Information Systems Review
Vol. 20, No. 3 September 2018 http://dx.doi.org/10.14329/isr.2018.20.3.051

정보보호 의사결정에서 정보보호 침해사고 발생가능성의 심리적 거리감과 상대적 낙관성의 역할

The Role of Psychological Distance and Relative Optimism in Information Security Decision Making

김 종 기 (Jongki Kim) 부산대학교 경영대학 교수
김 지 윤 (Jiyun Kim) 부산대학교 경영학과 박사수료, 교신저자

요 약

많은 정보보호 분야 연구들은 인식을 높여야 할 필요성을 밝히고 있다. 그러나 정보보호에 대한 인식이 상당한 수준으로 높아졌음에도 실제 보호행동은 최근까지 그에 미치지 못하고 있다. 이에 인식수준과는 별개로 정보보호 의사결정에 심리적 요인이 작용할 것으로 가정하고 정보보호에 대한 인식에 차이가 없는 실험상황에서 심리적 거리감과 낙관편향에 따른 차이를 확인하고 정보보호 행동에 대한 영향을 확인하고자 하였다.

연구결과 모바일 기기 사용자의 확률적 거리감에 따라 정보보호 위험의 지각에 차이가 있었으며, 사회적 거리감에 따라 상대적 낙관성의 정도에 차이가 있었다. 이를 바탕으로 상대적 낙관성을 개념화하고 정보보호 행동의도와의 관계를 분석한 결과 자신과 가까운 사람과 비교해 더 낙관적이라 생각했을 때 정보보호 위험의 수준을 낮게 평가하고 확률적 거리감에 따라 영향력이 달라짐을 확인했다.

본 연구는 방법론적 측면에서 의미 있는 시도를 하였고, 정보보호와 관련한 행동에 있어 심리적 요인을 고려함으로써 실질적 위험지각에 영향을 미치는 상대적 낙관성의 범위를 좁혔다는 데 의의가 있다. 정보보호를 위한 의사결정 과정에 다각도로 접근할 필요성을 실증적으로 규명함으로써 궁극적으로 정보기술 사용자의 정보보호 수준 향상과 정보자산의 보호에 기여할 것으로 기대한다.

키워드 : 정보보호, 상대적 낙관성, 낙관편향, 심리적 거리감, 사회적 거리, 확률적 거리

Ⅰ. 서 론

이제는 필수품이 된 스마트폰을 비롯하여 개인의 모바일 환경은 하루가 다르게 발전하고 있다. 네트워크를 기반으로 하는 모바일의 특성으로 인해 해킹, 스파이웨어, 랜섬웨어를 비롯한 악의적 활동 또한 급속히 증가하고 있다. 정보보호 침해사고(information security incident), 즉 정보보호를 위협할 가능성이 큰 예상치 못한 사건(ISO/IEC 27000, 2016)이 증가함에 따라 정보를 보호하기 위한 기술도 성장하였다. 그러나 기술적 보호의 수준이 높아졌음에도 악의적 활동으로 인한 모바일 사용자의 피해는 계속되고 있다.

정보보호(information security)에 있어 기술만으

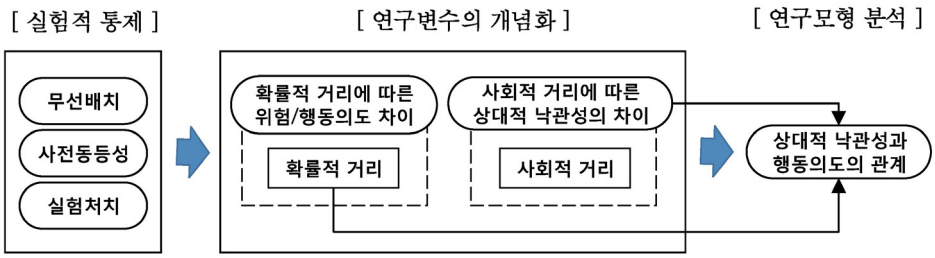
로는 충분하지 않으며 인간 측면의 보안에 주목해야한다(Anderson and Agarwal, 2010). 보안행동의 주체는 기술이 아니라 인간이기 때문에(Chen *et al.*, 2008) 위험을 관리하는 사용자의 노력이 더 중요한 것이다. 이를 위해 대다수의 IS 분야 연구들은 인지-행동 이론을 바탕으로 사용자의 인식을 높여야 할 것을 주장하며 이와 관련한 영향요인들에 집중해 왔다(Bauer, 1960; Bulgurcu *et al.*, 2010; 박정현, 강성민, 2017). 그 결과 각종 조사와 연구에서 정보보호에 대한 전반적 인식은 높아졌으나 보호조치의 수준은 높아진 인식 수준에 여전히 미치지 못하는 것으로 나타났다(한국인터넷진흥원, 2018). 이처럼 정보보호에 대한 인식이 상당한 수준으로 높아졌음에도 보호조치를 취하지 않는 현재의 상황을 살펴볼 필요가 있다. 정보보호는 최종적으로 사용자의 실천이 이루어지느냐에 달려있기 때문이다.

연구질문: 왜 모바일기기 사용자는 정보보호에 대한 높은 인식만큼 정보보호를 실천하지 않는가?

지금까지의 연구들은 인간을 합리적·계획적 행동 또는 계산을 기반으로 한 의사결정을 하는 이성적 정보처리자로 간주하는 것이 대부분이었으나 최근 들어 행동경제학 같은 새로운 접근방식에 대한 관심이 높아지고 있다. IS와 관련한 의사결정과 인간의 인지에 있어 행동경제학을 근간으로 하는 인지적 편향의 역할이 고려할만한 가치가 있기 때문이다(Park and Oh, 2016). 따라서 스마트폰·스마트 패드와 같은 모바일기기 사용자의 정보보호 행동의도를 정보보호를 위한 의사결정 단계로 간주하고 심리적 거리감과 낙관편향의 측면에서 접근하고자 다음과 같이 구체적인 연구질문을 설정하였다.

① 모바일기기 사용자는 '정보보호에 대한 인식 수준'과 관계없이 자신의 정보보호 침해사고의 발생 확률이 높거나 낮은지에 따라 위험의 지각과 보호조치에 대한 의사결정이 달라지는가?
② 모바일기기 사용자는 자신과 가까운 사람보다 자신과 가깝지 않은 사람과 비교했을 때 자신에게 '정보보호 침해사고 발생 가능성'이 더 낮을 것으로 생각하는가?
③ 모바일기기 사용자가 자신에게 '정보보호 침해사고 발생 가능성'이 타인보다 낮을 것으로 생각할수록 위험이 낮다고 생각해서 보호조치를 취하지 않으려 하는가?

위와 같은 연구질문을 해결하기 위해 본 연구에서는 다중기법 단계적 접근방법(multimethod phased approach, Anderson and Agarwal, 2010)을 적용하였다. 연구의 방법이나 기술적 측면을 다양하게 구현하는 다중기법방법론(multimethodology)은 더욱 풍부하고 신뢰성 높은 연구결과를 갖는다(Mingers, 2001). 또한 연구의 목적에 따라 단계별로 적용가능성을 점검하는 단계적 접근방법은 연구의 적절



〈그림 1〉 연구절차

성(relevance)을 높이고 엄격함과의 균형을 유지하는 장점이 있다(Rosemann and Vessey, 2008). 이러한 방법론적 이점을 받아들여 연구의 단계를 나누어 순차적으로 진행하고 다양한 분석을 시도하였다.

<그림 1>의 연구절차에 나타난 바와 같이 본 연구는 먼저 실험적 통제를 적용한 실험을 수행하고 실험을 통해 얻은 결과를 바탕으로 연구모형을 분석하는 단계적 연구과정의 특징을 갖는다. 1단계 실험적 통제를 거친 후 2단계에서 연구질문 ①과 연구질문 ②를 확인한 결과 사회적 거리와 확률적 거리에 따라 상대적 낙관성과 위험의 지각에 다른 영향을 미치는 것을 확인한다. 이로써 사회적 거리가 가까운 경우의 상대적 낙관성과 사회적 거리가 먼 경우의 상대적 낙관성을 각각의 구성개념으로 나누어 볼 근거를 마련한다. 이러한 과정을 통해 주요 구성개념을 다루기 위한 기준점(baseline)에 대한 이해를 높임으로써 연구변수를 개념화하고 연구모형을 설정하여 다음단계에서 최종적으로 연구질문 ③을 확인한다.

연구를 통해 실질적으로 위험지각에 영향을 미치는 심리적 요인들의 역할을 확인함으로써 정보보호를 위한 의사결정 과정에 다각도로 접근할 필요성에 대한 실증적 근거를 마련한다. 궁극적으로는 정보기술 사용자의 정보보호 수준 향상과 정보자산의 보호에 기여할 것으로 기대한다.

