

정보보호 교육이 청소년의 정보보호 실천에 미치는 영향

강민성* · 김태성** · 김택영***

Effects of Information Security Education on the Practice of Information Security for the Youth

Min-Seong Kang* · Tae-Sung Kim** · Taek-Young Kim***

Abstract

As reliance on information and communication becomes widespread, a variety of information dysfunctions such as hacking, viruses, and the infringement of personal information are also occurring. Korean adolescents are especially exposed to an environment in which they are experiencing information dysfunction. In addition, youth cybercrimes are steadily occurring. To prevent cybercrime and the damage caused by information dysfunction, information security practices are essential. Accordingly, the purpose of this study is to discuss the factors affecting the information security practices of Korean youths, considering information security education, perceived severity, and perceived vulnerability as leading factors of the theory of planned behavior. A questionnaire survey was administered to 118 middle and high school students. Results of the hypothesis test show that information security education affects perceived behavior control, and perceived severity affects attitude. Subjective norms, information security attitudes, and perceived behavioral control were found to influence adolescents' practices of information security. However, perceived vulnerabilities did not affect youths' information security attitudes. This study confirms that information security education can help youths to practice information security. In other words, information security education is important, and it is a necessary element in the information curriculum of contemporary youth. However, perceived vulnerability to youth information security threats did not affect information security attitudes. Consequently, we suggest that it is necessary to strengthen the contents of the information security education for Korean youths.

Keywords : Information Security Practice, Theory of Planned Behavior, Information Security Education, Information Curriculum

Received : 2018. 11. 27. 1st Revised : 2019. 04. 03. 2nd Revised : 2019. 04. 22. Final Acceptance : 2019. 04. 24.

※ This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2018S1A5A2A01039356).

* First Author, Korea Standards Association Media, e-mail : kangms4008@naver.com

** Corresponding Author, Professor, Chungbuk National University, 1 Chungdae-ro, Seowon-Gu, Cheongju, Chungbuk, 28644, South Korea, Tel : +82-43-261-3343, e-mail : kimts@chungbuk.ac.kr

*** Doctoral Candidate, Department of Management Information System, Chungbuk National University, e-mail : ecac987@naver.com

1. 서 론

4차 산업혁명 시대로 접어들며, 정보통신기술을 기반으로 이전에는 서로 단절되어 있던 분야들이 경계를 넘어 분야 간 융·복합을 통해 다양한 변화가 나타나고 있다[정보통신정책연구원, 2016]. 4차 산업혁명에서 인간에 관한 데이터가 중요한 부분이 될 가능성이 높다. 4차 산업혁명으로 도래할 미래 사회는 지금보다 더 많은 개인에 관한 정보가 수집되고 처리될 수밖에 없을 것으로 예측하고 있다[한국법제연구원, 2017]. 이렇듯 정보통신에 대한 의존성이 점차 증대됨에 따라 해킹, 바이러스, 개인정보침해와 같은 정보화 역기능 또한 증가하고 있다. 경찰청 사이버안전국 사이버범죄 통계자료에 따르면 2014년부터 2017년까지 매해 100,000건 이상의 사이버범죄가 발생하고 있으며, 정보통신망 침해범죄, 정보통신망 이용범죄, 불법콘텐츠 범죄 등 다양한 유형의 정보화 역기능이 발생하고 있다[경찰청 사이버안전국, 2018]. 정보화 역기능으로 인해 많은 피해가 발생하고, 청소년의 사이버 범죄도 해마다 10,000건 내외로 발생하고 있다[정재준 등, 2014]. 청소년의 경우 정보보호에 대한 인식이 취약하고 죄의식 없이 우발적으로, 호기심으로 사이버 범죄를 저지르는 것으로 나타나고 있다. 대표적인 사건으로 2015년 고교생 3명이 웹하드 사이트를 통해 악성코드를 배포하여 좀비 PC를 만들고 이를 통해 ㈜넥슨의 게임 서버에 장애를 일으킨 사고가 있다. 또 다른 사고로는 10대 청소년 1명이 페이스북 페이지의 관리자 권한을 탈취하여 판매하는 등 청소년의 정보보호 윤리 의식의 부족으로 인하여 각종 범죄가 발생하고 있다[보안뉴스, 2016. 01. 22].

