# 정보품질을 위한 개인정보 보호행위: 건강심리이론 관점을 중심으로

지범석*·판 류*·이상철**·서영호*†

*경희대학교 경영학부
**그리스도대학교 경영학부

# Personal Information Protection Behavior for Information Quality : Health Psychology Theory Perspectives

Bum-Suk Jee*·Liu Fan*·Sang-Chul Lee**·Yung-Ho Suh*†

*School of Management, Kyung Hee University
**Dept. of Business Administration, Korea Christian University

Key Words : Protection Motivation Theory, Personal Information Security, Health Psychology Theory, Threat, Behavior Theory

**Abstract**

The purpose of this research is to understand users' information protection behavior on personal information security from health psychology theory perspectives. Empirical results indicate that users' information protection behavior on personal information is predicted by perceived threat and perceived responsiveness. Perceived threat is determined by perceived susceptibility and perceived severity. Perceived responsiveness is determined by response efficacy and self-efficacy, but response cost is not significant. These findings provide an enriched understanding about users' information protection behavior on personal information security.

## 1. 서 론

인터넷과 정보기술의 발달로 인해 디지털사회로 빠르게 이동하고 있지만, 반대로 위험의 유형 또한 다양해지고 그 위험의 강도도 커지고 있다. 특히, 디지털사회에서는 네트워크로 서로 연결이 되어 있으며, 개방형 구조로 되어 있기 때문에 DDos, SQL 웜, 바이러스, 개인정보유출 등 이전보다 더 심각한 위험에 노출되어 있다(Bagchi and Udo, 2003; Kankanhalli, et al., 2003; Liang and Xue, 2010; Ng et al., 2009).

이러한 위험으로부터 개인 및 조직을 보호하기 위해 정부에서는 다양한 조직적, 법적, 제도적 장치를 마련하고 있다 (Chung et al., 2006, Ng et al., 2009). 우리나라의 경우에는 국가보안기술연구소(NSRI), 한국인터넷진흥원(KISA) 등 정보보호담당기관을 두고 있으며, 국가정보화기본법, 전자서명법 등 정보보호에 관한 법률 제정 및 내컴퓨터 내가 지키기 캠페인, 정보보호 캠페인 등 정보보호에 관한 캠페인을 지속적으로 벌이고 있다 (국가정보보호백서, 2011).

그러나 정보보호는 제도적이고 기술적인 노력만으로는 해결될 수 없으며, 개인적인 위험관리 노력이 더 필요하다 (Anderson and Agarwal, 2006; Liang and Xue, 2010; Ng et al., 2009; Woon et al., 2005). 정보보호와 관련된 다양한 제도와 활동들이 성공적으로 이루어지기 위해서는 개인의 정보보호행위에 대한 연구가 필요하다.

그러나 지금까지의 정보보호 연구들은 외부의 바이러스나 스파이웨어, 해킹 등 보안도구 개발과 같은 기

† 교신저자 suhy@khu.ac.kr

술적 측면의 연구들이 주를 이루어 왔다. 또한 보안활동지침개발, 법률, 제도적 장치 개발, 대응방안 개발 등 정보보안 방법론에 대한 연구들이 있어왔다 (국가정보보호백서, 2011). 그러나 개발된 보안도구를 실제로 사용자들이 사용하지 않거나 개발된 정보보안 지침에 따라 정보보호행위를 하지 않으면 개발된 기술과 방법은 아무런 의미가 없다(Rhodes, 2001). 효과적인 보안기술과 방법의 개발도 중요하지만 실질적으로 보안이 이루어지려면 개인의 행위가 중요하다 (Ng et al., 2009; Stanton et al., 2003). 따라서 이제는 사용자들이 어떻게 하면 개발된 보안도구를 사용하게 하며, 정보보호행위를 할 수 있는지에 대한 연구가 필요한 시점이다. 즉, 이제는 사용자들이 정보보호행위를 하는 원인이 무엇인지를 연구하는 것이 필요하다.

최근 들어서 정보보호행위는 PC보안, 개인정보보안(패스워드사용), 인터넷보안, SNS 보안, 스마트폰 보안 등 여러 형태로 구분되고 있다 (국가정보보호백서, 2011). 네이트온을 통한 개인정보유출사건에서 보이듯이 최근에는 PC보안보다는 개인정보보안에 대한 문제가 더 심각하게 대두되고 있다. 한국인터넷진흥원에서 발표한 2010 정보보호실태 조사에 의하면 해킹신고건수는 2005년 33,633건에서 2010년 16,295건으로 줄고 있으며, 바이러스 신고접수 건수도 2004년 107,994건에서 2010년 17,930건으로 줄고 있다. 반면 개인정보침해신고건수는 2004년 17,569에서 2010년 54,832건으로 늘고 있으며 2011년에는 6월까지만 해도 77,147건으로 보고되고 있다. 해킹에 대한 심각성을 인지하는 사람도 31%인 반면에 개인정보에 대한 심각성은 38.4%로 인식하고 있다 (한국인터넷진흥원, 2010)

이처럼 PC보안에 대한 심각성이 낮아지고 신고건수가 줄어드는 이유로는 대부분 바이러스 백신 프로그램과 안티 스파이웨어 등과 같은 보안도구를 PC에 설치(96.3%)하고 있으며, 지속적으로 보안패치도 설치(90%)하고 있기 때문으로 보인다. 그러나 이와는 달리 개인정보보호를 위해 PC 비밀번호를 설정하는 사용자는 아직 60%에 불과하며, PC 및 웹사이트의 비밀번호 변경 주기도 3개월에 1회 이상 하는 사용자는 26.3%에 불과한 실정이다. 이처럼 개인정보의 보호가 중요함에도 불구하고 사용자들이 개인정보를 보호하려는 행위를 하지 않고 있다.

따라서 본 연구의 목적은 왜 개인이 정보보호행위(information protection behavior)를 하려고 하는지에 대한 이유를 사용자의 행위관점에서 설명하고자 한다. 특히, 최근 들어 정보위험 중에서 가장 심각하게 대두되고 있는 개인정보의 보호행위에 대해서 연구하고자 한다. 특히, 기존의 정보시스템 분야의 이론이 아니라 전통적으로 예방 의료행위를 설명하는데 사용되고 있는 건강심리이론(health psychology theory)을 기반으로 개인의 정보보호행위에 미치는 영향요인에 대해서 연구하고자 한다. 개인정보 보호행위는 개인정보유출을 방지하는 예방행위로 볼 수 있으므로 예방 중심의 건강심리이론 관점의 연구가 유용할 수 있다.

