情報保護學會論文誌
第14券 第4號, 2004. 8

전자상거래환경에서 위험분석방법론의 타당성에 대한 연구*

김 종 기[a)†], 이 동 호[b)‡], 서 창 갑[c)]
부산대학교[a)], 부산대학교경영경제연구소[b)], 동명정보대학교[c)]

A Empirical Validation of Risk Analysis Model in Electronic Commerce

Jongki Kim[a)†], Dongho Lee[b)‡], Changgab Seo[c)]
Pusan National University[a)], Research Institute for Management & Economics of PNU[b)], Tongmyung University[c)]

요 약

위험분석모델은 정보시스템 보안과 관련된 위험을 자산, 위협, 취약성, 보안통제의 관계를 통해서 설명하는 체계화된 방법이다. 그러나 위험분석모델의 실증적인 연구가 이루어진 경우는 상당히 드물며, 특히 위험분석모델의 타당성 논의는 거의 없는 실정이다. 구조방정식모델을 적용하여 전자상거래 환경에서 위험분석모델의 타당성에 대한 실증적 분석을 한 결과, 위험의 수준에 영향을 미치는 요인으로 언급되는 위협과 보안통제는 통계적으로 유의한 것으로 나타났다. 본 연구는 전자상거래 이용자의 위험인지에 영향을 미치는 요인을 위험분석 접근법을 이용하여 모델화하여 검증함으로써 전자상거래 위험에 영향을 미치는 선행요인을 규명할 뿐만 아니라 위험분석접근법을 통한 전자상거래에 대한 새로운 관점에서의 접근을 가능하게 한다.

ABSTRACT

Risk analysis model is systematic and structural process that considers internal security problems and threat factors of the information systems to find optimal level of security control. But, the risk analysis model is just only defined conceptually and there are not so many empirical studies. This research used structural equation modeling(SEM) research methodology with rigorously validated research instrument. Based on results of this study, risk analysis methodology was proved to be practically useful in e-commerce environment. Factors like threat and control were significantly related to risk. In conclusion, the results of this study can be applied to general situation or environment of information security for analyzing and managing the risk and providing new approach to comprehend concept of risk in e-commerce environment.

Keywords : *Risk Analysis Model, E-Commerce, IS Security, SEM*

Ⅰ. 서 론

정보기술과 관련된 개인정보유출이나 서비스거부 공격과 같은 보안사고 발생의 증가추세와 보안위험에 대한 전반적인 인식이 높아지고 있는 상황에서 정보시스템과 관련된 위험을 보다 체계적으로 접근하고 대응하기 위한 여러 가지 방법들이 개발, 적용되고 있다. 이러한 방법들 중에 대표적인 것으로 위험분석을 통해 정보시스템의 위험을 효과적이고 체계적으로

접수일 : 2004년 3월 26일 ; 채택일 : 2004년 6월 30일
* 이 논문은 2003년도 한국학술진흥재단의 지원에 의하여 연구되었음.(KRF-2003-003-B00065)
† 주저자 : jkkim1@pusan.ac.kr
‡ 교신저자 : dghlee@pusan.ac.kr

분석하는 방법이 있다.

위험분석은 정보시스템에 내재한 보안상의 약점과 외부의 위협요인들을 고려하여 최적의 보안대책을 모색하는 체계적인 절차이며, 이에 관한 국제표준인 ISO/IEC 13335나 17799로 제정되어 있을 만큼 그 중요성이 크다[1,2]. 이러한 정보자산과 관련된 위험분석에는 위험분석 방법론이 보편적으로 적용되고 있다[3]. 위험분석에 있어서 핵심적인 내용은 정보시스템의 활용에 따른 보안상의 문제점에 대한 위험수준의 평가이다. 그러나 보안위험에 대한 정보시스템 사용자의 심리적 판단이 객관화되는 과정이 위험분석 절차에 있어서 매우 중요함에도 불구하고 위험분석 방법론은 규범적으로 정의되어 있을 뿐이며 위험분석 방법론 전반에 대한 실증적인 연구가 매우 드물다. 특히 정보시스템과 관련된 정보자산과 위협 그리고 보안통제와 같은 개념들을 통해서 위험분석을 수행하는 위험분석모델 자체의 타당성에 대한 연구는 거의 없는 실정이다. 또한 전자상거래 이용자가 인지하고 있는 위험이 구체적으로 전자상거래를 이용하려는 의도에 어떠한 영향을 미치고 있는 지에 대한 연구도 그다지 많지 않다. 위험이라는 개념은 자산, 위협, 보안통제와 같은 주요한 요인의 관계함수로 정의되고 있는데, 이러한 위험의 선행요인들을 통한 전자상거래에서 발생하는 위험에 대한 개인 사용자의 인지를 실증적으로 검정함으로써, 위험분석 방법론에 대한 타당성을 확인하고자 한다.

Ⅱ. 전자상거래에서의 위험과 위험분석모델

1. 전자상거래에서의 위험의 개념

정보보안과 관련된 개념으로는 보안통제나 인지된 위험과 같은 것을 주요요인으로 전자상거래관련 연구들에서 논의되고 있다. 보안통제의 개념을 가치를 가지는 자산을 보호하기 위한 기술적인 차원에서 대부분의 연구들에서 논의가 이루어지고 있지만 보안정책이나 교육과 같은 제도적인 차원의 개념도 포함된다. 한편, 정보보안과 관련된 개념 중에서 대부분의 문헌들에서 논의가 되는 것은 위험이다. 위험은 자원의 잠재적인 손실이나 소비자가 인지하는 부정적인 결과라고 정의 할 수 있으며, 이러한 위험의 개념은 대부분의 문헌연구들에서 인지된 위험(perceived risk)의 개념으로 논의되고 있다[4,5].

Jarvenpaa 등은 위험인지의 개념에 정보보안의 변수를 포함하여 연구를 수행하였으며[6], Kim and Prabhakar는 부정적인 결과나 영향에 대한 것을 위험의 개념으로 논의하고 있다[7]. 이 연구에서는 전자상거래 신뢰에 영향을 주는 주요한 요인으로 개별 사용자 혹은 구매자가 인지하는 위험을 주요한 요인으로 언급하고 있으며, 인지된 위험은 전자상거래를 이용함으로써 발생하는 상대적인 이점 혹은 이익과 그러한 이용을 통해서 발생되는 부정적인 결과간의 인지차이를 의미하는 것으로 주장하고 있다. Pavlou의 연구에서는 재무적인 관점의 위험만이 아니라 전자상거래에서 발생할 수 있는 정보차원의 위험도 포함하여 위험을 논의하고 있다[5]. 전자상거래에서 적용되는 이러한 위험의 개념은 단일한 개념으로 위험 그 자체로 정의되고 있으며, 체계적인 접근이나 분석을 위한 방법은 거의 적용되고 있지 않고 있는 실정이다.

2. 위험분석모델

위험분석모델은 위험분석에 적용되는 개념적인 틀로써, 위험에 대한 체계적인 접근과 분석을 위한 지침으로 활용된다. 위험분석의 공정은 기본적으로 보호대상 정보자원의 식별과 자산에 관련된 취약성과 위협의 수준, 그리고 그러한 관계를 통해서 산출되는 위험의 수준을 완화하기 위한 보안대책을 선정하는 과정으로 구성된다. 즉, 위험분석모델은 위험관리의 목적과 자산, 위협, 취약성과 같은 위험관리 요소의 식별과 이러한 요소들 간의 상호관계를 기술하는 것이며 위험관리 방법론은 실제적인 위험관리를 수행하기에 필요한 구체적인 절차와 단계 기법 등을 설명하는 것이다.

