연구논문 정보화정책 제20권 제3호, 2013년 가을호, pp.63-85

온라인 환경에서 프라이버시 행동의도에 미치는 영향*

- 보호동기이론을 중심으로 -

김 종 기**, 김 상 희***

요 약 온라인 환경에서 개인정보가 유출되는 사건이 빈번히 일어남에 따라 온라인 사용자들의 프라이버시 문제가 중요해지고 있다. 개인정보가 유출되는 사건을 직접 혹은 간접적으로 경험한 온라인 사용자는 자신의 프라이버시에 대해 위협을 느끼게 되고, 이로 인해 프라이버시 보호에 대한 기존의 인식이나 행동에 변화를 가져오게 된다. 본 연구에서는 온라인 환경에서 프라이버시를 보호하기 위한 행동의도에 영향을 미치는 요인을 보호동기이론을 기반으로 규명하고자 하였다. 보호동기이론은 위협소구에 의한 보호행동의 변화과정을 설명하기 위한 대표적인 이론으로, 위협과 효능감이라는 개인의 인지적 평가에 의해 보호동기가 형성되고 이를 통하여 프라이버시 행동의 변화가 일어난다는 것이다. 이때 인지적 매개과정에서 보호동기 요인을 개인의 프라이버시 태도 및 신념을 나타내는 프라이버시 신뢰와 프라이버시 위험으로 설정하여 구조방정식을 활용함으로써 실증분석을 수행하였다. 실증분석의 결과에 따르면, 보호동기요인과 선행요인인 위협 및 효능감과의 관계에서는 효능감과 프라이버시 위험 간의 경로를 제외하고 모든 경로가 통계적으로 유의한 것으로 분석되었다. 한편, 보호동기요인과 결과요인인 프라이버시 행동의도의 관계에서는 프라이버시 위험과 프라이버시 행동의도 간의 경로는 통계적으로 유의하나 프라이버시 신뢰와 프라이버시 행동의도 간의 경로는 통계적으로 유의하지 않은 것으로 분석되었다.

주제어: 프라이버시 보호행동, 프라이버시 신뢰, 프라이버시 위험, 보호동기이론, 위협, 효능감

Privacy Behavioral Intention in Online Environment:

Based on Protection Motivation Theory

Jongki Kim, Sanghee Kim

Abstract Drawing on Protection Motivation Theory(PMT), this study attempts to clarify antecedents that influence the intention to protect individuals' privacy on the Internet. Protection motivation forms through individuals' cognitive appeal involving threat and efficacy. Then protection motivation causes privacy behavioral change. Protection motivation factors are established privacy trust and privacy risk, which are related to privacy attitude and belief. This proposed model is empirically analyzed by utilizing structural equation analysis(SEM). According to the result of the empirical analysis, it is founded that almost paths have statistically significant explanatory power except path from efficacy to privacy risk and path from privacy trust to privacy behavioral intention. This study shows powerful evidence of antecedent factors based on protection motivation of individuals' privacy behavioral intention in online environment.

Keywords: privacy protection behavior, privacy trust, privacy risk, protection motivation theory, threat, efficacy

2013년 5월 23일 접수, 2013년 5월 24일 심사, 2013년 9월 16일 게재확정

* 이 논문은 부산대학교 자유과제 학술연구비(2년)에 의하여 연구되었음

** 부산대학교 경영학과 교수(jkkim1@pusan.ac.kr)

*** 교신저자, 부산대학교 경영학과 박사수료(ksh@pusan.ac.kr)

Ⅰ. 서론

최근 온라인 환경에서 사용자의 프라이버시가 침해되는 사례가 빈번하게 발생하여 온라인 사용자를 위협하고 있다. 대규모 쇼핑몰 사이트의 고객정보가 유출되는 사건이나 금융 사이트가 해킹되어 전산망이 마비되는 사건 등이 대표적인 예이다. 이러한 사건들로 인해 자신의 개인정보가 유출되어 직접적으로 심각한 프라이버시 침해를 경험한 온라인 사용자뿐만 아니라 직접 경험하지는 않았으나 뉴스나 주위 사람들을 통해서 간접적인 프라이버시 침해를 경험한 온라인 사용자도 존재한다.

프라이버시 침해를 직접적으로 경험한 온라인 사용자에게는 경제적 피해 및 심리적 피해, 시간손실 피해 등 여러모로 중대한 손해가 발생할 수 있으며, 간접적으로 경험한 온라인 사용자에게도 자신의 프라이버시에 대한 염려나 불안으로 인한 심리적 피해가 발생할 수 있다. 이처럼 프라이버시 침해를 경험한 사용자는 자신이 가지고 있던 기존의 프라이버시에 대한 인식이나 태도에 변화를 가져오게 된다.

온라인 사용자가 프라이버시 침해를 경험하지 않도록 사용자의 프라이버시 보호에 관한 법제도적 방안이나 기술적인 방안이 뒷받침되는 것이 중요하지만 사용자 스스로가 자신의 프라이버시를 지키기 위한 능동적인 노력 또한 매우 중요하다. 따라서 온라인 사용자의 프라이버시를 보호할 수 있도록 인식 및 행동을 변화시키기 위한 접근이 필요하며, 행동을 변화시키기 위해서는 행동에 영향을 미치는 요인에 대한 이해가 중요하다.

본 연구에서는 다양한 분야에서 보호행동의 변화과정을 설명하기 위한 대표적인 이론인 보호동기이론을 온라인 사용자의 프라이버시 보호행동에 영향을 미치는 요인을 규명하기 위해 적용하고자 한다. 보호동기이론을 프라이버시 보호 차원에서 살펴보면, 온라인상에서 사용되는 개인정보의 유출에 따른 위험수준에 대한 개인의 평가인 위협평가와 외부로부터 발생할 수 있는 위협에 대해 대처하는 능력에 대한 개인의 평가인 대처평가에 의해 인지적 매개과정이 일어난다. 위협평가와 대처평가는 보호동기를 유발하는 중요한 요인이고, 결과적으로 이러한 보호동기를 통해 보호행동이 변화한다는 것을 의미한다.

본 연구에서는 보호동기이론을 기반으로 프라이버시 보호행동의 변화를 설명하기 위해 보호동기를 유발하는 요인으로 프라이버시 위험과 프라이버시 신뢰를 설정하고, 이에 영향을 미치는 요인으로 위협과 효능감을 독립변수로 설정한다. 독립변수인 위협과 효능감을 2차 요인으로 측정한다. 위협을 발생가능성과 심각성 요인으로, 효능감은 자기효능감과 반응효능감 요인으로 구성하여 실증분석을 수행한다.

Ⅱ. 이론적 배경

1. 정보프라이버시

프라이버시 개념은 여러 학문 분야에서 다양하게 연구되어 왔다. 초기 연구에서 프라이버시는 주로 '혼자 있을 수 있는 권리'로 정의되어 개인의 사생활 영역에 대한 불가침의 권리를 나타내는 물리적인 개념으로 사용되었다(Smith, et al., 2011).

이후 정보통신기술이 발전함에 따라 대량의 정보가 신속하게 축적 및 분석되는 것이 가능해졌으며, 오프라인뿐만 아니라 온라인에 제공한 개인정보가 자신의 의지와는 상관없이 수집되어 활용될 가능성이 높아져 프라이버시 문제가 심화되고 있다. 따라서 프라이버시 개념을 초기에 정의된 '개인 사생활에 대한 권리'라는 소극적인 의미를 넘어서 '자신의 개인정보를 통제할 수 있는 권리'라는 적극적인 의미로 한층 확장된 개념으로 보는 것이 적절하다(Stone, et al., 1983; Pavlou, 2011). 이처럼 개인정보에 대해 자기결정권을 가지고 통제할 수 있는 적극적인 권리를 의미하는 프라이버시에 대한 정보적 측면이 강조된 개념을 정보프라이버시(Information Privacy)

라 한다.

정보프라이버시는 여러 연구자들에 의해 다양하게 정의되어 왔지만 대부분 '개인정보의 이차적 사용에 대한 통제력'을 내포하고 있다(Belanger, et al., 2006; Belanger, et al., 2011). 개인정보의 이차적 사용은 원래 수집된 것과는 다른 목적으로 데이터가 사용되는 것을 의미한다. 정보프라이버시는 이러한 상황에 대해 스스로 통제할 수 있는 자기결정권을 지니는 것으로 정의할 수 있다.

정보프라이버시에 대한 선행연구를 살펴보면, 정보프라이버시 개념을 다각도적인 관점에서 규명하는 연구가 존재한다. Smith, et al.(1996)은 정보프라이버시를 수집(Collection), 비권한의 이차적 사용(Unauthorized Secondary Use), 부적절한 접근(Improper Access), 오류(Errors)의 네 가지 차원으로 분류하여 정보프라이버시에 대한 개인의 염려와 관련지어 설명하고 있다.

한편, Solove(2006)은 정보프라이버시를 정보수집(Information Collection), 정보처리(Information Processing), 정보확산(Information Dissemination), 침해(Invasion)의 차원으로 분류하고, 정보에 대한 프라이버시 활동을 정보흐름에 따라 설명하고 있다. 이는 온라인 환경에서 사용자의 정보를 수집하여 처리 및 확산하는 과정에서 사용자의 정보가 침해당할 가능성이 존재한다는 것을 의미한다.

온라인 환경에서 사용자는 서비스를 이용하기 위해 자신과 관련된 정보를 직접 제공하기도 하고, 쿠키나 스파이웨어 등으로 인해 자신이 인식하지 못하는 사이에 자신과 관련된 정보가 수집되어 사용되기도 한다(Belanger, et al., 2006). 이러한 과정에서 자신이 제공한 정보가 동의 없이 이차적 사용이 발생하거나 제3자에 의해 불법적으로 사용되는 등의 자신의 개인정보에 대해 문제가 발생할 수 있다. 이렇듯 온라인 사용자가 온라인상에 제공된 자신의 개인정보에 대해 통제권을 잃게 되는 것을 정보프라이버시 침해라고 한다.

