「정보시스템연구」 제25권 제3호
한국정보시스템학회
2016년 9월, pp. 197~215

http://dx.doi.org/10.5859/KAIS.2016.25.3.197

온라인 환경에서 프라이버시 의사결정에 영향을 미치는 요인에 관한 연구: 이중계산모델을 중심으로

김 상 희* · 김 종 기**

〈목 차〉

Ⅰ. 서 론

최근 국내에서는 전자상거래 사이트를 비롯하여 은행이나 카드사와 같은 금융기업 사이트까지 해킹되는 등 대규모의 개인정보가 유출되는 사건이 잇따라 발생하고 있다. 이러한 사건들로 인해 개인정보가 직접적으로 드러나는 경우를 제외하고도 각종 스팸메일이나 보이스피싱과 같이 개인정보의 유출이 간접적으로 드러나는 경우가 매우 빈번하게 발생하고 있어 심각한 사회적 문제로 부각되고 있다(김영렬, 2010).

이에 따라 온라인 환경에 제공한 개인정보에 대한 소비자의 염려가 극에 달해 있지만, 그럼에도 불구하고 온라인상에서 특정 사이트에 가입하거나 서비스를 이용하기 위해서는 개인정보를 제공해야 하는 상황이다. 이처럼 외부의 환경으로 인해 소비자의 프라이버시에 대한 염려가 높아져 있는 상황에서 소비자가 개인정보 제공과 관련된 의사결정을 할 때 어떠한 요인이 중요한 역할을 하는지 파악해볼 필요가 있다.

프라이버시 연구에서는 소비자의 프라이버시 의사결정을 이해하기 위한 대표적인 이론적 기반으로 프라이버시 계산이 존재한다. 프라이버시 계산 이론은 개인이 정보제공과 관련된

* 부산대학교 경영연구소 박사후연구원, ksh@pusan.ac.kr
** 부산대학교 경영학과 교수, jkkim1@pusan.ac.kr, 교신저자

의사결정 시 '위험-이익 분석'을 수행하는 것을 의미하며, 개인정보를 제공하기 전에 그로 인해 발생되는 이익과 위험을 평가하여 이익이 위험보다 크다면 정보제공을 하게 된다는 것을 설명한다. 지금까지 프라이버시 계산 이론은 다수의 연구자들에 의해 프라이버시 의사결정 과정을 설명하기 위해 적용되어 오고 있다.

한편, 그동안 프라이버시 분야에서 수행되어 온 연구들의 포괄적인 이해를 위해 통합연구를 실시한 Li(2012)의 연구에서는 정보제공행동을 설명하기 위한 대표적인 이론인 이익과 위험의 상충관계를 나타내는 프라이버시 계산(Privacy Calculus)과 프라이버시에 대한 외부의 위협과 대처 메커니즘의 상충관계를 나타내는 위험 계산(Risk Calculus)을 통합하여 이중계산모델(Dual-Calculus Model)을 제안하고 있다. 프라이버시 계산의 위험 요인은 외부의 위협에 대한 개인의 평가와 그 위협에 대처할 수 있는 능력에 대한 개인의 평가에 의해 결정된다고 보며, 이는 보호동기이론(Protection Motivation Theory)을 기반으로 한다.

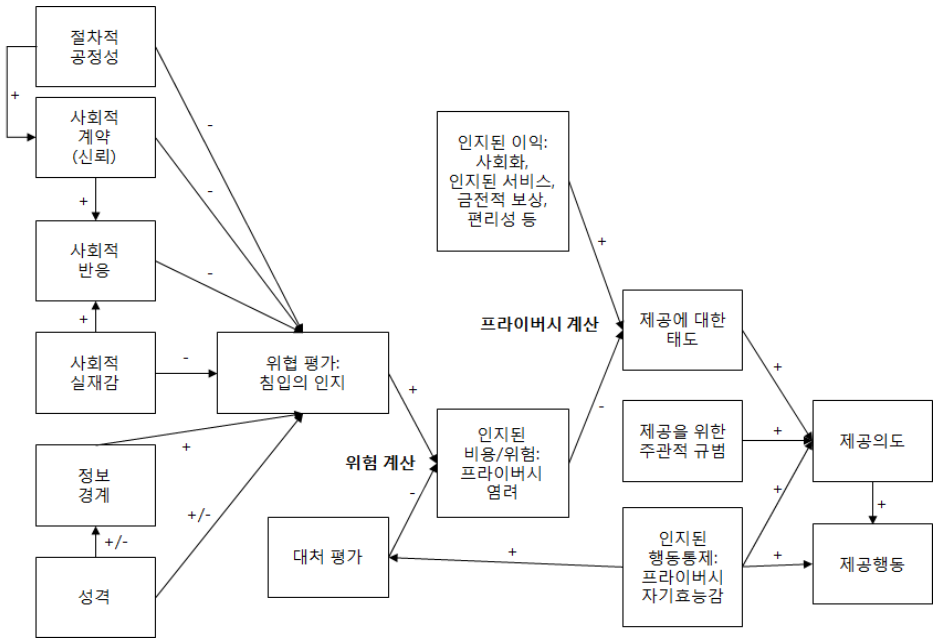
본 연구에서는 외부의 환경으로 인해 소비자들의 프라이버시 염려가 극에 달해 있는 상황에서 온라인 환경에서 소비자가 개인정보 제공과 관련된 의사결정에 영향을 미치는 요인을 Li(2012)가 제시한 이중계산모델에 근거하여 프라이버시 계산 이론과 보호동기이론을 통합하는 관점에서 규명하고자 한다. 프라이버시 계산 이론과 보호동기이론은 프라이버시 행동을 설명하기 위해 다소 적용되어 왔으나, 두 이론을 통합하여 설명하기 위해 시도한 연구는 찾아보기 어렵다. Li(2012)의 연구에서는 이를 이중계산모델로 제안하고 있지만 프레임워크만 제시할 뿐 실증연구는 이루어지지 않았다. 본 연구에서는 두 이론을 통합하는 관점에서 연구모형을 제안하고 실증연구를 통해 이들의 관계에 대해 검증하고자 한다.

Ⅱ. 이중계산모델

Li(2012)의 연구에서는 기존의 프라이버시 연구들을 수집하여 통합연구를 수행하여 최종적으로 개인의 프라이버시 의사결정에 영향을 미치는 요인을 두 가지 상충관계(Trade-Off)를 중심으로 설명하는 통합적 프레임워크를 제시하고 있다. 첫째는 프라이버시 이익과 프라이버시 위험 간의 상충관계를 나타내는 프라이버시 계산이고, 둘째는 프라이버시에 대한 외부의 위협과 대처 메커니즘인 효능감 간의 상충관계를 나타내는 위험 계산이다. 이러한 두 가지 상충관계는 밀접하게 연관되어 있으며, Li(2012)는 이들을 통합한 이중계산모델을 제안하고 있다. 이중계산모델에서 제시하는 프라이버시 계산은 프라이버시 계산 이론에 의해, 위험 계산은 보호동기이론에 의해 설명되고 있다.