위험분석은 정보시스템 보안관리의 핵심적인 요소로서 위험의 중요성과 인과관계를 식별하여 어떻게 처리할 것인가를 결정하는 체계적인 절차이다. 위험분석 공정을 통해서 식별된 위험은 그 파급 효과를 감소시키거나, 회피 또는 전이하거나, 수용하는 방법을 통해 위험을 관리하게 되며, 이러한 위험관리 방법으로는 운영적, 절차적, 물리적, 인적, 기술적 차원의 보안대책이 있다.

한편, 위험분석모델을 구성하는 요소들은 자산, 위협, 취약성, 보안통제와 같은 다양하게 구성되어 있으며, 현재 적용되고 있는 상당수의 위험관리 방법론들은 이러한 요소들 간의 관계를 통해서 구성된다[9]. 이러한 위험분석모델 중에서 대표적인 것이 다음

의 그림 1과 같은 ISO/IEC의 모델[1]이다.

이 모델에서는 위험이라는 개념을 자산, 사업영향, 가치, 보호요구사항, 보안대책, 위협, 취약성 등이 관련된 복합함수로 정의하고 있다. 즉, 위험은 단순한 하나의 개념으로 평가되는 것이 아니라 다양한 요인들 간의 관계에 의해서 결정되는 것으로 설명하고 있다. 모델에서 언급되는 요소에는 대부분의 다른 위험분석모델에서 언급되는 공통적인 항목들인 자산, 위협, 취약성, 보안통제와 함께 가치나 사업영향, 보호요구사항과 같은 다른 요소들도 포괄적으로 논의하고 있다는 특징이 있다.

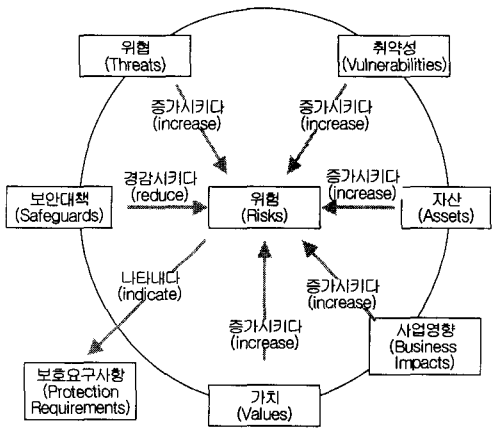


그림 1. ISO/IEC의 위험분석요소의 관련성

이와 유사한 맥락으로 BS7799의 정보보안관리체계의 수립과정에서는 위험의 평가와 관리의 개념을 자산의 가치나 중요도, 취약성의 수준, 위협의 빈도나 심각성과 같이 자산, 취약성, 위협의 함수로 정의하고, 이러한 함수관계를 통해서 해당조직의 위험수준을 평가하고 결정하는 방법을 제안하고 있다[10]. BS7799에서 논의되는 위험분석모델은 위험이라는 개념을 자산과 위협 그리고 취약성이라는 요소를 통해서 설명하고 있으며, 근본적인 큰 틀은 ISO/IEC와 크게 다르지 않다고 볼 수 있다.

앞서 설명한 두 위험분석모델은 기본적으로 자산을 기반으로 하는 위험분석방법론의 성격을 가지고 있으며, CRAMM과 같은 위험분석 방법론[11]도 거의 유사한 위험분석모델로 구성되어 있다. 물론 이러한 자산기반의 위험분석 접근법외에도 취약성을 중점적으로 다루는 VAF[12]나 위협을 중심으로 논의하는 CSE[13]나 GAO[14]와 같은 방법론에서도 세부적으로는 약간의 차이가 있으나, 기본적인 틀은 ISO/IEC 모델이나 BS7799와 상당한 유사성을 가지고 있다.

위험분석모델과 관련된 접근법들을 살펴보면, 앞서 논의한 방법론들을 보다 간결하게 적용하고 있는 방법론도 있다. 이러한 위험분석 방법으로 대표적인 것으로 IPAK[15]이나 FRAP[16]과 같은 것이 있으며, 이러한 방법론들에서는 위험을 자산과 위협간의 관계로 혹은 보안대책의 수준과 자산의 가치와의 상호평가를 통해서 혹은 특정의 보안대책과 관련된 항목들의 검증을 통해 접근하는 방법을 취하고 있다. 이러한 실무적인 접근법들에서 논의되는 위험분석모델은 자산, 위협, 취약점, 보안통제, 가치 등과 같은 모든 요소들 간의 관계를 제시하고 있는 것이 아니라, 특정 몇몇의 요소들로 설명하고 있다.

3. 위험분석절차

정보보안 차원에서 적용되는 대부분의 위험분석 접근법의 논의를 통해서 공통적으로 수행되는 공정과 요소들에 대해서 요약을 하면 그림 2로 나타낼 수 있다.

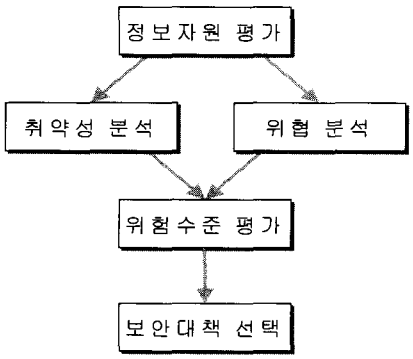


그림 2. 일반적인 위험분석 공정과 절차

위험분석은 먼저 보호 대상이 되는 정보자원을 식별하고 가치를 평가하는 단계에서 시작한다. 정보자원은 자산이라고도 지칭되며, 하드웨어, 소프트웨어, 데이터, 인적자원, 통신망 및 관련 장비 등을 모두 포괄하는 개념이다. 이러한 정보자원은 위험분석 단계의 초기에 그 분석의 대상과 범위를 결정하는 과정과 개별조직의 특성에 따라서 다양한 프로파일(profile)로 구성된다. 예를 들어 기존의 조직차원에서 정보자산으로 간주되는 서버, 네트워크, 운영설비와 같은 항목들은 본 연구에서 적용하는 전자상거

래 환경에서 그 적용범위와 대상의 특성으로 인해서 제외되며, 정보자산 특히 개인정보나 구매정보 배송정보와 같은 무형자산이 정보자원의 평가항목들로 구성된다.

자산의 식별과 평가의 과정은 위험분석과 관리에 있어서 보호하고자 하는 대상의 선정과 구현되는 보안 대책의 식별에 중요한 영향을 미친다. 정보자원 혹은 자산에 대한 식별과 평가는 기본적으로 정보보안의 3대 요소인 기밀성, 무결성, 가용성의 차원에서 평가되며, 이외에도 BS7799와 ISO/IEC에서는 수익의 감소, 시장점유율, 기업이미지와 같은 항목을 추가적으로 고려하는 것을 권장하기도 한다.

정보자원의 식별과 평가의 공정이 완료되면 그 다음 단계로 정보시스템 보안상의 취약성과 위협 요인을 식별하고 평가하는 공정이 진행된다. 위협은 원천에 따라 자연 발생적인 위협(화재, 수재, 정전 등), 인간에 의한 의도적인 위협(정보자원에 대한 파괴, 절취, 컴퓨터 바이러스, 해킹 등), 그리고 비의도적인 위협(시스템의 조작 미숙, 소프트웨어, 하드웨어, 통신장비 등 시스템의 결함)으로 구분할 수 있다[17]. 대부분의 위험분석모델에서 언급하는 이러한 위협은 자산에 의도하지 않는 결과를 초래하는 사건들로 정의되어 있으며, 평가항목은 공통적으로 빈도와 심각성의 개념으로 이루어져 있다.

