JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 19, No. 1, pp. 93-102, Jan. 2018

경험 및 습관이 신규서비스의 정보보호 행동에 미치는 요인에 대한 연구 - 보호동기이론과 UTAUT2을 중심으로

이홍제[1] · 고형석[1]· 노은희[2]· 한 경 석[3*]
[1]숭실대학교 IT정책경영 박사과정· [2]한성대학교 IT교육과정 조교수 ·[3*]숭실대학교 경영학부 교수

A Study on the Factors of Experience and Habit on Information Security Behavior of New Services - based on PMT and UTAUT2

Hong-Je Lee[1]· Hyeong-Seog Kho[1]· Eun-Hee Roh[2] ·Kyeong-Seok Han[3*]

[1]Department of IT Policy Management, Soongsil University, Seoul 06978, Korea
[2]Department of College of Liberal Arts & Sciences, Hansung University, Seoul 02876, Korea
[3*]Department of Business Administration, Soongsil University, Seoul 06978, Korea

[요 약]

본 연구는 지능화된 보안 위협에 인터넷 이용자의 정보보호 행동 요인을 분석하여 정책적 시사점을 제안하고자 한다. 연구 모델은 보호동기이론과 UTAUT2를 기반으로, 인지된 위협, 심각성, 사회적 영향, 자기효능감, 정보보안 제품 이용 경험 및 습관, PC/개인정보보호 행동, 신규 서비스의 정보보호 행동으로 구성 하였고, 인구 통계학적 특성과 인터넷 사용 장소, 유료 보안제품 이용, 침해사고 경험 등을 조절변수로 하여 인터넷 이용자의 보안 행동에 미치는 영향을 분석하였다. 연구 결과는 인지된 심각성, 자기효능감이 보안 제품 이용 경험 및 습관에 높은 영향을 미쳤으며, 경험 및 습관, 자기효능감은 PC/개인정보보호 행동에 높은 영향을 미치고, PC/개인정보보호 행동은 신규 서비스의 보안 행동에 높은 영향을 미치는 것으로 나타났다. 연령, 소득, 유료 보안제품 이용, 침해사고 경험은 인터넷 이용자의 정보보안 행동에 조절효과가 있었다. 본 연구의 결과가 인터넷 이용자의 정보보호 수준 향상을 위한 정책 의사결정에 도움을 줄 것으로 기대한다.

[Abstract]

This study aims to present policy implications by analyzing information security behavior factors of internet users. The research model, based on PMT and UTAUT2, consists of perceived threat, severity, social influence, self-efficacy, experience and habits, PC and privacy behaviors, security behaviors on new services and set demographic characteristics, use places of internet, use of paid products, and experiences of accident as moderate variables to analyze the effect on security behavior. The results showed that perceived severity, self-efficacy significantly influenced on experience and habits, and experience and habits and self-efficacy had a high influence on PC and privacy behavior. Also, PC and privacy behaviors have a high impact on security behavior of new services. Age, income, use of paid products, and experience of accidents have a moderating effects on security behaviors. The results of this study are expected to help policy decision making to improve the level of information security of internet users.

색인어 : 정보보호, UTAUT2, 보호동기이론, 경험 및 습관, 정보보호실태조사
Key word : Information Security, UTAUT2, Protection Motivation, Experience and Habit, Survey on Information Security

http://dx.doi.org/10.9728/dcs.2018.19.1.93

Received 20 November 2017 ; **Revised** 23 January 2018
Accepted 29 January 2018

***Corresponding Author;** Kyeong-Seok Han

Tel: +82-02-820-0585
E-mail: kshan@ssu.ac.kr

Ⅰ. 서 론

급속하게 변화하는 인터넷 환경과 4차 산업혁명의 새로운 기술(IoT, 클라우드, 빅데이타, 모바일)의 등장으로 사이버 위협이 현실 세계로 확대되고, 위협 또한 지능화 되고 있다. 올해 가장 많이 발견되고 있는 랜섬웨어의 경우[38] 다양한 신종, 변종 랜섬웨어가 등장하고 있다. 최근 랜섬웨어는 플랫폼(PC, 모바일 기기 등), 운영체제 구분 없이, PC 뿐만 아니라 모바일 기기로 공격 대상을 확대하고 있어 인터넷 이용자의 일상이 사이버 보안 위협에 노출되고 있다고 할 수 있다.
2017년 전 세계 150여 개국, 30 만대 이상을 감염시킨 WanaCry 랜섬웨어를 포함하여, 랜섬웨어 공격과 피해는 계속해서 증가할 것으로 예상된다. 국내외에 발생한 랜섬웨어들은 다양한 형태 (메일, 웹 사이트, 첨부파일 등)로 배포되고 있으며, 해커들은 비트코인을 획득하기 위한 금전적 목적 이외에도 정치적, 사이버전등 공격 목적도 다양하며, 조직과 자금, 지능화된 공격 도구로 더욱 발전하고 있다. 하지만, 고도화, 지능화 되고 있는 사이버 위협에 대해 인터넷 이용자의 대응은 부족한 현실이다.
KISA가 실시한 2016년 정보보호 실태 조사에 따르면[37], 인터넷 이용자의 대부분이 스마트 기기, 무선 랜, SNS, 클라우드 서비스를 이용하고, 다양한 목적으로 개인정보를 인터넷에 제공하고 있다. 그러나 인터넷 이용자의 14.2%는 무료 정보보호 제품조차도 이용하지 않고 있으며, 정보보호 제품 이용자의 대부분은 무료 소프트웨어를 이용하고 있다. 매일 또는 일주일에 1~2회 정도 악성코드를 검사하는 이용자도 10.9%에 불과하고, 중요 데이터를 백업하는 인터넷 이용자는 35.0%로 낮은 수준이다. 인터넷 이용자의 17.4%가 전해년도에 침해사고를 경험하였고, 악성코드, 개인정보 유출 및 사생활 침해를 경험한 것으로 조사 되었다. 개인정보를 제공한 인터넷 이용자의 7.6%가 개인정보 침해사고를 경험한 것으로 나타났다.

이처럼, 인터넷 이용자는 다양한 형태의 지능화된 공격에 노출되어 있고, IoT 등 4차 산업혁명의 서비스가 확산됨에 따라 프라이버시 침해 및 재산적 손실뿐만 아니라 안전(safety)까지 위협하는 위험에 대응해야 하는 문제를 갖고 있다[34]. 인터넷 이용자는 기업 종업원들과 다르게, 재정적, 기술적 지원을 기대할 수 없기 때문에 스스로 보안 제품을 설치, 운영(주기적인 악성코드 검사, 백업 등)해야 하며, 피해 예방 조치, 개인정보 유출 방지 행동을 해야 한다. 또한 정보보호에 대한 정보를 스스로 검색하거나 정보보호 관련된 학습을 해야 한다. 그러나 인터넷 이용자의 34.4%는 정보보호 관련 학습활동을 하지 않고 있으며, 학습자의 경우에도 용어가 어렵고, 복잡하며, 원하는 자료가 없는 어려움이 있는 것으로 나타났다[37].