2.1. 프라이버시 계산 이론

프라이버시 계산 이론은 기대가치이론을 기반으로 소비자의 정보제공과 관련된 의사결정을 이해하기 위해 Stone and Stone(1990)의 연구에서 최초로 제시되었다. 프라이버시 계산 이론에 따르면, 소비자가 정보를 제공할 것인지 여부를 결정하기에 앞서 정보제공을 함으로써 발생하는 이익과 위험을 평가하여 이익이 위



<그림 1> Li(2012)의 통합적 프레임워크

험보다 크거나 최소한 균형을 이룬다고 판단될 때 정보를 제공하게 된다(Culnan & Bies, 2003; Dinev & Hart, 2006). 즉, 소비자가 기업으로부터 개인정보 제공을 요구받았을 때 자신의 개인정보를 제공함으로써 발생되는 이익과 위험에 대한 프라이버시 계산을 수행하는 과정을 거쳐 정보제공여부와 관련된 행동을 결정하게 된다는 것을 설명하고 있다. 이때, 프라이버시 계산 이론에서 사용되는 '계산'이라는 용어는 경제학에서 사용되는 수치적인 값의 분석을 의미하는 것이 아니라 개인의 인지적 평가에 의한 상충관계를 강조하기 위해 사용되고 있다(Keith et al., 2013).

그동안 프라이버시 계산 이론을 적용한 선행연구들을 보면, 대체적으로 프라이버시 이익과 프라이버시 위험을 중심으로 정보제공과 관련된 의사결정을 설명하고자 한다. 프라이버시 계산의 주요 요인인 프라이버시 이익과 프라이버시 위험을 단일차원 구성개념으로 측정하는 연구(Xu et al., 2010; Li et al., 2011; Xu et al., 2011)와 다차원 구성개념으로 측정하는 연구(Krasnova & Veltri, 2010; Li et al., 2010; 김종기·김상희, 2012)가 존재한다. 프라이버시 계산의 선행요인은 다양한 형태로 나타나지만, 결과요인은 대부분 정보제공과 관련된 행동의도로 설정되어 있다. 기존 연구의 구체적인 구성개념은 <표 1>에 나타나 있다.

<표 1> 프라이버시 계산 관련 선행연구

연구자	연구분야	선행요인	프라이버시 계산	결과요인
Krasnova and Veltri (2010)	소셜 네트워크 사이트	• 신뢰	• 이익(즐거움, 자기표현, 관계유지) • 프라이버시 비용(인지된 가능성, 인지된 피해, 프라이버시 염려)	• 자기노출
Li et al. (2010)	온라인 정보제공	-	• 교환 이익(인지된 유용성, 금전적 보상) • 프라이버시 관련 비용(프라이버시 보호 신념, 프라이버시 위험 신념)	• 행동의도
Xu et al. (2010)	위치기반 서비스	• 프라이버시 관련 개입(보상, 산업자율규제, 정부규제)	• 프라이버시 이익 • 프라이버시 위험	• 개인정보제공의도
Li et al. (2011)	온라인 정보제공	• 감정(기쁨, 두려움) • 공정성 수단(정보의 인지된 적합성, 프라이버시 준수의 인식) • 프라이버시 염려	• 프라이버시 보호신념 • 프라이버시 위험신념	• 행동의도
Xu et al. (2011)	위치감지 마케팅	• 개인화 • 개인간 차이(이전 프라이버시 경험, 쿠폰이용성향)	• 정보제공의 인지된 이익 • 정보제공의 인지된 위험	• 정보제공의 인지된 가치 • 개인정보제공의도 • 구매의도
김종기와 김상희 (2012)	위치기반 서비스	• 프라이버시 염려	• 프라이버시 이익(편리성, 정보유용성, 개인화, 위치확인성) • 프라이버시 위험	• 인지된 가치 • 정보제공의도

2.2. 보호동기이론

Roger(1975)에 의해 제시된 보호동기이론은 다양한 분야에서 공포소구(Fear Appeal)에 의한 개인의 행동변화를 설명하고자 발전되어왔다. 보호동기이론에 따르면, 보호동기는 위협평가(Threat Appraisal)와 대처평가(Coping Appraisal)라는 개인의 인지적 평가에 의해 형성된다. 먼저, 위협평가는 외부에서 발생되는 위협적인 사건에 대한 개인의 평가로, 발생가능성(Susceptibility)과 심각성(Severity)으로 구성된다. 발생가능성은 위협적인 사건이 발생할 수 있는 가능성 정도를 의미하고, 심각성은 위협적인 사건이 발생하였을 때 그에 따른 문제가 심각한 정도를 의미한다.

다음으로, 대처평가는 위협적인 사건을 대처하는 능력에 대한 개인의 평가로, 반응효능감(Response Efficacy)과 자기효능감(Self-Efficacy)으로 구성된다. 반응효능감은 위협적인 사건에 대해 대처행동을 이행하였을 때 기대되는 능력에 대한 평가를 의미하고, 자기효능감은 위협적인 사건에 대해 대처할 수 있는 자신의 능력에 대한 평가를 의미한다. 이처럼 위협평가와 대처평가라는 인지적 매개과정을 통

해 보호동기를 조절하게 되고, 최종적으로 행동의 변화를 가져온다는 것을 설명하고 있다 (Rogers, 1975, 1983; Li, 2012).

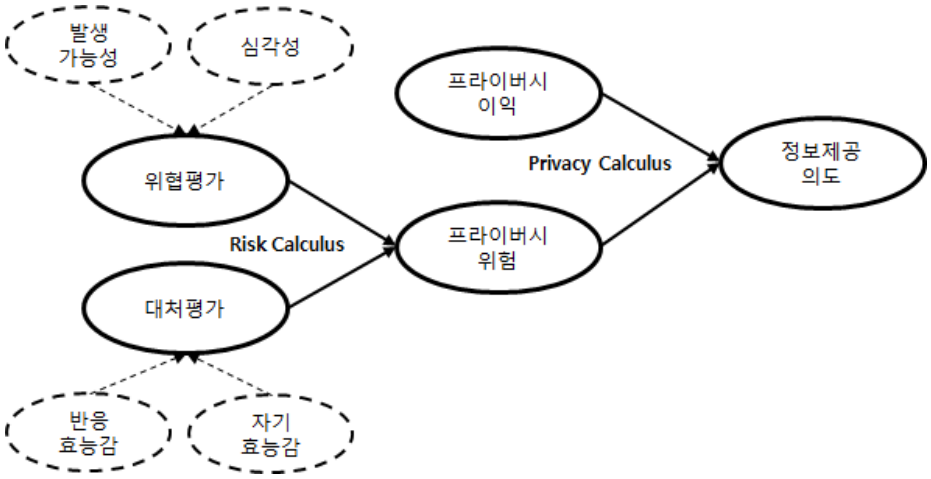
최초의 보호동기이론은 보건학에서 외부의 위협적인 메시지에 대한 보호행동의 변화를 설명하기 위해 연구가 시작되었다. 이후 위협에 대한 보호행동을 규명하고자 하는 다양한 분야의 연구로 확장되어 적용되었으며, 최근에는 정보시스템 분야에서도 정보시스템 보안행동 (Workman et al., 2009; Johnston & Warkentin, 2010; Liang & Xue, 2010) 또는 프라이버시 보호행동(Li., 2012; 김종기·김상희, 2012; 김상현·박현선, 2013)을 설명하기 위해 적용되고 있다.

