클라우드 컴퓨팅 환경에서 정보보호관리체계의 인식에 관한 연구

배 재 권*

<요 약>

최근 애플 사(Apple Inc.)의 아이클라우드(i-cloud) 서비스의 정보유출사고 및 해킹사고로 인해 개인용 클라우드 서비스의 데이터 보안 및 정보보호에 대한 우려가 급증하고 있다. 개인용 클라우드 사용에 영향을 주는 가장 큰 요인이 바로 정보유출과 프라이버시(privacy) 침해에 대한 우려이다. 본 연구는 개인용 클라우드 서비스 이용 시 사용자가 왜 정보보호행위를 하는지에 대한 이유와 개인정보의 보호행위에 대한 중요성을 인지하고 있는지를 실증적으로 검증하기 위해 전통적으로 예방 의료행위를 설명하는데 사용되는 건강신념모형(Health Belief Model, HBM)을 적용하고자 한다.

본 연구는 의료분야의 HBM을 기반으로 개인용 클라우드 서비스의 정보보호행위에 미치는 영향요인들을 파악하고 이들 요인이 개인의 정보보호행위에 어떠한 영향을 미치는지 분석하고자 한다. 연구모형을 실증적으로 검증하기 위해 개인용 클라우드 서비스를 이용한 경험이 있는 이용자를 대상으로 설문조사를 실시하였고, 요인들 간의 관계를 분석하기 위해 경로분석을 실시하였다. 경로분석결과, 개인용 클라우드 서비스의 정보보호행위 영향요인인 지각된 심각성, 지각된 개연성, 지각된 자기효능감은 지각된 대응성과 모두 유의한 영향을 미치는 것으로 나타났다. 또한 지각된 대응성은 개인정보보호행위에 유의한 영향을 미치는 것으로 나타났다.

주제어: 개인용 클라우드, 정보보호행위, 건강신념모형(Health Belief Model, HBM), 지각된 심각성, 지각된 개연성, 지각된 대응성.

* 계명대학교 경영정보학과 조교수, jkbae99@kmu.ac.kr

Ⅰ. 서 론

클라우드 컴퓨팅은 인터넷 기술을 활용하여 정보기술(IT)자원을 서비스로 제공하는 컴퓨팅으로 IT자원(소프트웨어, 스토리지, 서버, 네트워크)을 필요한 만큼 빌려서 사용하고, 사용한 만큼 비용을 지불하는 컴퓨팅을 의미한다. 클라우드 컴퓨팅은 기업의 IT인프라에 대한 유지보수 부담을 경감시키고, 사업초기 대규모 초기투자비용에 대한 부담도 경감시킬 수 있는 등 IT혁신을 통한 비용절감을 이룰 수 있다는 점에서 국내외 많은 기업들이 다양한 클라우드 서비스를 운영하고 있다. 시장조사기관 가트너(Gartner, Inc)에 의하면 전 세계 클라우드 컴퓨팅 시장은 2015년에 약 92조원에 달할 전망이며 전체 IT서비스 시장의 성장률이 5% 미만인 데 비해, 클라우드 분야는 2018년까지 연평균 약 23%의 가파른 성장세를 보일 것으로 전망하였다. 또한 시장조사기관 IDC(International Data Corporation)에 따르면 클라우드 서비스 시장은 전체 IT시장 내에서 가장 빠르게 성장하는 영역이며 향후 IT지출 및 성장의 견인차 역할을 담당할 것이라고 전망하였다. 최근의 클라우드 컴퓨팅 시장은 스마트폰 확산, 다양한 모바일 디바이스의 등장, 모바일 네트워크의 고도화 등으로 인해 개인용 클라우드 서비스(Personal Cloud Service)로 확장되어 가고 있다.

