

## BSC 관점에 의한 정보보호 투자효과 분석

공희경<sup>a</sup>, 김태성<sup>b</sup>

<sup>a</sup>충북대학교 경영정보학과 박사과정  
361-763 충북 청주시 흥덕구 개신동 12번지  
Tel: 043-276-3343, Fax: 043-273-2355, E-mail: konghk@paran.com

<sup>b</sup>충북대학교 경영정보학과 부교수  
361-763 충북 청주시 흥덕구 개신동 12번지  
Tel: 043-261-3343, Fax: 043-273-2355, E-mail: kimts@chungbuk.ac.kr

### Abstract

정보사회의 도래와 인터넷의 확산으로 정보보호의 중요성이 증가함에 따라 기업과 조직에 있어서 정보보호는 경쟁적 우위를 확보하기 위한 도구입과 동시에 비즈니스를 안정적으로 수행하기 위한 필수 경영요구사항으로 등장하고 있다. 또한 기업자산의 일원으로써 보호되어야 하는 유·무형 정보자산의 가치는 더욱 높아지고 있으며, 이를 관리하는 조직과 기업의 효율적이고 효과적인 정보자산 관리 및 정보보호 투자에 대한 중요성이 부각되고 있다. 그러나 조직의 정보보호 투자가 증가함에도 불구하고 이에 대한 성과측정을 위한 체계적 방법이 제시되지 않아 정보보호 투자 의사결정 및 개선방향 도출에 어려움이 있다. 기존의 재무적 측면위주의 정보보호 투자효과 분석은 정보보호 투자의 기회비용적인 특징으로 인해 체계적인 효과 분석 및 현황을 파악하기에는 부족하며 향후 정보보호 투자의 전략추진방향을 제시하기 어렵다. 본 논문에서는 정보보호 투자효과의 특성을 고려하여 균형성과표(Balanced Scorecard, BSC)관점의 정보보호 투자 전략과 성과에 대한 인과관계를 분석하고자 한다. 따라서 기존 정보보호 투자효과 분석의 선행연구를 중심으로 핵심성공요인과 측정지표를 도출하고, 관련 기업 및 조직을 대상으로 설문조사를 통해 수집된 자료를 구조방정식모형(Structural Equation Model, SEM) 분석기법을 활용하여 실증분석 하고자 한다.

**Keywords:** BSC, 정보보호 투자효과, 구조방정식모형

### 1. 서론

최근 기업의 가치기준이 유형자산에서 무형자산 중심으로 변화됨에 따라 기업자산의 일원으로써 보호되어야 하는 정보자산의 가치는 더욱 높아지고 있으며, 이를 관리하는 조직과 기업의 효율적이고 효과적인 정보자산 관리의 중요성 및 정보보호 투자에 대한 중요성이 부각되고 있다. 또한 유비쿼터스 정보환경의 다양한 위협에 대응

하기 위해서는 정보보호 투자와 활동의 폭을 넓혀야 한다는 요구가 증가하고 있다. 더불어 정보보호 관련 사고의 발생 건수가 증가함에 따라 국내·외적인 법적 요구사항이 증가하고 있어 기업에 있어서 정보보호 관리는 필수적 분야로 인식되기 시작했다. 이처럼 정보보호 중요성에 대한 인식이 확산되고 있음에도 불구하고 정보보호에 대한 적절한 투자가 이루어지지 않아 효과적인 정보보호 시스템 구현이 지연되고 있다. 또한 정보보호 성과측정을 위한 체계적 방법도 제시되지 않고 있어 정보보호 투자 의사결정 및 정보보호 개선 방향 도출에 어려움이 있다.

정보보호에 대한 적절한 투자가 이루어지지 못하는 이유는 의사결정자들에게 정보보호에 대한 객관적인 정당성이 충분히 제시되지 않았기 때문이다. 막연한 공포전술(threat tactics)에 기인한 정보보호 투자는 그 효과에 대한 정당화 논리를 뒷받침하기 어렵다[김정덕과 박정은, 2003]. 이는 정보보호에 대한 투자를 조직을 운영하기 위한 비용으로만 인식하게 하는 결과를 초래하게 된다. 또한 체계적인 정보보호 투자효과 분석 방법론 부재로 인해 정보보호 투자효과를 객관적으로 예측하거나 투자 의사결정을 하는데 어려움이 있다. 정보보호 투자 성과는 정보화 투자 성과와 같이 재무적 성과, 즉 정보보호 사고로 인한 손실의 방지와 같은 금전적 성과로만 평가하기에는 어려움이 있다. 따라서 정보보호 투자효과를 재무적으로만 반영하기에는 정보보호 투자의 특성상 여러 한계가 도출되고 있다. 대개 기업의 정보보호 투자 전략은 정보보호 시스템 도입에 따른 기업 이미지 향상과 불확실한 발생 가능성을 고려한 보안 사고에 대비한 보험 역할 등의 전략 수립 방식이 활용되고 있다. 이렇듯 대다수의 정보보호 투자 전략은 타당성 및 전략 간 인과관계에 대한 명확한 규명 없이 수립되고 있다. 따라서 본 연구에서는 정보보호 투자효과의 특성을 고려한 BSC 관점의 투자 전략과 성과에 대한 인과관계를 분석하고자 한다.

먼저 정보보호 투자 전략과 비전을 성취하기 위한 재무관점의 경영성과 목표를 설정한다. 다음 단계로 재무관점의 경영성과 목표를 성취하기 위하여 고객 관점에서

고객 만족도 증가에 대한 목표를 설정한다. 그 다음 고객 만족도 증가 목표를 달성하기 위해 내부 비즈니스 프로세스 관점에서 업무연속성 보호 및 자산위험 관리에 대한 목표를 설정한다. 마지막으로 성장 및 학습 관점에서 내부 프로세스 향상 목표의 선행 동인으로 정보보호 기술적·인적 인프라 구축을 목표로 설정한다. 이처럼 Top-Down 방식으로 구축된 BSC 모델은 각 관점의 목표가 인과관계에 의해 연결된다고 가정한다[Kaplan and Norton, 2001]. 예를 들면, 정보보호의 기술적·인적 인프라 구축은 기업 및 조직의 자산위험을 감소시키고, 업무를 연속적으로 지속시킴으로 내부 프로세스 관점의 목표 측정치를 개선하여 고객 만족도를 높이고, 높아진 고객 만족도는 기업 이미지 향상 및 고객 불평 감소 등을 개선하거나 재고함으로써 재무목표 달성에 연결된다고 가정한다. 그러나 이러한 인과관계에 대한 가정이 실증적으로 지지되지 않는 정보보호 투자 전략은 기업 및 조직의 입장에서 불확실성이 높은 모험적 시도가 될 수 있다.

본 연구의 목적 달성을 위해 정보보호 투자효과 분석에 관한 선행연구를 중심으로 BSC 관점에서 전사적 차원의 정보보호 투자 전략을 수립한다. 이렇게 수집된 전략을 구조방정식모형을 활용하여 정보보호 투자 전략과 투자 성과 간의 인과관계를 파악함으로써 해당 전략의 타당성을 검증하고자 한다. 아울러 이미 정보보호 투자 전략을 수립하여 실행하고 있는 기업 및 조직에게 기존에 수립된 자사의 정보보호 투자 전략의 타당성 검토 및 투자 성과측정을 위한 과학적 도구로서의 BSC 를 제시하고자 한다. 이를 통해 정보보호 투자효과 분석을 위한 정성적·정량적 효과(재무지표와 비 재무지표)간의 인과관계 분석을 위한 모형을 개발하고자 한다.

