의해 결과물에 대한 구체적인 처리와 접근이 가능하다고 주장하였다. D'Arcy et al.[10]는 최적의 보안 상태를 정의하기 위해 보안정책, SETA(security education, training, and awareness) 프로그램, 그리고 컴퓨터 모니터링과 같은 행동을 조절할 수 있는 제약적 접근이 필요하다고 하였다. 본 연구는 이와 같은 주장을 근거로 다음의 가설을 제안한다.

가설 1 : 보안대책은 금융 IT 보안 책임증가에 정(+)의 영향을 미칠 것이다.

가설 2 : 보안대책은 금융 IT 보안 위험감소에 정(+)의 영향을 미칠 것이다.

2.2 책임이론

책임(accountability)에 관한 연구의 난제는 그 개념이 철학, 윤리학, 정치학, 조직 행동을 포함한 다양한 영역에서 폭넓게 사용된다는 것이다[25]. 또한 연구자들은 책임에 대한 그들 자신만의 정의를 만들어내는 경향이 있는데, 이들은 아주 드물게 서로

호환이 가능하다[5]. 결과적으로, 현존하는 문헌에서는 책임을 단편적인(fragmented), 그리고 모순되는(inconsistent) 방식으로 다룬다. 책임을 이해하는 유용한 한 가지 방법은 가장 일반적인 두 가지의 사용에 대해 구별하는 것이다. (1) 하나의 덕목(virtue)으로써 그리고 (2) 하나의 메커니즘(mechanism)으로써 에 대한 것이다[5]. 덕목으로써의 책임은 한 사람이 책임감을 받아들이는데 기꺼이 그렇게 함을 나타내는 특성으로 볼 수 있으며, 메커니즘으로써의 책임은 잠재적 의무(obligation)를 가진 한 사람이 자신의 행동을 그 행위에 대한 판단을 내리는 권리를 가진, 그리고 자신의 행위로 인한 잠재적 결과에 영향을 받을 수 있는 다른 상대에게 설명하는 하나의 과정(process)이다[35]. 본 연구의 목적을 위해, 책임은 두 번째 사용에 더 맞추어 논의될 것이다. 책임은 이를 촉진하는 메커니즘 없이는 존재할 수 없는 조직적 관리방식의 주요한 형태이다. 이러한 메커니즘은 직원-경영자 관계의 조직에서 전형적이며 명백한 모니터링과 평가와 같은 구조적 대안들을 포함한다[35].

책임관련 문헌의 평가에서, Bovens[5]는 기존 문헌에 나타나는 대부분의 불명확함이 세밀한 연구가 없이 책임에 대해 다루고 있는 연구자들 때문이었다는 것을 발견했다. 주목할 만한 예외가 있었는데, 조직 내에서의 행동을 설명하기 위해 책임이론을 개발한 Tetlock과 동료들의 연구이다(예 : [33, 34]). 본 연구는 연구 모델의 기초로 Tetlock의 연구를 활용하였다. 책임이론은 어떻게 다른 사람에 대한 행동을 정당화하기 위해 지각된 욕구가 결정과 판단에 도달하는 그 과정을 고려하고 책임감을 느끼도록 만드는지를 설명한다[33]. 결정 과정과 결과를 설명하려는 이러한 욕구는 결국 그들의 절차상의 행동들을 기계적이거나 추론적 사고(heuristic processing)를 사용해서가 아니라, 깊게 그리고 체계적으로 생각할 가능성을 증가시킨다.

추론적 사고는 결정에 대한 얕은 인지적 사고와 관련되어 있는데, 이러한 사고는 결정을 내리기 위해 단순한 규칙을 사용하는 결과를 초래한다[24]. 이와는 대조적으로, 체계적인 사고(systematic processing)는 의사결정을 하기 위한 깊은 인지적 사고와 면밀하게 생각하는 것이 관련되어 있다[24]. 따라서 시스템 사용에 대한 결정을 내리기 위해 체계적으로 생각하는 사람은 자신만이 유일하게 선택할 수 있는 가장 바람직한 결정을 이끌어내기 위해 더 많은 투입 요소들을 고려하고 더 주의 깊게 생각할 것이다. 체계적인 사고에 더 중점을 두는 것은 결과적으로 그 해당 대상이 책임져야하는 효과적인 결과를 만들어내는 것에 더 역점을 두게 한다[27].

요약하자면, 책임이론의 이론적 사용에 있어서의 기본적인 가정은 인지된 책임의 증가가 위험을 감소시키고 이러한 유익한 영향은 조직 전반에 확대된다는 것이다. 기업은 그들의 내부 책임이 증가되었을 때 합리적 의사결정과 목적에 반하지 않는 방향을 설정할 수 있게 해준다[35]. 즉, 책임증가는 조직의 잠재적, 전략적 능력을 최대화하고 수동적 존재로써의 기업을 축소시킨다[32]. 기업 역기능의 대부분은 강제적 통제에 의존한 것에서 비롯되는데 이는 경영상의 문제로 다뤄진다. 문제 발생의 이유는 손실과 이익의 주체라는 역할에 대한 책임인식의 부족 때문이라고 할 수 있다[35]. 보안에서의 강력한 책임은 신뢰성을 전제한 경영보고서의 유지와 각종 규정 준수에 따른 위험감소의 효과를 지속한다[35]. 위험감소의 평가적 측면은 기업이 목표달성에 악의적 요소를 제거하는데 집중하고, 결과적으로 기업의 부실한 경영 상태를 방지하는 것과 같은 장기적 이익달성 및 객관적 성과 측정을 가능하게 한다[32]. 이러한 주장은 책임이 만드는 보안의 효율성을 예상할 수 있다. 이에 본 연구는 다음의 가설을 제안한다.

가설 3 : 금융 IT 보안 책임증가는 금융 IT 보안 위험감소에 정(+)의 영향을 미칠 것이다.

가설 4 : 금융 IT 보안 책임증가는 기업성과에 정(+)의 영향을 미칠 것이다.

가설 5 : 금융 IT 보안 위험감소는 기업성과에 정(+)의 영향을 미칠 것이다.

2.3 변혁적 리더십

변혁적 리더십(transformational leadership)은 일차적으로 조직 구성원 변화에 초점을 두고 나아가 개별의 구성원 뿐 아니라 조직 전반의 변화를 목적으로 한다. 변혁된 결과는 조직의 구성원이 그들의 리더 혹은 집단, 그리고 조직의 목표 달성을 위해 개인 희생과 헌신, 즉 이해관계의 상쇄를 강조하여 뛰어난 성과를 만든다. Bass[4]는 조직원에게 기대 그 이상의 성과를 이끌어 내도록 그들을 동기부여 시키는 것이라고 정의하였다. 이러한 방법을 제공하는 변혁적 리더십 차원에는 이상화된 행동 또는 카리스마(idealized behavior or charisma), 영감적 동기부여(inspirational motivation), 지적 자극(intellectual stimulation), 개인화된 배려(individualized consideration)를 포함한다[9]. 이상화된 행동 또는 카리스마, 즉, 변혁적 리더십의 첫 번째 차원은 리더가 높은 윤리적 행동의 역할 모델이 되고 구성원이 리더를 모방하고자 함으로써 이에 반응할 때 발생한다[19].