선진국에서는 애플 사(Apple Inc.)의 아이클라우드(i-cloud) 서비스를 주로 사용하고 있고, 중국에서는 바이두(Baidu)를 중심으로 개인용 클라우드 컴퓨팅 서비스가 비약적으로 발전하고 있다. 글로벌 IT기업들이 무료로 개인들에게 클라우드 서비스를 제공하고 있어 그 이용자는 폭발적으로 증가하고 있으나 이와 비례하여 클라우드 사용에 관한 피해와 사고도 급증하고 있다. 최근 애플의 아이클라우드의 정보유출사고 및 해킹사고로 인해 개인용 클라우드 서비스의 데이터 보안 및 정보보호에 대한 우려가 급증하고 있다. 개인용 클라우드 사용에 영향을 주는 가장 큰 요인이 바로 정보유출과 프라이버시(privacy) 침해에 대한 우려이다. 개인이나 기업, 정부의 데이터 관리를 클라우드 서비스 운영자가 함으로써 발생될 수 있는 각종 법적 보안 관련 이슈의 등장은 클라우드 산업 분야의 가장 주요 논쟁거리이다. 현재까지 다수의 클라우드 서비스 운영기업은 클라우드 서비스의 외부 침입 및 보안위험 요인에 대한 대응방안이 구체적으로 마련되어 있지 않는 상태이고, 정보보호관제시스템을 운영 및 관리할 직원도 매우 부족한 실정이다. 또한 클라우드 컴퓨팅 보안위험을 실질적으로 예방 및 대응하기 위한 대책마련이나 클라우드 컴퓨팅 정보보호행위 및 전략을 제언한 실증연구도 거의 없는 실정이다. 최근까지 진행된 클라우드 컴퓨팅 정보보호 관련 연구들은 클라우드 보안기술 및 설계에 관한 연구, 보안관리체계 및 보안기술 표준화 연구 등의 탐색적이고 기술적인 연구와 클라우드 컴퓨팅 보안 시장현황 및 평가와 정책이슈를

다룬 연구들이 주로 진행되었다. 따라서 정보보호 및 정보보안 문제에 대한 기술적 논의 외에도 사용자 입장에서의 인지 차원의 논의도 필요할 것으로 보인다.
본 연구의 목적은 개인용 클라우드 서비스 이용 시 사용자가 왜 정보보호행위를 하는지에 대한 이유와 개인정보의 보호행위에 대한 중요성을 인지하고 있는지를 실증적으로 검증하기 위해 전통적으로 예방 의료행위를 설명하는데 사용되는 건강심리이론(Health Psychology Theory)을 적용하고자 한다. 정보보호행위는 정보를 보호하거나 정보유출의 위협으로부터 예방하려는 부정적 관점에서 연구되어야 하나 기존의 정보시스템 연구들은 주로 수용이라는 긍정적 관점에서 연구되었기 때문에 예방 의료행위를 설명하는데 사용되는 건강심리이론을 적용하고자 하였다. 따라서 본 연구에서는 건강심리이론의 대표적인 연구모형인 건강신념모형(Health Belief Model, HBM)을 적용한 연구모형을 제시하고자 한다. 위 연구모형을 바탕으로 개인용 클라우드 서비스의 정보보호행위에 미치는 영향요인들을 분석하고 개인용 클라우드 시장의 경쟁력 제고와 활성화 방안에 관한 경영전략을 제언하고자 한다.

Ⅱ. 건강신념모형(Health Belief Model, HBM)

정보보호 및 정보보안 행위는 에이즈(AIDS)나 심장병 등 질병을 예방하기 위해서 수행하는 예방적 건강행위와 유사하다(Ng et al., 2009). 의료 및 보건 분야에서는 사람들의 건강행위에 영향을 주는 원인을 파악하기 위해 건강심리이론을 개발하여 오랫동안 연구하였다(Oliver and Berger, 1979; Rosenstock, 1974; Rosenstock et al., 1994; Weinstein, 2000). 이들 중에서 대표적인 모형이 바로 Rosenstock(1974)의 건강신념모형(HBM)이다.
HBM은 1950년대 공중건강 프로그램의 실패 원인을 찾기 위해 만들어진 연구모형으로 개인의 예방행동을 예측하는 모델로써 많이 사용되고 있다. HBM은 사람들의 질병예방 행동을 설명하는 두 가지 주요 신념을 제시하고 있다. 첫 번째 신념은 질병에 대한 위협(threats)이며 위협에는 지각된 심각성(perceived severity)과 지각된 개연성(perceived susceptibility)이 있다. 지각된 심각성은 질병으로 인해서 초래할 수 있는 부정적 결과에 대해 개인이 지각하고 있는 심각성의 정도를 말하고, 지각된 개연성은 질병에 개인이 노출된 정도와 감염될 개연성을 의미한다. 두 번째 신념은 행위에 대한 기대(expectation)이며, 기대에는 행위에 대한 지각된 장애(perceived barriers), 지각된 이익(perceived benefits), 지각된 자기효능성(perceived self-efficacy)이 있다. 지각된 장애란 건강에 관련한 행동에서 잠