## 2. 연구의 이론적 배경

### 2.1 정보보호 투자효과 분석에 관한 선행연구

투자는 투자에 따른 효과예측과 이에 대한 객관적인 평가가 수반된다. 정보보호 분야도 예외는 아니어서 기업이 정보보호에 대한 투자를 추진하고 이에 대한 의사결정 시 투자효과 분석과 객관적인 평가가 요구되고 있다. 시간이 지날수록 정보보호 분야에 있어 인간 행동의 중요성이 종종 기술적인 측면의 중요성을 뛰어 넘게 됨에 따라, 정보보호를 위한 적정 투자수준, 정보보호 이슈에 대한 정보공유 문제, 정보보호 문제를 해결하기 위한 유인체계의 정립 등의 경제적인 접근 방법들의 중요성이 새롭게 부각되고 있다. 정보보호에 대한 사회·경제적 연구의 필요성에 대해 Soo Hoo[2000]는 보험산업과 기업에서 정보보호 문제 연구의 필요성을 분석하고 효율적인 투자규모와 효과 분석에 대한 논의의 필요성을 제기하였다. Gordon et al.[2002], Gal-Or and Ghose[2003], 신일순[2005] 등의 사회과학자들 뿐만 아니라 전통적인 의미의 정보보호 전문가로 볼 수 있는 Odlyzko[2003], Anderson et al.[2001]은 정보보호의 문제들에 대한 수학적인 암호의 결함보다는 정보보호에

대한 사회·경제적 연구의 필요성을 강조하였으며, 효율적인 투자 규모와 효과 등에 대한 논의의 필요성을 제기하였다. Gordon and Loeb[2002]는 순현재가치(NPV) 모형을 이용하여 정보보호 투자효과를 분석하였으며, Cavusoglu et al.[2002]는 게임이론을 통해서 정보보호 영역의 경쟁자간 자산보호와 공격자간의 적정 평형점에서 정보보호 수준과 이를 위한 투자가 결정됨을 제시하였다[신일순, 2005]. 카네기멜론 대학교와 아이다호 대학은 정보보호 투자효과 분석에 관한 여러 변수를 이용하여 ROSI(Return on Security Investment)를 도출하는 방식을 제시하였다[김정덕과 박정은, 2003]. 그러나 이들 연구들은 관련 데이터의 수집 용이성 문제와 정보보호 효용성의 정량화 문제, 정보보호 비용에 대한 구체적인 산출방식의 부재로 실제 적용에는 한계가 있다. 이러한 한계를 극복하기 위해 김정덕, 박정은[2003]과 이종선, 이희조[2007]는 TCO(Total Cost of Ownership)에 기반을 둔 개선된 ROSI 방법을 제시하였다. 또한 Berinato[2002], Al-Humaigani and Dunn[2003], Tsiakis and Stephanides[2005], Hausken[2006], Davis[2005] 등도 정보보호 투자에 대한 경제성 평가를 ROSI 등으로 정의하고 정보보호 투자의 비용과 정보보호 효과의 상관관계를 수학적 모델링을 통하여 접근하였다. Blatchford[1995], Lee[2003], Cavusoglu et al.[2004a, 2004b]는 정보보호 투자 시 고려해야 할 여러 요인들을 분류하였다. Bodin et al.[2005], Scott[1998], Scott[2002] 역시 정보보호에 대한 투자 기준을 제시하고, 정보보호에 대한 투자는 일반적으로 장기적 측면의 보장적 성격이 강하므로 장기적 위험은 줄여주지만 단기적으로 정량적인 투자효과를 제공해주지 못하는 경우가 많음을 제시하였다. Blakely[2001], Witty et al.[2001], Harris[2001], Roper[1999], 선한길[2005] 또한 정보보호 투자에 대한 비용요인을 분류하였다. 홍기향[2003]은 정보보호 관리 수준을 측정하고 정보보호 노력이 조직에 미치는 영향을 분석하였다. 남상훈[2005]은 기업의 보안사고가 주식가격에 미치는 영향의 분석을 통해 정보보호 투자효과를 분석하였다. 권영옥, 김병도[2007]은 사회과학연구방법의 일종인 사건연구방법론을 통해, 기업 시장가치의 변화를 이용하여 정보보호 투자효과를 정량적으로 측정하였다.

### 2.2 정보보호 투자효과 분석을 위한 고려사항

투자효과를 분석하고 평가하는 것은 조직의 활동 상황 및 조직자산을 체계적으로 측정하고, 조직의 전략적 계획 수립을 가능하도록 하며, 조직의 장기적이고 무형적인 효과까지 다차원적으로 평가할 수 있어야 한다. 특히, 정보보호 투자효과 분석에서는 다음과 같은 사항이 고려되어야 한다[남상훈, 2006]. 첫째, 정보보호 투자효과 측정의 시간적 제약 특성이다. 정보보호 투자는 현재의 자산 가치 보존에 국한되어 있는 것이 아니라, 미래의 가치를 보존하기 위한 관점으로 고려되어야 한다. 둘째, 정보보호 투자효과 무형성이다. 정보보호는 비용과 편익에 무형적 요소가 많아 이를 파악하기 힘들고 파악되었다

할지라도 화폐가치로의 변환이 어렵다. 셋째, 정보보호 투자효과의 다면성이다. 이는 정보보호 투자효과는 질적인 측면과 양적인 측면이 동시에 존재하기 때문에 측정이 어려움이 많다는 것이다. 넷째, 정보보호 투자효과의 불명확성이다. 정보보호 투자의 성과측정 범위가 매우 광범위하며, 기존 설정된 조직의 목표와 연계하여 평가하기에는 어려움이 존재한다. 따라서 정보보호의 투자효과를 조직이나 기업의 경영활동에서 피드백 시킬 수 있는 구조를 통해 정보보호 투자의 타당성을 검증할 수 있는 분석체계의 개발이 필요하다.

### 2.3 BSC의 개요 및 CSF 및 KPI의 인과관계

BSC는 1992년 미국 하버드대학의 Kaplan과 Norton 교수에 의해 창시된 전략경영기법(Strategic Enterprise Management, SEM)이다. BSC는 가치경영(Value Based Management, VBM), 활동기준원가관리(Activity Based Costing/Management, ABC) 등과 함께 전략경영기법의 핵심내용이다[Kaplan and Norton, 1992]. 이상헌[2003]은 BSC란 기업과 조직의 재무적 측정지표와 비재무적 측정지표를 함께 반영하여 기업의 과거성과를 측정하고 현재와 미래의 기업 가치를 평가하는 전략적 성과 및 가치평가 기법이라고 정의하였다. 또한 BSC는 재무적 성과와 비재무적 성과측정을 통한 전략 실행의 관리 도구이자 조직 내 커뮤니케이션 도구 및 무형자산의 관리 도구로 정의할 수 있다[Kaplan and Norton, 1992]. 기존의 재무적 성과지표 중심의 성과평가는 무형자산의 비중이 커지고 있는 현대의 기업에 있어 적합하지 못하며, 유형자산만으로 기업의 가치를 평가하기에는 한계를 가지고 있다. 직원들의 지식, 고객관계 그리고 조직에 많은 가치를 창출해 주는 혁신과 변화 등으로 나타나는 무형자산이 기업을 이끌어가는 큰 역량으로써 인정을 받고 있다[Kaplan and Norton, 2001].

BSC는 이러한 기업이 가지고 있는 무형자산을 평가할 수 있는 도구로서 기업 전략과 비전을 구체화하고 그 비전과 전략을 성공적으로 수행하기 위한 핵심성공요인(Critical Success Factor, CSF)을 측정할 수 있는 핵심 성과지표(Key Performance Indicator, KPI)를 공유함으로써 전략의 실행력을 최대화할 수 있다[Kaplan and Norton, 1996]. Heskett 등은 Progressive 보험사, Southwest 항공사, MCI사 및 Taco Bell사와 같은 서비스 조직을 성공하게 만든 요인이 무엇인가에 대한 포괄적인 연구에서 밝힌 이익사슬에서 무형적 측정지표(예: 직원의 사기 또는 고객 만족도)의 개선으로부터 유형적 측정지표(예: 보다 높은 투자자본 수익률)가 도출됨을 보여주고 있다고 주장하였다[Kaplan and Norton, 1996].