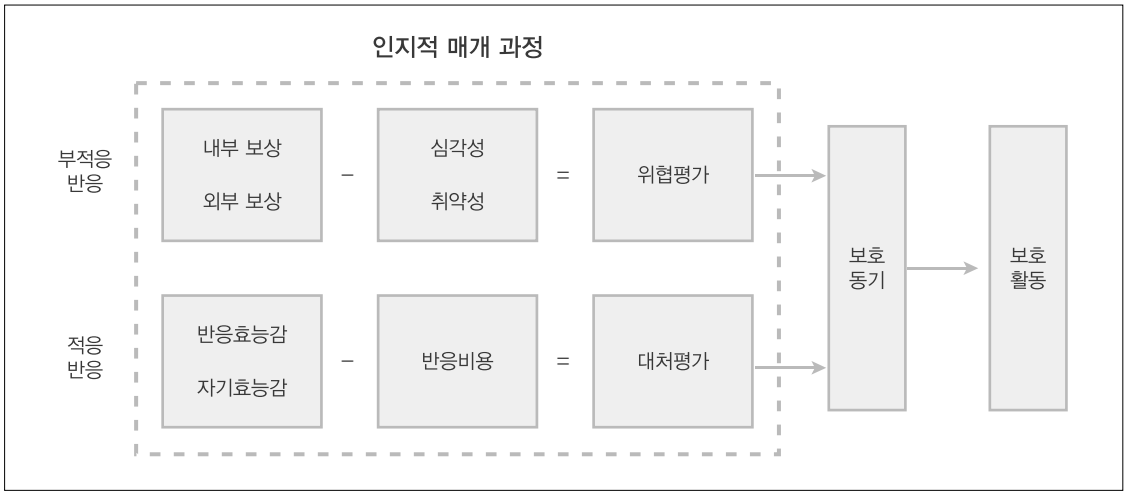
2. 보호동기이론

보호동기이론(PMT: Protection Motivation Theory)은 보건학, 심리학, 경영학 등 다양한 분야에서 사회인지적 차원에서의 보호행동을 설명하고자 연구되어 왔다. 보호동기이론은 기대가치이론(Expectancy-Value Theory)과 인지적 정보처리이론(Cognitive Processing Theory)을 기반으로 공포소구(Fear Appeal)에 의한 태도 및 행동의 변화과정을 설명한다(Ifinedo, 2012).

최초의 보호동기이론은 건강에 대한 태도 및 행동에서 공포소구의 효과를 설명하기 위해 개발되었다(Rogers, 1975). 보호동기이론에 따르면, 위험으로부터 자신을 보호하고자 하는 행동은 심리적 요인에 의하여 보호동기가 형성되어 최종적으로 행동이 결정된다. 즉, 위협 메시지에 노출된 사람은 공포를 느끼게 되고 그에 상응하는 개인의 인지적 평가가 이루어진다는 것이다. 이러한 인지적 매개과정을 통해 보호동기가 조절되고 결과적으로 행동이 변화하게 된다.

보호동기는 위협평가(Threat Appraisal)와 대처평가(Coping Appraisal)라는 인지적 평가과정에서 비롯된다(Rogers, 1975). 먼저, 위협평가는 위협적인 사건에 의해 제기된 위험수준에 대한 개인의 평가로 인지된 취약성(Perceived Vulnerability)과 인지된 심각성(Perceived Severity)으로 구성된다(Rogers, 1983; Woon, et al., 2005; Ifinedo, 2012). 인지된 취약성은 위협적인 사건이 발생하게 될 가능성 정도를 의미하고 인지된 심각성은 그 위협적인 사건에 대한 심각성 정도를 의미한다(Rogers, 1975).

다음, 대처평가는 위협으로부터 발생하는 잠재적인 손실을 방지하고 대처하는 능력에 대한 개인의 평가로 자기효능감(Self-Efficacy), 반응효능감



출처: Floyd, et al.(2000)

〈그림 1〉 보호동기이론의 인지적 매개과정

(Response Efficacy), 반응비용(Response Cost)으로 구성된다(Rogers, 1983; Woon, et al., 2005; Ifinedo, 2012). 자기효능감은 위협적인 사건에 대해 제안된 행동을 수행하거나 대처할 수 있는 개인의 능력에 대한 믿음을 의미하고, 반응효능감은 이러한 제안된 행동을 수행하였을 때 기대되는 능력에 대한 믿음을 의미한다. 반응비용은 제안된 행동을 수행할 때 지출된 금전, 시간, 노력 등의 인지된 기회비용을 의미한다(Rogers, 1975; Rogers, 1983; Woon, et al., 2005; Ifinedo, 2012).

〈그림 1〉에 나타난 바와 같이 위협평가는 부적응반응으로 '위협평가 = 보상 – 위협인지'로 표현할 수 있다. 보상은 부적응반응의 확률을 증기시키고 인지된 위협은 부적응반응의 확률을 감소시켜 결과적으로 위협평가가 이루어지게 한다(Floyd, et al., 2000).

한편, 대처평가는 적응반응으로 '대처평가 = 효능감 – 비용'으로 표현할 수 있다. 효능감 변수는 적응반응의 확률을 증가시키고 반응비용은 적응반응의 확률을 감소시켜 대처평가가 이루어지게 한다(Floyd, et al., 2000). 위협평가와 대처평가는 이러한 인지적 매개과정을 거쳐 보호동기를 조절하게 되고, 형성된 보호동기에 의해 결과적으로 보호행동의 변화가 일어나는 것이다.

초기의 보호동기이론은 보건학에서 건강에 대한 위협적인 메시지를 전달하였을 때 보호동기를 일으켜 자신의 건강을 보호하고자 하는 행동에 변화를 가져온다는 가정을 기반으로 메시지의 효과를 설명하기 위해 연구가 수행되었다(Rogers, 1975). 이후 보호동기이론은 건강증진이나 질병예방과 같은 보건학 이외에도 사고예방이나 환경적 위험 등 위협으로 인하여 보호행동이 요구되는 다양한 분야로 확장되어 연구되었다.

최근에는 IS 분야에서도 보호와 관련된 특정 행동을 설명하고자 보호동기이론을 기반으로 연구가 수행되고 있다. 〈표 1〉에 나타난 바와 같이 IS 분야에서 보호동기이론을 기반으로 수행된 연구는 크게 정보시스템 채택 연구와 보안 연구로 구분된다.

먼저, 정보시스템 채택에 대한 선행연구에서는 안티스파이웨어 채택행동(Chenoweth, et al., 2009), 안티표절소프트웨어 채택행동(Lee, 2011)을 설명하기 위해 보호동기이론이 활용되고 있다. 다음, 보안에 대한 선행연구는 다시 시스템보안 연구와 정보보안 연구로 구분된다. 시스템보안에 대한 연구에

〈표 1〉 IS 분야의 보호동기이론 관련 실증연구

연구자	연구분야	보호동기이론
Chenoweth, et al. (2009)	안티스파이웨어 채택	인지된 취약성, 인지된 심각성, 위협평가, 반응효능감, 자기효능감, 반응비용
Workman, et al. (2009)	정보시스템 보안행동	위협평가(위협의 심각성, 위협의 가능성) 효능감평가(대책효능감, 자기효능감, 통제위치)
Johnston, et al. (2010)	정보보안 행동	(인지된 위협 심각성, 인지된 위협 민감성) → (반응효능감, 자기효능감)
Liang, et al. (2010)	PC사용 보안행동 (회피행동)	(인지된 심각성, 인지된 민감성) → 인지된 위협 보호효과성, 보호비용, 자기효능감
Lee(2011)	안티표절 소프트웨어 채택	위협의 심각성, 위협의 취약성, 반응효능감, 자기효능감, 반응비용
Ifinedo(2012)	보안정책 준수	위협평가(인지된 취약성, 인지된 심각성) 대처평가(반응효능감, 반응비용, 자기효능감)

서는 정보시스템 보안행동(Workman, et al., 2009), PC사용에 대한 보안행동(Liang, et al., 2010)을 설명하기 위해, 정보 자체에 대한 보안 연구에서는 개인사용자의 정보보안 행동(Johnston, et al., 2010) 및 조직의 보안정책 준수행동(Ifinedo, 2012)을 설명하기 위해 보호동기이론이 활용되고 있다.

〈표 1〉에서 나타난 바와 같이 IS 분야에 적용된 보호동기이론 관련 연구가 국외연구에는 몇몇 존재하지만 국내 연구에서는 거의 없는 실정이다. IS 분야뿐만 아니라 프라이버시 분야에서도 특정 행동을 설명하기 위해 보호동기이론을 활용한 연구가 거의 전무하다.

이렇듯 정보보안 분야에서 정보 자체에 대한 보안행동에 영향을 미치는 요인을 살펴보기 위해 보호동기이론이 성공적으로 적용되었듯이 프라이버시 연구에서 자신의 개인정보에 대한 보호행동에 영향을 미치는 요인을 규명하기 위해 보호동기이론을 활용하는 것이 적절하다고 판단된다. 따라서 본 연구에서는 선행연구에서 사용된 보호동기이론의 주요 요인을 중심으로 온라인 사용자의 정보프라이버시 행동과의 관계를 살펴보고자 한다.

3. 신뢰-위험 모델

온라인 환경에서 사용자의 특정 행동을 설명하기 위해 신뢰와 위험 개념이 활발히 논의되어 왔다. 지금까지 수많은 연구에서 개인의 태도 및 행동을 설명하고자 신뢰나 위험 개념을 사용해 왔으며, 신뢰와 위험 개념을 동시에 사용하여 설명하는 연구도 다수 존재하다.

신뢰 개념은 크게 성격 관점, 행동 관점, 심리적 상태 관점의 세 가지 관점으로 구분할 수 있다. 먼저, 성격 관점의 신뢰는 상대방을 신뢰하는 개인의 성향이라는 관점으로 접근하는 것이다. 둘째, 행동 관점의 신뢰는 개인의 행동에 따라 상대방을 신뢰하는 정도의 관점으로 접근하는 것이다. 셋째, 심리적 상태 관점의 신뢰는 불확실성 하에서 피신뢰자의 행동에 대한 신뢰자의 위험 감수의 의지라는 관점으로 접근하는 것으로, 설문을 측정도구로 이용하는 연구에서 개인의 특정 행동을 설명하기 위해 사용되는 가장 대표적인 관점이다(문형구 외, 2011; 김종기 외, 2012).

심리적 상태 관점에 따른 신뢰는 불확실성 하에서 피신뢰자의 행동에 대해 신뢰자가 기꺼이 위험을 감

수하고자 하는 의지로 정의된다(Mayer, et al., 1995). 이때, 신뢰는 교환이나 거래 관계에 있어 불확실성 상황에서 존재하는 개념으로 확실성 상황에서는 설명되지 못한다는 특징을 가진다. 이처럼 심리적 상태 관점의 신뢰는 위험 및 위험감수와 직접적인 관계를 가지므로 사용자 행동을 설명하기 위해 위험 개념과 관련지어 수행된 연구가 다수 존재한다.

이처럼 신뢰와 위험 간의 관계를 설명하고 있는 신뢰-위험 모델에서는 어떤 개념이 선행요인으로 존재하는지에 따라 두 가지 관점이 존재한다. 신뢰를 위험의 선행요인으로 보는 관점과 위험을 신뢰의 선행요인으로 보는 관점이다. 전자는 신뢰가 높을수록 위험이 낮아진다는 관계이고 후자는 위험이 높을수록 신뢰가 낮아진다는 관계로 설정되고 있다.

