Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.1, Feb. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.1.187

패스워드 보안행위의도에 영향을 미치는 요인*

이 동 희,[1†] 김 태 성,[2‡] 전 효 정[3]
[1]충북대학교 정보보호경영학과, [2]충북대학교 경영정보학과/보안경제연구소,
[3]충북대학교 글로컬보안컨설팅전문인력양성사업단/보안경제연구소

Factors that Affect the Intention of Password Security Behavior*

Dong-Hee Lee,[1†] Tae-Sung Kim,[2‡] Hyo-Jung Jun[3]
[1,2,3]Chungbuk National University/Cybersecurity Economics Research Institute(CERI)

요 약

최근 다양한 핀테크 기술과 바이오 인증의 발달로 인해 사이버 공간에서의 금융 거래 및 전자 상거래가 더욱 빠르고 간편하게 이루어지고 있다. 그러나 이러한 새로운 서비스들에서조차 패스워드를 이용한 사용자 인증 방식은 여전히 큰 비중을 차지하고 있다. 따라서 안전한 패스워드의 생성과 관리는 개인의 정보와 자산을 지키기 위한 기초적이고 필수적인 사항이라고 할 수 있다. 본 연구에서는 설문을 통하여 사용자들의 패스워드 사용 실태를 알아보고, 건강신념모델을 활용하여 패스워드 보안행위의도에 영향을 미치는 요인을 분석하였다. 그 결과, 지각된 민감성, 지각된 심각성, 지각된 이익, 지각된 장애가 패스워드 보안행위의도에 유의한 영향을 미치는 것으로 분석되었으며, 그 중 지각된 심각성이 다른 요인들에 대하여 조절효과를 갖는 것으로 나타났다.

ABSTRACT

Recently, financial transactions and electronic commerce in cyberspace are being performed more quickly and conveniently, with the development in diverse types of fintech and biometric authentication. But user authentication using passwords still occupies a big proportion even in these new services. therefore, safe creation and management of passwords is fundamental and indispensable to protect personal information and asset. This study examined the patterns of password usage by conducting a survey and analyzed factors influencing password security behavior intentions using the heath belief model. As a result, perceived susceptibility, perceived severity, perceived benefits, and perceived barriers significantly affected security behavior intentions, and especially, perceived severity had a moderating effect in other factors.

Keywords: Password, Security behavior intention, Health belief model

I. 서 론

우리나라의 인터넷 이용자 수는 지속적으로 증가하여 2015년 기준 4천만 명을 넘어섰으며, 그 중 대다수는 인터넷을 통한 모바일 뱅킹, 쇼핑, 해외 직접구매, 주식투자 등의 다양한 거래행위를 하고 있다[1]. 또한 다수의 간편 결제 서비스와 비트코인과 같은 가상 화폐 등의 활성화로 인하여 온라인상에서 정

Received(08. 07. 2017), Modified(12. 07. 2017), Accepted(01. 07. 2018)
* 본 연구는 미래창조과학부 및 한국인터넷진흥원의 "고용계약형 정보보호 석사과정 지원사업"의 연구결과로 수행되었음 (과제번호 H2101-16-1001). 이 논문은 2015년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2015S1A5A2A01009763).
† 주저자, iluy3082@gmail.com
‡ 교신저자, kimts@cbnu.ac.kr(Corresponding author)

Table 1. Usage of authentication method (Unit: %)

	Certificate	SMS	i-PIN	E-mail	Credit card	ARS	Biometric
male	72.4	68.5	49.6	41.7	38.1	38.1	4.8
female	75.2	73.0	48.0	47.2	38.6	44.0	4.3
12 to 19 years old	51.1	74.3	49.5	54.3	13.8	25.1	5.9
20s	77.8	72.3	58.0	46.1	34.3	48.4	5.8
30s	75.6	70.5	49.5	40.8	43.8	44.5	4.0
40s	78.7	70.4	46.7	42.7	43.8	41.8	3.7
50s	77.1	66.8	40.5	41.5	40.2	39.0	4.1

※Sources: KISA.(2015) A Survey on Internet Economic Activities

보 유출이 직접적인 금전적 손실로 이어질 수 있는 가능성이 더욱 높아지고 있는 상황이다[2]. Table 1.에서와 같이 온라인 쇼핑과 간편 결제, 인터넷 뱅킹 등과 같은 핀테크 인증수단으로 주로 사용되는 것은 공인인증서, i-PIN, 이메일 등이다. 이처럼 전통적인 아이디와 패스워드를 기반으로 한 사용자 인증 방식은 여전히 대다수를 차지하고 있으며, 이를 이용한 온라인상의 금전거래가 폭발적으로 증가하고 있는 상황에서 패스워드 보안실패는 사용자에게 금전적인 손실로 직결될 가능성이 매우 높아지고 있다. 만일 공인인증서나 이메일 등의 패스워드가 유출되는 경우, 이로 인한 사생활 침해 뿐 만 아니라 타 계정 탈취, 무단 결제 등의 2차 피해가 발생 할 수 있다[3]. 따라서 안전한 패스워드의 생성과 관리는 다양한 인증 수단이 개발된 현재에도 매우 중요한 사항이다. 그럼에도 불구하고 다수의 인터넷 사용자들은 이러한 위험을 인지하지 못하거나 무시하는 경향이 있으며, 안전한 패스워드 생성에 대한 조언이나 패스워드 변경 요청을 무시하는 경우가 많다[4]. 이에 본 연구에서는 개인의 패스워드 보안 행위 의도에 영향을 미치는 요인들을 알아보고 개인의 보안행위를 유발하도록 하는 효과적인 방법에 대하여 제시하고자 한다. 특히 비밀번호 유출을 막기 위한 보안 행위가 질병에 걸리는 것을 막기 위한 예방적 건강 행위와 유사하다고 판단하였다[5]. 이에 따라 건강행동이론들 중 하나인 건강신념이론을 기반으로 패스워드 보안행위의도에 영향을 미치는 요인들을 살펴보고자 한다.