취약성은 정보시스템의 보안상의 문제점을 발생시킬 소지가 있는 정보시스템에 내재된 약점으로서 외부의 위협요인에 의해 현실화될 때 문제가 된다. 취약성의 개념은 BS7799나 ISO/IEC 그리고 CSE에서는 자산이 가진 약점이라는 차원에서 다루어지고 있으며, 실무적인 성격을 가지는 IPAK이나 FRAP에서는 보안통제의 부재나 정도의 개념으로 취약성을 평가하는 방법을 취하고 있다. 이러한 취약성의 개념적 접근은 관점에 따라서 자산의 속성으로 정의하는 것과, 보안대책의 부재로 정의하는 것, 그리고 자산과 위협간의 관계로 정의하는 관점이 존재한다[18].

취약성은 자산, 위협, 보안대책과 연계되어 식별되고 CRAMM에서도 이러한 이유로 취약성을 별도로 식별하여 평가하지 않고 위협과 연계하여 평가하는 접근법을 취하고 있다. 본 연구에서도 취약성을 전자상거래를 이용하는 일반사용자가 취약성에 대한 개념의 정확한 이해를 하기 힘들 것이라는 이유에서 보안대책이라는 개념을 통해 취약성의 개념을 대체하여 측정하였다.

위험평가는 위협 요인이 정보시스템의 취약성과 연관될 때 어떤 정보자원에 어떠한 형태(비밀성, 무결성, 가용성, 인증성 등)로 영향을 미치는지 분석하는 과정이다. 위험수준은 특정 자산에 대하여 식별된 위협이 현실화될 가능성과 심각성을 고려하여 표현된다. 위험분석의 마지막 단계는 측정된 위험수준에 대응할 수 있는 보안대책을 식별하고 최적의 대안을 선택하는 것이다.

요약하면 위험분석은 위험을 자산과 위협 그리고 취약성과의 관계로 평가하고 해당위험을 완화하는 적정의 보안대책을 수립하고 선택하는 일련의 과정을 거친다.

III. 연구내용

1. 연구모델 및 가설

앞에서 언급한 위험분석모델을 인터넷을 이용하는 전자상거래 환경에서 실증적으로 분석하기 위하여 본 연구에서는 그림 3과 같은 연구모델을 개발하였다. 연구에서 검정하고자 하는 가설은 위험에 영향을 주는 각 요소들 간의 관계에 대하여 수립되었다.

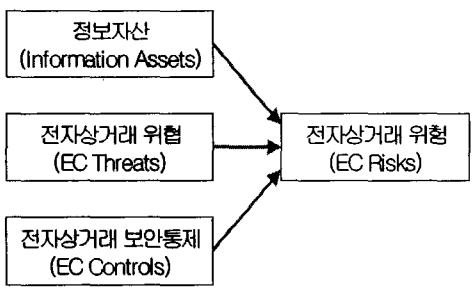


그림 3. 연구모델

H1 : 정보자산의 가치나 중요도가 높을수록 전자상거래의 위험은 높아질 것이다.
먼저, 정보자산의 가치나 중요도가 높을수록 사용자가 인지하는 전자상거래 위험이 높아질 것이라는 가설을 수립하였다.

H2 : 전자상거래 위협의 빈도나 심각성이 높을수록 전자상거래 위험은 높아질 것이다.
두 번째는 전자상거래에서 발생할 수 있는 위협의 빈도나 심각성이 높을수록 전자상거래위험의 수준이 높을 것이라는 가설을 검정하고자 하였다.

H3 : 전자상거래 보안통제가 높을수록 전자상거

래 위험은 낮아질 것이다.
마지막은 전자상거래 보안통제의 수준이 높을수록 이와 관련된 위험의 수준이 낮아질 것이라는 가설을 수립하였다.

연구모델은 앞에서 논의한 위험분석 모델의 주요한 요소들을 포함하고 있으며, 요인들에 대한 세부적인 설명은 다음과 같다.

1.1 정보자산

자산은 정보보안의 그 대상이 되는 것으로 중요한 가치를 가지는 유형적 무형적인 대상을 모두 지칭하는 것으로 정의할 수 있다. 즉, 하드웨어나 네트워크, 설비와 같은 유형의 정보자산과 개인정보, 기업의 업무문서, 고객정보, 금융관련 정보와 같은 무형의 정보자산을 모두 자산이라는 개념으로 지칭할 수 있다.

자산의 식별과 정의는 정보시스템과 관련된 위험의 분석과 관리에서 가장 우선적으로 이루어지는 공정으로 설명하고 있으며, 보호의 대상이 되는 자산을 식별하고 평가하는 것으로 논의되고 있다.

위험분석과 관리를 언급하고 있는 국제표준이나 현재 위험분석 분야에 적용되고 있는 다양한 제반 실무적인 기법별로 자산의 식별과 범주가 상당히 다양하게 설명되고 있다. 그러나 전자상거래라는 환경에서 이러한 자산의 개념은 상대적으로 협의적인 성격을 가지게 된다.

위험분석 접근법외에 전자상거래와 관련된 기존의 연구들에서도 정보자산, 특히 개인정보를 중요한 요인으로 다루고 있는 연구[19,20]가 다수 존재하는데, 이러한 연구들에서 정보자산의 개념은 전자상거래를 이용하는데 사용되는 프라이버시 관련 정보나 제품의 구매 정보와 같은 개념으로 위험분석 방법론에서 언급하고 있는 자산과 동일한 차원으로 사용되고 있다.

본 연구에서는 정보자산이라는 무형자산의 개념을 주요한 자산의 개념으로 사용하였으며 이러한 무형자산의 평가를 위해서 정성적인 평가 방법론의 관점에서 개별 항목을 조작적으로 정의하였다. 다음의 표 1은 연구에 적용된 정보자산의 개념에 대한 조작적 정의 항목을 나타낸다.

1.2 전자상거래 위협

위협은 정보시스템 혹은 정보기술과 관련되어 있는 자산에 대해서 의도하지 않은 결과를 초래하는 의도적 혹은 비의도적인 사건이라고 정의할 수 있다[1,21]. 이러한 위협의 개념적 정의에서 설명하는 위협은 다음과 같이 설명할 수 있다.

위협은 위협이 야기되는 동기와 발생가능성에 관련된 문제이다. 정보보안 문제를 야기하는 사건의 의도 혹은 동기가 비의도적인 것인가 의도적인 것인가에 따라서 위협에 대한 식별과 평가에서 다소 차이가 발생한다. 대부분의 위험분석 및 관리 방법론에서 언급하고 있는 구분에 따르면, 의도적인 위협은 인간, 특히 해커와 같은 악의적인 의도를 가진 사람에 의하여 발생하는 것으로 분류하고, 비의도적인 위협의 구분은 대부분 홍수, 지진, 정전과 같은 자연재해로 설명하고 있다.

본 연구에서는 위협의 발생가능성이나 빈도의 인지를 주요한 변수로 사용한다. 실제 전자상거래에서 발생 가능한 혹은 관련되어 있는 위협은 거래정보 노출이나, 해킹, 신용카드 번호의 노출 가능성과 같은 것들이 있다. 자산과 유사하게 위협의 개념도 전자상거래라는 맥락에서 물리적인 위협이 아닌 정보자산과 관련되어 있는 위협의 항목들에 대해 적용한다. 다음의 표 2는 연구에 적용된 위협의 설문항목을 요약하여 나타내고 있다.