Li(2012)가 제시한 이중계산모델에 따르면, 프라이버시 계산의 위험 요인은 보호동기이론에 의해 그 상충관계가 설명될 수 있다. 보호동기이론의 주요 요인인 위협평가와 대처평가로 인해 소비자가 인지하는 프라이버시 위험의 수준이 결정될 수 있다는 것이다. 소비자가 자신이 인지하는 위협평가의 수준보다 그 위협에 대하여 대처하는 능력인 대처평가의 수준이 높으면 프라이버시 위험이 낮게 나타날 것이고, 반대로 위협평가의 수준에 비해 대처평가의 수준이 부응하지 못한다면 프라이버시 위험은 높게 나타날 것이다. 이러한 과정을 통해 프라이버시 계산의 요인인 프라이버시 위험의 수준이 결정되고, 이는 프라이버시 이익과의 상충관계, 즉 프라이버시 계산을 통해 최종적으로 정보제공과 관련된 행동이 결정된다고 본다.

Ⅲ. 연구모형과 연구가설

3.1. 연구모형

본 연구에서는 온라인 환경에서 소비자의 프라이버시 의사결정에 영향을 미치는 요인을 실증적으로 분석하고자 <그림 2>와 같은 연구모형을 설계하였다. Li(2012)가 제시한 이중계산모델을 기반으로 크게 프라이버시 계산과 위험



<그림 2> 연구모형

계산으로 구분하고 이들의 관계를 규명하고자 한다. 먼저, 프라이버시 계산 이론에 따라 프라이버시 이익과 프라이버시 위험이 정보제공의도에 미치는 영향에 대해 살펴보고자 한다. 다음으로, 보호동기이론의 주요 요인인 위협평가와 대처평가가 프라이버시 계산에 있어 프라이버시 위험에 어떠한 영향을 미치는지 파악하고자 한다. 이때, 위협평가와 대처평가는 발생가능성과 심각성, 반응효능감과 자기효능감에 대한 2차 요인(Second-Order Factor)으로 구성하였다.

3.2. 연구가설

3.2.1. 프라이버시 계산 이론

Smith et al.(2011)의 프라이버시 관점의 분류에 따르면, 소비자들이 자발적으로 개인정보를 제공하는 현상을 설명하기 위해 프라이버시를 경제적 구성요소로 인식하는 상품으로서 프라이버시 관점이 존재한다. 이는 프라이버시를 개인정보를 제공하는 대가로 얻을 수 있는 이익, 즉 교환가능한 상품으로서 보는 관점으로, 프라이버시 계산 이론은 이에 해당한다.

프라이버시 계산 이론은 경제적 관점에서 언급되는 위험-이익 분석을 기반으로 이들의 상충관계를 추정함으로써 소비자가 개인정보를 제공할지 여부를 판단하게 된다는 현상을 설명한다. 프라이버시 계산 과정을 통해 개인정보를 제공함에 따른 이익과 위험을 비교하여 이익이 위험보다 크거나 적어도 균형을 이룬다고 평가할 때 소비자는 개인정보를 제공하게 된다는 것이다.

프라이버시 계산 이론에 근거하여 소비자의 정보제공과 관련된 행동을 규명하기 위해 다수의 연구들이 수행되어 왔다. 기존의 연구를 종합해보면, 프라이버시 이익과 프라이버시 위험을 단일차원 구성개념으로 측정한 연구(Xu et al., 2010; Li et al., 2011)와 다차원 구성개념으로 측정한 연구(Krasnova & Veltri, 2010; Li et al., 2010)로 구분된다. 본 연구에서는 프라이버시 이익을 온라인 환경에서 소비자가 개인정보를 제공함으로써 얻을 수 있는 혜택 정도로, 프라이버시 위험을 개인정보를 제공함으로써 기대되는 잠재적인 손실 정도로 정의하고, 이들을 단일차원 구성개념으로 구성하였다. 따라서 온라인 환경에서 소비자가 인지하는 프라이버시 이익이 높을수록 개인정보를 제공하고자 하는 의도가 높아지고, 소비자가 인지하는 프라이버시 위험이 높을수록 개인정보를 제공하고자 하는 의도가 낮아진다는 가설을 설정하였다.

[가설 1] 프라이버시 이익은 정보제공의도에 긍정적인 영향을 미칠 것이다.

[가설 2] 프라이버시 위험은 정보제공의도에 부정적인 영향을 미칠 것이다.

3.2.2. 보호동기이론

본 연구에서는 프라이버시 위험에 영향을 미치는 요인인 위협평가와 대처평가를 2차 요인으로 설정하였다. Rogers(1975, 1983)의 연구를 기반으로 위협평가는 발생가능성과 심각성으로, 대처평가는 자기효능감과 반응효능감으로 구성하였다.

먼저, 위협을 평가하기 위해서는 발생할 확률과 심각성이 모두 고려되어야 한다. 위협적인 사건이 발생할 확률은 낮더라도 위협적인 사건

이 발생하였을 때 심각한 문제를 초래한다면 위협은 높게 평가되어야 하고, 위협적인 사건이 발생할 확률은 매우 높지만 그로 인한 문제가 심각하지 않은 수준이라면 위협은 낮게 평가될 수 있다(김종기·이동호, 2005). 또한 정보시스템 분야에서 보호동기이론을 기반으로 진행되어온 다수의 선행연구에서도 위협평가는 발생가능성과 심각성에 의해 결정되고, 최종적으로 행동의 변화가 발생한다는 것이 실증분석을 통해 확인되었다(Chenoweth et al., 2009; Workman et al., 2009; Johnston & Warkentin, 2010; Liang & Xue, 2010; Lee, 2011; Ifinedo, 2012). 본 연구에서도 이러한 선행연구를 기반으로 위협평가는 온라인 환경에서 개인정보가 침해될 수 있는 잠재적 사건에 대한 인지로 정의하고, 개인정보 침해가 발생할 가능성 정도인 발생가능성과 개인정보 침해가 발생한다면 심각한 정도인 심각성을 위협을 형성하는 요인으로 설정하였다.

다음으로, 대처평가는 외부에 존재하는 위협으로부터 잠재적인 손실이 발생하지 않도록 대처하는 능력에 대한 평가를 의미한다. 정보시스템 분야에서 보호동기이론을 기반으로 수행된 다수의 선행연구에서도 위협에 대한 대처평가는 반응효능감과 자기효능감을 토대로 이루어지며, 결과적으로 행동의 변화를 가져온다는 것이 실증분석을 통해 검증되었다(Chenoweth et al., 2009; Workman et al., 2009; Johnston & Warkentin, 2010; Liang & Xue, 2010; Lee, 2011; Ifinedo, 2012). 본 연구에서도 이러한 선행연구를 토대로 대처평가는 온라인 환경에서 프라이버시의 침해로부터 개인정보를 보호할 수 있는 능력으로 정의하고, 개인정보 보호에 대하여 기대되는 결과에 대한 믿음 정도인 반응효능감과 개인정보 보호에 대하여 자신의 능력에 대한 믿음 정도인 자기효능감이 대처평가를 형성하는 요인으로 설정하였다.