Ⅱ. 이론적 배경

2.1 해석수준이론과 심리적 거리감

Liberman *et al.*(2007)은 심리적 거리감(psychological distance)을 설명하기 위해 사람들의 사실에 대한 주관적 경험, 경험에 따른 차이, 차이로 인한 결과를 종합하였다. 연구에 따르면 사람들이 직접적으로 경험하고 현재 주위에 존재하는 환경을 가까운 것, 반대로 현재에 존재하지 않는 것은 먼 것으로 정의한다. 먼 것들은 생각하고 구성하거나 재구성할 수 있지만 직접적으로 경험할 수 없다. 직접 경험할 수 없는 것들에는 각기 다른 이유들이 존재한다. 이를 바탕으로 <표 1>과 같이 심리적 거리의 4가지 차원인 시간적, 공간적, 사회적, 확률적 거리가 등장하였다.

〈표 1〉 심리적 거리의 차원

구 분	설명
시간적 (time/temporal)	과거 또는 미래의 특정 대상이나 사건으로부터의 시간적 거리
공간적(spatial)	지리적 거리
사회적 (social)	타인과의 거리(유사/비유사, 익숙한/낯선, 내부집단/외부집단)
확률적 (hypothetical)	확률적 가능성(높은 확률/낮은 확률, 실제상황/가상의 상황)

출처: Trope and Liberman(2010).

사회적 거리는 자신과 타인과의 거리감으로 자신과 유사한지, 친숙하거나 낯선지, 집단 내부와 외부를 구분한다. 사회적 거리는 오래전부터 공간적 관계와 구별하여 사용한 개념으로 사람들 사이의 개인적·사회적 관계를 특징짓는 이해(understanding)와 친밀감(intimacy)의 정도를 측정 가능한 용어로 축소한 것이다(Park, 1924). 사람과의 관계에서 가깝다고 생각하는 사람과 멀게 느껴지는 사람을 묘사하는 다양한 표현들이 있다. 예를 들어 개방적이고 호감가는 사람이라고 느끼거나, 자신과 동일한 그룹에 속하거나, 자신과 유사한 점을 가진 경우 가깝다고 생각한다. 반면 속마음을 드러내지 않거나 자신과 다른 그룹에 속하는 사람의 경우 멀게 느껴질 것이다. 그러나 사회적 거리에 해당하는 요인이나 상황에 대한 모든 것을 단순히 규정할 수 없으며 친밀감의 정도는 스스로가 명확하게 의식하고 있다(Park, 1924). 그러므로 본 연구에서는 대부분의 선행연구들(Liberman *et al.*, 2007; Trope and Liberman, 2010)과 마찬가지로 자신이 가깝다고 느끼거나 친밀하다고 느끼는 정도를 기준으로 사회적 거리를 나누어 적용한다.

확률적 거리는 확률이 높거나 낮음 또는 현실과 가상의 상태를 구분한다. Todorov *et al.*(2007)은 선

호에 대한 시간(지연)과 확률(위험)의 영향이 동일함을 근거하여 사건에 대한 확률을 심리적 거리의 한 차원으로 볼 수 있으며, 심리적 거리를 근간으로 하는 이들 차원들은 동등한 영향을 갖는다고 밝혔다.

해석수준이론(Construal Level Theory)에 따르면 심리적 거리에 따라 특정 대상에 대한 해석수준이 달라진다. 어떤 해석수준을 갖느냐에 따라 인물, 사물, 사건 등에 대해 다르게 생각하고 이어지는 태도, 인식, 확신, 선택, 행동 등에 서로 다른 영향을 줄 수 있다(Trope *et al.*, 2007; Trope and Liberman, 2010). 다수의 연구에서 상위 또는 하위 수준으로 상황을 해석하는 경향이 각각의 해석관련 인지과정을 활성화하는 조작을 통해 직접 유도될 수 있음을 보여준다(Freitas *et al.*, 2004). 심리적 거리와 해석수준을 적용한 연구는 심리학, 건강, 광고, 마케팅 등 분야에서 활발히 진행되고 있으나 IS 분야에서는 아직 일부(김민지 등, 2015)에 그치고 있다.

2.2 낙관편향

낙관편향(optimistic bias)은 자신이 부정적 상황에 처할 가능성이 다른 사람에 비해 낮다고 믿는 경향을 의미한다(Weinstein, 1989). 선호하지 않는 사건에서는 확률을 낮게 보고 긍정적 결과의 사건에서는 높은 확률을 할당하는 비현실적 낙관주의(unrealistic optimism)로부터 비롯된 개념이다(Weinstein, 1980).

낙관편향의 존재는 사업가들의 생존가능성, 프로젝트 완료시간 등 다양한 긍정적 사건의 연구에서 확인되었다. 부정적 사건에서는 주로 건강과 관련한 위험의 인식에서 연구되었으며 IS 분야의 위험과 관련한 연구(Cho *et al.*, 2010; Rhee *et al.*, 2012)에서도 확인되고 있다.

낙관편향의 원인으로는 자존감을 지키고 위험에 대한 두려움을 줄이기 위한 목적으로 동기부여 된 일종의 왜곡으로 보는 견해와 의도하지 않은 오류 등이 있다(Weinstein and Klein, 1996). 측정방법으로는 직접비교 또는 간접비교를 적용할 수 있다. 직접비교의 경우 다른 사람과 비교한 상대적 가능성을 정확한 숫자로 표현하기 어렵고 더 큰 편향을 생성하는 경향이 있으며 많은 선택이 있는 척도보다 적은 선택의 척도가 더 큰 편향을 갖는 것으로 알려져 있다(Otten and Van der Pligt, 1992; Weinstein and Klein, 1996). 비교대상은 연구에 따라 다양하지만 동료 또는 인구통계학적 특성이 유사한 그룹이 일반적이다. 본 연구에서는 Feng *et al.*(2017)에 따라 상대적 낙관성(relative optimism)을 낙관편향의 구성개념으로 사용하고 타인의 발생가능성에서 자신의 발생가능성을 차감하여 측정한다.

상대적 낙관성은 특정 대상에 대한 상대적 확률이기에 비교의 상대가 누구인지에 따라 달라질 수 있다. 본 연구에서는 심리적 거리의 한 차원인 사회적 거리의 개념을 적용하여 상대적 비교의 대상으로 친밀도가 높은 주변인과 직접적 관계가 없는 타인을 각각 설정하였다.

2.3 정보보호 행동

정보보호(information security)는 해킹, 악성코드 등의 내·외부 위협으로부터 자신이 가진 정보를 안전하게 지키기 위한 모든 활동(관리적·기술적 수단 또는 그러한 수단으로 이루어지는 행위)을 의미한다(김종기, 김지윤, 2017; 한국인터넷진흥원, 2018). 정보보호 행동에는 데이터를 다루고 패스워드와 네트워크의 설정과 사용에 주의를 기울이는 등의 위협을 줄이기 위한 행동이 해당하며 조직과 개인, 컴퓨터와 인터넷 환경을 모두 포함한다(Anderson and Agarwal, 2010; Guo *et al.*, 2011).

본 연구에서는 현재의 정보보호 행동을 통해 실험 참가자의 실험 전 정보보호 수준을 파악하고 실험적 조작 후에는 정보보호 행동의도에 대한 영향을 관측한다. 자기보고식 설문으로 실제 행동을 측정함에 어려움이 있기 때문이다. 같은 이유로 대부분의 연구에서 행동의 측정 대신 행동의도를

측정하고 있으며 의도와 실제 행동 사이의 일관성 있는 관계를 나타내고 있기에 행동의도를 통해 실질적인 행동을 파악하는 데 무리가 없다.

2.4 정보보호 위험

정보보호 관리체계(ISMS: information security management system)에서는 원하지 않는 사건의 중요성과 발생가능성의 조합으로 위험을 정의하고 있으며, 위협이 정보 자산의 취약점을 악용하여 해를 입힐 가능성으로 정보보호 위험(information security risk)을 설명하고 있다(ISO/IEC 27000, 2016).

지각된 위험은 결과에 대한 불확실성과 심각성을 바탕으로 한 주관적 판단(Bauer, 1960)이고 상황에 내재된 위험에 대한 의사결정자의 평가(Sitkin and Pablo, 1992)이며 정보시스템 보안과 관련한 사용자의 평가를 지각된 보호 위험(Guo *et al.*, 2011)으로 정의한 바 있다. 따라서 본 연구에서는 개인이 가진 정보와 관련하여 일어날 수 있는 위험을 정보보호 위험으로 정의하였다.

Ⅲ. 연구모형 및 가설

이론적 배경을 기반으로 선행연구에 대한 검토를 거쳐 정보보호 행동과 관련한 주요 연구변수로 확률적 거리, 사회적 거리, 상대적 낙관성, 지각된 위험을 선정하였다.