표 1. 자산 요인의 설문항목 요약

항목명	측정변수
AS1	인지된 개인정보 제공의 중요도
AS2	개인정보의 가치
AS3	구매관련 정보의 상대적 가치
AS4	개인정보의 중요도
AS5	지불관련 정보의 중요도

표 2. 위협 요인의 설문항목 요약

항목명	측정변수
TH1	개인정보 노출 확률
TH2	잠재적인 손실의 발생 가능성
TH3	가용성 피해의 확률
TH4	기밀성 피해의 가능성
TH5	잠재적 피해의 발생가능성
TH6	구매정보의 노출 확률
TH7	개인정보의 노출 확률

1.3 전자상거래 보안통제

보안통제라는 개념은 정보시스템의 자산을 위협으로부터 발생하게 되는 의도하지 않은 피해를 방지하거나 완화하는 일련의 기술적, 관리적, 정책적인 대책이라고 정의할 수 있다[1,10,22]. 또한, 보안대책의 개념에는 발생 가능한 위협으로부터 정보시스템 자산을 보호하고, 보안 사고를 사전에 혹은 조기에 발견하고, 위협의 실현으로 인한 피해나 영향을 경감하며, 정보시스템의 복구와 같은 행위를 포함한다.

보안통제 항목들의 예로 들 수 있는 것에는 거래정보의 노출을 방지하기 위한 암호화 기법의 사용, 제3자의 인증 마크의 존재, 법적 혹은 제도적 규정 준수사항의 명시와 같은 것들이 있다. 본 연구에서는 전자상거래에서 정보자산의 위협이나 위험을 감소시키거나 위협에 노출될 확률을 줄이게 하는 기술적인 그리고 관리적인 방법들을 보안통제라는 변수로 설정하였다.

즉, 보안통제요인의 측정을 위해서 전자상거래에서 사용되고 있는 보안통제의 전반적인 수준에 대한 사용자의 인지와 관련된 변수들을 연구에 적용하였다. 다음의 표 3은 이러한 보안통제와 관련된 설문항목을 요약하여 나타낸 것이다.

표 3. 보안통제 요인의 설문항목 요약

항목명	측정변수
CO1	인지된 개인정보 보안통제 수준
CO2	지불보안통제에 대한 인지된 수준
CO3	제도적인 보안대책 수준
CO4	개인정보의 기술적인 보안통제
CO5	구매정보의 기술적인 보안통제
CO6	배송정보의 보안통제
CO7	전자상거래 전반적인 보안통제 수준

1.4 전자상거래 위험

위험분석 접근법에서 논의되는 위험은 앞서 언급한 요인들 간의 관계를 포함하는 포괄적인 의미로 정의된다. 즉, 특정의 자산에 의도하지 않는 피해를 야기할 수 있는 위협이 현실화될 경우에 발생 가능한 피해의 수준이나 정도를 위험으로 정의하고 있다. 이러한 위험은 특정의 보안대책을 통해서 위험완화의 과정을 통해서 수용 가능한 수준으로 조정되며, 완벽한 수준의 위험제거의 개념이 아닌 잔여위험의 수용정도에 따라서 잔여위험의 정도가 수용할 만한 수준을 넘어서는 경우에는 추가적인 보안대책의 구현을 통해서 그 영향을 감소시키는 의사결정을 하게 되며, 그렇지 않은 경우에는 잔여위험을 수용하는 의사결정의 과정으로 진행된다.

위험은 이러한 선행요인들 간의 관계로 설명될 수 있으며, 개념적인 위험분석 방법론에서는 위험을 자산, 위협, 취약성의 함수로 정의하고 있다. 본 연구의 연구모델과 유사한 체계를 가지는 ISO/IEC의 모델에 나타나 있듯이 위험의 개념은 자산, 위협, 보안통제 등의 다수의 요인간의 관계로 설명된다.

BS7799에서도 자산, 위협, 취약성의 관련함수로 위험을 정의하고 있다. 이러한 복합적인 함수의 개념인 위험을 본 연구에서는 전자상거래를 통해서 구매하는 구매자들이 인지하고 있는 위험을 표 4와 같이 측정한다.

표 4. 위험 요인의 설문항목 요약

항목명	측정변수
RI1	전자상거래 매체의 상대적 위험
RI2	인지된 위험 수준
RI3	인지된 지불관련 위험
RI4	이용안전성에 대한 위험 인지
RI5	전자상거래 관련 전반적 위험인지

2. 실증분석

2.1 연구도구의 개발

선행연구의 검토를 통해서 위험분석에 대한 실증적인 연구를 수행한 문헌들을 찾을 수 없었다. 이러한 결과는 정보보안 분야에서 실증연구가 상당히 드물다는 것에 기인한다.

따라서 본 연구에서는 위험분석모델을 구성하는 개념들에 대한 실증적인 설문문항을 위험분석모델의 조작적인 정의와 전자상거래와 관련된 연구들에서 사용된 유사한 개념적인 정의를 수용하여 설문항목을 개발하였다.

실증분석을 위한 설문문항들은 연구자와 정보시스템 관련 전문가들에 의해서 반복적인 검토와 수정이 이루어졌으며, 최종적으로 연구에 적용된 설문문항들은 사전조사(pre-test)를 통해서 검증하였다. 사전

조사는 100명의 학부생들을 대상으로 수행되었다. 100부의 응답설문지 중에서 유효한 응답인 89부를 이용하여 설문항목의 의미에 대한 명확성의 확인과 설문항목의 적절성을 평가하였으며, 부분적인 타당성, 신뢰성을 검토하였다. 또한, 사전조사의 결과를 토대로 연구자와 정보시스템 전문가들에 의해서 전체 실증연구에 적용될 수 있도록 반복적인 검토가 수행되었다.

2.2 연구표본

본 연구에서 제시하는 연구모델을 검증하기 위해서는 전자상거래를 충분히 경험한 집단을 선정하는 것이 중요하다. 따라서 연구의 설문대상으로는 야간에 수업이 진행되는 경영대학원 학생들을 선정하였다.

경영학석사 학위과정을 수학 중인 경영대학원 학생 집단은 연령의 분포가 20대에서 50대로 분포하고 있다. 또한, 교육의 수준이 상대적으로 높다는 점과 인터넷의 이용이나 전자상거래의 이용에 대한 경험이 있다는 점에서 전체 전자상거래 사용자를 대표하는 특성을 충분히 가지고 있다. 또한 이들 학생들은 충분한 구매력을 가진 집단으로 전자상거래를 이용하는 인구를 충분히 반영하는 타당한 집단이라고 판단된다.

170부의 설문지를 경영대학원 학생들에게 배포하였으며, 이 중에서 158부가 회수되어 회수율은 93%로 나타났다. 회수된 설문지를 검토하여 성실하지 않은 답변을 한 설문지와 오류가 있는 설문지를 제외한 전체 배포 설문지의 85%인 145부가 분석에 사용되었다.

연구표본 집단의 성별구성은 남성이 전체의 89.4%인 128명, 여성이 10.6%인 15명이었다. 단, 전체 145명의 표본대상 중에서 성별을 기입하지 않은 설문지 2부는 제외되었다. 연구표본의 인구통계학적 특성을 살펴보면 전반적으로 연령층은 30대와 40대로 구성되어 있으며, 전자상거래 이용과 관련된 인터넷 사용 경력에 있어서는 전체의 80.4%가 3년 이상 인터넷을 이용한 것으로 나타났다.