영감적 동기부여, 즉, 변혁적 리더십의 두 번째 차원은 리더가 구성원에게 호소력이 있고 영감을 주는 비전을 명확히 표현할 때 발생한다. 이들은 조직 구성원이 높은 표준을 채택하도록 자극하고, 목표 등에 대한 낙관주의를 전달한다. 이러한 리더는 복잡한 개념을 간단하게 명확히 표현한다. 이에 대한 행동은 구성원이 리더와 함께 확인할 필요 없이 발생할 수 있다[23]. 지적 자극 행동, 즉, 세 번째 차원은 리더가 문제 해결에서 새로운 관점을 찾기 위해 전통적 가정과 믿음에 도전할 때 발생한다. 구성원의 지식과 합리성, 문제해결 능력의 제고를 위해 새로운 방식의 사고를 돕는다. 이 과정에서, 리더는 조직 구성원에 의해 자기 결정성과 자주적 방향 설정을 할 수 있는 환경을 구성한다[23]. 마지막으로, 리더가 조직원의 관심사와 필요성을 이해하고 공유하려고 시도하며 그들에게 개인화된 관심을 제공할 때, 개인화된 배려가 발생된다. 이는 구성원들이 자신의 능력 수준에 적합한 역할을 수행하도록 한다[23].

하나의 조직이 급격한 변화에 적응하기 위해서는 주어진 과제를 해결하는 변혁적 리더십에 의해 구성원을 개발함으로써 상위단계의 가치를 만들고 장기적 이익에 부합할 수 있다는 것이다. 특히, 변혁적 리더십은 전통적 구조의 사회나 조직이 위기상황에 놓였을 때 새로운 가치관과 구조를 제시하는데 효과적이라고 할 수 있다[30]. 따라서 본 연구는 이와 같은 논의를 바탕으로 다음의 가설을 제안한다.

가설 6 : 변혁적 리더십은 보안대책과 금융 IT 보안책임증가 사이의 관계를 더 강화시켜 줄 것이다.

가설 7 : 변혁적 리더십은 보안대책과 금융 IT 보안위험감소 사이의 관계를 더 강화시켜 줄 것이다.

2.4 국가비교 연구

본 연구는 금융 IT 보안의 효과와 예측에 국가간 비교를 통해 또 다른 관점의 연구 방향을 제안하고자 한다. 국가 간 비교 분석은 각 나라마다 내재된 문화적 차이를 이해하고 개발하는 하나의 좋은 조사 방법이다[13]. 일반적으로 예측할 수 없는 특정한 상황에 대해 이와 같은 비교 분석으로 좀 더 나은 이해를 제공할 수 있기 때문에 이러한 연구는 유사한 영역의 조사에 있어서 상당한 강점과 설득력을 가질 수 있다[17, 21]. 특히, 동양권과 서양권의 문화가 크게 다르다는 점에서 한국과 미국의 비교는 다양한 문화권에서 보여지는 함축적 행위의 유사성 혹은 차이를 설명해 줄 수 있다[17].

동일하거나 혹은 비슷한 기술과 체계들이 조직 내에 갖추어져 있다 하더라도 하나의 나라가 가지는 신념, 가치관, 사상, 등은 다른 수준에 머물고 그 나라에 속한 조직은 그 범위에서 벗어나지 않는 방식을 추구한다[21]. 다시 말하면, 이러한 문화적 특성에 따라 동·서양의 조직은 그들 내에서의 제어와 조화의 문제가 공통적이지 않는 다는 것을 강조한다. 따라서 국가 수준의 비교 측정은 글로벌 IS 사용에

대해 각각의 국가가 어떻게 다르게 설계, 도입, 구현, 그리고 진행하는가에 초점을 두고 IS 도구의 동등한 관점에서 보완할 수 있다[11]. 본 연구의 국가별 비교에 있어서는 국가를 전반적인 문화를 반영한 하나의 차원으로 이해하고 이론적 모델의 영향관계가 어떻게 같게 혹은 다르게 나타나는지를 살펴봄으로써 연구의 해석 능력을 향상시키고자 한다. 이에 한국과 미국에 대한 다음의 가설을 제안한다.

가설 8 : 보안대책이 금융 IT 보안 책임증가에 미치는 영향은 국가 간 차이가 있을 것이다.
가설 9 : 보안대책이 금융 IT 보안 위험감소에 미치는 영향은 국가 간 차이가 있을 것이다.
가설 10 : 금융 IT 보안 책임증가가 금융 IT 보안 위험감소에 미치는 영향은 국가 간 차이가 있을 것이다.
가설 11 : 금융 IT 보안 책임증가가 기업성과에 미치는 영향은 국가 간 차이가 있을 것이다.
가설 12 : 금융 IT 보안 위험감소가 기업성과에 미치는 영향은 국가 간 차이가 있을 것이다.

3. 연구 방법

3.1 자료수집

본 연구에서는 금융기관의 보안이 기업성과에 미치는 영향을 실증적으로 검정하기 위해 한국과 미국의 금융기관을 대상으로 연구모형의 각 변수별 영향력 분석을 위해 기업단위의 조사를 실시하였다. 분석을 위한 자료는 한국과 미국에서 금융기관을 대상으로 실시하였다. 한국에서는 인터넷 기반의 금융 서비스를 제공하는 은행, 보험, 카드회사와 같은 금융에 포함된 기업을 대상으로 전화, 이메일, 방문을 통해 자료를 수집하였다. 미국에서는 서부와 남부에 소재한 글로벌 금융기관(예 : BOA, Progressive 등)을 대상으로 전화, 우편 및 이메일 설문을 실시하였다. 본 연구의 목적에 적합한 기업으로부터 자료를 수집하기 위해 금융권 IT 보안에 대한 기본적인 설명과 연구의 목적을 설문전 충분히 설명하여 데이터의 타당성을 높이고자 하였다. 또한 설문에 참여하는 금융기관 응답자의 일반적 사항 외에도 금융 IT 보안에 대한 일반적 사항을 통해 응답 기업의 금융 IT에 대한 부분을 조사하였다.

총 2,000부의 설문지(한국 1,000부, 미국 1,000부)가 배포되어 이 중 179부의 한국 응답과 151부의 미국 금융기관 응답이 회수 되었다. 하지만 응답이 불완전한 한국 10부, 미국 19부를 제외한 한국 167부, 미국 132부를 최종 연구에 사용하였다. 설문에 참여한 기업의 응답자 일반 사항 및 금융 IT 보안 일반적 특징은 <표 1>에서 보여주고 있다.

3.2 측정변수

연구모형의 구성요소를 측정하기 위한 측정도구는 3단계에 걸쳐 최종 개발 하였다. 우선 기존 연구를 통해 관련 변수의 설문 항목을 본 연구의 내용에 적합하게 수정 및 보완 하였다. 도출된 설문항목들은 등간척도의 하나인 (1) 강한 부정에서부터 (7) 강한 긍정에 걸친 7점 리커트(seven-point Likert scale)의 항목으로 개발 되었다. 다음으로 대학 연구자 및 박사과정 학생을 대상으로 측정항목에 대한 내용타당성(content validity) 검정을 실시하였다. 내용타당성 검정을 통해 각 항목에 대한 어법, 정확성 등의 정교화 과정을 통해 설문항목의 타당성을 높이고자 시도 하였다. 마지막으로 금융기관을 대상으로 사전조사를 실시하여 통계적으로 각 항목의 신뢰성과 타당성에 문제가 없는지를 검정하여 최종 설문항목을 개발 하였다. 본 연구에서 사용한 변수의 조작적 정의와 관련연구는 <표 2>에서 보여주고 있다.