3.1 거리감에 따른 차이

지각된 위험은 객관적으로 위험이 존재하는지가 아니라 위험을 주관적으로 어떻게 지각하는지에 대한 개념(Bauer, 1960)이며, 발생가능성은 위험을 평가하는 중요한 요소(ISO/IEC 27000, 2016)이다. 즉, 위험이 발생할 가능성이 높으면 자신의 위험을 높이 평가하게 되는 것이다. 이와 같은 발생가능성과 위험의 관계로 미루어 볼 때 자신의 정보와 관련한 정보보호 위험은 위험한 사건의 발생가능성이 높고 낮음에 따라 그 정도를 다르게 받아들일 것으로 예상할 수 있으므로 다음과 같이 가설을 설정하였다.

H1: 모바일기기 사용자의 정보보호 침해사고에 대한 확률적 거리가 가까우면(확률이 높으면) 확률적 거리가 먼(확률이 낮은) 경우보다 정보보호 위험이 더 높다.

해석수준이론에 의하면 사람들은 심리적 거리에 따라 특정 사건에 대해 다르게 생각하고 그 결과 행동이나 선택 등에 서로 다른 영향을 미친다. 특히 심리적 거리의 한 차원인 확률적 거리의 경우 확률이 높으면 심리적 거리가 줄어들어 방법과 관련한 부차적 특징이 의사결정에 중요하게 작용하고 확률이 낮으면 심리적 거리가 멀어져 결과와 관련된 중요 특징이 작용한다(Todorov *et al.*, 2007). 이러한 확률적 거리의 특징은 발생 확률에 따른 심리적 거리가 도덕적 의사결정에 영향을 미치고, 확률적 거리인 가상성이 심리적 거리로 작용하여 광고내용의 처리에 영향을 미치는 것으로 확인되었으며, 다른 심리적 차원들과 함께 상호간의 영향이 확인되었다(Maglio *et al.*, 2013; 박도형, 2017).

즉, 자신에게 정보보호 침해사고가 발생할 확률이 낮다고 생각하는 것은 확률적 거리가 멀어져 추상적이며 결과 중심적으로 해석하게 되는 반면, 자신에게 정보보호 침해사고가 발생할 확률이 높으면 다가올 사건을 위해 어떻게 해야 할 것인지 과정과 방법에 대한 구체적이고 즉각적인 대응을 생각하게 될 것이다. 따라서 정보보호 침해사고의 발생가능성이 높은 경우 낮은 경우보다 실행가능성이 높은 의사결정을 하게 될 것이므로 다음과 같이 가설을 설정하였다.

H2: 정보보호 침해사고에 대한 확률적 거리가 가까우면(확률이 높으면) 확률적 거리가 먼(확률이 낮은) 경우보다 정보보호 행동의도가 더 높다.

사회적 거리에 따른 차이는 심리학을 비롯한 많은 연구분야에서 다루고 있으며 최근에는 IS 분야에서도 확인되고 있다. 특히 자신과 비교대상 사이의 사회적 거리가 확률 추정에 영향을 미칠 가능성에 주목한 결과 친구와 같은 특정한 대상과 비교했을 때 보다 일반적인 다른 사람과 비교했을 때 더 큰 낙관적 편향을 확인하였다(Harris and Middleton, 1994). 이와 같은 결과는 정보보호 관리자의 위험 지각에 대한 연구에서도 통제가능성과 위험지각의 관계에서 사회적 거리감을 바탕으로 나눈 집단에 따라 낙관편향의 정도에 차이가 있음을 보여주었다(Rhee *et al.*, 2012).

이러한 논의를 근거로 모바일기기 사용자들이 정보보호 침해사고가 발생할 확률을 다른 사람에 비해 낮게 책정하는 데 있어 자신과 친밀한 관계이거나 비슷한 상황의 사람과 비교했을 경우보다 자신과 관계가 없는 다른 사람과 비교하는 경우에 더 긍정적으로 평가할 것으로 예상하고 다음과 같은 가설을 설정하였다.

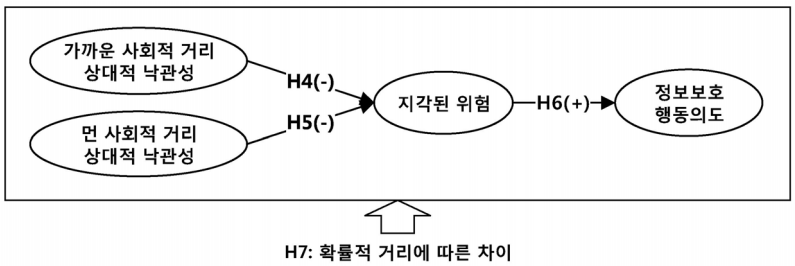
H3: 상대적 낙관성은 (사회적 거리가 가까운 경우보다) 사회적 거리가 먼 경우에서 더 높다.

3.2 주요 구성개념의 인과관계

이전 단계에서 심리적 거리감과 관련하여 살펴본 주요 연구변수를 바탕으로 인과관계의 파악에 필요한 구성개념을 도출하고 <그림 2>와 같이 연구모형을 구성하였다.

IS 분야에서 위험의 수준을 평가할 때 고려되는 개념에는 위협, 취약성, 심각성, 발생가능성 등이 있다(Floyd *et al.*, 2000; ISO/IEC 27000, 2016). 특히, 정보보호 위험은 상당히 주관적이고 계량화하기 어렵기 때문에 다른 사람과 비교하는 사회적 비교(social comparison)를 통해 정보보호에 대한 취약성을 추정함으로써 자신의 정보보호 위험을 평가한다(Rhee *et al.*, 2012). 여기에 위험을 지각하는 과정에서 나타나는 특성(Weinstein and Klein, 1996)인 낙관편향이 작용하면 다른 사람에 비해 자신의 상황이 나은 것으로 판단하게 되고 이는 자신에게 닥칠 절대적 위험의 수준에 영향을 미칠 것이다.

미래의 사건에 대한 비현실적 낙관주의는 특히 선호하지 않는 사건에서 두드러지는데(Weinstein, 1980), 이는 정보보호와 관련한 사고와 연결지어 생각할 수 있다. 따라서 자신에게 정보보호 침해사고가 발생할 가능성이 다른 사람보다 상대적으로 낮다고 생각할수록 정보보호와 관련한 위험 역시 실제보다 낮은 수준으로 평가할 것으로 예상할 수 있다. 또한 앞서 가설 3과 관련하여 설명한 바와 같이 낙관편향을 확인하는 상대적 낙관성은 비교의 대상에 따라 그 정도가 달라질 수 있으므로 사회적 거리에 따른 구성개념의 구분은 본 연구에서 충분히 의미가 있다. 그러나 위험 수준의 평가에 대한 영향력의 정도에는 차이가 있을지라도 방향성은 동일할 것으로 예상하고 다음과 같이 가설을 설정하였다.



〈그림 2〉 연구모형

H4: 사회적 거리가 가까운 사람에 대한 상대적 낙관성이 높을수록 지각된 위험에 부(-)의 영향을 미칠 것이다.

H5: 사회적 거리가 먼 사람에 대한 상대적 낙관성이 높을수록 지각된 위험에 부(-)의 영향을 미칠 것이다.

스트레스를 가져올 수 있는 사건에 대한 개인의 평가는 행동에 큰 영향을 줄 수 있으므로(Lazarus and Folkman, 1984) 위험에 대한 사용자의 주관적 평가인 정보보호 위험 지각과 정보보호 행동의도의 관계를 고려하고자 한다.

IS 분야의 연구에서 지각된 위험의 영향은 다양한 형태이다. 인터넷 뱅킹과 모바일 뱅킹, P2P 공유 소프트웨어 등 각종 수용행동에 대해서는 지각된 위험이 부정적 영향을 미치는 것으로 나타났다(Kim *et al.*, 2009; Luo *et al.*, 2010; Xu *et al.*, 2005). 반면 보호조치를 위한 행동에 대해서는 각 위험들이 행동의도를 증가시키는 요인임을 확인하였다(Van Schaik, 2018). 이외에도 IS 분야의 대표적 모델인 보호동기이론을 바탕으로 한 많은 연구들은 위험을 높이 지각할수록 보호행동에 대한 의도가 높아짐을 보여준다(Boss *et al.*, 2015; 김종기, 김지윤, 2017).

이처럼 지각된 위험의 영향은 연구의 대상인 사용자 행동의 성격에 따라 긍정적이거나 부정적으로 다른 결과를 보일 수 있다. 예를 들어 모바일 뱅킹 수용의 경우 사용에 따른 결과를 알 수 없기 때문에 위험을 높게 지각하면 조심스러워져서 모바일뱅킹을 사용하지 않으려는 부정적 영향을 보이지만 실질적 보호를 위한 보호행동의 경우에는 다른 결과가 나타나는 것이다. 따라서 정보보호 위험을 높게 지각하면 정보를 보호하기 위한 정보보호 행동을 수행하게 될 것으로 예상하고 다음과 같은 가설을 설정하였다.

H6: 지각된 정보보호 위험이 높을수록 정보보호 행동의도에 정(+)의 영향을 미칠 것이다.

