

## 전자상거래 사용자의 신뢰에 영향을 미치는 정보보안위험 기반의 선행요인 연구\*

김 종 기\*\*, 이 동 호\*\*\*

### A Research on Information Security Risk-based Antecedents Influencing Electronic Commerce User's Trust

Jongki Kim, Dongho Lee

It is generally believed that, compared to traditional commerce, Electronic Commerce(EC) is more difficult to gain and sustain customers. One of the major reasons that customers do not use EC is lack of trust. Previous researches on the EC user's trust suggested that risk is an antecedent of trust and the concept of trust is highly related to risk.

This study proposed a combined model in which includes the factors based on generic information security risk analysis methodology and trust factors in EC. The objectives of this study are follows; first, investigating the relationship between trust and risk that are antecedent factors of purchase intention, and second, examining the validity of information security risk analysis approach in EC environment.

Based on the survey results of 143 MBA students statistical analysis showed that factors like threats and controls were significantly related to risk, but assets did not have statistically significant relationship with risk. Controls and knowledge of EC had meaningful effect on user's trust. This study found that risk analysis methodology which is generally used at organizational level is practically useful at user level on EC environment. In conclusion, the results of this study would be applied to generic situation of information security for analyzing and managing the risk. Besides, this study emphasized that EC vendors need to pay more attention to the information security risk to gain customer's trust.

**Keywords :** Electronic Commerce, Risk Analysis Model, EC User's Trust, IS Security, Structural Equation Model

\* 이 논문은 2003년도 한국학술진흥재단의 지원에 의하여 연구되었음(KRF-2003-003-B00065).

\*\* 주저자, 부산대학교 경영학부 조교수

\*\*\* 교신저자, 동명정보대학교 유통경영학과 전임강사

## I. 서론

경제활동은 관련 당사자들 사이의 신뢰를 기반으로 이루어진다. 거래 당사자 간의 대면접촉을 통한 전통적인 상거래와 달리 웹을 통한 제한적인 상호작용을 통하여 거래가 이루어지는 전자상거래의 비가시적 특성으로 인하여 전자상거래 업체에 대한 신뢰가 고객 확보에 매우 중요한 요인으로 작용한다[Javenpaa et al., 2000; Reichheld and Scheffer, 2000; Gefen, 2002]. 한편, 소비자가 전자상거래를 이용하지 않는 이유로 가장 많이 언급되는 것 중에 하나가 바로 신뢰의 결여이다[Hoffman et al., 1999; Cheung and Lee, 2000]. 더욱이 정보보안에 매우 취약한 인터넷 기반의 정보기술을 사용하는 전자상거래에 대한 소비자의 우려는 전자상거래의 신뢰에 심각한 영향을 미치고 있다. 따라서 전자상거래 소비자의 구매 의도를 이해하는데 있어서 신뢰의 특성과 선행요인을 이해하는 것은 매우 중요하다[McKnight et al., 2002b; Gefen et al., 2003].

정보보안 분야에서는 정보시스템 보안계획 수립을 위한 분석적 틀로써 위험분석 방법론을 널리 활용하고 있다[김영결 등, 1998; Rainer et al., 1989; Barnard and Von Solms, 2000]. 위험분석은 정보시스템에 내재한 보안상의 약점과 외부의 위협요인을 고려하여 최적의 보안대책을 모색하는 체계적인 절차이며, ISO/IEC에 의해서 국제표준으로 제정되어 있다[ISO/IEC, 2000]. 위험분석에 있어서 핵심적인 내용은 정보시스템의 활용에 따른 보안상의 문제점에 대한 인지된 위험수준의 평가이다. 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 자체

의 타당성에 대한 연구는 거의 없는 실정이며, 전자상거래 이용자가 인지하고 있는 위험이 전자상거래를 이용하려는 의도에 어떠한 영향을 미치고 있는 지에 대한 연구도 그다지 많지 않다.

본 연구에서는 전자상거래의 이용에 영향을 미치는 다수의 요인들 중에서 중요하게 언급되는 신뢰와 그 선행요인으로서 위험에 대한 모델을 개발하고 실증적인 분석을 수행하였다. 본 연구의 주요 목적은 다음의 두 가지이다. 첫 번째는 전자상거래의 신뢰에 영향을 미치는 선행요인으로 위험의 의미를 실증적으로 규명하고자 한다. 즉, 신뢰의 개념이 실제 전자상거래를 이용하는 데 주요한 역할을 하고 있는지, 그리고 전자상거래를 이용하는데 있어서 발생하는 위험이 사용자가 인지하고 있는 신뢰의 개념과 어떠한 관계를 가지고 있는지를 분석하고자 한다.

두 번째는 위험분석 방법론에 대한 실증적인 분석을 통하여 위험분석 접근법의 타당성을 평가한다. 다수의 실무적인 문헌들과 이론적인 연구들 그리고 국제표준 문서들에서는 위험분석 접근법이 개념적으로 타당한 것으로 설명되고 있다. 그러나 이러한 위험분석 접근법이 전자상거래를 이용하는 개인 사용자가 인지하는 정보자산, 위협, 보안통제가 위험과 관련되어 있는지에 대한 실증적인 연구는 아직 미흡한 실정이다. 즉, 위험이라는 개념이 기존의 조직적 차원에서의 자산, 위협, 보안통제와 같은 주요한 요인의 관계함수로 정의되어 있는데, 이러한 위험의 선행요인들을 통해서 전자상거래에서 발생하는 위험에 대한 사용자의 인지를 실증적으로 검증함으로써 위험분석 방법론에 대한 타당성을 확인하고자 한다.

## II. 이론적 배경

### 2.1 전자상거래에서 신뢰의 개념과 특성

인터넷 쇼핑물과 같은 전자상거래의 이용에

있어서 중요한 영향요인으로 신뢰에 대한 개념적인 정의는 연구자에 따라서 다양하게 논의되고 있다[McKnight et al., 2002a]. 신뢰와 관련된 문헌연구들은 크게 개념적인 신뢰에 대한 내용을 다루고 있는 연구들과 실증적인 차원에서 신뢰를 논의하고 있는 연구로 나누어 볼 수 있는데, 먼저 신뢰에 대한 개념적 차원에서의 연구를 살펴보면 Mayer et al.[1995]은 신뢰라는 개념을 특정의 행위와 관련된 개인의 의도나 신념이라고 정의를 내리고 있다. 이러한 신뢰는 구매행위, 선택결정과 같은 구체적인 행동을 야기할 수 있는 선행요인의 개념으로 설명하고 있으며, 위협의 개념과 상당한 관련이 있는 것으로 설명하고 있다.

Luhmann[1979]은 확신이라는 개념과 신뢰와의 차이를 위협과 관련된 문제로 설명하며 특정의 상황에서 손실이나 피해를 입을 가능성에 노출되는 것으로 구분하고 있으며, Roy et al.[2001]도 역시 위협과의 관련성을 신뢰에 있어서 가장 핵심적인 것으로 설명하고 있다. 이러한 관점 외에도 개인이나 집단이 가지는 주관적인 믿음의 의지로 정의를 내리고 있는 연구들도 있는데, Morgan and Hunt[1994]는 거래상대방이 기대되는 행동을 할 것이라는 것에 대한 주관적인 믿음으로 신뢰의 개념을 정의하고 있다.

이론적인 관점에서 신뢰개념은 크게 특정의 영역에서 신뢰와 관련된 개체가 영향력을 가지게 되는 기술과 능력(ability), 신뢰자가 믿을 수 있는 혹은 믿을 만한 행동을 할 것으로 기대하게 되는 정도를 나타내는 호혜성(benevolence), 그리고 신뢰자가 수용하는 원칙이나 규칙을 피신뢰자가 어떠한 비용을 지불하더라도 지킬 것으로 인지하는 정도를 나타내는 무결성(integrity)의 세 차원으로 주로 논의가 된다[Kumar et al., 1995; Mayer et al., 1995].

한편, 신뢰의 정의에서 위협과 유사한 개념으로 취약성(vulnerability)이 있는데, 취약성의 개념은 정보보안에서의 개념과 약간의 차이가

있기는 하지만 위협과 유사한 것으로 정의된다. Rousseau et al.[1998]의 연구에서는 신뢰를 취약성을 수용하는 개인의 의지나 심리라고 정의하고 있는데, 여기서의 취약성은 불확실한 상황이나 의지 혹은 행동에 부정적인 영향을 주는 개념으로 사용되고 있다. Jarvenpaa and Todd[1997]의 연구에서도 역시 위협의 의미가 내포되어 있는 취약성을 신뢰의 정의에 있어서 중요한 개념으로 사용하고 있다. 그러나 이러한 개념적인 정의는 신뢰를 실증적으로 연구하는데 있어서 상당히 어려운 것으로 설명되기도 한다[Cowles, 1997; Jarvenpaa et al., 1998].

실증적인 차원에서 신뢰에 대한 개념을 다루고 있는 문헌연구들에서는 구체적인 행동이나 의도와 관련된 것으로 조작적인 정의를 연구에 포함하고 있다. Kim et al.[2001]은 신뢰를 그 대상에 따라서 정보에 대한 믿음, 제품에 대한 믿음과 같이 피신뢰의 대상이 되는 사람이라는 객체를 대신하여 정보나 제품과 같은 개념들에 대한 믿음이나 의지를 포함하는 개념으로 측정하고 있으며, McKnight et al.[2002a]의 연구에서는 전자상거래에서 언급되는 정책이나 법규 혹은 제3자 인증과 같은 정보시스템 보안의 차원을 포괄하는 제도적 신뢰라는 개념으로 개인 사용자의 전자상거래에 대한 신뢰의 개념을 측정하고 있다. Kini and Choobineh[2000]의 연구에서도 신뢰의 개념을 보안, 신뢰성, 능력의 세 차원으로 구분하여 연구를 수행하였으며, 신뢰와 관련된 요인으로 보안을 신뢰의 차원에 포함하여 연구를 수행하고 있다. 이외에도 신뢰와 관련된 연구들을 요약하면 <표 1>과 같이 나타낼 수 있다.

신뢰에 대한 문헌연구를 통해서 신뢰의 개념을 확률적인 위험을 수반하는 상황 하에서 신뢰의 주체가 가지고 있는 수단이나 방법, 사람이나 사물 등을 모두 포함하는 특정의 객체에 대해서 기대하는 사건이나 행위에 대한 믿음의 의지나 의도라고 정의할 수 있으며, 전자상거래

<표 1> 신뢰관련 연구 요약

연구자	신뢰개념	선행요인	결과요인
Anderson and Narus [1990]	다른 기업의 행동에 대한 기대	의사소통, 상대적 이익	만족
Crosby et al.[1990]	고객의 이해를 고려하는 행동에 대한 확신		지속적인 거래 기대
Gannesan[1994]	신용성, 무결성, 호혜성을 포함하는 믿음의 의지	규모, 평판, 경험, 만족	장기적인 관계
Morgan and Hunt [1994]	확신이 있는 집단에 대한 믿음 의지	공유가치, 의사소통, 기회행동	관계몰입, 협력, 갈등, 불확실성
Kumar et al.[1995]	정직성과 호혜성의 개념	경험, 관계의 질, 환경의 불확실성	장기적 관계, 획득 효익
Mayer et al.[1995]	위험상황 하에서의 믿음에 대한 의지	신뢰성향, 능력, 호혜성, 무결성	
Doney and Cannon [1997]	인지된 무결성, 호혜성	규모, 평판, 고객화의 의지, 기밀정보 공유	구매결정 장기적인 관계
Doney et al.[1998]	다른 사람에 대한 믿음 의지	규모, 평판, 고객화의 의지, 기밀정보 공유	구매결정 장기적인 관계
Jarvenpaa et al.[1998]	정직한 행위를 할 것이라는 기대에 대한 의지	인지된 규모, 인지된 평판	인지된 위험, 태도, 구매의도
Jarvenpaa and Todd [1999]	취약성이 존재하는 경우의 믿음의 의지	인지된 규모, 인지된 평판	인지된 위험, 태도, 구매의도
Gefen[2000]	의지하려는 의도	친밀감, 신뢰성향	구매, 방문
Jarvenpaa et al.[2000]	구매자와 판매자간의 지배구조	지각된 규모, 평판	지각된 위험, 태도, 구매의도
McKnight et al. [2002b]	신뢰 의도를 유도하는 믿음	신뢰성향, 신념, 제도기반신뢰, 구조적 보증, 인지적 과정	신뢰의도, 신뢰와 관련된 행동
Pavlou and Gefen [2002]	의지하려는 의도	제도적 구조(인증, 지불보장, 위탁)	인지된 위험, 만족, 거래의도

이용 행위를 유발하게 하는 중요한 개념으로 설명될 수 있다.

## 2.2 전자상거래에서의 정보보안관련 개념

정보보안과 관련된 개념으로는 보안통제나 인지된 위험과 같은 것을 주요요인으로 전자상거래관련 연구들에서 논의되고 있다. 가치를 가지는 자산을 보호하기 위한 기술적인 차원으로 보안통제의 개념을 선행연구들에서 설명하고 있지만 보안정책이나 교육과 같은 제도적인 차

원에서의 보안통제의 의미도 포함하고 있다. Wilson[1997]은 공개키기반구조(PKI), 전자서명, 암호화와 같은 보안기술이 전자상거래의 이용에 영향을 주는 것으로 언급하고 있으며, 이러한 논의는 Pavlou and Gefen[2002]에서도 유사하게 설명되고 있다. 이들의 연구에서는 주로 정보기술 차원의 요인들이 전자상거래의 수용 의도나 이용과 관련된 행위에 영향을 주는 것으로 나타나 있으며, 제도적인 차원의 보안기술에 대한 연구로는 조직적 차원의 보안정책이나 관리와 같은 개념들이 주요하게 사용되고 있

다. Grabner-Kraeuter[2002]는 개인정보보호정책이나 환불, 보증정책이 전자상거래이 이용에 영향을 주는 요인으로 다루고 있으며, Hoffman et al.[1999]도 역시 개인정보보호정책이나 인증마크와 같은 비기술적인 보안관련 개념에 대해 설명하고 있다.

