보안습관이 데이터백업에 미치는 요인
-보호동기이론을 중심으로-

김종기 (부산대학교 경영대학 경영학과 교수, 주저자 jkkim1@pusan.ac.kr)
김지윤 (부산대학교 경영대학 경영학과 박사과정, 교신저자 wowtnt@pusan.ac.kr)

Determinants of Data Back Up: Focused on Protection Motivation Theory

Jong-Ki Kim (Professor, Dept. of Business Administration,
College of Business, Pusan National Universityy)
Ji-Yun Kim (Graduate Student, Dept. of Business Administration,
College of Business, Pusan National University)

-원고매수: 00 페이지

[교신저자 연락처]
◎ 김지윤
◆ 주소 : 부산광역시 금정구 부산대학로 63번길2 부산대학교 경영대학 경영학과
◆ 전화번호: 051-510-2582
◆ 휴대폰: 010-9131-7836
◆ E-mail주소: wowtnt@pusan.ac.kr

보안습관이 데이터백업에 미치는 요인
-보호동기이론을 중심으로-
Determinants of Data Backup: Focused on Protection Motivation Theory

● 목차 ●

··· Abstract ···

This study uses Protection Motivation Theory as a theoretical framework to empirically test what people make back up data on their personal computers. Sources of information are the input variables to Protection Motivation Theory and include environmental and intrapersonal sources. Intrapersonal sources include personality aspects and feedback from prior experience including experiences associated with performing the behavior of interest.
In the context of IS security, many of approaches use an incomplete view of the cognitive mediating processes central to Protection Motivation Theory. Furthermore, past experience may be considered to be an important source of information influencing protection motivation. To address this, we integrated security habit as a background factor with Protection Motivation Theory to investigate sources of information antecedent to the Protection Motivation Theory process.

Key Words : Protection Motivation Theory, Information Security, Source of Information, Security Habit, Data Backup

Ⅰ. 서 론

인터넷과 IT 서비스의 활성화는 네트워크를 통한 손쉬운 정보 공유와 상호교류를 가능하게 만든 반면, 다양한 형태의 보안위협으로부터 데이터가 유실되거나 손상될 수 있는 상황이 되었다. 시간이 갈수록 보안위협의 형태는 물론 그 강도도 커지고 있는 현실에서 컴퓨터 사용자의 데이터에 대한 보안위협을 줄이고 데이터를 보호하기 위한 적합한 대응방법을 생각해 볼 필요가 있다.

인터넷의 특성인 개방형 구조는 바이러스(virus), 웜(worms), 스파이웨어(spiware, 트로이목마, 봇넷(botnets), 서비스거부공격(DDos), 개인정보유출 등과 같은 악의적인 정보기술에 노출되기 쉽다(Bagchi and Udo, 2003; Liang and Xue, 2010; Ng et al., 2009; Whiman, 2003). 실제 보안업체에서 실시한 '2016 보안 인식 설문조사'에서 본인 또는 주변에서 보안 피해를 경험한 비율이 51.2%의 심각한 수준으로 조사되었다(이스트소프트, 2016). 컴퓨터 사용자가 경험하게 되는 사이버 범죄의 하나는 중요한 문서를 훔치고 파괴하는 공격으로 바이러스, 웜, 트로이 목마, 해킹, 악성프로그램, 서비스 거부공격 등을 들 수 있다(Crossler, 2010). 특히 2016 상반기 보안업체들이 가장 주목하는 것은 랜섬웨어의 공격이다. 새로운 형태의 신·변종 랜섬웨어가 꾸준히 출현하고 더욱 지능적으로 변하여 사용자에게 큰 심리적 위협을 가함으로써 금품 갈취를 시도하는 것으로 분석되었다(이스트소프트, 2016). 이처럼 사이버 공격의 양상이 변화하면서 사이버 범죄조직으로까지 확장되고 있어 앞으로 더 큰 피해가 우려된다.

정보보호의 목적은 보안위협으로부터 정보를 보호하고 예방하는 것이다. 대부분의 정보보호 관련 연구들은 바이러스나 스파이웨어에 대응하는 백신과 같은 기술적 측면의 연구와 법적 또는 제도적 장치에 대한 정보보안 방법론이 중심이었다. 단순히 보호도구를 수용하는 관점의 접근은 정보보호의 일부분만을 연구하게 되므로 정보보호에 대한 부분적 이해만이 가능할 수 있다(Ng et al., 2009; Liang and Xue, 2010). 다양한 위협으로부터 정보를 보호하기 위해 사회적으로 법과 제도적 장치를 마련하고, 보안위협에 대한 정보와 교육을 제공하고 있지만(Chung et al., 2006; Ng et al., 2009), 정보보호는 제도적·기술적 노력만으로 해결될 수 있는 문제가 아니며, 개별사용자의 위험관리 노력이 더 중요하다(Ng et al., 2009; Anderson and Agarwal, 2006, Woon et al., 2005). 즉, 정보보호에서 사람은 가장 위험한 요소이면서, 해결책으로 인식되는 요소(Finne, 2000)이므로 정보를 보호하려는 행동의 관점이 중요할 것이다.