전자상거래를 통한 위험의 인지는 사용자들이 구매하는 금액과 관련이 있는 것으로 볼 수 있다. 즉, 구매 금액이 큰 사용자일수록 위험의 인지를 정확하게 하고 있는 것으로 볼 수 있다. 표본 집단의 최대 구매금액과 관련된 분석에서는 전체의 90%가 10만원 이상을 구매한 경험이 있는 것으로 나타나 전반적인 위험을 인지하기에는 충분하다고 판단된다.

2.3 연구도구의 검증

위험분석 모델의 실증적인 검정을 위해서 본 연구에서는 구조방정식모델(Structural Equation Modeling)을 적용하였다. 구조방정식모델은 구성개념간의 관계를 분석하는데 적용되며 자료들 간에 존재하는 상관관계, 공유 분산, 모델의 경로분석과 경로의 유의수준을 검토할 수 있는 모수추정을 위한 적절한 방법으로 평가[23]되고 있기에 본 연구에서 수행되는 전체 모델에 대한 분석에 적합한 도구로 사용될 수 있다. 본 연구에서는 구조방정식모델의 도구로 가장 보편적으로 이용되는 LISREL 8.20버전을 사용하여 분석을 수행하였다.

한편, 기존의 문헌연구들과 사전조사를 토대로 개발된 연구도구는 이 단계 접근법(two-step approach)으로 검정하였다. 이 단계 접근법은 전체 연구 모델의 분석과 잠재변수(latent variable)를 측정하기 위한 측정모델에 대한 분석을 분리하여 수행하는 방법론으로 해석상의 교락효과(interpretational confounding)를 줄일 수 있는 적합한 방법이다[24].

연구도구의 검정에 앞서서 실증분석에 적용된 각 항목들의 기술통계적인 내용은 다음의 표 5로 요약할 수 있다. 전체 설문문항은 리커트척도의 형태로 7점 척도로 작성이 되었으며, 매우 그렇지 않다(1)에서 매우 그렇다(7)로 개별 사용자가 인지하는 내용을 직접적으로 답하도록 개발되었다.

2.3.1 일차원성 분석

일차원성(unidimensionality)이란 각 측정항목이 평행 상관관계 형태(parallel correlational pattern)를 가지지 않으면서 소속된 요인에만 적재되는 정도를 말하여, 요인 분석의 관점에서는 하나의 요인을 구성하는 일차원성을 가진 측정항목들은 해당 요인만을 공유하며 다른 요인을 구성하는 측정항목들과는 유의한 상관관계를 가지지 않는다는 것을 의미한다.

일차원성의 분석은 구조방정식의 분석결과에 나타나는 표준화된 잔차(standardized residuals)의 검토를 통해서 이루어진다[25,26]. 즉, 측정 항목들 간의 표준화된 잔차가 유의한 수준을 심각하게 벗어나는 경우나 모델의 수정지수의 값이 5를 넘어서는 측정변수들 간의 관계에 대해서 각 측정 항목들을 하나씩 제거해 나가는 방법을 사용한다[27].

표 5. 측정 항목의 기술통계 요약

구성개념	항목	평균 (표준편차)
정보자산	AS1	6.434 (0.856)
	AS2	6.207 (0.881)
	AS3	5.897 (1.059)
	AS4	6.048 (0.974)
	AS5	6.297 (0.951)
전자상거래 위협	TH1	5.683 (1.091)
	TH2	4.897 (1.257)
	TH3	4.276 (1.304)
	TH4	4.772 (1.212)
	TH5	5.021 (1.233)
	TH6	5.069 (1.128)
	TH7	4.724 (1.325)
전자상거래 보안통제	CO1	4.200 (1.128)
	CO2	4.503 (1.081)
	CO3	3.800 (1.051)
	CO4	3.538 (1.225)
	CO5	3.690 (1.096)
	CO6	3.834 (1.093)
	CO7	3.834 (1.247)
전자상거래 위험	RI1	5.110 (1.297)
	RI2	5.262 (1.093)
	RI3	4.469 (1.375)
	RI4	4.490 (1.323)
	RI5	4.634 (1.212)

일차원 타당성에 대한 분석을 수행한 결과로 전체 24개의 설문항목들 중에서 자산요인의 두 항목(AS3, AS5), 위협요인의 세 항목(TH5, TH6, TH7), 보안통제의 세 항목(CO1, CO2, CO4), 위험의 한 항목(RI2)이 표준화된 잔차분산의 값이 유의수준을 지나치게 벗어나거나 수정지수가 5를 넘어서는 것으로 나타나 최종분석에서는 제외되었다. 물론 이러한 설문문항의 제거는 전반적인 일차원 타당성 분석의 기준에 의해서 이루어졌으며, 측정모델의 지표가 대부분 양호한 것으로 나타나 전체 15개의 항목을 모델의 분석에 적용하였다.

2.3.2 신뢰성 검정

실증분석을 통한 연구조사에 있어서 사용되는 측정도구는 그 의미가 유효하고 실제적인 효용을 가지기 위해서는 신뢰할 수 있어야 한다[28]. 이러한 측정도구의 신뢰성은 오차가 없고 일관된 결과를 얻을 수 있는 정도를 의미한다[29].

일반적으로 구조방정식 모델에서는 신뢰성의 검정을 합성구성개념 신뢰성(composite construct reliability)이나 평균 분산 추출 값(average variance extracted)으로 계산한다. 먼저 합성구성개념 신뢰성은 측정항목의 표준 적재값을 이용하여 하나의 구성개념을 이루는 측정항목의 내적 일관성을 계산하며, 0.7보다 클 때 구성개념의 신뢰성이 있는 것으로 볼 수 있다. 평균 추출 분산 값은 구성개념에 의해서 설명되는 분산의 양을 나타내며, 0.5보다 작은 경우에는 측정 오차(measurement error)가 구성개념에 의해서 설명되는 분산보다 크기 때문에 신뢰성이 없다고 할 수 있다[30].

측정모델의 신뢰성 분석의 결과는 다음의 표 6으로 나타낼 수 있으며, 이러한 신뢰성 분석의 결과는 연구의 측정모델에 대한 내적인 일관성이 충분히 확보되었음을 의미한다고 볼 수 있다.

표 6. 측정모델의 신뢰성 분석

구성개념	측정 항목수	합성 구성개념 신뢰성	평균분산 추출값
자산	3	0.802	0.576
위협	4	0.794	0.495
보안통제	4	0.844	0.579
위험	4	0.851	0.596

2.3.3 집중타당성 분석

집중타당성(convergent validity)은 동일한 개념을 측정하기 위하여 서로 다른 두 가지 측정항목을 개발하고 이를 통해서 얻어진 측정치들 간에 높은 상관관계가 존재해야 할 때 타당성이 있다고 설명된다[31]. 집중타당성의 분석은 측정모델의 요인 적재값과 t-값에 따라서 검정된다. 즉 각 항목의 추정치가 0.5 이상이며 그 추정치의 t-값이 2.0이상 일 때, 측정항목의 집중타당성이 있는 것으로 판단한다.