정보보안과 관련된 개념 중에서 대부분의 문헌들에서 논의가 되는 것은 위험이다. 위험은 자원의 잠재적인 손실이나 소비자가 인지하는 부정적인 결과라고 정의할 수 있으며, 이러한 위험의 개념은 대부분의 연구들에서 인지된 위험(perceived risk)의 개념으로 언급되고 있다 [Mayer et al., 1995; Salam et al., 1998; Jarvenpaa et al., 2000]. Swaminathan et al. [1999]은 전자상거래를 통한 구매의도와 관련된 연구에서 전자상거래를 이용할 때 발생하는 위험을 사용자나 구매자가 높게 인지할수록 그 시스템에 대한 이용이나 수용이 낮아지며, 그 반대의 경우 시스템의 수용이나 구매행위가 이루어진다고 주장하고 있다.

Jarvenpaa et al.[2000]은 위험인지의 개념에 정보보안의 변수를 포함하여 신뢰의 정도가 위험인지에 영향을 주는 선행요인으로 언급하고 있으며, Kim and Prabhakar[2000]는 부정적인 결과나 영향에 대한 것을 위험의 개념으로 설명하고 있다. 이들 연구에서는 전자상거래 신뢰에 영향을 주는 주요한 요인으로 개별 사용자 혹은 구매자가 인지하는 위험을 주요한 요인으로 지적하고 있으며, 인지된 위험은 전자상거래를 이용함으로써 발생하는 상대적인 이익과 그러한 이용을 통해서 발생하는 부정적인 결과간의 인지차이를 의미하는 것으로 주장하고 있다. Pavlou[2001]의 연구에서는 재무적인 관점의 위험만이 아니라 전자상거래에서 발생할 수 있는 정보차원의 위험도 포함하고 있다.

한편, 위험과 신뢰를 연구에 포함하고 있는 문헌들에서는 신뢰와 위험 중에서 어떤 요인을 선행요인으로 볼 것인가에 대한 관점의 차이가

있다. 김정규 등[2003]은 “신뢰와 위험의 관계는 상호 작용을 하며 복잡하기 때문에 인과 관계를 설정하기가 매우 어렵다”(p.1774)고 전제하고, 이들 사이의 관계를 양방향적 인과관계로 보았다. <표 2>에서 나타난 바와 같이 Jarvenpaa et al.[2000], Pavlou[2001, 2002], Gefen [2002]과 같은 연구들은 신뢰를 위험의 선행요인으로 보고 있는 반면에, Dayal et al.[1999], Chellappa and Pavlou[2002], Suh and Han [2003], Gefen et al.[2003]등과 같은 연구들은 위험을 신뢰의 선행요인으로 보고 있다. 신뢰와 위험의 관계에 대한 연구들에서 주목해야 할 것은 신뢰와 위험 중에 어느 것이 선행요인이나에 관계없이 둘 다 전자상거래를 이용하려는 의도나 이용에 영향을 미치는 주요한 선행요인이라는 점은 공통적이다.

## 2.3 위험분석모델

전자상거래와 관련된 연구들에서의 위험개념은 위험분석관련 연구나 실무에서의 위험과 유사한 특성을 가지고 있다. 그러나 세부적인 위험에 대한 분석에 있어서 정보보안 관련연구에서는 자산, 위험, 보안통제와 같은 다른 개념들과의 관계를 통해서 체계적으로 설명되고 있다. 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[CSE, 1996].

위험분석모델은 위험분석에 적용되는 개념적인 틀로서, 위험에 대한 체계적인 접근과 분석을 위한 지침으로 활용된다. 위험분석의 공정은 기본적으로 보호대상 정보자원의 식별과 자산

<표 2> 보안관련 연구 요약

연구자	사용된 보안관련 개념	선행요인	결과요인
김경규 등[2003]	위험의 규모, 가용성, 신뢰성, 보안		신뢰
Mayer et al.[1995]	인지된 위험, 정보 오/남용의 능력, 정보 무결성	능력, 호혜성, 무결성, 개인의 신뢰성향	위험수용, 구매행동
Selnes[1996]	인지된 위험	사용자 만족, 몰입, 의사소통	지속성, 향상
Cowles[1997]	조직수준의 보안대책		신뢰
Ratnasingham[1998a]	보안통제나 제반 기술		웹을 통한 구매
Salam et al.[1998]	인지된 위험, 제3자나 제도적인 기구에 의한 보증		인지된 인터넷을 통한 거래 위험
Dayal et al.[1999]	지불보안, 거래정보보안, 개인정보 보호		신뢰
Hoffman et al.[1999]	프라이버시, 개인정보		인터넷 구매
Cheng and Lee[2000]	인터넷 판매자의 신뢰성, 외부환경, 인지된 위험		신뢰
Jarvenpaa et al.[2000]	인지된 위험	신뢰	구매의도, 인터넷 쇼핑 태도
Kim and Prabhakar [2000]	인지된 위험, 제도적 보증	개인 신뢰성향, 구전효과	구매행동
Kim et al.[(2001]	정보기술 인프라의 수준, 제3자의 제도적 보증	정보내용, 제품, 거래, 기술, 제도, 소비자행동	신뢰
Pavlou[2001]	인지된 위험, 프라이버시 인지, 보안 인지	신뢰	구매의도
Chellappa and Pavlou [2002]	인지된 정보보안	암호화, 보호, 식별, 인증	전자상거래 신뢰
Gefen[2002]	인지된 위험, 제3자 보증	신뢰	고객충성도
McKnight et al.[2002a]	웹사이트의 구조적 보증, 인지된 웹 위험	판매자의 평판과 품질	웹 구매의도, 개인정보제공의도, 신뢰
Olivero and Lunt [2002]	개인정보 보호		전자상거래 이용
Pavlou and Gefen [2002]	제도적 인증, 인지된 위험	인지된 위험, 신뢰, 만족	신뢰, 인터넷을 통한 구매의도
Pavlou[2002]	인지된 위험, 제도기반 신뢰	호혜성, 신뢰성	구매만족, 지속적 구매행동
Shankar et al.[2002]	프라이버시, 지불보안, 제3자 인증		온라인 신뢰
Torkzadeh and Dhillon [2002]	개인정보 오남용, 지불 보안, 전자상거래 처리 보안		용이성, 유용성, 사용의도
Gefen et al.[2003]	제도 기반 구조적 보증		신뢰
Kim et al.[2003]	제3자 인증마크, 프라이버시 보호, 보안보호수준		신뢰
Suh and Han[2003]	인증성, 부인거부, 비밀성, 프라이버시 보호, 자료 무결성		신뢰

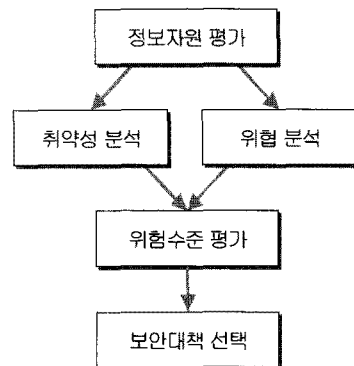
에 관련된 취약성과 위협의 수준, 그리고 그러한 관계를 통해서 산출되는 위협의 수준을 완화하기 위한 보안대책을 선정하는 과정으로 구성된다. 즉, 위험분석모델은 위험관리의 목적과 자산, 위협, 취약성과 같은 위험관리 요소의 식별과 이러한 요소들 간의 상호관계를 기술하는 것이며 위험관리 방법론은 실제적인 위험관리를 수행하기에 필요한 구체적인 절차와 단계 기법 등을 설명하는 것이다.

위험분석모델을 구성하는 요소들은 자산, 위협, 취약성, 보안통제와 같은 다양하게 구성되어 있으며[이성만과 이필중, 1994], 이러한 위험분석 모델 중에서 대표적인 것이 ISO/IEC[2000]의 모델이다. 이 모델에서는 위협이라는 개념을 자산, 사업영향, 가치, 보호요구사항, 보안대책, 위협, 취약성 등이 관련된 복합함수로 정의하고 있다. 이와 유사하게 BS7799[BSI, 1999]의 정보보안관리체계의 수립과정에서는 위협의 평가와 관리의 개념을 자산의 가치나 중요도, 취약성의 수준, 위협의 빈도나 심각성과 같이 자산, 취약성, 위협의 함수로 정의하고, 이러한 함수관계를 통해서 해당조직의 위협수준을 평가하고 결정하는 방법을 제안하고 있다[BSI, 1999]. BS7799[BSI, 1999]에서 논의되는 위험분석모델은 위협이라는 개념을 자산과 위협 그리고 취약성이라는 요소를 통해서 설명하고 있으며, 근본적인 틀은 ISO/IEC[2000]와 크게 다르지 않다고 볼 수 있다.

앞서 설명한 두 위험분석모델은 기본적으로 자산을 기반으로 하는 위험분석방법론의 성격을 가지고 있으며, CRAMM과 같은 위험분석 방법론[CCTA, 2001]도 거의 유사한 위험분석 모델로 구성되어 있다. 물론 이러한 자산기반의 위험분석 접근법외에도 취약성을 중점적으로 다루는 VAF[KPMG, 1996]나 위협을 중심으로 하는 CSE[1996]나 GAO[1999]와 같은 방법론에서도 세부적으로는 약간의 차이가 있으나 기본적인 틀은 ISO/IEC[2000] 모델이나 BS7799 [BSI, 1999]와 상당한 유사성을 가지고 있다.

위험분석모델과 관련된 접근법들을 살펴보면, 앞서 논의한 방법론들을 보다 간결하게 적용하고 있는 방법론도 있다. 이러한 위험분석 방법으로 대표적인 것으로 IPAK[CSI, 1997]이나 FRAP[Peltier, 2001]과 같은 것이 있으며, 이러한 방법론들에서는 위협을 자산과 위협간의 관계로 혹은 보안대책의 수준과 자산의 가치와의 상호평가를 통해서 혹은 특정의 보안대책과 관련된 항목들의 검증을 통해 접근하는 방법을 취하고 있다.

정보보안의 위험분석 접근법에서 공통적으로 수행되는 공정과 요소들에 대해서 요약하면 <그림 1>로 나타낼 수 있다. 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 전자상거래 환경에서 그 적용 범위와 대상의 특성으로 인해서 제외되며, 정보 자산 특히 개인정보나 구매정보, 배송정보와 같은 무형자산이 해당된다.



<그림 1> 일반적인 위험분석 절차

자산의 식별과 평가의 과정은 위험분석과 관리에 있어서 보호하고자 하는 대상의 선정과 구현되는 보안 대책의 식별에 중요한 영향을 미친다. 자산에 대한 식별과 평가는 정보보안의 3대 요소인 기밀성, 무결성, 가용성의 차원에서 평가되며, 이외에도 BS7799[BSI, 1999]와 ISO/IEC [2000]에서는 수익의 감소, 시장점유율, 기업이 미지와 같은 항목을 추가적으로 고려하는 것을 권장하기도 한다.

다음은 정보시스템 보안상의 취약성과 위협요인을 식별하고 평가하는 공정이다. 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 결합)으로 구분할 수 있다[Loch et al., 1992]. 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 BS7799[BSI, 1999]나 ISO/IEC[2000] 그리고 CSE[1996]에서는 자산이 가진 약점이라는 차원에서 다루어지고 있으며, 실무적인 성격을 가지는 IPAK[CSI, 1997]이나 FRAP[Peltier, 2001]에서는 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 정의하고 있다[Otwell and Aldridge, 1989].

취약성은 자산, 위협, 보안대책과 연계되어 식별되고 CRAMM에서도 이러한 이유로 취약성을 별도로 식별하여 평가하지 않고 위협과 연

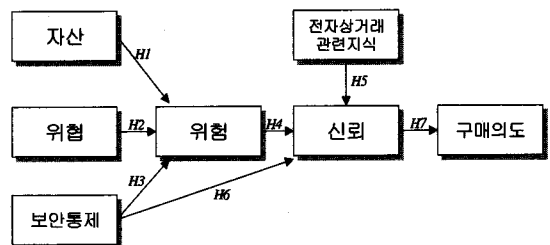
계하여 평가하는 접근법을 취하고 있다. 본 연구에서도 취약성을 전자상거래를 이용하는 일반사용자가 취약성에 대한 개념의 정확한 이해를 하기 힘들 것이라는 이유에서 보안대책이라는 개념을 통해 취약성의 개념을 대체하여 측정하였다.

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 위협을 자산과 위협 그리고 취약성과의 관계로 평가하고 해당위험을 완화하는 적절한 보안대책을 수립하고 선택하는 일련의 과정을 거친다.

### III. 연구모델과 가설

#### 3.1 연구모델

본 연구에서는 전자상거래 이용에 영향을 미치는 신뢰의 선행요인을 정보보안 위험분석의 관점에서 접근하는 연구모델을 <그림 2>와 같이 구성하였다.



<그림 2> 연구모델

연구모델은 크게 세 부분으로 구성되어 있다. 우선 위협에 영향을 미치는 요인들로 자산, 위



협 및 보안통제와 위협간의 관계에 대한 것으로 위험분석 접근법에서 논의되는 주요한 개념들이 타당한지를 실증적으로 분석하기 위한 것이다. 두 번째는 신뢰에 영향을 미치는 요인들로 위협과 전자상거래 관련지식, 그리고 보안통제 요인과 신뢰와의 관계로 구성되었다. 마지막 부분은 신뢰와 구매의도간의 관계이다.

설문항목을 작성하는 과정인 연구도구의 개발과정에서는 가급적 선행연구에서 검증된 연구도구를 사용하는 것이 연구도구의 신뢰성과 타당성 측면에서 바람직하다[Straub, 1989]. 앞서 살펴본 선행연구에서 사용된 전자상거래 이용의도, 신뢰, 사용자의 전자상거래 관련지식 등과 같은 개념을 측정하는 변수들은 다양한 문헌 연구에서 설명되거나 사용되는 기존의 측정항목을 적극적으로 수용하였다. 그러나 실증적 연구가 거의 이루어지지 않은 위험분석 방법론 관련 개념들이 포함되어 있으므로 사전조사와 함께 엄격한 연구도구 검증과정을 거쳐 연구모델을 분석하였다.