〈표 2〉는 온라인 환경에서 신뢰 및 위험과 관련된 선행연구가 제시되어 있다. 신뢰가 위험에 부의 영향을 미친다고 설정한 연구로는 Pavlou, et al.(2002), Malhotra, et al.(2004), 장명희(2005) 등이 있고,

〈표 2〉 온라인 환경에서 신뢰 및 위험 관련 실증연구

연구자	연구분야	선행요인	신뢰 및 위험 요인	결과요인
McKinght, et al. (2002)	전자 상거래	지각된 평판, 지각된 품질, 구조적 보장	지각된 위험 → 신뢰	구매의도, 개인정보 공유의도
Pavlou, et al. (2002)	온라인 시장	제도적 구조	신뢰 → 지각된 위험	거래의도
Malhotra, et al. (2004)	온라인 환경	프라이버시 염려 (수집, 통제, 인식)	신뢰 신념 → 위험 신념	개인정보 공개의도
Dinev, et al. (2006)	전자 상거래	-	프라이버시 위험 → 신뢰	개인정보 제공의도
Teo, et al. (2007)	전자 상거래	-	신뢰 → 지각된 위험	태도, 구매의도
Li, et al. (2010)	온라인 거래	인지된 적합성	프라이버시 위험 신념	행동의도
Li, et al. (2011)	온라인 환경	감정(즐거움, 두려움), 공정성 수단(정보의 인지된 적합성, 프라이버시 준수의 인식), 프라이버시 염려	프라이버시 위험 신념	행동의도
Xu, et al. (2011)	위치정보 마케팅	개인화, 개인적 특성 (이전 프라이버시 경험, 개인 혁신성, 쿠폰 이용성향)	지각된 위험	지각된 가치, 개인정보제공의도, 구매의도
서보밀 (2002)	인터넷 뱅킹	보안통제의 인지된 강도	지각된 위험 → 신뢰	사용태도, 사용의도, 실제 사용
김종기 외 (2005)	전자 상거래	자산, 위협, 보안통제	위험 → 신뢰	구매의도
장명희 (2005)	인터넷 쇼핑몰	이해 타산적 믿음, 구조적 보장, 상황적 규범, 친숙함	신뢰 → 위험	구매의도
이동주 외 (2010)	온라인 환경	정보투명성	정보프라이버시 위험, 인터넷 사이트 신뢰	정보제공의도
유일 외 (2008)	온라인 거래	인터넷 활용능력, 사회적 인지, 지각된 취약성, 지각된 정보통제능력, 프라이버시 염려	신뢰	거래의도

위험이 신뢰에 부의 영향을 미친다고 설정한 연구로는 McKinght, et al.(2002), Dinev, et al.(2006), 서보밀(2002) 등이 있다.

〈표 2〉를 보면, 신뢰-위험 모델의 선행요인은 연구 분야 및 목적에 따라 다르게 나타난다. 개인의 능력, 경험, 성향 등과 같은 사용자의 개인적 특성이나 사이트에 대한 평판, 품질, 구조적 보장 등과 같은 웹사이트 특성 등 다양하게 연구되어 왔다.

한편, 신뢰-위험 모델의 결과요인은 대부분 행동과 관련된 태도 및 의도로 연구되어 왔다. 신뢰와 위험 중 어떤 개념이 선행요인인지 상관없이 두 개념 모두 온라인 행동에 있어 중요한 영향을 미친다는 것이 실증분석을 통해 확인할 수 있다.

Ⅲ. 연구모형 및 연구가설

1. 연구모형

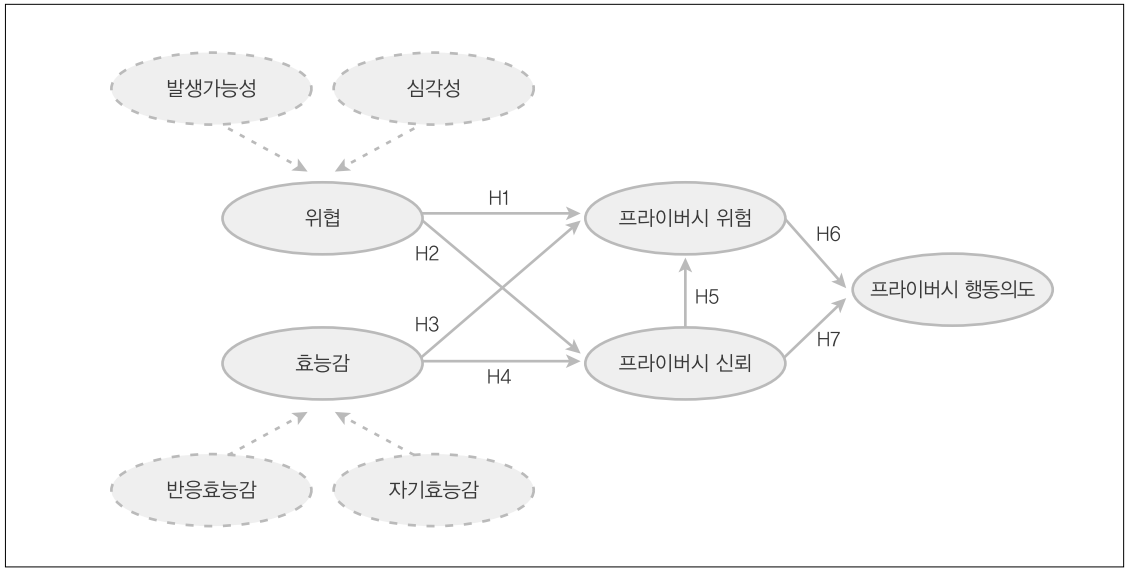
본 연구에서는 온라인 사용자의 정보프라이버시에 대한 보호행동의도에 영향을 미치는 요인을 실증적으로 분석하고자 〈그림 2〉와 같은 연구모형을 설계하였다. 보호동기이론을 기반으로 위협과 효능감이 보호동기요인인 프라이버시 위험과 프라이버시 신뢰에 미치는 영향과 보호동기요인이 프라이버시 보호행동의도에 미치는 영향에 대해 파악하고자 하였다.

2. 연구가설

1) 1차 요인

본 연구에서는 프라이버시 위험과 프라이버시 신뢰에 영향을 미치는 요인인 위협과 효능감을 2차 요인으로 설정하였다. 위협 개념을 발생가능성과 심각성의 1차 요인들로, 효능감 개념을 자기효능감과 반응효능감의 1차 요인들로 구성하였다.

보호동기이론에 따르면, 개인의 인지적 평가에 의해 보호동기가 형성되고 이를 조절함으로써 최종적으로 행동의 변화가 발생한다(Rogers, 1975). 이때, 보호동기는 인지된 취약성과 인지된 심각성에 의한 위협평가와 자기효능감과 반응효능감에 의한 대처평가라는 인지적 매개과정에서 비롯된다(Roger,



〈그림 2〉 연구모형

1983; Woon, et al., 2005; Ifinedo, 2012).

본 연구에서는 온라인 사용자의 정보프라이버시에 대한 위협을 평가하기 위한 요인으로 프라이버시 침해가 발생할 가능성 정도인 발생가능성과 프라이버시 침해가 발생할 경우 문제에 대한 심각성을 설정하였다. 또한 온라인 사용자가 외부의 위협으로부터 발생하는 잠재적인 손실을 방지하고 대처하는 능력을 의미하는 효능감을 평가하기 위한 요인으로 프라이버시 보호에 대하여 자신의 능력에 대한 믿음 정도인 자기효능감과 프라이버시를 보호함으로써 기대되는 결과에 대한 믿음 정도인 반응효능감을 설정하였다.

(1) 위협

김종기 외(2005)는 위협을 정보시스템과 관련된 자산에 대해 의도하지 않은 결과를 초래하는 사건이라고 정의하고, 위협은 발생할 확률과 심각성으로 평가할 수 있다고 설명하고 있다. 위협은 발생할 확률이 아주 낮은 경우라면 거의 무시할 수 있지만, 발생할 확률은 낮지만 발생할 경우 심각한 영향을 야기한다면 위협의 정도는 높게 평가될 수 있다. 반면에 발생할 확률이 높지만 그로 인해 야기될 심각성 수준이 낮다면 위협의 정도는 낮게 평가될 수 있을 것이다(BSI, 1999; ISO/IEC JTC1/SC27, 2000).

Liang, et al.(2010)은 TTAT(Technology Threat Avoidance Theory)를 기반으로 PC사용에 있어 위협을 회피하고자 하는 행동에 영향을 미치는 요인에 대한 연구를 수행하였다. 인지된 위협은 인지된 심각성과 인지된 발생가능성에 의해 결정되고, 이는 위협을 회피하고자 하는 행동에 변화를 가져온다고 가정하고 실증분석을 통해 검증하였다.

본 연구에서는 이러한 선행연구를 기반으로 위협을 온라인 환경에서 개인정보에 피해를 줄 수 있는 잠재적 사건에 대한 인지로 정의하고, 위협을 형성하는 요인을 발생가능성과 심각성으로 설정하였다. 발생가능성은 온라인 환경에서 사용자에게 프라이버시 침해가 발생할 가능성 정도를 의미한다. 온라인 서비스를 이용하거나 웹사이트에 가입하기 위해 제공한 개인정보가 제3자에게 유출되어 동의없이 다른 목적으로 사용될 가능성이 존재하는데, 이러한 잠재적인 위협적 상황에서 온라인 사용자가 프라이버시 침해를 경험할 가능성이 얼마나 높은지 인지하는 정도를 의미한다.

심각성은 온라인 환경에서 사용자에게 프라이버시 침해가 발생할 경우 부정적 결과에 대한 개인의 평가를 의미한다. 온라인상에서 자신의 개인정보가 유출된다면 자신이 입게 되는 피해를 어느 정도 심각하게 인지하는지에 관한 것으로, 자신의 개인정보에 대한 가치나 중요성을 높게 인지할수록 자신의 프라이버시에 대한 위협을 심각하게 받아들일 것이다.

(2) 효능감

Johnston, et al.(2010)은 보호동기이론을 기반으로 보안행동의도에 영향을 미치는 요인에 대한 연구를 수행하였다. 효능감은 위협에 대한 권고된 행동과 관련된 요인으로, 위협을 완화할 수 있는 권고된 행동이 효과적일 것이라는 믿음을 나타내는 반응효능감과 권고된 행동을 수행하기 위한 자신의 능력에 대한 믿음을 나타내는 자기효능감을 포함하고 있다(Witte, 1994).

Workman, et al.(2009)은 정보보안행동에 영향을 미치는 대처행동에 대한 연구를 수행하였다. 위협에 대한 대처가 이루어지기 전에 위협을 예방할 수 있는지 자신의 능력인 자기효능감에 대한 평가와 위협에 대한 대처가 효과적일 것인지 대책효능감에 대한 평가가 이루어진다고 설명하고 있다.