2017년 기준 10대의 99.9%가 인터넷 사용자로 나타났으며, 10대의 인터넷 이용 빈도는 하루에 1회 이상이 98.1%, 주당 평균 16.9시간을 이용한다[과학기술정보통신부, 2018]. 특히 한국 청소년들은 컴퓨터와 스마트폰 등 정보통신기기의 보급률이 높고 사용시간도 많은 편이기 때문에, 다양한 정보화 역기능의 피해를 경험하기 쉬운 환경에 처해 있다[한국교육학술정보원, 2014]. 이렇듯 청소년의 대부분이 인터넷을 이용하고 인터넷 접속빈도 및 이용시간이 높아지면서 위에서 언급한 정보보호 관련 문제의 심각성은 청소년에게도 예외가 될 수 없다. 정보화의 역기능과 청소년의 사이버 범죄로 인한 피해가 증가함에 따라, 정보화 역기능을 방지하고 청소년 정보윤리를 확립하기 위해 청소년에 특화된 정보

보호 교육의 확대와 더불어 체계화가 필요하다.

미국은 2016년 9월에 'K-12 Computer Science Framework'를 발표하고, 컴퓨터 교육에 대한 표준과 방향성을 수립하여 초등학교부터 고등학교에 이르기까지 정보보호를 포함한 컴퓨터 교육을 시행 중이다. 미국 청소년 대상의 컴퓨터 교육은 암호화, 개인정보보호, 온라인 불법복제, 사회공학기법, 피싱에 의한 피해방지, 랜섬웨어 등 정보보호 기술에서, 윤리, 대처방법에 이르기까지 다양한 주제로 청소년에 특화된 정보보호 교육을 실시하고 있다[CSTA, 2016]. 영국은 청소년이 정보기술을 평가하고 분석하여 문제를 해결할 수 있는 능력을 자발적으로 키울 수 있도록 정보보호가 포함된 컴퓨터 교육을 실시하고 있다. 주로 개인정보보호와 보안 위협 식별에 대하여 교육하고 있다[Department for Education(England), 2014].

우리나라는 컴퓨터와 인간 생활과의 관계 및 기본적인 구성 체계를 이해하고 조작 방법을 익혀서, 컴퓨터에 대한 친숙감과 올바른 가치관을 형성하여 컴퓨터 활용에 대한 적극적인 태도와 능력을 기르는 것을 목표로[교육부, 1992a; 교육부, 1992b] 제7차 2015 개정교육과정부터 중학생의 정보교과 필수지정을 시작으로 정보교과목을 통해 청소년에 대한 정보보호 교육이 진행되고 있다[교육부, 1997a; 교육부, 1997b]. 하지만 정보교과목의 정보보호 교육은 정보윤리의 하위 항목으로 구성되어 있어[교육부, 2015a; 교육부, 2015b] 정보보호 교육 자체는 많지 않으며, 정보교육 시수도 타 국가에 비해 현저히 적은 시수를 편성하고 있다. 더불어, 중학교 정보교과 담당 교사 확보 역시 학교 수 대비 20~30%에 불과한 실정이며 시행 중인 정보보호 교육의 실효성에 대하여 검증된 바도 없다[김도영, 2017]. 이에 본 연구에서는 정보보호 인식을 제고하고, 활동수행을 장려할 수 있는 수단 중 교육에 초점을 두어 청소년의 정보보호 실천 의도와 행동에 어떠한 영향을 미치는 지에 대하여 다루고자 한다. 이를 통해 청소년 대상 정보보호 교육의 방향성에 대하여 제시하고자 한다.

2. 이론적 배경

정보보호 교육이 청소년의 정보보호 실천에 미치는 영향 요인에 대하여 확인하기 위해 기술수용모형에서 출발한 계획행동이론에 대하여 문헌 연구를 진행하여 연구모형을 설계하고자 하였다. 계획행동이론모형을

기반으로 정보보호 실천에 미치는 영향 요인을 도출하기 위해 정보보호 실천, 행동, 의도와 관련된 문헌 연구를 수행하였다.

2.1 계획행동이론

계획행동이론(Theory of Planned Behavior, TPB)은 합리적 행동이론에서 발전된 이론이다[Fishbein and Ajzen, 1975]. 합리적 행동의 한계를 보완하기 위하여, Ajzen(1991)은 행동이 개인의 통제 밖의 상황의 행동을 예측하기 위하여 인지된 행동통제(Perceived Behavioral Control) 요인을 추가하여 계획행동이론 모형을 제시하였다. 계획행동이론은 태도, 주관적 규범, 인지된 행동통제가 행동의도에 영향을 미치며, 행동의도와 인지된 행동통제는 실제 행동에 영향을 미친다. 즉, 인지된 행동통제를 행동의도와 행동에 영향을 미치는 요인으로 규정하였다.

태도란 특정한 행동에 대해 개인이 가지고 있는 신념과 신념에 대한 평가로 이루어져 있으며 행위를 수행함에 있어 개인의 긍정적 혹은 부정적 느낌이라 할 수 있다. 주관적 규범이란 개인이 행위를 수행하는 것이 타인에게 중요한 것인지에 대한 평가로 사회적 압력에 대한 개인의 지각이라 할 수 있다[Fishbein and Ajzen, 1975].