증가하는 신규 보안 위협과 인터넷 이용자의 취약한 보안 대응 환경을 고려해 보면, 인터넷 이용자의 정보보호 수준 향상을 위해 인과 관계를 파악하는 것이 매우 중요하다고 할 수 있다. 본 연구는 인터넷 이용자의 정보보호 행위에 영향을 미치는 다양한 요인들을 찾고, 이를 바탕으로 이용자들의 정보보호 수준 향상을 위한 방안을 모색 하고자 한다.

Ⅱ. 관련 연구

2.1 보호동기 이론 (Protection Motivation Theory)

공포 소구(Fear Appeal)는 사용자에게 불안이나 공포를 통해, 권고를 따르지 않을 경우 발생되는 좋지 않은 결과를 제시(예: 금연, 마약 예방 광고)함으로써 사용자의 공포반응을 유발하여, 태도나 행동을 변화시키려고 한다[20,29].
Rogers(1975)는 공포 소구에 대한 개인의 태도와 행동의 변화 과정을 설명하기 위해, 기대가치(expectancy value)와 위협 평가(threat appraisal), 대처 평가(coping appraisal)의 인지 처리(cognitive processing) 과정에 기반을 둔 보호동기이론을 제시하였다[10, 20]. 개인은 위협 메시지에 노출되었을 때, 이를 피하기 위한 행동의 변화를 하는데, 위협을 느낀 메시지에 의해 행동의 변화가 일어나는 것이 아니라, 공포에 대한 인지적 처리 과정이 보호동기에 영향을 주어 행동을 변화하게 한다[20].

위협 평가는 위협적인 사건에 대한 개인의 평가로, 지각된 취약성(perceived vulnerability)과 지각된 심각성 (perceived severity)으로 구성된다[10,20].
□ 인지된 취약성 - 위협의 발생 가능성에 대한 자신의 평가
□ 지각된 심각성 - 위협이 성공할 경우 미치는 피해의 정도
대처 평가는 손실을 방지하고 대처하는 능력에 대한 개인의 평가로 자기효능감 (self efficacy), 지각된 대응효능감 (perceived response effectiveness), 지각된 장애(perceived barriers)로 구성된다 [16,19,21, 30].
□ 자기효능감 - 위협 대응 행동에 대한 개인의 능력과 자신감
□ 지각된 대응효능감- 권고된 행동이 위협으로부터 보호하는데 효과적일 것이라고 믿는 정도
□ 지각된 장애 - 대응 행동을 수행할 때 지출되는 금전적 비용, 시간, 어려움, 부작용 등 행동을 방해하는 요인

보호동기이론은 위협 메시지가 성공했을 경우를 가정 하여서, 메시지가 실패하는 이유를 설명하지는 못하는 한계점을 갖고 있었다. Witte(1992)는 “병행 과정 확장모델 (EPPM; Extended Parallel Process Model)” 을 제시하였는데[28], 개인은 위협에 대한 평가와 권고된 대응 효능감에 대한 평가를 토대로 ‘무반응’, ‘위험 통제반응’, ‘공포 통제 반응’ 의 행동을 한다.
무반응은 개인이 공포소구 메시지에 위협을 느끼지 못한 경우에 발생하고, 위협이 높고 효능감이 높을 때 개인은 위협을 회피하기 위한 권고된 행동을 이행(위험 통제반응)하게 한다. 반면에 위협은 높지만 효능감이 낮은 환경에서 개인은 방어적 회피 거부, 반발 등과 같은 부적응(공포통제반응)의 변화를 가져온다. 즉, 개인이 권장되는 행동을 하도록 하기 위해서는 인지된 위협과 자기효능감, 대응효능감을 높이는 것이다[6, 28, 29].

보호 동기는 위협을 회피하거나 완화 행동을 채택해하는데 (Rogers, 1975), 외부 보안 위협에 대한 정보 보안 대응책(보안 제품이용, 보호행동, 정책준수 등)을 채택하는 행동의도와 관계된다. 그래서 정보보호 분야에 이러한 보호동기이론을 활용하여, 개인의 정보보안 행동 및 조직의 보안정책 준수행동을 설명하는 연구를 수행 하였다.

표 1. 보호동기를 활용한 정보보호 관련 연구
Table 1. Research on Information Security using Protection Motivation

Research (year)	Result
Youn (2005)	A higher level of risk perception led to less willingness to provide information [31]
LaRose (2005)	Perceived efficiency affects the practice safe online behavior such as updating virus protection [13]
Siponen (2007)	Perceived severity, self-efficacy and response efficacy and sanctions have a significant impact on compliance with information security policies [22]
Gurung (2009)	The perceived severity, self-efficacy, and response efficacy are significantly related to use anti-spyware tools [7]
Johnston (2010)	Fear appeals do impact end user behavioral intentions to comply with recommended individual acts of security. Perception of self-efficacy, response efficacy, threat severity, social influence affect security behavior intent [12].
Ifinedo (2012)	Subjective norms, attitude toward compliance, self-efficacy, and response efficacy and perceived vulnerability positively influence on compliance behavior of information system security policy [10].
Hanus, Wu (2016)	Security awareness significantly affects perceived severity, response efficacy, self-efficacy and response cost. Constructs in coping appraisal process (except response cost) significantly impact recommended security behavior [8].
Jee, B.S (2011)	Users' protection behavior 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 [11].
Park, H.S (2013)	Self-efficacy, response efficacy, and perceived severity are significantly related to privacy awareness, and privacy protection awareness have a positive effect on protection behavior on SNS [35].
Park, C.U (2014)	Perceived vulnerability, severity, self-efficacy, and Privacy rights awareness have a positive impact on privacy behavior. Perceived barriers has a negative impact on privacy behavior[33]
Kim, S.H (2015)	The higher subjective norm, perceived usefulness, technology awareness, self-efficacy, the more intent to use security technology[32]

2.2 통합 기술 수용 이론 (UTAUT/UTAUT2)

Venkatesh, Morris, Davis, and Davis(2003)은 조직의 생산성 향상 등을 위한 IT 시스템 사용자(종업원)의 이용 의도와 행동을 위한 이론으로 TRA, TAM(Technology Acceptance Model), MM(motivation model), TPB, MPCU(model of PC utilization), IDT(innovation diffusion theory), SCT(social cognitive theory) 등을 통합한 UTAUT (Unified Theory of Acceptance and Use of Technology) 제시 하였다[23]. UTAUT는 행동의도(behavioral intention)에 영향을 주는 예측변수로 성과기대(Performance expectancy), 노력기대(Effort expectancy), 사회적 영향(Social influence), 촉진조건(Facilitating conditions) 제시 하였다.