본 연구에서는 이러한 선행연구를 기반으로 효능감을 온라인 환경에서 개인정보에 대한 피해를 줄 수 있는 위협으로부터 개인정보를 보호할 수 있는 능력으로 정의하고, 효능감을 형성하는 요인으로 자기효능감과 반응효능감을 설정하였다. 자기효능감은 온라인 환경에서 프라이버시 보호와 관련된 자신의 능력에 대한 자신감을 의미한다. 프라이버시가 침해받

는 위협적인 사건을 사전에 예방하는 능력으로 개인정보가 안전하게 보호될 수 있도록 잘 관리할 자신이 있는지에 관한 것이다.

반응효능감은 온라인 환경에서 프라이버시 보호에 대하여 기대되는 결과에 대한 믿음을 의미한다. 온라인 사용자가 개인정보를 보호하기 위한 행동을 함으로써 긍정적인 효과에 대한 인식으로, 자신의 개인정보가 유출되어 불법적으로 사용되는 것을 예방할 수 있을 것이라는 믿음에 관한 것이다.

2) 2차 요인 및 연구가설

(1) 위협 및 취약성과 보호동기요인 간의 관계

보호동기이론은 기대가치이론과 인지적 정보처리이론을 기반으로 보호행동의 변화 과정을 설명하고자 한다. 개인의 인지적 평가인 위협평가와 대처평가가 직접적으로 보호행동에 영향을 미치는 것이 아니라 보호동기를 유발하고 이를 통해 보호행동을 변화하게 된다는 것이다.

보호동기이론을 기반으로 한 대부분의 선행연구에서는 위협평가 및 대처평가에 해당하는 주요 요인들이 보호와 관련된 특정 행동과 직접적인 관계를 가지는 것으로 설정하고 있다(Workman, et al., 2009; Johnston, et al., 2010; Liang, et al., 2010). 그러나 보호동기이론에서 제시한 바와 같이 개인의 인지적 평가와 관련된 주요 요인들과 보호와 관련된 행동 사이에는 행동을 유발하는 동기에 해당하는 특정 요인이 존재하는 것이 타당하다. 개인의 인지적 평가로 인해 최종적으로 보호행동이 변화하기까지는 개인의 신념이나 태도가 매개의 역할을 할 것이라 고 판단된다.

다양한 연구 분야에서 개인의 신념이나 태도를 나타내는 대표적인 개념으로 신뢰와 위험이 있다. 신뢰와 위험 개념에 영향을 미치는 선행요인은 다양하게 나타나지만 개인적 특성이 공통적으로 설명되고 있다. 정보프라이버시의 선행연구에서도 개인적 특성이 프라이버시에 대한 신뢰 및 위험에 직접적인 영향을 미치는 것으로 나타났다. 개인적 성향인 프라이버시 염려(Malhotra, et al., 2004; Li, et al., 2011; 유일 외, 2008), 개인적 감정인 즐거움과 두려움(Li, et al., 2011), 개인적 평가인 인지된 적합성과 프라이버시 준수의 인식(Li, et al., 2010; Li, et al., 2011), 개인적 특징인 이전 프라이버시 경험, 개인혁신성(Xu, et al., 2011) 등의 여러 가지 형태의 개인적 특성이 프라이버시에 대한 신뢰 및 위험에 영향을 미치는 것으로 연구가 수행되어 왔다.

본 연구에서는 개인적 특성이 신뢰와 위험에 영향을 미친다는 여러 선행연구(Malhotra, et al., 2004; Li, et al., 2011; Xu, et al., 2011; 유일 외, 2008)를 바탕으로 보호동기요인을 프라이버시에 대한 신념이나 태도를 나타내는 프라이버시 신뢰와 프라이버시 위험으로 설정하였다. 프라이버시 위험은 개인정보와 관련하여 잠재적 손실이 발생할 가능성 정도이고, 프라이버시 신뢰는 개인정보가 올바르게 사용되고 있다고 믿는 정도를 의미한다.

한편, 프라이버시 신뢰와 프라이버시 위험에 영향을 미치는 요인으로 프라이버시와 관련하여 자신의 개인정보가 유출되어 피해를 입을 수 있다고 인지하는 정도인 위협을 설정하였다. 개인이 위협을 인지한다면 자신의 프라이버시에 대한 불안감을 없애기 위해 신념이나 태도를 변화하게 된다는 것이 선행연구를 통해 확인되었다(Johnston, et al., 2010). 따라서 온라인 환경에서 프라이버시 침해와 관련된 위협의 인지가 높을수록 프라이버시와 관련된 손실이 발생할 것이라는 위험의 수준이 높아지고, 프라이버시가 정직하게 사용될 것이라는 신뢰의 수준이 낮아진다는 가설을 설정하였다.

[가설 1] 개인이 지각한 프라이버시에 대한 위협이 높을수록 프라이버시 위험의 수준이 높아질 것이다.

[가설 2] 개인이 지각한 프라이버시에 대한 위협이

높을수록 프라이버시 신뢰의 수준이 낮아질 것이다.

사회인지이론에 따르면, 자신에게 이익이 되는 행동을 수행할 수 있는 능력을 가졌다고 인지하거나 그러한 행동을 수행 시 기대되는 결과를 긍정적으로 인지할 때 행동을 수행하기 위한 동기가 유발된다(Bandura, 2001). 외부의 위협에 대한 예방행동을 수행하기 전에 자신이 수행할 수 있는 능력을 가졌는지와 예방행동이 효과적인지 평가하게 된다(Rogers, 1975).

사회인지이론을 바탕으로 한 효능감 개념은 외부의 위협에 대한 예방행동을 수행할 때 자신이 가진 기술이나 능력에 대한 믿음과 예방행동으로 인한 결과에 대한 긍정적인 믿음으로 구분된다(Workman, et al., 2009). 개인의 신념이나 태도는 이러한 예방행동과 관련된 개인의 인지적 평가인 효능감에 의해서도 변화할 수 있다. 따라서 온라인 환경에서 위협으로부터 자신의 프라이버시를 보호할 수 있는 능력인 효능감이 높을수록 프라이버시에 잠재적 손실이 발생할 것이라는 위험의 수준이 낮아지고, 프라이버시가 올바르게 사용될 것이라는 신뢰의 수준이 높아진다는 가설을 설정하였다.

[가설 3] 개인이 지각한 프라이버시에 대한 효능감이 높을수록 프라이버시 위험의 수준이 낮아질 것이다.

[가설 4] 개인이 지각한 프라이버시에 대한 효능감이 높을수록 프라이버시 신뢰의 수준이 높아질 것이다.

(2) 보호동기요인과 보호의도 간의 관계

다양한 선행연구에서 사용자의 행동을 설명하기 위해 신뢰-위험 모델이 사용되어 왔다(McKnight, et al, 2002; Pavlou, et al., 2002; Malhotra, et al., 2004; Teo, et al., 2007; 서보밀, 2002; 김종기 외, 2005). 정보프라이버시의 선행연구에서도 프라이버시와 관련된 행동을 설명하기 위한 가장 중요한 신념으로 신뢰와 위험을 제시하고 있다(Malhotra, et al., 2004; Li, et al., 2010; Li, et al., 2011; 이동주 외, 2010).

신뢰-위험 모델에서는 신뢰와 위험 간의 관계에서 어떤 요인을 선행요인으로 볼 것인가에 따라 두 가지 관점이 존재한다. 본 연구에서는 신뢰를 위험의 선행요인으로 보는 관점(Pavlou, et al., 2002; Malhotra, et al., 2004; Teo, et al., 2007; 장명희, 2005)을 바탕으로 신뢰가 위험에 직접적으로 영향을 미친다는 연구가설을 설정하였다. 따라서 온라인 환경에서 프라이버시가 올바르게 사용될 것이라는 믿음인 신뢰가 높을수록 잠재적인 손실이 발생할 것이라는 위험이 낮아진다는 가설을 설정하였다.

[가설 5] 개인이 지각한 프라이버시에 대한 신뢰의 수준이 높을수록 프라이버시 위험의 수준이 낮아질 것이다.

위에서 언급한 바와 같이 신뢰와 위험이 사용자의 특정 행동에 영향을 미친다는 것이 여러 선행연구를 통해 확인되었다(Pavlou, et al., 2002; Teo, et al., 2007). 이러한 선행연구를 바탕으로 온라인 환경에서 자신의 프라이버시에 대한 위험의 수준을 높게 인지할수록 프라이버시를 보호하고자 하는 행동의도가 높아지고, 프라이버시에 대한 신뢰의 수준을 높게 인지할수록 프라이버시 보호행동의도가 낮아진다는 가설을 설정하였다.

[가설 6] 개인이 지각한 프라이버시에 대한 위험의 수준이 높을수록 프라이버시 행동의도가 높아질 것이다.

[가설 7] 개인이 지각한 프라이버시에 대한 신뢰의 수준이 낮을수록 프라이버시 행동의도가 낮아질 것이다.

〈표 3〉 조작적 정의 및 측정항목

구성개념	조작적 정의	측정항목	관련 문헌
발생가능성	개인정보가 노출될 가능성 정도	서비스 제공 이외의 다른 목적으로 사용될 가능성	Johnston, et al. (2010), Liang, et al. (2010)
		서비스 사용이 끝난 후에도 동의없이 사용될 가능성	
		제3자에게 공유될 가능성	
		비윤리적으로 사용될 가능성	
		불법적 접근이 발생할 가능성	
심각성	개인정보 노출 시 부정적인 결과에 대한 개인의 평가	개인정보 노출 시 심각한 문제 초래	Johnston, et al. (2010), Liang, et al. (2010)
		개인정보 노출 시 사생활 침해	
		개인정보 노출 시 신상에 대한 위험성	
		개인정보 노출 시 금전적 손실 발생	
자기효능감	개인정보 보호에 관하여 자신의 능력에 대한 믿음	개인정보가 안정하게 보호될 수 있도록 관리에 대한 자신감	Johnston, et al. (2010), Liang, et al. (2010)
		개인정보를 보호하기 위해 통제할 수 있는 능력	
		개인정보를 보호하기 위한 예방수칙 준수	
		웹사이트에서 제시하는 개인정보 보호정책 준수	
		필요할 때 언제든지 개인정보를 보호를 위한 조치 가능	
반응효능감	개인정보 보호에 관하여 기대되는 결과에 대한 믿음	개인정보에 불법적인 접근을 예방	Johnston, et al. (2010), Liang, et al. (2010)
		개인정보가 제3자에게 노출되는 것을 예방	
		신용사기 등의 금전적 손실을 예방	
		정보유출로 인한 이차적 피해에 대한 예방	
		전반적으로 개인정보가 안전하게 보호	
프라이버시 위험	개인정보와 관련하여 기대되는 잠재적인 손실 정도	개인정보 제공은 위험을 수반	Malhotra, et al. (2004), 김종기 외(2005)
		개인정보 제공은 예상치 못한 많은 문제 발생 위험	
		개인정보 제공은 많은 위험의 요소 존재	
		개인정보 제공은 안전에 대한 불안	
		개인정보 제공은 나에게 손실 발생 위험	
프라이버시 신뢰	개인정보가 올바르게 사용되고 있다고 믿는 정도	개인정보의 정당한 사용 및 고객과의 약속에 대한 믿음	Malhotra, et al. (2004), 김종기 외(2005)
		개인정보의 일관성있는 사용에 대한 믿음	
		개인정보를 정직하고 진실되게 다룰 것이라는 믿음	
		개인정보를 다룰 시 나에게 손해를 끼치는 일이 없도록 노력할 것이라는 믿음	
		개인정보 보호와 관련하여 전반적인 신뢰	
프라이버시 행동의도	개인정보를 보호하고자 하는 행동에 대한 의도	개인정보를 보호하기 위한 지속적인 행동	Milne, et al. (2004), Workman, et al. (2009)
		개인정보에 대한 위험을 감소시키기 위한 행동	
		개인정보의 유출을 방지하려는 적극적인 노력	
		개인정보를 안전하게 지키기 위하여 컴퓨터나 웹사이트의 설정을 수정	
		새로운 백신 프로그램과 바이러스, 스파이웨어 등에 대한 지속적인 관심	