일반적으로 위험이 확률적으로 낮게 평가될 때 낙관주의는 더 증가한다(Weinstein, 1989). 위험한 사건이 발생할 가능성이 낮을수록 다른 사람과 비교했을 때 자신의 상황을 더 낙관적으로 평가하게 될 것이다. 따라서 상대적 낙관성과 정보보호 행동의도의 전체 경로에서 확률적 거리감에 따라 영향력의 차이가 있을 것으로 가설을 설정하였다.

H7: 상대적 낙관성과 정보보호 행동의도의 관계는 모바일기기 사용자의 정보보호 침해사고에 대한 확률적 거리에 따라 달라질 것이다.

Ⅳ. 연구방법

4.1 측정항목의 개발 및 분석도구

선행연구의 측정항목을 바탕으로 연구목적에 맞게 일부 수정하고 설문사전조사(pre-test), 탐색적 요인분석, 응답자들과의 면담과 수정과정을 거쳐 개발된 총 27개의 측정항목이 최종 설문에서 사용되었다. 연구변수에 대한 조작적 정의와 측정항목은 다음 <표 2>와 같다.

상대적 낙관성은 타인의 발생가능성과 자신의 발생가능성을 측정하여 계산한 값으로 단일항목척도를 사용하였다. 단일항목척도는 제한적인 정보를 갖기 때문에 일반적으로 신뢰성을 낮게 평가한다. 그러나 구성개념이 명확한 하나의 의미를 갖고 모호하지 않다면 단일측정항목으로 충분하며 피로감을 줄일 수 있어 때로는 다중항목척도보다 더 효과적이다(Rossiter, 2011; Wottrich *et al.*, 2017). 따라서 낙관성과 같이 관찰할 수 없는 특성의 측정이라 하더라도 간접비교를 통해 산출된 측정값이 구성개념에 대한 명확하고 개별적으로 식별 가능한 하나의 의미를 가진 척도이므로 단일항목척도의 사용에 무리가 없다.

〈표 2〉 연구변수의 조작적 정의와 측정항목

연구변수	조작적 정의	측정항목	관련연구
정보보호 인식	모바일기기 사용자의 정보보호 행동에 대한 지식과 이해의 정도	1. 잠재적 '정보보호' 문제에 대해 충분히 알고 있다	Bauer and Bernroider(2017), Bulgurcu *et al.* (2010)
		2. '정보보호'와 관련한 우려와 위협이 야기하는 일반적인 위험에 대해 이해하고 있다	
		3. 잠재적 보안위협과 그로 인해 나타날 수 있는 부정적 결과에 대해 인식하고 있다	
		4. 나의 부주의한 행동 때문에 발생할 수 있는 잠재적 위협과 그로 인한 부정적 결과에 대해 알고 있다.	
정보보호 행동	모바일기기 사용자가 내·외부 위협으로부터 자신이 가진 정보를 보호하기 위한 행동	1. 모바일기기에 보안 잠금을 설정하여 이용(비밀번호/화면 패턴)	한국인터넷진흥원 (2017, 2018)
		2. 공식 앱 마켓이 아닌 다른 출처(출처를 알 수 없는 앱)의 앱은 설치하지 않음	
		3. 단문 문자(SMS) 또는 SNS 메시지에 포함된 URL 클릭하지 않음	
		4. 공인인증서는 모바일기기에 바로 저장하지 않고 USIM 등 안전한 저장장소에 보관	
		5. 운영체제(iOS, 안드로이드)와 모바일 백신 최신버전으로 업데이트	
		6. 루팅, 탈옥 등 모바일기기 구조 임의로 변경하지 않음	
		7. 앱 설치시 과도한 권한을 요구하는 앱은 설치하지 않음	
		8. 제공자가 불명확한 무선랜(WiFi) 이용하지 않음	
		9. 모바일기기에 저장한 중요한 정보 정리 (주민등록증, 보안카드가 찍힌 사진 등)	
		10. 블루투스, WiFi 등 무선 인터페이스는 사용 시에만 켜놓음	
		11. 사용하고 있는 모바일기기의 정보 백업(사진, 문서, 연락처 등)	
상대적 낙관성	자신이 부정적 상황에 처할 가능성이 다른 사람에 비해 낮다고 믿는 정도	1. 자신에게 '사이버 침해 사고'가 발생할 가능성의 정도	Feng *et al.*(2017), Weinstein(1980)
		2. 자신과 친밀하다고 생각하는 주변사람에게 '사이버 침해 사고'가 발생할 가능성	
		3. 자신과 전혀 상관없는 일반적인 주변사람에게 '사이버 침해 사고'가 발생할 가능성	
지각된 위험	모바일기기 관련 위험에 대한 사용자의 평가	1. 전반적으로, 모바일기기 사용은 내 정보를 위험에 처하게 할 것이다	Featherman and Pavlou(2003), Guo *et al.*(2011)
		2. 모바일기기를 사용함으로써 내 정보를 잃을 가능성이 있다	
		3. 모바일기기를 사용함으로써 내 정보에 대한 불확실성이 높아질 것이다	
		4. 모바일기기 사용은 나에게 중요한 정보를 위험하게 할 것이다	
정보보호 행동 의도	정보를 보호하기 위한 행동을 하고자 하는 모바일기기 사용자의 의도	1. 내 모바일기기에 보호조치를 취할 것 같다	Anderson and Agarwal(2010), Tu *et al.*(2015)
		2. 내 모바일기기에 보호조치를 취할 가능성이 있다	
		3. 반드시 내 모바일기기에 보호조치를 취할 것이다	
		4. 앞으로 보호조치를 취할 생각이 있다	
		5. 가능할 때마다 보호조치를 취할 생각이 있다	

정보보호 행동의 측정은 모바일 보안을 위한 예방조치 항목(한국인터넷진흥원, 2017)을 바탕으로 구성하였다. 해당 항목은 모바일기기를 사용하면서 입을 수 있는 피해를 방지하기 위해 실천해야 할 사항으로 한국인터넷진흥원(2016)이 『정보보호 실천수칙(스마트폰편)』을 통해 제공하고 있다. 이는 모바일기기를 사용하는 모든 사용자를 대상으로 하는 가이드이므로 모바일기기 사용자의 정보보호 행동 측정에 적합한 항목으로 판단하였다.

분석을 위한 도구로는 기초적 분석을 위해 SPSS 23.0을 사용하였으며 구조모형의 분석에는 자료의 분포에 대한 제약이 적고 상대적으로 소규모 표본에서 사용할 수 있는 SmartPLS 2.0을 사용하였다.

4.2 표본의 선정 및 실험집단의 구성

본 연구의 기반이 되는 연구방법인 실험은 독립변수에 대한 조작(manipulation)과 실험단위(experiment unit)를 실험 조건으로 통제하는 특징을 갖는다(Kirk, 2014). 실험 참가자는 모바일기기를 사용하는 대학 학부생으로 선정하였으며 피험자를 집단으로 나눠 각각 다른 처치(treatment)를 하는 피험자 간 설계(between subjects design)를 실시하였다. 실험적 통제 방법으로는 실험 단위에 처치조건을 무작위 배당하는 무선배치(random assignment)를 실시하여 선택편향(selection bias)을 제거하였으며 무선배치의 단위는 동일과목의 분반으로 설정하여 집단 간 사전 동등성(prior equivalence)을 확보하였다.

4.3 실험방법

실험도구로는 실험조작 내용을 포함한 온라인 설문 프로그램을 이용하였다. 표면적인 실험의 목적은 『모바일기기 사용자 실태조사』로 설정하여 실험의 목적이 드러나지 않도록 하였다. 실험을 위한 조작방법으로는 의사전달을 어떻게 하느냐에 따라 전달받은 사람의 태도나 행동이 달라지는 프레이밍효과(praming effect)를 이용하여 확률적 거리감을 조작하였다. 실험은 컴퓨터를 이용할 수 있는 강의실에서 수행하였으며 진행순서는 다음과 같다.

1. 실험을 위한 온라인 설문 프로그램을 준비하였다. 설문 프로그램에는 일반적인 설문내용과 함께 실험 조작물이 포함되어있다. 실험 조작물은 각 실험 집단별로 2가지 확률을 미리 지정하여 제작하였으며 확률이 높은 집단은 86%와 87%, 확률이 낮은 집단은 10%와 11%이다.
2. 실험을 위한 온라인 설문 프로그램을 실험실 컴퓨터에 설치하였다. 실험의 사실성(realism)을 높이기 위해 처치조건을 적용한 4가지 프로그램은 좌・우는 물론 앞・뒷자리와 중복되지 않을 것을 고려하였으며 같은 비율로 설치하였다.
3. 실험 참가자들이 특별한 제약 없이 원하는 자리를 선택하면 실험을 시작하였다.
4. 먼저 실험 참가자들에게 표면적 실험의 목적을 알리고 모바일기기에 대한 정의를 제공한 후 모바일기기의 사용여부와 종류를 묻는 가벼운 질문으로 시작하였다.
5. 정보보호에 대한 인식과 실천사항을 알아보기 위한 설문을 실시하였다.
6. 다음 화면에서 <그림 3>과 같이 '당신에게 사이버 침해사고가 발생할 확률'을 피험자에게 제공하였다. 화면에는 직전 단계에서 피험자가 응답한 정보보호에 대한 인식수준과 실천정보를 이용하여 계산되었다고 밝혔지만, 화면에 표시한 확률은 피험자에게 밝힌 것과 달리 실험을 위해 조작된 실험 조작물이다. 피험자의 실제 응답과 관계없이 피험자가 배치된 확률적 거리의 집단에 따라 각각 높거나(86%, 87%) 낮은(10%, 11%) 확률이 제공되었다.