□ 성과 기대 - 새로운 IT시스템 사용이 업무 성과를 높이는데 도움을 될 것이라고 믿는 정도
□ 노력 기대 - 새로운 IT시스템 사용이 쉽거나 어려운 정도
□ 사회적 영향 - 다른 중요한 사람들이 새로운 시스템을 사용하는 것이 중요하다고 믿는 정도
□ 촉진조건 - 새로운 정보기술을 사용하기 위한 조직적 자원과 기술적 기반이 갖춰져 있다고 믿는 정도
□ 행동의도 - 어떤 기술을 사용할 의도가 있는지의 정도

Venkatesh, Thong, and Xu(2012)는 일반 소비자(consumer)의 기술사용에 관심을 갖고, 쾌락 동기(hedonic motivation), 가격 가치(price value), 경험과 습관(experience and habit) 을 추가하여 UTAUT2로 확장 하였다[24].

□ 쾌락 동기 - 기술을 사용함으로써 발생되는 즐거움(fun)
□ 가격 가치 - 기술사용에 따른 비용과 이익 사이의 소비자가 갖는 인지적 교환 조건(trade-off)
□ 경험과 습관 - 학습으로 인해 행동을 자동적으로 수행하려는 경향의 정도

기업 내의 종업원과 다르게, 일반 사용자에게 가격은 중요한 요소인데, 소비자는 직접 제품이나 서비스를 구매(비용 지불)해야 하기 때문이다. 기술사용의 이익이 금전적 비용보다 더 크다고 지각될 때에, 소비자의 기술사용 의도에 긍정적 영향을 준다. 또한 이전 기술의 사용(경험)은 미래의 기술사용에 강력한 예측변수이다. 습관은 기술사용에 직접적 영향을 주고, 이전 경험으로부터 피드백(feedback)은 다양한 신념에 영향을 주게 되어, 결과적으로 행동에 영향을 준다[24].

UTAUT나 UTAUT2는 정보보호 기술사용 의도를 분석하기 위한 요소들을 포함하고 있지만, UTAUT에 기반을 둔 IT 보안 기술의 수용에 대한 연구는 부족한 편이다. UTAUT는 위험을 완화 하거나, 손실을 회피하는 기술 보다는 이익과 업무 성과를 제공하는 새로운 기술의 수용 연구에 더 적합하다고 할 수도 있다[3]. 기술수용모델(TAM), UTAUT 이론들은 여러 유형의 IT 시스템에 적용 되었지만, 방화벽, 안티-바이러스 등과 같은 보안 제품을 사용하지 않는 영향에 대해서는 고려하지 않았다. UTAUT나 기존의 기술 수용 모델에 기반을 둔 연구는 IT 시스템을 사용할 것인가 혹은 그렇지 않을 것인가에 한정하고 있어

서, 사용하지 않더라도 어떤 피해를 초래하지는 않는다[3, 27 30,]. 그러나 IT 보안 기술를 사용하지 않는 것은, 부정적인 결과(해킹, 서비스 거부 공격, 정보유출 등)를 초래한다.

Arekete(2014)는 UTAUT를 IT보안에 적용한 연구에서 노력 기대와 사회적 영향이 사용 행동에 직접적인 영향을 주는데, 기대되는 성과는 촉진조건(예:IT보안 전문가 업무 스킬과 역량)에 의해 직접적인 영향을 받을 수 있다고 하였다. 촉진 조건들은 개인이 기술에 대한 충분한 교육 훈련과 지원을 받으면 보안 행동을 더 쉽게 수행할 수 있다고 하였다[1].

정재원(2012)은 "스마트시대의 개인정보보호기술 수용에 대한 실증연구"에서 UTAUT의 연구모형을 설계하여 개인정보 보호기술의 수용의도에 영향을 미치는 요인을 분석 하였는데, 예상되는 성과, 사회적 영향, 촉진조건은 개인정보보호 기술 수용 및 이용에 긍정적 영향을 미치는 것으로 나타났으며, 예상되는 노력은 기각 되었다[39].

Ⅲ. 연구모형 및 가설

문헌 연구에서 고찰한 보호동기이론, UTAUT를 통해, 정보보호 행동을 요인 분석을 위한 연구문제와 이에 대한 가설과 연구 모형을 다음과 같이 설계하였다.

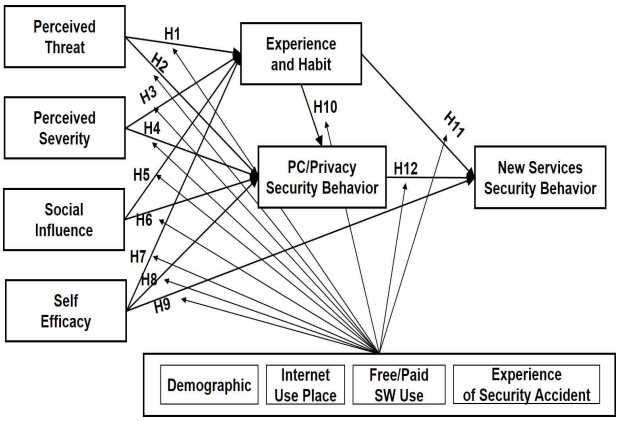

그림 1. 연구 모델
Fig. 1. Research Model

[연구문제 1] 인터넷 이용자의 정보보안 행동에 영향을 주는 요인들은 무엇이며, 어떠한 영향을 미치는가?

연구문제 1은 보호동기 이론과 UTAUT2의 변인들이 종속변수인 신규 정보서비스의 보안 행동에 어떤 영향을 미치는지를 실증하기 위한 것이다. 정보보안 행동을 분석하기 위해서는, 보호동기 이론의 인지된 취약성, 인지된 심각성, 자기효능감, 대응효능감, 장애와 UTAUT2의 사회적 영향, 촉진조건, 경험 및 습관, 가격가치 등을 고려하는 것이 적절하다고 판단하였다. 정보보안 기술의 사용 측면에서 보호 동기 이론과 UTAUT 모델을 비교해 보면, UTAUT는 보호동기 모델의 인지된 취약점과 인지된 심각성과 같은 구성 요소가 없다. UTAUT는 IT 기술 사용의 유형적인 이익에 집중하였기 때문에, 보안 기술을 사용하지 않음으로 발생되는 잠재적인 피해나, 보안 기술을 사용하더라도 간접적, 무형의 이익을 주는 보안 기술들은 UTAUT의 대상이 아니었다. 그래서 보안 기술의 수용을 설명하기 위해서는 인지된 취약점이나 인지된 심각성과 같은 구성요소가 필요하다. 반면에, 보호동기 이론은 사회적 영향이나 촉진조건, 경험 및 습관을 포함하지 않는다. 많은 기술 수용 관련한 문헌 연구는 사회적 영향과 촉진조건의 관계를 지지하고 있어서, 그러한 관계가 IT기술의 일부분인 보안 기술의 사용의도에도 존재할 것이 라는 가정은 합리적으로 보인다.