표 7. 집중 타당성 분석 결과

항목	추정치	t-값	항목	추정치	t-값
AS1	0.655	9.610	CO5	0.879	10.869
AS2	0.768	11.131	CO6	0.882	10.966
AS4	0.631	7.978	CO7	0.968	10.408
TH1	0.714	8.026	RI1	0.680	6.459
TH2	0.996	10.208	RI3	1.052	10.481
TH3	0.836	7.820	RI4	1.164	12.841
TH4	0.856	8.819	RI5	1.060	12.734
CO3	0.665	7.930			

표 7에 나타나 있듯이 모든 항목들의 추정치와 그 추정치의 t-값은 권고되는 수치를 충분히 만족시키는 것으로 나타나 연구에 적용된 항목들의 집중타당성은 충분히 있다고 판단할 수 있다.

2.3.4 판별타당성 분석

판별타당성(discriminant validity)은 서로 다른 개념을 측정했을 때 얻어진 측정치들 간에 상관관계가 낮을 때 타당성이 있는 것으로 판단한다[32]. 판별 타당성의 분석은 상관계수와 표준오차를 사용하는 방법[33]과 각 개념들 간의 쌍 비교(pairwise discriminant analysis)를 통한 방법[34]이 있는데, 본 연구에서는 쌍 비교를 통한 기법을 측정 모델의 판별 타당성 검정을 위해서 사용하였다.

쌍비교를 통한 방법은 측정모델과 다른 조합된 모델들 간의 카이자승치에 대한 차이가 유의한 지를 분석하는 과정을 통해서 이루어진다. 표 8과 같이 전체 4개의 요인을 각각 쌍으로 조합한 모든 경우의 수인 6개의 모델에 대한 카이자승치의 분석을 통해서 측정모델과의 유의한 차이가 존재하는 지를 검정한다.

표 8. 판별 타당성 분석 결과

모델	자유도 (df)	카이자승치 (x^2)	p-값 (p-value)
측정모델	84	80.741	0.581
자산-위협 개념 조합모델	87	331.205	0.000
자산-보안통제 개념 조합모델	87	408.877	0.000
자산-위험 개념 조합모델	87	469.956	0.000
위협-보안통제 개념 조합모델	87	421.342	0.000
위협-위험 개념 조합모델	87	228.009	0.000
보안통제-위험 개념 조합모델	87	347.646	0.000

측정 모델만이 유일하게 p-값이 0.05이상으로 나타나 있으며, 나머지의 쌍으로 조합된 모델들은 모두 유의적인 차이가 있지 않는 것으로 분석되었다. 또한 원 모델과 조합된 모델간의 카이자승치의 차이에 대한 검정에서도 자유도차이의 값인 3에서 카이자승치 차이를 모두 비교한 결과, 판별 타당성이 확보되는 것으로 나타났다. 따라서 연구에 적용된 전체 4개의 요인들은 판별 타당성이 있는 것으로 분석되었다.

2.3.5 측정모델의 적합도 분석

측정모델에 대한 전반적인 타당성의 분석이 완료되면, 적합도 지표와의 비교를 통해서 측정모델의 전반적인 설명력에 대한 검정이 이루어지게 된다. 이러한 세부적인 모델의 적합도와 관련된 지표를 살펴보면, 측정모델에서 카이자승치를 자유도로 나눈 값이 일반적으로 요구되는 카이자승치가 자유도의 3배 이상 혹은 그보다 엄격한 2배 이상이 되어서는 안 된다는 조건을 충족하였다.

또한, 카이자승치의 p-값의 경우에 있어서도 일반적으로 논의되는 유의수준인 0.05를 넘는 0.581로 측정모델이 유의한 것으로 분석되었다. 다른 일반적인 적합도 지표에 있어서도 수정부합지수(AGFI)가 0.82, 간명기초부합지수(PGFI)가 0.69, 표준부합지수(NFI)가 0.86, 비교부합지수(CFI)와 증분부합지수(IFI)가 각각 0.98로 분석되었다.

한편, 적합도 지표 중에서 GFI의 값과 NFI의 값이 각각 0.86으로 일반적으로 권고되는 0.90보다 약간 낮은 것으로 분석되었다. 그러나 RMR의 값과 RMSEA의 값이 각각 0.05와 0.024로 나타났으며, 대부분의 구조모델 적합도 지표가 일반적으로 논의되는 수준을 충족하고 있는 것으로 분석되어, 분석결과에 따르면, 측정모델의 전반적인 모델적합도는 양호한 것으로 나타나 연구모델에서 사용하고 있는 개념들이 전반적으로 의미가 있는 것으로 분석되었다.

2.3.6 연구모델과 가설 검정

연구모델의 모델적합도는 표 9에 나타나 있듯이, 구조방정식모델의 적합도에 기준이 되는 모든 항목에서 권장수용기준을 초과하고 있는 것으로 나타나 전반적인 모델의 적합도는 상당히 높은 것으로 분석되었다.

기초 부합 지수(GFI)의 값이 권고되는 수준인 0.90을 넘어서는 0.93으로 산출되었으며, 표준 원소 잔차(SRMR)의 값도 일반적인 수용기준인 0.05이하이어야 한다는 조건을 충족하고 있다. 또한, 수정부합지수(AGFI)와 표준부합지수(NFI)도 역시 둘 다 권장되는 수용기준인 0.90을 넘어서는 것으로 분석되었다. 즉, 연구모델의 적합도는 일반적으로 모델적합도의 판단기준으로 사용되는 지표에서 모든 권고되는 기준을 충족하고 있는 것으로 나타났다.

표 9. 연구모델의 적합도 지수

적합도 유형	적합도 지수	권장 수용기준	모델의 통계량
절대 부합 지수	x2 / 자유도	≤ 3.00	0.96
	x2 자유도(df) p-값	≥ 0.05	80.74 84 0.581
	기초부합지수(GFI)	≥ 0.90	0.93
	표준원소평균잔차(SRMR)	≤ 0.05	0.05
	근사원소평균자승잔차 (RMSEA)	≤ 0.08	0.000
증분 부합 지수	수정부합지수(AGFI)	≥ 0.80	0.91
	표준부합지수(NFI)	≥ 0.90	0.91
	관계부합지수(RFI)	1.0근사양호	0.89
	증분부합지수(IFI)	1.0근사양호	0.99
	비교부합지수(CFI)	1.0근사양호	0.99
간명 부합 지수	간명기초부합지수(PGFI)	≥ 0.60	0.65
	간명표준부합지수(PNFI)	≥ 0.60	0.73

연구모델의 구조방정식 검정 결과는 다음의 그림 4와 같다. 일반적으로 위험분석 접근법에서는 자산의 가치나 중요도가 클수록 사용자가 인지하는 위험의 수준이 높다고 설명되고 있으며, 본 연구에서도 이러한 내용의 검정을 위해서 가설 1을 수립하였다. 그러나 연구모델에 대한 실증적인 분석결과에서는 자산의 중요도나 가치는 인지된 위험의 수준과 정의 관계를 나타내고 있으나 그 관계는 유의수준 α=0.01에서 유의하지 않은 것으로 나타났다.

한편 인지된 위협의 수준이 높을수록 그에 따른 위험 수준이 높을 것이라는 가설2는 실증분석결과 통계적으로 유의한 것으로 나타났다. 추정된 경로계수의 값이 0.429로 이상적인 수치로 권고되는 0.3을 상위하여 상당히 높은 영향을 주는 것으로 분석되었으며, 추정치의 유의수준에 있어서도 t-값이 3.990으로 나타나 유의수준 α=0.01의 t-값인 2.58과 비교할 때, 유의수준 α=0.01에서 유의한 것으로 분석되었다.