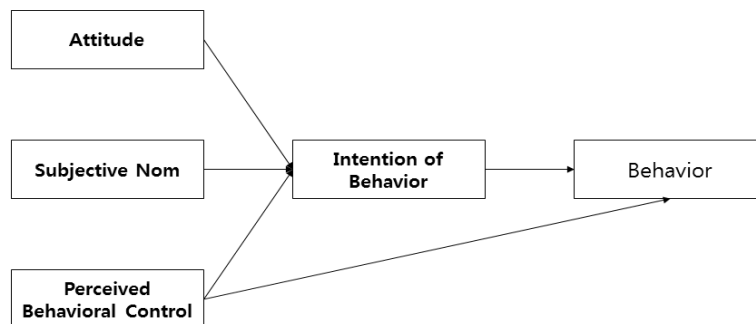
인지된 행동통제는 주어진 행동을 실행하는데 있어 개인이 느끼는 용이함 또는 어려움을 나타내는 자기 효능감과 비슷한 개념으로 볼 수 있다[Bandura, 1977]. 개인의 행동을 통제하는 것에 대하여 얼마나 쉬운지 또는 어려운지에 대한 개인의 인식으로 정의할 수 있으며, 개인의 행동을 수행할 능력이 있다고 믿는 정도에 따라 그러한 행동을 할 수 있는 자원과 기회에 의해 지

각된 행동통제가 결정된다.

이에 본 연구에서는 계획행동이론을 중심으로 정보보호 교육이 청소년의 태도와 주관적 규범, 인지된 행동통제와 함께 정보보호 실천 의도에 영향을 미치며 더 나아가 정보보호 실천 의도를 넘어 행동에 영향을 미친다는 전제에서 출발하였다.

2.2 정보보호 실천 관련 문헌 연구

현재까지 정보보호 실천에 대한 연구는 주로 기업이나 일반인을 대상으로 연구가 진행되었다. Arachchilage and Love(2014)는 개념적 지식이나 절차적 지식이 컴퓨터 이용자의 피싱 위협을 저지하기 위한 자기 효능감에 긍정적인 영향을 미치며 이는 피싱 위협 방지 행동에 긍정적인 영향을 미치는 것으로 확인하였다. Bulgurcu et al.(2009)은 조직의 464명 종업원을 대상으로 정보보호 정책준수의도에 영향을 미치는 요인에 대하여 조사하였다. 직원의 정보보호 인식과 조직 규정의 공정성 여부가 정보보호 행동에 영향을 미치며, 이는 정보보호 정책준수 의도에 영향을 미친다고 하였다. Bulgurcu et al.(2010)은 조직의 정보보호 정책 준수에 영향을 미치는 요인으로 정책 준수로 인한 이익, 정책 준수 비용, 정책을 준수하지 않음으로 생기는 비용으로 가정하였으며, 위의 요인들이 조직의 정보보호 정책 준수 태도에 영향을 미친다고 하였다. Herath and Rao(2009)은 조직의 보안행동이 내재적 동기와 외재적 동기 모두에 의해 영향을 받을 수 있으며, 주관적 규범과 동료 행동에 의해 가해지는 압력은 직원의 정보보호 행동에 영향을 미친다고 하였다. 즉, 직원의 행동에 대한 본질적인 동기가 정보보호 정책 준수 의도에 중요한 역할을 미친다는 것이다. Liang and Xue(2010)은



〈Figure 1〉 Theory of Planned Behavior Model

인지된 위협, 보안장치의 효과에 대한 이해, 보안장치의 비용, 자기 효능감 등이 보안 위협의 회피 동기에 영향을 미치며, 보안 위협 회피 동기에 의해 위협 회피 행위가 발생하는 것으로 나타났다.