본 연구에서는 Li(2012)에서 제시된 이중계산모델에 따라 보호동기이론에서 사용되는 개인의 인지적 평가인 위협평가와 대처평가의 두 가지 주요 요인으로 프라이버시 위험이 결정되는 과정 즉, 프라이버시 위험의 계산 과정을 설명하고자 한다. 프라이버시 계산을 기반으로 수행된 선행연구를 살펴보면, 프라이버시 위험 구성개념에 영향을 미치는 선행요인은 다양하게 나타나지만, 크게 개인적 특성(Krasnova & Veltri, 2010; Li et al., 2011)과 상대방 주체의 특성(Xu et al., 2010; Li et al., 2011)으로 구분할 수 있다. 본 연구에서는 개인적 특성이 프라이버시 위험에 영향을 미친다는 여러 선행연구를 바탕으로 보호동기이론의 주요 요인인 위협평가 및 대처평가와 프라이버시 위험 간의 관계를 설정하였다. 온라인 환경에서 소비자가 자신의 개인정보가 침해될 수 있다고 인지하는 정도인 위협평가가 높을수록, 외부의 위협으로부터 자신의 개인정보를 보호할 수 있는 능력을 인지하는 정도인 대처평가가 낮을수록 온라인 환경에 개인정보를 제공함으로 인해 기대되는 잠재적인 손실 정도를 나타내는 프라이버시 위험의 수준이 높아진다는 가설을 설정하였다.

[가설 3] 위협평가는 프라이버시 위험에 긍정적인 영향을 미칠 것이다.

[가설 4] 대처평가는 프라이버시 위험에 부정적인 영향을 미칠 것이다.

<표 2> 조작적 정의 및 측정항목

구성개념		조작적 정의	측정항목		관련 연구
위협평가	발생가능성	개인정보 침해가 발생할 가능성 정도	나는 전자상거래 사이트에 제공한 나의 개인정보가		Johnston and Warkentin (2010) Liang and Xue (2010) 김종기와 김상희 (2013)
			SUS1	서비스 제공 이외의 다른 목적으로 사용될 가능성이 있다	
			SUS2	서비스 사용이 끝난 후에도 동의없이 사용될 가능성이 있다	
			SUS3	제3자에게 공유될 가능성이 있다	
			SUS4	비윤리적으로 사용될 가능성이 있다	
			SUS5	불법적 접근이 발생할 가능성이 있다	
	심각성	개인정보 침해가 발생한다면 심각한 정도	전자상거래 사이트에 제공한 나의 개인정보가 유출된다면		
			SEV1	나에게 있어 심각한 문제 초래할 수도 있다	
			SEV2	나의 사생활이 침해당할 수도 있다	
			SEV3	나의 신상이 위험해질 수도 있다	
			SEV4	금전적 손실이 발생할 수도 있다	
			SEV5	온라인 서비스 이용하는데 문제가 생길 수 있다	
대처평가	자기효능감	개인정보 보호에 대해여 자신의 능력에 대한 믿음 정도	나는		
			SEL1	나의 개인정보가 안전하게 보호될 수 있도록 잘 관리할 자신이 있다	
			SEL2	개인정보를 보호하기 위한 예방수칙들을 잘 지킬 수 있다	
			SEL3	웹사이트에서 제시하는 개인정보 보호정책을 잘 따를 수 있다	
			SEL4	필요할 때 언제든지 나의 개인정보를 보호하기 위한 조치를 취할 수 있다	
			SEL5	개인정보를 보호하기 위해서 개인정보를 통제할 능력이 있다	
	반응효능감	개인정보 보호에 대하여 기대되는 결과에 대한 믿음 정도	개인정보를 보호하기 위한 개인적 노력(일반적 주의행동, 기술적 보호행동)을 하는 것은		
			RES1	나의 개인정보에 불법적인 접근을 예방할 수 있다	
			RES2	나의 개인정보가 제3자에게 노출되는 것을 예방할 수 있다	
			RES3	신용사기 등의 금전적 손실을 예방할 수 있다	
			RES4	정보유출로 인한 이차적 피해에 대해 예방할 수 있다	
			RES5	전반적으로 나의 개인정보를 안전하게 보호할 수 있다	
프라이버시 이익		개인정보를 제공함으로 인해 얻을 수 있는 혜택 정도	전자상거래 사이트를 이용하는 것은		Krasnova and Veltri(2010) Xu et al.(2010) Xu et al.(2011)
			BEN1	나에게 유용하다	
			BEN2	나에게 가치가 있다	
			BEN3	나에게 도움이 된다	
			BEN4	나에게 이익이 된다	
프라이버시 위험		개인정보를 제공함으로 인해 기대되는 잠재적인 손실 정도	전자상거래 사이트에 개인정보를 제공하는 것은		Xu et al.(2010) Li et al.(2011) Xu et al.(2011)
			RIS1	위험이 수반된다	
			RIS2	예상치 못한 문제를 발생시킬 수 있다	
			RIS3	불확실성(불안전성) 요소가 많을 것이다	
			RIS4	나에게 손실이 발생할 수 있다	
			RIS5	안전하지 못하다	
정보제공 의도		개인정보를 제공하고자 하는 정도	나는 전자상거래 서비스를 이용하기 위해 개인정보가 요구될 때		Dinev and Hart (2006) Xu et al.(2010)
			INT1	개인정보를 기꺼이 제공한다	
			INT2	대체로 개인정보를 제공한다	
			INT3	개인정보를 흔쾌히 제공한다	
			INT4	개인정보를 자주 제공한다	

Ⅳ. 실증분석

4.1. 자료의 수집 및 분석

본 연구에서는 이중계산모델을 기반으로 전자상거래 사용자의 프라이버시 의사결정에 영향을 미치는 요인을 규명하고자 실증분석을 실시하였다. 먼저, 본 설문조사를 수행하기 전에 설문항목이 적절하게 구성되었는지 확인하기 위해 사전조사(Pre-Test)를 실시하였다. 사전조사를 위해 경영학과 대학원생 및 학부학생들을 대상으로 약 50부를 배포하여 45부를 회수하였으며, 탐색적 요인분석과 응답자의 면담을 통해 해당 요인에 제대로 적재되지 않거나 문맥상 이해하기 어려운 설문항목을 삭제 및 수정하여 최종적으로 본 설문조사에 사용될 7개의 구성개념에 대해 총 33개의 측정항목을 개발하였다.