인지된 보안통제의 수준이 높을수록 인지된 위험 수준이 낮아질 것이라는 가설3도 역시 실증 분석 결과 통계적으로 유의한 것으로 나타났다. 보안통제와 위험간의 경로계수는 -0.261로 나타나 인지된 보안통제의 수준이 높을수록 전자상거래에 대한 인지된 위험이 감소하는 인과관계가 있는 것으로 설명할 수 있으며, 경로계수의 t-값도 -2.774로 분석되어 유의수준 α=0.01에서 통계적으로 유의한 결과를 나타내었다.

전체 모델을 구성하는 위험분석 방법론의 구성 개념을 구조 방정식으로 분석을 한 결과에 근거해 볼 때, 모든 적합도 지수가 일반적으로 권고되는 모델 적합도 지수를 충족시키고 있으며, 조직적 차원에서 적용되는 위험분석 접근법의 개념적인 내용들이 전자상거래를 이용하는 개인사용자 차원에서도 역시 구조

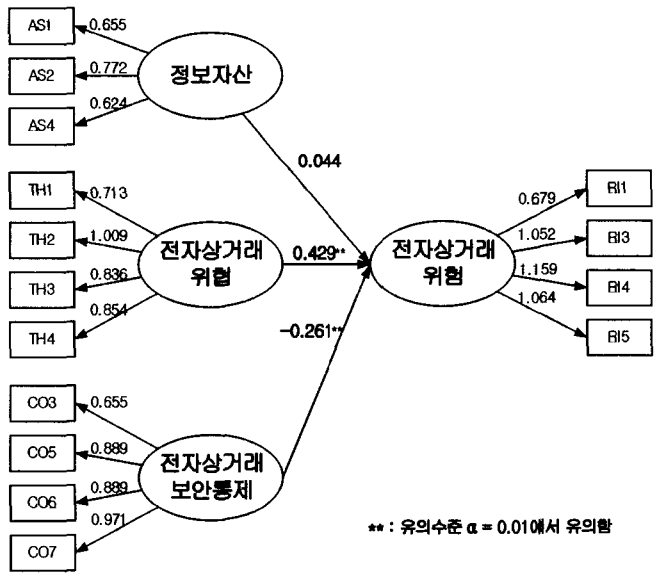


그림 4. 연구모델의 구조방정식 모델

모델의 전반적인 설명력이 높은 것으로 분석되었다. 따라서 기존의 위험분석 접근법을 인터넷 쇼핑몰의 이용과 같은 전자상거래에 적용하여 개별 사용자가 인지하는 위험수준을 평가하는 방법이 의미가 있는 것으로 설명할 수 있다.

2.4 연구결과의 논의

연구모델을 통해서 분석한 결과에서 위협과 보안통제는 위험에 영향을 주는 선행요인의 개념들로 타당한 것으로 통계적인 결과가 도출되었다. 그러나 위험분석 접근법의 개념적인 틀에서 언급되는 자산, 특히 정보자산의 중요도나 가치는 실제 사용자가 인지하는 위험과는 실증 분석결과 통계적으로 유의하지 않는 것으로 나타났다. 자산의 가치와 중요도는 실제 사용자가 인지하는 피해의 정도를 상대적으로 평가할 수 있는 대표적인 지표가 될 수 있음에도 불구하고, 본 연구의 분석결과에서는 그러한 관계가 통계적으로 유의하게 입증되지 않았다. 이러한 자산과 위험간의 관계에 대한 실증 분석의 결과는 다음과 같은 이유들로 설명될 수 있을 것이다.

먼저, 자산, 특히 정보자산에 대한 전자상거래 이용자의 과대평가의 가능성을 지적할 수 있다. 표 5의 구성개념에 대한 기술통계에 나타나 있듯이 위험분석 접근법의 다른 구성개념들의 기술 통계치와 자산의 기술 통계치는 그 평균에서 상당한 차이를 나타내고 있다. 이러한 차이는 전체 표본 집단에서 대부분의 설문 응답자들이 자신들과 관련된 개인정보를 위협의 수준이나 전자상거래를 통한 구매에서 발생할 수 있는 위험에 비해서 상대적으로 높게 인지하고 있다고 볼 수 있을 것이다. 즉, 사용자에게 그들이 가지고 있는 정보자산의 가치나 중요도를 측정하게 하는 경우 그들은 대부분 최악의 상황(worst case scenario)을 가정하고 평가를 하게 되는 특성을 가지고 있다는 것이다. 이러한 특성으로 인해서 측정하고자 하는 정보자산의 개념이 다른 개념들에 비해서 높게 평가되었을 것으로 판단된다.

한편, 사용자가 인지하고 있는 그들의 개인정보나 구매 관련 정보, 혹은 프라이버시 정보와 같은 정보자산의 가치나 중요도는 전자상거래라는 정보기술을 통해서 얻게 이익이나 효용에 대한 교환적 가치로 사용자가 인지하고 있을 수 있다는 점을 살펴볼 필요가 있다. 또 다른 가능성으로는 실제 전자상거래를 이용하는 대부분의 사용자들이 개인정보 유출의 피해를 직접 경험하지 않은 경우가 대부분일 것이라는 점을 감안할 때, 그들이 직접 소유하고 있는 자산의 중요도나 가치에 비해서 위험이라는 개념이 직접경험에 의해서 체득되었거나 직접적으로 평가된 것이 아니라는 점에서 상대적으로 정보자산의 가치가 높게 평가가 되었을 가능성도 있을 것으로 판단된다.

IV. 연구의 의의 및 결론

본 연구의 주요한 의의로는 위험분석접근법에 대한 실증적인 분석을 수행하였다는 점으로 설명될 수 있다. 특히, 다수의 위험분석방법론이 평가자의 인지수준에 기초하여 분석이 수행되는 점을 고려할 때, 전자상거래 이용자의 위험인지에 영향을 미치는 요인을 위험분석 접근법을 이용하여 모델화한 검증을 함으로써 전자상거래 위험에 영향을 미치는 선행요인을 규명할 뿐만 아니라 위험분석접근법 자체의 타당성도 검토하고 있다는 점을 연구의 의의로 볼 수 있다.

본질적으로 자산 특히 사용자와 관련된 개인정보 자산과 같은 항목은 위험과의 관련성이 낮다는 점에서 전자상거래의 위험을 연구함에 있어 배제할 수 있는 개념으로 간주하는 것이 아니라, 사용자들이 기본적으로 그 가치나 중요도를 높게 평가한다는 점에서 전반적인 보안통제와 위협의 관리와 함께 부가적으로 정보자산에 대한 관리와 관심을 기울일 필요가 있다는 점으로 해석을 하는 것이 타당하다고 판단된다.

향후 연구에 있어서는 전자상거래 이용경험이나 보안침해 사고 경험을 조절변수로 연구모델에 추가하여 연구가 이루어질 수 있을 것으로 판단된다. 또한, 본 연구에서 적용한 전자상거래라는 상황적 요인과 그리고 그러한 환경에서 적용될 수 있는 세부적인 자산항목에 대한 추가적인 분석이 필요할 것이며, 보다 광범위한 사용자를 대상으로 한 실증적인 연구과정을 통해 위험분석모델을 일반화할 수 있는 외적타당성을 보다 높일 수 있도록 하는 것이 필요하다.

참 고 문 헌

[1] ISO/IEC JTC1 SC27, Guidelines for the management of IT security(GMITS) -Part 1: Concepts and models of IT security, TR 13335-1, 2000.