### 3.1.1 자산

자산은 보호할 가치가 있는 혹은 그러한 자산이 소유자나 관련된 조직에서 중요한 의미를 가지는 유형, 무형의 모든 것이다[CSE, 1996; CSI, 1997; BSI, 1999; ISO/IEC, 2000]. 즉, 조직이나 개인이 가지고 있는 유형/무형의 가치가 있는 재화나 서비스를 지칭하며, 물리적 자산, 소프트웨어 자산, 조직이나 개인의 무형 이미지등을 포괄하는 개념으로 사용된다. 위험분석 방법론에서 설명하는 자산의 개념 중에서 전자상거래와 관련되어 있는 사용자 측면의 자산은 전자상거래를 사용함에 있어서 발생하는 제품이나 서비스의 구매정보나 지불과 관련된 사용자의 정보 혹은 개인의 프라이버시와 관련된 개인정보에 한정된다.

위험분석 접근법외에 전자상거래와 관련된 기

존의 연구들에서도 정보자산, 특히 개인정보를 중요한 요인으로 다루고 있는 연구가 다수 있는데, 이러한 연구들에서는 제공되는 정보의 중요도나 가치[Kini and Choobineh, 2000; Pavlou and Gefen, 2002], 개인정보나 프라이버시 정보의 중요성[Kini and Choobineh, 2000; Kim et al., 2001; Salisbury et al., 2001; Torkzadeh and Dhillon, 2002], 판매업자와의 개인정보 제공과 공유수준[Hoffman et al., 1999]과 같이 전자상거래를 이용하는 데 사용되는 프라이버시 관련 정보나 제품의 구매 정보와 같은 정보자산에 대한 개념으로 위험 방법론에서 언급하고 있는 자산과 동일한 차원의 개념으로 사용되고 있다.

본 연구에서는 기존의 전자상거래와 관련하여 정보자산의 개념을 연구에 포함한 선행연구들과 위험분석 접근법과 같은 이론적인 내용들을 기반으로 하여 정보보안에서 논의되는 정보자산의 개념을 적용하며, 정보자산의 범주와 평가에 관한 내용들은 기존의 문헌연구들과 위험분석 접근법의 이론들을 참고하여 측정항목을 개발하였다. 또한, 전자상거래를 이용하는 사용자의 주관적인 정보자산의 인지도나 평가가 주요한 변수로 설정되고, 정보자산이라는 무형자산의 평가를 위해서 정성적인 방법론의 관점에서 개별 항목을 정의하였다.

### 3.1.2 위협

위협이라는 개념은 자산에 대해서 잠재적인 손실이나 파괴를 가져올 수 있는 의도되거나 의도되지 않은 행위나 사건을 의미하며, 자산에 부정적인 피해를 줄 수 있는 위협의 원천으로 정의된다[BSI, 1999; ISO/IEC, 2000]. 위협의 개념에서 주요한 특징은 사건이 발생할 수 있는 확률적 개념이라는 것이다. 대부분의 위험분석 방법론에서는 발생원천에 따라 내부와 외부위협으로 구분하고, 발생할 확률의 수준과 심각성

의 차원으로 평가한다.

전자상거래와 관련된 연구들에서 위협의 개념을 위험분석 접근법에서처럼 적용하는 경우는 없지만, 연구에 사용된 변수나 설문문의 세부적인 내용들에서 상당히 유사한 개념적인 정의가 이루어지고 있다. Jarvenpaa et al.[2000]과 Pavlou and Gefen[2002]은 정보보안 차원에서 위협개념과 유사한 개념으로 잠재적인 손실의 발생 확률이나 빈도를 연구에 포함하고 있으며, 개인정보와 같은 정보자산에 영향을 미칠 수 있는 위협의 개념으로 개인정보 유출의 확률이나 빈도[Urban et al., 2000]나 개인정보의 외부 노출[Olivero and Lunt, 2004]의 변수를 조작적 정의를 통해서 연구에 적용하고 있다.

서비스 거부와 같이 정보보안에서 주요한 보안의 목적으로 언급되는 가용성의 위협에 대한 개념으로 Salisbury et al.[2001]은 인터넷 쇼핑몰의 이용의 장애나 이용불가의 빈도와 확률을 연구에 적용하고 있으며, 비밀성이나 인증성과 같은 개념에 대해서는 해커나 악의적인 사용자와 같은 외부로부터 발생하는 개인 정보의 이용 가능성이나 빈도에 대한 변수를 조작적으로 사용하고 있는 연구도 있다[Ratnasingham, 1998a].

이러한 위협의 구분들 중에서 전자상거래를 사용함에 있어서 주요하게 작용하게 되는 것은 인간에 의한 의도적인 위협으로서, 해커나 악의적인 사용자들에 의한 정보자산의 피해를 발생시킬 수 있는 사건의 빈도나 발생가능성, 개인정보의 권한 없는 접근이나 수정, 전자상거래를 사용하는데 발생하는 가용성의 문제와 같은 것이 있다. 본 연구에서는 위협요인에 대한 측정을 전자상거래라는 맥락에서 물리적인 위협이 아닌 정보자산과 관련되어 있는 위협의 항목들을 주요한 변수로 설정하였다.

### 3.1.3 보안통제

보안통제는 특정자산을 그와 관련된 위협으

로부터 보호할 수 있는 모든 수단이나 방법으로 정의할 수 있다[CSE, 1996; CSI, 1997; BSI, 1999; ISO/IEC, 2000]. 구체적인 보안통제에 대해서 기술적인 보안대책들이 주로 언급이 되지만, 정책이나 관리방법과 같은 비기술적인 내용도 포함된다. 암호화와 기밀성에 대한 기술적인 통제[Dayal et al., 1999; Borchers, 2001; Kim et al., 2001; McKnight et al., 2002b]나, 인터넷 쇼핑에서 지불수단에 대한 안전[Belanger et al., 2002; Torkzadeh and Dhillon, 2002; Yoon, 2002]과 같은 변수들이 기술적인 보안대책의 변수로 기존의 연구에서 사용되었다.

이외에도 Kini and Choobineh[2000], 그리고 Pavlou[2001]는 개인정보와 관련된 보안대책에 대해 개인정보의 권한 없는 수정이나 입력과 관련된 측정항목들을 보안 통제라는 변수를 사용하고 있으며, Dayal et al.[1999]과 McKnight et al.[2002a]은 개인정보 보호를 위한 전반적인 보안대책을 보안통제 관련 변수로 사용하고 있다.

비기술적인 보안통제 관련 연구변수로는 제도적인 보안 구조[Kim and Prabhakar, 2000; Urban et al., 2000; Yoon, 2002; Chen and Dhillon, 2003]와 법적인 규제[Cheung and Lee, 2000; Grazioli and Jarvenpaa, 2000; Borchers, 2001]를 활용한 연구들도 있으며, 개괄적인 차원에서의 인터넷 쇼핑에 대한 전반적인 보안수준[Pavlou, 2001; McKnight et al., 2002b]에 대한 항목으로 보안통제의 개념을 변수로 적용한 연구도 있다. 본 연구에서는 이러한 위험분석접근법에서 논의되는 이론적인 내용들과 전자상거래에서 기술적, 비기술적인 보안통제의 개념을 논의한 연구들에서 적용되어 있는 변수와 측정항목들을 근거로 관련 설문항목을 작성하였다.

### 3.1.4 위협

위험분석 방법론에서는 위협을 자산과 취약

성 그리고 위협의 조합을 통한 산술적인 계산과정을 통해서 그 수준을 평가하는데, 이렇게 평가되는 위협에 있어서 중요한 것은 실제 위협이 현실화 되었을 경우에 발생하는 자산의 영향이나 피해의 정도를 나타내는 포괄적인 개념이라는 것이다.

Salam et al.[1998]과 Cheung and Lee[2000]는 개인이 인지하는 부정적인 결과의 수준으로 위협에 대한 측정항목으로 설정하고 있으며, 전반적인 전자상거래의 위협과 관련된 측정항목이나 변수로는 인터넷쇼핑 이용의 불안감[Jarvenpaa et al., 2000; Salisbury et al., 2001; McKnight et al., 2002b], 인터넷쇼핑이용에 수반되는 위협정도[Cheung and Lee, 2000; Grazioli and Jarvenpaa, 2000; Jarvenpaa et al., 2000; Borchers, 2001]와 같은 내용들이 논의되고 있다. 한편, 전자상거래가 기반으로 하는 네트워크와 관련된 위협과 관련된 변수들에는 다른 구매수단과의 상대적 위험[Cheung and Lee, 2000; Jarvenpaa et al., 2000; Borchers, 2001; Kehoe, 2002], 인터넷쇼핑의 지불수단에 대한 위험[Gefen, 2002; Kehoe, 2002; McKnight et al., 2002a]과 같은 항목들이 위협의 수준과 평가를 하는데 사용되고 있다. 이외에도 Yoon[2000]은 전자상거래 자체가 가지는 거래의 위험성이라는 변수를 전자상거래와 관련된 위협에 대한 조작적 정의로 연구에 도입하였다.

기존의 위협과 관련된 연구들에서는 단순히 재무적인 차원에서의 피해의 개념으로 논의하고 있는 연구들도 있지만, 정보보안의 차원에서 연구들에서는 개인정보나 프라이버시와 같은 정보자산과 관련된 개념으로 위협에 대한 측정변수로 언급되고 있다. 이러한 관점에서 기존의 전자상거래와 관련된 연구들과 위협 접근법에서 논의되는 위협의 공통된 개념으로 측정항목을 본 연구에서는 적용한다. 위협을 본 연구에서는 전자상거래를 통해서 구매하는 구매자들이 인지하고 있는 위협의 조작적 정의를 통해 평가

하고, 인지된 위협과 선행 요인들과의 관계를 통해서 그 의미를 실증적으로 분석하고자 한다.

### 3.1.5 전자상거래 관련지식

전자상거래도 사용자가 이용하는 정보기술이라는 하나라고 볼 때, 전자상거래를 이용하는데 요구되는 지식은 전자상거래를 이용하려는 의도나 행동에 주요한 영향을 줄 것이다. Novak et al.[2000]과 Koufaris[2002]는 웹을 사용하는데 필요한 전문지식의 수준이라는 변수를 통해서 사용자가 알고 있는 전자상거래의 지식을 측정하고 있다. 그들의 연구에서는 인터넷을 사용하는 방법에 대한 지식의 정도와 검색과 같은 인터넷 서비스에 대한 기능적인 내용들의 인지를 전자상거래를 이용하는데 있어서 영향을 미치는 주요한 요인으로 설명하고 있다.

Gefen et al.[2003]의 연구모델에서도 전자상거래에 대한 익숙함이나 기존의 경험 그리고 웹을 통한 절차에 대한 사용자의 인지 등과 같은 지식의 개념이 신뢰에 영향을 주는 것으로 모델에 포함하여 설명하고 있다. 연구에서는 익숙함이나 구매자에 대한 신뢰는 누적된 혹은 학습된 지식과 관련성이 있으며 그 지식의 정도가 높을 경우 전자상거래 이용자들은 보다 높은 수준의 신뢰를 가지게 되는 것으로 설명하고 있다. Ratnasingham[1998b]은 전자상거래에 사용되는 관련된 유용한 기술들에 대해서 어느 정도 사용자가 알고 있는가와 같은 지식의 수준에 따라서 인터넷 쇼핑과 같은 전자상거래에 대한 사용자의 신뢰가 영향을 받는 것으로 주장하고 있다. 즉, 사용자가 암호화(encryption), 전자서명(digital signature), 인터넷 프로토콜(internet protocol)과 같은 전자상거래 관련기술에 대해서 충분한 지식이나 이해가 있는 경우 인터넷 쇼핑물 이용과 같은 전자상거래에 대한 신뢰가 더 쉽게 형성된다는 것이다[Ratnasingham, 1998a; Kehoe, 2002].

이와 비슷한 맥락에서 Kini and Choobineh [2000]는 인터넷 쇼핑물에 대한 전문적인 검색이나 이용관련 지식을 전자상거래에 영향을 주는 변수로 연구에 포함하고 있다. 전자상거래와 관련된 지식의 개념을 포함하고 있는 이러한 연구들을 근거로 본 연구에서는 전자상거래 신뢰에 영향을 미치는 요인으로 지식을 설정하였다.

### 3.1.6 신뢰

전자상거래 이용과 관련된 연구들에서 중요한 개념으로 논의되고 있는 것이 신뢰이다. 그러나 신뢰에 대한 개념적 정의와 측정은 상당히 어려운 것으로 설명된다. Mayer et al.[1995]의 연구는 대부분의 신뢰와 관련된 문헌들에서 공통적으로 인용되는 것으로 거래의 주체가 되는 소비자와 판매자 사이에서 발생할 수 있는 정직성과 믿고 의지할 수 있는 정도라는 조작적 정의를 통해서 신뢰라는 개념을 측정하고 있다. 신뢰의 주요한 측정항목으로는 판매자의 정직성[Pavlou and Gefen, 2002], 판매자 대한 믿음가능성[Grazioli and Jarvenpaa, 2000; Kehoe, 2002; Pavlou and Gefen, 2002], 판매자의 윤리성[Lau and Lee, 1999], 판매자에 대한 안전감[Lau and Lee, 1999; Grazioli and Jarvenpaa, 2000]과 같은 것이 있다.

Kim and Prabhakar[2000]의 연구와 Salisbury et al.[2001]의 연구에서는 전자상거래 채널에 대한 안전성의 개념으로 신뢰의 정도나 수준을 측정하고 있으며, 정보자산이나 제공되는 콘텐츠에 대한 신뢰의 개념으로 Hoffman et al. [1999]과 McKnight et al.[2002a]은 판매자가 제공하는 정보에 대한 신뢰를 측정 변수로 도입하고 있다. 그들의 연구에서는 인터넷 쇼핑물이 제공하는 콘텐츠나 약속과 같은 정보자산에 대한 정확성과 성실한 이행 등을 신뢰의 측정을 위한 조작적 변수로 정의하고 있다.