<표 3> 표본 집단의 개인정보 관련 경험적 특성

구분			빈도(명)	비율(%)
개인정보 유출경험 정도		경험없음	23	11.7
		주변사람 경험	25	12.7
		간접적인 경험	96	48.7
		직접적인 경험	53	26.9
개인정보 보호행동	개인정보 요구시 불응	하지않음	25	12.7
		가끔 함	78	39.6
		항상 함	94	47.7
	텔레마케팅 전화 항의	하지않음	146	74.1
		가끔 함	38	19.4
		항상 함	13	6.5
	개인정보 기입된 종이 폐기	하지않음	21	10.7
		가끔 함	64	32.5
		항상 함	112	56.8
	개인정보 관련 뉴스 관심	하지않음	40	20.3
		가끔 함	129	65.5
		항상 함	28	14.2
	개인정보보호 서비스 이용	하지않음	81	41.1
		가끔 함	76	38.6
		항상 함	40	20.3
개인정보 보호성향		전혀 그렇지 않다	3	1.5
		약간 그렇지 않다	42	21.3
		보통이다	74	37.6
		약간 그렇다	69	35.0
		매우 그렇다	9	4.6

본 설문조사는 2015년 10월 약 한달동안 부산 및 경남지역의 대학생들을 대상으로 설문지를 배포하였다. 총 215부를 배포하여 206부를 회수하였으며 결측치를 포함한 응답이나 불성실한 응답이 존재하는 9부를 제외하고 총 197부를 실증분석을 위해 사용하였다. 탐색적 요인분석을 위해서는 SPSS 23.0을, 연구모형 분석을 위해서는 SmartPLS 2.0을 활용하였다. PLS는 형성지표와 반영지표로 설정된 구성개념과 고차원 요인으로 설정된 구성개념의 측정이 가능한 장점이 있다(김종기·김진성, 2014). 본 연구에서는 위협평가와 대처평가를 2차 요인으로 설정하고 있으며, 이들을 구성하는 1차 요인과의 관계를 형성지표로 설정하고 있어 PLS를 분석도구로 활용하는 것이 적절하다고 판단하였다.

본 연구에서 수집된 표본 집단의 인구통계학적 특성을 살펴보면, 남성이 104명(52.8%), 여성이 93명(47.2%)으로 남성의 비율이 다소 높은 것으로 나타났으며 대학생을 대상으로 설문이 진행되었기 때문에 모두 20대인 것으로 나타났다. 표본 집단의 개인정보와 관련된 경험적 특성은 <표 3>에 제시되어 있다. 응답자의 개인정보유출에 대한 간접적 경험이 96명(48.7%), 직접적 경험이 53명(26.9%)으로 나타나 대부분의 응답자가 개인정보유출경험이 있는 것으로 나타났으며, 자신의 개인정보에 대한 보호성향을 '보통이다'와 '약간 그렇다'로 인식하는 경우가 많은 비중을 차지하는 것으로 나타났다.

4.2. 연구도구의 검증

본 연구에서는 이단계 분석법(Two-Step Analysis)에 따라 구조모형을 검정하기 전에 먼저 측정변수의 신뢰성 및 타당성 평가를 통해 연구도구를 검증하고자 하였다. 연구도구의 신뢰성을 평가하기 위해 Cronbach's α, 합성신뢰도(CR: Composite Reliability), 평균분산추출(AVE: Average Variance Extracted)을 이용하였다. 내적일관성을 나타내는 Cronbach's α가 0.7 이상, 측정변수들의 공유분산을 나타내는 CR이 0.7 이상, 측정변수들이 설명되는 분산의 비율을 나타내는 AVE가 0.5 이상이면 구성개념의 신뢰성이 확보된 것으로 평가된다(Nunnally & Bernstein, 1994).

한편, 연구도구의 타당성 평가는 집중타당성과 판별타당성으로 구분된다. 집중타당성은 각 구성개념의 측정변수들이 일치하는 정도로, 각 구성개념에 대한 측정변수들의 추정치가 0.5 이상인 경우 집중타당성이 확보된 것으로 평가된다(Segars & Grover, 1993). 판별타당성은 다른 구성개념의 측정변수들과의 차이 정도로, 각 구성개념의 AVE 제곱근이 0.7 이상이며 다른 구성개념과의 상관계수보다 클 때 판별타당성이 확보된 것으로 평가된다(Barclay et al., 1995; Chin, 1998). 본 연구에서 각 구성개념들의 신뢰성 및 타당성을 분석한 결과, 모두 수용기준을 충족한다는 것을 <표 4>와 <표 5>에서 확인할 수 있다.

<표 4> 1차 요인의 신뢰성 및 집중타당성 분석

구성개념	측정변수	추정치	t값	α	CR	AVE
발생가능성 (SUS)	SUS1	0.880	49.089	0.933	0.949	0.789
	SUS2	0.907	47.666			
	SUS3	0.923	76.192			
	SUS4	0.888	45.247			
	SUS5	0.841	32.749			
심각성 (SEV)	SEV1	0.882	46.732	0.899	0.925	0.713
	SEV2	0.883	50.902			
	SEV3	0.816	29.403			
	SEV4	0.869	41.841			
	SEV5	0.767	22.925			
자기효능감 (SEL)	SEL1	0.796	4.152	0.902	0.921	0.700
	SEL2	0.913	4.122			
	SEL3	0.878	4.337			
	SEL4	0.740	3.859			
	SEL5	0.845	4.602			
반응효능감 (RES)	RES1	0.892	4.209	0.944	0.934	0.740
	RES2	0.891	4.202			
	RES3	0.946	3.418			
	RES4	0.786	3.638			
	RES5	0.774	3.834			
프라이버시 이익 (BEN)	BEN1	0.927	68.241	0.943	0.959	0.855
	BEN2	0.906	49.397			
	BEN3	0.945	92.149			
	BEN4	0.919	59.267			
프라이버시 위험 (RIS)	RIS1	0.863	37.883	0.910	0.933	0.737
	RIS2	0.894	52.204			
	RIS3	0.889	40.928			
	RIS4	0.834	32.139			
	RIS5	0.809	28.629			
정보제공의도 (INT)	INT1	0.905	60.158	0.903	0.932	0.774
	INT2	0.893	49.833			
	INT3	0.882	48.975			
	INT4	0.838	31.653			

<표 5> 1차 요인의 판별타당성 분석

	SUS	SEV	SEL	RES	BEN	RIS	INT
AVE제곱근	**0.888**	**0.844**	**0.837**	**0.860**	**0.925**	**0.858**	**0.880**
SUS	1.000						
SEV	0.480	1.000					
SEL	-0.012	0.156	1.000				
RES	-0.133	0.067	0.546	1.000			
BEN	0.187	0.187	0.042	0.060	1.000		
RIS	0.593	0.558	0.135	0.103	0.048	1.000	
INT	-0.021	-0.033	-0.169	-0.199	0.392	-0.199	1.000

<표 6> 2차 요인의 다중공선성 분석

구성 개념	측정변수	공차	VIF	상태 지수
위협	발생가능성	0.769	1.300	1.217
	심각성	0.769	1.300	1.687
효능감	자기효능감	0.702	1.424	1.243
	반응효능감	0.702	1.424	1.844

다음으로, 본 연구모형에서 설정된 2차 요인에 대한 연구도구의 검증이 이루어졌다. 2차 요인이 포함된 연구모형은 먼저 1차 요인으로만 구성된 연구모형을 분석한 결과 나타난 잠재변수 요인점수(Latent Variable Score)를 2차 요인의 측정항목으로 사용하게 된다. 이때, 잠재변수 요인점수는 SmartPLS에서 제시하는 값을 활용한다. 본 연구에서도 2차 요인으로 설정된 위협과 효능감 구성개념에 대하여 앞서 1차 요인의 분석결과 나타난 잠재변수 요인점수를 2차 요인의 측정지표로 적재하여 실증분석을 실시하였다.