4. 자료 분석

4.1 측정모형의 신뢰성 및 타당성 검정

구조모형 분석에 앞서 측정항목의 신뢰성과 타당

〈표 1〉 응답자 특성

분류		빈도 및 비율 (한국)	빈도 및 비율 (미국)
성별	남자	97(57.40%)	85(64.39%)
	여자	72(42.60%)	47(35.61%)
연령	29세 이하	7(04.14%)	15(11.36%)
	30-39세	58(34.32%)	66(50.00%)
	40-49세	73(43.20%)	38(28.79%)
	50세 이상	31(18.34%)	13(09.85%)
응답자 직위	이사급 이상	17(10.06%)	24(18.18%)
	부장/차장	79(46.75%)	59(44.70%)
	과장/대리	54(31.95%)	33(25.00%)
	기타	19(11.24%)	16(12.12%)
금융업종	은행	50(29.59%)	53(40.15%)
	증권	32(18.93%)	21(15.91%)
	보험	54(31.95%)	45(34.09%)
	카드	29(17.16%)	10(07.58%)
	기타	4(02.37%)	3(02.27%)
금융 IT 환경에서 발생된 문제의 주요 원인 (복수응답)	전자금융거래 증가	132(78.11%)	89(67.42%)
	스마트 기기 사용 증가	99(58.58%)	53(40.15%)
	보안에 대한 금융기업의 책임결여	53(31.36%)	71(53.79%)
	해킹 기술이 발달	151(89.35%)	62(46.97%)
	내부 정보유출	75(44.38%)	38(28.79%)
	기타	16(09.47%)	9(06.82%)
금융 IT 보안 강화를 위한 구체적 사항 (복수응답)	금융기관의 CISO 도입 의무화	92(54.44%)	45(34.09%)
	보안 인력 및 예산 모범 규정	107(63.31%)	58(43.94%)
	전자금융 보안 강화 프로그램 실행	70(41.42%)	82(62.12%)
	IT기반 구조(예 : HW/SW, 네트워크 등)	68(40.24%)	36(27.27%)
	보안에 대한 구성원 교육	101(59.76%)	44(33.33%)
	기타	14(08.28%)	10(07.58%)
합계		169	132

성 검정을 위해 부분최소자승(Partial Least Square : PLS) 분석을 실시하였다. 분석 도구로는 Smart PLS2.0을 사용하였으며, PLS 접근방법을 통해 본 연구와 같은 탐색적 성향의 구조방정식 분석 뿐 아니라 표본에 대한 편리함을 제공 받을 수 있다. 즉, PLS에서는 작은 수의 표본으로도 변수 간 관계 검증이 가능하다. 우선 측정모형의 신뢰성 검증은 PLS 산출물 중 평균분산추출((Average Variance Extracted : AVE)값과 복합신뢰도(Composite Reliability : CR) 값을 사용하였다. 신뢰성 존재 여부는 조직단위 연구에서 AVE 0.5 이상, CR 0.7 이상이 되어야 된다[14]. 또한 PLS 분석에서 도출 되는 요인값을 통해 측정모형의 집중타당성(convergent validity)을 AVE 제곱근 값과 연구모형이 구성요소 간 상관계수값을 통해 판별타당성(discriminant validity) 검정을 실시하였다. 각 측정항목에 대한 요인

〈표 2〉 연구변수에 대한 조작적 정의 및 관련연구

연구변수		조작적 정의	관련연구
보안 대책	절차적 대책	조직 내 보안정책과 보안관련 교육 · 훈련 · 인식 프로그램(예, 보안 브리핑 및 코스)에 대한 의존정도	Hovav and D'Arcy[17]
	기술적 대책	조직 내 컴퓨터 활동을 추적하고, 보안 감사를 수행하는 기술적 해결 능력의 정도	D'Arcy et al.[10]
변혁적 리더십		조직이 IT 보안에 대해 지향하는 목표와 비전을 구성원들에게 전달하고, 동기 유발 및 자발적 노력을 이끄는 리더십의 정도	Li et al.[23]
금융 IT 보안책임 증가		IT 보안에 대한 조직 행동의 결과 및 판단을 설명할 잠재적 의무 정도	Vance et al.[35]
금융 IT 보안위험 감소		IT 보안에 대한 인식 제고와 긍정적 행동변화 및 보안 위협/사고의 감소 정도	Vance et al.[35]
기업성과		금융사의 금융 IT환경 개선에 따른 기업의 신뢰도 제고 및 IT리스크 감소 등 기업 경영의 효율성 증가 정도	Tan and Kao[32] Kotulic and Clark[20]

〈표 3〉 구성요소의 신뢰성 및 집중타당성 분석결과

잠재변수		항목	표준오류	요인값	t-값
보안대책 (Security Countermeasures)	AVE = 0.579 CR = 0.938	sc1	0.144	0.838	22.310
		sc2	0.081	0.718	6.914
		sc3	0.106	0.797	17.382
		sc4	0.073	0.761	18.639
		sc5	0.132	0.760	12.965
		sc6	0.121	0.576	11.440
		sc7	0.096	0.721	7.729
		sc8	0.182	0.728	12.309
		sc9	0.039	0.793	14.956
		sc10	0.101	0.843	15.592
		sc11	0.128	0.801	12.375
		sc12	0.104	0.443	7.047
변혁적 리더십 (Transformational Leadership)	AVE = 0.608 CR = 0.925	tl1	0.091	0.731	8.751
		tl2	0.073	0.727	8.406
		tl3	0.112	0.835	12.187
		tl4	0.098	0.823	16.392
		tl5	0.092	0.778	18.159
		tl6	0.098	0.764	16.282
		tl7	0.044	0.769	14.549
		tl8	0.116	0.805	16.874
금융 IT 보안책임 증가 (Increased Financial IT Accountability)	AVE = 0.697 CR = 0.902	acct1	0.128	0.828	13.412
		acct2	0.108	0.872	14.440
		acct3	0.086	0.841	17.752
		acct4	0.130	0.797	14.554
금융 IT 보안위험 감소 (Reduced Financial IT Risks)	AVE = 0.584 CR = 0.892	ris1	0.123	0.811	14.925
		ris2	0.082	0.810	13.982
		ris3	0.134	0.807	12.497
		ris4	0.105	0.752	12.618
		ris5	0.100	0.541	13.903
		ris6	0.136	0.826	12.024
기업성과 (Firm's Performance)	AVE = 0.643 CR = 0.926	fp1	0.068	0.767	16.722
		fp2	0.076	0.893	14.069
		fp3	0.094	0.804	21.429
		fp4	0.120	0.729	17.425
		fp5	0.101	0.809	11.756
		fp6	0.081	0.836	13.285
		fp7	0.102	0.766	15.839

값은 조직단위 연구에서는 최소 0.6 이상이 되어야 집중타당성에 문제가 없다고 할 수 있다[14]. 마지막으로 판별타당성은 각 구성요소의 AVE 제곱근 값은 종과 횡의 구성개념간 상관계수값 보다 커야 판별타당성이 존재한다고 할 수 있다[12].

이러한 분석 방법을 통해 측정모형을 검정한 결과는 <표 3>과 <표 4>에서 보여주듯 신뢰성과 판별타당성은 문제가 없는 것으로 나타났다. 하지만 집중타당성 검정에서 3개의 항목(sc5, sc12, ris5)에 대한 요인값이 기준치인 0.6 이하로 나와 이 3개 항목은 추후 분석에서 제외되었다.