본 연구는 건강심리이론을 이용해서 우리나라에서 개인의 정보보안행위에 대해서 처음으로 모델을 세우고 실증적으로 분석하는 논문으로, 우리나라의 컴퓨터 사용자들의 개인정보 보호행위에 대해서 이해를 하는데 도움을 줄 수 있을 것이다. 따라서 본 연구의 결과는 국내 보안관련 단체 및 기업에게 실무적으로 중요한 시사점을 줄 수 있을 것이다. 또한 본 연구는 기존에 정보시스템 연구에서는 사용하지 않았던 새로운 요인을 사용함으로써 정보시스템 연구 분야에 새로운 관점을 제시해 줄 수 있을 것이다.

## 2. 문헌연구

### 2.1 정보시스템 이론

합리적 행위이론 (theory of reasoned action: TRA), 계획된 행위이론 (theory of planned behavior: TPB), 기술수용이론 (technology acceptance model; TAM) 등 지금까지의 정보시스템 연구들은 왜 사용자들이 정보기술을 수용하려고 하는지에 대해서 연구하여왔다 (Ajzen, 1991; Fishbein and Ajzen, 1975; Davis, 1989). 그러나 정보보호행위와 관련된 분야에 기존의 정보시스템 연구들의 이론을 적용하는 데는 몇 가지 문제점이 있다.

먼저, 정보보호행위는 정보를 보호하거나 정보의 위협으로부터 예방하려는 부정적 관점에서 연구되어야 하지만, 기존의 정보시스템 연구들은 수용이라는 긍정적 관점에서 연구하였기 때문에 정보보호행위 연구에 적용하기 어렵다. 기존의 정보시스템 수용이론은 새로운 기술을 사용하지 않는 사람들에게 새로운 기술을 수용하게 하는 영향요인을 찾는 이론으로, 기술을 수용함으로써 얻을 수 있는 긍정적 기대감을 기반으로 한다. 반면에 정보보호행위는 악성코드, 피싱, 스팸메일, 해킹, 정보유출 등과 같은 위험한 사건이나 환경으로부터

보호 및 예방하려는 활동에 영향을 주는 요인을 찾는 것으로, 부정적 결과에 대한 위협과 이러한 위협에 대응할 수 있는 대응력을 기반으로 한다는 점에서도 차이가 있다. 정보보안 분야의 최근 연구들에 의하면 업무의 유용성(usefulness)을 추구하는 긍정적 기술(positive technologies)과 부정적 결과를 막기 위해서 설계된 보호 기술(protective technologies)은 차이가 있다고 보고 있다 (Carver and White 1994; Dinev and Hu, 2007; Elliot 2006; Elliot and Covington 2001; Lee, 2011; Liang and Xue, 2010; Ng et al., 2009).

두 번째로 정보보호는 정보를 보호하려는 행위의 관점이 중요하지만 기존의 연구들은 안티 스파이웨어, 바이러스 백신 프로그램들과 같은 도구의 수용 관점을 중요하게 보고 있다. TAM이나 TPB 등과 같은 이론은 정보보안도구를 사용하고자 하는 개인의 수용에 대해서 연구할 때는 유용할 수 있다 (Ng et al., 2009). 그러나 정보보호는 단순히 보안도구를 수용하면 되는 것이 아니다. 따라서 단순히 보안도구에 대한 수용이라는 관점으로 접근한다면 전반적인 정보보호에 대한 일부분만을 연구하게 되어 정보보안을 부분적으로만 이해하게 된다 (Liang and Xue, 2010; Ng et al., 2009).

정보보호의 궁극적인 목적은 특정한 보안도구를 수용하는 것이 아니라 위협으로부터의 보호와 예방이다. 그러므로 보호에 중심을 둔 더 광범위한 이론이 필요하지만 지금까지 정보시스템 연구들에 있어서 이처럼 광범위한 접근법을 제안한 연구들은 없었다. 따라서 단순하게 정보보안도구들을 수용하는 관점이 아니라 사용자들이 정보보안활동을 하는 관점에서의 이론적 연구가 필요하다.

이처럼 정보기술 보안행위에 대한 정보기술이론의 한계로 인해 최근 들어 다른 분야의 이론들을 받아들이고 있으며, 그 중의 하나가 바로 의료 및 보건 분야의 이론이다 (LaRose, 2005; Lee, 2011; Liang and Xue, 2010; Ng et al., 2009; Woon et al., 2005). 정보보안은 위험과 관련된 분야로 이는 의료분야의 질병과 비슷하다. 의료에서는 질병이라는 위험을 예방하고 개인의 삶을 보호하기 위하여 건강심리이론이 발전해 왔다. 따라서 예방 중심의 의료행위와 보호 중심의 보안행위가 비슷하기 때문에 본 연구에서는 정보보호행위를 연구하는데 건강심리이론을 적용하고자 한다.

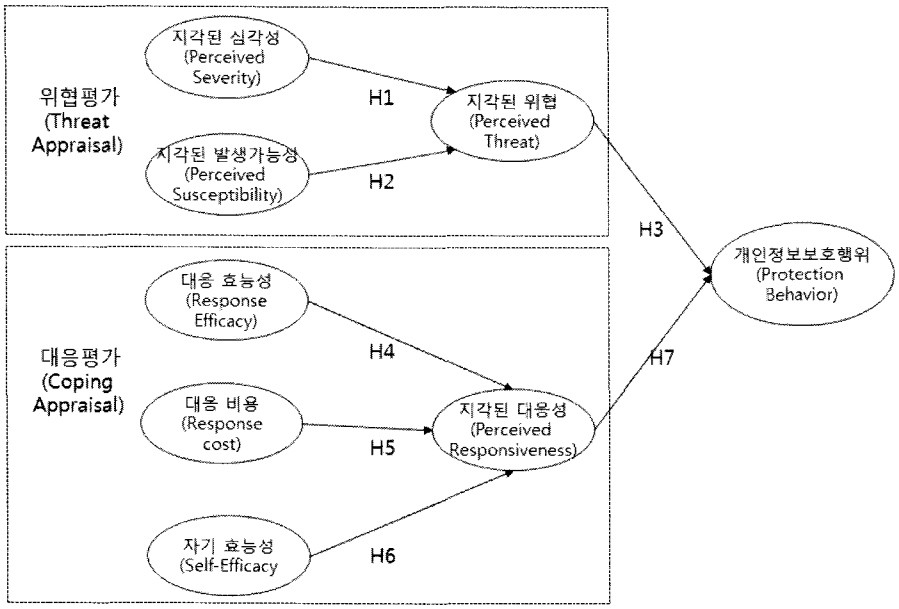
## 2.2 건강심리이론

다른 사람이 내 정보에 침입하지 못하도록 강력한 비밀번호를 설정하고 주기적으로 비밀번호를 변경하는 보안행위는 AIDS나 심장병 등 질병을 예방하기 위해서 수행하는 예방적 건강행위와 유사하다 (Jayanti and Burns, 1998; Ng et al., 2009). 의료 및 보건 분야에서는 사람들의 건강행위에 영향을 주는 원인을 파악하기 위해 건강심리이론을 개발하여 오랫동안 연구해왔다 (Oliver and Berger, 1979; Rosenstock, 1974; Rosenstock et al., 1994; Rogers, 1975, 1983; Weinstein, 2000). 이중에 대표적인 이론이 건강신념모델(Health Belief Model)(Rosenstock, 1974; Rosenstock et al., 1994)과 보호동기이론(protection motivation theory; PMT)(Rogers, 1975, 1983)이다.