Safa et al.(2016)은 정보보호 기술이 전적으로 정보의 안전한 환경을 보장할 수 없으며, 기술 측면 이외에도 인간의 정보보호 측면을 고려해야 한다고 했다. 사회유대이론을 활용해 직원들이 조직의 정보보호 정책을 준수하고 행동위험은 완화하는 방법을 제시하였다. 정보보호에 대한 지식공유, 협업, 개인의 경험, 주관적 규범은 정보보호 정책준수 태도에 영향을 미치며, 정보보호 정책준수 태도가 정보보호 정책준수 행동의도에 영향을 미치는 것으로 파악하였다. Shropshire et al.(2015)은 사람의 개인의 성향, 태도에 따라 보안 소프트웨어의 사용여부를 확인하였다. 보안 소프트웨어 사용의 용이성, 인지된 유용성이 보안 소프트웨어 사용 행동의도에 영향을 미치며, 사용의도와 실질적 행동의 관계의 양성과 동등성을 매개변수로 포함하여 양성과 동등성 수준이 높을수록 보안 소프트웨어를 사용할 가능성이 높다고 하였다. Siponen(2000)은 정보보호 분야에서의 인간의 동기 부여의 역할의 중요성을 강조하였다. 인간의 행동을 이해하기 위해, 내재적 동기 부여, 계획된 행동 이론 및 기술수용모델을 활용하여 정보보호 태도에 영향을 미치는 요인을 분석하였다. Vance et al.(2012)은 보호 동기 이론을 활용하여 정보보호 정책 준수에 영향을 미치는 요인을 파악하였다. 개인의 습관이 정보보호 정책 준수에 영향을 미치는 요인에 영향을 미치는 것으로 나타났으며, 취약성, 위협, 보상, 자기 효능감, 인지된 비용이 보안 정책을 준수하려는 직원의 의도에 중요한 영향을 미치는 것으로 나타났다. Wang(2010)은 인터넷 사용자의 정보보호 지식이 정보보호 태도와 행동의도에 영향을 미치며, 태도와 행동의도가 실질적으로 보안 솔루션의 사용 여부에 영향을 미치는 것으로 나타났다.

박찬욱 등(2014)는 개인정보에 대한 위협 평가항목과 대처항목으로 요인을 나누어 개인정보 보호행동에 영향을 미치는 요인에 대한 분석을 실시하였으며, 지각된 취약성, 지각된 심각성, 자기 효능감, 지각된 장애 등이 개인정보 보호행동에 영향을 미치는 것으로 나타났다. 최승재 등(2016)은 초등학생을 대상으로 정보보호 실천에 영향을 미치는 요인에 대하여 실증분석을 실시했다. 분석 결과 정보윤리 인식과 정보보호 인식이 초등학

생의 정보보호 실천에 영향을 미치는 것으로 나타났다.

정보보호 실천과 관련 선행 연구들을 통해 정보보호 정책, 정보보호 교육 등이 정보보호 실천 의도와 행위에 영향을 미치는 것을 알 수 있다. 또한, 주로 조직원 혹은 일반 성인을 대상으로 연구되었으며, 최승재 등(2016) 연구에서는 초등학생을 대상으로 정보보호 실천에 대하여 연구하였다. 하지만 성인에 비해 정보 윤리에 취약하고 정보보호 교육의 수혜를 받기 어려우며 초등학생보다 IT를 많이 활용하고 있는 청소년층을 대상으로 정보보호 실천에 대하여 연구된 바 없다. 이에 본 연구에서는 정보보호 실천에 영향을 미치는 수단인 정보보호 교육이 청소년의 정보보호 실천에 어떠한 영향을 미치는지에 대하여 연구하였다.

3. 연구 설계

3.1 연구모형의 변수와 가설설정

연구모형의 변수와 가설을 설정하기 위해 제 2장의 선행연구와 더불어 청소년과 관련된 문헌연구를 통해 정보보호 교육이 청소년의 정보보호 실천에 영향을 미치는 요인들을 도출하고 정의하였다.

정보보호의 취약성에 대하여 인지하고 있다는 것은 정보보호에 대한 태도에 영향을 미치는 요인 중 하나이다(Bulgurcu et al., 2010). 정보, 기기, 시스템, 시설 등 정보 자산들이 악의적인 공격 혹은 내부 실수로 인하여 발생할 수 있는 위협으로부터 취약할 수 있다는 인식의 정도가 태도를 형성하는데 영향을 미친다. 이러한 인식의 정도는 성인과 청소년이 차이가 있을 것이라는 것에서 출발하여 다음과 같은 가설을 도출하였다.

H1 : 인지된 취약성이 정보보호 태도에 긍정적인(+) 영향을 미칠 것이다.

인지된 심각성에 대해서 조직의 정보시스템을 보호함에 있어 개인이 자신의 상황에서 위협을 인지하지 못한다면 조직의 지침을 준수하지 않을 것이다(Ifinedo, 2012). 또한 인지된 심각성은 직원이 정보시스템 정책을 채택하려는 의도에 중요한 영향을 미치는 것으로 나타났다(Herath and Rao, 2009). 따라서, 인지된 심각성이 높다고 생각하는 개인은 정보보호 태도에 긍정적인 영향을 미칠 것이다. 이를 통해 다음과 같은 가설을 도출하였다.

H2 : 인지된 심각성이 정보보호 태도에 긍정적인(+) 영향을 미칠 것이다.