기술적 측면의 보안대책이 정보보호를 도울 수 있지만(Straub, 1990) 보안위협을 충분하게 해결할 수는 없다(Cavusoglu et al., 2009; Dhillon and Backhous, 2001). 즉, 시시각각 출현하는 신·변종 악의적 정보기술의 공격에 대한 기술적 보안대책은 창과

방패의 관계와 같이 선제대응이라기 보다는 즉시적 후발대응에 가깝기 때문에 완벽히 방어할 수 없다. 또한 사용자의 부주의나 실수에 의해 언제든 발생할 수 있어 피해가능성은 언제나 열려있는 것이다. 따라서 데이터 백업과 같은 추가대응을 통해 데이터를 복구함으로써 예방과 보호라는 정보보호의 궁극적 목적을 실현할 수 있을 것이라 판단된다.

본 연구는 위협으로부터 보호하려는 행동과 관련한 개인의 의도를 예측하는 보호동기이론을 중심으로 컴퓨터 사용자의 백업에 대한 요인을 파악하고자 한다. 건강, 심리 등 다양한 사회 인지적 차원의 보호행동을 설명하기 위해 연구되고 있는 보호동기이론은 IS분야에서도 꾸준히 활용되고 있으므로, 보안위협으로부터 정보를 안전하게 보호하기 위한 백업의도의 영향요인을 알아보고자 하는 본 연구에 적용할 수 있다.

특히, 본 연구는 개인의 백업행동을 유발하는 과정에 선행하는 배경요인에 주목한다. 일상생활에서 무의식적이고 반복적으로 수행된 보안행동들이 보안습관을 형성한 결과가 보호동기를 일으켜 정보를 보호하기 위한 개인의 백업행동에 미치는 영향에 대해 논의하고자 한다. 이는 기존의 연구들에서 보호동기이론의 핵심부분에만 집중하였던 것과 구별되는 것으로 인지적 매개과정에 영향을 미치는 배경요인이 충분히 고려되지 못했음을 감안한 것이다.

Ⅱ. 이론적 배경

1. 정보보호와 데이터 백업

한국정보통신기술협회의 정의에 따르면 위협은 자산에 손실을 발생시키는 원인이나 행위 또는 보안에 해를 끼치는 행동이나 사건을 의미하고, 정보 보호(information security)는 정보의 수집·가공·저장·검색·송신·수신 중에 정보의 훼손·변조·유출 등을 방지하기 위한 관리적·기술적 수단, 또는 그러한 수단으로 이루어지는 행위를 말한다. 정보를 보호한다고 하면 흔히 정보가 유출되는 것을 막는 것만을 생각하지만 정보보호는 그것 이상의 개념으로, 보호대상이 되는 정보의 기밀성(confidentiality), 무결성(integrity), 가용성(availability)이 모두 만족되었을 때 정보가 안전(security)하다고 할 수 있다(신승중 외, 2005). 기밀성은 허가받지 않은 대상에게는 정보가 제공되어서는 안된다는 것이고, 무결성은 정보가 정확해야 하므로 허가 없이는 수정될 수 없도록 하는 것이며, 가용성은 허가된 접근의 경우 정보에 대한 접근이 가능해야만 한다는 것을 말한다. 즉, 정보보호란 해킹, 개인정보유출, 악성코드감염, 랜섬웨어 감염, 디도스 공격과 같은 다양한 보안위협으로부터 정보자산을 안전하게 지키기 위한 모든 보

호행동이라 할 수 있다.

데이터 백업(data backup)은 데이터를 미리 임시로 복제하여 문제가 일어나도 데이터를 복구할 수 있도록 준비해두는 것을 의미한다. 백업에 대한 선행연구들은 백업 기법에 대한 기술적 연구와 운영에 관한 연구들이 대부분으로 직접적인 보호조치와 관련한 연구는 많지 않다. Crossler(2010)는 악의적인 정보기술의 공격으로 잃게 된 파일들을 되살리는 방법으로 중요한 파일과 폴더들을 정기적으로 백업하는 것을 들고 있다. 양원석 외(2014)는 데이터의 손상과 유실을 방지하는 최종적 방법으로 데이터 백업의 중요성을 주장한다. 그러나 악성코드와 같은 악의적인 정보기술에 의해 데이터가 손상되었을 때 중요한 데이터를 백업해두지 않았다면 그 데이터는 영원히 잃게 되는 것이 분명함에도 불구하고, 컴퓨터 사용자들은 정기적으로 백업을 수행하지 않는다(Karabacak and Sogukpinar, 2005).