의료분야에서 기대-가치이론을 받아들여서 나온 이론이 바로 건강신념모델이다. 건강신념모델은 1950년 공중건강 프로그램이 성공하지 못하게 된 원인이 무엇인지를 찾기 위해 만들어진 모델로써, 개인의 예방행동을 예측하는 모델로써 많이 사용되고 있다 (Rosenstock, 1974). 지금까지의 연구들은 의료 및 보건 분야에서 많이 사용되어 왔다. 건강신념모델은 사람들의 질병예방행동을 설명하는 두 가지 주요 신념을 제시하고 있다. 첫 번째 신념은 질병에 대한 위협(threats)이며 위협에는 지각된 심각성과 지각된 발생가능성이 있다. 두 번째 신념은 행위에 대한 기대(expectation)이며, 기대에는 행위에 대한 지각된 이익, 지각된 장애, 지각된 자기효능성이 있다. IT분야에서 건강신념모델을 적용한 연구로는 Ng et al.(2009)의 이메일 보안활동에 대해 연구가 있다.

보호동기이론은 로저스가 발표한 이론으로 개인이 어떻게 위험을 인지적으로 처리하고 반응하는지를 설명하는 이론이다 (Rogers, 1975, 1983). 여기서 실제적인 행동이 이루어지기 위해서는 보호동기가 유발되어야 하며, 보호동기는 두 가지 변수에 의해서 영향을 받는다고 보고 있다. 하나는 위협평가 과정(Threat-appraisal process)이고, 다른 하나는 대응평가 과정(coping-appraisal process)이다. 위협평가 과정은 위협에 대해서 인지하는 과정으로 위협에 대한 심각성과 개인적인 발생가능성으로 구성되어 있다. 대응평가과정은 대응행위에 대해 평가하는 과정으로 대응행위의 효능성과 대응행위에 대한 비용, 그리고 자기 효능성에 대한 평가로 구성되어 있다.

보호동기이론은 건강신념모델을 확장하여 개발되었기 때문에 두 이론에서 사용되는 영향변수들은 이름만 상이할 뿐 서로 유사하다. 그러나 건강심리이론과는 달




**<그림 1> 연구모형**

리 보호동기이론이 위협평가과정과 대응평가과정이라는 프로세스적인 측면에서 이론적으로 더 잘 설명하고 있기 때문에 두려움(fear)에 대한 자극에 반응하는 행위를 설명하는데 더 좋은 모델이라고 보고 있다(Claar, 2011). IT분야에서 보호동기이론을 이용한 연구로는 표절보호소프트웨어 수용에 대한 연구(Lee, 2011), 안티 스파이웨어 사용에 대한 보호행위에 대한 연구가 있다 (Liang and Xue, 2010).

## 2.3 연구모형 및 가설

본 연구는 의료분야의 건강심리이론을 기반으로 개인의 정보보호행위에 미치는 영향요인이 무엇인지를 연구하고자 한다. 건강심리이론은 정보기술수용이론이 다루지 못하지만 개인정보 보안행위에 있어서 중요한 개념들을 포함하고 있는 이론이다. 건강심리이론 중에서 본 연구에서는 보호동기이론을 기반으로 개인이 왜, 그리고 어떻게 개인정보 유출이라는 위협을 회피하는지를 설명하고자 한다.

본 연구는 보호동기이론의 기본 이론을 적용하여 개인이 정보유출에 대한 위협(threat)을 인지하게 될 때 위협으로 벗어날 수 있는 대응방안을 찾게 되고, 대응방안이 위협으로부터 개인정보를 보호할 수 있다고 인지하게 되면 실제로 개인정보 보호행위를 하려고 한다는 것을 기본이론으로 하고 있다. 본 연구에서는 개인정보유출을 정보보안의 위협으로 정의하였으며, 대응방안으로 강력한 패스워드사용 및 주기적 패스워드 변경 등으로 정의하였다. 특히, 위협과 대응성을 개인정보의 보호행위와 영향변수들을 매개하는 매개변수로 보았다.

본 연구에서는 보호동기이론을 적용하여 <그림 1>과 같이 연구모형을 개발하였다. 먼저, 개인이 개인정보 보호행위를 하는 이유는 패스워드 도용으로 인한 개인정보유출과 같은 위협을 지각하기 때문이다. 지각된 위협이란 개인정보유출이 위협적이라고 개인이 직각하는 정도라고 정의할 수 있다 (Liang and Xue, 2009, 2010). 일반적으로 사람들은 위협을 지각하게 되면 위협을 피하기 위해 위협평가과정(threat appraisal process)을 거치게 된다. 따라서 개인정보유출에 대한 위협을 지각하게 되면 사람들은 이러한 위협으로부터 개인정보를 보호하려고 할 것이며, 위협에 대한 지각이 클수록 개인은 위협으로부터 더 멀어 지려고 할 것이다. 이러한 긍정적인 관계는 이미 많은 건강심리이론에서 검증되었다 (Lee, 2011; Liang and Xue, 2010; Ng et al., 2009; Rippetoe and Rogers, 1987; Rosenstock, 1974; Weinstein, 2000; Woon et al, 2005)

보호동기이론에 의하면 지각된 위협은 지각된 심각성과 지각된 발생가능성이라는 두 변수에 의해 결정된다 (Rogers, 1975, 1983; Weinstein, 2000). 건강심리

이론에서 지각된 심각성(perceived severity)이란 특정한 건강문제가 얼마나 심각한 결과를 초래하는지에 대해서 지각하는 개인의 신념이라고 정의할 수 있다 (Rosenstock, 1974; Rosenstock et al., 1994; Rogers, 1975, 1983). 지각된 발생가능성이란 어떤 질병에 걸릴 수 있다는 주관적 위험이라고 정의할 수 있다 (Rosenstock, 1974; Rosenstock et al., 1994; Rogers, 1975, 1983). 본 연구에서는 지각된 심각성을 개인정보유출로 인해서 발생할 수 있는 부정적인 결과에 대한 개인의 인지정도로 정의하고, 지각된 발생가능성은 개인정보유출로 인해 본인이 큰 피해를 입을 수 있다는 주관적 가능성이라고 정의한다.

사람들은 주민등록번호, 신용카드 등과 같은 개인정보유출로 심각한 피해를 입게 된다고 지각할수록 위협에 대해서 더 높게 지각할 것이다. 그러나 이러한 위협이 나에게 일어나지 않는다고 생각한다면 나에게는 위협으로 지각되지 않을 것이다. 즉, 개인정보가 유출이 될 수 있다는 가능성에 대해 같은 정보를 제공받더라도 어떤 사람은 가능성이 매우 높다고 지각할 것이고, 어떤 사람은 결코 일어나지 않을 것이라고 판단할 것이다. 따라서 개인정보유출 가능성을 높게 인식할수록 개인정보 보호행위를 더 하려고 할 것이다.