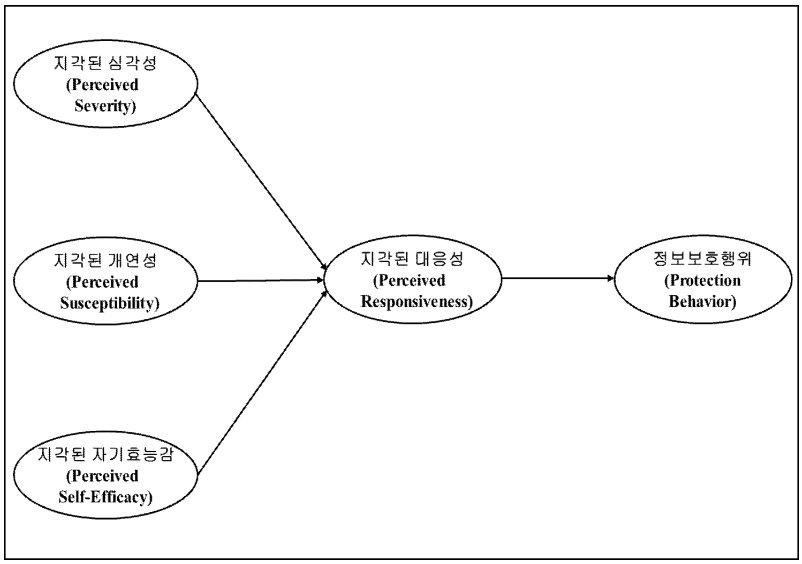
재적으로 발생 가능한 부정적인 결과와 이러한 행동을 실천하는데 방해하는 요인들을 말하며, 지각된 이익은 특정 행동으로 인해 지각된 위험 요인들이 제거되거나 감소될 수 있는 것을 의미한다. 마지막으로 지각된 자기효능성은 질병을 예방하기 위해서 또는 질병을 이겨낼 수 있다는 일련의 조치를 조직하고 실행해 낼 수 있다는 자신의 능력에 대한 믿음을 의미한다.

HBM을 이론적 틀로 활용한 많은 연구자들은 모델의 확장 및 설명력을 높이고자 확장된 HBM을 제시하였다. Sheeran and Abraham(2001)은 지각된 심각성, 지각된 개연성, 지각된 자기효능감, 지각된 대응성, 정보보호행위의 연구변수로 구성된 확장된 HBM을 제시하였다. HBM은 개인이 정보유출에 대한 위협을 인지하게 될 때 위협으로 벗어날 수 있는 대응방안을 찾게 되고, 대응방안이 위협으로부터 개인정보를 보호할 수 있다고 인지하게 되면 실제로 정보보호행위를 하려고 한다는 것을 기본이론으로 하고 있다. 정보보호 및 정보보안행위는 정보를 보호하거나 정보의 위협으로부터 예방하려는 부정적 관점에서 연구되어야 하나 기존의 정보시스템 연구들은 주로 수용이라는 긍정적 관점에서 연구되었기 때문에 정보보호행위 연구에 적용하기 어렵다. 따라서 질병을 예방하는 의료행위를 설명하는데 사용되는 HBM이 정보보호행위 연구에 적합하며 본 연구의 개인용 클라우드 컴퓨팅 서비스의 정보보호행위에 적용하는 것도 적합하다고 할 수 있다.

Ⅲ. 연구 설계

3.1 연구모형의 설정

본 연구는 의료분야의 HBM을 기반으로 개인용 클라우드 서비스의 정보보호행위에 미치는 영향요인들을 파악하고 이들 요인이 개인의 정보보호행위에 어떠한 영향을 미치는지 분석하고자 한다. 본 연구모형은 HBM을 기반으로 개인이 정보유출에 대한 위협을 인지하게 될 때 위협으로 벗어날 수 있는 대응방안을 찾게 되고, 대응방안이 위협으로부터 개인정보를 보호할 수 있다고 인지하게 되면 실제로 정보보호행위를 하려고 한다는 것을 기본이론으로 하고 있다. 구체적으로 개인용 클라우드 서비스의 정보보호행위 영향요인인 지각된 심각성, 지각된 개연성, 지각된 자기효능감이 지각된 대응성과 종속변수인 개인정보보호행위에 어떠한 영향을 미치는지 알아보고자 하였다. 본 연구모형은 <그림 1>과 같다.