한편, 한국인터넷진흥원에서 배포한 '랜섬웨어 피해 예방 5대 수칙'에서도 소중한 자료를 지키는 방법 중 하나로 백업을 권장하고 있다. 주목할 것은 2004년 한국정보보호진흥원에서 '정보보호 실천수칙'을 통해 중요문서에 대한 백업을 생활화할 것을 권장했으나, 2009년 한국인터넷진흥원으로 통합 이후 '한국인터넷진흥원의 안전하고 건전한 정보보호 생활가이드'(2009), '정보보호 실천수칙'(2016) 등의 가이드에서는 백업과 관련한 내용이 빠졌다가 최근 랜섬웨어와 관련한 가이드에 포함되었다는 것이다. 이러한 사실은 지능적인 신·변종 보안위협이 증가함에 따른 보호조치로서, 백업이 중요해졌음을 반영한 것으로 생각할 수 있다.

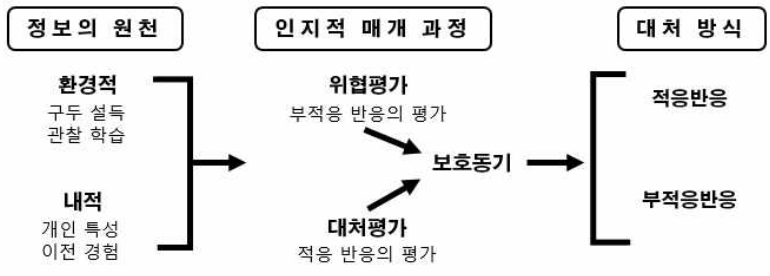
2. 보호동기이론

보호동기이론(Protection Motivation Theory)은 보호 행동과 관련한 개인의 의도를 예측하기 위한 가장 강력한 설명적 이론 중 하나로 주목받는 이론이다(Ifinedo, 2012). 보호동기이론은 기대-가치 이론(Expectancy-Value Theory)과 인지적 처리 이론(Cognitive Processing Theory)을 기반으로 공포소구(fear appeal)를 설명하기 위해 발전하였으며, 개인이 어떻게 위험을 인지적으로 처리하고 반응하는가를 설명한다(Maddux and Rogers, 1983; Ifinedo, 2012; Boss et al., 2015).

초기 보호동기이론은 기대-가치 이론을 기반으로 개인이 공포를 직면한 후 행동의 변화를 설명한 것으로, 위협에 대한 대처와 관련 프로세스를 설명하면서 인지된 취약성(perceived vulnerability), 인지된 심각성(perceived security), 반응 효능감(response efficacy)의 요인을 확인하였다(Rogers, 1975). 이어진 후속연구에서 자기효능감(self efficacy), 보상(reward), 반응비용(response cost), 정보의 원천(source information)이 추가되며 수정되었다(Rogers, 1983; Maddux and Rogers, 1983; Sommestad et al.,

2015).

보호동기이론의 전체 모델은 <그림 1>과 같이 정보의 원천으로부터 시작해 인지적 매개과정을 통해 대처 방식으로 이어진다. 정보의 원천은 환경적 원천과 내적 원천으로 구분되며 환경적 원천으로는 구두 설득과 관찰학습, 내적 원천으로는 성격적 측면과 이전 경험으로부터의 반응 등으로 구성된다. 인지적 매개과정은 위협평가와 대처평가로 나뉜다. 위협평가는 위협적인 사건의 위험 수준에 대한 개인의 평가를 의미하며 인지된 취약성과 인지된 심각성으로 구성된다. 인지된 취약성은 위협적인 사건이 발생하게 될 가능성의 정도를 의미하고, 인지된 심각성은 그 위협적인 사건으로 인한 피해의 심각성 정도를 의미한다. 대처평가는 자기효능감, 반응효능감, 반응비용으로 구성된다. 자기효능감은 위협으로부터 발생하는 잠재적 손실을 방지하고 대처하는 능력에 대해 자기가 가지고 있는 확신의 정도를 의미하고, 반응효능감은 권장된 행동을 수행했을 때 얻어지는 혜택에 대한 믿음을 의미하며, 반응비용은 시간, 돈, 노력 등의 관점에서 지각되는 기회비용을 의미한다. 대처반응은 위협을 줄이고자하는 행동인 적응반응(adaptive responses)과 위험에 대한 부인 또는 무시와 같은 부적응 반응(maladaptive responses)으로 구성된다.