Ⅳ. 실증분석

1. 자료의 수집 및 분석

1) 사전조사 및 자료수집

본 연구에서는 보호동기이론을 기반으로 온라인 사용자의 프라이버시 보호행동의도에 영향을 주는 요인을 규명하고자 실증적인 분석을 실시하였다. 본 실증조사가 이루어지기 전에 설문항목이 연구모형의 구성개념에 적절하게 반영되는지 확인하기 위해 부산대학교 경영학과 대학원생들과 학부 학생들을 대상으로 사전조사(Pre-test)를 실시하였다. 탐색적 요인분석 및 응답자들과의 면담을 통해서 설문항목 중 이해가 어렵거나 구성개념을 적절하게 반영하지 못하는 설문항목을 수정하거나 삭제하였다. 여러 차례의 수정과정을 통해 최종 설문에서 사용될 총 7개의 구성개념에 대해 34개의 측정항목이 개발되었다.

본 설문조사는 부산지역의 대학생을 대상으로 설문지를 배부하여 총 230부를 회수하였으며, 그 중 불성실하게 응답을 하거나 결측치가 있는 5부를 제외하고 총 225부가 실증분석을 위해 사용되었다. 기초적인 자료를 분석하기 위해 SPSS 17.0과 구조방정식 모형을 분석하기 위해 SmartPLS 2.0을 분석도구로 활용하였다.

2) 표본의 특성

본 연구에서 수집된 표본 집단의 인구통계학적 특성은 〈표 4〉와 같다. 표본 집단은 대학생을 대상으로 이루어졌기 때문에 대부분 20대로 나타났으며, 성별 비율은 남성이 143명(63.6%), 여성이 82명(36.4%)으로 상대적으로 남성이 높은 것으로 나타났다. 표본 집단의 하루 중 평균 인터넷 이용시간은 컴퓨터를 활용할 때와 스마트폰을 활용할 때 모두 1-2시간이 가장 많은 비중을 차지하는 것으로 나타났다. 표본 집

〈표 4〉 표본의 인구통계학적 특성

구분		빈도 (명)	비율 (%)
성별	남성	143	63.6
	여성	82	36.4
연령	20세 미만	5	2.2
	20-24세	176	78.2
	25-30세	44	19.6
1일 인터넷이용 [컴퓨터]	1시간 미만	64	28.4
	1-2시간	78	34.7
	2-3시간	57	25.3
	3시간 이상	26	11.6
1일 인터넷이용 [스마트폰]	1시간 미만	60	26.7
	1-2시간	85	37.8
	2-3시간	46	20.4
	3시간 이상	34	15.1
개인정보유출 경험정도	경험 없음	26	11.6
	주변사람 경험	18	8.0
	간접적인 경험	116	51.6
	직접적인 경험	65	28.9

단의 개인정보유출 경험 정도를 보면, 경험이 없는 경우가 26명(11.6%), 자신의 경험은 없으나 주변 사람들이 경험을 한 경우가 18명(8.0%), 스팸메일이나 메시지 등으로 간접적인 경험을 한 경우가 116명(51.6%), 해킹 등으로 인해 직접적인 경험을 한 경우가 65명(28.9%)으로 스팸메일이나 메시지로 인해 자신의 개인정보유출이 의심되는 경우가 가장 많은 비중을 차지하는 것으로 나타났다.

2. 측정모형의 평가

본 연구에서는 일반적으로 구조방정식모델링에서 사용되는 이단계 분석법(Two-step Analysis)으로 연구모형을 검증하였다. 이단계 분석법은 먼저 측정모형을 추정하여 측정변수의 질을 평가한 후 구조모형을 추정하여 연구모형에 대한 가설검증을 수행한다. 이는 측정모형과 구조모형을 구분하지 않고 동시에 추정하는 일단계 분석법(One-step Analysis)와는 달리 측정모형과 구조모형을 구분하여 분석함으로써 측정변수의 신뢰성을 정확히 추정할 수 있어 해석상 혼동을 줄일 수 있다(Anderson, et al., 1988).

본 연구에서도 이단계 분석법에 따라 구조모형을 분석하기 전에 측정변수의 신뢰성 및 타당성을 평가하기 위하여 측정모형을 분석하였다. 측정모형의 신뢰성을 평가하기 위해 Cronbach's α, 평균분산추출(AVE: Average Variance Extracted), 합성신뢰도(CR: Composite Reliability)를 이용하였다. Cronbach's α는 한 구성개념을 이루고 있는 측정변수들의 내적일관성을 측정하기 위한 값이고, 평균분산추출은 한 구성개념을 이루고 있는 측정변수들이 설명되는 분산의 비율을 의미하며 합성신뢰도는 측정변수들 간의 공유분산을 의미한다. 일반적으로 Cronbach's α가 0.7 이상, 평균분산추출이 0.5 이상, 합성신뢰도가 0.7 이상이면 신뢰성이 있다고 평가한다(Nunnally, et al., 1994).

타당성은 집중타당성과 판별타당성에 대한 평가로 이루어진다. 집중타당성은 한 구성개념을 이루고 있는 측정변수들이 일치하는 정도를 의미하고, 판별타당성은 다른 구성개념의 측정변수들 간의 차이 정도를 의미하는 것이다. 일반적으로 각 구성개념에 대한 측정변수들의 추정치가 0.5 이상일 때 집중타당성은 확보되고, 각 구성개념에 대한 평균분산추출의 제곱근이 다른 구성개념과의 상관계수보다 크고 그 값이 0.7 이상일 때 판별타당성이 확보된다(Fornell, et al., 1981; Segars, et al., 1993; Barclay, et al., 1995; Chin, 1998).

1) 1차 요인의 측정모형 분석

본 연구에서는 먼저 2차 요인으로 설정된 위협과 효능감 구성개념의 1차 요인에 대한 측정모형의 평가를 실시하였다. 〈표 5〉에 나타난 바와 같이 모든 구성개념들의 Cronbach's α가 0.7 이상, 평균분산추출이 0.5 이상, 합성신뢰도가 0.7 이상으로 나타났고, 각 구성개념의 추정치도 모두 0.5 이상으로 나타나 측정모형의 신뢰성과 집중타당성이 확보된 것으로 평가할 수 있다. 또한 판별타당성 분석을 수행한 결과, 〈표 6〉에서 나타난 바와 같이 평균분산추출의 제곱근이 모두 0.7 이상이고 다른 구성개념과의 상관계수보다 큰 것으로 나타나 판별타당성이 있는 것으로 평가할 수 있다.

2) 2차 요인의 측정모형 분석

1차 요인의 측정모형을 분석한 후 이를 토대로 2차 요인의 측정모형의 분석이 이루어져야 한다. 1차 요인의 측정모형 분석결과로 나타난 잠재변수 요인점수(Latent Variable Score) 측정치를 2차 요인의 측정지표로 사용한다. 본 연구에서는 2차 요인으로 구성된 위협과 효능감 구성개념에 잠재변수 요인점수을 측정지표로 적재하여 측정모형을 평가하였다.

구성개념과 측정변수 간의 관계가 모두 반영지표로 구성된 1차 요인의 모형과는 달리 2차 요인 모형은 반영지표와 형성지표를 모두 포함한다. 구성개념

〈표 5〉 1차 요인의 신뢰성 및 집중타당성 분석

잠재변수	측정변수	표준화 추정치	t-값	Cronbach's α	AVE	CR
발생 가능성	SUS1	0.909	5.450	0.945	0.818	0.957
	SUS2	0.894	4.793			
	SUS3	0.924	5.473			
	SUS4	0.901	4.702			
	SUS5	0.893	5.963			
심각성	SEV1	0.883	48.719	0.887	0.746	0.922
	SEV2	0.894	47.467			
	SEV3	0.853	33.972			
	SEV4	0.823	24.727			
자기효능감	SEL1	0.820	25.030	0.901	0.715	0.926
	SEL2	0.862	30.017			
	SEL3	0.872	45.948			
	SEL4	0.874	44.836			
	SEL5	0.798	26.739			
반응효능감	RES1	0.910	34.426	0.943	0.814	0.956
	RES2	0.916	27.174			
	RES3	0.879	28.775			
	RES4	0.907	40.376			
	RES5	0.897	39.397			

〈표 6〉 1차 요인의 판별타당성 분석

	발생가능성	심각성	자기효능감	반응효능감
AVE 제곱근	0.904	0.864	0.846	0.902
발생가능성	1.000			
심각성	0.397	1.000		
자기효능감	-0.219	-0.051	1.000	
반응효능감	-0.200	0.019	0.436	1.000

과 측정변수 간의 관계가 반영지표인지 형성지표인지에 따라 신뢰성 및 타당성 분석방법이 다르게 평가되어야 한다.