4.2 구조모형 분석

전체 자료를 대상으로 측정모형에 대한 타당성과 신뢰성을 검정 한 후 구조모형 분석에서는 크게 3가지 단계를 통해 본 연구의 목적을 실증적으로 검정하였다. 구조모형 분석은 측정모형 분석과 마찬가지로 SmartPLS2.0을 사용하였다. 첫 번째 분석은 연구모형에서 제시한 직접효과에 대한 분석이다. 이는 곧 가설 1~가설 5에 대한 검정으로 한국 금융기관과 미국 금융기관의 자료를 나누어 분석 하였다. 이를 통해 본 연구에 참여한 한국과 미국 금융기관에서 보안 대책과 금융 IT 보안책임 증가, 금융 IT 보안위험 감소 및 기업성과 간의 관계를 알 수 있다. 둘째, 본 연구에서 제안하는 변혁적 리더십의 조절효과 분석은 Carter and Russell[7]의 연구에서 제안한 조절된 다중회귀(Moderated Multiple Regression : MMR) 방법에 따라 검정 하였다. 마지막으로 각 경로에 대해 한국과 미국 금융기관의 차이 검정을 위해 다중집단 조절효과(multi-group moderation effect) 분석을 실시하여 연구모형의 직접효과에서 그룹 간 차이가 존재하는지를 검정하였다.

4.2.1 한국 금융기관

연구모형이 직접효과에 대한 가설은 PLS 알고리듬에서 경로계수를 구하고, 부스트랩 리샘플링 방법(bootstrap resampling method)을 통해 각 경로계수의 t-값을 통해 가설에 대한 지지여부를 검정하였다. 한국 금융기관(n = 169)로 가설 1~가설 5를 검정한 결과 모든 경로에서 유의한 것으로 나타났다. 또한 내생변수의 설명력 정도를 알려주는 결정계수 R^2과 관련해서 금융 IT 보안책임 증가는 0.137, 금융 IT 보안위험 감소는 0.307, 기업성과는 0.416으로 각각 13.7%, 30.7%, 41.6%의 분산을 나타내고 있다. [그림 2]는 한국 금융기관에서 각 변수에 대한 PLS 구조모형 분석에 대한 결과를 보여준다.

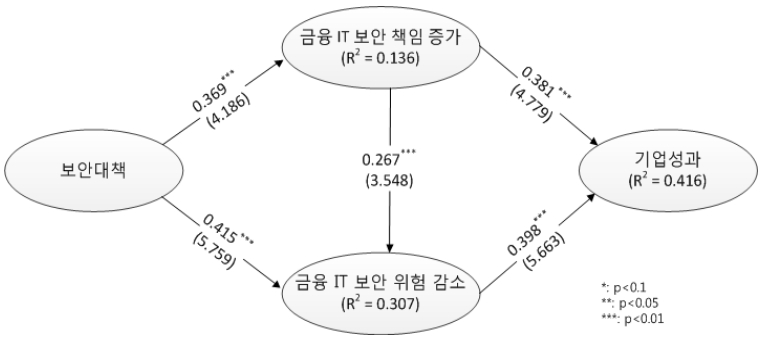
4.2.2 미국 금융기관

미국 금융기관을 대상으로 한 분석에서는 가설 4를 제외한 나머지 경로에서 모두 유의한 결과를 보여주고 있다. 이는 곧 미국 금융기관의 구성원들은 금융 IT 보안에 대한 책임이 증가되면 금융 IT 보안위험은 감소시킬 수 있지만 직접적으로 금융 기관의 성과에는 영향을 미치지 않는다는 것을 알 수 있다. 또한 내생변수의 설명력 정도를 알려주는 결정계수 R^2과 관련해서 금융 IT 보안책임 증가는 0.059, 금융 IT 보안위험 감소는 0.395, 기업성과는

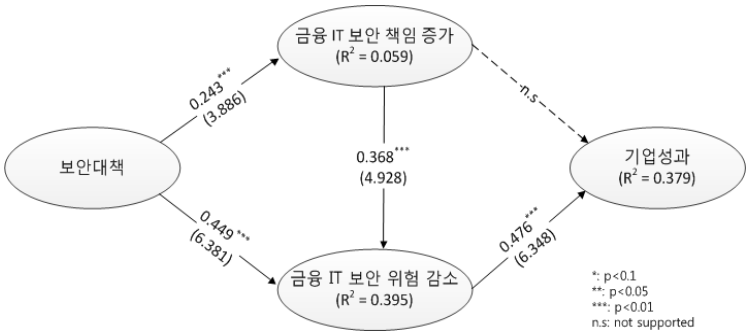
〈표 4〉 구성요소의 판별타당성 분석결과

변수	1	2	3	4	5
1. 보안대책	**0.761**				
2. 변혁적 리더십	0.339	**0.780**			
3. 금융 IT 보안책임 증가	0.392	0.266	**0.835**		
4. 금융 IT 보안위험 감소	0.451	0.178	0.350	**0.764**	
5. 기업성과	0.282	0.142	0.394	0.416	**0.802**

주) 진하게 표시된 대각선 값은 AVE의 제곱근 값임.



[그림 2] 직접효과 분석결과(한국 금융기관)



[그림 3] 직접효과 분석결과(미국 금융기관)

0.379으로 각각 5.9%, 39.5%, 37.9%의 분산을 나타내고 있다. [그림 3]은 미국 금융기관에서 각 변수에 대한 PLS 구조모형 분석에 대한 결과를 보여준다.

4.2.3 조절효과 분석

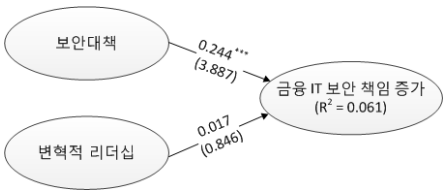
본 연구에서 제안한 변혁적 리더십의 조절효과는 Carter and Russell[7]가 제안한 조절된 다중회귀(Moderated Multiple Regression : MMR) 방법에 따라 검정 하였다. 이 연구에서는 기존의 조절효과 검정에서 발생하는 오류를 지적하고, 해결방안으로 MMR 사용을 권장하였다. MMR 접근방법에서는 조절변수가 영향을 주는 변수 간 관계에서 독립변수와 조절변수를 선행변수로 했을 때의 R^2값 그리고 독립변수, 조절변수 그리고 독립변수와 조절변수를 곱한 상호작용변수를 선행으로 했을 때 R^2값을 통해 F-값으로 조절변수의 영향을 분석하는 방법이다. MMR 방법에서 상호작용변수를 선행변수로 포함한 R_m^2 값과 상호작용변수가 없는 R_a^2 값 차이인 $\triangle R^2$ 값이 크면 조절효과가 있다고 할 수 있다. 두 경우 선행 변수의 수 즉, 자유도와 분석에 사용한 총 표본수를 고려하여 아래 식에 따라 F-값을 구할 수 있다.

$$F_{(df_m - df_a, N - df_m - 1)} = \frac{\triangle R^2/(df_m - df_a)}{(1 - R_m^2)/(N - df_m - 1)}$$

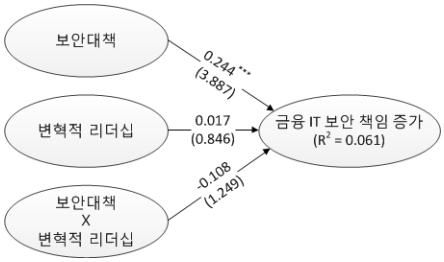
우선 한국 금융기업(n = 169)을 대상으로 변혁적 리더십의 조절효과를 분석 하였다. 이에 가설 6(보안대책 → 금융 IT 보안책임 증가 사이에서 변혁적 리더십의 조절효과) 그리고 가설 6(보안대책 → 금융 IT 보안위험 감소 사이에서 변혁적 리더십의 조절효과)을 검정 하였다. MMR 방식에 따라 보안대책과 변혁적 리더십을 선행변수로 했을 때 금융 IT 보안책임 증가에 대한 R_a^2 값, 0.137([그림 4-1])과 0.309([그림 4-3])를 구했고, 여기에 보안대책과 변

혁적 리더십의 곱한 상호작용변수를 선행 변수로 추가 했을 때 IT 보안책임 증가에 대한 R_m^2 값, 0.153([그림 4-2])과 0.328([그림 4-4])을 구했다. 이를 기반으로 각 조절효과에 대한 F-값 검정 결과 가설 6은 2.919 그리고 가설 7은 4.665에서 각각 유의수준 0.1과 0.05에서 지지되었다. 한국의 금융기관을 대상으로 한 변혁적 리더십의 조절효과 분석은 [그림 4] 보여주고 있으며, <표 5>는 가설검정 결과에 대해 요약하고 있다.