먼저, 보호 동기이론과 관련된 연구들에서 인지된 위협과 심각성이 높을수록 보호 행동은 증가한 것으로 나타났다. 따라서 인지된 위협, 심각성은 보안 제품의 이용의 경험 및 습관, PC나 개인정보보호 행동에 정(+)의 영향을 미칠 것으로 예측 하였다.

H1: 인지된 위협은 보안 제품 이용의 경험 및 습관에 정(+)의 영향을 미칠 것이다.

H2: 인지된 위협은 PC나 개인정보보호 행동에 정(+)의 영향을 미칠 것이다.

H3: 인지된 심각성은 보안 제품 이용의 경험 및 습관에 정(+)의 영향을 미칠 것이다.

H4: 인지된 심각성은 PC나 개인정보보호 행동에 정(+)의 영향을 미칠 것이다.

UTAUT의 사회적 영향은 정보보호 제품을 사용하거나, 권고된 하는 것이 중요하다고 믿는 정도로 조작적 정의를 할 수 있는데, UTAUT의 사회적 영향은 주관적 규범(Subjective Norm)을 포함하고 있다[23]. 관련 연구들에서도 정보보안 기술사용에 대한 사회적 영향(주관적 규범)이 높을수록 정보보안 행동 의도는 높은 것으로 나타나고 있다. 따라서 사회적 영향은 보안 제품의 이용의 경험 및 습관, PC나 개인정보보호 행동에 정(+)의 영향을 미칠 것으로 예측 하였다.

H5: 사회적 영향은 보안 제품 이용의 경험 및 습관에 정(+)의 영향을 미칠 것이다.

H6: 사회적 영향은 PC나 개인정보보호 행동에 정(+)의 영향을 미칠 것이다.

보호동기 이론의 독립 변수 중에서 자기효능감은 행동의도에 가장 강력한 효과를 갖고 있음이 밝혀졌다[2, 4, 5, 16, 18] 보호동기이론의 자기효능감과 UTAUT의 촉진조건은 비슷한데, 자기효능감은 사용자가 추천된 대응 행동을 잘 수행할 능력을 갖고 있는지를 나타내는 반면에, 촉진조건은 개인의 새로운 IT기술사용 지원을 위한, 조직적 자원과 기술적 기반이 갖춰져 있다고 믿는 정도를 나타낸다. 인터넷 이용자의 경우, 정보보호 행동을 위한 최신 정보보호 관련 정보나 이슈에 대한 관심과 최신 정보보호 관련 학습 자료에 대한 이해/검색 용이성 및 풍부한 학습 자료 제공, 침해사고 발생 시 침해사고 대응센터 등 상담 및 조치 등이 자기효능감(촉진조건)을 증가시킬 것이다. 실태조사에서 정보보호 제품을 이용하지 않는 이유(복수응답)

로 '이용방법을 몰라서'가 41.3%로 가장 높았고, 운영체제 보안패치 업데이트를 실시하지 않는 이유(복수응답)로는 '직접관리하지 않아 모름(38.5%)' '업데이트하는 것이 번거로움(24.8%)', '업데이트 하는 방법을 모름(23.1%)' 등의 순으로 조사되어[37], 인터넷 이용자의 자기효능감이 정보보호 제품 이용이나 행동에 중요한 영향을 미칠 것으로 예측 하였다.

H7: 자기효능감은 보안 제품 이용의 경험 및 습관에 정(+)의 영향을 미칠 것이다.

H8: 자기효능감은 PC나 개인정보 보호 행동에 정(+)의 영향을 미칠 것이다.

UTAUT의 촉진조건은 기술 이용 의도를 통해 기술 이용에 영향을 주기도(간접효과) 하지만, 기술 이용에 직접적인 영향(직접효과) 을 미친다. 따라서 자기효능감에 아래 가설을 추가하였다.

H9: 자기효능감은 신규 정보서비스의 보안 행동에 정(+)의 영향을 미칠 것이다.

[연구문제 2] 인터넷 이용자의 이전 정보보호 제품(예:안티-바이러스)의 사용 경험과 습관은 신규 서비스의 보안 행동에 어떤 영향을 미치는가?

UTAUT2의 이전 기술의 사용 경험과 습관은 미래의 기술 수용과 행동을 예측하기 위한 매우 중요한 변수인데, 이전 기술의 사용 경험과 습관을 통해 미래의 기술 수용과 행동을 예측할 수 있다. 관련연구에서도 경험은 촉진조건과 사용의도 관계를 조절할 수도 있는데, 경험이 많을수록 기술과 사용자의 학습을 촉진하는 것으로 나타났다[24]. 인터넷 이용자의 대부분(85.8%)은 PC 관련 정보보안 제품 (안티-바이러스, 안티-스타이웨어, 보안 USB, OTP 등) 이미 사용하고 있고, 악성코드 검사, 백업, 백신 업데이트 자동화 등의 습관을 갖고 있으며, 개인정보 유출 방지를 위한 행동을 경험하고 있다[37]. 이러한 정보보호 제품 이용이나 개인정보보호 행동의 경험과 습관이 신규 서비스(모바일, 무선 랜, SNS, 클라우드)의 정보 보안 행동에 어떤 영향을 미치는지 분석하기 위해 가설을 설정하였다.

H10: 보안 제품 이용의 경험 및 습관은 PC나 개인정보보호 행동에 정(+)의 영향을 미칠 것이다.

H11: 보안 제품 이용의 경험 및 습관은 신규 정보서비스의 보안 행동에 정(+)의 영향을 미칠 것이다.

H12: PC나 개인정보보호 행동은 신규 정보서비스의 보안 행동에 정(+)의 영향을 미칠 것이다.

[연구문제 3] 인구통계학적 특성(성별, 연령, 학력, 소득)과 전해년도 보안침해사고 경험, 유료 보안 제품 사용 여부 등은 인터넷 이용자의 보안 행동에 어떤 영향을 주는가?

본 연구에서는 인구통계학적 특성(성별, 연령, 학력, 소득), 인터넷 이용장소, 유료/무료 보안 제품 이용, 전해년도 침해사고 경험을 조절변수로 설정하였고, 조절효과가 있을 것으로 예측 하였다.

표 2. 조작적 정의 및 측정변수

Table 2. Definitions and Measurement of the Constructs

Construct	Measure		Source
Perceived Threat (THR)	THR1	Malware threats	PMT
	THR2	Threat of personal information leakage	
	THR3	Phishing/pharming/ smishing threats	
	THR4	Ransomware threats	
Perceived Severity (SER)	SER1	Malware severity	PMT
	SER2	Severity of personal information leakage	
	SER3	Phishing/pharming/ smishing Severity	
	SER4	Ransomware Severity	
Social Influence (SOC)	SOC1	The degree of recognition of importance of security	UTAUT
	SOC2	The degree of recognition of the importance of privacy	
Self Efficacy (SELF)	SEL1	The degree of interest in information security	PMT, UTAUT
	SEL2	The degree of information security learning activity	
	SEL3	The degree of ease of security learning	
Experience and Habit (HAB)	HAB1	The degree of use of security software product	UTAUT2
	HAB2	Malware Inspection Cycle	
	HAB3	Vaccine update cycle	
	HAB4	The degree of update automation	
PC/Privacy Behavior (PCP)	PCP1	PC/Network Security Behavior	
	PCP2	Secure password management behavior	
	PCP3	Purpose of providing personal information	
	PCP4	Personal Information Leak Prevention Behavior	
New Service Security Behavior (NEW)	NEW1	Smart Device security Behavior	
	NEW2	Wireless LAN security behavior	
	NEW3	SNS security behavior	
	NEW4	Cloud security behavior	

인터넷 이용자의 정보보호 행위를 분석하기 위한 구성요소의 조작적 정의와 측정 항목은 위의 표2와 같다.