전자상거래 자체에 대한 믿음이나 의지의 정

도를 변수로 사용하고 있는 연구들도 있는데, 이러한 범주에 속하는 것으로는 인터넷 쇼핑에 대한 믿을 만한 가치[Grazioli and Jarvenpaa, 2000; Pavlou, 2001; Roy et al., 2001], 전자상거래 시스템에 대한 신뢰[Kini and Choobineh, 2000; Kehoe, 2002]와 같은 변수를 예로 들 수 있다. 전자상거래의 차원에서 적용되는 이러한 신뢰 개념의 측정은 앞서 언급하였듯이 다수의 선행연구들에서 실증적으로 타당한 연구도구로 충분히 논의가 되어온 설문문항이나 변수들을 가급적 최대한으로 수용하도록 하였으며, 신뢰의 차원과 관련된 부분은 전반적인 신뢰와 인터넷 쇼핑물에 대한 신뢰, 그리고 구매수단으로써의 전자상거래에 대한 매체 신뢰를 주요한 측정항목으로 설정하였다.

### 3.1.7 구매의도

구매의도는 전자상거래를 이용할 것인지, 자주 사용할 의도가 있는지와 같은 조작적인 정의를 통해서 개발된 설문항목을 연구에 적용하였다. 전자상거래와 관련된 문헌들에서는 구매의도와 관련된 개념의 조작적 정의가 직접적인 형태의 변수로 구매의도라는 용어를 설문문항으로 사용하여 측정이 되는 경우가 대부분이며 [Belanger et al., 2002; Pavlou and Gefen, 2002], 미래의 인터넷 쇼핑물 이용의도[Pavlou, 2001]나, 장기적이고 지속적인 인터넷 쇼핑물 이용의도[McKnight et al., 2002b; Shankar et al., 2002]와 같은 항목들로 구성되어 있다. 본 연구에서도 그러한 항목들을 이용하여 설문문항을 개발하였다. 연구모델을 구성하는 개념들에 대한 설문항목은 부록에 첨부하였다.

## 3.2 연구가설

연구모델에서 제시된 각 개념들 간의 경로에 대해서 검정하고자 하는 가설을 수립하였으며,

가설은 다음과 같다.

가설 1: 전자상거래 이용자가 인지하는 자산의 가치나 중요도가 높을수록 이용자가 인지하는 위협의 수준은 높아진다.

위험분석 접근법과 전자상거래와 관련된 연구들에서 사용자가 인지하고 있는 위협의 수준은 정보자산의 가치나 중요도와 상당히 높은 관련이 있는 것으로 논의되고 있다[CSI, 1997; CSE, 1998; KPMG, 1998; BSI, 1999; CMU/SEI, 1999; ISO/IEC, 2000]. 즉, 개별 사용자와 관련된 혹은 정보자산을 소유한 사용자가 인지하는 정보자산의 가치나 중요도가 클수록 그들이 위협에 대한 인지된 수준도 높아진다는 것이다. 가설 1은 이러한 정보자산의 중요도나 가치와 위협간의 관계를 검증한다.

가설 2: 전자상거래 이용자가 인지하는 위협이 클수록 이용자가 인지하는 전자상거래의 위협 수준은 높아진다.

가설 2는 위협과 위협간의 관계를 검증하기 위한 것으로, 기존의 연구들과 이론들에서는 의도하지 않는 결과를 초래할 수 있는 사건인 위협의 발생빈도나 확률이 높을수록 사용자는 그러한 위협이 실현될 때 발생하게 되는 구체적인 영향인 위협을 높게 인지하는 것으로 설명하고 있다[CSI, 1997; CSE, 1998; KPMG, 1998; CMU/SEI, 1999; GAO, 1999; ISO/IEC, 2000; Peltier, 2001].

가설 3: 전자상거래 이용자가 인지하는 보안통제의 수준이 높을수록 이용자가 인지하는 위협의 수준은 낮아진다.

위험과 관련된 선행요인 중 마지막 요인은 보안통제와 관련된 항목이다. 위험분석 접근법에

서는 보안통제의 수준이나 보안통제의 정도가 높을수록 위협을 전이시키거나 감소시킬 수 있다고 설명되고 있다[CSI, 1997; CSE, 1998; KPMG, 1998; BSI, 1999; CMU/SEI, 1999; GAO, 1999; ISO/IEC, 2000; CCTA, 2001; Peltier, 2001]. 또한, 전자상거래와 관련된 다수의 문헌들에서 보안통제와 위협간의 관계에 대한 논의가 이루어졌다[Wilson, 1997; Dayal et al., 1999; Hoffman et al., 1999; Nöteberg et al., 1999; Kim and Prabhakar, 2000; Kini and Choobineh, 2000; Kim et al., 2001; Chellappa and Pavlou, 2002; Grabner-Kraeuter, 2002; Pavlou and Gefen, 2002; Shankar et al., 2002]. 이러한 연구들을 요약하면, 전자상거래를 이용하는 데 있어서 전자상거래에 적용된 혹은 사용자가 인지하고 있는 전자상거래의 보안통제 수준이 높을수록 그와 관련된 위협의 수준이나 정도는 낮게 인식된다는 것이다. 이론적인 근거에 입각하여 가설 3을 위협과 보안통제와의 관련성의 검정을 위해서 연구가설로 설정하였다.

가설 4: 전자상거래 이용자가 인지하는 위협의 수준이 높을수록 이용자의 전자상거래에 대한 신뢰는 낮아진다.

위험과 신뢰의 관계는 연구모델을 크게 나누었을 때 두 번째 부분에 해당하는 것으로, 신뢰는 전자상거래에 있어서 주요한 요인으로 지적되고 있다[Settle et al., 1994; Mayer et al., 1995; Javenpaa and Todd, 1997; Jarvenpaa et al., 1998; Ratnasingham, 1998b; Jarvenpaa et al., 1999; Jarvenpaa et al., 2000; Kini and Choobineh, 2000; Pavlou and Gefen, 2002]. 위협과 신뢰 사이의 인과관계에 대해서는 상충되는 관점이 있지만[김경규 등, 2003], 여러 선행연구[Cowles, 1997; Dayal et al., 1999; Chellappa and Pavlou, 2002; Kim et al., 2003; Suh and Han, 2003]에서 위협을 신뢰의

선행요인으로 보고 있다. 위험을 신뢰의 선행요인으로 보는 연구들의 공통점은 위험을 정보보안과 관련된 개념으로 본다는 점이다. 본 연구는 정보보안 위험분석의 관점에서 전자상거래 이용자의 위험인지를 살펴보고자 한다.

가설 5: 전자상거래 이용자의 전자상거래 관련 지식의 수준이 높을수록 전자상거래의 신뢰는 높아진다.

가설 5는 전자상거래에서 정보기술과 관련된 지식이 신뢰에 유의한 영향을 준다는 기존의 연구들[Ratnasingham, 1998a; Ratnasingham, 1998b; Kini and Choobineh, 2000; Novak et al., 2000; Kehoe, 2002; Koufaris, 2002]을 기반으로 하여 전자상거래와 관련된 사용자의 지식수준과 신뢰와의 관계에 대한 검정을 위해서 수립되었다. 전자상거래 관련 지식 요인은 구매자가 가지고 있는 전자상거래 관련 기술에 대한 이해나 전자상거래를 이용하는데 필요한 기본적인 지식을 의미한다. 전자상거래가 이루어지는 방법에 대한 지식, 전자상거래에 사용되는 다양한 기술들에 대한 사용자의 인지가 높을수록 전자상거래에 대한 신뢰의 정도는 높아지는 것으로 설명될 수 있다. 이러한 관점에서 사용자가 전자상거래와 관련된 각종 기술적 혹은 관리적인 지식을 알고 있는 정도가 높을수록 전반적인 전자상거래에 대한 신뢰는 높아질 것으로 가설을 설정하였다.

가설 6: 전자상거래 이용자가 인지하는 보안통제의 수준이 높을수록 전자상거래의 신뢰수준은 높아진다.

전자상거래와 관련된 보안통제는 위험분석 접근법에서 뿐만 아니라 전자상거래와 관련된 다른 문헌들에서도 위험과 관련이 있는 것으로 나타나 있다[Kim and Prabhakar, 2000; Urban et al.,

2000; Pavlou, 2001; Yoon, 2002; McKnight et al., 2002a; Chen and Dhillon, 2003]. 또한, 이러한 보안통제는 사용자가 인지하고 있는 전자상거래에 대한 신뢰의 수준에도 영향을 주는 것으로 설명되고 있으며, 전자상거래를 이용하는데 있어서 전자상거래에 적용되어 있는 보안통제의 수준이 높다고 인지하는 경우 사용자는 전자상거래의 이용에 대하여 상당히 긍정적이고 높은 신뢰를 하게 될 것으로 판단되며, 이러한 내용에 대한 검정을 위해서 가설 6이 수립되었다.

가설 7: 전자상거래 이용자의 신뢰의 수준이 높을수록 전자상거래를 통한 제품이나 서비스의 구매의도가 높아진다.

마지막으로, 가설 7은 신뢰와 구매의도간의 관계에 대한 기존의 연구들[Belanger et al., 2002; McKnight et al., 2002b; Pavlou and Gefen, 2002; Shankar et al., 2002]의 내용 바탕으로 수립되었다. 개인 사용자들의 전자상거래에 대한 신뢰의 정도가 높은 경우, 그것은 구체적으로 전자상거래를 이용하고자 하는 사용의도에 상당한 영향을 미칠 것으로 판단되며, 이러한 내용이 가설에 포함되었다. 즉, 전자상거래에 대한 신뢰가 높을수록 사용자들은 구매빈도를 증가시킬 의도가 있거나, 구매횟수를 높게 할 의도가 있을 것이다. 본 연구모델에서는 사용자들의 인지된 신뢰의 수준이나 정도가 실제 전자상거래를 통한 구매의도와 유의한 관계가 있는지를 검정하기 위하여 상기의 내용으로 가설을 수립하였다.

## IV. 실증분석

### 4.1 사전조사

사전조사는 전문가 의견조사와 선행조사의 두

단계로 이루어 졌다. 먼저 관련분야 교수 및 연구원들로 구성된 전문가 집단과 면접을 통해서 개발된 연구도구의 적절성을 확인하였으며, 연구도구인 설문항목이 응답자들에게 연구자의 의도가 제대로 전달되는지 확인하기 위하여 선행 조사를 수행하였다. 전체 100부의 설문을 경영학 전공 학부 학생들을 대상으로 배포하여 이중 미회수된 설문과 성실하지 않은 답변을 한 설문을 제외한 89부의 설문을 사전조사에 사용하였다. 이러한 사전조사는 2주간의 기간을 통해서 수행, 분석, 검토되었으며, 전자상거래 이용 경험의 수준이 다른 응답자가 포함될 수 있도록 설문대상자를 선정하여 다양한 피드백을 얻을 수 있도록 하였다.

사전조사를 통해서 설문항목이 명확하지 않다고 생각되는 부분을 기록하고, 문제가 되는 항목을 응답자와의 면담을 통하여 필요한 경우 수정하거나 보완하였다. 전체 설문항목은 리커트 7점 척도의 형태로 구성되었으며, 사전조사를 통해서 초기 개발된 설문문항 중 일부가 수정되거나 삭제 혹은 새로운 용어로 변경되었다. 또한 전반적인 설문문항의 신뢰성과 타당성에 문제가 발견된 항목들은 반복적인 수정과정을 통해서 연구도구의 적절성을 확보할 수 있도록 개선, 보완되었다.

## 4.2 연구표본과 설문실시

본 연구의 모델을 검증을 위해서는 전자상거래를 충분히 경험한 집단을 선정하는 것이 중요하다. 실제 연구모델에 대한 전체 설문조사는 경영대학원 학생들을 연구 표본으로 선정하여 실시하였다. 야간에 수업이 이루어지는 경영학 석사 학위과정을 수학중인 경영대학원의 학생들은 대부분 직장인이며, 전자상거래에서 중요한 항목으로 평가되는 실질적인 구매력에서도 전체 전자상거래 이용자를 대표할 수 있는 타당성이 있다고 판단된다.

설문조사는 설문 응답자들에게 10~15분 가량의 시간을 설문응답 시간으로 할애한 뒤 설문지를 직접 회수하는 방식으로 진행하였다. 설문에 대한 높은 참여와 성실한 답변을 유도하기 위한 방법으로 모든 응답자에게 소액의 답례품을 증정하였다. 설문조사를 통해서 전체 배포 설문지 170부 중에서 93%인 158부의 설문지가 회수되었으며, 미응답항목이 있거나 성실하지 않은 답변을 한 설문지를 제외한 143부가 분석에 사용되었다.

<표 3> 연구표본의 인구통계학 자료 요약

성별	표본수(명)	비율(%)
남	128	89.4
여	15	10.6
합 계	143	100.0
인터넷 사용경력	표본수(명)	비율(%)
6개월 이하	1	0.7
1년 이하	1	0.7
3년 이하	26	18.2
5년 이하	42	29.4
5년 이상	73	51.0
합 계	143	100.0
최대구매금액	표본수(명)	비율(%)
1만원 이하	0	0
5만원 이하	14	10.5
10만원 이하	24	17.9
15만원 이하	29	21.6
20만원 이하	10	7.5
20만원 이상	57	42.5
응답합계	134	100.0
미응답	9	
총합계	143	

연구표본의 인구통계학적인 특성을 살펴보면, 먼저 연구표본 집단의 성별구성은 남성이 전체의 89.4%인 128명, 여성이 10.6%인 15명이었다. 표본의 연령층은 20대에서 50대까지 다양하

게 구성되어 있으나, 30대와 40대가 가장 많은 비중을 차지하고 있는 것으로 나타났다. 전자상거래 이용과 관련된 인터넷 사용 경력에 있어서는 전체의 80.4%가 3년 이상 인터넷을 이용한 것으로 나타났다. 표본 집단의 최대구매금액에 있어서는 전체의 90% 이상이 10만원 이상을 구매한 경험이 있는 것으로 나타나 표본집단이 전자상거래와 관련된 전반적인 위험을 충분히 인지하고 있다고 판단된다. 이러한 기술통계적인 내용은 <표 3>으로 요약하였다.

### 4.3 분석결과

본 연구에서는 구조방정식모델을 이용하여 연구모델을 분석하였다. 분석도구로는 LISREL 8.20 버전을 사용하였으며 잠재변수를 측정하기 위한 측정모델의 분석과 연구모델의 분석을 분리하여 수행하는 이 단계 접근법(two-step approach)을 적용하였다[Anderson and Gerbing, 1988]. 측정모델을 이용하여 연구 개념의 일차원성과 신뢰성 및 타당성을 검토한 후, 구조모델의 분석결과를 통하여 전체 모델의 타당성과 가설을 검증하였다.