II. 이론적 배경

2.1 컴퓨터 보안 행동에 대한 연구

Liang and Xue[6]는 개인 컴퓨터 이용자들의 IT 위협으로부터의 회피 행동을 이해하기 위하여 심리학, 위험 분석, IS 분야의 문헌들을 종합하여 이론을 제안하였다. 이를 기반으로 한 모델을 설문 데이터를 통해 검증한 결과, 실제 위협의 존재와 이를 막기 위한 대처 행동의 유효성을 인식시키는 것이 위협을 회피하기 위한 행동을 유발하는 중요한 요소임을 확인하였다. Stanton et al.[7]은 전문가 인터뷰를 통해서 보안 행위를 기술적인 숙련도와 의도에 따라 총 6가지로 분류하였고, 특히 패스워드 보안 행위에 관련된 설문을 통해 인식교육이나 보상을 통해 보다 바람직한 보안 행동을 유도할 수 있다고 주장하였다. Guo[8]는 조직 내부자의 보안 행동에 관한 다양한 연구에서 상반된 결과가 나오는 이유는 보안 행동에 대한 연구에서 정의한 보안 행동의 개념이 저마다 다른 의미로 사용되었기 때문이며, 이런 정의의 문제를 해소하기 위하여 보안 행동의 개념에 대한 프레임워크를 제시하였다.

2.2 패스워드 보안에 대한 연구

패스워드 보안을 다룬 연구는 크게 안전한 비밀번호의 생성과 관리를 다루는 연구와 패스워드와 관련된 보안 행위에 영향을 미치는 요인들에 대한 연구로 나눌 수 있다. Zviran et al[9]는 보호하고자 하는

데이터의 속성, 패스워드의 길이, 조합, 사용빈도 등의 특성에 따라서 패스워드를 기억할 것인지, 어딘가에 적어놓고 사용할지가 결정된다고 주장하였다. Vu et al[10]은 여러 계정과 패스워드를 제시한 후 이를 각 계정의 패스워드를 기억하도록 하는 실험을 통해 다수의 계정과 패스워드를 사용하는 경우 암호를 적어둘 가능성이 높아지고 공격자에 의한 무차별 공격에 취약해 질 수 있음을 경고하였다. Ives et al[11]는 전자 상거래의 증가로 인한 개별 사용자들이 사용하는 암호가 증가하면서 같은 암호를 반복적으로 사용하는 경우가 많아지는 현상이 발생하였으며, 이는 마치 도미노처럼 하나의 패스워드가 탈취당하는 경우 보안이 잘 갖춰진 시스템도 공격을 받을 수 있음을 경고하면서 개별 사용자들에게 안전한 패스워드 생성과 관리에 대한 교육의 필요성과 이를 위한 학계에서의 연구가 필요하다고 강조하였다. 한편 Adams and Sasse[12]는 사용자들에게 적절한 교육과 처벌의 위협을 통해 적절한 보안 행위가 수행되도록 동기를 부여할 수 있으며, 실제 사용자들의 행태를 고려하지 않은 보안 메카니즘은 오히려 사용자들의 보안 행위의 동기를 떨어뜨려 바람직한 행위를 저해할 수 있음을 경고하였다. Weirich and Sasse[4]는 패스워드 자체로 인하여 보안 문제가 발생하는 경우보다 이를 사용하는 사용자들의 행동에 의해 보안 사고가 발생하고 있으며, 때문에 사용자들로 하여금 보안 정책을 강요할 수 없는 경우에는 다소 불편하지만 보안을 위한 노력을 기울이도록 설득하고 교육함으로써 정보보호를 달성할 수 있다고 주장하였다. 이 외에도 실험을 통해 패스워드의 보안성과 기억 용이성 사이의 상충 관계를 실증적으로 밝힌 Yan et al[13]의 연구가 있다.

2.3 건강행동이론을 적용한 정보보호 분야 연구

Workman et al[14]은 조직원들이 보안 수준을 높이는 행동을 인식하고 있음에도 불구하고 실제로는 실천하지 않는 문제를 제기하고, 이에 대한 해소방안을 제안하기 위하여 보호 동기 이론을 활용하였다. Ng et al[5]는 컴퓨터 보안 행동, 특히 안전한 이메일 사용을 위한 보안 행동에 초점을 맞춘 연구에서 건강 신념 모형을 활용한 모델을 통해 지각된 민감성, 심각성, 이익 등이 이메일에 관련된 보안 행동에 미치는 영향을 밝혔다. Ifinedo[15]는 계획된 행동이론과 보호 동기 이론을 결합한 모델을 구성하여 정보시스템 보안 정책 준수 의도에 관한 설문을 통해 자기 효능감, 반응 효능감 등이 보안 정책 준수 의도에 긍정적인 영향을 미친다는 것을 확인하였다.

III. 연구 모형 및 가설

본 연구에서는 인터넷 사용자들이 안전한 패스워드를 생성하고, 주기적으로 변경하는 행위에 영향을 미치는 요인을 도출하기 위하여 건강신념모형에서 제시하는 주요 변수인 지각된 심각성, 지각된 민감성, 지각된 장애, 지각된 이익, 그리고 행동 계기가 사용자들의 패스워드 보안행위의도에 어떠한 영향을 미치는지 알아보고자 하였으며, 연구모형은 Fig. 1.과 같다. 건강신념모델에서 지각된 심각성(Perceived Seve rity)이란 개인이 질병에 감염되었거나 그 질병을 치료하지 않고 방치하였을 경우 초래될 수 있는 결과의 심각성에 대해 개인이 지각하는 정도를 의미한다[16][17]. 본 연구에서는 패스워드 생성 시 권장되는 사항을 지키지 않거나, 주기적인 변경이 이루