## 3. 연구모형 및 가설설정

### 3.1 연구모형 설계

본 연구에서는 선행연구를 중심으로 하는 문헌연구와 관련 업체를 대상으로 하는 실증분석을 병행하여 연구를 수행하고자 한다. 먼저 문헌연구를 중심으로 정보보호 투자효과 분석에 대한 일반적 개념을 고찰하여 본 연구의 대상이 되는 정보보호 투자 전략의 정의를 명확히 하고자 한다. 본 연구는 기업들의 경영환경변화에 능동적으로 대응하기 위한 정보보호 투자 전략 수립 방법론의 제시와 수립된 전략의 타당성 검증에 목적을 두고 있다. 따라서 본 연구의 대상이 되는 정보보호 투자 전략은 기존에 정보보호 투자를 하고 있는 기업의 정보보호 투자 전략을 그 연구 범위로 한다.

정보보호 투자효과 분석에 관한 선행연구를 통해 정보보호 투자 CSF와 KPI를 도출하여 기업의 정보보호 투자 전략 수립 시 고려해야 하는 이론적 근간이 되도록 한다. 선행연구를 통해 도출된 정보보호 투자 전략 CSF 및 KPI를 BSC의 네 가지 관점(재무, 고객, 내부 프로세스, 학습 및 성장)에 대응하여, 전사적 차원의 정보보호 투자 전략을 수립한다. 이렇게 수립된 전략을 BSC 인과관계 다이어그램에 기반하여 연구모형과 연구가설로 제시하고자 한다. 실증분석에는 기존에 정보보호에 대한 투자를 수행하고 있는 우리나라 기업을 대상으로 설문조사를 통해 자료를 수집하고, 수집된 자료를 구조방정식 모형 분석기법을 활용하여 연구모형의 적합성 평가 및 연구가설을 검증한다. 실증분석을 위해서는 각 변수 별 특성이 반영되도록 Likert 5 점 척도로 작성된 설문조사를 실시하고, Amos 7.0을 사용하여 연구모형을 분석하고자 한다. 이러한 실증분석 결과를 바탕으로 BSC를 활용한 정보보호 투자 전략의 수립 및 단계적 투자 전략 추진방안을 제시하고자 한다.

본 연구의 경우 CSF는 기업이 정보보호 투자를 통해 달성하고자 했던 목표를 성취할 수 있도록 하는 '기업 정보보호 투자 전략'을 의미한다고 할 수 있다. 따라서 CSF는 실증분석에서의 이론변수에 해당한다. 또한 KPI는 CSF보다 상세한 기업차원의 '세부 정보보호 투자 전략'을 의미하며, 기업이 현재의 경영성과뿐만 아니라 미래의 가치를 증대시키기 위해서 관리해야 하는 것들을 계량적 수치를 통해 객관화 한 것을 의미한다. 따라서 KPI는 실증분석에서의 측정변수에 해당된다. 본 연구에서는 문헌 연구를 통해 BSC의 관점 별 성과측정 지표를 도출해 구성하였다. 각 관점은 BSC 연구에서 가장 널리 활용되고 있는 4가지 관점을 적용하였으며, BSC 관련 문헌과 정보보호 투자효과 분석 및 성과평가 관련 문헌을 중심으로 CSF와 KPI를 구성하였다.

재무 관점은 정보보호 투자에 대한 화폐적 가치에 대한 평가로 기존의 정보보호 투자 경제성 분석 연구에서의 지표들을 인용한 것이 상당수이다. 정보보호에 대한 경제적인 접근은 정량화된 데이터를 기초로 하지만 정보보호와 관련된 보안사고 및 장애 관련 정보가 전사적으로 측정되고 관리되기 위해서는 많은 현실적인 문제를 가지고 있다. 정보보호의 문제점들은 보안사고 및 장애 등이 정상적으로 보고되고 관리되지 못하고 있는 실정이다. 그 이유는 보안사고로 인해 기업의 주가와 기업 이미지

에 부정적 영향을 미치고, 타 경쟁사가 이를 악용하기 때문이라고 볼 수 있다. 그러나 기업 내에선 정보보호 투자의 경제적 접근을 위해 전사적 부문에서 발생하는 정보보호의 사고와 장애가 체계적으로 보고되고 관리되어야 한다. 남상훈[2005], 권영욱과 김병도[2007]에 의하면 정보보호 사고가 주식가격에 미치는 영향을 보안사고 및 장애로 구분하여 평가하고 그 결과를 비교하였다. 또한 정보보호 투자의 효과는 정보시스템과 같이 그 자체가 기업경영의 직접적인 성과라기보다는 간접적으로 조직의 목표를 달성하도록 지원하는 역할을 하므로, 기업 및 조직 전략의 지원체계, 기업 및 조직 구조의 변화와 같이 조직적 단위 효과라고 여겨지는 비계량적 지표도 포함된다. 따라서 본 연구에서는 재무적 관점에 주식시세 및 재무가치를 측정지표로 포함하였다.

고객 관점은 제공된 정보보호 시스템을 사용하는 사용자 관점으로 기업의 내·외부 사용자를 고객으로 포함한다. 사용자 관점의 지표는 사용자 만족도의 지표를 사용하게 되는데, 이는 정보보호 투자를 통해 정보시스템 이용이 증가하거나 정보보호 투자를 통한 고객의 불평이 감소하는 정도 등을 고객 만족도 지표로 측정하고자 한다.

내부 프로세스 관점은 정보보호 투자를 통해 정보시스템 제품 및 서비스 제공의 효율성과 효과성을 다루었다. 여기서는 업무연속성 보호 측면에서 일반직원 및 정보보안 관리 직원의 생산성 향상 같은 효율성 측면을 다루고 있다. 또한 정보자산의 보호를 통해 절감되는 비즈니스 손실 경감 및 장애발생 시간 단축, 보안사고 감소율 등 정보자산의 비용 절감적 측면과 정보자산의 보호 및 정보시스템 품질유지 등 자산위험 관리 측면을 다루고 있다. 즉, 내부 프로세스 관점은 정보시스템 및 정보자산 관리 및 보호 등에 대한 프로세스 효율성을 측정하는 것이다. 정보보호 투자를 통해 정보시스템과 정보자산을 최대한 보호하며 업무를 영속할 수 있도록 해야 한다. 이를 위해서 내부 프로세스를 최적으로 관리하고 운영상의 성과들을 계속적으로 평가함으로써 효율성을 제고시켜야 한다. 따라서 이와 관련한 측정지표들을 정기적으로 측정하고 관리하여야 할 뿐만 아니라 산업 표준 및 평균과 비교함으로써 생산성을 평가할 수 있어야 한다.

성장 및 학습 관점은 기업 및 조직이 정보보호 기술의 변화에 얼마만큼 대비할 수 있는가를 측정하고 있으며, 다른 세 가지 관점의 성과동인 역할을 하게 된다. 정보보호 지식 및 기술을 가진 인력 육성의 중요성은 대부분의 연구에서 강조되고 있으며 더 나아가서 정보보호 기술적인 문제보다 유인체계에 대한 중요성이 더욱 언급되고 있다. 따라서 정보보호 정책수립 및 기술도입, 관련 인프라 구축이나 정보보호 교육을 통해 사용자의 역량을 강조하거나, 기반기술 수준 또는 신기술을 적용하려는 기업 및 조직문화를 강조하기도 한다.

[표 1]에서 제시하는 각 관점 별 CSF 와 이에 속하는 KPI 는 현업의 정보보호 관련 실무를 담당하고 있는 전문가 그룹을 대상으로 델파이 조사를 통해 그 타당성을 인정받았다. 델파이 조사에 참여한 전문가 그룹은 정보

보호 투자를 하고 있는 기업의 의사결정 권한을 갖고 있는 부서의 최고 담당자 및 실무진과 정보보호 관리 부문의 연구소 및 학계 연구진을 대상으로 2008년 1월 23일부터 2월 15일까지 약 3주간에 걸쳐 실시하였다.