기존의 건강심리이론과 최근 정보시스템분야에서 건강심리이론을 적용한 연구들의 결과에 의하면 지각된 발생가능성과 부정적 결과에 대한 심각성은 위협에 대한 지각을 증가시키며, 그 결과 개인이 보호행위를 하는 원인이 된다고 하였다 (Ng et al., 2009; Rosenstock, 1974; Workman et al., 2008; Woon et al., 2005). 기존의 건강심리이론들은 지각된 심각성과 지각된 발생가능성이 직접적으로 보호행위에 영향을 준다고 보았으나, 본 연구에서는 두 개의 변수가 개인의 위협지각에 영향을 주고, 위협을 인지한 개인이 보호행위를 하는 것으로 보았다. 이러한 이론적 배경을 통해서 본 연구에서는 다음과 같은 가설을 설정하였다.

가설 1: 개인정보가 유출될 수 있다는 지각된 발생가능성은 지각된 위협에 긍정적인 영향을 줄 것이다.

가설 2: 개인정보가 유출됨으로 해서 발생할 수 있는 지각된 심각성은 지각된 위협에 긍정적인 영향을 줄 것이다.

가설 3: 지각된 위협은 개인의 정보보행위에 긍정적인 영향을 줄 것이다.

두 번째로 위협에 대해서 지각하게 되면 사용자들은 여러 가지 대응방안에 대해서 평가하는 대응평가과정(coping appraisal process)을 거치게 되며, 대응방안이 위협으로 부터 보호해줄 수 있다고 지각하게 되면 정보보호행위를 할 것이다. 지각된 대응성이란 효과적인 패스워드 사용 및 패스워드의 주기적 변경 등이 패스워드 도용 및 개인정보유출을 얼마나 보호할 수 있는지에 대한 개인의 평가로 정의할 수 있다 (Liang and Xue, 2009).

기대이론에 의하면 사용자들은 가장 가치 있는 결과를 얻을 수 있는 대응방안을 선택하려고 한다 (Steers et al. 2004;). 이처럼 개인정보 보안행위를 하려는 이유는 보안행위(대응방안)가 개인정보유출 위협으로부터 얼마나 보호할 수 있는 지로 평가된다. 지각된 대응성이 클수록 사용자는 더 많이 대응방안을 받아들이려고 할 것이다.

건강심리이론을 기반으로 본 연구에서는 지각된 대응성에 영향을 주는 변수로 대응 효능성(response efficacy), 대응 비용 (response cost), 자기 효능성 (self-efficacy)을 설정하였다. 즉, 사람들은 대응방안이 정보기술의 위협을 방어하는데 효과적인지, 대응방안을 수행하기 위해 어떤 비용을 지불해야 되는지, 그리고 본인이 잘 할 수 있다는 확신을 얼마나 가지고 있는 지로 대응방안을 평가하게 된다. (Compeau et al., 1999; Liang and Xue, 2009, 2010; Maddus and Rogers, 1983).

건강심리이론에서 대응 효능성은 질병의 위협을 감소할 수 있는 행위에 대한 상대적 효과성이라고 정의한다 (Rosenstock, 1974; Rosenstock et al., 1994; Rogers, 1975, 1983). 본 연구에서 대응 효능성이란 대응방안이 개인정보유출의 위협을 회피하는데 얼마나 효과적인지에 대한 주관적인 평가라고 정의할 수 있다. 대응 효능성은 대응방안을 사용함으로서 발생되는 객관적 결과에 대한 사용자의 지각이다. 건강신념모델에서는 이를 지각된 이익(perceived benefits)이라는 변수로 사용하고 있다 (Rosenstock, 1974; Rosenstock et al., 1994). 기존의 건강심이론들과 정보기술 보안연구들에 의하면 대응효능성이 보안행위를 영향을 준다고 하였다. (Anderson and Agarwal, 2006; Ng et al., 2009; Woon et al., 2005).

사람들이 대응방안을 선택할 때는 효과성뿐만 아니라 비용도 고려한다. 대응비용이란 시간, 돈, 불편함, 이해력 등과 같이 대응방안을 사용하기 위해서 발생하는

심리적이고 인지적인 노력을 의미한다. 대응방안이 위협을 감소하는데 효과적이라고 지각할 지라도 이러한 행위가 귀찮고 불편하다고 느낄 수 있다. 따라서 사람들은 개인정보 보호행위를 하려고 할 때 보호행위를 하면서 발생할 수 있는 수익과 비용을 비교하게 되고, 비용이 높다면 건강행위를 하지 않을 수 있다 (Rosenstock, 1974; Rosenstock et al., 1994).

자기효능성이란 건강심리이론의 주요한 선행변수이다. (Rosenstock, 1974; Rosenstock et al., 1994; Rogers, 1975, 1983). 자기효능성은 사회인지이론으로 나온 변수로 어떤 행위를 수행할 수 있는 개인의 능력에 대한 자신감이라고 정의할 수 있다. (Bandura, 1977). 자기효능성은 이전의 정보기술 수용의도를 연구하는 많은 연구들에서 이미 검증되었다. (Bandura, 1977; Compeau et al., 1999; Venkatesh, 2000). 따라서 사용자의 대응방안에 대한 자기확신이 높을수록 지각된 대응성은 더 높을 것이다. 이러한 이론적 배경을 통해서 본 연구에서는 다음과 같은 가설을 설정하였다.

가설 4: 대응 효능성은 지각된 대응성에 긍정적인 영향을 줄 것이다.

가설 5: 대응 비용은 지각된 대응성에 부정적인 영향을 줄 것이다.

가설 6: 자기 효능성은 지각된 대응성에 긍정적인 영향을 줄 것이다.

가설 7: 지각된 대응성은 개인의 정보보행위에 긍정적인 영향을 줄 것이다.

# 3. 연구방법

## 3.1 표본 및 자료수집

본 연구에서는 연구모형을 검증하기 위해 설문조사(survey study)를 통한 실증분석을 실시하였다. 설문조사방법은 온라인 설문이 아닌 설문지를 인쇄하여 직접 설문하였으며, 대학생들과 직장인들을 대상으로 2011년 5월부터 6월까지 2개월에 걸쳐 진행되었다. 회수된 자료를 검증하여 불완전하거나 부적절한 자료를 제외한 결과, 최종적으로 202개의 표본이 분석에 사용되었다.