<그림 1>보호동기이론 전체 모델(Floyd et al., 2000)

보호동기이론은 보건학, 사회심리학, 환경 등 다양한 분야에서 사회 인지적 차원의 보호행동을 설명하기 위해 연구되고 있으며 IS 분야의 연구에서도 다양하게 적용하고 있다. 또한, 정보보호분야에서도 특정 보호행동을 설명하기 위해 보호동기이론을 기반으로 한 연구가 수행되고 있다. Rogers and Prentice-Dunn(1997)는 광범위한 연구를 통해 보호동기이론이 다양한 주제의 연구에 적용되었음을 밝히며, 보호동기가 개인이 효과적인 권장반응(recommended response)을 수행할 수 있는 모든 위협과 관련이 있음을 밝혔다. 이와 같은 선행연구를 바탕으로 본 연구에서는 보안위협으로부터 정보를 안전하게 보호하기 위한 백업행동에 미치는 요인을 확인하기 위해 보호동기이론을 적용하고자 한다.

3. 배경요인

사회인지이론(Social Cognitive Theory)에서는 개인의 행동은 개인의 특성, 환경적 요인, 행동이 상호작용에 따른다고 설명한다(Bandura, 1986). 즉, 한 개인의 행동은 내부의 힘 또는 외부의 자극 하나만으로 이루어지는 것이 아니라 환경적 요인, 행동적 요인, 개인의 인지적 요인이 맞물려 서로 영향을 미친다는 것이다. 사회인지이론은 지식이나 태도보다 행동변화에 초점을 맞추고 환경의 영향에 대해 가치를 두는 것이 특징이다.

Ajzen and Albarracin(2007)은 합리적행동이론을 적용한 연구에서 배경요인의 잠재적 중요성을 인식하고 행동 등에 간접적으로 영향을 미칠 수 있는 행동과 관련한 추가적인 요인들을 선정하여 그 역할을 확인하였다. Fishbein and Ajzen(2010)은 배경요인을 연구에 포함하는 것이 행동의도에 대한 보다 정확한 설명과 행동의 근원에 대한 통찰력을 가질 수 있다고 주장한다. 안호주 외(2015)는 보호동기이론과 합리적행동이론이 인지이론임을 이유로, 인간의 동기와 인지의 바탕이 되는 배경지식과 관련한 요인을 포함하고 있으며, 그 배경요인이 인지요인과 보호동기에 영향을 주거나 개인적 차이를 발생시켜 간접적으로 행동의도에 영향을 준다고 설명한다. 배경요인은 설득, 관찰학습, 성격, 경험, 지식, 미디어 노출 등 다양한 요인들로 표현될 수 있다(Bandura, 1986; Fishbein and Ajzen, 2010; Floyd et al., 2000).

보호동기이론의 대부분 연구는 핵심부분인 인지적 매개 과정에 집중하고 있는 실정이다. IS분야에서 보호동기이론의 배경요인을 적용한 연구를 살펴보면 다음 <표 1>과 같다.

<표 1> 보호동기이론의 배경요인을 적용한 선행연구

연구자	배경요인	적용이론	연구내용
Siponen et al.(2006)	<환경적 영향> 규범적 신뢰, 가시성	TRA, PMT	IS보안정책준수에 대한 환경적 영향
Vance et al.(2012)	<정보의 출처> 습관	PMT	IS보안정책준수에 대한 환경적 영향
Tu et al.(2015)	<정보의 출처> 지식, 경험 사회적영향,	PMT, 사회학습이론	분실과 도난으로 인한 모바일 장치의 정보보안위험 대응
안호주 외(2015)	<배경요인> 보안인식교육, 보안회피습관	PMT	금융기관 종사자의 정보보안위험관리에 대한 영향.

이와 같은 선행연구를 바탕으로 본 연구에서는 배경요인의 잠재적 영향력을 고려하기 위해 보안습관을 보호동기이론의 배경요인으로 설정하고 보호동기이론의 주요 요인에 대한 영향을 확인하고자 한다.

4. 습관

습관(habit)에 대한 일반적인 정의는 특정한 목표나 최종상태를 얻고자 하는 특정 상황에 대한 자동적 반응과 같은 행동의 학습된 결과이다(Verplanken et al., 1997; Limayem et al., 2003). IS분야의 연구에서 습관은 IS습관, 보안습관, 습관적 사용 등 다양한 개념으로 사용되고 있다. 이론적 정의를 살펴보면 학습을 통한 자동적 행동 경향(Limayem et al., 2001; Khalifa et al., 2002; Limayem and Hirt, 2003; Limayem et al., 2007), 목표지향 자동적 행동(Limayem et al., 2003; Wu and Kuo, 2008; Kim et al., 2005), 행동적 선호도(Gefen, 2003), 의식적 관심을 벗어나 발생하는 행동(Kim and Malhotra, 2005) 등이다.