표 1. 정보보호 투자 전략의 BSC 관점 별 CSF와 KPI

관점	핵심성공요인(CSF)	핵심성과지표(KPI)	참고문헌
학습 및 성장	정보보호 기술적·인적 인프라 구축	· 일반직원 보안교육 및 관리 · 정보보안 관리직원 정보보호 교육 및 관리 · 정보보호 기술적 인프라 구축 · 정보보호 전담핵심인력 확보 · 정보보호 신기술 도입건수 · 정보보호 보안 인증 획득 · 정보보호 정책수립과 검토	Blathchford(1995), Lee(2003), 홍기향(2003), Kim and Lee(2005), 선한길(2005), 남상훈(2005)
내부 프로세스	업무연속성 보호	· 일반직원 생산성 향상 · 보안관리 직원 생산성 향상율	Blathchford(1995), Scott(1998), Scott(2002), Harris(2001), 홍기향(2003), Cavusoglu et al.(2004), 선한길(2005)
	자산위험 관리	· 비즈니스 손실 감소 · 경쟁우위 획득 · 업무결손 경감 · 자산손실 감소 · 장애발생시간 감소 · 해킹발생 건수 · 장애 및 해킹 이외 보안사고 감소율 · 정보시스템 취약성 감소율	Blathchford(1995), NIST(1996), Scott(1998), Scott(2002), Harris(2001), Cavusoglu et al.(2004), 홍기향(2003), 선한길(2005)
고객	고객만족도 증가	· 고객 불평 감소율 · 시장 점유율 · 신규고객 확보 및 기존고객 유지율 · 기업이미지 향상도 · 정보시스템 이용 증가율	Scott(1998), Scott(2002), 홍기향(2003), Cavusoglu et al.(2004), 남상훈(2005), Kim and Lee(2005), 선한길(2005), 권영욱(2007)
재무	경영성과 증가	· 직접 손실액 절감율 · 정보보호 사고 보상비 절감율 · 정보보호 유지보수비 절감율 · 주식시세 및 재무가치	Blathchford(1995), NIST(1996), 카네기멜론대학(1988), 아이다호대학(2000), Blakely(2001), Gordon and Loeb(2002), Berinato(2002), Al-Humagani and dunn(2003), Campbell et al.(2003), 김정택(2003), Cavusoglu et al.(2004), Kumar(2004), Davis(2005), Tsiakis and Stephanides(2005), Kim and Lee(2005), Bordin et al.(2005), 남상훈(2005), 권영욱(2007)

본 연구에서 제시하는 CSF 들을 관점 별로 분류하고 각 요인들이 상호 간에 미치는 영향 및 관계를 분석하기 위해 BSC 전략맵의 인과관계를 [그림 1]과 같이 연구모형으로 제시하였다.

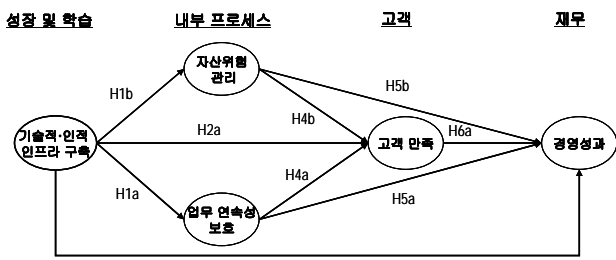


그림 1. BSC 관점의 정보보호 투자효과 분석 연구모형

### 3.2 연구 가설의 설정

본 연구가설은 [그림 1]에서 보듯이 각 관점 사이의 CSF 간 인과관계를 가정하고 이를 토대로 다음과 같은 직·간접 효과의 각 단계로 구성된다. 각 단계의 가설에서는 다시 세부적인 하위 가설이 수립되었다.

가설 1: 성장 및 학습 관점의 성공요인은 내부 프로세스 관점의 성공요인에 정(+)의 영향을 미칠 것이다.

- H1a: 정보보호의 기술적·인적 인프라 구축은 업무연속성 보호에 정(+)의 영향을 미칠 것이다.
- H1b: 정보보호의 기술적·인적 인프라 구축은 자산위험 관리에 정(+)의 영향을 미칠 것이다.

가설 2: 성장 및 학습 관점의 성공요인은 고객 관점의 성공요인에 정(+)의 영향을 미칠 것이다.

- H2a: 정보보호의 기술적·인적 인프라 구축은 고객만족도에 정(+)의 영향을 미칠 것이다.

가설 3: 성장 및 학습 관점의 성공요인은 재무 관점의 성공요인에 정(+)의 영향을 미칠 것이다.

- H3a: 정보보호의 기술적·인적 인프라 구축은 경영성과에 정(+)의 영향을 미칠 것이다.

성장 및 학습 관점의 성공요인은 정보보호 기술적·인적 인프라 구축으로 이를 통해 내부 프로세스 향상을 제고시키는 동인이 된다. 본 연구에서는 내부 프로세스 향상을 정보보호 투자효과 관점에서 업무연속성 보호와 자산위험 관리로 구분한다. 이론적으로 성장 및 학습 관점의 성공요인들이 내부 프로세스 관점에 정(+)의 영향을 주는 것으로 예상할 수 있다. 성장 및 학습 관점은 지속적인 정보보호 교육 및 투자로 인해 학습과 성장의 토대를 구축하는 것으로 정보보호의 미션을 달성하기 위한 1차적인 성과동인에 해당한다. 이러한 성과동인은 직접적

으로는 내부 프로세스 향상에 영향을 주고, 이러한 영향이 직·간접적으로 고객 관점과 재무 관점에 영향을 미치게 되는 것으로 예상할 수 있다. 따라서 정보보호 관련 인력관리 및 전문 지식의 교육 및 관리 등은 실제 업무를 효율적으로 운영하는 있어서 기반 인프라 및 역량으로 작용할 것이다.

가설 4: 내부 프로세스 관점의 성공요인은 고객 관점의 성공요인에 정(+)의 영향을 미칠 것이다.

- H4a: 정보보호 투자를 통한 업무연속성 보호는 고객만족도에 정(+)의 영향을 미칠 것이다.
- H4b: 정보보호 투자를 통한 자산위험 관리는 고객만족도 증가에 정(+)의 영향을 미칠 것이다.

가설 5: 내부 프로세스 관점의 성공요인은 재무 관점의 성공요인에 정(+)의 영향을 미칠 것이다.

- H5a: 정보보호 투자를 통한 업무연속성 보호는 경영성과에 정(+)의 영향을 미칠 것이다.
- H5b: 정보보호 투자를 통한 자산위험 관리는 경영성과에 정(+)의 영향을 미칠 것이다.

내부 프로세스 관점은 고객 관점의 성과에 영향을 미치게 되며, 내부 프로세스 향상 정도는 업무연속성 보호와 자산위험 관리 수준에 의해 측정된다. 본 연구에서 제시하는 내부 프로세스 관점의 성공요인은 정보보호 투자를 통한 업무연속성 보호와 정보자산의 위험 관리로 구분하였다. 이러한 내부 프로세스 관점의 성공요인은 정보보호 투자를 통해 기존 정보시스템 및 정보자산의 위험 관리와 정보보안 사고 및 관련 장애로부터 업무의 연속성을 보호하는 목적이다. 이러한 성공요인은 고객 관점으로 직접적인 영향을 주며, 고객 관점을 통해 재무 관점에도 간접적인 영향을 미치게 된다. 또한 고객 관점을 거치지 않고 직접적으로 재무 관점에 영향을 미칠 수도 있다. 이는 내부 프로세스 향상이 고객 만족도 증가와 경영성과 증가에 영향을 미칠 수 있는 성과동인으로서 정의될 수 있다.

가설 6: 고객 관점의 성공요인은 재무 관점의 성공요인에 정(+)의 영향을 미칠 것이다.

- H6a: 정보보호 투자를 통한 고객 만족도 증가는 경영성과 증가에 정(+)의 영향을 미칠 것이다.