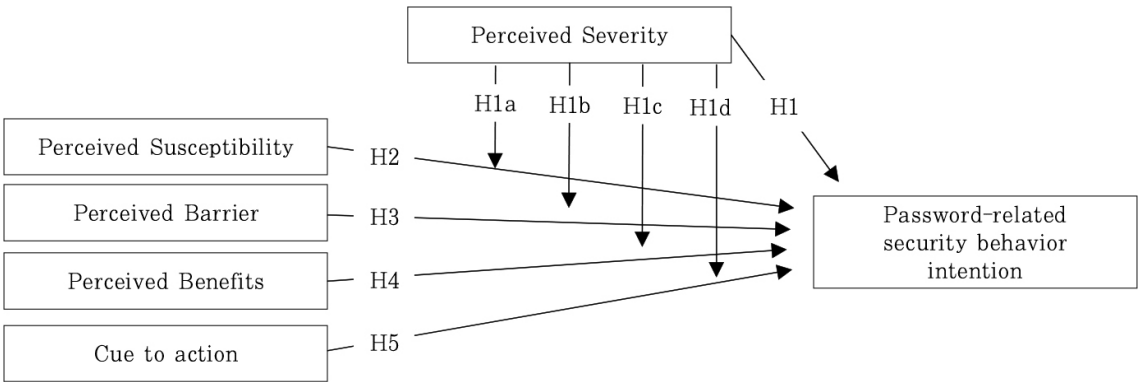

Fig. 1. Research model

어지지 않음으로 인해 발생할 수 있는 보안 사고의 심각성을 지각하는 것으로 정의하였다. 또한 Ng et al[5]의 연구에서 지각된 심각성은 건강신념모델의 다른 변수에 대하여 조절효과를 갖는 것으로 나타났다. 따라서 다음과 같은 가설을 설정하였다.

가설 1. 지각된 심각성은 패스워드 보안 행위 의도에 정(+)의 영향을 미칠 것이다.

가설 1a. 지각된 심각성이 높을수록 지각된 민감성이 패스워드 보안행위의도에 미치는 영향이 크게 나타날 것이다.

가설 1b. 지각된 심각성이 높을수록 지각된 장애가 패스워드 보안행위의도에 미치는 영향이 작게 나타날 것이다.

가설 1c. 지각된 심각성이 높을수록 지각된 이익이 패스워드 보안행위의도에 미치는 영향이 크게 나타난다.

가설 1d. 지각된 심각성이 높을수록 행동 계기가 패스워드 보안행위의도에 미치는 영향이 크게 나타난다.

지각된 민감성(Perceived Susceptibility)이란 한 개인이 자신의 건강을 위협하는 위험에 대한 주관적인 인식을 의미한다[18]. 각 개인들은 같은 조건에 대해서도 매우 다양한 개인적 인식을 갖기 때문에 이러한 인식은 주관적이라고 할 수 있다. 본 연구에서는 자신의 패스워드가 유출되어 무단 변경, 서비스 이용 불가, 개인정보 유출 등의 피해를 입을 가능성에 대해 인지하고 있는지에 대한 것으로 정의하고 다음과 같은 가설을 설정하였다.

가설 2. 지각된 민감성은 패스워드 보안 행위 의도에 정(+)의 영향을 미칠 것이다.

지각된 장애(Perceived Barriers)란 개인에게 권장되는 건강 관련 행위를 하는데 장애가 될 수 있는 부정적 측면을 의미하며, 금전적 지출, 신체적 위험, 불쾌함, 불편함, 시간을 소모하는 것 등을 말한다[18]. 본 연구에서는 패스워드의 생성과 주기적 변경에 따르는 불편함, 귀찮음, 시간 소모 등의 패스워드 보안행위를 실천하는데 방해가 되는 요소들로 정의하고 다음과 같은 가설을 설정하였다.

가설 3. 지각된 장애는 패스워드 보안 행위 의도에 부(-)의 영향을 미칠 것이다.

지각된 이익(Perceived benefits)이란 자신이 질병을 예방하기 위해 하는 행동이 어느 정도 효과가 있을지를 판단하는 주관적인 평가이다[5]. 건강조치는 각 개인에게 충분히 실천가능하고 효과적이라고 판단될 때에 받아들여진다[16]. 본 연구에서는 패스워드 보안행위를 실천함에 따라 자신의 패스워드가 유출 가능성이 낮아지고, 개인정보보호에 미치는 긍정적인 영향에 대해 인지하는 것 등의 보안상의 이익에 대한 주관적인 평가를 의미한다. 따라서 다음과 같은 가설을 설정하였다.

가설 4. 지각된 이익은 패스워드 보안 행위 의도에 정(+)의 영향을 미칠 것이다.

마지막으로 행동 계기(Cues to action)는 병으로 인한 이상 증상과 같은 내부적 요인이나 대중 매체의 선전, 의사의 권유 등과 같은 외부적 요인처럼 건강 관련 행위를 하도록 촉발시키는 요인을 말한다[18] 본 연구에서는 패스워드 보안행위를 하도록 유도하거나, 패스워드의 변경 시기를 상기시키는 것 등을 의미한다. 따라서 다음과 같은 가설을 설정하였다.

가설 5. 행동 계기는 패스워드 보안 행위 의도에 정(+)의 영향을 미칠 것이다.

IV. 실증분석

4.1 표본의 특성

표본은 주 평균 인터넷 이용시간이 가장 많고 공인인증서, 바이오 인증, 간편 결제 등의 개념을 이해하고 사용 경험이 있는 20대 청년층을 대상으로 하였다[1]. 2016년 10월 2일부터 25일까지 온라인 설문을 통해 조사하였다. 총 101개의 회수된 응답 중 불성실한 응답을 제외한 100개의 응답을 분석에 사용하였다. 응답자들의 특성은 총 응답자 100명 중 남자 55%, 여자 45%로 구성되었으며, 평균연령은 25.2세로 나타났다. 또한 응답자들이 사용하는 여러 패스워드 중 비교적 길고 복잡한 것과 짧고 쉬운 패스워드를 비교해서 응답하도록 요청하였다. 길고 복잡한 비밀번호의 경우에는 평균적으로 10개 이상의 자리수로, 특수문자를 포함하는 경우가 88.2%로 대부분

Table 2. Demographics of respondents

	Short, Simple P/W		Long, Complex P/W	
P/W change cycle	Do not change	33.7%	Do not change	25.3%
	3 months	6.4%	3 months	9.5%
	6 months	7.4%	6 months	12.5%
	1 Year	20%	1 Year	23.2%
	over 2 years	32.6%	over 2 years	29.5%
Average P/W digits	9.1 digits		10.7 digits	
Include special characters	55.5%		88.2%	