보호동기이론의 전체 모델에서는 이전 경험이 인지처리과정의 선행요인으로 사용되고 있다. 또한, 상황적 단서와 습관이 보호행동을 수행하는 의사결정 과정에 대한 중요한 영향을 가정하고 있다(Maddux, 1993). Aart et al.(1998)은 보호동기이론이나 합리적 행동이론에서 매일, 반복적이며, 일상화 되거나 습관화 된 행동이라는 중요한 관점을 간과하고 있음을 지적한다. Yoon et al.(2012)은 보안행동은 매일 밤 잠들기 전 문단속을 하는 행동처럼 반복되는 행동으로 여겨질 수 있음을 예로 들어, 안전 조치와 같은 정보 보안 행동이 반복적인 행동을 통해 일상화 되거나 습관이 될 수 있다고 주장하면서, 보안습관이 학생들의 보안행동 의도에 유의한 영향을 미치는 것을 확인했다. Vance et al.(2012)은 습관이론을 통해 습관을 일상화된 행동의 형태로 정의하고, 행동을 위한 자각적 결정 없이 발생되고 그러한 수행에 익숙해져 수행되는 많은 행동으로 설명한다.

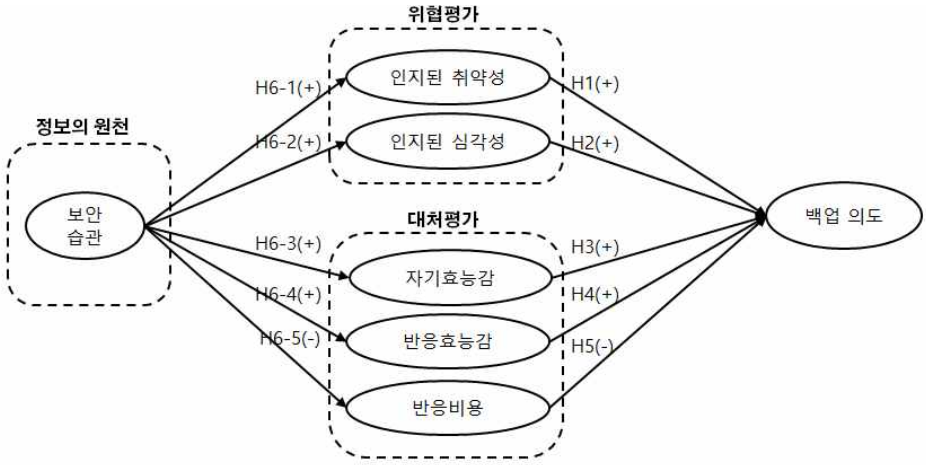
IS분야의 연구에서 습관에 대한 접근형태는 의도와 IT사용사이의 조절효과, IT사용에 대한 직접효과, IT사용의도에 대한 직접효과 등이 일반적이다. 본 연구에서는 Vance et al.(2012)과 안호주 외(2015)의 연구를 바탕으로 보호동기이론의 주요 요인에 대한 습관의 영향을 논의하고자 한다.

Ⅲ. 연구모형 및 가설

1. 연구모형

본 연구는 이론적 배경을 기반으로 선행연구에서 실증적으로 분석한 연구변수를 도출하여 <그림 2>와 같은 연구모형을 개발하였다. 연구목적을 달성하기 위하여 선행연구에 대한 포괄적인 검토를 거쳐 정보보호 행동과 관련한 주요 연구변수로 보안습관, 인지된 취약성, 인지된 심각성, 자기효능감, 반응효능감, 반응비용, 등을 선정하

였으며, 구성개념을 도출하고 이들 변수간의 관계에 대한 가설을 정립하였다.



<그림 2> 연구 모형

2. 연구가설

1) 보호동기이론의 요인과 백업의도 간의 관계

정보보호와 관련한 연구에서 보호동기이론의 요인들은 의도와 같은 보호동기에 대해 유의한 영향을 미치며 실제 행동과도 관계가 있다고 알려져 있다(Floyd et al., 2000; Milne et al., 2000). 따라서 본 연구에서는 컴퓨터 사용자의 백업의도에 대한 영향요인으로 보호동기이론의 주요 요인들을 설정하고자 한다.

인지된 취약성은 위협적인 사건이 발생할 수 있는 가능성 정도를 말한다(Rogers, 1975; Johnston and Warkentin, 2010). Ifinedo(2012)는 인지된 취약성을 위협적인 사건의 발생 가능성에 대한 개인의 평가로 정의하고 보안정책 불이행으로 인한 위협의 발생 가능성 정도를 설명하였다. 위협에 대한 취약성을 높이 인지할수록 보안정책을 준수하려하고(Ifinedo, 2012), 개인정보를 보호하려 하는 것으로(박찬욱, 2014) 나타났다. 반면, Crossler(2010)의 연구에서는 개인데이터의 백업에 유의한 부의 영향을 나타냈다.

선행연구의 결과를 바탕으로 보안위협으로 인해 데이터가 손상될 가능성을 높이 인지하면 백업의도가 높아질 것이라는 가설을 설정하였다.

H1: 인지된 취약성은 백업의도에 정(+)의 영향을 미칠 것이다.