## 4. 실증분석 및 가설검증

### 4.1 자료의 수집

실증분석을 위한 설문조사는 비즈니스 환경에서 정보보호가 중요하게 고려되는 것으로 여겨지는 관련기업으로 은행과 증권업을 포함한 금융업, 홈쇼핑업체, 인터넷 Portal업체 및 SI업체, ISP관련기업, 게임관련기업, 이러닝 관련기업, 의료서비스 관련기업,

국공립 연구소 및 공공기관을 대상으로 전체 표본을 선정하였다. 이와 같은 업체 및 조직을 대상으로 설문조사를 수행한 이유는 연구의 목적이 정보보호 투자효과의 특성을 고려한 BSC 관점의 투자 전략과 성과에 대한 인과관계 규명을 통한 전략의 타당성 검증에 있으므로, 기존에 이미 정보보호 투자를 하고 그 성과에 대한 평가를 수행하고 있는 업체를 대상으로 한 것이다.

정보보호 투자의 성과에 대한 전문성과 정확성을 보유한 응답을 얻기 위해 선정한 표본은 다음과 같다. 우선, 기존에 정보보호에 대한 투자를 이미 하고 있다고 객관적으로 판단되는 조직으로, 정보보안 사고에 대해 대비조직을 보유하고 운영하고 있는 업체들과, 2002년부터 정보통신부에서 주최하는 정보보호 大賞 수상 기업, 정보보안 관련인증인 ISO 27001과 ISMS 인증 획득 기업, 정보보호 실천협의회 소속 회원업체를 포함하였다. 또한 본 연구의 목적인 정보보호 투자의 성과 조사에 부합하도록 정보보호 기술지원이나 정보보호 기술관련 업무 담당자가 아닌 정보보호 투자에 대한 의사결정에 참여하고 그 성과를 분석하고 평가할 수 있는 정보보호 부서의 담당 임·직원을 대상으로 하였다. 설문조사의 방법은 대인면접법(personal interview)과 e-mail, 우편 이용법, 인터넷을 통한 웹(web)설문을 활용하였다. 정보보호 투자에 대한 성과를 측정하고 평가를 수행중인 업체 및 조직 리스트를 종합하여 이를 토대로 600여개 업체 및 조직을 선정하였다. 설문조사는 1차로 2008년 1월 23일부터 2월 15일까지 설문지의 타당성 검토 및 pilot test를 실시한 후 네 가지 관점 별로 학습 및 성장 관점의 7개 항목, 내부 프로세스 관점의 10개 항목, 고객 관점의 6개 항목, 재무 관점의 4개 항목, 응답업체 및 응답자의 현황분석을 위한 8개 문항, 총 35개 항목으로 구성하여, 2008년 2월 18일부터 2008년 3월 24일까지 5주간 2차 본 설문을 측정하였다. 대인 면접법을 제외한 나머지 설문조사에서는 설문 회수율 및 응답내용의 질을 높이기 위해 직접 해당 업체와의 전화를 통하여 설문지의 취지를 설명하고 협조를 요청하였다. 그 결과 배포한 설문지 600부 중 총 133부가 회수되어 회수율은 약 22.1%에 이르렀다.

#### 4.2 경로모형을 이용한 가설 검증

본 연구에서는 이론적 측정모델의 확인적 검증을 위해 각 관점 별 핵심성공요인 및 측정지표를 포함한 전체변수를 대상으로 Amos 7.0을 이용한 확인적 요인분석(confirmatory factor analysis)을 실시하였다. 확인적 요인분석은 이론적인 배경 하에서 변수들 간의 관계를 미리 설정한 후 실제 자료를 통해 가설화된 요인구조를 검증하는 기법이다[유일 외, 2007].

전체 측정모형에 대한 확인적 요인분석을 실시한 결과를 살펴보면 [표 2]에 나타난 바와 같이 측정항목들과 각 구성개념간의 표준 부하량들이 모두

통계적으로 유의하여( $t$ -value>2)들이 측정항목의 집중 타당성(convergent validity)이 있다고 할 수 있다[유일 외, 2007].

본 연구에서는 설문문항 중 F1(X6)을 설문문항 설계의 척도오류로 인해 코딩 변경하였다. F1(X6)은 기업의 보안인증 획득 여부를 묻는 설문문항으로 측정대상이 어느 집단에 속하는지 분류하는 경우에 사용되는 명목척도로 설계되어야 하나, 설문문항 설계 및 본 설문 시 서열을 구분하는 순서척도로 설계되어 실제 연구모형에서는 F1(X6) 문항을 (X6\_1)로 코딩 변경하여 보안인증 획득의 가부를 확인할 수 있는 자료로 변경하였다.

표 2. 전체 구성개념의 확인적 요인분석 결과

연구 변수	측정 항목	표준 부하량	t-value (C.R.)	측정 오차 분산	개념 신뢰도	평균 분산 추출값	Cronbach's $\alpha$
F1	X1	0.863	-	0.34	0.902	0.26	0.897
	X2	0.858	12.981	0.32			
	X3	0.786	10.717	0.425			
	X6_1	0.617	7.653	0.128			
	X7	0.802	11.057	0.456			
F2	Y1	0.899	-	0.186	0.896	0.811	0.889
	Y2	0.89	13.035	0.186			
F3	Y3	0.756	-	0.199	0.940	0.695	0.865
	Y4	0.715	8.043	0.166			
	Y5	0.756	8.387	0.147			
	Y6	0.76	8.603	0.133			
	Y7	0.794	9.05	0.181			
	Y8	0.519	5.708	0.456			
F4	Y11	0.632	-	0.495	0.934	0.741	0.911
	Y12	0.885	8.286	0.148			
	Y13	0.917	8.42	0.112			
	Y14	0.821	7.829	0.29			
F5	Y16	0.883	8.29	0.169	0.865	0.685	0.863
	Y17	0.913	-	0.177			
	Y18	0.927	16.387	0.146			
	Y19	0.664	8.859	0.657			

본 연구에서는 내적 일관성 신뢰도 측정방법인 Cronbach's  $\alpha$  분석을 통해 신뢰성을 분석하였다. 채서일[1995]에 의하면, 설문지의 신뢰도 검증에 가장 많이 사용되는 것이 내적 일관성법의 산출계수인 Cronbach's  $\alpha$  값인데, 동일한 개념을 측정하기 위해 여러 개의 항목을 찾아내어 측정도구의 신뢰성을 높이는 것으로 여러 개의 항목 중 신뢰도를 저해하는 항목을 측정도구에서 제외시킴으로써 신뢰도를 향상시킬 수 있다고 하였다[배병렬, 2007]. 이 과정에서 신뢰도를 저해하는 F3(Y10)과 F4(Y15), F5(Y20)의 측정변수

항목을 각각 1개씩 제거하였다. 본 연구에서는 연구 성격을 고려하여 Cronbach's  $\alpha$  값 0.8 이상을 기준으로 신뢰성 분석을 실시하였다. 요인분석을 통해 추출된 각 요인에 대한 Cronbach's  $\alpha$ 의 측정 결과는 모든 요인이 0.863~0.911의 구간 내에 존재하였다. 따라서 본 연구의 각 항목들도 각 요인들의 신뢰성이 검증되었다고 볼 수 있다.

이상과 같이, 확인적 요인분석을 통해 요인적재량들이 모두 통계적으로 유의한 p 값을 가지는 것으로 나타났다. 따라서 각 구성개념간의 수렴타당도와 단일차원성이 확보되고 있고, 지표의 내적 일관성을 측정하는 각 구성개념에 대한 개념신뢰도가 모든 요인에서 수용가능 수준인 0.8을 상회하고 있어 신뢰도가 확보되었다[유일 외, 2007]. 또한 신뢰도의 다른 측정치로 평균분산추출을 들 수 있는데, 이 측정치는 이론변수에 대해 지표가 설명할 수 있는 분산의 크기로서 0.5이상이어야 신뢰도가 있는 것으로 알려져 있다. 본 연구에서는 모든 요인의 평균분산 추출값이 수용가능 기준을 상회하여 신뢰도에는 이상이 없는 것으로 나타났다[배병렬, 2007].