<그림 1> 연구모형

3.2 연구가설의 설정

본 연구는 개인용 클라우드 컴퓨팅 서비스의 정보보호행위 영향요인으로 지각된 심각성, 지각된 개연성, 지각된 자기효능감의 요인을 제시하고자 한다. 이들 영향요인이 지각된 대응성과 개인정보보호행위에 미치는 영향에 관한 가설은 다음과 같다.

지각된 심각성(perceived severity)이란 특정한 건강문제가 얼마나 심각한 결과를 초래하는지에 대해서 지각하는 개인의 신념을 말한다. 본 연구에서는 지각된 심각성을 개인정보유출로 인해서 발생할 수 있는 부정적인 결과에 대한 개인의 인지정도로 정의한다. 지각된 개연성(perceived susceptibility)은 어떤 질병에 걸릴 수 있다는 주관적 위험을 말한다. 본 연구에서는 지각된 개연성은 개인정보유출로 인해 본인이 큰 피해를 입을 수 있다는 주관적 가능성이라고 정의한다. 지각된 자기효능감(perceived self-efficacy)은 정보기술의 위협을 방어하는데 있어 본인이 잘 할 수 있다는 확신과 자신감, 능력에 대한 믿음을 말한다(Compeau et al., 1999; Liang and Xue, 2009, 2010).

HBM에서는 지각된 대응성(perceived responsiveness)에 영향을 주는 변수로 위에서 언급된 지각된 심각성, 지각된 개연성, 지각된 자기효능감을 언급하였다. 지각된 대응성은 효과적인 패스워드 사용 및 패스워드의 주기적 변경 등이 패스워드 도용 및 개인정보유출을 얼마나 보호할 수 있는지에 대한 개인의 평가를 말

한다(Liang and Xue, 2009). 사용자의 대응방안에 대한 자기확신이 높을수록 지각된 대응성은 더 높을 것이다. 마지막으로 HBM에서는 개인이 정보유출에 대해 인지할 때 이를 벗어나고자 하는 대응방안을 찾게 될 것이고, 이들 대응방안으로부터 개인정보를 보호할 수 있다고 언급하였다(Rosenstock, 1974; Rosenstock et al., 1994; Rogers, 1975, 1983). 이상의 이론적 배경을 토대로 개인용 클라우드 서비스의 정보보호행위 영향요인과 지각된 대응성, 정보보호행위간의 가설은 다음과 같다.

[가설 1] 개인정보가 유출됨으로써 발생할 수 있는 지각된 심각성은 지각된 대응성에 긍정적인 영향을 줄 것이다.

[가설 2] 개인정보가 유출될 수 있다는 지각된 개연성은 지각된 대응성에 긍정적인 영향을 줄 것이다.

[가설 3] 지각된 자기효능성은 지각된 대응성에 긍정적인 영향을 줄 것이다.

[가설 4] 지각된 대응성은 개인의 정보보호행위에 긍정적인 영향을 줄 것이다.

Ⅳ. 연구방법

4.1 연구변수와 설문도구의 개발

본 연구는 선행연구를 기반으로 도출된 개인용 클라우드 이용자의 정보보호행위에 관한 개념적 정의를 내리고 선행연구자들의 측정항목을 수정하여 연구문항을 구성하였다. 본 연구에서 사용한 설문문항은 HBM의 문헌연구(Rosenstock, 1974; Rosenstock et al., 1994; Rogers, 1983)로부터 나온 설문문항과 건강심리이론을 토대로 연구된 정보기술 분야 선행연구(Lee, 2011; Liang and Xue, 2009, 2010; Ng et al., 2009; Woon et al., 2005; 지범석 외, 2011)의 설문문항을 개인정보보호행위에 맞게 수정하였다.

독립변수는 개인용 클라우드 서비스 이용자의 정보보호행위 영향요인인 지각된 심각성, 지각된 개연성, 지각된 자기효능감으로 정의하였다. 매개변수는 지각된 대응성이며, 종속변수는 개인용 클라우드 서비스 이용자의 정보보호행위이다.