특수문자를 포함하도록 하고 있었다. 또한 3개월 이내에 비밀번호를 변경한다고 응답한 비율이 9.5%였고, 6개월 이내에 변경하는 경우는 12.6%, 12개월 이내에 변경하는 경우는 23.2%, 그리고 24개월 이상 또는 변경하지 않는다는 응답은 각각 29.5%, 25.3%로 절반 이상이 2년 이상 비밀번호를 변경하지 않거나 전혀 변경하지 않는 것으로 나타났다. 한편, 자신이 사용하는 비밀번호 중 짧고 단순한 비밀번호의 경우 비밀번호의 자리 수가 평균적으로 9.1개였고, 특수문자를 포함한다고 응답한 경우는 55.5%로 상대적으로 특수문자를 덜 포함시키는 것으로 나타났다. 짧고 단순한 비밀번호의 경우 3개월 이내에 비밀번호를 변경한다고 응답한 비율은 6.4%, 6개월 이내 7.4%, 12개월 이상 20%, 24개월 이상 32.6%, 그리고 변경하지 않는다고 응답한 비율은 33.7%로 나타났다.

4.2 측정 모형의 분석

본 연구에서는 수집된 자료를 분석하기 위해 SmartPLS 2.0을 이용하였다. PLS 분석은 구성개념과 측정 문항에 대해 각 변수들의 타당성을 검증하기 위한 탐색적 요인 분석과 확인적 요인분석을 수행하였다. 탐색적 요인 분석으로 각 연구 모형의 변수에 대한 타당성을 검증하기 위하여 신뢰성분석방법인 Cronbach's alpha값을 확인하였다. 그 결과 모든 변수들이 0.7 이상의 값을 갖는 것으로 나타나 설문의 신뢰성이 확인되었다. 또한 확인적 요인분석을 위하여 집중 타당성(Convergent Validity), 내적 일관성 (Internal Consistency), 판별 타당성(Discriminant Validity)의 검증을 실시하였다[19]. 측정 문항의 적합도를 나타내는 복합 신뢰도는 측정 모형의 집중 타당성을 측정하는 지표로 사용되며, Nunnally[20]이 주장하는 기준치인 0.7 이상일 때 복합신뢰도가 확보된다고 할 수 있다. 본 연구에서 사용된 각 변수들의 복합 신뢰성은 모두 0.7 이상으로 이를 모두 충족하였다. 설문을 구성하는 구성개념들의 내적일관성을 검증하기 위한 평균분산추출값(Average Variance Extracted, AVE)은 Fornell and Larcker[21], Chin[22]등이 주장한 기준치인 0.5를 모두 상회하는 것으로 나타나 본 모델은 집중 타당성과 내적 일관성을 만족하였다[Table 3.]. 또한 판별 타당성은 한 잠재 요인이 다른 잠재 요인과 얼마나 다른가에 관련된 것으로, 구성 개념들 간의 상관계수의 대각선 축에 표시되는 AVE 제곱근 값이 다른 구성 개념간의 상관계수보다 큰지를 확인하여 검증된다[11]. 분석 결과 AVE의 제곱근 값 중 가장 작은 값(0.773)이 가장 큰 상관계수(0.605)보다 큰 것으로 나타나 본 연구의 구성개념에 대한 판별 타당성을 검증하였다[Table 4.].

Table 3. Composite reliabilities, AVEs, and Cronbach's alpha

Construct	CR	AVE	Cronbach's alpha
PESU	0.863	0.677	0.782
PESV	0.938	0.717	0.920
PEBA	0.852	0.761	0.828
PEBE	0.941	0.599	0.918
CUEA	0.916	0.687	0.894

Notes.
Composite Reliability(CR), Average Valance Extracted(AVE), Perceived Susceptibility (PESU),Perceived Severity(PESV), Perceived Barrier(PEBA), Perceived Benefits, Cue to Action(CUEA)

4.3 구조 모형의 분석

본 연구에서 제시한 구조모형의 분석결과는 Fig.

Table 4. Discriminant validity

	Perceived susceptibility	Perceived severity	Perceived barrier	Perceived benefits	Cue to action	Behavior intention
Perceived susceptibility	(0.822)					
Perceived severity	0.466	(0.846)				
Perceived barrier	-0.050	0.055	(0.872)			
Perceived benefits	0.440	0.453	-0.193	(0.773)		
Cue to action	0.453	0.423	-0.031	0.335	(0.830)	
Behavior intention	0.448	0.434	-0.337	0.605	0.284	(0.828)

2.와 같다. 경로모델의 설명력을 나타내는 분산설명력(Explained Variance) R^2 값이 0.491로 Falk and Miller[23]가 제시한 적정 검정력인 0.1%를 상회하였다. 경로계수와 PLS의 부스트랩 방식을 이용한 t 값을 통해 살펴본 각 가설의 검증결과는 Table 5.와 같다. 지각된 심각성, 지각된 민감성, 지각된 이익이 패스워드 보안행위의도에 정(+)의 영향을 줄 것이라는 가설이 채택되었으며, 지각된 장애는 패스워드 보안행위의도에 부(-)의 영향을 줄 것이라는 가설도 채택되었다. 한편 패스워드 보안행위의도에 정(+)의 영향을 줄 것으로 가정한 행동 계기는 기각되었다. 또한 지각된 심각성이 다른 독립변수가 종속변수에 미치는 영향력을 조절할 것이라는 가설은 일부 채택되었다. 지각된 심각성의 조절효과를 확인하기 위하여 Chin et al[24]가 PLS를 이용하여 조절효과를 분석하기 위해 제시한 방법을 활용하였다. 이는 조절변수와 조절효과를 측정하고자 하는 하나의 독립변수, 그리고 이 두 변수 간의 상호작용변수를 생성한 후, Bootstrapping과 PLS Algorithm을 통해 상호작용변수의 조절효과와 통계적 유의성을 확인하는 순서로 진행하였다. 그 결과 Table 5.에 제시한 것과 같이 지각된 심각성은 지각된 이익에만 조절효과를 갖는 것으로 나타났다. Chin et al의 조절효과에 대한 연구에서 주장한 바에 의하면, 지각된 심각성의 조절효과로 인하여 지각된 이익의 경로계수(0.434)는 H1c의 0.282를 더한 0.716까지 증가할 수 있다고 해석할 수 있다. 한편 상호작용의 효과를 검증하기 위해 Cohen[25]이 제시한 f^2 값의 크기를 통한 검증방법을 사용하여 확인하였다. 조절효과의 효과크기 f^2는 $[R^2$(상호작용모델)$-R^2$(주 효과모델)$]/[1-R^2$(상호작용모델)$]$의 수식을 통해 계산되며, 그 값이 Cohen이 제시한 임계치인 0.02보다 큰 경우에 조절효과가 존재한다고 할 수 있다. 또한 조절효과의 크기는 $0.02 < f^2 < 0.15$ 인 경우 소-중, $0.15 < f^2 < 0.35$ 인 경우 중-대, 0.35 이상인 경우 큰 효과를 나타내는 것으로 볼 수 있다. 따라서 Cohen의 검증방법을 통해 본 연구의 조절효과의 크기 값 f^2의 값을 계산한 결과, $(0.441-0.362) / (1-0.441) = 0.141$로 소-중 정도의 크기를 갖는 것으로 확인되었