표 3. 구성개념간의 상관관계 행렬

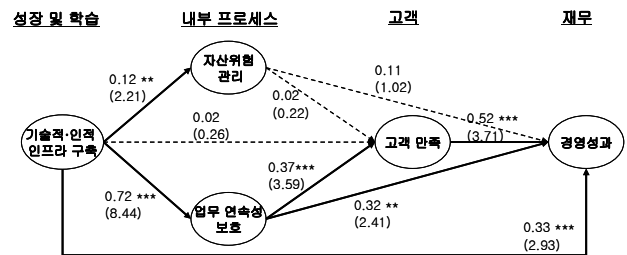
	기술적·인적 인프라 구축	업무연속성 보호	자산위험 관리	고객 만족	경영성과
기술적·인적 인프라 구축	0.807				
업무연속성 보호	0.760	0.901			
자산위험 관리	0.216	0.174	0.901		
고객 만족	0.472	0.591	0.123	0.861	
경영성과	0.688	0.743	0.222	0.651	0.828

※ 모든 상관계수는 0.01수준(양쪽)에서 유의함.

한편, Fornell and Larcker[1981]에 따르면, 각 요인의 추출된 평균분산(average variance extracted, AVE)의 제곱근이 해당요인과 다른 요인간의 상관관계수보다 크면, 해당모형의 판별 타당성(discriminant validity)이 존재하는 것으로 간주한다[이정훈 외, 2007]. 따라서 구성개념 간 판별력을 높이기 위해 다른 구성개념과의 상관관계가 높은 것으로 나타나는 F1(X4), F1(X5) 변수를 제거하였다. 구성개념간의 판별 타당성을 검정하기 위하여 연구모형에 포함된 5개 이론변수들 간의 상관관계를 살펴본 결과, 표 3에 나타난 바와 같이 상관관계수의 95% 신뢰구간에 1.0이 포함되지 않았고, 보다 엄격하게는 평균분산 추출값이 개념들 간 상관관계수의 제곱 값( $\phi^2$ )을 상회하고 있어 구성개념들의 판별 타당성이 있다고 할 수 있다[유일 외, 2007].

모형의 적합도는  $\chi^2$ 값이 작을수록 바람직하고,  $\chi^2$ 에 대한 p값이 0.05보다 작거나 커야 하며, Q값( $\chi^2/df$ )이 2보다 작거나 같아야 바람직하다고 제시하고 있다[엄명용과 김태웅, 2006]. 또한 각 요인 별 항목구성의 최적상태는 원소간 평균차이(root mean-square residual,  $RMR \leq 0.05$ , root

mean-square error of approximation,  $RMSEA < 0.05 \sim 0.08$ ), 표준적합지수(normed fit index,  $NFI \geq 0.9$ ), 비교적합지수(comparative fit index,  $CFI \geq 0.9$ ), 충분적합지수(Turker-Lewis index,  $TLI \geq 0.9$ ), 기초적합지수(goodness-of-fit index,  $GFI \geq 0.9$ ), 조정적합지수(adjusted goodness-of-fit index,  $AGFI \geq 0.9$ )와 같은 적합도 지수를 통해 평가하였다[배병렬, 2007]. 한편, Hair(2003)은 관측변수와 설문지의 수에 따라 통계량이 250개 이하이고, 관측변수의 수가 12개에서 30개 사이인 경우, CFI가 0.95이상이면, RMSEA, RMR 값은 0.08이하 기준으로도 고려가 가능하다고 제시하였다[배병렬, 2007]. 또한 Yu, J.E. et al.[2005]는 기초적합지수( $GFI \geq 0.8$ ), 조정적합지수( $AGFI \geq 0.8$ ) 등과 같은 권장기준을 고려해 모형의 적합도를 평가하였다. 이러한 절차에 따라 확정된 전체 측정모형의 적합도를 확인한 결과,  $\chi^2=298$ ,  $df=199$ ,  $p=0.00$ , Q값( $\chi^2/df$ )=1.499,  $RMR=0.049$ ,  $RMSEA=0.061$ ,  $NFI=0.86$ ,  $CFI=0.94$ ,  $TLI=0.94$ ,  $GFI=0.82$ ,  $AGFI=0.78$ , 등으로 나타나 전반적으로 좋은 적합도를 보였다.



\*\*\*: 1% 유의수준, \*\*: 5% 유의수준.

그림 2. 연구모형의 분석결과

본 연구에서 구조방정식모형 분석을 통해 모형의 적합도와 모수들을 추정하였다. 본 연구에서 분석된 최적 연구모형의 적합도 지수를 살펴보면,  $\chi^2=216$ ,  $df=192$ ,  $p=0.112$ , Q값( $\chi^2/df$ )=1.125,  $RMR=0.44$ ,  $RMSEA=0.030$ ,  $NFI=0.90$ ,  $CFI=0.98$ ,  $TLI=0.98$ ,  $GFI=0.87$ ,  $AGFI=0.83$ 으로 나타나 전반적인 적합도 평가지수에는 문제가 없는 것으로 나타났다. 따라서 제안된 모형이 적합한 것으로 보이며, 본 연구변수들 간의 관계를 추정하는데 문제가 없는 것으로 판단된다. [그림 2]는 연구모형의 AMOS 분석 결과 나타난 경로도형(path diagram)이다.

가설 1a 와 가설 1b 의 경우 성장 및 학습 관점의 정보보호 기술적·인적 인프라 구축이 내부 프로세스 관점의 자산위험 관리와 업무연속성 보호에 유의한 영향을 주는 것으로 나타났다. 가설1의 경우 성장 및 학습 관점의 기술적·인적 인프라 구축이 내부 프로세스 관점의 자산위험 관리보다 업무연속성 보호에 내부 프로세스 향상의 성공요인으로 더 많이 영향을 주는 것으로 나타났다. 반면에 기술적·인적 인프라 구축이 고객 만족에 직접적으로는 유의한 영향을 미치지 않는

것으로 나타나 가설 2a 는 기각되었다. Lee[2003]을 비롯한 여러 선행연구에서 정보보호에 대한 투자는 기술, 인력, 교육, 정책 및 컨설팅과 같은 정보자산의 가용성, 무결성, 기밀성을 보호하기 위한 것이라고 정의하였으며 기업 정보보호 수준 향상으로 직결될 것이라고 주장하였다. 이들의 연구결과는 본 연구결과와 일치하고 있으며, 향후 정보보호 투자 성과평가의 연관관계에 대해 지속적인 연구가 필요한 부분이라고 판단된다.

표 4. 연구가설의 검정결과

가설	경로	경로계수	t 값	수용여부
H1a	기술적·인적 인프라 구축→업무연속성 보호	0.72	8.44***	채택
H1b	기술적·인적 인프라 구축→자산위험 관리	0.12	2.21**	채택
H2a	기술적·인적 인프라 구축→고객 만족	0.02	0.26*	기각
H3a	기술적·인적 인프라 구축→경영성과	0.33	2.93***	채택
H4a	업무연속성 보호→고객 만족	0.37	3.59***	채택
H4b	자산위험 관리→고객 만족	0.02	0.22*	기각
H5a	업무연속성 보호→경영성과	0.32	2.41**	채택
H5b	자산위험 관리→경영성과	0.11	1.02*	기각
H6a	고객 만족→경영성과	0.512	3.71***	채택

내부 프로세스 관점의 자산위험 관리도 고객 만족에 직접적으로 유의한 영향을 미치지 않는 것으로 나타나 가설 4b 도 기각되었다. 또한 자산위험 관리가 재무 관점의 경영성과에도 직접적으로 유의한 영향을 미치지 않는 것으로 나타났다. 그러나 내부 프로세스 관점의 업무연속성 보호가 고객 관점의 고객 만족과 재무 관점의 경영성과에도 직·간접적으로 유의한 영향을 미치는 것으로 나타나 가설 4a 와, 가설5a는 채택되었다. Cavusoglu et al.[2004a, 2004b]는 정보보호 투자 시 기업의 신뢰도 등을 고려해야 한다고 주장하였으며, 경제적 측면에서 관리의 중요성을 언급하였다. 이는 본 연구의 결과와 일치하는 것으로 볼 수 있다. 가설4와 5의 경우 내부 프로세스 관점 중에서 업무연속성 보호의 성공요인만 고객 관점과 재무 관점에 영향을 주는 것으로 나타났다. 이는 내부 프로세스 관점의 성공요인 중에서 자산위험 관리 요인보다는 업무연속성 보호 요인이 보다 많은 영향을 주는 성과동인임을 확인할 수 있다.