인지된 심각성은 위협적인 사건의 결과에 대한 심각성(Ifinedo, 2012), 위협적인 사건에 의해 발생하는 부정적 결과에 대한 개인의 주관적 평가(Liang and Xue, 2010)이다. 보안위협의 심각성을 높이 인지할수록 보안정책 준수의도가 높아지고(Ifinedo, 2012), 안티-멀웨어프로그램 수용의도를 높이며(Lee and Larsen, 2009), 백업의도를 높이는 것으로(Boss et al., 2015) 나타난 반면 Crossler(2010)의 연구에서는 개인데이터의 백업에 유의한 부의 영향을 나타냈다.

선행연구의 결과를 바탕으로 보안위협으로 인한 데이터의 손상을 심각하게 생각하면 백업을 하고자 할 것이라는 가설을 설정하였다.

H2: 인지된 심각성은 백업의도에 정(+)의 영향을 미칠 것이다.

자기효능감은 위협적인 사건을 처리할 수 있는 능력에 대해 자기가 가지고 있는 믿음이다(Rogers, 1975; Johnston and Warkentin, 2010; Ifinedo, 2012). Bandura(1977)는 자기효능감을 주어진 과업을 수행할 수 있는 구체적인 자신감으로 정의하고 행동적 변화를 중재하는 인지기제로 개인이 갖고 있는 기술자체가 아니라 그 기술을 어느 정도 수행할 수 있는가 하는 판단이라고 설명하고 있다. 선행연구에서는 자기효능감이 높을수록 개인데이터를 더 자주 백업하게 되고(Crossler, 2010), 스마트폰 이용자의 악성코드용 백신 이용 의도가 높아지고(장재영 외, 2014), 모바일 장치의 분실이나 절도를 막기 위한 대처행동의 동기를 불러일으키는 것으로(Tu et al., 2015) 나타났다.

선행연구의 결과를 바탕으로 보안위협으로 인한 데이터의 손실을 방지하거나 줄이기 위해 자신이 데이터를 백업할 수 있다는 믿음이 크면 백업을 하고자 할 것이라는 가설을 설정하였다.

H3: 자기효능감은 백업의도에 정(+)의 영향을 미칠 것이다.

반응효능감은 어떤 행동이 실행되었을 때 특정한 결과로 이어질 것이라는 믿음의 정도이다(Bandura, 1977). 적응반응인 대처평가의 수행에서, 보호행동이 효과적일 것으로 믿는 신념(Floyd et al., 2000)이며, 대처평가에서 고려되어야 할 효과성(Liang and Xue, 2010), 보안위협을 방지하기 위한 보호도구의 능력에 대한 주관적 평가(Liang and Xue, 2010), 권장된 대처행동의 효율성 정도(Johnston and Warkentin, 2010) 등으로 정의할 수 있다. 선행연구에서는 반응효능감이 높을수록 가정의 무선 네

트워크에서 방화벽을 많이 사용하고(Woon et al., 2005), 강한 패스워드 사용에 대한 의도를 높이고(Zhang and McDowell, 2009), 직장에서 보안행위를 수행할 가능성이 크며(Bulgurcu et al., 2010), 정보보호를 위한 행위의도에 긍정적인 영향을 미치는 것으로(Johnston and Warkentin, 2010) 나타났다.

선행연구의 결과를 바탕으로, 데이터를 백업함으로써 보안위협으로 인한 데이터의 손실을 방지하거나 줄일 수 있다고 믿으면 백업을 하고자 할 것이라는 가설을 설정하였다.

H4: 반응효능감은 백업의도에 정(+)의 영향을 미칠 것이다.

반응비용은 시간, 돈, 노력 등의 관점에서 지각되는 기회비용이다(Rogers, 1983). Woon et al.(2005)은 권장 대처행동을 수행하는 과정에서 인지되는 돈, 비용, 불편함, 어려움, 대처행동 수행의 부작용 등을 포함하는 비용으로 정의했다. 반응비용이 높을수록 가정의 무선 네트워크에서 방화벽을 많이 사용하지 않고(Woon et al., 2005), 개인데이터의 백업을 자주 하지 않으며(Crossler, 2010), 회피동기를 낮추는 것으로(Liang and Xue, 2010) 나타났다. 반면, 보안정책 준수의도에는 유의한 영향을 주지 않았다(Ifinedo, 2012).

선행연구의 결과를 바탕으로, 보안위협으로 인한 데이터의 손실을 방지하거나 줄이기 위한 데이터 백업에 필요한 비용이 높아진다면 백업을 하고자하지 않을 것이라는 가설을 설정하였다.

H5: 반응비용은 백업의도에 부(-)의 영향을 미칠 것이다.