Table 5. Results of hypothesis test

	Coefficient	t-value	Result
H1	0.200	1.797*	supported
H1a	0.137	0.780	Not supported
H1b	-0.029	0.178	Not supported
H1c	0.282	1.724*	supported
H1d	0.121	0.712	Not supported
H2	0.139	1.792*	supported
H3	-0.210	2.040**	supported
H4	0.434	4.556***	supported
H5	-0.100	1.056	Not supported

notes. *p<0.1,**p<0.05,***p<0.01

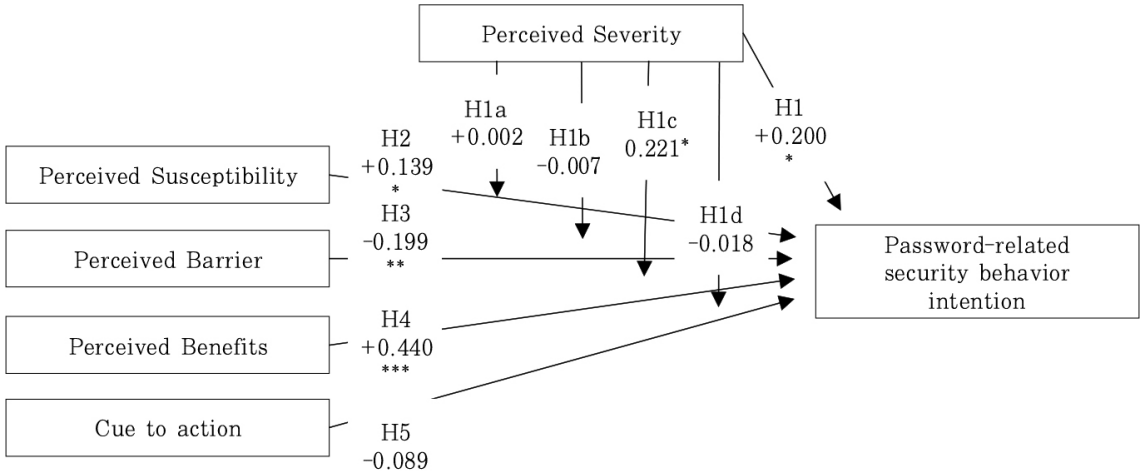

Fig. 2. Result of path analysis *p<0.1,**p<0.05,***p<0.01

다. 따라서 지각된 심각성은 지각된 이익이 패스워드 보안행위의도에 미치는 영향에 대해 조절효과를 갖는 것으로 나타났다. 결과적으로 가설 H1, H1c, H2, H3, H4는 채택되었으며, 가설 H1a, H1b, H1d, H5는 통계적으로 유의하지 않은 것으로 나타나 기각되었다.

한편, 비교적 패스워드 변경 주기가 짧은 그룹과 패스워드 변경 주지가 긴 그룹으로 분류하여 분석을 실시하였다. 본 연구에서는 설문 응답자들에게 본인이 사용하고 있는 패스워드 중 짧고 간단한 패스워드와 길고 복잡한 패스워드를 구분하여 질문하였다. 이를 통해 패스워드 종류에 관계없이 2년 이상 변경하지 않거나, 절대 변경하지 않는다는 응답을 한 사람은 43명이었다. 그리고 두 종류의 패스워드 모두 12개월 이내에 변경한다고 응답한 응답자는 57명 이었다. 따라서 이를 두 개의 그룹으로 분류하여 Fig. 1.의 연구모델로 분석하였으며, 분석 결과는 Table 6·7.과 같다. 먼저 상대적으로 패스워드 변경주기가 짧은 그룹의 경우 지각된 민감성과 지각된 이익만이 패스워드 보안행위의도에 유의한 영향을 미치는 것으로 나타났다. 반면 상대적으로 패스워드 변경주기가 긴 그룹은 지각된 이익과 지각된 장애가 통계적으로 유의한 것으로 나타났다. 특히 기존에 지각된 이익이 가장 큰 영향을 미쳤던 것과는 달리 지각된 장애가 가장 큰 영향력을 갖는 것으로 나타났다. 한편, 집단을 구분하지 않은 분석에서 조절변수로 활용된 지각된 심각성은 집단을 나누어 실시한 분석에서는 조절효과를 나타내지 않는 것으로 확인되었다. 결과적으로 두 개의 집단으로 나누어 실시한 분석의 주요 결과는 다음과 같다. 첫째, 설문 응답자들 전체를 분석한 경우와 마찬가지로 집단을 나누어 분석한 경우에

Table 6. Results of hypothesis test for groups with relatively short password change cycles

	Coefficient	t-value	Result
H1	0.215	1.599	Not supported
H2	0.268	2.068**	supported
H3	-0.149	0.898	Not supported
H4	0.346	2.731***	supported
H5	-0.025	0.182	Not supported

notes. **p<0.05,***p<0.01

Table 7. Results of hypothesis test for groups with relatively long password change cycles