Ⅳ. 실증분석

4.1 표본의 특성

한국 인터넷 진흥원(KISA)은 인터넷 이용자들의 정보보호 인식 수준을 파악하기 위해, 전국의 만 12~59세의 인터넷 이용자를 대상으로 방문 면접조사 통해 조사하고 있다[37]. 본 연구에서는, 모바일, 무선 랜, SNS 이용자를 대상으로, 결측 데이터와 불성실 데이터를 제외하고 분석 하였다.

표 3. 인구통계학적 특성
Table 3. The Demographic Characteristic of Data

Category			%	Category			%
Gender	Male	1,295	52.6	Income(A)	~200	59	2.4
	Female	1,165	47.4		200~300	408	16.6
Age	12~19 old	443	17.6		300~400	929	37.8
	20's	564	22.9		400~500	688	28
	30's	527	21.4		500~	376	15.3
	40's	523	21.2	B	No	909	37
	50's	411	16.7		Yes	1,551	63
Education	E1	334	13.5	C	No	2,160	87.8
	E2	712	28.9		Yes	300	12.2
	E3	333	13.5	D	No	2,047	83.2
	E4	1,081	43.9		Yes	413	16.8

* E1 – Elementary, middle and high school students
E2 – under high school graduate
E3 – College(graduate) student
E4 – College or higher
A: ten thousand won (unit)
B: Public/commercial Internet Access
C: Use paid security products
D: Experience of previous year's infringement

4.2 측정 항목의 타당성 및 신뢰도 분석

구성 개념의 측정 항목들의 집중타당성과 판별타당성을 평가하기 위해 AMOS의 확인적 요인 분석을 한 결과는 표4, 표5와 같다.

구조방정식 모델의 집중타당성을 검증하기 위해서는 표준화 계수가 0.5이상이어야 하며, 개념 신뢰도 (CR: Composite Reliability)값이 0.7 이상이 되어야 하며, 평균분산추출(AVE: Average Variance Extracted)값이 0.5 이상이면 측정 도구의 신뢰성이 있는 것으로 볼 수 있다.

판별타당성을 검증을 확인하기 위해, 변수 간의 평균분산추출(AVE) 값이 상관계수의 제곱값 보다 반드시 커야 한다. 잠재요인 각각의 표준 분산 추출값(AVE)과 잠재요인 간의 상관관계 제곱을 비교한 결과, 표준분산추출(AVE) 값이 모두 상관관계 제곱보다 크므로, 집중 타당성가 판별 타당성이 있다고 할 수 있다.

표 4. 집중 타당성 분석 결과
Table 4. The result of Convergent Validity

Constructs	Measure	Factor Loading	CR	AVE
THR	THR1	.682	.789	.555
	THR2	.707		
	THR3	.630		
SER	SER4	.733	.798	.571
	SER3	.664		
	SER2	.598		
SOC	SOC2	.800	.902	.822
	SOC1	.769		
SEL	SEL2	.780	.879	.710
	SEL3	.727		
	SEL1	.631		
HAB	HAB2	.975	.912	.785
	HAB3	.961		
	HAB1	.538		
PCP	PCP1	.645	.827	.583
	PCP2	.610		
	PCP3	.668		
	PCP4	.575		
NEW	NEW3	.795	.813	.591
	NEW2	.824		
	NEW1	.837		

표 5. 판별 타당성 분석 결과
Table 5. The result of discriminant Validity

	THR	SER	SOC	SEL	HAB	PCP	NEW
THR	.525						
SER	.378	.571					
SOC	.278	.299	.785				
SEL	.107	.194	.148	.822			
HAB	-.022	.243	.097	.242	.710		
PCP	.183	.305	.248	.423	.417	.583	
NEW	.026	.274	.269	.201	.213	.390	.591

4.3 가설 검증

가설검증을 위한 경로분석 과정에서 사회적 영향이 신규 정보 서비스의 보안 행동에 직접적으로 정(+) 영향을 주는 가설이 추가되었다. 정보보호 제품 이용 경험 및 습관에 영향을 미치는 요인으로 인지된 위협, 심각성, 자기효능감이 채택되었고, 인지된 심각성, 자기효능감이 높은 영향을 주지만, 사회적 영향은 기각되었다(C.R.=1.230, p=.219). PC 와 개인정보보호 행동에 영향을 미치는 요인으로 인지된 위협, 인지된 심각성, 사회적 영향, 자기효능감이 채택되었고, 자기효능감이 높은 영향을 주는 것으로 나타났다. 신규서비스의 정보보호 행동에 영향을 미치는 요인으로 경험 및 습관, PC나 개인정보보호 행동, 사회적 영향이 채택되었고, PC나 개인정보보호 행동이 높은 영향을 미치지만, 자기효능감은 기각되었다 (C.R.=1.037, p=.300).

표 6. 가설 검증 결과
Table 6. The Result of Path Analysis

Hypothesized Path		Standardized Estimate	S.E.	C.R.	p-value	Result
H1	THR→HAB	-.146	.053	-5.32	***	Supported
H2	THR→ PCP	.069	.026	2.37	.018	Supported
H3	SER→HAB	.250	.054	8.69	***	Supported
H4	SER→PCP	.123	.027	3.96	***	Supported
H5	SOC→HAB	.031	.054	1.23	.219	NOT
H6	SOC→PCP	.117	.027	4.30	***	Supported
Ha	SOC→NEW	.183	.043	7.23	***	Supported
H7	SEL→HAB	.204	.025	8.69	***	Supported
H8	SEL→PCP	.301	.013	11.2	***	Supported
H9	SEL→NEW	.028	.023	1.03	.300	NOT
H10	HAB→PCP	.304	.012	12.3	***	Supported
H11	HAB→NEW	.060	.019	2.50	.012	Supported
H12	PCP→NEW	.311	.056	9.45	***	Supported

χ^2=1192.414,df=172,CMIN/df=6.933,RMSEA=.049 GFI=.956 AGFI=.941,PGFI=.712,CFI=.947,NFI=.939,IFI=.947, PNFI=.769,PCFI=.776

*** p-values < 0.01
Not = Not Supported (기각), Supported (채택)

4.4 조절효과 분석

조절효과 분석은 대응별 모수 비교 (pairwise parameter comparison) 방법을 하였는데, 모수의 차이(critical ratio for difference between parameters)가 ±1.96 이상이거나 또는 ±2.58 이상이면 각각 α=0.05, α=0.01에서 유의한 차이가 있다고 할 수 있다.