2) 습관과 보호동기이론의 요인 간의 관계

Vance et al.(2012)의 실증연구에서 IS보안정책 준수의도에 대한 습관은 보호동기이론의 모든 요인에 유의한 영향을 나타냈다. 안호주 외(2015)는 보안회피습관이 보호동기이론의 요인인 인지된 심각성, 인지된 취약성, 자기효능감, 반응효능감에 대한 유의한 영향을 확인했다. 따라서 평소의 보안습관은 보호위협을 심각하게 인식하고, 위협의 발생가능성을 높이 인식하고, 자신의 백업에 대한 자신감을 높이며, 백업의 효과에 대한 믿음이 높아질 것이며, 백업에 소요되는 비용은 낮게 인지하게 될 것이라는 가설을 설정하였다.

H6-1: 보안습관은 인지된 취약성에 정(+)의 영향을 미칠 것이다.

H6-2: 보안습관은 인지된 심각성에 정(+)의 영향을 미칠 것이다.
H6-3: 보안습관은 자기효능감에 정(+)의 영향을 미칠 것이다.
H6-4: 보안습관은 반응효능감에 정(+)의 영향을 미칠 것이다.
H6-5: 보안습관은 반응비용에 부(-)의 영향을 미칠 것이다.

참 고 문 헌

박찬욱, 이상우, “인터넷상에서의 개인정보 보호행동에 관한 연구: 보호동기이론을 중심으로,” 인터넷정보학회논문지, 제15권, 제2호, 2014, pp.59-71.

신승중, 류대현, 김석우, 정보보호의 기초, 인터비젼, 2005.

안호주, 장재영, 김범수, "금융기관 종사자들을 정보보안 위험관리로 이끄는 요인,“ Information Systems Review, 제17권, 제3호, 2015, pp.39-64.

양원석, 김태성, 이두호, “정보보호위협하에서 경제적인 데이터백업 운영 정책 분석,” 한국콘텐츠학회논문지, 제14권, 제10호, 2014, pp.270-278.

이스트소프트, 2016 정보보호 보안 인식 실태조사, 2016, 7, 14, (http://blog.alyac.co.kr/706).

장재영, 김지동, 김범수, “스마트폰 이용자의 악성코드용 모바일 백신 이용 의도에 영향을 미치는 요인,” 한국 IT 서비스학회지, 제13권, 제2호, 2014, pp.113-131.

한국정보통신기술협회, 정보통신용어사전, (http://terms.tta.or.kr/dictionary/dictionaryView.do).

Aarts, H., Verplanken, B., and Knippenberg, A. V., “Predicting behavior from actions in the past: Repeated decision making or a matter of habit,” *Journal of Applied Psychology*, Vol.28, No.15, 1998, pp.1355-1374.

Ajzen, I., and Albarracin, D., “Predicting and Changing Behavior : A Resoned Action Approach,” In *Prediction and Change of Health Behavior: Applying the Reasoned Action Approach,* eds.I. Ajzen, D. Albarracin, and R. Hornik, Lawrence Erlbaum Associates, 2007, pp.1-22

Anderson, C. L., and Agarwal, R., “Practicing Safe Computing: Message Framing, Self-View, and Home Computer User Security Behavior Intentions,” In *International Conference on Information Systems*, 2006, pp.1543-1561.

Bagchi, K., and Udo, G., “An analysis of the growth of computer and Internet security breaches,” *Communications of the Association for Information Systems*, Vol.12, No.1, 2003, pp.684-700.

Bandura, A., “Self-efficacy: toward a unifying theory of behavioral change,” *Psychological review*, Vol.84, No.2, 1977, pp.191-215.

Bandura, A., “Social foundations of thought and action: A social cognitive theory,”

Prentice-Hall, 1986.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P., "What Do 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.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I., "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.

Chung, W., Chen, H., Chang, W., and Chou, S., "Fighting Cybercrime: A Review and the Taiwan Experience," *Decision Support Systems*, Vol.41, No.3, 2006, pp.669-682.

Crossler, R. E., "Protection motivation theory: Understanding determinants to backing up personal data," In *System Sciences, 2010 43rd Hawaii International Conference*, 2010, pp.1-10.

Dhillon, G., and Backhouse, J., "Current directions in IS security research: towards socio-organizational perspectives," *Information Systems Journal*, Vol.11, No.2, 2001, pp.127-153.

Finne, T., "Information systems risk management: key concepts and business processes," *Computers & Security*, Vol.19, No.3, 2000, pp.234-242.

Fishbein, M., and Ajzen, I., "*Predicting and changing behavior: The Reasoned Action Approach,*" Taylor & Francis, 2010.

Floyd, D. L., Prentice-Dunn, S., and Rogers, R., "A Meta-Analysis of Research on Protection Motivation Theory," *Journal of Applied Social Psychology*, Vol.30, No.2, 2000, pp.407-429.

Gefen, D., "TAM or just plain habit: A look at experienced online shoppers," *Journal of Organizational and End User Computing*, Vol.15, No.3, 2003, pp.1-13.