	Coefficient	t-value	Result
H1	0.143	0.763	Not supported
H2	0.202	1.257	Not supported
H3	-0.399	2.857***	supported
H4	0.311	1.752*	supported
H5	-0.063	0.335	Not supported

notes. *p<0.1,***p<0.01

서도 지각된 이익은 종속변수인 패스워드 보안행위의도에 유의한 영향을 미치는 것으로 나타났다. 둘째, 비교적 자주 패스워드를 변경하는 응답자 그룹은 지각된 이익 이외에도 지각된 민감성이 보안행위의도에 유의한 영향을 미치는 것으로 나타났다. 셋째, 패스워드를 변경하지 않거나 변경주기가 상대적으로 긴 그룹의 경우에는 지각된 이익 이외에 지각된 장애가 유의한 영향을 미치는 것으로 나타났다. 특히 지각된 장애의 영향력이 지각된 이익보다 더 큰 것으로 나타났는데, 이 그룹으로 분류된 응답자들은 패스워드 변경으로 인한 불편함, 귀찮음, 시간 소모 등의 요인을 더 크게 지각하는 것으로 나타났다. 넷째, Ng et al[5]의 이메일 보안에 관한 연구와 마찬가지로 본 연구에서도 지각된 이익이 가장 큰 영향을 미치는 것으로 나타났다. 반면 지범석 외[26]의 연구에서는 지각된 발생가능성이 가장 큰 영향을 미치는 요인으로 나타났다. 지각된 발생가능성은 본 연구에서의 지각된 민감성과 동일한 변수이며, 본 연구에서는 지각된 민감성의 영향력이 비교적 작은 것과는 다소 다른 결과이다. 결국 선행연구와 본 연구의 종속변수가 컴퓨터 보안 행위라는 동일한 범주에 속하지만 어떤 종류의 보안행위냐에 따라 건강행동이론 변수의 영향력이 각기 다를 수 있음을 나타낸다. 한편, 패스워드 변경주기에 따라 집단을 구분하여 분석한 결과 패스워드 변경주기가 긴 집단의 경우에는 지각된 장애가 가장 큰 영향을 미치는 요인으로 나타났다. 결국 건강행동이론으로부터 유래한 유사한 독립변수들을 사용하더라도 종속변수의 종류, 응답 대상의 성향에 따라서 보안행위의도에 영향을 미치는 요인은 달라질 수 있다는 것을 알 수 있다.

V. 결 론

5.1 연구 결과의 논의 및 시사점

본 연구의 주요 결과는 다음과 같다. 첫째, 행동계기는 패스워드 보안행위의도에 유의한 영향을 주지 못 한다. 현재 패스워드를 통한 사용자 인증 방식을 채택하고 있는 수많은 서비스에서 사용자들의 패스워드 변경을 유도하기 위한 방법은 일정 기간 동안 패스워드 변경을 하지 않으면 패스워드를 변경할 것을 권유하는 것이다. 그러나 본 연구의 결과에 따르면 패스워드 변경 주기를 알려주는 등의 행동 계기는 패스워드 보안행위의도에 유의한 영향을 미치지 않는 것으로 나타났다. 이는 단순히 행동 계기를 제공하는 것이 보안 행위를 유발하는데 유의한 영향을 미치지 않는다는 다른 연구의 결과와 상통한다[5]. 따라서 일반 사용자들에게 흔히 시행하는 보안 캠페인이나 비밀번호 변경을 장려하는 노력들이 실제 비밀번호 변경과 강한 비밀번호 생성을 유도하는데 효과적인 방법이 아니라는 것을 의미한다. 본 연구의 결과에 따르면 패스워드 보안행위의도를 높이기 위해서는 행동계기를 제공하는 것 대신 패스워드 변경을 통해 얻을 수 있는 보안상의 이익을 인지시키고, 패스워드 유출 가능성과 유출 시 발생할 수 있는 문제의 심각성을 설명해 주는 것이 보다 효과적이다. 둘째, 지각된 이익은 패스워드 보안행위의도에 가장 큰 영향을 미치는 요인이며, 지각된 심각성이 지각된 이익의 영향력에 대해 조절효과를 갖는다는 것을 확인하였다. Ng et al[5]의 연구에서도 지각된 이익은 컴퓨터 보안 행동에 가장 큰 영향을 미치는 변수이며, 지각된 심각성은 지각된 이익과 자기효능감에 대해 조절효과를 나타냈다. 그러나 본 연구와는 달리 지각된 심각성의 조절효과는 부(-)의 영향을 나타내는 것으로 나타났다. 집단을 구분한 경우에도 지각된 이익이 큰 영향을 미치고 있었으며, 특히 패스워드 변경주기가 긴 응답자 집단의 경우에는 지각된 장애가 가장 큰 영향을 미치는 변수로 밝혀졌다. 따라서 컴퓨터 보안 행위 내에서도 이메일 보안, 패스워드 보안 등 어떤 보안행위인지에 따라 독립변수의 영향력이 크게 차이가 날 수 있는 것으로 나타났으며, 지각된 심각성의 조절효과 역시 보안행위의 종류에 따라서 달라질 수 있는 것을 알 수 있었다. 결과적으로 지각된 심각성은 독립변수로서 패스워드 보안행위의도에 상대적으로 작은 영향을 끼치고 있으나, 가장 큰 영향을 끼치는 것으로 나타난 지각된 이익의 효과를 조절하는 변수로 작용한다는 점에서 지각된 이익과 함께 패스워드 보안행위의도를 높이고자 할 때 고려해야할 중요한 변수임을 의미한다. 셋째, 패스워드 보안행위를 실천하는 것에 있어서 장애가 되는 요인을 더 크게 지각하는 사람일수록 보안 행위 의도가 낮은 것으로 나타났다. 특히 패스워드 변경주기가 긴 집단의 경우 지각된 장애가 가장 큰 영향을 주는 변수로 나타났다. 결국 패스워드 생성과 변경에 따른 번거로움, 귀찮음, 시간 소모 등의 장애요인을 줄이는 것은 패스워드 보안행위의도를 높이기 위해 매우 중요한 요인이라 할 수 있다. 특히 지각된 장애를 줄이기 위한 노력, 즉 쉽게 보안성이 높은 패스워드 생성을 돕는