본 연구는 대부분 선행연구를 통해 그 타당성이 충분히 입증된 항목만을 이용하였다. 또한 설문지 문항에 대한 클라우드 서비스 운영자, 단말솔루션업체, 응용업체, 인프라솔루션업체, 하드웨어업체 등의 실무자와 관련 연구자들의 내용 검토, 설문지에 대한 사전조사(pre-test) 등을 실시하여 구성개념의 내용 타당성 및 가독성을 확보하였다.

4.2 표본선정 및 자료수집 방법

본 연구는 개인용 클라우드 서비스 사용자를 대상으로 연구대상을 선정하였다. 대표적인 개인용 클라우드 서비스로는 애플의 iCloud(아이클라우드), 구글의 Android(안드로이드), 마이크로소프트의 My Phone(마이폰) 서비스가 있으며, 이들 기업의 서비스를 이용한 경험이 있는 이용자를 대상으로 설문조사를 실시하였다. 설문조사는 개인용 클라우드 서비스를 이용한 경험이 있는 서울 소재 S대학과 지방 소재 K대학의 대학생들을 대상으로 실시하였으며, 직접 방문하거나 또는 이메일을 이용해 설문을 배포, 회수하였다. 설문조사는 2013년 9월 11일부터 29일까지 19일간 실시되었다. 이 기간에 총 251부의 설문이 회수되었으며, 이 중 불성실한 답변이 포함된 69부를 제외한 182부의 설문지가 자료 분석에 사용되었다.

Ⅴ. 가설검정

5.1 표본의 기술적 특성

<표 1>은 자료 분석에 사용된 총 182개 표본의 성별 및 연령 분포, 무선이동통신기술 사용기간, 1일 무선이동통신기술 사용시간, 클라우드 서비스 사용빈도에 대한 응답자의 특성을 보여준다. 표본의 성별 분포는 남자가 114명(62.6%), 여자가 68명(37.4%)이며, 연령 분포는 21~25세가 96명(52.7%)으로 가장 많았고, 20세 이하가 33명(18.1%)으로 전체 표본의 70.9%가 20대 초중반인 것으로 조사되었다. 클라우드 서비스 이용에 필요한 무선이동통신기술의 사용기간은 3~5년이 78명(42.9%), 1~3년이 62명(34.1%), 5년 이상이 30명(16.5%)으로 나타나 설문조사 대상자들이 무선이동통신기술에 익숙한 것으로 판단할 수 있다. 1일 무선이동통신기술 사용시간은 1시간에서 2시간 이하가 75명(41.2%)으로 가장 많았고, 1시간 미만인 경우는 54명(29.7%)으로 조사되었다. 마지막으로 클라우드 서비스 사용빈도를 살펴보면, 한 달에 한번 방문한다는 응답자가 57명(31.3%)으로 가장 많았고, 15일에 한번 방문한다는 응답자는 47명(25.8%)으로 조사되었다. 전체 표본의 63.2%가 15일에 적어도 1번 이상은 클라우드 서비스를 이용하는 것으로 조사되었다.

<표 1> 표본의 인구통계학적 특성

구 분	항 목	빈 도(*N*=182)	비 율(%)
성 별	남 성	114	62.6%
	여 성	68	37.4%
연 령	20세 이하	33	18.1%
	21~25세	96	52.7%
	26~30세	53	29.1%
무선이동통신기술 사용기간 (스마트폰, 스마트패드, 넷북, 울트라북 등)	1년 미만	12	6.6%
	1~3년	62	34.1%
	3~5년	78	42.9%
	5년 이상	30	16.5%
1일 무선이동통신기술 사용시간	1시간 이하	54	29.7%
	1~2시간 이하	75	41.2%
	2~4시간 이하	43	23.6%
	4시간 이상	10	5.5%
모바일 클라우드 서비스 사용빈도	하루에 2번 이상	4	2.2%
	하루에 한번	9	5.0%
	2~3일에 한번	16	8.8%
	일주일에 한번	39	21.4%
	15일에 한번	47	25.8%
	한 달에 한번	57	31.3%
	기타	10	5.5%

5.2 측정모형 검정

가설 검정에 앞서 본 연구에서 사용된 변수들의 측정도구에 대한 신뢰성과 타당성을 검정하였다. 이를 위해 확증적 요인 분석 도구인 *SMARTPLS version 2.0*을 사용하였다. 이론적 견고성, 표본의 수, 설문의 자체 개발이라는 연구특성을 고려하여 데이터 분석방법으로 *PLS*를 채택하였다. 모형의 적합도 보다는 구성개념의 설명력을 측정하고자 한 최근의 정보기술 관련 연구에서도 *PLS*를 분석도구로 채택하고 있다. 가설 검정 이전에 측정모형의 검정을 통해 각 변수의 신뢰성과 타당성을 먼저 체크하였다. 이를 위해 개별항목 신뢰성, 내적 일관성, 수렴타당성, 그리고 판별 타당성을 분석하였다.