중학생에게 공학적 설계와 과학 탐구 기반의 STEAM (Science, Technology, Engineering, Arts and Mathematics) 교육을 적용한 결과 자기 효능감이 향상되었다[이영은 등, 2014]. 또한, 통합적 STEM (Science, Technology, Engineering and Mathematics) 교육을 일반계 고등학교 학생들의 기술 교과에 대한 자기 효능감에 영향을 미치는 것으로 나타났다[성의석 등, 2012]. 즉 교육은 자기 효능감에 긍정적인 영향을 미친다고 할 수 있다. TPB 이론의 인지된 행동통제 개념은 Bandura의 자기 효능감(self-efficacy)을 발전시킨 개념이다[Ajzen, 1991]. 즉, 지각된 행동통제는 자기 효능감과 행동 통제를 모두 포괄하고 있는 상위 개념이라 할 수 있다[Ajzen, 2002]. 따라서 본 가설에서는 정보보호 교육이 자기 효능감에 긍정적인 영향을 미치는 것과 더불어 통제성을 포함하여 정보보호 교육은 인지된 행동통제에 긍정적인 영향을 미칠 것이라 가정한다. 따라서 다음과 같은 가설을 도출하였다.

H3 : 정보보호 교육이 인지된 행동통제에 긍정적인(+) 영향을 미칠 것이다.

정보보호 행동을 장려하기 위하여 내재적인 동기와 외재적 동기로 구분하였으며, 내재적 동기요인 주관적인 규범은 규범적인 신념과 동료 행동으로 구분하였다. 규범적인 신념과 동료의 행동에 의해 가해지는 압력은 직원들의 정보보호 행동에 영향을 미친다[Herath and Rao, 2009]. 따라서 다음과 같은 가설을 도출하였다.

H4 : 주관적 규범은 행동의도에 영향을 미칠 것이며, 주관적 규범은 행동의도에 긍정적인(+) 영향을 미칠 것이다.

태도와 행동의도 사이의 관계는 정보시스템 관련 문헌에서 널리 사용되어 왔으며, TPB 이론에서는 개인의 태도가 행동의도에 영향을 미친다고 한다[Ajzen, 1991]. 조직에서 종업원의 태도는 정보시스템 보안 정책 준수 행동의도에 직접적으로 영향을 미치며, 행동의도를 구성하는 주요 요인이다[Ifinedo, 2012]. 따라서 다음과 같은 가설을 도출하였다.

H5 : 태도는 행동의도에 긍정적인(+) 영향을 미칠 것이다.

인지된 행동통제란 행동 수행의 용이성 또는 자신의 의지대로 통제가 가능한 정도를 말한다. 사용자의 정보보호 경험과 참여는 정보보호 행동을 수행함에 있어 자신의 인식에 영향을 미치는 중요한 요소다[Albrechtsen, 2007]. 따라서 다음과 같은 가설을 도출하였다.

H6 : 인지된 행동통제는 행동의도에 긍정적인(+) 영향을 미칠 것이다.

행동 의도는 실제 행동에 영향을 미친다. 청소년의 경우 진로정보탐색 행동 의도가 진로정보탐색 행동에 영향을 미치는 요소로 작용하였다[이재창 등, 2008]. 또한, 청소년의 청소년활동 참여의도는 청소년활동에 참여하는데 영향을 미치는 요소로 작용하였다[김도영, 2017]. 따라서 다음과 같은 가설을 도출하였다.

H7 : 행동의도는 정보보호 실천에 긍정적인(+) 영향을 미칠 것이다.

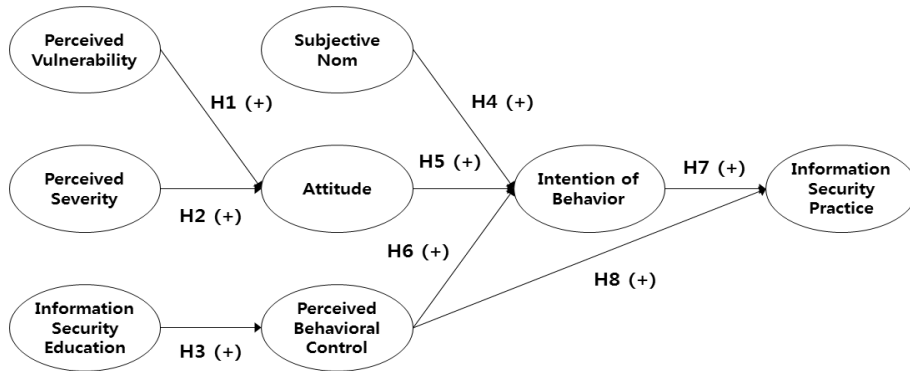
인지된 행동통제는 행동의도에 영향을 미칠 뿐 아니라 행동에도 영향을 미치는 것으로 보았다[Ajzen, 1991]. 따라서 본 연구에서도 정보보호 실천에 대한 인지된 행동통제가 정보보호 실천에 영향을 주는 가설을 도출하였다.