방법 등을 교육하고, 비밀번호 생성 시 보안 정도를 측정하는 비밀번호 진단 도구를 제공하는 등의 노력이 필요하다. 한편, 지각된 장애 또는 대응 비용과 같은 유사한 개념을 사용한 다른 연구들의 결과에서는 지각된 장애가 보안 행위에 유의한 영향을 주지 않는 것으로 나타났다[5][26]. Ng et al[5]의 연구의 경우 이메일 첨부파일과 관련된 보안 행위를 중점적으로 다루었다. 설문 문항으로는 '첨부파일을 함부로 열지 않는다', '송신자를 확인한다' 등의 비교적 간단하고 특정 행위를 하지 않는다는 것을 기본으로 하고 있어 본 연구의 패스워드와 관련된 보안행위에 비해 이메일과 관련된 보안행위실천에 따른 불편함, 귀찮음 등의 장애를 크게 느끼지 않은 것으로 보인다. 또한 지범석 외[26]의 연구에서는 대응 비용이라는 변수가 본 연구의 지각된 장애와 유사하였다. 그러나 본 연구의 지각된 장애와 달리 대응 비용은 종속변수인 보안행위에 유의한 영향을 미치지 않는 것으로 나타났다. 이는 지범석 외[26]의 연구에서 사용된 종속변수인 개인정보보호행위가 패스워드의 생성에 대한 질문으로 구성된 반면, 독립변수인 대응 비용에서는 비밀번호의 변경과 계정 관리에 관한 다양한 문항으로 설문이 구성되어 있었기 때문에 유의하지 않은 결과가 나타난 것으로 보인다. 넷째, 본 연구의 설문 응답자들의 응답에 의하면 짧고 단순한 패스워드의 경우 패스워드를 변경하지 않고 더 오래 사용하는 경향을 보였다. 이는 단순히 한 계정이 탈취되는 것으로 인한 1차적인 피해뿐만 아니라 다른 정보와 결합하여 또 다른 계정의 탈취, 개인정보와 금융정보의 유출 등의 2차적 피해가 발생 할 수도 있다는 사실을 사용자들이 인지하지 못 하거나 무시하고 있다는 것을 의미한다[11]. 따라서 사용자들에게 본인이 사용하는 약한 패스워드의 유출 시 자신의 또 다른 계정이 연쇄적으로 위태로워질 수 있다는 사실을 인지시킬 필요성이 있다. 결과적으로 본 연구는 다음과 같은 시사점이 있다. 첫째, 건강신념모델의 변수를 활용하여 사용자의 패스워드 보안행위의도에 영향을 미치는 요인을 알아내고자 하였으며, 특히 동일한 건강신념모델의 변수라 할지라도 컴퓨터 보안행위의 종류에 따라서 보안행위의도에 미치는 영향이 상이할 수 있다는 것을 검증하였다. 둘째, 건강신념모델의 변수 중 지각된 심각성의 조절효과에 대하여 제시한 Ng et al[5]의 연구결과와 마찬가지로 본 연구에서도 지각된 심각성이 일부 다른 독립변수들의 영향력을 조절한다는 것을 확인하였다. 본 연구에서 지각된 심각성은 패스워드 보안행위의도에 비교적 작은 영향을 미치는 것으로 나타났으나, 가장 큰 영향을 미치는 변수인 지각된 이익의 영향을 조절하는 것으로 나타났다. 따라서 보안행위를 유도하고자 할 때, 지각된 이익에 영향을 미치는 지각된 심각성도 중요하게 고려해야 할 요인인 것으로 밝혀졌다. 셋째, 패스워드 보안행위를 유도하기 위한 가장 보편적인 방법인 행동계기를 제공하는 방식은 보안행위의도에 유의한 영향을 미치지 않는다는 것으로 나타났다. 따라서 이를 대신해 패스워드 보안행위로 인한 보안상의 이익에 대하여 사용자에게 설명하고, 사용자의 패스워드가 유출될 수 있다는 가능성과 유출에 따른 심각성에 대해 인지시키는 것이 보다 효과적인 방법이라는 것을 실증적으로 검증하였다. 넷째, 패스워드 변경주기에 따라 2개의 집단으로 나누어 분석한 결과, 변경주기가 긴 사람들에게서만 지각된 장애의 영향력이 강하게 작용하는 것으로 나타났다. 따라서 지각된 이익과 함께 패스워드 보안행위의도를 결정하는 매우 중요한 요인임을 확인할 수 있었다. 결과적으로 이 같은 본 연구의 결과를 바탕으로 사용자의 패스워드 보안행위의도를 높이기 위한 합리적인 계획수립에 도움을 줄 수 있을 것으로 기대한다.

5.2 연구의 한계와 향후 연구 방향

본 연구의 한계로는 표본이 20대에 편중되어 있어 본 연구의 결과를 전 연령대에 적용하는 것에는 다소 무리가 있다. 또한 일부 웹 사이트나 시스템에서는 강제로 패스워드를 변경해야만 서비스를 이용할 수 있는 경우를 본 연구에서는 반영하지 못하고 있다는 한계가 있다. 한편, 본 연구에서는 사용자들의 실제 행위 대신 행위의도를 측정하였다. 행위의도가 실제 행위를 측정하기 어려운 경우에 행위를 예측하기 위한 합리적인 방법이 될 수 있으나, 가장 좋은 방법은 실제 행위를 측정하는 것이다[27]. 따라서 향후 연구로는 다양한 연령대, 지역, 문화 등을 고려하여 표본을 선정하고, 실제 행위를 측정하기 위하여 실험환경을 조성하거나 기술적인 방법을 통하여 보안행위를 종속변수로 하는 연구가 수행될 필요가 있다. 또한 본 연구에서 종속변수에 가장 큰 영향을 미치는 것으로 나타난 지각된 이익이나 지각된 장애가 다른 변수들을 조절하는 역할을 할 수 있는지 추가적인 연구가 필요하다. 이외에도 일부 집단에서 가장 큰 영향을 미치는 것으로 나타난 지각된 장애를 효과적으로 낮

출 수 있는 방안에 대한 연구가 필요하다. 이에 향후 연구로 패스워드 변경에 따른 장애를 감소시킬 수 있는 여러 방법들 중에 가장 효과적인 방법이 무엇인지 탐색하는 연구가 진행될 수 있을 것이다.