5.2.1 신뢰성 분석 및 타당성 분석

신뢰성 검정을 위해 클론바흐 알파(Cronbach's Alpha)값과 유사한 종합요인 신뢰성 지수(Composite Scale Reliability Index, CSRI)값을 산출하였다. CSRI값이

0.7이상이면 변수의 측정이 내적으로 일관성이 있다고 판단된다(Fornell and Larcker, 1981). <표 2>에서 알 수 있듯이, 모든 변수의 CSRI값이 0.7이상이므로, 본 연구의 측정항목들은 신뢰성이 있다고 볼 수 있다. 또한 각 변수들의 측정항목에 대한 개념 타당성을 알아보기 위해 수렴 타당성과 판별 타당성을 조사하였다. <표 2>에서 보듯이 각 측정항목의 해당 변수에 대한 요인 적재값이 모두 0.7이상이므로 이는 수렴 타당성이 있음을 나타내는 것이다. 다음으로 판별 타당성 측정을 위해 Fornell and Larcker(1981)가 제안한 평균분산추출(Average Variance Extracted, AVE)값을 사용하였다. <표 3>에서 별표(*)로 표시한 값은 AVE 제곱근 값이며 나머지 행렬에서의 값은 각 변수의 상관계수 값을 나타낸다. AVE 제곱근 값이 0.7이상이고, AVE 제곱근 값이 다른 변수의 상관계수 값보다 커야 판별 타당성이 있는 것으로 판단할 수 있다. 본 연구에 사용된 항목들은 모두 0.7보다 큰 AVE 제곱근 값을 보여주고 있고, 나머지 변수간의 상관계수가 AVE 제곱근 값보다 작게 나타나 판별 타당성의 조건을 만족시키고 있다. 이상의 결과로 본 연구에서 사용한 측정항목은 개념적으로 타당한 것으로 볼 수 있다.

<표 2> 최종 연구변수의 내적 일관성 및 수렴 타당성 검정

연구 변수	구성 개념	요인값	CSRI	AVE
지각된 심각성 (PS)	PS1	0.9077	0.8849	0.7199
	PS2	0.8222		
	PS3	0.8123		
지각된 개연성 (PESU)	PESU1	0.8146	0.8942	0.7384
	PESU2	0.9068		
	PESU3	0.8540		
지각된 자기효능감 (PSE)	PSE1	0.9102	0.9039	0.7589
	PSE2	0.7944		
	PSE3	0.9040		
지각된 대응성 (PR)	PR1	0.8614	0.8997	0.7495
	PR2	0.8422		
	PR3	0.8928		
정보보호행위 (PB)	PB1	0.8864	0.9286	0.8126
	PB2	0.9230		
	PB3	0.8944		

<표 3> 최종 연구변수의 AVE(평균분산추출) 값을 통한 판별 타당성 검정

	PS	PESU	PSE	PR	PB
PS	0.8485*				
PESU	0.6211	0.8593*			
PSE	0.4685	0.3946	0.8711*		
PR	0.4609	0.3601	0.4094	0.8657*	
PB	0.5615	0.5366	0.3422	0.4214	0.9014*

주) *AVE 제곱근 값(Square Root of the AVE).
PS: 지각된 심각성, PESU: 지각된 개연성, PSE: 지각된 자기효능감
PR: 지각된 대응성, PB: 정보보호행위.

5.2.2 구조모형 분석

이상의 측정모형의 분석 결과를 통해 신뢰성과 타당성이 검증되었다. 이 측정모형 하에서 각 변수간의 경로에 대한 유의성 검증을 실시하여 가설을 검증하였다. 경로분석 결과와 가설채택 여부는 <표 4>와 같다.
개인용 클라우드 컴퓨팅 서비스의 정보보호행위 영향요인인 지각된 심각성, 지각된 개연성, 지각된 자기효능감은 지각된 대응성과 모두 유의수준 1%에서 채택되었다. 또한 지각된 대응성은 개인정보보호행위와 유의수준 1%에서 채택되었다. 이로써 HBM이 정보보호행위 관련 연구에도 적합하다는 것을 연구결과로 제시할 수 있다.