#### 4.3.1 연구도구의 검증

##### (1) 일차원성 분석

일차원성(unidimensionality)이란 각 측정항목이 평행 상관관계 형태(parallel correlational pattern)를 가지지 않으면서 소속된 요인에만 적재되는 정도를 말하여, 요인분석의 관점에서는 하나의 요인을 구성하는 일차원성을 가진 측정항목들은 해당 요인만을 공유하며 다른 요인을 구성하는 측정항목들과는 유의한 상관관계를 가지지 않는다는 것을 의미한다[Hair et al., 1998; Gefen et al., 2000].

일차원성의 분석은 표준화된 잔차에 대한 비교를 통해서 이루어지며, 표준화된 잔차의 절대

치가 지나치게 큰 항목들은 단계적으로 제거된다[Garver and Mentzer, 1999]. 공유된 잔차 분산의 값이 지나치게 크다는 것은 측정 항목에 의해서 유의적인 수준에서 설명되지 못하는 정도가 높음을 의미하며, 또한 원소평균잔차(RMR) 혹은 표준원소평균잔차(SRMR)의 수치가 권고기준에 비해 지나치게 높은 경우나 구조방정식모델의 분석결과에서 변수의 오차항(THETA-EPS)의 수정지수가 5.0을 상회하는 경우에도 일차원성에 대한 추가적인 분석이 요구된다[Gefen et al., 2003].

일차원성에 대한 분석을 수행한 결과, 전체 41개의 설문항목들 중에서 자산요인의 2항목(AS3, AS5), 위협요인의 3항목(TH5, TH6, TH7) 보안통제의 3항목(CO1, CO2, CO4), 전자상거래 관련지식 요인의 2항목(KN1, KN4) 위협요인의 1항목(RI2), 신뢰요인의 2항목(TR2, TR6), 구매의도요인의 1항목(PI4)이 표준화된 잔차분산의 값이 유의수준을 지나치게 벗어나거나 수정지수가 5를 넘는 것으로 나타나 이후의 분석에서 제외되었다.

##### (2) 측정 모델의 신뢰성 검증

실증분석을 통한 연구조사에 있어서 사용되는 측정도구는 그 의미가 유효하고 실제적인 효용을 가지기 위해서는 신뢰할 수 있어야 하며 [Chau, 1999], 측정도구의 신뢰성은 오차가 없고 일관된 결과를 얻을 수 있는 정도를 의미한다[Peter, 1979]. 구조방정식 모델에서는 신뢰성의 검정을 합성구성개념 신뢰성(composite construct reliability)이나 평균 분산 추출 값(average variance extracted)으로 계산하는데[Graver and Mentzer, 1999; Sukpanich and Chen, 1999], 평균 분산 추출 값은 구성개념에 의해서 설명되는 분산의 양을 나타내며, 0.5보다 작은 경우에는 측정 오차가 구성개념에 의해서 설명되는 분산보다 크기 때문에 신뢰성이 없다고 할 수 있다[Fornell and Larcker, 1981; Mishra,



2000].

합성 구성개념 신뢰성은 측정항목의 표준 적 재값을 이용하여 하나의 구성개념을 이루는 측정항목의 내적 일관성을 계산하며, 0.7보다 클 때 구성개념의 신뢰성이 있다고 본다[Segars, 1997; Hair et al., 1998]. 측정 모델에 대한 신뢰성 검증결과는 초기의 전체 항목들에 대한 결과 <표 4>에 나타나 있듯이 전체 개념의 신뢰성은 일반적으로 권고되는 수준을 모두 충족하고 있는 것으로 분석되었다.

**(3) 집중 타당성 분석**

개념 타당성에 대한 분석 중에서 집중 타당성은 각 구성개념에 속한 변수의 추정치가 0.5이상이고 t-값이 |2.0| 보다 큰 경우 구성개념의 집

중 타당성이 인정된다[Segars and Grover, 1993]. <표 5>의 분석결과에 나타나 있듯이 집중 타당성의 분석 결과 측정 모델에 적용된 모든 항목들의 추정치가 최소값이 0.525로 분석되어 기준통계량 0.50을 넘어서고 있으며 그 추정치의 t-값이 역시 최소값이 6.459로 기준통계량인 |2.0| 을 넘어서고 있는 것으로 나타나 모델에 적용된 전체 항목들의 집중 타당성은 충분히 확보되고 있다고 볼 수 있다.

**(4) 판별 타당성 분석**

판별 타당성의 분석은 상관계수와 표준오차를 사용하는 방법[Bagozzi et al., 1991]과 각 개념들 간의 쌍비교를 통한 방법[Bagozzi and Phillips, 1982; Anderson, 1987; Steenkamp

<표 4> 구성개념의 신뢰성과 상관관계

구성개념	합성구성개념신뢰성	평균분산추출값	자산	위험	보안통제	관련지식	위험	신뢰	구매의도
자 산	0.80	0.58	1.000						
위 험	0.79	0.50	0.666 (0.096) <sup>a</sup> 2.782 <sup>b</sup>	1.000					
보안통제	0.84	0.58	0.116 (0.097) 1.189	-0.285 (0.094) -3.030	1.000				
관련지식	0.80	0.51	0.246 (0.096) 2.562	0.090 (0.102) 0.877	0.197 (0.097) 2.033	1.000			
위 험	0.85	0.60	0.128 (0.095) 1.349	0.515 (0.077) 6.704	-0.378 (0.084) -4.514	0.055 (0.098) 0.568	1.000		
신뢰	0.89	0.67	0.048 (0.095) 0.501	-0.252 (0.092) -2.738	0.502 (0.074) 6.792	0.197 (0.094) 2.097	-0.513 (0.071) -7.264	1.000	
구매의도	0.95	0.82	0.117 (0.092) 1.270	-0.164 (0.093) -1.771	0.283 (0.086) 3.311	0.384 (0.083) 4.654	-0.397 (0.077) -5.160	0.683 (0.051) 13.470	1.000

주) a: 표준편차, b: t-값

<표 5> 집중 타당성 분석 결과 요약

항목	추정치	t-값	항목	추정치	t-값
AS1	0.766	9.610	KN6	0.632	7.724
AS2	0.871	11.131	RI1	0.525	6.459
AS4	0.646	7.978	RI3	0.763	10.481
TH1	0.657	8.026	RI4	0.877	12.841
TH2	0.792	10.208	RI5	0.879	12.734
TH3	0.640	7.820	TR1	0.765	10.543
TH4	0.707	8.819	TR3	0.893	13.564
CO3	0.633	7.930	TR4	0.890	13.207
CO5	0.800	10.869	TR5	0.676	8.904
CO6	0.809	10.966	PI1	0.905	13.989
CO7	0.775	10.408	PI2	0.952	15.303
KN2	0.658	8.742	PI3	0.918	14.325
KN3	0.793	9.851	PI5	0.855	12.721
KN5	0.728	9.348			

<표 6> 측정 모델의 쌍비교 판별 타당성 분석 결과 요약

모 델	자유도	$\chi^2$	p-값
기반모델	303	327.74	0.16
자산-위협 개념 조합모델	309	520.51	0.00
자산-보안통제 개념 조합모델	309	612.69	0.00
자산-관련지식 개념 조합모델	309	475.65	0.00
자산-위협 개념 조합모델	309	678.27	0.00
자산-신뢰 개념 조합모델	309	779.28	0.00
자산-구매의도 개념 조합모델	309	495.86	0.00
위협-보안통제 개념 조합모델	309	551.07	0.00
위협-관련지식 개념 조합모델	309	601.24	0.00
위협-위협 개념 조합모델	309	465.53	0.00
위협-신뢰 개념 조합모델	309	558.92	0.00
위협-구매의도 개념 조합모델	309	576.44	0.00
보안통제-지식 개념 조합모델	309	595.39	0.00
보안통제-위협 개념 조합모델	309	616.29	0.00
보안통제-신뢰 개념 조합모델	309	547.81	0.00
보안통제-구매의도 개념 조합모델	309	644.76	0.00
관련지식-위협 개념 조합모델	309	764.04	0.00
관련지식-신뢰 개념 조합모델	309	584.24	0.00
관련지식-구매의도 개념 조합모델	309	527.75	0.00
위협-신뢰 개념 조합모델	309	639.05	0.00
위협-구매의도 개념 조합모델	309	698.16	0.00
신뢰-구매의도 개념 조합모델	309	600.13	0.00

and van Trijp, 1991; Stewart and Segars, 2002]이 있는데, 본 연구에서는 최근의 다수의 연구에서 적용되고 있는 쌍비교 기법을 측정 모델의 판별 타당성 검증에 사용하였다. 쌍비교를 통한 방법은 측정모델과 다른 조합된 모델들 간의 카이제곱치에 대한 차이가 유의한 지를 분석한다. <표 6>은 전체 7개의 개념을 하나씩 쌍으로 묶어서 분석한 21개의 모델에 대한 분석표이다.

<표 6>에서 각각의 조합모델에 대해서 기반 모델과의 카이제곱치( $\chi^2$ ) 값과 조합모델의 카이제곱치 값의 차이가 주어진 자유도에서 유의하게 나타나는 경우 조합된 두 개념이 독립된 개념임을 의미하는 것이다. 기반모델과 조합된 모델간의 카이제곱치의 차이에 대한 쌍비교 검증에서 모든 조합모델에 대해서 유의한 차이가 있는 것으로 나타나 판별 타당성이 있는 것으로 나타났다.

(5) 측정모델의 적합도 분석

측정모델의 적합도 지표와의 비교를 통해서 측정모델의 전반적인 설명력에 대한 검증결과, 전반적인 모델적합도는 양호한 것으로 나타났다. 세부적인 모델 적합도지표를 살펴보면, 먼저 측정 모델의 카이제곱치는 자유도 303에서 327.751로 나타났으며, 측정모델에서 카이제곱치를 자유도로 나눈 값이 1.08로 일반적으로 요구되는 카이제곱치가 자유도의 3배 이상이 되어서는 안 된다는 조건을 충족하였다. 또한, 유의수준인 p-값의 경우에 있어서도 일반적으로 적용되는 유의수준인 0.05를 넘는 0.157로 나타났다. 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. 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 나타

났으며, 대부분의 적합도 지표가 일반적으로 논의되는 수준을 충족하고 있는 것으로 분석되었다.

### 4.3.2 구조 모델의 분석과 가설검정

#### (1) 구조방정식모델의 전반적 분석

전체 구조모델의 적합도에 대해서 살펴보면, 전반적으로 연구모델이 연구하고자하는 주요한 요인들 간의 관계를 양호하게 설명하고 있는 것으로 나타났다. 연구모델의 카이제곱치는 346.603으로 나타났으며, 자유도는 311로 산출되어 절대부합지수 평가의 하나로 사용되는 카이제곱치를 자유도로 나눈 값이 1.11로 일반적으로 권고되는 수용기준인 3이하의 조건을 충족하고 있는 것으로 분석되었으며, 유의수준 값인 p-값도 0.05 이상 이어야 한다는 권고수준을 만족하였다. 전체 연구모델의 다른 적합도 지수를 <표 7>에서 살펴보면, AGFI가 0.82, NFI가 0.85, RMSEA가

0.03으로 전반적으로 연구 모델의 적합도는 양호한 것으로 판단된다.

GFI와 SRMR의 적합도 지수가 일반적인 수용기준에 약간 못 미치는 0.85와 0.06으로 분석되었으나 권고하는 적합도 지수가 GFI의 경우 0.80이상과 SRMR의 경우 0.1이하를 적정한 적합도로 권고하거나 적용되는 경우[Segars and Grover, 1993; Hartwick and Barki, 1994; Etezadi-Amoli and Farhoomand, 1996; Somers et al., 2003]도 있기에 연구 모델의 설명력에는 크게 문제가 없는 것으로 판단된다. 또한, PGFI, IFI, CFI, PNFI와 같은 다른 전체 구조 방정식 모델의 지수가 권고되는 수용 기준에 양호하게 충족하고 있는 것으로 분석되어 전반적인 연구모델의 설명력이나 모델의 적합도는 충분히 양호하다고 설명할 수 있다.

#### (2) 연구가설검정과 경로분석

구조방정식모델을 통한 연구모델의 분석결과는 <그림 3>과 같이 나타낼 수 있다. 그림에서 각 구성개념간의 경로는 연구가설로 설정되었으며 각 가설에 대한 검정의 내용을 살펴보면 가설 1을 제외한 모든 가설이 통계적으로 유의한 것으로 분석되어 채택되었다.

세부적으로 살펴보면, 자산 개념과 위험간의 관계가 가설 1로 수립되었는데, 사용자가 인지하고 있는 자산의 가치가 높을수록 인지되는 위험도 높을 것이라는 내용이었다. 구조 방정식에서 분석된 결과에 따르면 유의수준  $\alpha = 0.05$ 에서 경로계수가 0.046으로 나타나 약간의 정의 관계가 존재하고 있으나 통계적으로 유의하지 않았다. 사용자가 인지하고 있는 정보자산의 중요도나 가치가 높을수록 인지되는 위험의 정도나 수준이 높을 것이라는 가설은 통계적인 검정과정에서 채택이 되지 못하였다.