〈그림 3〉 참가자에게 제공된 실험 조작 화면

〈표 3〉 '자신에게 침해사고 발생확률'의 집단별 차이분석

집단	표본 수	평균	표준편차	평균차이	t값	p값
정보보호사고 발생확률 낮음	65	4.150	1.413	-0.473	-2.497	0.013 (양측)
정보보호사고 발생확률 높음	61	4.620	1.337			

7. 실험 조작물에 노출 후 지각된 위험, 정보보호 행동의도, 상대적 낙관성에 대한 설문을 실시하였다.
8. 마지막으로 인구통계학적 항목과 처치점검을 위한 설문에 응답함으로써 실험을 마쳤으며 실험에는 평균 10분 정도 소요되었다.
9. 설문결과는 온라인으로 즉시 수집되었으며 동일한 방법으로 반복하였다.

4.4 처치점검과 조작점검

실험에서는 관심있는 현상이 일어나는 조건을 의도적으로 조작함으로써 연구내용에 부합하는 상황을 만들어 관심있는 요소를 관찰한다. 관심요소의 특정한 상태를 구성하기 위한 실험조건의 조작은 실험적 처치를 통해 이루어지므로 연구자가 의도적으로 조작한 실험조건에 피험자가 주목했는지 먼저 확인할 필요가 있다. 따라서 실험조건에 부적합한 데이터를 걸러내는 방법인 처치점검(treatment check)을 실시하였다(Marett, 2015). 설문 마지막에 자신의 '사이버 침해사고 발생률'을 '높다/낮다'로 응답하도록 하고 각 집단별 처치 내용과 일치하는 응답의 참가자를 구분하였다. 점검결과 전체 실험 참가자 211명 중 126건의 응답을 최종 분석대상으로 선정하였다.

다음으로 실험조작이 실제 이루어졌는지 집단별로 확인하는 조작점검(manipulation check)을 수행하였다. <표 3>과 같이 집단별로 자신에게 '사이버 침해사고'가 발생할 확률(7점 척도)의 응답 차이를 비교해보면 정보보호 침해사고의 발생확률이 높은 집단(평균 4.620, 표준편차 1.337)과 낮은 집단(평균 4.150, 표준편차 1.413)은 통계적으로 유의한($p < 0.05$, 양측) 차이가 있는 것으로 나타나 실험을 위한 조작이 적절히 이루어진 것으로 판단하였다.

4.5 표본의 특성

인구통계학적 분석 결과는 <표 4>와 같다. 응답자의 대부분은 20대로 하루 모바일기기 사용시간은 3~4시간이 가장 많았으며 54.0%가 사이버 침해사고의 경험이 없고 직접 사이버 침해사고를 경험한 사람과 주변사람이 경험한 경우는 27.7%와 18.3%로 나타났다.

〈표 4〉 표본의 인구통계학적 특성

구 분		빈도	백분율(%)
성별	남	71	56.3
	여	55	43.7
연령	10대	1	0.8
	20대	123	97.6
	30대	2	1.6
OS	안드로이드	62	49.2
	iOS	64	50.8
사용 시간	1시간 미만	3	2.5
	1~2시간	11	8.7
	3~4시간	71	56.3
	5시간 이상	41	32.5
침해 경험	경험 없음	68	54.0
	직접 경험	35	27.7
	주변사람 경험	23	18.3

4.6 실험조작 전 두 집단의 정보보호 인식과 행동의 차이 검증

<표 5>에 나타난 바와 같이 실험조작 전 정보보호에 대한 인식과 행동은 집단 사이에 통계적으로 유의한 차이가 없으므로 확률적 거리를 조작하기 전 두 집단은 정보보호 인식과 행동의 수준이 유사한 집단으로 판단하였다.

〈표 5〉 확률적 거리 집단에 따른 인식과 행동의 차이

	확률적 거리	표본 수	평균	표준 편차	t값 (p:양측)
정보보호 인식	먼	65	4.745	1.186	0.795 (0.428)
	가까운	61	4.612	1.259	
정보보호 행동	먼	65	7.222	2.093	0.711 (0.478)
	가까운	61	7.010	2.251	

Ⅴ. 실증분석

5.1 거리감에 따른 차이 검증

확률적 거리에 따른 지각된 위험과 정보보호 행동의도의 차이를 분석한 결과는 <표 6>과 같다. 확률적 거리가 멀거나 가까운가에 따라 지각된 위험은 통계적으로 유의한 차이($F = 3.838$, $p < 0.05$)가 있는 것으로 나타나 H1은 채택되었으나 행동의도에는 유의한 차이가 없어 H2는 기각되었다. 자신에게 정보보호 침해사고가 발생할 확률을 높다고 생각하면 낮게 생각하는 경우보다 정보보호와 관련한 위험이 높을 것으로 생각하는 반면 정보보호 행동을 취하고자 하는 마음에는 차이가 없음을 확인한 것이다.

사회적 거리에 따른 상대적 낙관성의 차이를 분석한 결과는 <표 7>과 같다. 상대적 낙관성은

〈표 6〉 확률적 거리의 집단에 따른 위험과 정보보호 행동의도

가설	요인	확률적 거리	표본 수	평균	표준편차	F(p)	채택여부
H1	지각된 위험	먼	65	4.525	1.343	3.838 (0.025)	채택
		가까운	61	4.859	1.115		
H2	정보보호 행동의도	먼	65	5.285	1.234	0.075 (0.393)	기각
		가까운	61	5.241	1.115		

〈표 7〉 사회적 거리에 따른 상대적 낙관성

가설	요인	사회적 거리	평균	표준편차	평균 차이	t(p)	채택여부
H3	상대적 낙관성	먼	0.680	1.370	0.384	6.093 (0.000)	채택
		가까운	0.290	0.883			

자신과 가까운 사람과 자신과 먼 거리의 사람 사이에 통계적으로 유의한 차이($t = 6.093$, $p<0.001$)가 있는 것으로 나타나 H3은 채택되었다. 자신과 가까운 사람들보다 자신과 관계가 없는 사람들과 비교했을 때 상대적으로 자신을 더 낙관적으로 생각한다는 것을 확인한 것이다.

5.2 구조모형을 이용한 인과관계의 검증

측정도구의 타당성과 신뢰성을 검증하고 경로분석 결과를 이용하여 가설을 검정한다. 구성개념을 측정에 적합한 도구임을 먼저 평가함으로써 가설검정 결과를 충분히 지지할 수 있는 모형임을 증명한다.

5.2.1 측정도구의 평가

연구에서 사용된 요인에 대한 측정도구 평가 결과는 <표 8>과 같다. 각 요인에 대한 적재치가 0.8 이상이고 모든 Cronbach's α가 0.9 이상, CR이 0.9 이상, AVE가 0.7 이상, AVE의 제곱근 값이 다른 구성개념과의 상관계수보다 크고 0.8 이상으로 나타나 측정도구의 신뢰성과 타당성이 충분한 것을 확인하였다.

5.2.2 구조모형의 평가

구조모형에 대한 분석 결과 <표 9>에 나타난 바와 같이 모든 구성개념의 중복성 값이 양수이고 R^2 값이 0.143 이상으로 각 구성개념에 대한 설명력은 다소 낮으나 모형 전체 설명력은 '상'으로 평가되었다. 따라서 본 연구의 구조모형은 연구가설 대한 설명에 무리가 없는 것으로 판단하였다.

〈표 9〉 구조모형의 설명력 분석

구성개념	R^2	중복성	공통성
상대적 낙관성 1	-	-	1.000
상대적 낙관성 2	-	-	1.000
지각된 위험	0.143	0.083	0.796
행동의도	0.234	0.193	0.844
평균값	0.169	0.055	0.910
전체 설명력	$\sqrt{0.169 \times 0.910} = 0.392$		

〈표 8〉 측정도구의 신뢰성 및 타당성 분석 결과

구성개념	측정지표		α	AVE	CR	행동의도	상대적 낙관 1	상대적 낙관 2	지각된 위험
정보보호 행동의도	1	0.895	0.942	0.811	0.955	(0.900)			
	2	0.912							
	3	0.887							
	4	0.910							
	5	0.898							
상대적 낙관 1	1	1.000	1.000	1.000	1.000	0.072	1		
상대적 낙관 2	1	1.000	1.000	1.000	1.000	0.123	0.752	1	
지각된 위험	1	0.917	0.903	0.770	0.940	0.316	-0.190	-0.141	(0.877)
	2	0.855							
	3	0.839							
	4	0.895							

주) 괄호는 AVE 제곱근.