<표 4> 경로분석 결과와 가설채택 여부

가설	인과관계	경로계수	T값	P값	검정
H1	지각된 심각성 → 대응성	0.2604	3.7756	0.0002	채택
H2	지각된 개연성 → 대응성	0.1945	2.7570	0.0064	채택
H3	지각된 자기효능감 → 대응성	0.2072	3.1005	0.0022	채택
H4	지각된 대응성 → 정보보호행위	0.4216	7.1916	0.0000	채택

Ⅵ. 결론 및 시사점

클라우드 서비스의 경우 개인정보보호 및 개인정보유출에 대한 우려가 가장 큰 이슈이다. 개인정보보호 행위의 경우 예방의 목적의 성격이 강하므로 정보를 보호하거나 정보유출의 위협으로부터 예방하려는 부정적 관점에서 연구되어야 하므로 본 연구에서는 보건의료예방 및 의료행위를 설명하는 건강심리이론을 적용

하였다. 따라서 본 연구는 HBM의 주요 연구변수를 클라우드 서비스 분야에 적용한 확장된 HBM 연구모형을 제시하였다. 구체적으로 개인용 클라우드 서비스의 정보보호행위 영향요인인 지각된 심각성, 지각된 개연성, 지각된 자기효능감이 지각된 대응성과 종속변수인 개인정보보호행위에 어떠한 영향을 미치는지 알아보고자 하였다. 위 연구모형을 실증적으로 검증하기 위해 개인용 클라우드 서비스를 이용한 경험이 있는 이용자를 대상으로 설문조사를 실시하였다.

본 연구의 주요 연구결과와 시사점은 다음과 같다. 첫째, 개인용 클라우드 컴퓨팅 서비스의 정보보호행위 영향요인인 지각된 심각성, 지각된 개연성, 지각된 자기효능감은 지각된 대응성과 모두 유의한 영향을 미치는 것으로 나타났다. HBM 관련 연구에서도 질병으로 인해서 초래할 수 있는 부정적 결과에 대해 개인이 지각하고 있는 심각성의 정도와 질병에 개인이 노출된 정도와 감염될 개연성을 가진다면 이들 위협으로부터 벗어날 수 있는 대응방안을 찾게 된다고 언급하였다. 또한 Sheeran and Abraham(2001)은 지각된 심각성과 지각된 개연성이 지각된 대응성에 유의한 영향을 미친다는 연구결과를 제시한 바 있다. Liang and Xue (2009)와 HBM에서는 지각된 대응성(perceived responsiveness)에 영향을 주는 변수로 지각된 자기효능감을 언급하였고, 사용자의 대응방안에 대한 자기확신이 높을수록 지각된 대응성은 더 높을 것이라는 연구결과를 제시한 바 있다.

둘째, 지각된 대응성은 개인정보보호행위에 유의한 영향을 미치는 것으로 나타났다. HBM 관련 선행연구(Rosenstock, 1974; Rosenstock et al., 1994; Rogers, 1975, 1983)에서는 개인이 정보유출에 대해 인지할 때 이를 벗어나고자 하는 대응방안을 찾게 되고, 이들 대응방안으로부터 개인정보를 보호할 수 있다고 언급한 바 있다.

이처럼 개인용 클라우드 사용자는 개인정보유출에 대한 우려와 염려가 매우 크므로 클라우드 시스템의 보안에 대한 믿음을 가질 수 있도록 대응방안을 마련해야 하며 '클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률안(이하 클라우드법)'이 조속히 제정되어 통과되어야 할 것이다. 또한 클라우드 컴퓨팅은 보안과 프라이버시에 매우 민감한 기술로 보안정책 및 표준화 가이드라인이 매우 중요하다. 단계별 암호화 등 데이터 프라이버시에 대한 치밀하고 엄격한 기준을 세우고 클라우드 서비스 운영자는 사이버보안 및 정보보호 관련 국제표준과 표준화 가이드라인을 엄격히 준수해야 한다. 마지막으로 사용자가 요구하면 언제라도 보안 관련 서비스 내용을 상세히 공개하여 투명성을 갖추어야 하겠다.