가설 2는 위협과 위협간의 관계에 대한 검정이다. 사용자가 인지하고 있는 위협의 정도나 수준이 클수록 인지하는 위협이 커진다는 가설

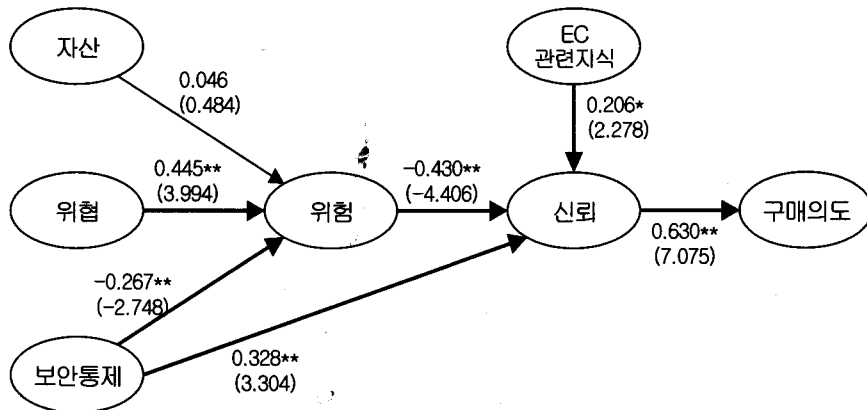
<표 7> 전체 구조 모델의 적합도 지표 요약

적합도 유형	적합지수	권장수용기준	모델의 통계량
절대부합지수	$\chi^2$ /자유도 (346.60/311)	$\leq 3.00$	1.11
	p-값	$\geq 0.05$	0.08
	기초부합지수(GFI)	$\geq 0.90$	0.85
	표준원소평균잔차 (SRMR)	$\leq 0.05$	0.06
중분부합지수	근사원소평균잔차(RMSEA)	$\leq 0.08$	0.03
	수정부합지수 (AGFI)	$\geq 0.80$	0.82
	표준부합지수(NFI)	$\geq 0.90$	0.85
	관계부합지수(RFI)	1.0 근사 양호	0.83
간명부합지수	중분부합지수(IFI)	1.0 근사 양호	0.97
	비교부합지수(CFI)	1.0 근사 양호	0.97
	간명기초부합지수 (PGFI)	$\geq 0.60$	0.70
	간명표준부합지수 (PNFI)	$\geq 0.60$	0.75

은 위협과 위험간의 경로계수가 0.445추정되어 상당히 높게 나타났으며, 또한 그 경로의 유의성도 유의수준  $\alpha=0.01$ 에서 통계적으로 유의한 것으로 분석되었다. 위협분석 접근법의 요인으로 언급되는 개념 중에서 사용자가 인지하는 보안통제의 수준이나 정도가 높을수록 인지하는 위협은 낮을 것이라는 가설 3은 경로계수의 직접효과 추정치가 -0.267로 분석되었으며, 유의

수준은 유의수준  $\alpha=0.05$ 에서 통계적으로 유의한 것으로 나타났다. 보안통제의 신뢰에 대한 영향은 경로계수가 0.328로 나타났으며, 유의수준은 유의수준  $\alpha=0.01$ 에서 통계적 유의성이 있는 것으로 분석되었다.

위험과 신뢰와의 관계분석을 가설로 설정한 가설 4의 검증에서는 구조 방정식의 전체효과 추정치가 -0.430으로 나타났으며, 유의수준은



주) 괄호안은 t-값. \*\*:유의수준  $\alpha=0.01$ 에서 유의함. \*:유의수준  $\alpha=0.05$ 에서 유의함.

<그림 3> 전체 구조 모델의 분석

<표 8> 전체구조방정식모델의 직접/간접 효과 분석 요약

	위험			신뢰			구매의도		
	직접	간접	전체	직접	간접	전체	직접	간접	전체
자산	0.05		0.05		-0.02	-0.02		-0.01	-0.01
t-값	0.48		0.48		-0.48	-0.48		-0.48	-0.48
위험	0.45**		0.45**		-0.19**	-0.19**		-0.12**	-0.12**
t-값	3.99		3.99		-3.15	-3.15		-3.04	-3.04
보안통제	-0.27**		-0.27**	0.32**	0.12*	0.44**		0.28**	0.28**
t-값	-2.75		-2.75	3.30	2.44	4.28		4.00	4.00
관련지식				0.21*		0.21*		0.13*	0.13*
t-값				2.28		2.28		2.24	2.24
위험				-0.43**		-0.43**		-0.27**	-0.27**
t-값				-4.41		-4.41		-4.10	-4.10
신뢰							0.63**		0.63**
t-값							7.08		7.08

주) \*: 유의수준  $\alpha=0.05$ 에서 유의함. \*\*: 유의수준  $\alpha=0.01$ 에서 유의함.

유의수준  $\alpha=0.01$ 에서 유의한 것으로 나타나, 사용자가 인지하는 위협의 수준이 높을수록 전자상거래에 대한 신뢰가 낮아진다는 가설 4는 통계적으로 유의한 것으로 분석되었다. 전자상거래와 관련된 사용자의 지식수준이 신뢰에 영향을 줄 것이라는 가설 5는 구조 방정식의 경로 계수가 0.206으로 산출되었으며, 유의수준  $\alpha=0.05$ 에서 유의한 것으로 분석되었다. 신뢰의 수준이나 정도가 구매의도에 영향을 줄 것이라는 가설은 그 경로계수가 유의수준  $\alpha=0.01$ 에서 0.630으로 추정되었다. 즉, 기존의 연구들에서 언급하고 있는 신뢰의 수준과 구매의도 간의 관계가 유의하다는 것이 실증적으로 검증되었으며, 구매의도에 영향을 주는 요인으로 판명되었다. 또한 구조방정식모델에서 분석된 직접효과 이외에 간접효과에 대한 분석의 결과에서도 신뢰에 위험분석차원의 요인들이 간접적으로 유의한 영향을 주는 것으로 나타났다. 구매의도에 미치는 간접효과에 대한 분석은 <표 8>로 요약할 수 있는데, 여기서도 자산을 제외한 모든 요인들이 주어진 유의수준에서 모두 의미가 있는 것으로 분석되었다. 전체 가설검정의 결과는

<표 9>로 요약하여 나타낼 수 있다.

#### 4.4 분석 결과에 대한 논의

전자상거래를 통해 제품이나 서비스의 구매하려는 의도에 대하여 사용자의 믿음의 정도를 나타내는 신뢰를 본 연구에서는 주요한 영향요인으로 설정하였다. 전자상거래를 이용하는 대부분의 사용자들이 인지하는 신뢰의 수준은 전자상거래를 수용할 것인지 아니면 수용하지 않을 것인지를 결정하는 주요한 개념으로 논의되고 있으며, 선행 연구들[Crosby et al., 1990; Morgan and Hunt, 1994; Kumar et al., 1995; Doney and Cannon, 1997; Jarvenpaa et al., 1998; Gefen, 2000; Pavlou and Gefen, 2002]에서 거론되었듯이, 전자상거래를 통한 제품이나 서비스를 구매하려는 의도는 전자상거래에 대한 전반적인 신뢰나 전자상거래와 같은 정보기술에 대한 사용자의 신뢰의 수준에 따라서 영향을 받게 된다는 것이 실증 분석을 통해서 확인되었다.

연구모델을 분석한 결과에서 위험분석접근법

<표 9> 연구가설의 검증 결과 요약

연구 가 설	모델의 경로	경로계수(t-값)	검정결과
가설 1: 전자상거래 이용자가 인지하는 자산의 가치나 중요도가 높을수록 이용자가 인지하는 위협의 수준은 높아진다.	자산 → 위협	0.046(0.484)	기각
가설 2: 전자상거래 이용자가 인지하는 위협이 클수록 이용자가 인지하는 전자상거래의 위협 수준은 높아진다.	위험 → 위협	0.445(3.994)	채택
가설 3: 전자상거래 이용자가 인지하는 보안통제의 수준이 높을수록 이용자가 인지하는 위협의 수준은 낮아진다.	보안통제 → 위협	-0.267(-2.748)	채택
가설 4: 전자상거래 이용자가 인지하는 위협의 수준이 높을수록 이용자의 전자상거래에 대한 신뢰는 낮아진다.	위험 → 신뢰	-0.430(-4.406)	채택
가설 5: 전자상거래 이용자의 전자상거래 관련지식의 수준이 높을수록 전자상거래의 신뢰는 높아진다.	관련지식 → 신뢰	0.206(2.278)	채택
가설 6: 전자상거래 이용자가 인지하는 보안통제의 수준이 높을수록 전자상거래의 신뢰수준은 높아진다.	보안통제 → 신뢰	0.328(3.304)	채택
가설 7: 전자상거래 이용자의 신뢰의 수준이 높을수록 전자상거래를 통한 제품이나 서비스의 구매의도가 높아진다.	신뢰 → 구매의도	0.630(7.075)	채택

과 관련된 개념인 위협과 보안통제는 위협에 영향을 주는 선행요인의 개념들로 타당한 것으로 통계적인 결과가 도출되었다. 그러나 자산, 특히 정보자산의 중요도나 가치는 실제 사용자가 인지하는 위협과는 실증 분석결과 통계적으로 유의하지 않는 것으로 나타났다. 자산의 가치와 중요도는 실제 사용자가 인지하는 피해의 정도를 평가할 수 있는 대표적인 지표가 될 수 있음에도 불구하고, 본 연구의 분석결과에서는 그러한 관계가 통계적으로 유의하게 입증되지 않았다. 이러한 자산과 위협간의 관계에 대한 가설의 기각된 이유는 먼저, 자산 특히 정보자산에 대한 전자상거래 이용자의 과대평가의 가능성을 지적할 수 있다.

부록의 기술통계에 나타나 있듯이 자산의 기술 통계치와 위협분석 접근법의 다른 구성개념들의 기술 통계치 사이에는 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 위협에 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, 위협분석 접근법의 구성요소 중에서 보안 통제는 전자상거래의 구매의도와 신뢰에 상당한 영향을 주는 것으로 분석되었다. 전자상거래를 이용하는 데 있어서 존재하는 위협의 수준도 역시 위협에 상당한 영향을 주는 주요 선행요인으로 나타났으며, 이러한 결과는 전자상거래를 이용하려는 사용자들에게 있어서 의도하지 않는 사건을 초래할 수 있는 위협의 발생 빈도나 그 심각성을 개별 사용자들이 중요하게 고

려하고 있음을 의미한다. 따라서 보안통제와 위협에 대한 고려를 통해서 체계적인 위협분석이나 관리가 일반 조직적 차원에서 뿐만이 아니라, 전자상거래 환경에서도 주요한 방법론으로 의미를 가지고 있다고 판단된다.

개인 사용자 차원의 요인으로 연구모델에서 제시하고 있는 전자상거래에 대한 지식수준이 신뢰에 미치는 영향은 실제 사용자가 전자상거래와 관련된 기술이나 절차 등에 대한 지식이 높을수록 전자상거래에 대한 신뢰가 증가하는 것으로 분석되어, 인터넷 쇼핑몰을 운영하는 기업의 차원에서는 그들이 사용하는 정보기술과 함께 구매과정, 지불과정, 탐색과정의 전반에 대해서 충분히 이용자들이 숙지할 수 있도록 하는 방법이 필요하다고 판단된다.

## V. 결 론

본 연구는 전자상거래 이용에 영향을 미치는 요인의 규명을 위해 신뢰와 위협을 주요한 요인으로 설명하고자 하였다. 또한 전자상거래를 이용하는 사용자가 인지하는 위협을 단순한 차원이 아닌 정보보안에서 논의되고 있는 위협분석 접근법 모델을 적용하여 위협의 선행요인으로 언급되는 자산, 위협, 보안통제의 세부적인 개념으로 구분하여 사용자의 의도나 신뢰에 대한 전자상거래환경에서의 타당성에 대한 분석을 연구의 목적으로 하였다. 전자상거래를 이용하는 사용자의 의도를 설명하기 위해 연구에 포함된 신뢰와 위협의 개념은 실증분석결과 유의한 것으로 나타났으며, 세부적으로 위협분석방법론을 적용하여 분석한 위협도 통계적으로 유의하게 분석되었다. 정보보안에서 논의되는 보안통제의 개념 전반적인 위협의 수준을 완화하거나 감소시키는 주요한 수단으로 나타났다. 이러한 이론적인 내용들을 전자상거래의 상황에서 신뢰라는 개념과의 관계를 통해 분석한 결과, 사용자가 인지하고 있는 보안통제 수준이 신뢰에 영향

을 미치며 위협과는 부의 상관관계를 가지고 있는 것으로 나타났다. 따라서 본 연구에서 논의된 연구결과의 의미는 신뢰의 선행요인으로의 보안통제가 주요한 영향요인으로서의 가치를 가지며, 소비자와의 장기적인 관계나 브랜드 이미지와 같은 차원의 접근법과 함께 사용자와 관련된 정보자산에 대한 보안대책이나 정책과 같은 방법들이 중요함을 강조할 수 있는 근거가 된다고 할 것이다.

본 연구를 통해서 위험분석 접근법은 전자상거래와 같은 환경에서도 위험을 체계적으로 이해하고 그와 관련된 선행요인들과의 관계를 통해서 설명할 수 있는 유의한 방법으로 분석되었다. 즉, 암호화나 전자지불 시스템과 같은 기술 지향적인 정보보안의 내용과 함께 사용자의 보안통제에 이해나 인지 그리고 위협의 발생빈도와 심각성에 대한 분석과 같은 측면에 대한 논의를 통해서 전자상거래의 이용에 대한 새로운 차원에서의 접근을 시도하였다는 점을 본 연구의 의의로 볼 수 있다. 또한, 연구에서 제시하고 있는 위험분석 접근법을 이용한 전자상거래 신뢰의 선행요인으로서의 위험은 사용자의 전자상거래를 통한 구매의도를 이해하는데 체계적인 분석을 가능하게 하며, 사용자의 전자상거래에 대한 신뢰를 강화하기 위한 방법으로 전자상거래에 대한 전반적인 보안 수준의 향상과 전자상거래에 적용되는 관련 정보기술에 대해서 사용자가 정확하게 알 수 있도록 지속적인 정보기술 지식의 제공이 주요한 방법으로 적용될 수 있다는 점을 의미한다.

본 연구의 한계점으로는 위험분석 접근법을

전자상거래환경에서 적용함에 있어서 기존의 위험분석 접근법에서 적용된 자산의 개념이 전자상거래라는 상황적인 특성으로 인하여 무형자산인 정보자산에 국한되어 연구가 되었다는 점을 들 수 있다. 위험분석 접근법에서는 유형과 무형자산을 포함한 모든 개별자산의 합으로 정의되는 자산의 개념이 전자상거래의 사용자 측면에서는 정보자산에 국한되어 측정, 분석될 수밖에 없다는 것이다.