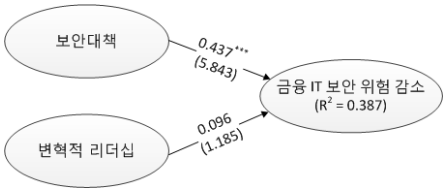
다음으로 미국의 금융기관(n = 132)을 대상으로 한국의 경우와 똑 같은 절차로 분석을 실시하였다. 우선 조절효과에 대한 검정 결과 <표 6>에서 보여주



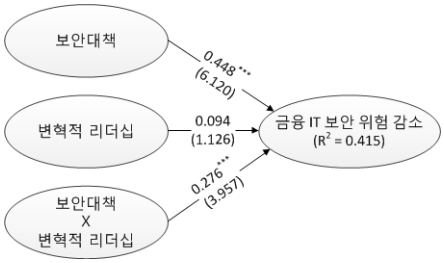
[그림 5-1]



[그림 5-2]



[그림 5-3]



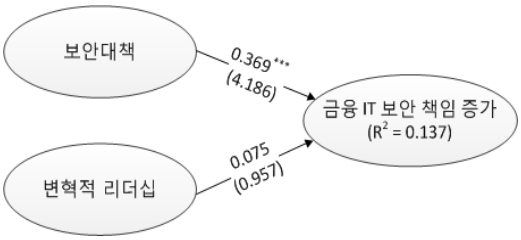
[그림 5-4]

[그림 5] 조절효과 분석결과(미국 금융기관)

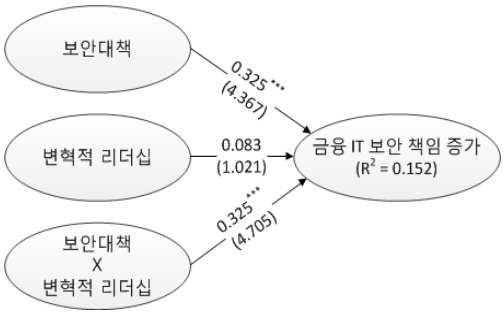
〈표 6〉 가설검정 결과요약(미국 금융기관)

가설	경로	표준화된 경로계수	t-값	차이	F-값	결과
가설 1	보안대책 → 금융 IT 보안책임 증가	0.243***	3.886	-	-	채택
가설 2	보안대책 → 금융 IT 보안위험 감소	0.449***	6.381	-	-	채택
가설 3	금융 IT 보안책임 증가 → 금융 IT 보안위험 감소	0.368***	4.928	-	-	채택
가설 4	금융 IT 보안위험 감소 → 기업성과	0.032	0.674	-	-	기각
가설 5	금융 IT 보안위험 감소 → 기업성과	0.476***	6.348	-	-	채택
가설 6	보안대책 → 금융 IT 보안책임 증가 ↑ 변혁적 리더십	-	-	0	0	기각
가설 7	보안대책 → 금융 IT 보안위험 감소 ↑ 변혁적 리더십	-	-	0.028	6.126**	채택

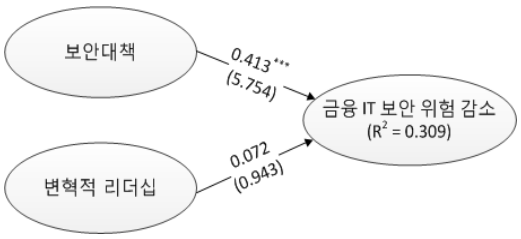
주) * : $p < 0.1$, ** : $p < 0.05$, *** : $p < 0.01$.



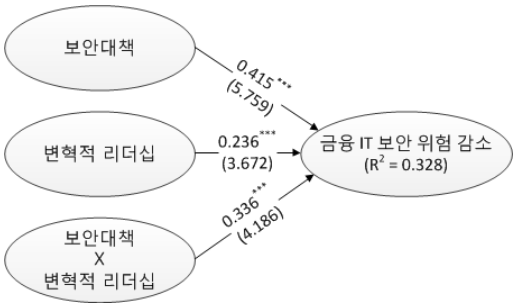
[그림 4-1]



[그림 4-2]



[그림 4-3]



[그림 4-4]

[그림 4] 조절효과 분석결과(한국 금융기관)

〈표 5〉 가설검정 결과요약(한국 금융기관)

가설	경로	표준화된 경로계수	t-값	차이	F-값	결과
가설 1	보안대책 → 금융 IT 보안책임 증가	0.369***	4.186	-	-	채택
가설 2	보안대책 → 금융 IT 보안위험 감소	0.415***	5.759	-	-	채택
가설 3	금융 IT 보안책임 증가 → 금융 IT 보안위험 감소	0.267***	3.548	-	-	채택
가설 4	금융 IT 보안위험 감소 → 기업성과	0.381***	4.779	-	-	채택
가설 5	금융 IT 보안위험 감소 → 기업성과	0.398***	5.663	-	-	채택
가설 6	보안대책 → 금융 IT 보안책임 증가 ↑ 변혁적 리더십	-	-	0.015	2.919*	채택
가설 7	보안대책 → 금융 IT 보안위험 감소 ↑ 변혁적 리더십	-	-	0.019	4.665**	채택

주) * : $p < 0.1$, ** : $p < 0.05$, *** : $p < 0.01$.

듯이 가설 7은 한국과 같이 F-값 6.126으로 유의수준 0.01에서 채택되었다. 하지만 가설 6은 R_m^2 값과 R_a^2 값이 동일하게 0.061로 나왔기 때문에 가설 6은 기각되었다. [그림 5]는 미국 금융기관의 변혁적 리더십의 조절효과에 대한 분석 결과를 보여주며, <표 6>은 가설검정 결과에 대해 요약 하고 있다.