5.2.3 가설의 검증

구조모형의 각 경로에 대한 유의성을 검증하기 위해 반복적인 샘플링을 통해 t-값을 제시하는 부트스트랩핑(bootstrapping)을 실시하고, 반복샘플링의 횟수는 5,000회로 설정하였다. 본 연구의 구조모형에 대한 경로분석 결과는 <그림 4>와 같다.

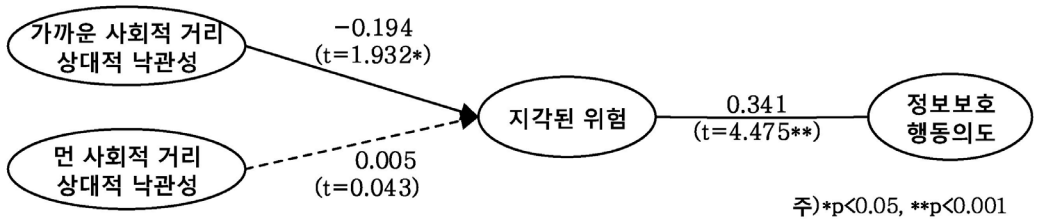
연구모형의 각 경로를 살펴보면, 사회적 거리가 가까운 사람과의 상대적 낙관성은 지각된 위험에 부정적 영향(-0.194, t = 1.932, p < 0.050)을 미치는 것으로 나타나 가설 4는 채택되었으나 사회적 거리가 먼 사람과의 상대적 낙관성은 지각된 위험에 통계적으로 유의한 영향을 미치지 않는 것으로 나타나 가설 5는 기각되었다. 지각된 위험과 행동의도의 관계에서는 (0.341, t = 4.475, p < 0.001)로 긍정적 영향을 미치는 것으로 나타나 가설 6은 채택되었다. 가설 검정 결과는 <표 10>에 정리한 바와 같다.

5.2.4 확률적 거리감의 조절효과 분석

확률적 거리감의 조절효과를 확인하기 위해 집단비교 접근방법인 다중집단분석(MGA: Multi Group Analysis)을 실시하였다. 각 집단은 경로의 복잡성과 구성개념들의 최소 R^2 값을 충족시키는 Cohen(1992)의 통계적 검증력 수준(power level)을 적용했을 때 유의확률 5%에서 R^2 값 0.25정도를 목표로 검증력 수준 80%의 엄격한 기준에 대한 최소 표본크기 요구량을 확보하였기에 검증에 무리가 없다.

조절효과의 유의성 검증에 있어 t검증을 통해 두 집단 경로계수의 유의적 차이를 확인하는 방법이 일반적이다. 그러나 PLS-SEM을 사용한 집단 간 경로계수의 차이 비교를 모수적방법으로 수행하는 것은 자료 분포에 대한 자유로운 가정을 전제하는 PLS-SEM의 특성과 맞지 않다(Hair *et al.*, 2014; Rigdon *et al.*, 2010). 따라서 중심화된 부트스트랩 추정치(centered bootstrap estimate)를 사용하여 비모수적 절차를 실행하는 Henseler(2012)의 제안을 적용하여 확률적 거리감이 다른 집단 사이의 영향력 차이를 검증하였다.

가설검정 결과 채택된 관계를 대상으로 분석한 결과는 <표 11>과 같다. 두 집단 계수의 차이를 나타내는 확률(P)은 집단의 차이에 대한 오류확률을 나타낸다. 정보보호 침해사고의 발생확률이 낮은 집단(L)의 경로계수가 높은 집단(H)의 경로계수보다 크다고 할 오류확률은 상대적 낙관성과 지각된 위험의 관계에서 1.7%, 지각된 위험과 행동



〈그림 4〉 구조모형 분석 결과

〈표 10〉 가설 검정 결과

가설	모형의 경로	경로계수	t값	p값	유의수준	채택여부
H4	상대적 낙관성 1 → 지각된 위험	-0.194	1.932	0.027	0.050	채택
H5	상대적 낙관성 2 → 지각된 위험	0.005	0.043	0.483	-	기각
H6	지각된 위험 → 행동의도	0.341	4.475	0.000	0.001	채택

〈표 11〉 확률적 거리감의 조절효과 분석결과

경로	정보보호 침해사고 확률 높음(H) (N = 61)			정보보호 침해사고 확률 낮음(L) (N = 65)			집단 차이 오류 확률 (P)	조절 효과 (p<0.05)
	경로 계수	표준 편차	t(p)	경로 계수	표준 편차	t(p)		
상대적 낙관성 1 → 지각된 위험	0.159	0.252	0.630 (0.266)	-0.500	0.180	2.783 (0.004)	0.017	있음
지각된 위험 → 행동의도	0.251	0.283	0.886 (0.190)	0.484	0.139	3.484 (0.001)	0.604	없음

의도의 관계에서는 60.4%로 나타났다. 따라서 5% 유의수준에서 상대적 낙관성과 지각된 정보보호 위험의 관계에 확률적 거리감 집단에 의한 유의한 조절효과가 있는 것으로 나타났으나 지각된 정보보호 위험과 정보보호 행동의도의 관계에는 통계적으로 유의한 영향력의 차이가 없었다.

5.2.5 지각된 위험의 매개효과 분석

가설검증 결과를 바탕으로 상대적 낙관성과 정보보호 행동의도의 관계에서 지각된 위험의 매개역할에 대한 추가검증을 실시하였다. 매개효과의 분석은 회귀분석과 구조방정식모델 모두에서 가능하나 표본크기와 측정항목을 고려해서 결정할 수 있다(배병렬, 2015). 본 연구의 경우 표본크기가 200개 미만이고 단일측정항목을 포함하므로 회귀분석을 이용하는 것이 적합한 것으로 판단하였다. 부트스트랩을 기반한 Hayes(2013)의 분석법을 이용하여 매개효과를 분석한 결과는 <표 12>와 같으며 간접효과(0.101)의 신뢰구간(0.010~0.240)이 0보다 크게 나타났다. 즉, 상대적 낙관성과 정보보호 행동의도의 관계에서 매개효과는 있으나 직접효과는 없는 간접매개(indirect-only mediation)의 역할을 확인하였다.

Ⅵ. 결 론

본 연구는 모바일기기 사용자의 정보보호 의사결정에 심리적 거리감과 상대적 낙관성이 어떤 역할을 하는지 살펴보고자 하였다. 연구의 목적을 달성하기 위해 단계별로 적용가능성을 점검하고 다양한 기술적 연구방법을 구현하는 다중기법 단계적 접근방법을 적용하였다. 먼저 모바일기기 사용자의 정보보호 인식과 행동에 대한 분석을 실시하여 정보보호 인식에 차이가 없음을 확인하였다. 다음으로 실험적 통제와 프레이밍효과를 적용하여 연구의 관심요소인 심리적 요인을 관찰하였다. 실험결과를 바탕으로 관심요소를 개념화하고 연구모형을 설정한 후 통계적 검정을 실시하였다.

〈표 12〉 지각된 위험의 매개효과 분석 결과

구 분	경로 계수	표준편차	t	p	신뢰구간	
					하한	상한
상대적 낙관성 1 → 지각된 위험(a)	0.300	0.120	2.497	0.014	0.062	0.538
지각된 위험 → 행동의도(b)	0.336	0.095	3.548	0.001	0.148	0.524
상대적 낙관성 1 → 행동의도(c´)	-0.190	0.118	-1.613	0.110	-0.424	0.044
총 효과(c)	-0.089	0.121	-0.739	0.462	-0.329	0.150
직접효과	-0.190	0.118	-1.613	0.110	-0.424	0.044
간접효과(a×b)	0.101	0.058			0.010	0.240

본 연구의 결과는 다음과 같다. 첫째, 모바일기기 사용자의 확률적 거리감에 따라 정보보호 위험의 지각과 보호조치에 대한 의사결정에 차이가 있는지를 확인하였다. 자신에게 사이버 침해 사고가 발생할 가능성을 높게 인식한 집단이 발생 가능성이 낮은 집단보다 정보보호 위험을 높이 평가하였으나 정보보호를 위한 조치를 취할지에 대해서는 발생 가능성에 따른 차이가 없는 것으로 나타났다. 정보보호에 대한 일반적 인식 수준에 차이가 없는 두 집단에서 사이버 침해 사고가 발생할 가능성만을 높거나 낮게 인식시킨 후 얻어진 이러한 결과는 자신이 처할 수 있는 사이버 침해 사고의 발생확률이 모바일기기 사용자의 위험 지각에 실질적으로 영향을 미친다는 것을 보여주었다.