세 번째 관점인 고객 관점의 고객 만족은 재무 관점의 경영성과에 유의한 영향을 미치는 것으로 나타났다. 가설 6의 경우 정보보호 투자를 통한 기업 이미지 향상 등의 고객 만족도 증가가 경영성과에 긍정적인 영향을 미치는 것으로 볼 수 있다. 이는 최근 들어 기업들이 경영성과 증가를 위해 정보보호 수준 향상이 선행되어야 함을 인식하고 있다고 볼 수 있다. 고객과의 관계 개선 및 기업 이미지 향상 제고가 점차적으로 경영성과에 영향을 미치게 됨으로 분석할 수 있다.

마지막으로 성장 및 학습 관점의 기술적·인적 인프라 구축이 재무 관점의 경영성과에 직접적으로 유의한 영향을 미치는 것으로 나타나 가설 3a 가 채택되었다.

최근 국내외 기업의 상당수가 정보보호의 신기술 도입과 교육을 통해 자사의 정보보호 수준을 제고하고자 하는 현상을 보이고 있다. 이는 정보보호의 기술적·인적 인프라 구축이 기업 및 조직의 정보보호 성과관리에 있어서 매우 중요한 요소가 되고 있음을 알 수 있다. 또한 Scott[1998]의 연구에서는 정보보호에 대한 투자가 일반적으로 장기적 측면의 보장적 성격이 강하기 때문에 단기적으로 정량적인 투자효과를 제시하기는 어렵다고 했으며, 정보보호의 통제가 부족할 경우에 발생할 수 있는 손실 요인으로 생산성 감소, 이익 감소, 기업이미지 낙후, 금전적 손실 등을 제시하였다[Scott, 2002]. 이는 곧 정보보호 투자가 직접적으로 경영성과로 직결됨과 함께 기업의 전사적 정보보호 수준 향상을 통해 장기적으로 기업 내부의 효율성 향상과 외부의 고객 만족도 증가가 그 성과로 연결된다고 언급하고 있다. 이러한 연구 결과는 본 연구의 결과와 일치하고 있는 것으로 분석할 수 있다.

## 5. 결론

본 연구는 기업 경영환경의 변화로 인해 전사적 차원의 정보보호 전략에 대한 분석도구로서 BSC 를 제시하고자 하였다. 정보보호 투자효과의 특성을 고려하여 BSC 관점의 정보보호 투자 전략을 수립하고 이를 구조방정식모형을 활용하여 정보보호 투자 전략과 성과간의 인과관계를 규명함으로써 BSC 관점의 정보보호 투자 전략의 타당성을 검증하고자 하였다. 이를 위해 우선 BSC 의 인과관계를 모형화하여 각 관점 사이의 인과관계를 몇 가지 유형의 가설로 가정한 후, 이러한 인과관계를 Amos 의 경로모형을 적용하여 실증 분석하였다. 수립된 정보보호 투자 전략을 BSC 인과관계 전략지도로 도출하여 이를 연구모형으로 설정하고, 5개의 CSF 를 이론변수로 27개의 KPI 를 측정변수로 하여 변수간의 인과관계를 분석하고자 하였다. 또한 BSC 연구모형의 경로를 중심으로 9개의 연구가설을 제시하였다.

본 연구의 의의 및 향후 연구과제는 다음과 같다. 본 연구는 정보보호 투자 전략과 관련하여 실무에 적용가능하며, 정보보호 투자 전략의 수립과 실행 및 정보보호 투자 전략 분석도구와 프레임워크로서 BSC 를 제시하고자 하였다. 이를 위해 BSC 관점의 정보보호 투자 전략의 타당성, 즉 전략간 인과관계 및 정보보호 투자 성과에 미치는 영향을 실증분석을 통해 검증하였다. 이를 통해 도출된 결과를 바탕으로 본 연구가 시사하는 바는 다음과 같다.

첫째, BSC 관점의 정보보호 투자 전략은 정보보호 투자 전략간 인과관계가 있으며, 기업의 정보보호 투자 성과 제고에 긍정적인 영향을 준다. 둘째, 이미 정보보호 투자 전략을 수립하여 추진하고 있는 기업들은 수립된 전략의 타당성 평가 및 정보보호 투자 성과측정을 위한 과학적 도구로서 BSC 를 활용할 수 있다. 또한 정보보호 투자 전략의 신규 수립을 위한 과학적 정보보호 투자 전략 수립 방법론으로서 BSC 를 활용할 수 있다.



결론적으로 본 연구의 결과를 종합하면, 기업 및 조직의 정보보호 수준을 높이기 위해서는 무엇보다 학습 및 성장 관점의 기술적·인적 인프라 구축을 통해 자산위험 관리와 업무연속성이 보호되어야 하고 이러한 내부 프로세스 향상의 성공여부는 다음단계인 고객관점의 고객 만족도 증가로 영향을 미친다는 것이다. 또한 기술적·인적 인프라 구축과 함께 고객 만족도가 증가되면 재무관점의 경영성과가 향상될 수 있을 것이라는 결론을 맺을 수 있다.

본 연구는 연구의 의의에도 불구하고 향후 본격적인 실증분석을 위한 탐색적인 연구의 성격이 강하다는 점을 밝힌다. 기존의 선행연구에 의해 정보보호 투자 전략을 수립하였으며 정보보호 투자 전략에 대한 이해가 다소 제한적일 수 있는 대상으로 투자 전략의 타당성을 측정하였다는 점이다. 본 연구 결과는 정보보호에 대한 투자를 이미 수행하고 있거나 진행 중에 있는 업체를 대상으로 설문조사를 수행하였다 하더라도 실제 기업체들은 정보보호 투자에 대한 성과를 제대로 파악하고 분석하기 보다는 기업의 대내외적 이미지나 인증심사 등 일시적으로만 정보보호 수준 제고에 관심이 있음을 반증해 주고 있다. 또한 BSC 관점의 전략 수립과정에서 선행연구를 기반으로 전략을 수립하였기 때문에 현실성 있는 전략이 적절하게 제시되지 못했을 가능성이 있으며, 선행연구에 의존하여 측정변수들을 추출하고 요인을 측정할 수 있도록 설문문항을 구성하였기 때문에 표본으로 선정된 기업들에게 현실성 있는 문항이 적절하게 제공되지 못했을 가능성이 있다.

향후 연구에서는 정보보호 성과평가 업무 담당자, 정보보호 투자 전략 전문가들과의 면담 및 사례분석 등을 통해 보다 현실적이고 구체적인 전략을 제시할 필요가 있다. 또한 지표의 선정에 있어서 현실적인 기업 활동을 분석할 수 있는 보다 실제적인 지표개발이 필요하며, 이를 통해서 정보보호 투자 성과를 보다 정확하게 측정하고 이를 기반으로 한 다양한 인과관계에 대한 연구가 가능할 것이다.