먼저, 구성개념과 측정변수 간의 관계가 반영지표인 경우 1차 요인의 측정모형 분석과 동일하게 Cronbach's α, 평균분산추출, 합성신뢰도를 이용하여 신뢰성 평가가 이루어지고 각 구성개념에 대한 측정변수들의 추정치를 이용하여 집중타당성 평가가 이루어진다. 〈표 7〉에서 나타난 바와 같이 반영지표로 구성된 프라이버시 위험, 프라이버시 신뢰, 프라이버시 행동의도 구성개념은 Cronbach's α가 0.7 이상, 평균분산추출이 0.5 이상, 합성신뢰도가 0.7 이상으로 모두 수용기준치보다 높게 나타나 신뢰성이 있는 것으로 평가할 수 있다. 집중타당성도 각 구

〈표 7〉 2차 요인의 신뢰성 및 집중타당성 분석

잠재변수	측정변수	가중치	추정치	t-값	Cronbach's α	AVE	CR
위협	발생가능성(SUS)	0.773	-	8.179	-	-	-
	심각성(SEV)	0.397		3.321			
효능감	자기효능감(SEL)	0.530	-	3.722	-	-	-
	반응효능감(RES)	0.648		5.005			
프라이버시 위험	RIS1	-	0.879	51.741	0.930	0.781	0.947
	RIS2		0.894	49.142			
	RIS3		0.908	59.422			
	RIS4		0.879	48.164			
	RIS5		0.859	39.183			
프라이버시 신뢰	TRU1	-	0.896	49.386	0.951	0.837	0.963
	TRU2		0.928	77.962			
	TRU3		0.934	92.465			
	TRU4		0.899	59.963			
	TRU5		0.918	94.594			
프라이버시 행동의도	INT1	-	0.906	60.380	0.924	0.770	0.943
	INT2		0.924	96.530			
	INT3		0.897	49.623			
	INT4		0.878	47.380			
	INT5		0.774	20.550			

〈표 8〉 2차 요인의 판별타당성 분석

	위협	효능감	프라이버시 위험	프라이버시 신뢰	프라이버시 행동의도
AVE 제곱근	-	-	**0.994**	**0.915**	**0.877**
위협	1.000				
효능감	-0.196	1.000			
프라이버시 위험	0.552	-0.267	1.000		
프라이버시 신뢰	-0.462	0.481	-0.445	1.000	
프라이버시 행동의도	0.281	0.324	0.361	0.117	1.000

성개념의 표준화추정치가 모두 0.5 이상으로 나타나 집중타당성이 확보된 것으로 평가할 수 있다.

판별타당성 평가는 평균분산추출의 제곱근이 0.7 이상이고 다른 구성개념들과의 상관계수보다 큰 것으로 나타나면 판별타당성이 있다고 판단한다. 〈표 8〉에 나타난 바와 같이 반영지표로 구성된 프라이버시 위험, 프라이버시 신뢰, 프라이버시 행동의도 구성개념이 판별타당성에 대한 수용기준을 만족하므로 판별타당성이 확보된 것으로 평가할 수 있다.

한편, 구성개념과 측정변수 간의 관계가 형성지표인 경우 각 구성개념에 대한 측정변수의 가중치로 신뢰성 평가가 이루어지고 다중공선성의 존재유무를

〈표 9〉 2차 요인의 형성지표에 대한 다중공선성 분석

잠재변수	측정변수	공차	VIF	상태지수
위협	발생가능성	0.847	1.180	10.619
	심각성	0.847	1.180	12.130
효능감	자기효능감	0.810	1.234	8.310
	반응효능감	0.810	1.234	9.148

확인함으로써 타당성 평가가 이루어진다(Chin, 1998; Doz, et al., 2000; Gray, et al., 2004). 형성지표의 측정변수들은 낮은 상관관계를 가지기 때문에 반영지표의 측정변수들이 각 구성개념에 잘 반영되는지를 의미하는 내적일관성 분석은 의미가 없다(Petter, et al., 2007).

다중공선성을 분석하기 위해 공차(Tolerance), VIF(Variance Inflation Factor), 상태지수(Condition Index)를 이용한다. 공차가 0.1보다 크고 VIF가 10보다 작으며, 상태지수가 30 이하이면 측정변수들 간 다중공선성이 없는 것으로 판단되어 타당성을 확보할 수 있다(Stevens, 1992; Chin, 1998; Petter, et al., 2007).

본 연구에서는 〈표 7〉에서 나타난 바와 같이 형성지표로 구성된 위협과 효능감 구성개념의 측정변수의 가중치가 모두 통계적으로 유의한 것으로 나타나 신뢰성이 있다고 평가할 수 있다. 또한 위협과 효능감 구성개념의 다중공선성 분석을 실시한 결과, 〈표 9〉에 나타난 바와 같이 수용기준을 모두 만족하는 것으로 나타나 타당성이 있다고 평가할 수 있다.

3. 구조모형의 평가 및 가설검증

측정모형의 신뢰성 및 타당성을 평가한 후 연구가설을 검증하기 위해 구조모형의 분석을 실시하였다. 먼저, 구조모형의 인과관계를 검증하기에 앞서 적합도 평가를 실시하였다.

적합도 평가는 각 구성개념에 대한 적합도와 모형 전체 적합도에 대한 평가로 이루어진다. 각 구성개념에 대한 적합도는 구조모형의 통계추정량을 나타내는 Redundancy값과 내생변수의 설명된 분산을 나타내는 R^2로 평가한다. 각 구성개념의 Redundancy 값이 양수이고, R^2값이 0.26 이상이면 적합도가 '상', 0.13 이상 0.26 미만이면 '중', 0.13 미만이면 '하'로 평가할 수 있다(Cohen, 1988; Chin, 1998).

구조모형의 전체 적합도는 R^2의 평균과 Communality의 평균을 곱한 값의 제곱근으로 평가하는데, 이 값이 0.36 이상이면 전체 적합도가 '상',

〈표 10〉 구조모형의 적합도 분석

변수	R^2	Redundancy	Communality
위협	-	-	0.682
효능감	-	-	0.716
위험	0.357	0.030	0.781
신뢰	0.373	0.189	0.837
행동의도	0.226	0.077	0.770
평균값	0.319	0.099	0.757
전체 적합도	$\sqrt{0.319 \times 0.757} = 0.491$		

0.25 이상 0.36 미만이면 '중', 0.1 이상 0.25 미만이면 '하'로 평가할 수 있다(Tenenhaus, et al., 2005).

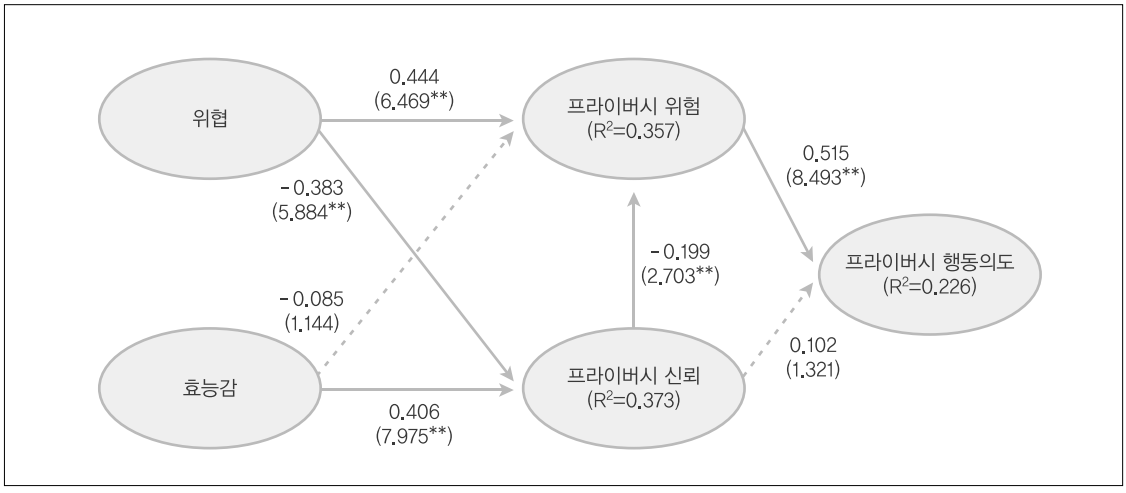
본 연구에서는 〈표 10〉에 나타난 바와 같이 각 구성개념의 Redundancy값은 모두 양수이고, 위험과 신뢰 구성개념의 R^2은 각각 0.357, 0.373으로 적합도가 '상'의 수준으로 높은 것으로 나타났지만 행동의도 구성개념의 R^2은 0.226으로 적합도가 '중'의 수준으로 나타났다. 하지만 구조모형의 전체 적합도가 0.491로 높은 수준으로 나타나 본 연구의 구조모형은 구성개념 간의 인과관계를 설명하는데 적절한 것으로 판단할 수 있다.

구조모형의 각 경로에 대한 유의성을 검정하기 위해 반복적인 샘플링을 통해 t-값을 제시하는 부트스트랩핑(Bootstrapping)을 실시하였고, 반복샘플링의 수는 500회로 설정하였다(Efron, et al., 1997; Chin, 1998). 본 연구의 구조모형에 대한 경로분석을 실시한 결과는 〈그림 3〉과 같다. 연구모형의 각 경로를 살펴보면, 효능감과 프라이버시 위험 간의 경로와 프라이버시 신뢰와 프라이버시 행동의도 간의 경로를 제외한 다른 모든 경로들은 통계적으로 유의한 것으로 분석되었다.

위협 및 효능감과 보호동기요인인 프라이버시 위험 및 프라이버시 신뢰 간의 관계에서는 효능감이 프라이버시 위험에 영향을 미친다는 경로를 제외하고는 모두 통계적으로 유의성이 있는 것으로 나타났다. 가설 1인 위협과 프라이버시 위험 간의 관계에서는 경로계수가 0.444로 긍정적인 영향(t=6.469, p〈0.01)을 미치는 것으로 나타났고, 가설 2인 위협과 프라이버시 신뢰 간의 관계에서는 경로계수가 -0.383으로 부정적인 영향(t=5.884, p〈0.01)을 미치는 것으로 나타났다.

가설 3인 효능감과 프라이버시 위험 간의 관계에서는 경로계수가 -0.085로 부정적인 관계(t=1.144, p〉0.05)는 가지나 통계적으로 유의하지 않은 것으로 나타났다. 가설 4인 효능감과 프라이버시 신뢰 간의 관계에서는 경로계수가 0.406으로 긍정적인 영향(t=7.975, p〈0.01)을 미치는 것으로 나타났다.

보호동기요인인 프라이버시 위험과 프라이버시 신뢰 간의 관계를 설정한 가설 5는 경로계수가 -0.199로 프라이버시 신뢰가 프라이버시 위험에 부정적인 영향(t=2.703, p〈0.01)을 미치는 것으로 나타났다. 보호동기요인인 프라이버시 위험 및 프라이버시 신뢰와 프라이버시 보호행동의도 간의 관계에서 프라



주: * p〈0.05, ** p〈0.01

〈그림 3〉 구조모형의 분석결과

이버시 위험과 프라이버시 행동의도 간의 관계를 설정한 가설 6는 경로계수가 0.515로 긍정적인 영향(t=8.493, p<0.01)을 미치는 것으로 나타났다. 하지만 가설 7인 프라이버시 신뢰와 프라이버시 행동의도 간의 관계에서는 경로계수가 0.102로 부정적인 영향을 미칠 것이라는 가설과는 달리 긍정적인 영향(t=1.321, p>0.05)이 있는 것으로 나타났으며 통계적으로 유의하지 않는 것으로 분석되었다.