References

[1] Korea internet and Security Agency. "Survey on Internet Utilization in 2015," 2015.

[2] Korea internet and Security Agency, "A Survey on Internet Economic Activities in 2015," 2015.

[3] Korea Communications Commission & Korea internet and Security Agency. "Password Selection and Use Guide," 2010.

[4] Weirich, D., and Sasse, M. A. "Pretty good persuasion: a first step towards effective password security in the real world," Proceedings of the 2001 Workshop on New Security Paradigms pp. 137-143. ACM, Sep. 2001.

[5] 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, pp. 815-825, 2009.

[6] Liang, H., & Xue, Y. "Understanding security behaviors in personal computer usage: A threat avoidance perspective," Journal of the Association for Information Systems, vol. 11, no. 7, pp. 394, 2010.

[7] Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. "Analysis of end user security behaviors," Computers & Security, vol. 24 no. 2 pp. 124-133, 2005.

[8] Guo, K. H.. "Security-related behavior in using information systems in the workplace: A review and synthesis," Computers & Security, vol. 32, no.1, pp. 242-251, 2013.

[9] Zviran, M., and Haga, W. J. "Password security: an empirical study," Journal of Management Information Systems, vol. 15, no. 4, 161-185, 1999.

[10] Vu, K. P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B. L. B., Cook, J., and Schultz, E. E. "Improving password security and memorability to protect personal and organizational information," International Journal of Human-Computer Studies, vol. 65, no. 8, pp. 744-757, 2007.

[11] Ives, B., Walsh, K. R., and Schneider, H. "The domino effect of password reuse," Communications of the ACM, vol. 47, no. 4, pp. 75-78, 2004.

[12] Adams, A., and Sasse, M. A. "Users are not the enemy," Communications of the ACM, vol. 42, no. 12, pp. 40-46, 1999.

[13] Yan, J., Blackwell, A., Anderson, R., and Grant, A. "Password memorability and security: Empirical results," IEEE Security & Privacy, vol. 2, no. 5, pp. 25-31, 2004.

[14] Workman, M., Bommer, W. H., and Straub, D. "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, 2008.

[15] 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, pp. 83-95, 2012.

[16] Lee Byung-Kwan, Oh Hyun Jung, Shin Kyung Ah, & Ko Chae Young. "The effect of media campaign as a cue to action on influenza prevention

behavior: extending health belief model," The Korean Journal of Advertising and Public Relations, vol. 10, no. 4, pp. 108-138, 2008.
[17] Rosenstock, I. M., Strecher, V. J., and Becker, M. H. "The health belief model and HIV risk behavior change," In Preventing AIDS (pp. 5-24). Springer US. 1994.
[18] Janz, N. K., and Becker, M. H.. "The health belief model: A decade later," Health Education & Behavior, vol. 11, no. 1, pp. 1-47, 1984.
[19] Bagozzi, R. P., & Yi, Y. "On the evaluation of structural equation models," Journal of the Academy of Marketing Science, vol. 16, no. 1, pp. 74-94, 1988.
[20] Nunnally, J. C., Bernstein, I. H., & Berge, J. M. T. *Psychometric Theory* (Vol. 226). New York: McGraw-Hill, 1967.
[21] Fornell, C., & Larcker, D. F. "Evaluating structural equation models with unobservable variables and measurement error," Journal of Marketing Research, vol. 18, no. 1, pp. 39-50, 1981,
[22] Chin, W. W., "The partial least squares approach to structural equation modeling," Modern Methods for Business Research, vol. 295, no. 2, pp. 295-336, 1998.
[23] Falk, R. F., & Miller, N. B. "*A Primer for Soft Modeling,*" University of Akron Press, 1992.
[24] Chin, W. W., Marcolin, B. L., & Newsted, P. R. "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, 2003.
[25] Cohen, J., "A power primer," Psychological Bulletin, vol. 112, no. 1, pp. 155, 1992.
[26] Bum Suk Jee, Liu Fan, Sang Chul Lee, and Yung Ho Suh, "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.
[27] Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R., "Future directions for behavioral information security research," Computers & Security, vol. 32, pp. 90-101, 2013.

〈저자소개〉

이 동 희 (Dong-Hee Lee) 학생회원
2015년 8월 : 충북대학교 경영정보학과 학사
2016년 2월~현재 : 충북대학교 정보보호경영학과 석사과정
〈관심분야〉 정보보호정책, 정보보호관리체계, 개인정보보호

김 태 성 (Tae-Sung Kim) 종신회원
1997년 2월: KAIST 산업경영학과 박사
1997년 2월~2000년 8월: 한국전자통신연구원 정보통신기술경영연구소 선임연구원
2005년 1월~2006년 2월: Univ. of North Carolina at Charlotte 방문교수
2010년 7월~2012년 7월: Arizona State University 방문연구원
2000년 9월~현재: 충북대학교 경영정보학과 교수, 보안경제연구소장, 보안컨설팅연계전공 주임교수, 일반대학원 정보보호경영전공 주임교수, 국가정보원 보안관리실태평가 자문 및 평가위원, 행정안전부 전자정부 민관협력포럼 자문위원, 국방부 사이버보안 자문위원, KISA ISMS/PIMS 인증위원회 위원, 한국전력 정보보안 자문위원
〈관심분야〉 정보통신과 정보보호 분야의 경영 및 정책의사결정

전 효 정 (Hyo-Jung Jun) 정회원
2001년 2월: 충북대학교 경영정보학과 학사
2003년 8월: 충북대학교 경영정보학과 석사
2003년 9월~2007년 5월: 한국전자통신연구원 사업기획팀 기술원
2014년 2월: 충북대학교 경영정보학과 박사
2014년 3월~2017년 2월: 충북대학교 정보보호경영학과 Post-Doc
2018년 1월~현재: 충북대학교 글로컬 보안컨설팅 전문인력 양성사업단 Post-Doc
〈관심분야〉 정보보호정책, 정보보호인력, 정보자원관리, 보안경제성