## References

- [1] 김상균, “인터넷 차단 시스템의 경제성 분석에 대한 연구”, *한국컴퓨터정보학회논문지*, 제10권, 제6호, 2005, pp.269-278.
- [2] 김정덕, 박정은, “TCO 기반 정보보호 투자수익률(ROSI)에 대한 연구”, *디지털정책학회 창립학술대회*, 2003, pp.251-261.
- [3] 권영욱, 김병도, “정보보안 사고와 사고방지 관련 투자가 기업가치에 미치는 영향”, *Information Systems Review*, 제9권, 제1호, 2007, pp.105-120.
- [4] 남상훈, “기업 정보보호 투자효과 분석방법에서 보안 Event가 주가가격에 미치는 영향 실증연구”, 고려대학교 박사학위논문, 2006.
- [5] 민경기, “BSC관점에 의한 한국제조기업의 물류전략과 물류성과간의 관계에 관한 연구”, 광운대학교 박사학위논문, 2005.
- [6] 박성욱, 윤종민, “산업연관분석을 이용한 정보보호 산업의 연구개발투자에 대한 경제기여도”, *한국기술혁신학회 춘계학술대회*, 2006, pp.19-29.
- [7] 배병렬, *Amos 7에 의한 구조방정식 모델링*, 도서출판 청람, 2007.
- [8] 선한길, “국내기업의 정보보호 정책 및 조직 요인이 정보보호성에 미치는 영향”, *한국경영정보학회 춘계학술대회*, 2005, pp.1087~1095.
- [9] 신일순, “정보보호의 경제학적 의미에 대한 소고”, *Information Security Review*, 제1권, 제1호, 2005, pp.27-40.
- [10] 엄명용, 김태우, “성별 차이를 중심으로 본 이터닝 만족도 영향요인에 관한 연구”, *경영학연구*, 제35권, 제1호, 2006, pp.51-80.
- [11] 유석천, 이재우, 염정호, “정보보호 부문에 대한 투자모형에 관한 연구”, *정보통신정책연구*, 제8권, 제2호, 2001, pp.17-48.
- [12] 유일, 조건, 박이숙, 소순후, “인터넷쇼핑몰에서 관계지향성 요인이 고객만족과 고객충성도에 미치는 영향”, *Journal of Information Technology Applications & Management*, 제14권, 제2호, 2007, pp.129-149.
- [13] 이상헌, “전자정부 정보화사업 성과측정을 위한 BSC 활용방안”, 한국과학기술원 석사학위논문, 2003.
- [14] 이정훈, 신태수, 임종호, “PLS 경로모형을 이용한 IT 조직의 BSC 성공요인간의 인과관계 분석”, *경영정보학연구*, 제17권, 제4호, 2007, pp.207-228.
- [15] 이종선, 이희조, “TCO기반 Security ROI를 활용한 정보보호 투자성과 평가방법”, *한국정보처리학회 춘계학술대회*, 2007, pp.1125-1128.
- [16] 채서일, *마케팅조사론*, 학현사, 1995.
- [17] 한국정보사회진흥원, *정보보호 투자 추이분석 및 성과연구 최종보고서*, 2007.
- [18] 허종락, “BSC 성과지표간 인과관계 분석”, 계명대학교 박사학위논문, 2003.
- [19] 홍기향, “정보보호 통제와 활동이 정보보호

- 성과에 미치는 영향에 관한 연구” , 국민대학교 박사학위논문, 2003.
- [20] Al-Humaidani, M. and Dunn, D.B., “A Model of Return on Investment for Information Systems Security,” *Circuits and Systems*, Vol.1, 2003, pp.483–485.
- [21] Anderson, Ross, “Why Information Security is Hard—An Economic Perspective,” *Computer Security Application Conference*, 2001, pp.358–365.
- [22] Blakley, B., “Returns on Security Investment: an Imprecise but Necessary Calculation,” *Secure Business Quarterly*, Vol. 1, No.2, 2001, p.27.
- [23] Blatchford, C., “Information Security Controls Are They Cost-effective,” *Computer Audit Journal*, Vol.3, 1995, pp.11–19.
- [24] Bodin, L.D., Gordon, L.A., Loeb, M.P., “Evaluating Information Security Investments Using the Analytic Hierarchy Process,” *Communications of the ACM*, Vol.48, 2005, pp.79–83.
- [25] Cavusoglu, H., Mishra, B.K. and Raghunathan, S., “Optimal Design of IT Security Architecture,” Working Paper, University of Texas at Dallas, 2002.
- [26] Cavusoglu, H.(Hasan), Cavusoglu, H.(Huseyin), Raghunathan S., “Economics of IT Security Management: Four Improvements to Current Security Practices,” *Communications of the Association for Information System*, Vol.14, 2004a, pp.65–75.
- [27] Cavusoglu, H., Mishra, B. and Raghunathan, S., “A Model for Evaluating IT Security Investments,” *Communications of the ACM*, Vol.47, No.7, 2004b, pp.87–92.
- [28] Campbell, K., Gordon, L.A., Loeb, M.P. and Zhou, L., “The economic cost of publicly announced information security breaches: Empirical evidence from the stock market,” *Journal of Computer Security*, Vol.11, No.3, 2003, pp.431–448.
- [29] CSI/FBI, *Computer Crime and Security Survey*, 2007.
- [30] Davis, A., “Return on Security Investment—Proving It's Worth It,” *Network Security*, Vol.2, 2005, pp.8–10.
- [31] Gal-Or, E. and Ghose, A., “The Economic Incentives for Sharing Security Information,” Working Paper, University of Pittsburgh and Carnegie Mellon University, 2004.
- [32] Gordon, L.A., Loeb, M.P., “The Economics of Information Security Investment,” *ACM Transactions on Information and System Security*, Vol.5, No.4, 2002, pp.438–457.
- [33] Gordon, L.A., Loeb, M.P. and Lucyshyn, W., “An Economics Perspective on the Sharing of Information Related to Security Breaches,” *Proceedings of Workshop on the economics of Information Security*, 2002.
- [34] Harris, S., *CISSP All-in-One Exam Guide*, McGraw-Hill, 2001.
- [35] Hausken, K., “Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability,” *Information System Frontiers*, Vol.8, No.5, 2006, pp.338–349.
- [36] Kaplan, R.S. and Norton, D.P., “The Balanced Scorecard—Measures that Drive,” *Harvard Business Review*, Jan/Feb, 1992, pp.71–79.
- [37] Kaplan, R.S. and Norton, D.P., *The Balanced Scorecard—Translating Strategy into Action*, Harvard Business School Press, 1996.
- [38] Kaplan, R.S. and Norton, D.P., *The Strategy-Focused Organization*, Harvard Business School Press, 2001.
- [39] Kim, S.K., Leem, C.S., “Implementation of the Security System for Instant Messengers,” *Lecture Notes in Computer Science*, Vol.3314, 2004, pp. 739–744.
- [40] Kim, S.K., Leem, C.S., “Security of the Internet-based Instant Messenger: Risks and Safeguards,” *Internet Research: Electronic Networking Applications and Policy*, Vol.15 No. 1, 2005, pp. 88–98.
- [41] Kim, S.K., Lee, H.J., “Cost-Benefit Analysis of Security Investments: Methodology and Case Study,” *International Conference on Computational Science and its Applications*, Vol. 3482, 2005, pp.1239–1248.

- [42]Lee, Vincent C.S., “A Fuzzy Multi-criteria Decision Model for Information System Security Investment,” *Lecture Notes in Computer Science*, Vol.2690, 2003, pp.436–441.
- [43]Leem, C.S., Kim, S.K., “Introduction to an Integrated Methodology for Development and Implementation of Enterprise Information Systems,” *Journal of Systems and Software*, Vol.60 No. 3, 2002, pp. 249–261.
- [44]Roper, C.A., *Risk Management for Security Professionals*, Butterworth–Heinemann, 1999.
- [45]Scott, D., *Security Investment Justification and Success Factors*, Gartner.
- [46]Scott, D., *Best Practices and Trends in Business Continuity Planning*, U.S. Symposium/ITxpo, 2002.
- [47]Soo Hoo K.J., *How much is enough? A Risk-Management Approach to Computer Security*, Stanford University, 2000.
- [48]Tanaka H., Matuura K., Sudoh O., “Vulnerability and Information Security Investment: An Empirical Analysis of E-local Government in Japan,” *Journal of Accounting and Public Policy*, Vol.24, 2005, pp.37–59.
- [49]Tsiakis, T. and S., George, “The Economic Approach of Information Security,” *Computers & Security*, Vol.24, No.2, 2005, pp.105–108.
- [50]Witty, R.J, Girard, J., Graff, J.W., Hallawell, A., Hildreth, B., MacDonald, N., Malik, W.J., Pescatore, J., Reynolds, M., Russell, K., Wheatman, V., Dubiel, J.P., Weintraub, A., *The Price of Information Security*, Gartner, 2001.
- [51]Yu, J.E., Ha, I.S., Choi, M.K., Rho, J.J., “Extending the TAM for a t-commerce,” *Information & Management*, Vol.42, 2005, pp. 965–976.