수집된 표본의 인구통계학적 특성을 분석해보면 다음과 같다. 성별은 남성(58.9%)이 여성(41.1%)보다 많았으며, 연령대는 20대(44.1%)와 30대(34.1%)가 많았다. 40대도 16.8%로 조사되었다. 직업은 직장인(49.5%)이 학생(40.6%)보다 조금 많게 조사되었다. 조사대상자의 인터넷사용특성을 분석한 결과에 의하면, 하루 컴퓨터 사용시간이 6시간 이상(43.1%)이 가장 많았으며, 하루 인터넷 사용시간은 2-3시간(43.6%)이 가장 많게 나타났다. 인터넷을 주로 사용하는 장소로는 회사(49.0%)가 가장 많았으며, 가정(30.7%)이 그 다음으로 많게 나타났다.

## 3.2 설문도구의 개발

본 연구에서는 개인정보의 보호행위에 영향을 주는 요인이 무엇인지를 검증하기 위해 건강심리이론의 변수를 이용하여 설문문항을 개발하였다. 그러나 기존에 개인정보 보호행위에 대한 이론적 연구가 없기 때문에 개인정보 보호행위에 대한 설문문항은 개인정보 보안행위에 대한 실무지침서를 참고하여 직접 설문문항을 개발하였다 (한국인터넷진흥원, 2010).

본 연구는 기본적으로 건강심리이론의 변수들을 그대로 사용하였다. 따라서 본 연구에서 사용한 설문문항은 가능하면 기존 건강심리이론의 문헌연구(Rosenstock, 1974; Rogenstock et al., 1994; Rosers, 1983)으로부터 나온 설문문항과 건강심리이론을 토대로 연구된 정보기술 분야 선행연구(Lee, 2011; Lian and Xue, 2009, 2010; Ng et al., 2009; Woon et al., 2005)의 설문문항을 개인정보의 보호행위에 맞게 수정해서 사용하였다.

본 연구에서는 리커트(Likert) 7점 척도를 이용하여 측정도구를 개발하였으며, 동의여부를 묻는 일반 설문항목을 이용하여 측정도구를 개발하였다. 본 설문을 진행하기에 앞서 개발된 기초문항을 토대로 보안전문가들에게 내용타당도를 검증받았으며, 이를 통해 개인정보의 보안행위를 평가하는 평가도구로써 적당한지, 설문의 표현이 적당한지에 대해 검증받았다.

# 4. 연구결과

## 4.1 측정모형 분석

구조방정식모형을 통해 가설을 검증하기에 앞서서 구조모형에 투입될 설문문항과 요인들의 타당도를 검증하였다. 이를 위해 AMOS 18.0을 이용한 확인 요인분석을 실시하였으며, 이를 통해 집중타당도와 판별타당도를 검증하였다.

먼저 집중타당도를 검증하기 위해서 설문문항과 요인간의 표준요인부하량 (Standardized Factor Loadings: FL >0.7), 개념 신뢰도(Construct Reliability: CR>0.7), 표준분산추출(Average Variance Extracted: AVE>0.5)을 검증하였다(Bagozzi and Yi. 1988). 분석결과는 <부록 1>에 나타나듯이, 모든 설문문항들의 표준요인부하량이 기준치인 0.7 이상으로 나타났으며, 요인들의 개념 신뢰도와 평균분산추출도 모두 기준치인 0.7과 0.5이상으로 나타났다.

다음으로 집중타당도가 검증되었으므로 판별타당도를 검증하였다. 본 연구에서는 요인들 간의 상관계수가 각 요인의 AVE의 제곱근 값보다 작은지를 검증하였다(Chin et al., 1997). 판별타당도를 검증한 결과는 <표 1>과 같으며, 모든 요인들의 상관계수가 AVE의 제곱근보다 낮으므로 판별 타당성이 있는 것으로 나타났다.

최종적으로 측정모형의 적합도는 $\chi 2$=349, p=0.000, $\chi 2$/d.f=1.557, GFI=0.872, NFI=0.908, CFI=0.965, RMSEA=0.053로 전체적으로 적합도 기준을 만족하는 것으로 나타났다.

### 4.2 구조모형 분석 및 가설 검정

최종적으로 구조모형분석을 통해 요인들 간의 인과관계를 검증하였다. 모형의 설명력(SMC: Squared Multiple Correlation)은 지각된 위협=55.2%, 지각된 대응성=37.9%, 개인정보의 보호행위=25.4%로 나타났다. 개인정보의 보호행위에 영향을 미치는 요인을 분석한 결과는 <그림 2>와 같다.

먼저, 지각된 위협(b=0.338)은 개인정보호행위에 긍정적인 영향을 미치는 것으로 나타났다. 지각된 발생가능성(b=0.609)과 지각된 심각성(b=0.249)도 지각된 위협에 긍정적으로 영향을 주는 것으로 나타났으며, 특히 지각된 발생가능성이 지각된 심각성보다 더 큰 영향을 주는 것으로 나타났다. 따라서 가설1, 가설 2, 가설 3은 모두 채택되었다.

다음으로 지각된 대응성(b=0.383)도 지각된 위협과 마찬가지로 개인정보호행위에 긍정적인 영향을 미치는 것으로 나타났다. 대응효능성(b=0.252)과 자기 효능성(0.496)이 지각된 대응성에 긍정적인 영향을 주는 것으로 나타난 반면에 지각된 비용(b=-0.016, p=0.826)은 영향을 주지 않는 것으로 나타났다. 특히, 자기 효능성이 대응효능성 보다 더 큰 영향을 주는 것으로 나타났다. 따라서 가설 4, 가설 6, 가설 7은 채택된 반면에 가설 5는 기각되었다.

가설을 검증한 결과, 총 7개의 가설 중에서 가설 5만 기각되었고, 나머지 6개 가설은 유의한 것으로 나타났다.