여성의 경우 자기효능감이 PC/개인정보보호 행동에 남성보다 더 영향을 미치는 것(남성: .264, 여성: .364, 차이검정통계량 (2.31) 유의확률 99%) 으로 나타났다.

40대 이하는 자기효능감이 정보보호 제품 이용 경험 및 습관에 더 영향을 미치는 반면, 40대 이상은 경험 및 습관이 PC/개인정보보호 행동에 더 큰 영향을 미치며, PC/개인정보보호 경험이 신규 서비스의 정보보호 행동에 더 큰 영향을 미치는 것으로 나타났다.

표 7. 연령에 따른 조절 효과 분석
Table 7. Moderating Effects of Age

Hypothesized Path	Age Group				Critical Ratio for difference
	Under 40's		more than 40's		
SEL→ HAB	.324	***	.245	***	2.535
HAB → PCP	.200	***	.415	***	3.468
PCP → NEW	.246	***	.427	***	3.106

주: *** p-value <0.001

대졸 이상 이용자들은 사회적 영향 → PC나 개인정보보호 행동에 영향(.142, p-value(***))을 주지만, 고졸 이하(초/중/고등학생 포함)는 (0.029, p-value(.288)) 기각 되었다.

월 가구 소득이 많을수록(300만원 이상) 사회적 영향이 신규 서비스 보호 행동에 더 큰 영향을 미치고, 경험 및 습관이 PC/개인정보보호 행동에 더 큰 영향을 주는 것으로 나타났다.

상업 시설이나 공공 인터넷을 사용하지 않는 그룹(.172 p-value (***))이 사용하는 그룹(.085 p-value (***), 차이검정통계량:-2.143)) 보다 사회적 영향이 신규 정보서비스의 보안 행동에 더 큰 영향을 미치는 것으로 나타났다.

침해사고를 경험한 이용자는 사회적 영향(정보보호 중요성)이 PC/개인정보보호 보안 행동에 매우 큰 영향을 주고, 개인정보보호 행동이 신규 서비스의 정보보호 행동에 는 큰 영향을 마치는 것으로 나타났지만, 사회적 영향, 경험 및 습관이 직접 신규 서비스의 정보보호 행동에 미치는 영향은 기각되었다.

표 8. 침해사고에 따른 조절 효과 분석
Table 8. Moderate Effects of Security Accident in last year

Hypothesized Path	Security accident experience				Critical Ratio for difference
	No		Yes		
SOC→PCP	.048	.102	.350	***	-2.738
SOC→NEW	.187	***	.059	.373	2.538
SEL→NEW	.053	.047	-.007	***	1.959
HAB→NEW	.070	.005	-.056	.316	2.068
PCP→NEW	.286	***	.588	***	-2.43

주:* p-value <0.05, ** p-value <0.01, *** p-value <0.001

유료 보안제품 이용자는, 사회적 영향이 경험 및 습관에 더 큰 영향을 미치지만, 신규 서비스의 보안 행동 미치는 영향은 기각 (p-value(.658))되었고, 무료 이용자는 사회적 영향이 신규 정보서비스의 보안 행동에 영향을 미치며, 경험 및 습관에 미치는 영향은 기각(p-value(.735) 되었다.

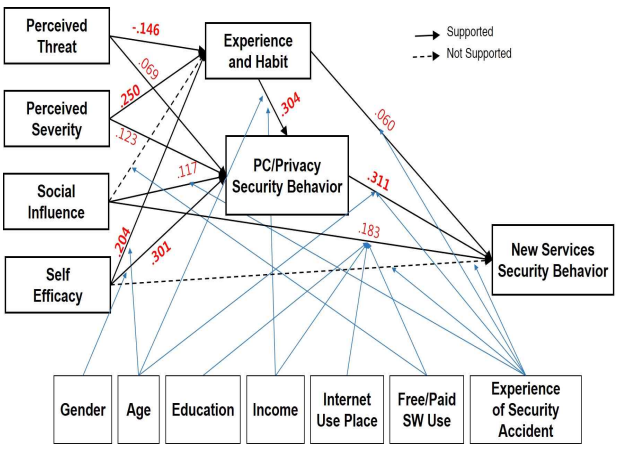

그림 2. 가설 및 조절효과 검증 결과
Fig. 2. Hypothesis and Moderating Effects Result

Ⅴ. 연구결과

본 연구에서는 인터넷 이용자의 정보보호 수준 제고를 위해서 인지된 위협, 심각성, 사회적 영향, 자기 효능감이 정보보호 제품 경험 및 습관, PC/개인정보보호 행동, 신규 서비스의 정보보호 행동에 미치는 전체 경로를 파악했다. 인터넷 이용자의 경우, 경제적, 기술적 지원을 기대할 수 없는 환경에서, 진화하는 보안 위협에 노출되고 있고, 피해 사례도 증가하고 있어, 보안 위협에 대응하기 위해서는 다음과 같은 정책적 고려가 필요하다.

첫째, 인지된 위협이 정보보호 제품 이용 경험 및 습관에 부정적인(-) 영향을 미치는 것으로 나타났다. 이는 Witte(1992)의 병행과정 확장모델(EPPM)에서 설명한 것처럼 위협이 대응효능감이나 자기효능감보다 커서 보안 제품 이용이 적거나, 악성코드 검사나 업데이트를 잘 하지 않는 것으로 보인다. 정보보호 실태 조사에서 대부분 무료 보안 제품을 사용하고 있고, 유료 보안 제품을 사용하거나 운영체제에 탑재된 보안 제품을 사용하는 비율(43.9%)은 낮게 나타나고 있다[37]. Windows의 경우 Windows Defender 뿐만 아니라, Windows 10에서는 생체 인증을 통한 계정보호나 디스크 암호화나 업무용과 개인용 PC 분리, 부트 레코드 암호화, 멀웨어 방지나 신뢰할 수 있는 응용프로그램만 실행하게 하는 기능을 탑재하여 사용자의 보안 환경을 강화하고 있다. 20대, 대학(원)생, 전문/관리직은 운영체제 보안제품 이용률이 상대적으로 높은데, 자기효능감이 운영체제에 탑재된 보안 소프트웨어 사용에 영향을 주는 것으로 판단된다. 이에 대한 더 깊은 연구가 필요할 것으로 보인다.