2차 요인으로 설정된 위협과 효능감 구성개념은 구성개념과 측정변수 간의 관계가 형성지표로 설정되어 있다. 형성지표로 설정된 특정 구성개념은 그들을 구성하고 있는 측정변수들에 의해 형성된다고 가정하기 때문에 측정변수들 간의 상관관계가 낮아야 하며, 쉽게 제거되거나 교체될 수 없다는 특징을 가진다(Hair et al., 2013). 따라서 형성지표로 구성된 구성개념은 반영지표와는 다르게 측정변수들이 특정 구성개념을 잘 반영하는지를 나타내는 내적일관성 분석이 의미가 없으며, 측정변수들 간의 다중공선성을 분석함으로써 타당성을 평가하게 된다.

다중공선성 분석은 공차(Tolerance), VIF (Variance Inflation Factor), 상태지수 (Condition Index)를 통해 이루어진다. 공차가 0.1 이상, VIF가 10 이하, 상태지수가 30 이하일 때, 측정변수들 간의 다중공선성이 없는 것으로 판단되어 구성개념의 타당성이 확보된다 (Stevens, 1992; Chin, 1998). 본 연구에서는 형성지표로 구성된 위협과 효능감 구성개념의 다중공선성 분석을 실시한 결과, <표 6>에 나타난 바와 같이 수용기준을 모두 충족시키는 것으로 나타나 타당성이 확보되는 것을 확인할 수 있다.

4.3. 연구모형의 평가 및 가설검정

연구모형에서 설정한 인과관계를 검정하기에 앞서 구조모형에 대한 적합도 평가를 실시하였다. 적합도 평가는 각 구성개념에 대한 적합도와 모형 전체에 대한 적합도 평가로 구분된다. 각 구성개념에 대한 적합도는 내생변수들의 설명된 분산을 나타내는 R^2과 통계추정량인 Redundancy로 평가한다. Redundancy가 양수이고, R^2이 0.26 이상이면 적합도 수준이 '상', 0.13 이상 0.26 미만이면 '중', 0.13 미만이면 '하'로 평가된다(Cohen, 1988; Chin, 1998).

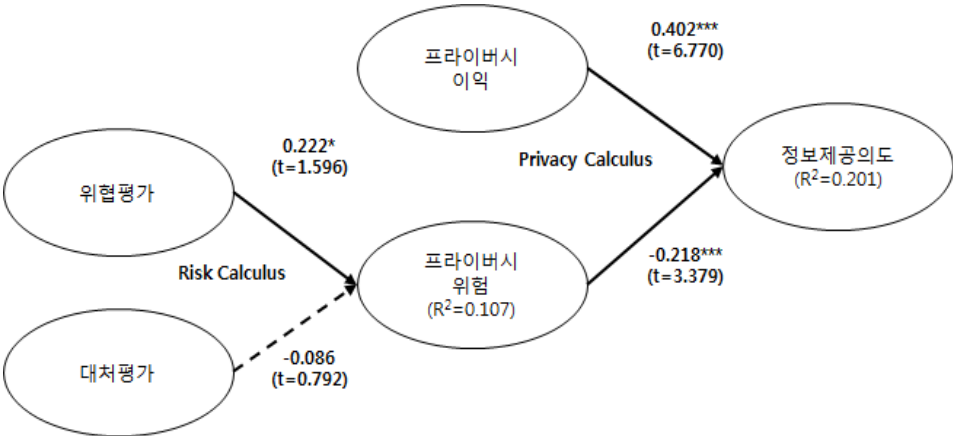
<표 7> 구조모형의 적합도 분석

구성개념	R^2	Redundancy	Communality
위협			0.247
효능감			0.744
프라이버시이익			0.855
프라이버시위험	0.107	0.012	0.736
정보제공의도	0.201	0.116	0.774
평균값	0.154	0.064	0.671
전체 적합도	**0.322**		

구조모형 전체에 대한 적합도는 R^2의 평균과 Communality의 평균을 곱한 값의 제곱근이 0.36 이상이면 전체 적합도 수준이 '상', 0.25 이상 0.36 미만이면 '중', 0.1 이상 0.25 미만이면 '하'로 평가된다(Tenenhaus et al., 2005). 본 연구에서는 <표 7>에 제시된 바와 같이 프라이버시 위험의 적합도가 0.107로 낮은 수준, 정보제공행동은 0.201로 중간 수준으로 나타났으며 전체 적합도는 0.322로 중간 수준으로 나타나 연구모형의 인과관계를 설명하는데 문제가 없는 것으로 판단할 수 있다.

다음으로 연구가설로 설정된 경로의 유의성을 검정하기 위해 반복적인 샘플링을 통해 t값을 제시하는 부트스트래핑(Bootstrapping)을 실시하였으며, 서브샘플링의 수는 500회로 설정하였다. 본 연구모형에 대한 경로분석을 실시한 결과는 <그림 3>과 같다. 연구모형의 각 경로를 살펴보면, 대처평가와 프라이버시 위험 간의 경로를 제외한 다른 모든 경로들은 통계적으로 유의한 것으로 분석되었다.

먼저 프라이버시 계산에 대한 관계를 살펴보면, 프라이버시 이익이 정보제공의도에 긍정적인 영향(t=6.770, p<0.01)을 미치는 것으로 나타났으며 프라이버시 위험은 정보제공의도에 부정적인 영향(t=3.379, p<0.01)을 미치는 것으로 나타났다. 위험 계산에 대한 관계를 살펴보면, 위협평가는 프라이버시 위험에 긍정적인 영향(t=1.596, p<0.1)을 미치는 것으로 나타났으나 대처평가는 프라이버시 위험에 부정적인 영향(t=0.792, p>0.1)은 미치지만 통계적 유의하지 않는 것으로 분석되었다.



<그림 3> 연구모형의 인과관계 분석

Ⅴ. 결 론

본 연구는 전자상거래 사용자의 프라이버시 의사결정에 영향을 미치는 요인을 이중계산모델을 기반으로 살펴보고자 하였다. 프라이버시 이익과 프라이버시 위험의 상충관계를 설명하는 프라이버시 계산과 프라이버시에 대한 외부 위협과 대처 효능감의 상충관계를 설명하는 위험 계산을 통합적인 관점에서 규명하고자 Li(2012)가 제안한 이중계산모델을 통계적으로 검증하였다.

본 연구의 분석결과는 다음과 같다. 첫째, 프라이버시 계산 과정에서 프라이버시 이익과 프라이버시 위험은 정보제공의도에 모두 유의한 설명력을 가지는 것으로 나타났다. 전자상거래 사용자가 서비스를 이용함으로써 얻게 되는 이익을 높게 인지할수록 개인정보를 제공하게 되며, 전자상거래에 제공하는 개인정보에 대한 잠재적 손실을 높게 인지할수록 개인정보를 제공하지 않게 된다.