[2] ISO/IEC 17799:2000, Information technology-Code of practice for information

security management, 2000.
[3] 김영걸, 이종만, 이재남, "정보시스템의 위험도 분석에 대한 연구: 통합적 분석 틀을 중심으로," 경영정보학연구, 8권 2호, pp. 37-53, 1998.
[4] Mayer, R., J. Davis, and F. Schoorman, "An Integrative Model of Organizational Trust," Academy of Management Review, Vol. 20, No. 3, pp. 709-734, 1995
[5] Salam, F., R. Rao, and C. Pegels, "An Investigation of Consumer-perceived Risk on Electronic Commerce Transactions: The Role of Institutional Trust and Economic Incentive in a Social Exchange Framework," Proceedings of Americas Conference on Information Systems, pp. 335-337, 1998
[6] Jarvenpaa, S., N. Tractinsky, and M. Vitale, "Consumer trust in an Internet store," Information Technology and Management, Vol. 1, No. 1, pp. 45-71, 2000.
[7] Kim, K., and B. Prabhakar, "Initial Trust, Perceived Risk, and the Adoption of Internet Banking," Proceedings of International Conference on Information Systems, pp. 537-543, 2000.
[8] Pavlou, P., "Institution-based trust in interorganizational exchange relationships: the role of online B2B marketplaces on trust formation," Strategic Information Systems, Vol. 11, No. 3, pp. 215-243, 2002.
[9] 이성만, 이필중, "해외의 보안위험분석 방법론 현황 및 분석," 한국통신정보보호학회지, 4권 1호,pp. 316-323, 1994.
[10] BSI, BS7799: Code of Practices for information Security Management, United Kingdom, 1999.
[11] CCTA, United Kingdom Government CRAMM User Guide, 2001.
[12] KPMG Peat Marwick LLP, Vulnerability Assessment Framework 1.1, Critical Infrastructure Assurance Office, October 1998.
[13] CSE, Guide to Security Risk Management for IT Systems, Government of Canada, Communications Security Establishment, 1996
[14] GAO, Information Security Risk Assessment-Practices of Leading Organizations, Exposure Draft, U.S. General Accounting Office, August 1999.
[15] CSI, IPAK : Information Protection Assessment Kit, Computer Security Institute, 1997.
[16] Peltier, T., Information Security Risk Analysis, Auerbach, 2001.
[17] Loch, K., H. Carr, and M. Warkentin, "Threats to Information Systems: Today's Reality, Yesterday's Understanding," MIS Quarterly, Vol. 16, No. 2, pp. 173-186, 1992.
[18] Otwell, K., and B. Aldridge, "The Role of Vulnerability in Risk Management," IEEE Proceedings of the Fifth Annual Computer Security Application Conference, pp. 32-38, 1989.
[19] Torkzadeh, G., and G. Dhillon, "Measuring Factors the Influence the Sucess of Internet Commerce," Information System Research, Vol. 13, No. 2, pp. 187-204, 2002.
[20] Kim, D., Y. Song, S. Braynov, and R. Rao, "A B-To-C Trust Model for On-Line Exchange," Proceedings of Seventh Americas Conference on Information Systems, pp. 784-787, 2001.
[21] NIST, Risk Management Guide for Information Technology Systems- Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-30, October 1998.
[22] CMU/SEI, Operationally Critical Threat, Asset, Vulnerability Evaluation(OCTAVE) Framework, Version 1.0, CMU/SEI-99-TR-017, June 1999.
[23] Garver, M., and J., Mentzer, "Logistics

Research Methods : Employing Structural Equation Modeling to Test for Construct Validity," Journal of Business Logistics, Vol. 20, No. 1, pp. 33-57, 1999.

[24] Burt, S., "Interpretational Confounding of Unobserved Variables in Structural Equation Models," Sociological Methods and Research, Vol. 5, pp. 3-52, 1976.

[25] Gerbing, D., and J. Anderson, "An Updated Paradigm for Scale Development Incorporating Unidimensionality and Its Assessment," Journal of Marketing Research, Vol. 25, pp. 186-192, 1988.

[26] Gefen, D., "E-Commerce: The Role of Familiarity and Trust," Omega, Vol. 28, No. 6, pp. 725-737, 2000.

[27] Gefen, D., E. Karahanna, and D. Straub, "Trust and TAM in Online Shopping: An Integrated Model," MIS Quarterly, Vol. 27, No. 1, pp. 51-90, 2003.

[28] Chau, P., "On the use of construct reliability in MIS research: a meta analysis," Information and Management, Vol. 35, No. 4, pp. 217-228, 1999.

[29] Peter, J., "Reliability: A Review of Psychometric Basics and Recent Marketing Practices," Journal of Marketing Research, Vol. 16 No. 1, pp. 6-17, 1979.

[30] Fornell, C., and D. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," Journal of Marketing Research, Vol. 18, pp. 39-50, 1981.

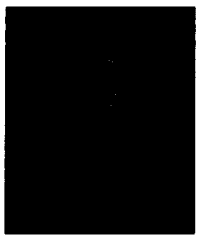
[31] 채서일, 사회과학 조사방법론, 2판, 학현사, 1995.

[32] Gefen, D., "Assessing Unidimensionality through LISREL: An Explanation and Example," Communications of the Association for Information Systems, Vol. 12, pp. 23-47, 2003.

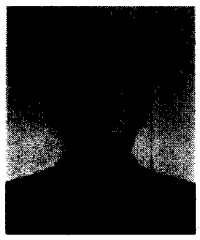
[33] Bagozzi, R., and L. Phillips, "Representing and Testing Organizational Theories : A Holistic Construct," Administrative Science Quarterly, Vol. 23, No. 3, pp. 459-489, 1982.

[34] Anderson, J., "An Approach for Confirmatory Measurement and Structural Equation Modeling of Organizational Properties," Management Science, Vol. 33, No. 4, pp. 525-541, 1987.

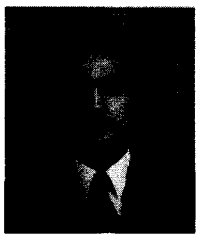
〈著者紹介〉



김 종 기(Jongki Kim)
1987년 : 부산대학교 경영학과 졸업
1988년 : Arkansas State University, MBA
1992년 : Mississippi State University, Ph.D in MIS
1993년 3월~1998년 12월 : 국방정보체계연구소 선임연구원
1999년 3월~현재 : 부산대학교 경영학부 조교수
〈관심분야〉 정보시스템보안관리, 전자상거래, 프로젝트관리



이 동 호(Dongho Lee)
1995년 2월 : 부산대학교 경영학과 졸업
1998년 2월 : 부산대학교 대학원 경영학 석사
2004년 2월 : 부산대학교 대학원 경영학 박사(경영정보·생산관리 전공)
2004년 3월~현재 : 부산대학교 경영경제연구소 전임연구원
〈관심분야〉 정보시스템보안관리, 전자상거래(E-Biz), 웹기반어플리케이션 설계/개발



서 창 갑(Changgab Seo)
1992년 2월 : 경남대학교 경영학과 졸업
1994년 8월 : 서강대학교 대학원 경영학석사(MIS전공)
1999년 2월 : 서강대학교 대학원 경영학박사(MIS전공)
1999년 9월~현재 : 동명정보대학교 경영학과 조교수
〈관심분야〉 전통기업의 e-비즈니스화, 정보시스템가치측정, e-Learning 등