둘째, 인지된 심각성과 자기효능감이 정보보호 제품 이용 경험과 습관에 높은 영향을 주는 것으로 나타났는데, 병행과정 확장모델(EPPM)에 제시된 것처럼, 높은 심각성에 대해 높은 자기효능감이 있는 경우에 정보보호 행위도 높아진다는 것을 보여준다. 특히 20대, 30대는 자기효능감이 높아 정보보호 제품 이용이 높은 반면, 40대 이후 연령층은 정보보호 관련 정보 수집 및 학습활동이 낮으며, 정보 수집 및 학습 어려움이 많은 것으로 나타났다. 이에 따라 정보보호 관련 제품 이용률이 상대적으로 낮고, 악성코드 검사 주기 등이 낮게 나타나고 있다. 자기효능감은 PC/개인정보보호 행동에도 가장 높은 영향을 미치는 것으로 나타나고 있어서 정보보호 제품 이용 및 PC/개인정보보호를 향상을 위해서는 자기효능감을 높이는 정책이 가장 필요하다. 하지만, 인터넷 이용자 의 대부분은 관련 정보를 대부분 인터넷에서 스스로 검색(44.1%)하거나 주변으로부터 정보를 확보(42.8%)하고 있고, 정보보호 관련 민간업체(11.7%), 공공기관 문의(7.5%)는 낮은 상황이다. 또한 정보보호 관련 용어가 어렵고(33.2%), 정보의 양이 너무 많아 복잡함(31%)을 느끼고 있다. 인터넷 이용자의 정보보호 수준을 제고하기 위해서는 이용자 스스로 정보보안에 대한 관심과 학습이 필요하지만, 공공기관이나 민간기관(예: 인터넷 서비스 제공자(ISP))의 정보보호 지원 체계 및 이용 활성화 등이 촉진조건이 필요하다. 자기효능감은 새로운 정보서비스의 보안 행동에 미치는 영향이 기각되었는데, 인터넷 이용자의 관심과 학습활동에 신규 서비스에 대한 위협과 대응방안 관련 내용이 어렵거나 관련 자료가 부족한 것으로 파악된다.

셋째, 정보보호 제품 이용의 경험과 습관이 개인정보보호 행동에 높은 영향을 미치고, PC/개인정보보호 경험은 신규 서비스의 보안 행동에 영향을 미치는 연쇄(cascading) 효과가 있는 것으로 나타났다. 이전의 정보보호 경험이 새로운 서비스의 보안 위협 대응에 매우 긍정적인 영향을 미치는 것으로 파악 되었다. 특히 연령, 소득, 전해년도 침해 사고 경험은 이전의 경험이 새로운 정보보호 행동에 영향을 주는 것으로 나타났다. 따라서 신규 서비스의 정보보호 수준 향상을 위해서는 정보보호제품 이용이나 개인정보보호 수준을 향상하는 정책이 병행되어야 한다.

넷째, 사회적 영향은 신규 서비스의 정보보호 행동에 영향을 미치지만, 이미 경험한 보안제품 이용 및 습관에 미치는 영향은 기각 되었다. 안티-바이러스 보안 제품처럼 오랜 경험과 습관은 사회적 영향에 영향을 낮추는 것으로 나타났는데, UAUT2에서도 습관이 증가함에 따라 기술의 사용 의도가 감소함을 제시하고 있다[24].

다섯째, 조절효과 분석에서 연령과 침해사고 경험은 다양한 경로에서 조절효과가 있는 것으로 파악되어, 이에 대한 정책적 고려가 필요해 보인다. 초중고 학생의 경우 정보보호와 개인정보 중요성 인식이 낮게 나타나고 있어, 정보보호 교육을 통해 정보보호 중요성 인식 제고가 필요하다. 20~30대는 신규 정보서비스의 보안 자료 제공 및 학습 환경 용이성 제고를 통해 자기효능감을 높이는 정책이 필요하다. 40대 이상은 정보보호 제품 이용과 개인정보보호 행동 경험을 통해 보안 경험과 습관을 확대할 필요가 있다. 침해사고 경험자의 경우, 정보보호 관심, 학습활동은 높으나, 학습 어려움이 더 높아 자기 효능감이 떨어지고 있다. 침해사고 시 보안업체 및 공공기관, ISP 업체 등 촉진조건(침해사고 대응센터 이용 활성화 등)을 향상할 수 있는 정책이 필요하다. 침해사고가 발생하더라도 이용자는 신고나 상담문의를 하지 않은데(57.9%), 피해가 경미해서(33.7%)라기보다는 신고/상담이 번거롭거나, 절차나 상담기관을 모르거나, 효과가 없어서 (66.3%)가 더 높은 비율을 차지하고 있다.

본 연구의 연구 모델은 이용자는 대부분 무료 보안 제품을 사용하고 있고, 수집된 데이터의 제약 등으로 성과기대(대응효능감), 노력기대 (이용용이성)는 고려하지 않았다. 정보보호 제품을 이용하지 않거나(14.2%), 보안 업데이트를 하지 않는(16.8%)의 경우, 대부분 자기효능감과 관련된 비율이 높지만, 정보보안 제품이 필요가 없거나(40.2%), 효과가 없을 것 같아서(25.1%)로 응답하였고, 운영체제 보안 업데이트가 번거롭거나 (23.1%), 필요성을 느끼지 못하는(21%) 것으로 나타나기도 하였다. 향후 연구를 통해 보안 제품의 대응효능감과 노력기대 (이용 용이성)에 대한 분석도 필요할 것으로 보인다.

참고문헌

[1] Arekete, Samson, Princely Ifinedo, and Boluwaji Ade Akinnuwesi, "Antecedent factors to end-users' symbolic acceptance of enterprise systems: An analysis in Nigerian organization," in *Adaptive Science & Technology (ICAST), 2014 IEEE 6th International Conference,* pp. 1-8, 2014.

[2] Bandura, A., Adams, N. E., Hardy, A. B. and Howells, G. N, "Tests of the generality of self-efficacy theory," *Cognitive therapy and research*, Vol. 4, No. 1, pp. 39-66, 1980.

[3] Chenoweth, Tim, Robert Minch, and Sharon Tabor, "Expanding views of technology acceptance: seeking factors explaining security control adoption," *AMCIS 2007 Proceedings,* 2007.

[4] Condiotte, Mark M., and Edward Lichtenstein, "Self-efficacy and relapse in smoking cessation programs," *Journal of consulting and clinical psychology,* Vol. 49, No. 5, 1981.

[5] Fruin, Donna J., Chris Pratt, and Neville Owen, "Protection motivation theory and adolescents' perceptions of exercise," *Journal of Applied Social Psychology,* Vol. 22, No. 1, pp. 55-69, 1992.

[6] Gore, Thomas D., and Cheryl Campanella Bracken, "Testing the theoretical design of a health risk message: Reexamining the major tenets of the extended parallel process model," *Health Education & Behavior,* Vol. 32, No. 1, pp.27-41, 2005.

[7] Gurung, Anil, Xin Luo, and Qinyu Liao, "Consumer motivations in taking action against spyware: an empirical investigation," *Information Management & Computer Security,* Vol. 17, No. 3, pp. 276-289, 2009.

[8] Hanus, Bartlomiej, and Yu and Wu, "Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective," *Information Systems Management,* Vol. 33, No. 1, pp.2-16, 2016.