프라이버시 이익이 프라이버시 위험보다 정보제공의도에 더 많은 영향을 미치는 것으로 나타났다. 이는 이익은 현재 시점에서 즉각적으로 발생하는 반면에 위험은 미래 시점에서 잠재적이므로 프라이버시 의사결정 시 개인정보를 제공함으로 인해 얻게 되는 혜택이 상대적으로 중요한 역할을 한다는 것을 의미한다. 이는 Acquisti(2004)와 Smith et al.(2011)의 견해와 일치하는 결과를 보인다.

둘째, 프라이버시 계산의 주요 요인인 프라이버시 위험을 계산하는 과정에서는 위협평가는 프라이버시 위험을 결정하는데 유의한 설명력을 가지는 것으로 나타났지만 대처평가는 유의한 설명력을 가지지 않는 것으로 나타났다. 외부로부터 발생하는 프라이버시 위협에 대한 평가가 높을수록 전자상거래에 제공하는 개인정보에 대한 잠재적 손실이 발생할 수도 있다고 인지하게 되지만 그 위협에 대하여 대처하는 능력 즉, 효능감이 높다고 해서 잠재적 위험의 수준을 낮춰주지는 않는다. 결국, 부정적인 요인인 위협에 대한 평가가 위험 수준을 높이는 결정적인 역할을 한다는 것을 의미한다. 이는 김종기와 김상희(2013)의 연구에서 나타난 분석결과와 일치하는 결과를 보인다.

본 연구는 다음과 같은 학술적 시사점을 가진다. 첫째, 본 연구에서는 기존의 연구에서 제시된 프라이버시 계산 이론과 보호동기이론을 통합하는 관점에서 연구를 진행하였다. 그동안 프라이버시 연구에서는 프라이버시 행동을 설명하기 위해 프라이버시 계산 이론과 보호동기 이론이 각각 적용되어 왔으나, 두 이론을 통합하여 설명하고자 하는 연구는 찾아보기 어려웠다. 최근 Li(2012)의 연구에서 두 이론을 통합하는 관점에서 연구를 진행하였지만, 프레임워크만 제시할 뿐 실증적인 검증은 이루어지지 않았다. 따라서 본 연구에서는 온라인 환경에서 사용자의 정보제공의도를 두 이론을 통합하는 관점에서 설명하고 이들의 관계를 검증하기 위해 실증분석을 시도하였다는데 의의가 있다고 볼 수 있으며, 이는 프라이버시 연구의 이론적 기반을 확대할 수 있는 계기가 된다고 판단된다.

둘째, 본 연구에서 프라이버시 위험이 계산되는 과정을 보호동기이론의 주요 요인인 위협평가와 대처평가를 통해 설명하고자 하였다. 보호동기이론을 다루는 기존의 연구에서는 대부

분 위협평가와 대처평가를 다차원적 개념으로 설정하고 있지만, 본 연구에서는 위험 계산을 포함하는 연구모형의 설명력을 높이고자 위협평가와 대처평가에 해당하는 요인들을 하위 요인으로 보고 이들을 통해 2차 요인이 형성되는 구조를 제안하였다. 위험 계산을 구성하는 위협평가와 대처평가를 고차원 요인으로 설정하여 보다 설명력 있는 연구모형을 도출하기 위한 새로운 시도를 함으로써 관련 연구가 발전하는데 학문적 기여를 할 수 있을 것이라고 예상되는 바이다.

이러한 학술적 시사점을 바탕으로 온라인 환경에서 소비자의 정보제공과 관련된 행동을 강화하기 위한 방안을 논의할 수 있다. 본 연구의 분석결과에 따르면, 온라인 환경에서 소비자는 개인정보 제공여부에 있어서 자신의 개인정보를 제공함으로 인해 기대되는 이익이 보장되는 것이 중요할 뿐만 아니라 소비자가 자신의 개인정보를 제공함으로 인해 기대되는 위험을 줄여주는 것이 무엇보다 중요하다고 판단된다.

이에 따라 본 연구결과를 통해 프라이버시 위험을 감소하기 위한 방안을 강구해 볼 수 있다. 프라이버시 위험의 계산에 영향을 미치는 요인을 외부의 위협에 대한 평가와 이에 대한 대처능력에 대한 평가라고 가정하였으나, 부정적인 요인인 위협평가가 위험인지에 있어 결정적인 역할을 한다는 것을 알 수 있다. 외부의 위협에 대한 평가는 프라이버시와 관련된 과거의 경험으로부터 비롯된다고 할 수 있으며, 이는 오랜 기간에 걸쳐 축적되어 나타나는 결과라고 할 수 있다. 따라서 근본적으로 개인의 위협평가 수준을 낮추기 위하여 정부 및 개인정보보호 기관의 지속적인 노력이 필요할 것으로 예상된다.

본 연구의 한계점 및 향후 연구방향은 다음과 같다. 첫째, 본 연구의 표본 집단은 부산 및 경남 지역의 대학생들로 구성되었기 때문에 연령별 및 지역별과 관련하여 표본의 대표성 문제가 존재한다. 본 연구의 일반화를 위해서 향후 연구에서는 표본을 보다 다양한 지역과 연령층을 대상으로 확장하여 연구가 분석되어야 할 필요가 있다.

둘째, Li(2012)의 통합연구에서 제시된 프레임워크에 따르면 정보제공행동에 영향을 미치는 요인이 다양하게 나타나고 있으나 본 연구에서는 이중계산모델 즉, 프라이버시 계산과 위험 계산에 초점을 맞추어 연구를 진행하였다. 연구모형의 설명력을 높이기 위해서는 보다 다양한 요인이 고려되어야 하며, 아울러 연령층이나 직업군에 따른 비교연구 등 더욱 구체적인 연구도 지속적으로 이루어진다면 보다 의미있는 연구가 될 수 있을 것이다.

셋째, 본 연구에서는 전자상거래 사용자를 대상으로 설문지가 구성되어 연구가 진행되었다. 온라인 환경에는 특정 서비스를 이용하기 위해 제공하는 개인정보의 유형이 다양하게 존재한다. 전자상거래에 제공하는 소비자의 일반적인 신상정보뿐만 아니라 보다 민감한 금융정보, 특정 서비스를 받기 위해 자신의 위치를 제공하는 위치정보 등 다양한 유형의 개인정보가 존재하며, 이러한 개인정보의 유형에 따라 프라이버시 의사결정 과정에도 차이가 있을 것이라고 예상된다. 따라서 개인정보의 유형에 따른 비교연구로 확장된다면 프라이버시 분야에서 더욱 의미있는 연구로 발전할 수 있을 것이다.

참고문헌

김상현, 박현선, “프라이버시 보호인식 및 보호행동의도에 미치는 영향 요인과 프라이버시 침해경험의 조절효과에 관한 연구,” 인터넷전자상거래연구, 제13권, 제4호, 2013, pp. 79-105.

김영렬, “개인 정보 보호 의식 측정 정도의 개발과 개인정보 중요성에 관한 인지도 조사,” 한국산업정보학회논문지, 제15권, 제5호, 2010, pp. 259-271.