본 연구의 학문적, 실무적 기여도는 다음과 같다. 학문적으로는 개인용 클라우드 서비스의 정보보호행위에 영향을 주는 요인을 사용자 관점에서 도출하여 실증적으로 검증하였다. 개인용 클라우드의 정보보호 관련 행동학적 관점의 연구가 전무한 상황에서 보건의료예방 및 의료행위를 설명하는데 사용되는 HBM의 연구

변수를 고려한 확장모형을 개인용 클라우드 정황에 적용함으로써 정보보호행위 모형에 대한 이론적 발전에 기여하였다. 또한 본 연구결과는 개인용 클라우드 사용자가 왜 정보보호행위를 하는지에 대한 포괄적인 이해를 제공한다. 실무적으로는 개인용 클라우드 서비스 운영자, 단말솔루션업체, 응용업체, 인프라솔루션업체, 하드웨어업체들에게 클라우드 보안 및 정보보호 서비스의 운영 및 관리적인 고려사항을 제시하였다.

차후 연구에서는 다양한 측면에서 보완이 이루어져야 할 필요성이 있다. 첫째, 연구 표본의 일반화와 측정 도구에 관련된 것이다. 본 연구는 개인용 클라우드 서비스에 익숙할 것으로 생각되는 20대 대학생으로 표본을 한정하였다. 또한 측정도구에 있어서도 설문지법을 이용하였는데, 이 방법은 설문지의 내용과 응답자의 반응태도에 따라 조사결과가 좌우된다는 점을 완전히 통제할 수 없다는 한계점이 있다. 따라서 개별 면담이나 관찰법 등의 탐색적 조사를 병행 실시하여 연구결과의 타당성을 향상시켜야 할 필요성이 있다. 둘째, 대표적인 건강심리이론 중 Rogers(1983)의 보호동기이론(Theory of Protection Motivation)을 HBM의 주요변수와 통합하여 개인용 클라우드 서비스에 적용한 확장 연구가 필요할 것으로 보인다. 또한 기업용 모바일 클라우드 사용자를 대상으로 한 정보보호행위에 관한 연구도 필요할 것으로 생각된다.

참 고 문 헌

지범석·판류·이상철·서영호(2011), “정보품질을 위한 개인정보 보호행위: 건강심리이론 관점을 중심으로”, 품질경영학회지, 제3권, pp. 432-443.

Janz, N. K. & Becker, M. H. (1984). The health belief model: A decade later. Health Education Quarterly, Vol. 11, No. 1, pp. 1-47.

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

Liang, H. and Y. Xue (2009), "Avoidance of information technology threats: A theoretical perspective", MIS Quarterly, Vol. 33 No. 1, pp. 71-90.

Liang, H. and Y. Xue (2010), "Understanding security behaviors in personal computer usage: A threat avoidance perspective", Journal of the Association for Information Systems, Vol. 7 No. 2, pp. 393-413.

Ng, B. Y., Kankanhalli, A., and Xu, Y. C., (2009), “Studying users′ computer security behavior: A health belief perspective.” Decision Support System,

Vol. 46, No. 4, pp. 815-825.

Maddusm J.E. and R.W., Rogers (1983), "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change", Journal of Experimental Social Psychology, Vol. 19, pp. 469-479.

Rogers, R.W. (1983). "Cognitive and physiological process in fear appeals and attitude change: A revised theory if protection motivation", in Social Psychophysiology: A Source Book, R. Petty (ed.), New York : Guiford Press, pp. 153-176.

Rosenstock, I. M. (1974). Historical Origin of the Health Belief Model. In M. H. Becker (Ed.),The Health Belief Model and personal health behavior (pp. 1-8). Thorofare, NJ: B. Slack, Inc.Charles.

Stonebumer, G., Goguen, A., and Feringa, A (2004), Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology(NIST) Special Publication, Washington D.C.

Sheeran, P., and Abraham, C. (2001). The health belief model. Predicting health behaviour (pp.23-61). Buckingham: Open University Press.

Stonebumer, G., A. Goguen, and A. Feringa, Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology(NIST) Special Publication, Washington D.C., 2004.

Humphreys, E.(2008), "Information Security Management Standards : Compliance, Governance and Risk Management," Information Security Technical Report, Vol. 13, No.4, pp. 247-255.

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