[9] Hsu, Chien-Lung, Ming-Ren Lee, and Chien-Hui Su, "The role of privacy protection in healthcare information systems adoption," *Journal of medical systems,* Vol. 37, No. 5, 2013.

[10] Ifinedo, Princely, "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, pp. 83-95, 2012.

[11] Jee, B. S., Fan, L., Lee, S. C., & Suh, Y. H., "Personal Information Protection Behavior for Information Quality: Health Psychology Theory Perspectives," *Journal of the Korean society for quality management*, Vol. 39, No. 3, pp. 432-443, 2011.

[12] Johnston, Allen C., and Merrill Warkentin, "Fear appeals and information security behaviors: an empirical study," *MIS quarterly,* pp. 549-566, 2010.

[13] LaRose, R., Rifon, N., Liu, S., & Lee, D., "Understanding online safety behavior: A multivariate model," *The 55th annual conference of the international communication association*, New York, 2005.

[14] Liang, Huigang, and Yajiong Xue, "Understanding security behaviors in personal computer usage: A threat avoidance perspective," *Journal of the Association for Information Systems,* Vol. 11, No. 7, 2010.

[15] Maddux, James E., and Melinda A. Stanley, "Self-efficacy theory in contemporary psychology: An overview," *Journal of Social and Clinical psychology,* Vol. 4, No. 3, pp. 249-255, 1986.

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

[17] Milne, George R., Andrew J. Rohm, and Shalini Bahl, "Consumers' protection of online privacy and identity," *Journal of Consumer Affairs*, Vol. 38, No. 2, pp. 217-232, 2004.

[18] Milne, Sarah, Paschal Sheeran, and Sheina Orbell, "Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory," *Journal of Applied Social Psychology,* Vol. 30, No. 1, pp. 106-143, 2000.

[19] Mohamed, Norshidah, and Ili Hawa Ahmad, "Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia," *Computers in Human Behavior,* Vol. 28, No. 6, pp. 2366-2375, 2012.

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

[21] Rogers, Ronald W, "Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation," *Social psychophysiology: A sourcebook,* pp. 153-176, 1983.

[22] Siponen, Mikko, Seppo Pahnila, and Adam Mahmood, "Employees' adherence to information security policies: an empirical study, in " *IFIP International Information Security Conference,* Boston, 2007.

[23] Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D., "User acceptance of information technology: Toward a unified view," *MIS quarterly,* pp. 425-478, 2003.

[24] Venkatesh, Viswanath, James YL Thong, and Xin Xu, "Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology," *MIS Quarterly,* Vol. 36, No. 1, pp. 157-178, 2012.

[25] Wang, Ping An, and Easwar Nyshadham, "Knowledge of online security risks and consumer decision making: An experimental study," in *2011 44th Hawaii International Conference on System Sciences,* 2011.

[26] Wang, Ping An, "Assessment of cyber security knowledge and behavior: An anti-phishing scenario, in " *Proc. IEEE Int. Conf. Internet Monitor. Protection (ICIMP),* p. 1-7, 2013.

[27] Wang, Ping An, "Information security knowledge and behavior: An adapted model of technology acceptance," in *2010 2nd International Conference on Education Technology and Computer,* Vol. 2, pp. 364-367, 2010.

[28] Witte, K, The handbook of communication and emotion: Research, theory, applications, and contexts, in P. A.Andersen & L. K.Guerrero Eds. San Diego, CA: Academic Press, pp. 423–450, 1998.

[29] Witte, Kim, "Fear control and danger control: A test of the extended parallel process model (EPPM)," *Communications Monographs,* Vol. 61, No. 2, pp. 113-134, 1994.

[30] Woon, Irene, Gek-Woo Tan, and R. Low, "A protection motivation theory approach to home wireless security," I*CIS 2005 proceedings,* 2005.

[31] Youn, Seounmi, "Teenagers' perceptions of online privacy and coping behaviors: a risk–benefit appraisal approach," J*ournal of Broadcasting & Electronic Media,* Vol. 49, No. 1, pp. 86-110, 2005.

[32] Kim, Sang-Hoon, and Gab-Su Lee, "An Empirical Study on Influencing Factors of Using Information Security Technology," *Journal of Society for e-Business Studies,* Vol. 20, No. 4, pp. 151-175, 2015.

[33] Park, Chanouk, and Sang-Woo Lee, "A Study of the User Privacy Protection Behavior in Online Environment: Based on Protection Motivation Theory," *Journal of Internet Computing and Services,* Vol. 15, No. 2, pp. 59-71, 2014.

[34] Lee, Sang-Gi, Sei-Yoon Lee, and Jeong-Chul Kim, "A Study on Security Vulnerability Management in Electric Power Industry IoT," *Journal of Digital Contents Society,* Vol 17, No. 6, pp. 499-507, 2016

[35] Park, H. S., and S. Kim, "An Empirical Study on SNS Users' Privacy Protection Behaviors," *Management and Economics,* Vol. 46, No. 2, pp. 69-91, 2013.

[36] Jung, J. W, Empirical study on acceptance of personal information protection technology in the 'Smart' era, Ph.D. dissertation, Busan University, Busan, 2012.

[37] KISA. 2016 Survey on Information Security Individual. Available:https://isis.kisa.or.kr/board/?pageId=060200.

[38] KISA. Cyber Threat Trend Report (Q3 2017). Available: https://www.boho.or.kr/data/reportView.do?bulletin_writing_sequence=26797.

이홍제 (Hong-Je Lee)

1998년: 고려대학교 대학원(이학 석사)
2015년: 고려대학교 정보보호대학원 박사수료
2017년: 숭실대학교 일반대학원 재학중 정보관리기술사,정보시스템감리사

※관심분야 : 정보보안, 데이터베이스, 빅데이타, HTML5, 디지털 콘텐츠 등

고형석 (Hyeongseog Kho)

2008년: 서울시립대 경영정보학(석사)
2017년: 숭실대학교 일반대학원 재학 정보관리기술사,정보시스템감리사

※관심분야 : 엔터프라이즈아키텍처(EA), IT거버넌스, 정보화계획, ISP, 정보보안 등

노은희 (Eun-HeeShin Roh)

2001년 : 숙명여자 대학교 대학원 (교육학 석사)
2015년 : 숭실대학교 일반대학원 (공학박사)

2017년～현 재 : 한성대학교 상상력교양교육원 조교수
※관심분야 : HTML5, 하이브리드 앱, 스마트러닝, 디지털 콘텐츠, 정보보안 등

한경석 (Kyeong-Seok Han)

1979년 : 서울대학교 문학사 졸업
1983년 : 서울대학교 경영학과 (경영학 석사)
1989년 : 미국 퍼듀대에서 MIS 박사

1993년～현 재: 숭실대학교 경영학부 교수
※관심분야 : 경영정보시스템,Digital Economy, Agent-Based Simulation, Web Programming,ERP, C++,회계정보시스템, e-Business, 전자상거래, 중소기업정보화, 기업자금지원. 정책 연구, ERP 등