H8 : 인지된 행동통제는 정보보호 실천에 긍정적인(+) 영향을 미칠 것이다.

3.2 연구변수의 조작적 정의와 측정항목

본 연구는 선행연구를 기반으로 구성개념에 대한 조작적 정의와 구성개념에 대한 측정항목을 도출하였다. 연구 변수인 인지된 취약성, 인지된 심각성, 정보보호 교육, 주관적 규범, 태도, 인지된 행동 통제, 행동의도, 정보보호 실천에 대하여 정의하였다.

인지된 취약성은 실제 생활에서 정보보호 위험이 발생할 가능성을 인식한 정도를 뜻한다. 인지된 심각성은 보안 위험이 발생하였을 경우 보안 위험의 발생이 미칠 부정적 영향을 인식하는 정도를 뜻한다. 정보보호 교육은 청소년이 학교와 학교 밖 기관에서 정보보호 교육을



〈Figure 2〉 Research Model

받았는지의 여부, 교육을 받은 정도를 뜻한다. 이는 중·고등학교에서 진행되는 정보교과 교육내용을 근간으로 하여 본 연구에 맞게 수정 및 보완하였다. 주관적 규범은 정보보호 실천이 타인에게 중요한 것인지에 대한 개인의 인식을 뜻한다. 태도는 정보보호 실천에 대한 긍정적인 또는 부정적인 느낌을 뜻한다. 인지된 행동통제는 정보보호 실천이 자신의 의지대로 통제 가능한 정도를 뜻한다. 행동 의도는 정보보호 실천을 수행할 의지의 정도를 뜻한다. 정보보호 실천은 실질적으로 정보보호를 실천하는 정도를 뜻한다.

행동 의도의 경우, 정보보호 행동을 이전 단계로서 정보보호 행동 의지의 정도를 뜻하며, 정보보호 실천은 현재 자신의 정보보호 행동 의지의 정도와 행동 통제에 따라 실제 정보보호 행동을 하고 있는 정도를 말한다.

모든 항목들은 신뢰성을 높이기 위해 ‘(1) 전혀 그렇지 않다’에서 ‘(5) 매우 그렇다’에 걸친 5점 리커트 척도로 측정하였다.

3.3 연구모형

문헌연구를 통해 정보보호 교육이 청소년의 정보보호 실천에 영향을 미치는 요인에 대하여 분석하기 위해 연구모형을 설계하였다. 본 연구의 모형은 계획행동이론을 기반으로 하고 있으며, 정보보호 분야의 특성인 인지된 취약성과 인지된 심각성을 연구 변인으로 추가하고, 정보보호 교육을 인지된 행동통제와의 상관관계를 설정하여 연구모형을 보완하였다. 기존의 계획행동이론은 주관적 규범, 인지된 행동통제가 행동 의도에 영향을 미치며 행동 의도와 행동 통제가 실제 행동에 영향을 미친다는 이론으로서 정보보호 분야의 특

성을 담기에는 한계가 존재하기 때문에 문헌연구를 통해 인지된 취약성과 인지된 심각성이 태도를 형성하는데 영향을 미친다는 가설을 추가하였다. 또한 정보보호 교육은 정보보호 행위를 통제하는데 영향을 미치고 이는 행동 의도와 실제 정보보호 실천에 영향을 미친다는 가설을 반영하였다. 이에 따라 본 연구모형을 통해 정보보호 교육이 청소년의 정보보호 실천에 영향을 미칠 것이라는 주제에 대하여 검증하였다. 설계한 연구모형은 〈Figure 2〉와 같다.

4. 실증분석

4.1 자료의 수집 및 표본의 특성

설문은 중학교와 고등학교에 재학 중인 청소년을 대상으로 실시하였다. 자료 수집은 2018년 5월 21일부터 6월 7일까지 약 3주간 국내 중학교와 고등학교 학생들에게 온라인 설문지와 오프라인 설문지를 구성하여 배포하여 설문조사를 진행하였다. 총 143부를 회수하여 그 중 성실하게 응답한 118부의 설문지를 분석에 사용하였다. 본 연구에 참여한 응답자의 인구 통계학적 특성은 〈Table 1〉과 같다.