김종기, 이동호, “전자상거래 사용자의 신뢰에 영향을 미치는 정보보안위험 기반의 선행요인 연구,” 경영정보학연구, 제15권, 제2호, 2005, pp. 65-96.

김종기, 김상희. “스마트폰 위치기반서비스에서 정보제공의도: 프라이버시 계산 관점을 중심으로,” 정보시스템연구, 제21권, 제4호, 2012, pp. 55-79.

김종기, 김상희, “온라인 환경에서 프라이버시 행동의도에 미치는 영향,” 정보화정책, 제20권, 제3호, 2013, pp. 63-85.

김종기, 김진성, “전자상거래에서 정보 프라이버시 염려를 유발하는 원인과 보호반응에 관한 연구: 주인-대리인 이론을 중심으로,” 정보시스템연구, 제23권, 제4호, 2014, pp. 119-145.

Acquisti, A., “Privacy in Electronic Commerce and the Economics of Immediate Gratification,” *Proceedings of the 5th ACM Electronic Commerce Conference*, 2004, pp. 21-29.

Barclay, D., Thompson, R., and Higgins, C., “The Partial Least Squares (PLS) Approach to Causal Modeling, Personal Computer Adoption and Use as an Illustration,” *Technology Studies,* Vol. 2, No. 2, 1995, pp. 285-324.

Chenoweth, T., Minch, R., and Gattiker, T., “Application of Protection Motivation Theory to Adoption of Protective Technologies,” *Proceedings of the 42nd Hawaii International Conference on System Science*, 2009.

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

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

Culnan, M. J. and Bies, J. R., “Consumer Privacy: Balancing Economic and Justice Considerations,” *Journal of Social Issues,* Vol. 59, No. 2, 2003, pp. 323-342.

Dinev, T. and Hart, P., “An Extended Privacy Calculus Model for E-Commerce Transactions,” *Information Systems Research,* Vol. 17, No. 1, 2006, pp. 61-80.

Hair, J. F., Hult, G. T. M., Ringle, C. M., and Sarstedt, M., *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM),* SAGE Publication, 2013.

Ifinedo, P., “Understanding Information Systems Security Policy Compliance: An Integration of the Theory of

Planned Behavior and the Protection Motivation Theory," *Computers & Security,* Vol. 31, 2012, pp. 83-95.

Johnston, A. C. and Warkentin, M., "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly,* Vol. 34, No. 3, 2010, pp. 549-566.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., and Greer, C., "Information Disclosure on Mobile Devices: Re-Examining Privacy Calculus with Actual User Behavior," *International Journal of Human-Computer Studies,* Vol. 71, 2013, pp. 1163-1173.

Krasnova, H. and Veltri, N. F., "Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA," *Proceedings of the 43rd Hawaii International Conference on System Sciences*, 2010, pp. 1-10.

Lee, Y., "Understanding Anti-plagiarism Software Adoption: An Extended Protection Motivation Theory Perspective," *Decision Support Systems,* Vol. 50, 2011, pp. 361-369.

Li, H., Sarathy, R., and Xu, H., "Understanding Situational Online Information Disclosure as a Privacy Calculus," *Journal of Computer Information Systems,* 2010, pp. 1-29.

Li, H., Sarathy, R., and Xu, H., "The Role of Affect and Cognition on Online Consumers' Decision to Disclose Personal Information to Unfamiliar Online Vendors," *Decision Support Systems,* Vol. 51, No. 3, 2011, pp. 434-445.

Li, Y., "Theories in Online Information Privacy Research: A Critical Review and an Integrated Framework," *Decision Supports Systems,* Vol. 54, 2012, pp. 471-481.

Liang, H. and Xue, Y., "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems,* Vol. 11, No. 7, 2010, pp. 394-413.

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

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

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

Segars, A. and Grover, V. "Re-Examining Perceived Ease of Use and Usefulness: A Confirmatory Factor Analysis," *MIS Quarterly,* Vol. 17, No. 4, 1993, pp. 517-525.

Smith, H. J., Dinev, T., and Xu, H.,

"Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly,* Vol. 35, No. 4, 2011, pp. 989-1015.

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

Stone, E. F. and Stone, D. L., "Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms," *Research in Personnel and Human Resources Management,* Vol. 8, No. 3, 1990, pp. 349-411.

Tenenhaus, M., Vinzi, V. E., Chatelin, Y. M., and Lauro, C., "PLS Path Modeling," *Computational Statistics & Data Analysis,* Vol. 48, No. 1, 2005, pp. 159-205.

Workman, M., Bommer, W. H., and Straub, D., "The Amplification Effects of Procedural Justice on a Threat Control Model of Information Systems Security Behaviours," *Behaviour & Information Technology,* Vol. 28, No. 6, 2009, pp. 563-575.

Xu, H., Teo, H., Tan, B. C. Y., and Agarwal, R., "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Service," *Journal of Management Information Systems,* Vol. 26, No. 3, 2010, pp. 135-173.

Xu, H., Luo, X., Carroll, J. M., and Rosson, M. B., "The Personalization Privacy Paradox: An Exploratory Study of Decision Making Process for Location-Aware Marketing," *Decision Support Systems,* Vol. 51, No. 1, 2011, pp. 42-52.

김 상 희(Kim, Sanghee)

부산대학교 경영학과에서 박사학위를 취득하고 현재 부산대학교 경영연구소에서 박사후연구원으로 재직 중이다. 주요 연구 관심분야는 프라이버시, 정보보안, 행동경제학 등이다.

김 종 기(Kim, Jongki)

부산대학교 경영학과에서 학사를 마쳤으며, 미국 Arkansas State University에서 경영학 석사학위, Misissippi State University에서 경영학 박사학위를 취득하였다. 현재 부산대학교에서 경영학과 교수로 재직 중이며, 주요 관심분야는 정보보안관리, 프라이버시, 전자상거래, 기술경영 등이다.

<Abstract>

A Study on Factors Influencing Privacy Decision Making on the Internet: Focus on Dual-Calculus Model

Sanghee Kim · Jongki Kim

Purpose

This study aims to investigate the factors that influence decision making in relation to providing personal information on the internet with respect to the integration of the privacy calculus theory and protection motivation theory based on the dual-calculus model proposed by Li(2012).

Design/methodology/approach

The privacy calculus theory and protection motivation theory have been applied to explain privacy behavior to a certain degree but few studies have been conducted to explain privacy behavior based on the integration of these two theories. Although Li(2012) proposed the dual-calculus model, he only proposed its framework and did not carry out an empirical study. Therefore, this study proposes a research model that integrates these two theories and examines the relationship between the two theories through an empirical study.

Findings

According to the results of empirical analysis, it was found that all relations have statistically significant explanatory power except the relation between coping appraisal and privacy risk in the risk calculus process. Thus, the results verify that external threat played a decisive role in increasing the risk level of a consumer's privacy. It can be discussed the ways to enhance the privacy behavior of consumer on the internet through these findings.

Keywords: Dual-Calculus Model, Privacy Calculus, Risk Calculus, Protection Motivation Theory, Information Disclosure Intention

* 이 논문은 2016년 7월 13일 접수, 2016년 8월 23일 1차 심사, 2016년 9월 23일 게재 확정되었습니다.