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, No.1, 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.

Karabacak, B., and Sogukpinar, I., "ISRAM: information security risk analysis method," *Computers & Security*, Vol.24, No.2, 2005, pp.147-159.

Khalifa, M., Limayem, M., and Liu, V., "Online customer stickiness: a longitudinal study," *Journal of Global Information Management*, Vol.10, No.3, 2002, pp.1-14.

Kim, S. S., and Malhotra, N. K., "A Longitudinal Model of Continued IS Use: An Integrative View of Four Mechanisms Underlying Postadoption Phenomena," *Management Science*, Vol.51, No.5, 2005, pp.741-755.

Kim, S. S., Malhotra, N. K., and Narasimhan, S., "Two Competing Perspectives on Automatic Use: A Theoretical and Empirical Comparison," *Information Systems Research*, Vol.16, No.4, 2005, pp.418-432.

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.

Limayem, M., and Hirt, S. G., "Force of habit and information systems usage: Theory and initial validation," *Journal of the Association for Information Systems*, Vol.4, No.1, 2003, pp.65-97.

Limayem, M., Hirt, S. G., and Cheung, C. M., "How habit limits the predictive power of intention: The case of information systems continuance," *Mis Quarterly*, Vol.31, No.4, 2007, pp.705-737.

Limayem, M., Hirt, S. G., and Chin, W. W., "Intention Does Not Always Matter: The Contingent Role of Habit on IT Usage Behavior," In *Proceedings of the 9th European Conference on Information Systems*, 2001, pp.274-286.

Limayenm, M., Hirt, S. G., and Cheung, C. M., "Habit in the context of IS continuance: theory extension and scale development," In *ECIS 2003 Proceedings*, 2003.

Maddux, J. E., "Social cognitive models of health and exercise behavior: An introduction and review of conceptual issues," *Journal of Applied Sport Psychology*, Vol.5, No.2, 1993, pp.116-140.

Maddux, J. E., and Rogers, R. W., "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *Journal of experimental social psychology*, Vol.19, No.5, 1983, 469-479.

Milne, S., Sheeran, P., and Orbell, S., "Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory," *Journal of*

Applied Social Psychology, Vol.30, No.1, 2000, pp.106-143.

Ng, B. Y., Kankanhalli, A., and Xu, Y. C., "Studying Users' Computer Security Behavior: A Health Belief Perspective," *Decision Support Systems*, Vol.46, No.4, 2009, pp.815-825.

Rogers, R. W., "A protection motivation theory of fear appeals and attitude change," *The journal of psychology*, Vol.91, No.1, 1975, pp.93-114.

Rogers, R. W., "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation," In *Social Psychophysiology: A Sourcebook*, eds. J. T. Cacioppo, and R. E. Petty, Guilford, 1983, pp.153-176.

Rogers, R. W., and Prentice-Dunn, S., "Protection motivation theory," In *Handbook of health behavior research I: Personal and Social Determinants*, ed.Gochman, D. S., Springer, 1997, pp.113-132.

Siponen, M., Pahnila, S., and Mahmood, A., "Factors influencing protection motivation and IS security policy compliance," In *2006 Innovations in Information Technology*, 2006, pp.1-5.

Sommestad, T., Karlzén, H., and Hallberg, J., "A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour," *International Journal of Information Security and Privacy*, Vol.9, No.1, 2015, pp.26-46.

Straub Jr, D. W., "Effective IS security: An empirical study," *Information Systems Research*, Vol.1, No.3, 1990, pp.255-276.

Tu, Z., Turel, O., Yuan, Y., and Archer, N., "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.

Vance, A., Siponen, M., and Pahnila, S., "Motivating IS security compliance: insights from habit and protection motivation theory," *Information & Management*, Vol.49, No.3, 2012, pp.190-198.

Verplanken, B., Aarts, H., and van Knippenberg, A., "Habit, Information Acquisition, and the Process of Making Travel Mode Choices," *European Journal of Social Psychology,* Vol.27, 1997, pp.539-560.

Woon, I., Tan, G. W., and Low, R., "A Protection Motivation Theory Approach to Home Wireless Security," In *International Conference on*

Information Systems, 2005, pp.366-380.

Wu, M. C., and Kuo, F. Y., "An empirical investigation of habitual usage and past usage on technology acceptance evaluations and continuance intention," *ACM Sigmis Database*, Vol.39, No.4, 2008, pp.48-73.

Yoon, C., Hwang, J. W., and Kim, R., "Exploring Factors That Influence Students' Behaviors in Information Security," *Journal of Information Systems Education*, Vol.23, No.4, 2012, pp.407-415.

Zhang, L., and McDowell, W. C., "Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords," *Journal of Internet Commerce*, Vol.8, No.3, 2009, pp.180-197.Management," *Strategic Management Journal*, Vol. 18, No. 7, 1997, pp. 509-533.