〈Table 1〉 Feature of Respondents by Gender and Age

Classification		# of Respondents
Gender	Male	49
	Female	69
Age	Middle schooler	20
	high school student	98
Total		118

4.2 신뢰성 및 타당성 분석

수집한 데이터를 바탕으로 PLS 2.0을 이용하여 연구모형의 신뢰성과 타당성을 분석하였다. PLS 분석은 측정 문항과 구성 개념에 대하여 내적일관성(internal consistency), 집중타당성(convergent validity), 판별타당성(discriminant validity) 검증을 요구한다. 내적일관성 검증을 위해 인지된 취약성, 인지된 심각성, 정보보호 교육, 주관적 규범, 태도, 인

지된 행동통제, 행동의도, 정보보호 실천을 대상으로 Fornell and Larcker(1981)의 복합신뢰도(Composite reliability)와 신뢰성을 분석하였다. 복합신뢰도는 Thompson(1995)이 주장하는 기준치인 0.7 이상으로 나타났고, 신뢰성 검증에 널리 사용되는 크론바흐 알파(Cronbach Alpha) 값은 0.6 이상으로 나타났다. 따라서 내적일관성은 적합한 것으로 나타났다.

집중타당성은 AVE(average variance extrac-

<Table 2> Analysis of Convergent Validity and Internal Consistency

Component	Item	Factor Load Value	t-value	Composite Reliability	AVE	Cronbach's Alpha
Perceived Vulnerability	PV1	0.890	39.342	0.927	0.809	0.885
	PV2	0.912	38.420			
	PV3	0.895	32.135			
Perceived Severity	PS1	0.877	55.592	0.948	0.821	0.927
	PS2	0.886	38.823			
	PS3	0.921	79.878			
	PS4	0.937	99.343			
Information Security Education	EDU1	0.680	3.950	0.859	0.551	0.813
	EDU2	0.725	4.971			
	EDU3	0.774	5.938			
	EDU4	0.834	7.901			
	EDU5	0.687	5.446			
Subjective Nom	SN1	0.801	15.151	0.905	0.762	0.841
	SN2	0.938	80.035			
	SN3	0.873	29.174			
Attitude	AT1	0.953	89.575	0.972	0.921	0.957
	AT2	0.961	111.883			
	AT3	0.964	116.35			
Perceived Behavioral Control	PCB1	0.705	12.861	0.816	0.526	0.713
	PCB2	0.770	14.342			
	PCB3	0.686	7.422			
	PCB4	0.737	9.331			
Intention of Behavior	BI1	0.729	16.374	0.872	0.630	0.804
	BI2	0.845	23.801			
	BI3	0.802	21.405			
	BI4	0.795	28.607			
Information Security Practice	AC1	0.734	16.715	0.809	0.515	0.686
	AC2	0.705	16.300			
	AC3	0.762	20.202			
	AC4	0.665	11.374			

ted)와 구성개념에 대한 요인적재값으로 검증하였다. AVE는 Fornell and Larcker(1981), Chin(1998) 등이 주장하는 기준치인 0.5 이상으로 나타났고, 구성개념의 요인적재값은 모두 0.6 이상으로 나타났다(<Table 2> 참조).

확인적 요인분석에서는 구성개념에 대한 요인적재값이 다른 구성개념에 대한 요인적재값보다 커야 한다 [Chin, 1998]. 분석결과 모든 설문문항이 본 요건을

충족하였다(<Table 3> 참조).

판별타당성은 구성개념 간의 상관계수 값들의 대각선 축에 표시되는 AVE의 제곱근 값이 다른 구성개념 간의 상관계수 값보다 큰가의 여부로 검증하였다[Fornell and Larcker, 1981]. AVE의 제곱근 값 중 가장 작은 값(0.7180)이 가장 큰 상관계수 값(0.6573)보다 상회하였기 때문에 판별타당성은 적합한 것으로 나타났다(<Table 4> 참조).