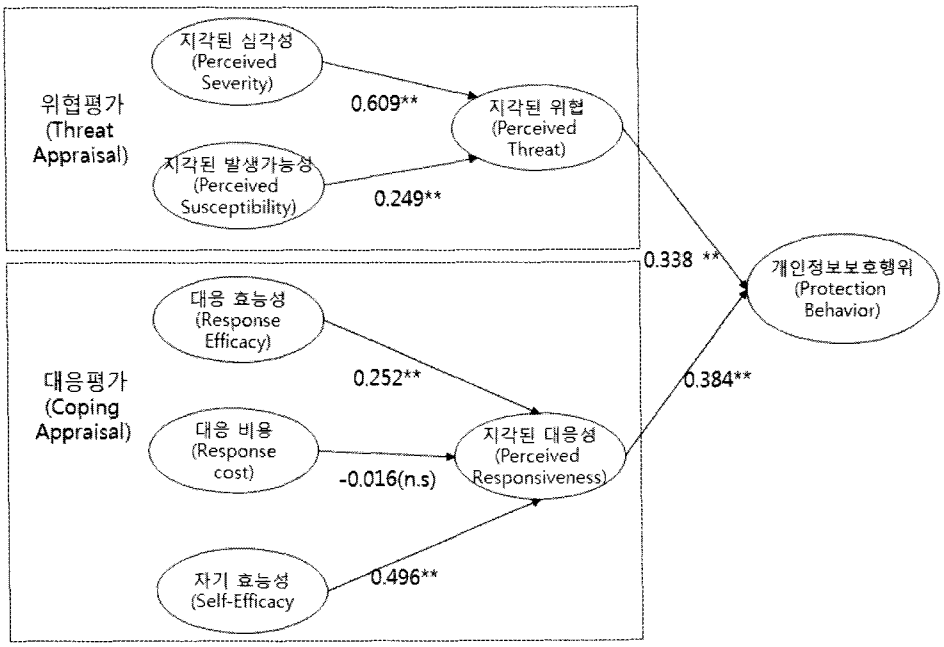
## 5. 결론 및 한계점

### 5.1 논의 및 의의

본 연구는 개인용 컴퓨터 사용자들이 개인정보유출 위협을 피하기 위하여 왜 강력한 비밀번호 사용과 주기적인 비밀번호 변경과 같은 개인정보 보호행위를 수행하는지에 대해서 실증적으로 분석하였다. 본 연구에서는 위협을 질병과 같은 것으로 보고 기존의 정보수용이론과는 달리 건강신념이론을 기반으로 연구를 수행하였다.

**<표 1> 판별타당도 분석결과**

| | 지각된 발생가능성 | 지각된 심각성 | 대응 효능성 | 자기 효능성 | 대응 비용 | 지각된 위협 | 지각된 대응성 | 개인정보 보호행위 |
|---|---|---|---|---|---|---|---|---|
| 지각된 발생가능성 | 0.767 | | | | | | | |
| 지각된 심각성 | 0.397 | 0.892 | | | | | | |
| 대응 효능성 | 0.111 | 0.276 | 0.722 | | | | | |
| 자기 효능성 | -0.047 | -0.211 | 0.264 | 0.761 | | | | |
| 대응 비용 | 0.323 | 0.392 | 0.224 | -0.362 | 0.820 | | | |
| 지각된 위협 | 0.487 | 0.703 | 0.177 | -0.174 | 0.267 | 0.874 | | |
| 지각된 대응성 | -0.293 | -0.099 | 0.375 | 0.572 | -0.131 | -0.141 | 0.852 | |
| 개인정보 보호행위 | 0.265 | 0.303 | 0.309 | 0.05 | 0.136 | 0.268 | 0.342 | 0.725 |




**<그림 2> 구조모형 분석결과**

구체적으로 살펴보면, 지각된 위협은 개인정보보호행위에 긍정적인 영향을 미치는 것으로 나타났으며, 지각된 발생가능성과 지각된 심각성도 모두 지각된 위협에 긍정적으로 영향을 주는 것으로 나타났다. Woon et al. (2005)는 지각된 발생가능성이 보호행위에 영향을 주지 않는 다고 한 반면, Ng et al.(2009)는 지각된 심각성이 영향을 주지 않는다고 하였다. 그러나 대부분의 연구 결과에 의하면 두 개의 변수 모두 보안행위에 영향을 준다고 보고 있다 (Lee, 2011; Liang and Xue, 2010; Workman et al., 2008). 특히 본 연구에서는 지각된 발생가능성이 지각된 심각성 보다 지각된 위협에 더 큰 영향을 주는 것으로 나타났는데, 이러한 결과는 Liang and Xue (2010)의 결과와 유사하다.

따라서 컴퓨터 사용자들이 개인정보 보호행위를 하도록 하기 위해서는 개인정보유출에 대한 위협이 존재한다고 믿게 해야 한다. 만약 사용자들이 위협에 대해서 인지하지 못한다면, 사람들은 개인정보 보호행위를 하지 않을 것이다. 이처럼 위협평가는 개인정보 보호행위를 하도록 하는데 중요하며, 위협을 지각하기 위해서는 개인정보유출 위협의 발생가능성에 대해 인지하고 위협으로부터 발생할 수 있는 위험이 심각하다는 것을 인지해야 한다. 특히, 개인정보유출이 본인에게 발생할 수 있다고 지각하게 하는 것이 더 중요하다고 볼 수 있다.

다음으로 지각된 대응은 개인정보보호행위에 긍정적인 영향을 미치는 것으로 나타났으며, 대응 효능성과 자기 효능성은 지각된 대응에 긍정적으로 영향을 주는 것으로 나타난 반면, 대응 비용은 영향을 주기 않는 것으로 나타났다. 대응 효능성과 자기 효능성이 긍정적인 영향을 주는 것은 기존연구와 같은 결과이다. 그러나 대응 비용이 효과가 없다는 연구결과는 Lee (2011)와 Liang and Xue (2010)의 연구와는 다른 연구결과를 보여주고 있지만, Ng et al. (2009)의 연구 결과와는 일치하고 있다.

이는 Lee (2011)와 Liang and Xue (2010)의 연구와 같이 안티 스파이웨어나 표절보호 소프트웨어와 같은 보안도구를 대상으로 하는 연구에서는 소프트웨어를 설치하는 비용과 시간적 노력이 많이 들기 때문에 대응비용이 부정적인 영향을 주는 것으로 나타난 것으로 보인다. 그러나 Ng et al.(2009)의 이메일 보안행위나 본 연구의 개인정보 보호행위는 특별한 보안도구를 설치하지 않고 개인의 행위를 바탕으로 보안행위가 이루어지기 때문에 대응 비용에 대해서는 중요하게 생각하지 않는 것으로 보인다.

이러한 결과는 대응 효능성과 자기 효능성에 대한 중요성에서도 나타난다. 기존의 연구들에서는 대응 효능성이 자기 효능성보다 더 중요하게 나타난 반면 (Lee, 2011; Liang and Xue, 2010), 개인의 행위가 중심인 본 연구에서는 자기 효능성이 더 큰 영향을 주는 것으

로 나타났다.

본 연구는 다음과 같은 점에서 학문적, 실무적 의의가 있다. 먼저, 학문적으로는 본 연구는 건강심리이론 관점을 기반으로 개인정보보안에 대한 정보보호행위이론을 개발하고자 하였으며, 기존의 정보시스템 연구들이 설명하지 못하는 정보기술 현상에 대해서 설명해 줄 수 있다는 점에서 의의가 있다고 하겠다. 본 연구에서 사용된 건강심리이론의 변수들은 정보시스템연구에서는 상대적으로 새로운 변수이며, 본 연구는 이러한 변수들이 컴퓨터 보안행위를 설명하는데 적합한지에 대해서도 검증해 주었다. 또한 그 동안 정부 및 정보보안 부서에서 제시하고 있는 정보보안방법들, 특히 개인정보 보안행위지침에 대한 효과를 검증함으로써 보안분야 연구의 한계점인 이론적 배경을 마련해 줄 수 있을 것으로 기대한다.