표본과 관련된 연구의 한계점으로는, 전자상거래를 이용하는 사용자 집단의 특성을 완벽하게 대표하기에는 연구에서 사용된 표본의 인구통계학적인 특성이 약간의 차이가 있다는 점이다. 전반적인 연령층이 기존의 연구들에서 사용하고 있는 표본의 평균적인 연령보다 다소 높다는 점은 구매력을 충분히 가지고 있는 집단이며 그와 관련된 위험을 충분히 인지하고 있는 집단으로의 대표성을 가지고 있다고 할지라도 연구 결과에 대한 외적타당성에 있어서는 추가적인 논의가 필요할 것이다. 따라서 향후의 연구에서는 연구모형을 포괄적이고 광범위한 표본을 대상으로 수행하여 보다 일반화의 가능성을 높일 수 있는 연구가 수행될 수 있을 것이다.

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 것이다.

## 〈참 고 문 헌〉

- [1] 김경규, 이정우, 김혜선, "인터넷 뱅킹 채택 행위에 있어서 신뢰와 위협의 영향," *경영학연구* 제32권 제6호, 2003, pp. 1771-1797.
- [2] 김영걸, 이종만, 이재남, "정보시스템의 위험도 분석에 대한 연구: 통합적 분석 틀을 중심으로," *경영정보학연구*, 제8권 제2호, 1998, pp. 37-53.
- [3] 이성만, 이필중, "해외의 보안위험분석 방

- 법론 현황 및 분석," *한국통신정보보호학회지*, 제4권 제1호, 1994, pp. 316-323.
- [4] Anderson, J., "An Approach for Confirmatory Measurement and Structural Equation Modeling of Organizational Properties," *Management Science*, Vol. 33, No. 4, 1987, pp. 525-541.
- [5] Anderson, J. and D. Gerbing, "Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach," *Psychological Bulletin*, Vol. 103, No. 4, 1988, pp. 411-423.
- [6] Anderson, J. and J. Narus, "A Model of Distributor Firm and Manufacturer Firm Working Partnership," *Journal of Marketing*, Vol. 54, No. 1, 1990, pp. 42-58.
- [7] Bagozzi, R. and L. Phillips, "Representing and Testing Organizational Theories: A Holistic Construct," *Administrative Science Quarterly*, Vol. 23, No. 3, 1982, pp. 459-489.
- [8] Bagozzi, R., Y. Yi and L. Phillips, "Assessing Construct Validity in Organizational Research," *Administrative Science Quarterly*, Vol. 36, No. 3, 1991, pp. 421-458.
- [9] Barnard, L., and R. von Solms, "A Formalized Approach to the Effective Selection and Evaluation of Information Security Controls," *Computers and Security*, Vol. 19, No. 2, 2000, pp. 185-194.
- [10] Belanger, F., J. Hiller and W. Smith, "Trustworthiness in Electronic Commerce: The Role of Privacy, security, and Site Attributes," *Journal of Strategic Information Systems*, Vol. 11, No. 3, 2002, pp. 245-270.
- [11] Borchers, A., "Trust in Internet Shopping: A Test of a Measurement Instrument," *Seventh Americas Conference on Information Systems*, 2001, pp. 799-803.
- [12] BSI, *BS7799: Code of Practices for information Security Management*, United Kingdom, 1999.
- [13] CCTA, *United Kingdom Government CRAMM User Guide*, 2001.
- [14] Chau, P., "On the Use of Construct Reliability in MIS Research: A Meta Analysis," *Information and Management*, Vol. 35, No. 4, 1999, pp. 217-228.
- [15] Chellappa, R. and P. Pavlou, "Perceived Information Security, Financial Liability and Consumer Trust in Electronic Commerce Transactions," *Logistics Information Management*, Vol. 15, No. 5, 2002, pp. 358-368.
- [16] Chen, S. and G. Dhillon, "Interpreting Dimensions of Consumer Trust in E-Commerce," *Information Technology and Management*, Vol. 4, No. 3, 2003, pp. 303-318.
- [17] Cheung, C. and M. Lee, "Trust in Internet Shopping: A Proposed Model and Measurement Instrument," *Proceedings of Americas Conference on Information Systems*, 2000, pp. 681-689.
- [18] CMU/SEI, *Operationally Critical Threat, Asset, Vulnerability Evaluation(OCTAVE) Framework*, Version 1.0, CMU/SEI-99-TR-017, June 1999.
- [19] Cowles, D., "The Role of Trust in Customer Relationships: Asking the Right questions," *Management Decision*, Vol. 35, No. 4, 1997, pp. 273-282.
- [20] Crosby, L., K. Evans and D. Cowles, "Relationship Quality in Services Selling: An Interpersonal Influence Perspective," *Journal of Marketing*, Vol. 54, No. 3, 1990, pp. 68-81.
- [21] CSE, *Canadian Handbook on Information*



- Technology Security*, Communications Security Establishment, Government of Canada, 1998.
- [22] CSE, *Guide to Security Risk Management for IT Systems*, Government of Canada, Communications Security Establishment, Government of Canada, 1996.
- [23] CSI, *IPAK: Information Protection Assessment Kit*, Computer Security Institute, 1997.
- [24] Dayal, S., H. Landesberg and M. Zeisser, "How to Build Trust Online," *Marketing Management*, Vol. 8, No. 3, 1999, pp. 64-69.
- [25] Doney, P. and J. Cannon, "An Examination of the Nature of Trust in Buyer-Seller Relationships," *Journal of Marketing*, Vol. 61, No. 2, 1997, pp. 35-51.
- [26] Doney, P., J. Cannon and M. Mullen, "Understanding the Influence of National Culture on the Development of Trust," *Academy of Management Review*, Vol. 23, No. 3, 1998, pp. 601-620.
- [27] Etezadi-Amoli, J. and F. Farhoomand, "A Structural Model of End User Computing Satisfaction and User Performance," *Information and Management*, Vol. 30, No. 2, 1996, pp. 65-73.
- [28] Fornell, C. and D. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research*, Vol. 18, No. 1, 1981, pp. 39-50.
- [29] Gannesan, S., "Determinants of Long-Term Oriented in Buyer-Seller Relationships," *Journal of Marketing*, Vol. 58, No. 2, 1994, pp. 1-19.
- [30] GAO, *Information Security Risk Assessment - Practices of Leading Organizations, Exposure Draft*, U.S. General Accounting Office, August 1999.
- [31] 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, 1999, pp. 33-57.
- [32] Gefen, D., "Customer Loyalty in E-Commerce," *Journal of the Association for Information Systems*, Vol. 3, 2002, pp. 27-51.
- [33] Gefen, D., "E-Commerce: The Role of Familiarity and Trust," *Omega*, Vol. 28, No. 6, 2000, pp. 725-737.
- [34] Gefen, D., E. Karahanna and D. Straub, "Trust and TAM in Online Shopping: An Integrated Model," *MIS Quarterly*, Vol. 27, No. 1, 2003, pp. 51-90.
- [35] Grabner-Kraeuter, S., "The Role of Consumer's Trust in Online-Shopping," *Journal of Business Ethics*, Vol. 39, No. 1, 2002, pp. 43-50.
- [36] Grazioli, S. and S. Jarvenpaa, "Perils of Internet Fraud: An Empirical Investigation of Deception and Trust with Experienced Internet Consumers," *IEEE Transaction on System*, Vol. 30, No. 4, 2000, pp. 395-410.
- [37] Hair, J., R. Anderson, R. Tatham and W. Black, *Multivariate Data Analysis with Readings*, Prentice Hall, 1998.
- [38] Hartwick, J. and H. Barki, "Explaining the role of User Participation in Information System Use," *Management Science*, Vol. 40, No. 4, 1994, pp. 440-465.
- [39] Hoffman, D., T. Novak and C. Peralta, "Building consumer Trust Online," *Communications of the ACM*, Vol. 42, No. 4, 1999, pp. 80-85.
- [40] ISO/IEC JTC1 SC27, *Guidelines for the man-*

- agement of IT security(GMITS) - Part 1: Concepts and models of IT security, TR 13335-1, 2000.
- [41] Jarvenpaa, S. and P. Todd, "Consumer Reactions to Electronic Shopping on the World Wide Web," *International Journal of Electronic Commerce*, Vol. 1, No. 2, 1997, pp. 59-88.
- [42] Jarvenpaa, S., K. Knoll and D. Leidner, "Is Anybody Out There? Antecedents of Trust in Global Virtual Teams," *Journal of Management Information Systems*, Vol. 14, No. 4, 1998, pp. 29-64.
- [43] Jarvenpaa, S., N. Tractinsky, and M. Vitale, "Consumer Trust in an Internet Store," *Information Technology and Management*, Vol. 1, No. 1, 2000, pp. 45-71.
- [44] Kehoe, M., *The Role of Perceived Risk and Consumer Trust in Relation to on-line Shopping and Security*, Ph. D. Dissertation, Florida State University, 2002
- [45] Kim, D., D. Ferrin and R. Rao, "Antecedents of Consumer Trust in B-to-C Electronic Commerce," *Proceedings of Seventh Americas Conference on Information Systems*, 2003, pp. 157-167
- [46] 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*, 2001, pp. 784-787.
- [47] Kim, K. and B. Prabhakar, "Initial Trust, Perceived Risk, and the Adoption of Internet Banking," *Proceedings of International Conference on Information Systems*, 2000, pp. 537-543.
- [48] Kini, A. and J. Choobineh, "An Empirical Evaluation of the Factors Affecting Trust in Web Banking Systems," *Proceedings of Americas Conference on Information Systems*, 2000, pp. 185-191.
- [49] Koufaris, M., "Applying the Technology Acceptance Mode and Flow Theory to Online Consumer Behavior," *Information Systems Research*, Vol. 13, No. 2, 2002, pp. 205-223.
- [50] KPMG Peat Marwick LLP, *Vulnerability Assessment Framework 1.1*, Critical Infrastructure Assurance Office, October 1998.
- [51] Kumar, N., L. Scheer, and J. Steenkamp, "The Effect of Supplier Fairness on Vulnerable Resellers," *Journal of Marketing Research*, Vol. 32, No. 1, 1995, pp. 54-65.
- [52] Lau, G. and S. Lee, "Consumer's Trust in a Brand and the Link to Brand Loyalty," *Journal of Market Focused Management*, Vol. 4, No. 4, 1999, pp. 341-370.
- [53] Loch, K., H. Carr and M. Warkentin, "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly*, Vol. 16, No. 2, 1992, pp. 173-186.
- [54] Luhmann, N., *Trust and Power*, John Wiley & Son, Chichester, New York, 1979.
- [55] Mayer, R., J. Davis and F. Schoorman, "An Integrative Model of Organizational Trust," *Academy of Management Review*, Vol. 20, No. 3, 1995, pp. 709-734.
- [56] McKnight H., V. Choudhury and C. Kacmar, "Developing and Validating Trust Measures for e-Commerce: An Integrative Typology," *Information Systems Research*, Vol. 13, No. 3, 2002a, pp. 334-359.
- [57] McKnight, H., V. Choudhury and C. Kacmar, "The Impact of Initial Consumer Trust on Intentions to Transact with a Web Site: A Trust Building Model," *Journal of Strategic*

- Information Systems*, Vol. 11, No. 3, 2002b, pp. 297-323.
- [58] Mishra, D., "An Empirical Assessment of Measurement Error in Health-Care Survey Research," *Journal of Business Research*, Vol. 48, No. 3, 2000, pp. 193-205.
- [59] Morgan, R., and S. Hunt, "The Commitment-Trust Theory of Relationship Marketing," *Journal of Marketing*, Vol. 58, No. 3, 1994, pp. 20-38.
- [60] Nöteberg, A., E. Christiaanse and P. Wallage, "The Role of Trust and Assurance Services in Electronic Channels: An Exploratory Study," *Proceedings of International Conference on Information Systems*, 1999, pp. 472-478.
- [61] Novak, T., D. Hoffman and Y. Yung, "Measuring the customer experience in online environments: A structure modeling approach," *Marketing Science*, Vol. 19, No. 1, 2000, pp. 22-42.
- [62] Olivero, N. and P. Lunt "Privacy Versus Willingness to Disclose in e-commerce Exchange: The effect of Risk Awareness on the Relative Role of Trust and Control," *Journal of Economic Psychology*, Vol. 25, No. 2, 2004, pp. 243-262.
- [63] Otwell, K. and B. Aldridge, "The Role of Vulnerability in Risk Management," *IEEE Proceedings of the Fifth Annual Computer Security Application Conference*, 1989, pp. 32-38.
- [64] Pavlou, P., "Institution-based Trust in Interorganizational Exchange Relationships: The Role of Online B2B Marketplaces on Trust Formation," *Journal of Strategic Information Systems*, Vol. 11, No. 3, 2002, pp. 215-243.
- [65] Pavlou, P., "Integrating Trust in Electronic Commerce with the Technology Acceptance Model: Model Development and Validation," *Proceedings of Seventh Americas Conference on Information Systems*, 2001, pp. 816-822.
- [66] Pavlou, P. and D. Gefen, "Building Effective Online Marketplaces with Institution-Based Trust," *Twenty-Third International Conference on Information Systems*, 2002, pp. 667-675.
- [67] Peltier, T., *Information Security Risk Analysis*, Auerbach, 2001.
- [68] Peter, J., "Reliability: A Review of Psychometric Basics and Recent Marketing Practices," *Journal of Marketing Research*, Vol. 16, No. 1, 1979, pp. 6-17.
- [69] Rainer, R., C. Snyder and H. Carr, "Risk Analysis for Information Technology," *Journal of Management Information Systems*, Vol. 8, No. 1, 1989, pp. 129-147.
- [70] Ratnasingham, P., "The Importance of Trust in Electronic Commerce," *Internet Research: Electronic Networking Applications and Policy*, Vol. 8, No. 4, 1998a, pp. 313-321.
- [71] Ratnasingham, P., "Trust in Web-based Electronic Commerce Security," *Information Management and Computer Security*, Vol. 6, No. 4, 1998b, pp. 162-166.
- [72] Reichheld, F., and P. Scheffer., "E-Loyalty: Your Secret Weapon on the Web," *Harvard Business Review*, Vol. 78, No. 4, 2000, pp. 105-113.
- [73] Rousseau, D., S. Sitkin, R. Burt, and C. Camerer, "Not so Different After All: A Cross-Discipline View of Trust," *Academy of Management Review*, Vol. 23, No. 3, 1998, pp. 393-404.