둘째, 상대적 낙관성의 정도가 사회적 거리감에 따라 달라진다는 것을 확인했다. 자신과 가까운 사람보다 자신과 관계가 없는 사람들과 비교했을 때 상대적으로 더 낙관적으로 생각하는 것이다. 사회적 거리에 따른 낙관편향은 기존의 연구에서도 확인할 수 있으나 비교상대가 누구인지에 따라 상대적 발생가능성을 다르게 인식한다는 것은 정보보호의 측면에서 의미 있는 결과이다.

셋째, 상대적 낙관성과 정보보호 행동의도의 관계에서 자신과 가까운 사람과 비교했을 때 정보보호 위험의 수준을 낮추는 것으로 나타났다. 앞서 결과에서는 비교 상대와의 사회적 거리감이 먼 경우 상대적 낙관성이 높아지는 것으로 나타났다. 그러나 실제로 자신의 위험수준을 평가할 때는 사회적 거리감이 가까운 주변사람과 비교한 결과가 영향을 미쳤다. 이러한 결과는 심리적 거리에 따른 해석수준이 작용한 것으로 판단된다. 사회적 거리가 가까우면 하위수준의 해석이 이루어져 단점이 부각되고 구체적인 사고가 이루어지므로 사회적 거리가 먼 경우보다 위험의 평가에 직접적인 영향을 미치는 것이다.

넷째, 가까운 사람과 비교한 상대적 낙관성이 정보보호 위험을 낮추는데 있어 확률적 거리감에 따라 영향력이 달라짐을 확인했다. 확률적 거리감이 먼 경우 즉, 정보보호 침해사고의 확률이 낮을 때 상대적 낙관성이 정보보호 위험을 더 낮게 평가하며 이는 확률이 낮은 위험일 때 더 커지는 낙관주의 특성(Weinstein, 1987)이 반영된 것으로 보인다.

본 연구의 시사점은 다음과 같다. 첫째, 방법론적 측면에서 의미 있는 시도를 하였다. 정보보호 분야에서 실험 연구의 수행은 현실적으로 어려움이 있다. 그럼에도 불구하고 정보보호의 위험지각과 행동의도에 대한 심리적 거리감과 낙관편향의 영향을 실험을 통해 규명하고자 하였다. 또한 다중기법 단계적 접근방법을 적용함으로써 연구의 목적을 달성하기 위한 과정의 신뢰성을 높이고자 하였다.

둘째, 정보보호와 관련한 심리적 요인의 역할을 확인함으로써 정보보호를 위한 의사결정 과정에 대한 다양한 접근이 필요함을 실증적으로 규명하였다. 정보보호에 대한 자신의 인식수준과 상관없이 타인과 비교한 상대적 낙관성이 자신이 지각하는 위험의 정도에 영향을 미치고, 자신에게 발생할 가능성에 따라 영향력이 달라져 정보보호를 위한 실천 여부가 달라질 수 있다. 이는 인지가 행동으로 이어진다는 기존의 단순한 이론으로 설명할 수 없는 중요한 결과이다. 즉, 모바일기기 사용자가 정보보호의 중요성이나 필요성을 높이 인식하더라도 행동에 이르는 과정의 심리적 영향을 심각하게 고려해야 한다는 것을 증명한 것이다. 지금까지 많은 연구들에서는 정보보호를 위해 인식을 높이는 것에 초점을 맞췄다. 그러나 정보보호 인식과 행동 사이의 과정에 심리적 요인에 관심을 두어야 할 충분한 이유가 있음을 본 연구의 결과가 설명하고 있다. 인식을 높이기 위한 일방적인 정보보호 지식의 전달보다 정보보호의 실천을 위한 더욱 현실적이고 효과적인 방안이 모바일기기 사용자에게 필요할 것이다.

셋째, 실질적 위험지각에 영향을 미치는 상대적 낙관성의 범위를 좁혔다는 데 실무적 의의가 있다. 개인의 위험 지각에 있어 낙관편향은 위험

을 감소시키기 위한 노력을 심각하게 방해할 수 있기 때문에 중요한 문제이다(Weinstein, 1989). 자신의 상태를 낙관적으로 판단하여 위험한 상태나 상황을 극복하려는 적극적 행동에 대한 의도가 낮아지기 때문이다. 사회적 거리감이 먼 경우 낙관편향이 더 큰 것은 다수의 연구에서 밝히고 있으나 본 연구에서는 가까운 사회적 거리감에서 발생하는 낙관편향이 실질적 위험 지각에 영향을 미치며 이는 막연한 위험평가 과정의 인지적 오류가 아닌 심리적 해석에 의한 근거 있는 현상임을 밝혔다. 이러한 결과는 정보보호 분야의 교육 및 정책의 수립을 비롯한 다양한 분야에 적용할 수 있을 것이다. 이로써 다양하고 심각해지는 사이버 위험으로부터 정보기술 사용자의 정보자산을 지키고 정보보호 수준을 높일 것으로 기대한다.

본 연구의 한계점은 다음과 같다. 첫째, 전체 실험참가자에 비해 처치점검 후 최종 분석대상이 약 60%에 그쳤다. 이는 실험의 설계에 미흡한 점이 있을 수 있을 것으로 짐작되므로 향후 실험적 통제를 보완한 연구로 확장시킬 수 있을 것이다. 둘째, 표본의 수가 충분하지 않아 인과관계 검증에 부족함이 있다. 표본 수를 늘려 통계적 검증을 보완함으로써 연구결과의 의의를 높일 수 있을 것이다.

참 고 문 헌

[1] 김민지, 민병아, 신현식, 황성욱, 이인성, 김진우, “해석수준 이론에 기반한 모바일 기부 플랫폼 사례연구: 빅워크와 트리플래닛을 대상으로”, *Information Systems Review*, 제17권, 제3호, 2015, pp. 135-157.

[2] 김종기, 김지윤, “컴퓨터 사용자의 데이터 백업의도에 영향을 미치는 요인”, *연세경영연구*, 제54권, 제3호, 2017, pp. 77-106.

[3] 박도형, “심리적 거리로서의 가상성: 가상성에 따른 광고메시지 전략”, *Journal of Information Technology Applications & Management*, 제24권, 제2호, 2017, pp. 39-54.

[4] 박정현, 강성민, “사용자의 PC와 스마트폰에 대한 정보보안 인식 차이에 관한 연구”, *Information Systems Review*, 제19권, 제3호, 2017, pp. 69-89.

[5] 배병렬, *SPSS Amos LISREL SmartPLS에 의한 조절효과 및 매개효과분석*, 청람, 서울, 2015.

[6] 한국인터넷진흥원, *2016년 정보보호 실태조사*, 2017.

[7] 한국인터넷진흥원, *2017년 정보보호 실태조사*, 2018.

[8] Anderson, C. L. and R. Agarwal, “Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions”, *MIS Quarterly*, Vol.34, No.3, 2010, pp. 613-643.

[9] Bauer, R. A., “Consumer behavior as risk taking”, *Risk Taking and Information Handling in Consumer Behavior*, Harvard University Press, Cambridge, MA, 1960.

[10] Bauer, S. and E. W. Bernroider, “From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization”, *The DATABASE for Advances in Information Systems*, Vol.48, No.3, 2017, pp. 44-68.

[11] Boss, S. R., D. F. Galletta, P. B. Lowry, G. D. Moody, and P. Polak, “What do system users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors”, *MIS Quarterly*, Vol.39, No.4, 2015, pp. 837-864.

[12] Bulgurcu, B., H. Cavusoglu, and I. Benbasat, “Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness”, *MIS Quarterly*, Vol.34, No.3, 2010, pp. 523-548.

[13] Chen, C. C., B. Dawn Medlin, and R. S. Shaw,

"A cross-cultural investigation of situational information security awareness programs", *Information Management & Computer Security*, Vol.16, No.4, 2008, pp. 360-376.

[14] Cho, H., J. S. Lee, and S. Chung, "Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience", *Computers in Human Behavior*, Vol.26, No.5, 2010, pp. 987-995.

[15] Cohen, J., "A power primer", *Psychological Bulletin*, Vol.112, No.1, 1992, pp. 155-159.

[16] Featherman, M. S. and P. A. Pavlou, "Predicting e-services adoption: A perceived risk facets perspective", *International Jurnal of Human-Computer Studies*, Vol.59, No.4, 2003, pp. 451-474.

[17] Feng, Y., P. Wu, G. Ye, and D. Zhao, "Risk-Compensation behaviors on construction sites: Demographic and psychological determinants", *Journal of Management in Engineering*, Vol.33, No.4, 2017, pp. 1-10.