실무적으로 본 연구는 사람들이 어떻게 위협을 평가하고, 해결책을 찾고, 궁극적으로 보호행위를 수행함으로써 개인정보유출 위협을 피하는지를 이해할 수 있는 평가틀을 제공함으로써 보안 실무자들에게 중요한 의미를 줄 수 있다. 본 연구의 결과를 토대로 보안 실무자들은 사람들이 개인정보유출 위협을 피할 수 있는 보호행위를 하도록 하기 위해서는 정보기술의 위협 및 대응방안을 평가하는 두 가지 인지적 프로세스가 중요하다는 것을 알아야 한다.

개인정보유출에 대한 위협지각을 높이기 위해서는 위협의 심각성과 특히 개인정보유출에 대한 위협이 본인에게 발생할 가능성이 매우 높다는 것을 인지시켜주어야 한다. 따라서 기업이 보안교육을 실시하거나 정부의 보안 캠페인을 설계할 때 개인정보 유출에 대한 위협과 더불어 발생가능성이 높다는 것을 인지시켜줄 수 있는 문안을 만드는 것이 중요하다. 또한 본 연구모형은 보안 담당자들이 정보보안에 대해서 종업원들을 교육시킬 때 좀 더 효과적인 방법을 설계할 수 있도록 도움을 줄 수 있을 것이다.

### 5.2 한계점 및 추후 연구과제

이러한 연구 결과 및 의의에도 불구하고 본 연구는 한계점을 가지고 있다. 본 연구에서는 여러 가지 컴퓨터 보안행위 중에서 개인정보보안이라는 한 가지를 선택해서 연구하였다. 따라서 PC보안, 인터넷보안, SNS 보안, 스마트폰 보안 등 다른 형태의 보호행위에 본 연구의 결과를 일반화시키기에는 무리가 있을 수 있다. 따라서 추후에는 여러 가지 컴퓨터 보안에 대한 다양한 연구들이 이루어진다면 컴퓨터 보안행위에 대한 공통된 인과관계를 밝혀내는데 도움이 될 것이다.

## 참고문헌


[1] 방송통신위원회, 행정안전부, 지식경제부(2011), 「2011 국가정보 보호백서」

[2] 한국인터넷진흥원(2010), 「정보보호 관련 대국민 홍보 방안 연구」

[3] Ajzen, I. (1991), "The theory of Planned behavior," *Organizational Behavior & Decision Processes*, Vol. 50, pp. 179-211.

[4] Anderson, C.L. and R. Agarwal (2006), "Practicing Safe Computing: Message Framing, Self-View, and Home Computer User Security Behavior Intentions," *in International Conference on Information Systems*, pp. 1543-1561. Milwaukee, WI.

[5] Bagchi, K. and G. Udo (2003), "An analysis of the growth of computer and internet security breaches," *Communications of the AIS*, Vol. 12, pp. 684-700.

[6] Bagozzi, R.P. and Y. Yi (1998), "On the Evaluation of Structural Equation Models," *Journal of the Academy of Marketing Science*, Vol. 16 No. 2, pp. 74-94.

[7] Bandura, A. (1977), "Self-efficacy: Toward a unifying theory of behavior change," *Psychological Review*, Vol. 84, pp. 191-215.

[8] Carver, C.S. and T.L., White (1994), "Behavioral inhibition, behavioral activation, and affective responses to impending reward and punishment: the bis/bas scales," *Journal of Personality and Social Psychology*, Vol. 67, pp. 319-333.

[9] Chin, W.W., B.L. Marcolin and P.R. Newsted (2003), "A partial least squares latent variable modeling approach for measuring interaction effects: Results from a monte carlo simulation study and an electronic-mail emotion/adoption study," *Information Systems Research*, Vol. 14 No. 2, pp. 189-217.

[10] Chung, W., H. Chen, W. Chang and S. Chou (2006), "Fighting cybercrime: a review and the taiwan experience," *decision support systems*, Vol. 41, pp. 669-682.

[11] Claar, C.L. (2011), "The adoption of computer security: An analysis of home personal computer user

behavior using the health belief model," *All graduate theses and dissertations*, utah state university, Logan, Utah.

[12] Compeau, D.R., C.A. Higgins, and S. Huff (1999), "Social cognitive theory and individual reactions to computing technology: a longitudinal study," *MIS Quarterly*, Vol. 23 No. 2, pp. 145-158.

[13] Davis, F.D. (1989), "Perceived usefulness, perceiv ed ease of use, and user acceptance of information technology," *MIS Quarterly*, Vol. 13 No. 3, pp. 319-338.

[14] Dinev, T. and Q. Hu (2007), "The centrality of awa reness in the formation of user behavioral intention toward protective information technologies," *Journal of the Association for Information Systems*, Vol. 8 No. 7, pp. 386-408.

[15] Elliot, A.J. (2006), "The hierarchical model of appr oach-avoidance motivation," *Motivation and Emoti on* Vol. 30, pp. 111-116.

[16] Elliot, A.J. and M.V., Covington (2001). "APPROA CH AND AVOIDANCE MOTIVATION," *Educational Psychology Review*, Vol. 13(2), pp. 73-92.

[17] Fishbein, M. and I., Ajzen (1975), Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research, Reading, MA: Addison-Wesley.

[18] Jayanti, R.K. and A.C., Burns (1998), "The antecede nts of preventive health care behavior: an empirical study," *Academy of Marketing Science Journal*, Vol. 26 No. 1, pp.6-15.

[19] Kankanhalli, A., H.H., Teo, B.C.Y. Tan and K.K., Wei (2003), "An integrative study of information systems security effectiveness," *International Journal of Information Management*, Vol.23, pp. 139-154.

[20] LaRose, R., N., Rifon, S., Liu and D., Lee (2005), "Online safety strategies: a content analysis and theoretical assessment," *The 55th Annual Confer ence of the International Communication Associa tion*, New York City.

[21] Lee, Y. (2011), "Understanding anti-plagiarism sof tware adoption : An extended protection motivation theory perspective," *Decision Support Systems*, Vol.50, pp.361-369.

[22] Liang, H. and Y. Xue (2009), "Avoidance of in-formation technology threats: A theoretical per-spective," *MIS Quarterly*, Vol.33 No. 1, pp.71-90.

[23] Liang, H. and Y. Xue (2010), "Understanding Secu rity Behaviors in Personal Computer Usage: A threat Avoidance Perspective," *Journal of the Asso ciaton for Information Systems*, Vol. 7 No. 2, pp. 393-413.

[24] Maddus, J.E. and R.W., Rogers (1983), "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *Journal of Exper imental Social Psychology*, Vol. 19, pp. 469-479.

[25] Ng, B.Y., A., Kankanhalli and Y.C., Xu (2009), "Studing users' omputer security behavior; A health belief perspective," *Decision Support System*, Vol. 46 No. 4, pp. 815-825.