4.2.4 다중집단 차이분석

각 나라를 대상으로 연구모형의 직접효과와 조절효과를 검정한 후 연구모형에서 제안한 직접효과에 대해 한국과 미국 금융기관에 차이가 존재하는지를 검정 하였다. 각 경로에 대한 차이검정은 Chin[8]의 다중집단차이검정(multi-group difference analysis) 방법을 따라 아래 공식으로 t-값을 계산하여 판단하였다. 분석결과 부안대책과 금융 IT 보안책임 증가에 대해서는 한국과 미국의 금융기관 사이에 차이가 있는 것으로 나타났다. 따라서 가설 8은 채택되었다. 이 경로는 한국, 미국 금융기관 모두 유의한 결과를 나타냈지만 한국 데이터에서 더 높은 경로계수를 보여주고 있다. 이는 곧 보안대책이 금융 IT 보안책임 증가에 미치는 영향이 한국 금융기관에서 더 크다는 것을 알 수 있다.

$$t = \frac{Path_{sample\_1} - Path_{sample\_2}}{\left[\sqrt{\frac{(m-1)^2}{(m+n-2)} \times S.E._{sample1}^2 + \frac{(n-1)^2}{(m+n-2)} \times S.E._{sample2}^2}\right] \times \left[\sqrt{\frac{1}{m}+\frac{1}{n}}\right]}$$

또한 금융 IT 보안책임 증가와 금융 IT 보안위험 감소, 금융 IT 보안책임 증가와 기업성과 모두 한국과 미국 금융기관 사이에 차이가 있는 것으로 나타났다. 따라서 가설 10과 가설 11은 채택되었다. 금융 IT 보안책임 증가 → 금융 IT 보안위험 감소에 대한 경로는 미국 금융기관이 더 높은 경로계수를 보이며, 금융 IT 보안책임 증가 → 기업성과에 대해서는 한국 금융기관에서는 유의한 결과를 보이지만 미국 금융기관에서는 유의하지 않은 것으로 나타났다. 이러한 결과는 한국 금융기관 종사자와 미국 금융기관 종사자들 사이에서 본 연구에서 제안하는 요소에 대한 인식의 차이가 존재한다는 것을 알 수 있다.

마지막으로 보안대책 → 금융 IT 보안책임 증가, 금융 IT 보안위험 감소 → 기업성과에서는 두 나라 금융기관 사이에 차이가 존재하지 않는 것을 알 수 있다. 이 두 경로에 대해서 한국과 미국 금융기관 모두 유사하게 큰 경로계수 값으로 영향을 주는 변수에 중요한 요소로 인식되고 있다. 하지만 한국과 미국의 금융기관 종사자들이 이 변수들에 대해 가지는 영향력의 크기에는 차이가 없다는 것을 알 수 있다.

5. 토의 및 결론

본 연구에서는 보안대책이 기업성과에 영향을 주

〈표 7〉 한국과 미국 금융기관 차이분석결과

가설	경로	경로계수	표준오차	t-값	집단 간 차이	
					t-값 (유의수준)	결과
가설 8	보안대책 → 금융 IT 보안책임 증가	0.369	0.031	4.186	1.669 (0.048)	채택
		0.243	0.076	3.886		
가설 9	보안대책 → 금융 IT 보안위험 감소	0.415	0.094	5.759	0.230 (0.409)	기각
		0.449	0.117	6.381		
가설 10	금융 IT 보안책임 증가 → 금융 IT 보안위험 감소	0.267	0.029	3.548	1.750 (0.041)	채택
		0.368	0.054	4.928		
가설 11	금융 IT 보안위험 감소 → 기업성과	0.381	0.039	4.779	4.399 (0.000)	채택
		0.032	0.029	0.674		
가설 12	금융 IT 보안위험 감소 → 기업성과	0.398	0.102	5.663	0.664 (0.254)	기각
		0.476	0.027	6.348		

는 데 있어서, 보안대책이 금융 IT 보안책임 증가와 금융 IT 보안 위험감소에 어떻게 영향을 주며, 그 영향이 기업성과에 어떠한 영향을 미치는지를 국내·외 금융기관으로부터 자료를 수집하여 실증적으로 증명하고자 한다. 또한, 금융기관 경영진의 변혁적 리더십이 보안대책과 금융 IT 보안책임 증가와 위험감소에서 어떤 역할을 하는지에 대해서도 알아보았다. 한국과 미국의 금융기관을 대상으로 수집한 데이터를 분석한 결과를 요약하면 다음과 같다.

첫째, 한국 금융기관에서 모든 가설이 유의한 영향을 미치는 것으로 나타나 이는 곧 한국의 금융기업의 보안대책이 금융 IT 보안책임을 증가시키고, 금융 IT 보안 위험을 감소시켜, 기업성과에 긍정적인 영향을 미친다는 것을 알 수 있다. 반면, 미국의 금융기관 표본에서는, 보안대책이 금융 IT 보안책임 증가에는 유의한 영향을 주지는 않지만, 금융 IT 보안 위험감소에는 긍정적인 영향을 미치는 것으로 나타났고, 순차적으로 기업성과를 증진시키는 것으로 발견되었다. 위와 같은 실증적인 증거는 금융기관 내의 여러 형태의 보안대책, 즉 금융 IT 보안 향상에 대한 노력이 금융기업의 신뢰성을 향상시키고, 이는 곧 금융 리스크를 감소시켜 기업의 영업성과를 증진시키는 것을 의미한다.

둘째, 한국 금융기관 자료에서는 경영진의 변혁적 리더십이 긍정적인 조절 역할을 하는 것으로 나타났다. 이는 곧 금융기관의 경영진이 현실에 안주하는 수동적이지 않고, 혁신적인 조직 관리의 중요성을 의미한다. 반면, 미국 금융기관의 표본에서는 변혁적 리더십이 보안대책과 금융 IT 보안 위험감소 사이의 관계는 강화 시키지만, 금융 IT 보안 책임증가에서는 변혁적 리더십의 유의한 조절효과가 나타나지 않았다. 이는 금융기업의 최고 경영자나 금융보안 담당 경영자가 구성원들에게 금융 보안의 중요성의 심각성을 일깨우고, 이에 대한 일관된 목표와 비전을 전달 혹은 제시하고 동기를 부여시키는 것이 금융 IT 보안과 기업의 경영 효율성 증대에 있어서 핵심적인 요소임을 의미하는 것이다. 셋째, 한국과 미국 금융기관 간 비교에 있어서는 한국과 미국의 금융기관 종사자들 사이에 본 연구에서 제안하는 요소에 대해 약간의 행동에 대한 차이는 존재 할 수 있지만 그 차이가 크지 않다는 것을 알 수 있다. 즉, 보안대책은 금융 IT 보안위험을 감소하고, 금융 IT 보안위험이 감소되면 기업은 정성적 성과를 이룰 것이라는 일반적 논리가 한국과 미국 금융기관에 모두 적용이 된다.

본 연구는 금융보안 대책과 기업성과와의 관계에 있어서 그 구조적 관계를 실증적으로 규명하여, 학문적, 실무적으로 보안대책의 타당성과 보안대책의 설계에 있어서 중요한 토대가 되고자 하였다. 본 연구의 학문적, 실무적 시사점은 다음과 같다. 우선 학문적으로 본 연구는 기존의 선행연구에서 보여주지 못한 금융보안대책과 기업성과의 관계에 있어서 이론적인 구조적 모델을 제시하였다. 본 연구에서 제시한 연구모형은 금융 IT 보안에 대한 관심이 부각되고 있는 시점에서 보안대책과 이를 측정하는 세분화된 측정 변수들을 제시하고, 타당성을 검정하였다. 또한, 각 변수들의 개념을 구체화시키고 명확하게 함으로써, 향후 새로운 연구에 있어서 구조적 모델과 보안대책의 세분화된 개념에 대한 좋은 초석을 제공하였다. 본 연구는 실무적으로도 최근 잇따르고 있는 금융보안사고와 금융 IT 보안의 중요성의 심각한 인식 속에 본 연구는 금융보안대책과 기업성과의 구조적인 관계에 대해 실증적인 증명을 제공하였다. 이는 곧 금융 기업이 IT 기반의 금융 서비스를 제공함에 있어 고객들에게 안전성을 인식 시키지 못하면 기업의 신뢰도 향상이 어렵다는 점을 시사한다. 이러한 점들이 고객의 입장이 아닌 금융기관 종사자들 입장에서 규명 되어 금융기관 내부에서도 기업 성과를 증진시키기 위해 금융보안대책의 중요성과 당위성을 일깨우는 역할을 하게 될 것이다. 또한 본 연구는 보안대책과 기업성과의 그 구체적이고 근본적인 구조적인 관계를 보여줌으로써, 기업 이윤 증대를 목표로 하는 금융기업 경영자에게 구체적으로 어떠한 노력과 관심을 기울여야 하는지에 대한 가이드라인을 제공할 것이다.