Ⅴ. 결론

본 연구는 온라인 사용자의 프라이버시 보호행동의도에 영향을 미치는 요인을 보호동기이론을 기반으로 살펴보고자 하였다. 먼저, 프라이버시 보호행동의도에 영향을 미치는 보호동기요인으로 프라이버시 신뢰와 프라이버시 위험을 설정하고 이들 간의 관계를 규명하고자 하였다. 또한 보호동기요인인 프라이버시 신뢰와 프라이버시 위험에 영향을 미치는 요인으로 개인의 인지적 평가인 위협과 효능감을 설정하여 인과관계를 살펴보기 위해 연구모형을 설계하였다.

보호동기를 유발하는 요인인 위협과 효능감을 2차 요인으로 설정하였다. 위협은 발생가능성과 심각성으로, 효능감은 자기효능감과 반응효능감으로 구성하였다. 먼저, 1차 요인에 대한 측정모형을 평가한 후 이를 토대로 2차 요인에 대한 측정모형 및 구조모형의 평가가 이루어졌다. 1차 요인에 적재된 잠재변수 요인점수(Latent Variable Score)를 2차 요인의 측정지표로 사용하여 분석하였다.

본 연구의 분석결과는 다음과 같다. 총 7가지 가설 중 효능감과 프라이버시 위험 간의 관계를 설정한 가설과 신뢰와 프라이버시 행동의도 간의 관계를 설정한 가설을 제외한 5가지의 가설이 채택되었다.

첫째, 위협과 보호동기요인 간의 관계에서는 위협이 프라이버시 신뢰와 프라이버시 위험에 모두 유의한 설명력을 가지는 것으로 나타났다. 온라인 사용자는 외부로부터 자신의 프라이버시를 위협받고 있다. 온라인 환경에서 개인정보가 유출되는 사건을 직접적으로나 간접적으로 경험할 때 자신의 프라이버시에 대한 위협을 보다 높게 인지하게 된다.

이처럼 자신의 개인정보가 유출되는 사건이 발생하여 피해를 입을 수 있다고 인지하는 정도인 위협의 수준이 높을수록 온라인 환경에서 자신이 제공한 개인정보에 손실이 발생할 수도 있다고 인지하는 위험의 수준이 높아질 뿐만 아니라 자신의 개인정보가 올바르게 사용되고 있다고 믿는 신뢰의 수준이 낮아지게 된다.

둘째, 효능감과 보호동기요인 간의 관계에서는 효능감이 프라이버시 신뢰에는 유의한 설명력을 가지나 프라이버시 위험에는 유의한 설명력을 가지지 않는 것으로 나타났다. 온라인 사용자가 외부의 위협으로부터 자신의 개인정보가 잘 보호될 것이라는 믿음이 높을수록 온라인 환경에서 자신이 제공한 개인정보가 올바르게 사용되고 있다고 인지하는 신뢰의 수준이 높아지지만 손실이 발생할 수도 있다고 인지하는 위험의 수준이 낮아진다고 할 수는 없다.

효능감은 프라이버시 위험에 직접적인 영향을 미치지는 않지만 프라이버시 신뢰를 통한 간접적인 효과가 있는 것으로 나타났다. 외부의 위협으로부터 자신의 프라이버시를 보호할 수 있는 능력에 대한 믿음이 낮다고 해서 위험의 수준을 직접적으로 높게 하는 것은 아니지만 프라이버시에 대한 신뢰의 수준을 낮아지게 하는 효과를 가져다주며, 결과적으로 이러한 낮은 신뢰 수준이 위험 수준을 높이는 영향을 준다고 할 수 있다.

온라인 환경에 제공한 프라이버시가 정직하게 사용되고 있다고 믿는 정도인 프라이버시 신뢰와 선행요인 간의 관계를 살펴보면, 위협보다 효능감이 프라이버시 신뢰에 더 많은 영향을 미치는 것으로 나타났다. 또한 온라인 환경에 제공한 프라이버시에 대한 손실 발생가능성 정도인 프라이버시 위험과 선행요인 간의 관계를 살펴보면, 위협만이 프라이버시 위험

에 영향을 미치는 것으로 분석되었다. 하지만 프라이버시 신뢰가 프라이버시 위험에 유의한 설명력을 가지는 것으로 분석되어 효능감이 프라이버시 신뢰를 통해 프라이버시 위험에 영향을 주는 매개효과를 확인할 수 있었다.

2차 요인으로 형성된 위협과 효능감의 1차 요인들을 살펴보면, 위협을 형성하는 발생가능성과 심각성 요인 중에서 발생가능성이 위협을 형성하는데 더 큰 영향을 미치는 것으로 나타났다. 한편 효능감을 형성하는 자기효능감과 반응효능감 요인 중에서는 반응효능감이 자기효능감보다 효능감을 형성하는데 더 큰 영향을 미치는 것으로 나타났다.

셋째, 보호동기요인인 프라이버시 위험 및 프라이버시 신뢰와 프라이버시를 보호하고자 하는 행동의도 간의 관계에 대해 살펴보았다. 프라이버시 위험은 프라이버시 보호행동의도에 유의한 설명력을 가지나 프라이버시 신뢰는 프라이버시 보호행동의도에 유의한 설명력을 가지지 않는 것으로 분석되었다.

그러나 프라이버시 신뢰는 프라이버시 행동의도에 직접적인 영향을 미치지는 않지만 프라이버시 위험을 통한 간접적인 효과가 있는 것으로 나타났다. 온라인 환경에서 사용되는 개인정보가 올바르게 사용되고 있다고 믿는 정도인 프라이버시 신뢰의 수준이 낮다고 해서 프라이버시를 보호하고자 하는 행동의도를 직접적으로 높게 하는 것은 아니라 프라이버시에 대한 위험을 증폭시키는 효과를 가져다주며, 결과적으로 프라이버시 위험을 높게 인지하는 것이 프라이버시를 보호하고자 하는 행동의도를 높아지게 한다고 할 수 있다.

본 연구의 시사점은 다음과 같다. 본 연구에서는 다양한 분야에서 보호행동의 변화를 설명하고자 제시된 보호동기이론을 프라이버시 분야에 적용하여 프라이버시 보호행동의도에 미치는 영향에 대한 접근을 시도하였다. 보호동기이론을 기반으로 개인의 인지적 평가 과정을 통하여 보호동기가 형성됨으로 인해 프라이버시 보호행동의 변화가 일어난다고 보았다. 본 연구에서는 다양한 선행연구에서 행동을 설명하기 위해 대표적으로 사용되어온 개인의 신념 및 태도를 나타내는 신뢰와 위험을 보호동기요인으로 설정하여 실증적인 분석을 시도하였다는 점에서 의의를 찾을 수 있다.

다음으로 보호동기이론의 기존 연구에서는 보호동기를 유발하는 개인의 인지적 평가를 크게 위협평가와 대처평가로 구분하고 주로 다차원적인 개념으로 측정하고 있는데, 본 연구에서는 프라이버시와 관련된 보호동기를 유발하는 인지적 평가를 위협과 효능감으로 설정하여 이를 2차 요인 구조로 제안하였다. 위협을 발생가능성과 심각성으로, 효능감을 자기효능감과 반응효능감으로 구분하여 이를 각각 위협과 효능감을 형성하는 2차 요인 구조로 설정하여 실증적으로 분석하였다는데 의의가 있다.

이러한 학술적 시사점을 바탕으로 온라인 환경에서 사용자의 프라이버시 보호행동을 강화시키기 위한 방안을 제시할 수 있다. 본 연구의 실증분석 결과에 따르면, 프라이버시 보호행동은 프라이버시 위험에 직접적인 영향을 받고, 프라이버시 위험은 위협에 직접적인 영향을 받는다. 다시 말해, 외부의 위협을 높게 인지하는 사용자가 자신의 프라이버시에 대한 위험을 높게 인지하게 되고, 이로 인해 프라이버시를 보호하고자 하는 행동을 강화시킨다고 할 수 있다.

위협은 이전 경험이나 외부의 환경에 의해서 지각된다. 프라이버시 침해에 대해 직접적인 경험이나 뉴스 및 주위 사람들을 통한 간접적인 경험은 사용자로 하여금 프라이버시에 대한 위협을 높아지게 한다. 따라서 웹사이트의 고객정보 유출 사건이나 금융기관의 해킹 사건 등 온라인 사용자의 프라이버시를 침해하는 사건이 발생한다면, 해당 웹사이트뿐만 아니라 대중매체 및 인터넷을 통해 가급적 많이 노출시켜 사용자들이 사건에 대해 민감하게 반응을 할 수 있도록 하는 노력이 필요하다. 직접적인 피해가 있는 사용자에게는 피해 정도나 그에 따른 대책방안도 제시되어야 하며, 직접적인 피해가 없는 사용자에게도 그들의

프라이버시도 안전하지 않다고 각인시켜줄 필요성이 있다. 그럼으로 인해 온라인 사용자는 프라이버시에 대한 위험을 높게 인지하게 되어 보호행동을 강화할 것이라고 예상된다.

반면에, 온라인 환경에서 개인정보를 취급하는 모든 기업이나 기관은 정부에서 개정한 개인정보보호법 기준에 따라 개인정보를 엄격하게 관리해야할 책임이 있다. 또한 사용자에게 그들의 개인정보가 엄격한 기준으로 관리되고 있다는 것을 숙지시켜줌으로써 사용자의 불안을 줄이고 신뢰를 확보해야 할 의무가 있다.

본 연구의 결과에 따르면, 프라이버시에 대한 신뢰수준을 높이기 위해서는 위협으로부터 자신의 프라이버시가 보호될 수 있다는 믿음인 효능감을 높여주는 것이 중요하다. 자기효능감은 프라이버시 보호에 대한 자신의 능력으로 보호하기 위해 필요한 지식이나 기술에 대한 자신감과 관련이 있다. 반응효능감은 프라이버시 보호대처에 대한 믿음으로 사용자가 대처방법을 확실히 숙지하고 있을 때 반응효능감이 높아진다. 이처럼 자기효능감과 반응효능감은 모두 프라이버시에 대한 교육을 통해 사용자의 지식을 높여줌으로써 형성할 수 있다. 따라서 온라인 환경에서 사용자의 신뢰수준을 높이기 위해서는 사용자의 지식을 향상시키기 위한 프라이버시 교육이 필요하며, 이를 위해 정부나 개인정보보호 기관에서는 구체적이고 실현가능한 정책적 방안을 마련해야 한다.