[26] Oliver, R.L. and P.K., Berger (1979), "A path analy-sis of preventive health care decision models," *Journal of Consumer Research*, Vol.6 No. 2, pp. 113-122.

[27] Rhodes, K. (2001), "Operations security aware-ness: the mind has no firewall," *Computer Security Journal*, Vol. 16 No. 2, pp. 27-36.

[28] Rippetoe, P.A. and R.W., Rogers (1987), "Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat," *Journal of Personality and Social Psycho logy*, Vol. 52 No. 3, pp. 596-604.

[29] Rogers, R.W. (1975), "A protection motivation the ory of fear appeals and attitude change," *Journal of Psychology*, Vol. 91, pp. 93-114.

[30] Rogers, R.W. (1983), "Cognitive and physiological process in fear appeals and attitude change: A re-vised theory of protection motivation," in Social Psychophysiology: A Source Book, R. Petty (ed.), New York : Guilford Press, pp. 153-176.

[31] Rosenstock, I.M. (1974), "The health belief model and preventive health behavior," *Health education Monographs*, Vol. 2, pp. 354-386.

[32] Rosenstock I., V., Strecher, and M., Becker (1994), "The Health Belief Model and HIV risk behavior change", In R.J. DiClemente & J.L. Peterson (Eds.), Preventing AIDS: Theories and methods of behav-ioral interventions (pp. 5-24). New York, NY: Plenum Press.

[33] Stanton, J.M., P.R., Mastrangelo, K.R., Stam and J., Jolton (2004), "Behavioral information security: two end user survey studies of motivation and se-curity practices," *Proceedings of the Tenth America' Conference on Information Systems*, New York, 2004.

[34] Steers, R.M., R.T., Mowday and D.L., Shapiro (2004), "The future of work motivation theory," *Academy*

*of Management Review*, Vol.29(3), pp. 379-387.

[35] Venkatesh, V. (2000), "Determinants of perceived ease of use : Integrating control, intrinsic motivation, and emotion into the technology acceptance model", *Information System Research*, Vol.11 No. 4, pp.342-365.

[36] Weinstein, N.D. (2000), "Perceived probability, perceived severity, and health-protective behavior," *Health Psychology*, Vol. 19 No. 1, pp. 65-74.

[37] Woon, I., G.W., Tan, and R., Low (2005), "A protection motivation theory approach to home wireless security," *International Conference on Information Systems*, pp. 367-390.

[38] Workman, M., W.H., Bommer and D., Straub (2008), "Security lapses and the omission of information security measures: A threat control model and empirical test," *Computers in Human Behavior*, Vol. 24 No. 6, pp. 2799-2816.

2011년 9월 9일 접수, 2011년 9월 19일 수정, 2011년 9월 22일 채택

## 부 록 : 설문문항 및 확인적 요인분석 결과

| 요인 | 문항 번호 | 설문문항 | 요인 적재량 | CR | AVE |
|---|---|---|---|---|---|
| 지각된 발생가능성 (Perceived Susceptibility) | SUS1 | 나는 내 개인정보가 유출될 가능성이 높다고 생각한다. | 0.808 | 0.810 | 0.588 |
| | SUS2 | 나는 내 신용카드 정보가 유출될 가능성이 높다고 생각한다. | 0.888 | | |
| | SUS3 | 나는 내 아이디와 비밀번호가 도용될 가능성이 높다고 생각한다. | 0.774 | | |
| 지각된 심각성 (Perceived Serverty) | SER1 | 내 개인정보가 유출되어 사이버 범죄에 악용된다는 것은 나에게는 매우 심각한 문제이다. | 0.915 | 0.921 | 0.796 |
| | SER2 | 내 개인정보도용으로 경제적인 피해를 입는다는 것은 나에게는 매우 심각한 문제이다. | 0.947 | | |
| | SER3 | 내 개인정보가 유출되어 내 사생활이 침해당한다는 것은 나에게는 매우 심각한 문제이다. | 0.887 | | |
| 대응 효능성 (Response Efficacy) | EFF1 | 영문/숫자 등을 조합하여 남들이 알수 없는 패스워드를 사용한다면 개인정보 유출을 효과적으로 막을 수 있을 것이다. | 0.829 | 0.766 | 0.522 |
| | EFF2 | 정기적으로 패스워드를 변경한다면 개인정보 유출을 효과적으로 막을 수 있을 것이다. | 0.809 | | |
| | EFF3 | 개방환경(PC방 또는 공공장소)에서 금융거래를 하지 않는다면 개인정보 유출을 막을 수 있을 것이다. | 0.762 | | |
| 대응 비용 (Response Cost) | COS1 | 정기적으로 비밀번호를 변경하는 것은 매우 불편하다. | 0.807 | 0.860 | 0.672 |
| | COS2 | 사이트마다 다른 아이디와 비밀번호로 관리하는 것은 많은 시간과 노력이 필요하다. | 0.905 | | |
| | COS3 | 비밀번호를 안전하게 유지관리하는 것은 많은 노력이 소요된다. | 0.870 | | |
| 자기 효능성 (Self-efficacy) | SEL1 | 누가 말해주지 않아도 정기적으로 비밀번호를 쉽게 변경할 수 있다. | 0.864 | 0.805 | 0.579 |
| | SEL2 | 사이트마다 다른 아이디와 비밀번호로 관리하는 것은 쉽다. | 0.908 | | |
| | SEL3 | 비밀번호를 안전하게 유지하는 것은 쉽다. | 0.880 | | |
| 지각된 위협 (Perceived Threat) | THR1 | 개인정보유출은 나에게 심각한 위협이 되고 있다. | 0.888 | 0.906 | 0.764 |
| | THR2 | 개인정보유출로 인해 발생하게 되는 문제는 나에게 위협이 되고 있다. | 0.931 | | |
| | THR3 | 내 아이디와 비밀번호의 도용은 나에게 위협이 되고 있다. | 0.823 | | |
| 지각된 대응성 (Perceived Responsiveness) | RES1 | 내 개인정보는 인터넷 환경에서 잘 보호되고 관리되고 있다. | 0.897 | 0.888 | 0.725 |
| | RES2 | 내 신용카드 정보는인터넷 환경에서 잘 보호되고 관리되고 있다. | 0.870 | | |
| | RES3 | 내 아이디와 비밀번호는 인터넷 환경에서 잘 보호되고 관리되고 있다. | 0.951 | | |
| 개인정보보호행위 (Protection Behavior) | BEH1 | 회원가입시 비밀번호를 타인이 유추하기 어렵도록 영문/숫자 등을 조합하여 8자리 이상으로 설정한다. | 0.798 | 0.769 | 0.526 |
| | BEH2 | 자신의 아이디나 비밀번호를 친구나 타인에게 알려주지 않는다. | 0.783 | | |
| | BEH3 | 잘 모르는 사이트에 회원가입을 하지 않으며, 회원가입시에도 꼭 필요한 정보만 입력한다. | 0.782 | | |