이와 같은 시사점에도 불구하고 연구가 가지고 있는 몇 가지 한계점과 이를 통한 향후 연구방향을 제시하면 다음과 같다. 우선 본 연구는 보안대책과 기업성과의 관계 검정에 있어서 구조적 모델을 제시하고, 제안된 측정도구의 신뢰성과 타당성을 검정하였는데, 향후 연구에서는 이를 다시 검토하고 평가하여 이론적, 실증적으로 더 적합한 모델과 측정도구를 개발해야 할 것이다. 다음으로 각 금융 기관의 서비스 유형에 따라 보안대책에 대한 개념과 중요성, 또한 기업성과에 대한 직접효과가 다르게 나타날 수 있다. 따라서 향후 연구에서는 세분화된 금융기관의 사업 형태에 따라 차이검정을 통해 이를 확인하고, 그 차이가 존재한다면 세부집단 간 직접효과가 차이가 나는 요인에 대한 연구가 요구될 것이다. 마지막으로 본 연구에서 사용한 데이터, 특히 미국 금융기관의 데이터에 대한 한계점이 있다. 미국의 경우 금융의 중심이 동부지역의 금융기관으로부터 자료가 수집 되었으면 그 타당성이 더 높을 것이다. 이에 향후 연구에서는 응답자의 개별 특성 및 금융기관 특성을 고려해 자료 수집을 한 분석이 필요하다.

참 고 문 헌

[1] 김상현, 김근아, "정보보안관리에 영향을 미치는 기업환경요소와 규제자 영향의 조절효과", 「한국경영과학회지」, 제37권, 제3호(2012), pp. 79-94.

[2] 천성용, "금융 소비자 만족도에 영향을 미치는 요인", 「한국경영과학회지」, 제38권, 제1호(2013), pp.89-101.

[3] 하홍열, "은행서비스 산업에서 범주형 회귀분석을 이용한 지속적 거래의도 평가", 「한국경영과학회지」, 제37권, 제3호(2012), pp.1-12.

[4] Bass, B.M., *Leadership and Performance Beyond Expectations*, New York : Free Press, 1985.

[5] Bovens, M., "Two Concepts of Accountability : Accountability as a Virtue and as a Mechanism," *West European Politics*, Vol.33, No.5(2010), pp.946-967.

[6] Carmines, E.G. and R.A., Zeller, *Reliability and Validity Assessment*, Newbury Park, CA : Sage Publications, 1979.

[7] Carte, T.A. and C.J. Russell, "In Pursuit of Moderation : Nine Common Errors and Their Solutions," *MIS Quarterly*, Vol.27, No.3(2003), pp.479-501.

[8] Chin, W.W. and J. Dibbern, A Permutation Based Procedure for Multi-Group PLS Analysis : Results of Tests of Differences on Simulated Data and a Cross of Information System Services between Germany and the USA, *in Handbook of Partial Least Squares : Concepts, Methods and Applications in Marketing and Related Fields*, V.E. Vinzi, W.W. Chin, J. Henseler, and H. Wang(eds), Berlin : Springer, 2009.

[9] Cho, J., I. Park, and J.W. Michel, "How Does Leadership Affect Information Systems Success? The Role of Transformational Leadership," *Information and Management*, Vol.48, No.7(2011), pp.270-277.

[10] D'Arcy, J., A. Hovav, and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse : A Deterrence Approach," *Information Systems Research*, Vol.20, No.1(2009), pp.79-98.

[11] Deng, X., W.J. Doll, S.S. Al-Gahtani, T.J. Larsen, J.M. Pearson, and T.S. Raghunathan, "A Cross-Cultural Analysis of the End-User Computing Satisfaction Instrument : A Multi-Group Invariance Analysis," *Information and Management*, Vol.45, No.4(2008), pp.211-220.

[12] Fornell, C. and D.F. Larcker, "Evaluating Structural Equation Models with Unobserva-

ble Variables and Measurement Error," *Journal of Marketing Research*, Vol.18, No.1(1981), pp.39-50.

[13] Gallagher, S.E. and T. Savage, "Cross-Cultural Analysis in Online Community Research : A Literature Review," *Computers in Human Behavior*, Vol.29, No.3(2013), pp.1028-1038.

[14] Gefen, D. and D. Straub, "A Practical Guide to Factorial Validity Using PLS Graph : Tutorial and Annotated Example," *Communications of the Association for Information Systems*, Vol.16, No.5(2005), pp.91-109.

[15] Gefen, D., E. Karahanna, and D. Straub, "Inexperience and Experience with Online Stores : The Importance of TAM and Trust," *IEEE Transactions on Engineering Management,* Vol.50, No.3(2003), pp.307-321.

[16] Gewald, H. and J. Dibbern, "Risks and Benefits of Business Process Outsourcing : A Study of Transaction Services in the German Banking Industry," *Information and Management*, Vol.46, No.4(2009), pp.249-257.

[17] Hovav, A. and J. D'Arcy, "Applying and Extended Model of Deterrence Across Cultures : An Investigation of Information Systems Misuse in the U.S. and South Korea," *Information and Management*, Vol.49, No.2(2012), pp.99-110.

[18] Jacobs, B.A., "Deterrence and Deterrability," *Criminology*, Vol.8, No.2(2010), pp.417-441.

[19] Jung, D.I., C. Chow, and A. Wu, "The Role of Transformational Leadership in Enhancing Organizational Innovation : Hypotheses and Some Preliminary Findings," *The Leadership Quarterly*, Vol.14, No.4/5(2003), pp.525-544.

[20] Kotulic, A.G. and J.G. Clark, "Why There aren't More Information Security Research Studies," *Information and Management*, Vol. 41, No.5(2004), pp.597-607.

[21] Ku, Y.C., R. Chen, and H. Zhang, "Why Do Users Continue Using Social Networking Sites? An Exploratory Study of Members in the United States and Taiwan," *Information and Management*, Vol.50, No.7(2013), pp.571-581.

[22] Lerner, J.S. and P.E. Tetlock, "Accounting for the Effects of Accountability," *Psychological Bulletin*, Vol.125, No.2(1999), pp.255-275.

[23] Li, Y., C.H. Tan, and H.H. Teo, "Leadership Characteristics and Developers' Motivation in Open Source Software Development," *Information and Management*, Vol.49, No.5(2012), pp.257-267.

[24] Lowry, P.B., G. Moody, A. Vance, M. Jensen, J.L. Jenkins, and T. Wells, "Using an Elaboration Likelihood Approach to Better Understand the Persuasiveness of Website Privacy Assurance Cues for Online Consumers," *Journal of the American Society for Information Science and Technology*, Vol.63, No.4(2012), pp.755-766.

[25] Mulgan, R., "'Accountability' : An Ever-Expanding Concept?," *Public Administration*, Vol.78, No.3(2000), pp.555-573.

[26] Parker, D.B., *Fighting Computer Crime : A New Framework for Protecting Information*, Hoboken, NJ : Wiley, 1998.