본 연구의 한계점과 향후 연구방향은 다음과 같다. 첫째, 본 연구의 표본 집단이 대학생을 대상으로 이루어졌기 때문에 표본의 대표성 문제가 존재한다. 본 연구를 일반화시키기 위해서는 표본 대상을 확대하여 포괄적이고 광범위하게 분석되어야 할 필요성이 있다. 연령이나 직업과 같은 인구통계학적 특성에 따라 또는 프라이버시에 대한 이전의 경험이나 민감성 정도와 같은 프라이버시 관련 특성에 따라 프라이버시에 대한 인지 수준이 달라질 수 있다. 따라서 여러 특성에 따른 집단별 분석이나 조절효과 분석과 같은 구체적이고 통제적인 실증연구가 이루어질 수 있을 것이다.

둘째, 본 연구에서는 프라이버시 보호행동의 변화에 영향을 주는 보호동기요인을 프라이버시와 관련된 개인의 신념 및 태도를 나타내는 요인인 프라이버시 신뢰와 프라이버시 위험으로 설정하였다. 이외에도 프라이버시 연구에서 보호행동에 영향을 미치는 보호동기와 관련된 요인이 다양하게 존재할 것이라 예상된다. 따라서 프라이버시와 관련된 행동과 개인의 인지적 평가 사이에서 매개효과를 가져오는 요인에 관한 연구가 지속적으로 이루어져야 할 것이다.

셋째, 본 연구에서는 한 시점에 대한 표본의 특성을 파악하는 것이 목적인 횡단적(Cross-sectional) 연구를 실시하였다. 보호동기이론을 기반하여 프라이버시 보호행동의 변화를 설명하기 위해서 향후 위협적 사건의 경험 전후에 대한 종단적(Longitudinal) 연구가 수행된다면 더욱 의미있는 연구가 될 수 있을 것이다.

■ 참고문헌

김종기·이동호 (2005). “전자상거래 사용자의 신뢰에 영향을 미치는 정보보안위험 기반의 선행요인 연구.” 「경영정보학연구」, 15(2): 65-96.

김종기·김진성·김상희 (2012). “온라인 환경에서 신뢰와 위험 관계에 대한 문헌적 고찰.” 「한국IT서비스학회지」, 11(1): 59-81.

김종기·김상희 (2013). “온라인 사용자의 프라이버시 보호행동에 대한 연구: 프라이버시 역설 관점에서.” 「인터넷전자상거래연구」, 13(1): 41-64.

문형구·최병권·내은영 (2011). “국내 신뢰 연구의 동향과 향후 연구방향에 대한 제언.” 「경영학연구」, 40(1): 227-250.

서보밀 (2002). “Security Control and Risk Analysis under EC Environment.” Ph.D. Thesis, Graduate School of Management, KAIST.

유일·신정신·이경근·최혁라 (2008). “프라이버시 염려

영향요인이 인터넷 이용자의 신뢰와 온라인 거래 의도에 미치는 영향." 「Journal of Information Technology Applications & Management」, 15(4): 37-59.

이동주·방영석·배윤수 (2010). "온라인상의 개인 정보 제공에 있어서 정보 투명성의 역할." 「정보화정책」, 17(2): 68-85.

장명희 (2005). "인터넷 쇼핑몰에서 신뢰와 지각된 위험이 태도 및 구매의도에 미치는 영향." 「정보시스템연구」, 14(1): 227-249.

Anderson, J. & Gerbing, D. (1988). "Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach." *Psychological Bulletin*, 103(4): 411-423.

Bandura, A. (2001). "Social Cognitive Theory: An Agentive Perspective." *Annual Review of Psychology*, 52: 1-26.

Barclay, D. & Thompson, R. & Higgins, C. (1995). "The Partial Least Squares (PLS) Approach to Causal Modeling, Personal Computer Adoption and Use as an Illustration." *Technology Studies*, 2(2): 285-324.

Belanger, F. & Hiller, J. S. (2006). "A Framework for E-Government: Privacy Implications." *Business Process Management Journal*, 12(1): 48-60.

Belanger, F. & Crossler, R. E. (2011). "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems." *MIS Quarterly*, 35(4): 1017-1041.

BSI (1999). *BS7799: Code of Practices for Information Security Management.* United Kingdom.

Chenoweth, T. & Minch, R. & Gattiker, T. (2009). "Application of Protection Motivation Theory to Adoption of Protective Technologies." Proceedings of the 42nd Hawaii International Conference on System Science.

Chin, W. W. (1998). "The Partial Least Squares Approach to Structural Equation Modeling." In G. A. Marcoulides(ed.), *Modern Methods for Business Research*, 295-336. New Jersey: Lawrence Erlbaum Associates.

Cohen, J. O. (1988). *Statistical Power Analysis for the Behavioral Sciences(2nd ed.).* New Jersey: Lawrence Erlbaum.

Dinev, T. & Hart, P. (2006). "An Extended Privacy Calculus Model for E-Commerce Transactions." *Information Systems Research*, 17(1): 61-80.

Doz, Y. L. & Olk, P. M. & Ring, P. S. (2000). "Formation Processes of R&D Consortia: Which Path to Take? Where Does It Lead?" *Strategic Management Journal*, 21(3): 239-266.

Efron, B. & Tibshirani, R. (1997). "Improvements on Crossvalidation: The 0.632+ Bootstrap Method." *Journal of the American Statistical Association*, 92(438): 548-560.

Floyd, D. L. & Prentice-Dunn, S. & Rogers, R. W. (2000). "A Meta-Analysis of Reseach on Protection Motivation Theory." *Journal of Applied Social Psychology*, 30(2): 407-429.

Fornell, C. & Larcker, D. F. (1981). "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error." *Journal of Marketing Research*, 18: 39-50.

Gray, P. H. & Meister, D. B. (2004). "Knowledge Sourcing Effectiveness." *Management Science*, 50(6): 821.

Ifinedo, P. (2012). "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory." *Computers & Security*, 31: 83-95.

ISO/IEC JTC1/SC27 (2000). *Guidelines for the Management of IT Security(GMITS)-Part 1: Concepts and Models of IT Security*, TR 13335-1.

Johnston, A. C. & Warkentin, M. (2010). "Fear Appeals and Inforamtion Security Behaviors: An Empirical Study." *MIS Quarterly*, 34(3): 549-566.

Lee, Y. (2011). "Understanding Anti-plagiarism Software Adoption: An Extended

Protection Motivation Theory Perspective." *Decision Support Systems*, 50: 361-369.

Li, H. & Sarathy, R. & Xu, H. (2010). "Understanding Situational Online Information Disclosure as a Privacy Calculus." *Journal of Computer Information Systems*, 51(1): 62-71.

Li, H. & Sarathy, R. & Xu, H. (2011). "The Role of Affect and Cognition on Online Consumers' Decision to Disclose Personal Information to Unfamiliar Online Vendors." *Decision Support systems*, 51(3): 434-445.

Liang, H. & Xue, Y. (2010). "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective." *Journal of the Association for Information Systems*, 11(7): 394-413.

Malhotra, N. K. & Kim, S. S. & Agarwal, J. (2004). "Internet Users' Information Privacy Concerns(IUIPC): The Construct, the Scale, and a Causal Model." *Information Systems Research*, 15(4): 336-355.

Mayer, R. & Davis, J. H. & Schoorman, F. D. (1995). "An Integrative Model of Organizational Trust." *Academy of Management Review*, 20(3): 709-734.

McKnight, D. H. & Choudhury, V. & Kacmar, C. (2002). "The Impact of Initial Consumer Trust on Intentions to Transact with a Web Site: A Trust Building Model." *Journal of Strategic Information Systems*, 11(3): 297-323.

Milen, G. & Culnan, M. (2004). "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices." *Journal of Interactive Marketing*, 18(3): 15-29.

Nunnally, J. C. & Bernstein, I. H. (1994). *Psychometric Theory(3rd ed.)*. New York: McGraw-Hill.

Pavlou, P. A. & Gefen, D. (2002). "Building Effective Online Marketplaces with Institution-Based Trust." Twenty-Third International Conference on Information Systems.

Pavlou, P. A. (2011). "State of the Information Privacy Literature: Where Are We Now and Where Should We Go?" *MIS Quarterly*, 35(4): 977-988.

Petter, S. & Straub, D. & Rai, A. (2007). "Specifying Formative Constructs in Information Systems Research." *MIS Quarterly*, 31(4): 623-656.

Rogers, R. W. (1975). "A Protection Motivation Theory of Fear Appeals and Attitude Change." *The Journal of Psychology*, 91: 93-114.

Rogers, R. W. (1983). "Cognitive and Physiological Processes in Fear-based Attitude Change: A Revised Theory of Protection Motivation." In J. Cacioppo & R. Petty(eds.), *Social Psychophysiology: A sourcebook*, 153-176. New York: Guilford Press.

Segars, A. & Grover, V. (1993). "Re-Examining Perceived Ease of Use and Usefulness: A Confirmatory Factor Analysis." *MIS Quarterly*, 17(4): 517-525.

Smith, H. J. & Milberg, S. J. & Burke, S. J. (1996). "Information Privacy Measuring Individuals' Concerns about Organizational Practices." *MIS Quarterly*, 20(2): 167-196.

Smith, H. J. & Dinev, T. & Xu, H. (2011). "Information Privacy Research: An Interdisciplinary Review." *MIS Quarterly*, 35(4): 989-1015.

Solove, D. J. (2006). "A Taxonomy of Privacy." *University of Pennsylvania Law Review*, 154(3): 477-564.

Stevens, J. (1992). *Applied Multivariate Statistics for the Social Sciences*. New Jersey: Lawrence Erlbaum Associates.

Stone, E. F. & Gardner, D. G. & Gueutal, H. G. & McClure, S. (1983). "A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes across Several Types of Organizations." *Journal of Applied*

Psychology, 68(3): 459-468.

Tenenhaus, M. & Vinzi, V. E. & Chatelin, Y. M. & Lauro, C. (2005). "PLS Path Modeling." *Computational Statistics & Data Analysis*, 48(1): 159-205.

Teo, T. S. H. & Liu, J. (2007). "Consumer Trust in e-commerce in the United States, Singapore, and China." *The International Journal of Management Science*, 35: 22-38.

Witte, K. (1994). "Fear Control and Danger Control: A Test of the Extended Parallel Process Model(EPPM)." *Communication Monographs*, 61: 113-134.

Woon, I. M. Y & Tan, G. W. & Low, R. T. (2005). "A Protection Motivation Theory Approach to Home Wireless Security." Proceedings of the 26th International Conference on Information Systems.

Workman, M. & Bommer, W. H. & Straub, D. (2009). "The Amplification Effects of Procedural Justice on a Threat Control Model of Information Systems Security Behaviours." *Behaviour & Information Technology*, 28(6): 563-575.

Xu, H. & Luo, X. & Carroll, J. M. & Rosson, M. B. (2011). "The Personalization Privacy Paradox: An Exploratory Study of Decision Making Process for Location-Aware Marketing." *Decision Support Systems*, 51(1): 42-52.