- [74] Roy, M., O. Dewit, and B. Aubert, "The impact of interface usability on trust in web retailers," *Internet Research: Electronic Networking Applications and Policy*, Vol. 11, No. 5, 2001, pp. 388-398.
- [75] 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*, 1998, pp. 335-337.
- [76] Salisbury, D., R. Pearson, A. Pearson and D. Miller, "Perceived security and World Wide Web purchase intention," *Industrial Management and Data Systems*, Vol. 101, No. 4, 2001, pp. 165-176.
- [77] Segars, A., "Assessing the Unidimensionality of Measurement: A Paradigm and Illustration Within the Context of Information Systems Research," *Omega*, Vol. 25, No. 1, 1997, pp. 107-121.
- [78] Segars, A. and V. Grover, "Re-Examining Perceived Ease of Use and Usefulness: A Confirmatory Factor Analysis," *MIS Quarterly*, Vol. 17, No. 4, 1993, pp. 517-525.
- [79] Selnes, F., "Antecedents and Consequences of Trust and Satisfaction in Buyer-seller Relationships," *European Journal of Marketing*, Vol. 32, No. 3, 1998, pp. 305-322.
- [80] Settle, B., L. Alreck and E. McCorkle, "Consumer Perceptions of Mail/phone Order Shopping Media," *Journal of Direct Marketing*, Vol. 8, No. 4, 1994, pp. 365-378.
- [81] Shankar, V., G. Urban, and F. Sultan, "Online Trust: A Stakeholder Perspective, Concepts, Implications, and Future Directions," *Journal of Strategic Information Systems*, Vol. 11, No. 3, 2002, pp. 325-344.
- [82] Smith, H., J. McKeen, and S. Staples, "Risk Management in Information Systems: Problems and Potential," *Communications of the Association for Information Systems*, Vol. 7, No. 13, 2001, pp. 1-27.
- [83] Somers, T., K. Nelson, and J. Karimi, "Confirmatory Factor Analysis of the End-user Computing Satisfaction Instrument: Replication within an ERP Domain," *Decision Sciences*, Vol. 34, No. 3, 2003, pp. 595-621.
- [84] Steenkamp, J. and H. von Trijp, "The Use of LISREL in Validating Marketing Constructs," *International Journal of Research in Marketing*, Vol. 8, No. 4, 1991, pp. 283-299.
- [85] Stewart, K. and A. Segars, "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research*, Vol. 13, No. 1, 2002, pp. 36-49.
- [86] Straub, D., "Validating Instruments in MIS Research," *MIS Quarterly*, Vol. 13, No. 2, 1989, pp. 147-169.
- [87] Suh, B. and I. Han, "The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce," *International Journal of Electronic Commerce*, Vol. 7, No. 3, 2003, pp. 135-161.
- [88] Sukpanich, N. and L. Chen, "Measuring Consumers' Attitudes to Web Advertising," *Electronic Markets*, Vol. 9, No. 1, 1999, pp. 20-24.
- [89] Swaminathan, V., E. Lepkowska-White, and B. Rao, "Browser or Buyers in Cyberspace? An Investigation of Factors Influencing Electronic Exchange," *Journal of*

- Computer-Mediated Communication*, Vol. 5, No. 2, 1999.
- [90] Torkzadeh, G. and G. Dhillon, "Measuring Factors the Influence the Success of Internet Commerce," *Information System Research*, Vol. 13, No. 2, 2002, pp. 187-204.
- [91] Urban, G., F. Sultan, and W. Qualls, "Placing Trust at the Center of Your Internet Strategy," *Sloan Management Review*, Vol. 42, No. 1, 2000, pp. 39-69.
- [92] Wilson, S., "Certificates and trust in electronic commerce," *Information Management and Computer Security*, Vol. 5, No. 5, 1997, pp. 175-181.
- [93] Yoon, S., "The Antecedents and Consequences of Trust in Online-Purchase Decisions," *Journal of Interactive Marketing*, Vol. 16, No. 2, 2002, pp. 47-63.

<부록: 설문문항과 기술통계량>

개념	항목명	측정변수	설문항목	최종분석 포함여부	평균 (표준편차)
자산	AS1	개인정보 제공의 중요도	전자상거래를 이용하는 과정에서 인터넷 쇼핑물에 제공되는 나의 개인정보는 중요하다고 생각한다.	포함	6.434 (0.856)
	AS2	개인정보의 가치	전자상거래를 이용하는데 사용되는 개인정보의 가치는 높다고 생각한다.	포함	6.207 (0.881)
	AS3	구매관련 정보의 상대적 가치	인터넷 쇼핑물을 통해서 구매한 제품구매정보는 판매자에게 중요한 가치를 가진다고 생각한다.		5.897 (1.059)
	AS4	인지된 개인정보의 중요도	인터넷 쇼핑물의 회원가입을 위해서 입력하는 정보들은 중요한 정보라고 생각한다.	포함	6.048 (0.974)
	AS5	지불관련 정보의 중요도	인터넷 쇼핑물을 이용하는데 있어서, 지불과 관련된 대금지불정보는 중요한 것이라고 생각한다.		6.297 (0.951)
위험	TH1	인지된 개인정보 노출 확률	인터넷 쇼핑물과 같은 전자상거래를 이용하는데 있어서 개인정보가 타인에게 노출될 경우가 많을 것이라고 생각한다.	포함	5.683 (1.091)
	TH2	잠재적인 손실의 발생 가능성	인터넷 쇼핑물을 이용하는 경우에 사기나 금전적인 피해를 입을 확률이 높다고 생각한다.	포함	4.897 (1.257)
	TH3	가용성 피해의 확률	해커나 다른 악의적인 사람에게 의해서 인터넷 쇼핑물을 이용하지 못하는 경우가 자주 발생할 것이라고 생각한다.	포함	4.276 (1.304)
	TH4	기밀성 피해의 가능성	전자상거래를 사용하면서 발생한 지불정보들은 해커나 악의적인 사람들에게 알려질 경우가 많을 것이라고 생각한다.	포함	4.772 (1.212)
	TH5	잠재적 피해의 발생가능성	인터넷 쇼핑물을 지속적 이용하는 경우, 발생할 수 있는 피해의 횟수가 점점 더 증가할 것이라고 생각한다.		5.021 (1.233)
	TH6	구매정보의 노출 확률	인터넷 쇼핑물을 통해서 구입한 제품이나 서비스와 관련된 정보가 타인에게 알려질 확률이 높다고 생각한다.		5.069 (1.128)
	TH7	개인정보의 노출 가능성	인터넷 쇼핑물 운영자가 의도적으로 개인정보를 외부에 유출할 경우가 많을 것이라고 생각한다.		4.724 (1.325)
보안 통제	CO1	인지된 개인정보 보안통제 수준	인터넷 쇼핑물들은 사용자의 개인정보를 보호하기 위한 보안기술을 잘 활용하고 있다고 생각한다.		4.200 (1.128)
	CO2	지불보안통제에 대한 인지된 수준	인터넷 쇼핑물들은 사용자의 개인정보를 보호하기 위한 보안기술을 잘 활용하고 있다고 생각한다.		4.503 (1.081)
	CO3	제도적인 보안대책 수준	전반적으로 개인정보보호를 위한 기업의 정책이나 법률적인 규제가 전자상거래에 잘 적용되고 있다고 생각한다.	포함	3.800 (1.051)
	CO4	개인정보의 기술적 인 보안통제 수준	인터넷 쇼핑물을 이용하는데 사용되는 개인정보는 기술적으로 안전하게 보호될 것이라고 생각한다.		3.538 (1.225)
	CO5	구매정보의 기술적 인 보안통제 수준	인터넷 쇼핑물을 통해서 발생한 제품의 구매정보는 다양한 보안기술을 통해서 안전하게 보호될 것이라고 생각한다.	포함	3.690 (1.096)
	CO6	배송정보의 보안통제 수준	인터넷 쇼핑물에서 사용하는 나의 배송관련 정보들은 안전하게 관리될 것이라고 생각한다.	포함	3.834 (1.093)
	CO7	전자상거래 전반적 인 보안통제 수준	전반적으로 전자상거래를 수행하는 인터넷 쇼핑물의 보안수준은 높다고 생각한다.	포함	3.834 (1.247)

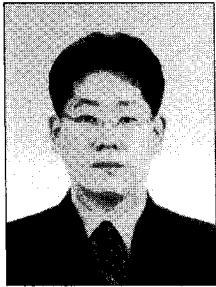
개념	항목명	측정변수	설문항목	최종분석 포함여부	평균 (표준편차)
위험	RI1	전자상거래 매체의 상대적 위험	실제 점포에서 제품이나 서비스를 구매하는 것보다 인터넷 쇼핑몰을 통한 구매가 더 위험하다고 생각한다.	포함	5.110 (1.297)
	RI2	인지된 위험 수준	인터넷 쇼핑몰을 이용하는데 있어서 위험의 요소는 많을 것이라고 생각한다.		5.262 (1.093)
	RI3	인지된 지불관련 위험	인터넷을 통한 전자상거래에서 온라인으로 대금을 지불하는 것은 안전하지 못하다고 생각한다.	포함	4.469 (1.375)
	RI4	이용안전성에 대한 위험 인지수준	나는 인터넷 쇼핑몰과 같은 전자상거래를 이용할 때 불안함을 느낀다.	포함	4.490 (1.323)
	RI5	전자상거래 관련 전반적 위험인지	나의 경험에 의하면 인터넷 쇼핑몰을 이용하는 데에는 위험이 수반된다고 생각한다.	포함	4.634 (1.212)
전자상거래 관련 지식	KN1	전자상거래 구매관련 지식	나는 인터넷 쇼핑몰을 통해서 제품이나 서비스를 구매하는 방법을 알고 있다.		5.855 (1.258)
	KN2	전자상거래 지불관련 지식	나는 인터넷 쇼핑몰을 통한 제품이나 서비스의 대금 지불과정을 알고 있다.	포함	5.738 (1.247)
	KN3	보안통제에 대한 지식	인터넷 쇼핑몰에서 설명하는 개인정보보호정책이 무엇인지를 나는 알고 있다.	포함	4.690 (1.362)
	KN4	웹 이용관련 지식	인터넷 쇼핑몰에서 내가 구매하고자 하는 제품이나 서비스를 찾는 방법을 알고 있다.		5.703 (1.155)
	KN5	개인정보 보안관련 지식	인터넷 쇼핑몰에 제공한 개인정보를 수정, 삭제하는 과정이나 절차를 잘 알고 있다.	포함	4.724 (1.579)
	KN6	전자상거래 이용 위험 지식	인터넷을 사용하는데 있어서 발생할 수 있는 사고나 피해에 대해서 잘 알고 있다.	포함	4.531 (1.400)
신뢰	TR1	전자상거래에 대한 전반적 신뢰	전반적으로 인터넷 쇼핑몰을 이용한 전자상거래는 신뢰할 수 있다고 생각한다.	포함	4.055 (0.941)
	TR2	법적, 제도적 차원의 신뢰	인터넷 쇼핑몰을 통한 제품의 구매는 법적, 제도적으로 믿을 수 있다고 생각한다.		3.814 (0.965)
	TR3	인터넷 쇼핑몰의 전반적 신뢰	전자상거래를 이용하는데 있어서 인터넷 쇼핑몰을 믿고 의지할 수 있다고 생각한다.	포함	3.834 (1.074)
	TR4	구매수단으로써의 신뢰	인터넷을 통해서 제품과 서비스를 구매하는 것은 신뢰 할 수 있는 구매수단이라고 생각한다.	포함	3.910 (1.111)
	TR5	제공되는 내용이나 설명에 대한 신뢰	인터넷 쇼핑몰들이 설명하는 내용들을 믿을 만한 가치가 있다고 생각한다.	포함	3.841 (1.045)
	TR6	전자상거래 기술의 신뢰 수준	인터넷 쇼핑몰과 같이 전자상거래에 사용되는 정보기술들은 믿을 수 있다고 생각한다.		4.048 (1.030)
구매 의도	PI1	전반적인 구매의도	나는 인터넷 쇼핑몰을 통한 제품이나 서비스의 구매를 할 의도가 있다.	포함	5.007 (1.320)
	PI2	구매의 지속의도	만약 구매하려는 제품이 전자상거래를 통해서 구매가 가능하다면, 나는 계속해서 전자상거래를 이용할 것이다.	포함	4.986 (1.359)
	PI3	전자상거래이용의 긍정적의도	나는 인터넷 쇼핑몰을 이용하는 전자상거래에 대해서 긍정적으로 생각하고 있다.	포함	4.979 (1.315)
	PI4	고가제품의 구매의도	인터넷 쇼핑몰을 통해서 비교적 높은 가격의 제품이나 서비스를 구매할 의향이 있다.		4.186 (1.379)
	PI5	반복적 구매의도	인터넷 쇼핑몰을 통해서 제품이나 서비스의 구매를 자주 할 의도가 있다.	포함	4.531 (1.395)

## ◆ 저자소개 ◆



김중기 (Kim, Jongki)

부산대학교 경영학과를 졸업하고, 미국 Arkansas State University에서 경영학석사와 Mississippi State University에서 경영학박사를 취득하였다. 국방정보체계연구소와 국방과학연구소에서 선임연구원으로 재직하였으며, 현재 부산대학교 경영학부에서 조교수로 재직중이다. 관심분야는 정보시스템 보안관리, 정보보안 평가방법론, 그리고 프로젝트 관리방법론이다.



이동호 (Lee, Dongho)

부산대학교 경영학과를 졸업하고, 부산대학교에서 경영학석사와 경영학박사 학위(경영정보/생산관리 전공)를 취득하였다. 부산대학교 경영경제연구소의 선임연구원으로 근무하였으며, 현재 동명정보대학교 유통경영학과에서 전임강사로 재직중이다. 주요 관심분야는 정보시스템 보안관리, 정보보안 평가방법론, E-Biz와 웹 기반 어플리케이션 모델링/개발이다.

◆ 이 논문은 2004년 5월 26일 접수하여 1차 수정을 거쳐 2004년 12월 5일 게재확정되었습니다.