[18] Floyd, D. L., S. Prentice-Dunn, and R. W. Rogers, "A meta-analysis of research on protection motivation theory", *Journal of Applied Social Psychology*, Vol.30, No.2, 2000, pp. 407-429.

[19] Freitas, A. L., P. Gollwitzer, and Y. Trope, "The influence of abstract and concrete mindsets on anticipating and guiding others' self-regulatory efforts", *Journal of Experimental Social Psychology*, Vol.40, No.6, 2004, pp. 739-752.

[20] Guo, K. H., Y. Yuan, N. P. Archer, and C. E. Connelly, "Understanding nonmalicious security violations in the workplace: A composite behavior model", *Journal of Management Information Systems*, Vol.28, No.2, 2011, pp. 203-236.

[21] Hair, J. F., G. T. M. Hult, C. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, Sage Publications, 2014, (PLS 구조모델의 이해: BASIC, 김장현, 심경환, 이철성 옮김, 피앤씨미디어, 2014).

[22] Harris, P. and W. Middleton, "The illusion of control and optimism about health: On being less at risk but no more in control than others", *British Journal of Social Psychology*, Vol.33, No.4, 1994, pp. 369-386.

[23] Hayes, *Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach*, The Guilford Press, 2013.

[24] Henseler, J., "PLS-MGA: A non-parametric approach to partial least squares-based multi-group analysis", *Challenges at The Interface of Data Analysis, Computer Science, and Optimization*, Springer, 2012, pp. 495-501.

[25] ISO/IEC 27000, *Information Technology-Security Techniques-Information Security Management Systems-Overview and Vocabulary*, International Organization for Standardization, 2016.

[26] Kim, K. K., B. Prabhakar, and S. K. Park, "Trust, perceived risk, and trusting behavior in Internet banking", *Asia Pacific Journal of Information Systems*, Vol.19, No.3, 2009, pp. 1-23.

[27] Kirk, R. E., *Experimental Design: Procedures for the Behavioral Sciences (4th ed.)*, Sage, 2014.

[28] Lazarus, R. S. and S. Folkman, *Stress, Appraisal, and Coping*, Springer, 1984, (스트레스와 평가 그리고 대처, 김정희 옮김, 대광문화사, 2001).

[29] Liberman, N., Y. Trope, and E. Stephan, "Psychological Distance", *Social Psychology: Handbook of Basic Principles*, 2007, pp. 353-383.

[30] Luo, X., H. Li, J. Zhang, and J. P. Shim, "Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services", *Decision Support Systems*, Vol.49, No.2, 2010, pp. 222-234.

[31] Maglio, S. J., Y. Trope, and N. Liberman, “Distance from a distance: Psychological distance reduces sensitivity to any further psychological distance”, *Journal of Experimental Psychology*, Vol.142, No.3, 2013, pp. 644-657.

[32] Marett, K., “Checking the manipulation checks in information security research”, *Information & Computer Security*, Vol.23, No.1, 2015, pp. 20-30.

[33] Mingers, J., “Combining IS research methods: Towards a pluralist methodology”, *Information Systems Research*, Vol.12, No.3, 2001, pp. 240-259.

[34] Otten, W. and J. Van der Pligt, “Risk and behavior: The mediating role of risk appraisal”, *Acta Psychologica*, Vol.80, No.1, 1992, pp. 325-346.

[35] Park, J. and C. G. Oh, “Cognitive bias and information security research: Research trends and opportunities”, *Asia Pacific Journal of Information Systems*, Vol.26, No.2, 2016, pp. 290-298.

[36] Park, R. E., “The concept of social distance as applied to the study of racial attitudes and racial relations”, *Journal of Applied Sociology*, Vol.8, No.6, 1924, pp. 339-344.

[37] Rhee, H. S., Y. U. Ryu, and C. T. Kim, “Unrealistic optimism on information security management”, *Computers & Security*, Vol.31, No.2, 2012, pp. 221-232.

[38] Rigdon, E. E., C. M. Ringle, and M. Sarstedt, “Structural modeling of heterogeneous data with partial least squares”, *Review of Marketing Research*, Emerald Group Publishing Limited, 2010, pp. 255-296.

[39] Rosemann, M. and I. Vessey, “Toward improving the relevance of information systems research to practice: The role of applicability checks”, *MIS Quarterly*, Vol.32, No.1, 2008, pp. 1-22.

[40] Rossiter, J. R., “Marketing measurement revolution: The C-OAR-SE method and why it must replace psychometrics”, *European Journal of Marketing*, Vol.45, No.11, 2011, pp. 1561-1588.

[41] Sitkin, S. B. and A. L. Pablo, “Reconceptualizing the determinants of risk behavior”, *Academy of Management Review*, Vol.17, No.1, 1992, pp. 9-38.

[42] Todorov, A., A. Goren, and Y. Trope, “Probability as a psychological distance: Construal and preferences”, *Journal of Experimental Social Psychology*, Vol.43, No.3, 2007, pp. 473-482.

[43] Trope, Y. and N. Liberman, “Construal-level theory of psychological distance”, *Psychological Review*, Vol.117, No.2, 2010, pp. 440-463.

[44] Trope, Y., N. Liberman, and C. Wakslak, “Construal levels and psychological distance: Effects on representation, prediction, evaluation, and behavior”, *Journal of Consumer Psychology*, Vol.17, No.2, 2007, pp. 83-95.

[45] Tu, Z., O. Turel, Y. Yuan, and N. Archer, “Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination”, *Information & Management*, Vol.52, No.4, 2015, pp. 506-517.

[46] Van Schaik, P., J. Jansen, J. Onibokun, J. Camp, and P. Kusev, “Security and privacy in online social networking: Risk perceptions and precautionary behaviour”, *Computers in Human Behavior*, Vol.78, 2018, pp. 283-297.

[47] Weinstein, N. D., “Optimistic biases about personal risks”, *Science*, Vol.246, No.4935, 1989, pp. 1232-1234.

[48] Weinstein, N. D., “Unrealistic optimism about future life events”, *Journal of Personality and Social Psychology*, Vol.39, No.5, 1980, pp. 806-820.

[49] Weinstein, N. D., “Unrealistic optimism about susceptibility to health problems: Conclusions from a community-wide sample”, *Journal of*

Behavioral Medicine, Vol.10, No.5, 1987, pp. 481-500.

[50] Weinstein, N. D. and W. M. Klein, “Unrealistic Optimism: Present and Future”, *Journal of Social and Clinical Psychology*, Vol.15, No.1, 1996, pp. 1-8.

[51] Wottrich, V. M., E. A. van Reijmersdal, and E. G. Smit, “The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns”, *Decision Support Systems*, Vol.106, No.1, 2017, pp. 44-52.

[52] Xu, H., H. Wang, and H. H. Teo, “Predicting the usage of P2P sharing software: The role of trust and perceived risk”, *Proceedings of the 38th Hawaii International Conference*, System Sciences, 2005, pp. 1-10.

Information Systems Review
Volume 20 Number 3
September 2018

The Role of Psychological Distance and Relative Optimism in Information Security Decision Making

Jongki Kim* · Jiyun Kim**

Abstract

Many studies in the field of information security reveal the need to increase awareness. However, although awareness of information security has been raised to a considerable extent, actual security behavior has been shown to fall short of that. Therefore, we wanted to identify the role of psychological factors in making information security decisions by conducting a experimental study.

The results show that there are differences in perception of information security risks according to the probabilistic distance and the degree of relative optimism due to social distance. In relation to their relative optimism and intention of information security, they reduced the level of perceived risk compared to those close to them and found that their influence varied according to their probabilistic distance.

This study has made valuable attempt in terms of methodology and it is meaningful that the psychological factor is taken into consideration for the information protection behavior, so that the range of relative optimism that actually affects the perception of risk is narrowed. It is expected to contribute to the improvement of information security level of information technology users and protection of information assets by empirically identifying necessity of various approaches to decision making process for information security.

Keywords: Information Security, Relative Optimism, Optimistic Bias, Psychological Distance, Social Distance, Hypothetical Distance

* Professor, Department of Business Administration, Pusan National University
** Corresponding Author, Doctoral Student, Graduate School, Pusan National University

◐ 저 자 소 개 ◑

김 종 기 (jkkim1@pusan.ac.kr)

부산대학교 경영학과에서 학사를 마쳤으며, 미국 Arkansas State University에서 경영학 석사학위, Mississippi State University에서 경영학 박사학위를 취득하였다. 현재 부산대학교 경영학과 경영정보전공 교수로 재직 중이다. 주요 연구 관심분야는 정보보안관리, 프라이버시, 전자상거래, 기술경영, 행동경제학 등이다.

김 지 윤 (wowtnt@pusan.ac.kr)

부산대학교 경영학과에서 박사과정을 수료하였다. 주요 연구 관심분야는 정보보안, 행동경제학, 위험분석 등이다.

논문접수일 : 2018년 07월 20일 **게재확정일 : 2018년 09월 21일**
1차 수정일 : 2018년 09월 17일