[27] Scholten, L., D.V. Knippenberg, B. Nijstad, and C.D. Dreu, "Motivated Information Processing and Group Decision-Making : Effects of Process Accountability on Information Processing and Decision Quality," *Journal of Experimental Social Psychology*, Vol.43, No.4 (2007), pp.539-552.

[28] Sedikides, C., K.C. Herbst, D.P. Hardin, and G.J. Dardis, "Accountability as a Deterrent to Self-Enhancement : The Search for Mechanisms," *Journal of Personality and Social Psychology*, Vol.83, No.3(2002), pp.592-605.

[29] Seron, C., J. Pereira, and J. Kovath, "How Citizens Assess just Punishment for Police Misconduct," *Criminology*, Vol.44, No.4(2006), pp.925-960.

[30] Shao, Z., Y. Feng, and L. Liu, "The Mediating Effect of Organizational Culture and Knowledge Sharing on Transformational Leadership and Enterprise Resource Planning Systems Success : An Empirical Study in China," *Computers in Human Behavior*, Vol. 28, No.6(2012), pp.2400-2413.

[31] Tadmor, C. and Tetlock, P.E. Accountability, In D. Matsumoto(ed.), *The Cambridge Dictionary of Psychology*, Cambridge : Cambridge University Press, 2009.

[32] Tand, H.T. and A. Kao, "Accountability Effects on Auditors' Performance : The Influence of Knowledge, Problem-Solving Ability, and Task Complexity," *Journal of Accounting Research*, Vol.37, No.1(1999), pp.209-223.

[33] Tetlock, P.E. Accountability Theory : Mixing Properties of Human Agents with Properties of Social Systems, In L.L. Thompson, J.M. Levine, and D.M. Messick(eds.), *Shared Cognition in Organizations : The Management of Knowledge*, Hillsdale, NJ : Lawrence Erlbaum, (1999), pp.117-137.

[34] Tetlock, P.E., L. Skitka, and R. Boettger, "Social and Cognitive Strategies for Coping with Accountability : Conformity, Complexity, and Bolstering," *Journal of Personality and Social Psychology*, Vol.57, No.4(1989), pp.632-640.

[35] Vance, A., P.B. Lowry, and D. Eggett, "Using Accountability to Reduce Access Policy Violations in Information Systems," *Journal of Management Information Systems*, Vol.29, No.4(2013), pp.263-289.

[36] Vatanasombut, B., M. Igbaria, A.C. Stylianou, and W. Rodgers, "Information Systems Continuance Intention of Web-Based Applications Customers : The Case of Online Banking," *Information and Management*, Vol.45, No.7 (2008), pp.419-428.

[37] Willison, R. and M. Warkentin, "Beyond Deterrence : An Expanded View of Employee Computer Abuse," *MIS Quarterly*, Vol.37, No.1(2013), pp.1-20.

[38] Zhang, J., B.J. Reithel, and H. Li, "Impact of Perceived Technical Protection on Security Behaviors," *Information Management and Computer Security*, Vol.17, No.4(2009), pp. 330-340.

[39] Zhao, X. and M.E. Johnson, "Managing Information Access in Data-Rich Enterprises with Escalation and Incentives," *International Journal of Electronic Commerce*, Vol.15, No.1 (2010), pp.79-112.

〈부록〉 설문 문항

연구변수		측정항목	
보안 대책	절차적 대책	우리 조직은 …	
		sc1	이메일 사용을 설명하는 구체적인 가이드라인이 있다.
		sc2	컴퓨터 자원의 사용을 위한 행동 규칙을 구축하고 있다.
		sc3	사용 권한이 없는 컴퓨터 시스템에 접근하는 것에 대한 직원을 금지하는 공식적인 정책을 가지고 있다.
		sc4	직원에게 컴퓨터와 정보보안 문제에 대한 그들 인식 개선에 도움을 주는 훈련을 제공한다.
		sc5	직원들이 인증되지 않은 방법으로 컴퓨터 데이터 수정의 결과에 대해 브리핑을 한다.
		sc6	직원들의 그들 컴퓨터 보안 책임/의무에 대한 교육을 한다.
		sc7	직원들은 사용 권한이 없는 컴퓨터 시스템 접근의 결과에 대한 설명을 한다.
	기술적 대책	우리 조직은 …	
		sc8	직원에 의한 컴퓨터 데이터의 수정이나 변경을 모니터링 한다.
		sc9	직원들이 명시적으로 권한이 부여된 작업을 수행하는 것을 보장하기 위해 컴퓨터 활동을 모니터링 한다.
		sc10	직원의 컴퓨팅 활동의 로그기록에 대한 평가를 한다.
		sc11	컴퓨터에 인증되지 않은 소프트웨어 사용을 감지하는 정기적인 감사를 실시한다.
		sc12	적극적으로 직원의 이메일 메세지의 내용을 모니터링 한다.
변혁적 리더십	이상화된 행동	우리 조직의 최고 경영자는 …	
		tl1	우리에게 자신의 가장 중요한 가치와 신념에 대해 명확히 표현한다(이메일, 포럼 등을 통하여).
		tl2	우리에게 IT 보안에 대한 강력한 목적의식을 가지는 것의 중요성을 구체화 한다.
	영감적 동기부여	우리 조직의 최고 경영자는 …	
		tl3	IT 보안과 관련된 미래에 대해 낙관적으로 이야기 한다.
		tl4	IT 보안에 대한 강력한 비전을 분명하게 말한다.
	지적 자극	우리 조직의 최고 경영자는 …	
		tl5	문제를 해결할 때 우리로부터 상이한(서로 다른) 관점/의견을 구한다.
		tl6	IT 보안의 오래된 문제에 대해 새로운 기능성을 개발하는 새로운 방법을 제시한다.
	개별화된 배려	우리 조직의 최고 경영자는 …	
		tl7	각 직원들이 타인과는 다른 필요성, 능력 및 영감을 가지고 있다고 여긴다.
		tl8	각 직원들이 자신의 강점을 개발하도록 돕는다.
금융 IT 보안책임 증가		우리 조직 전반의 …	
		acct1	모든 시스템은 고유한 사용자 계정을 가지고 있다(식별 가능성).
		acct2	모든 시스템은 사용자의 현재 동작 내역을 기록하고 살펴볼 수 있다(로깅 인식).
		acct3	시스템은 모든 사용자 활동을 종합적으로 감사를 실시한다(평가 우려).
		acct4	시스템은 다른 사용자의 행동을 볼 수 있도록 설정되어 있다(전자적 영향력).
금융 IT 보안위험 감소		우리 조직의 IT 보안에 대한 …	
		ris1	위험을 감지하기 위해 시스템 및 모니터링이 잘 실행되고 있다.
		ris2	투자(인적, 기술적)가 예전에 비해 높아졌다.
		ris3	접근성이 강화되었다.
		ris4	내부 및 외부의 위협요소(해킹, 바이러스, 유출)가 상당히 감소되었다.
		ris5	직원교육이 정기적으로 이루어지고 있다.
		ris6	의무 및 규율이 잘 지켜지고 있다.
기업성과		동종업계 경쟁사 평균 수준과 비교하여 …	
		fp1	업무 생산성의 향상 정도가 높다.
		fp2	기업 경쟁력 향상 정도가 높다.
		fp3	종합 고객만족도가 높다.
		fp4	기존 고객 유지율이 높다.
		fp5	상품 및 서비스의 질이 좋다.
		fp6	주 고객층 사이에서 평판이 좋다.
		fp7	비용구조의 개선 정도가 높다.