<Table 3> Analysis of Confirmatory Factor

	Perceived Vulnerability	Perceived Severity	Information Security Education	Subjective Nom	Attitude	Perceived Behavioral Control	Intention of Behavior	Information Security Practice
PV1	0.890	0.677	0.077	0.372	0.357	0.096	0.234	0.241
PV2	0.912	0.488	0.031	0.322	0.281	0.230	0.375	0.295
PV3	0.895	0.443	0.097	0.264	0.230	0.177	0.361	0.250
PS1	0.546	0.877	0.036	0.494	0.484	0.215	0.421	0.261
PS2	0.618	0.886	-0.017	0.474	0.397	0.111	0.249	0.180
PS3	0.523	0.921	0.102	0.533	0.507	0.130	0.330	0.206
PS4	0.560	0.937	0.074	0.474	0.483	0.137	0.255	0.199
EDU1	0.040	-0.004	0.680	0.238	-0.059	0.018	-0.0008	0.049
EDU2	0.048	0.152	0.725	0.382	0.024	0.164	0.112	0.051
EDU3	0.028	0.022	0.774	0.269	-0.001	0.126	0.162	0.072
EDU4	0.036	-0.007	0.834	0.301	-0.101	0.216	0.090	0.057
EDU5	0.107	0.027	0.687	0.102	-0.104	0.188	0.107	0.083
SN1	0.316	0.598	0.193	0.802	0.589	0.168	0.363	0.207
SN2	0.283	0.427	0.326	0.938	0.392	0.263	0.421	0.250
SN3	0.363	0.414	0.379	0.873	0.288	0.198	0.356	0.165
AT1	0.310	0.524	-0.049	0.483	0.953	0.127	0.309	0.299
AT2	0.299	0.487	-0.135	0.427	0.961	0.143	0.298	0.291
AT3	0.348	0.484	-0.026	0.478	0.964	0.144	0.348	0.302
PCB1	0.082	0.099	0.304	0.203	0.095	0.705	0.344	0.406
PCB2	0.084	0.152	0.081	0.167	0.220	0.770	0.410	0.407
PCB3	0.185	0.100	0.102	0.139	0.041	0.686	0.230	0.214
PCB4	0.211	0.123	0.152	0.182	0.020	0.737	0.337	0.287
BI1	0.187	0.180	0.172	0.288	0.213	0.372	0.729	0.478
BI2	0.347	0.356	0.104	0.427	0.328	0.345	0.845	0.509
BI3	0.273	0.286	0.149	0.294	0.165	0.273	0.802	0.544
BI4	0.289	0.279	0.055	0.367	0.327	0.482	0.795	0.551
AC1	0.133	0.112	0.196	0.154	0.161	0.317	0.471	0.734
AC2	0.305	0.318	-0.073	0.273	0.360	0.316	0.468	0.705
AC3	0.266	0.204	-0.056	0.128	0.303	0.216	0.462	0.763
AC4	0.138	0.053	0.159	0.131	0.084	0.481	0.475	0.665

<Table 4> Analysis of Discriminant Validity

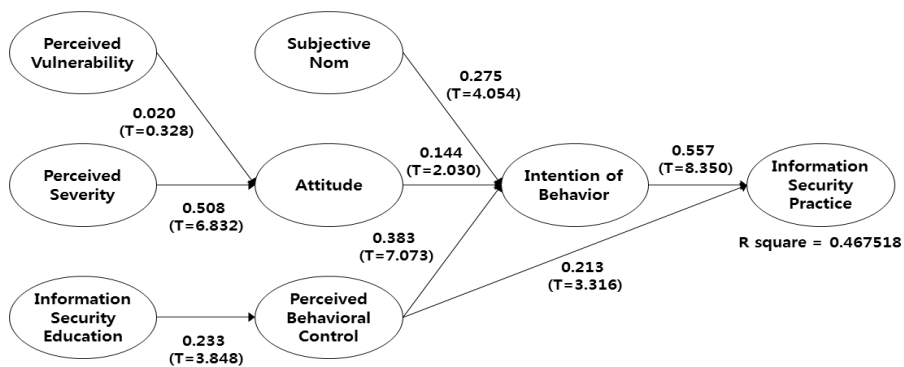
	Information Security Education	Subjective Nom	Information Security Practice	Perceived Severity	Perceived Vulnerability	Attitude	Intention of Behavior	Perceived Behavioral Control
Information Security Education	0.742							
Subjective Nom	0.344	0.873						
Information Security Practice	0.058	0.546	0.906					
Perceived Severity	0.146	0.437	0.350	0.794				
Perceived Vulnerability	0.075	0.364	0.616	0.349	0.899			
Attitude	-0.072	0.483	0.520	0.332	0.333	0.959		
Intention of Behavior	0.086	0.240	0.235	0.657	0.290	0.310	0.718	
Perceived Behavioral Control	0.232	0.243	0.165	0.470	0.179	0.143	0.475	0.725

4.3 구조모형 및 가설검정

본 연구모형의 PLS 분석결과이다. PLS 분석에서 경로모형의 설명력은 분산설명력(Explained variance)인 R²값으로 표현된다(Chin and Gopal, 1995). PLS의 R² 분석결과, 정보보호 행동의도는 정보보호 실천의 46.75%를 설명하였다. 이는 Falk and Miller [1992]이 제시한 적정 검정력 10%를 상회하는 것이다 (<Figure 3> 참조).

연구모형의 적합도(goodness-of-fit, GoF)를 검증한 결과, GoF 영향도는 0.7006으로서, Wetzels et al.[2009]이 제시한 강(large)보다 크기 때문에 모형의 적합도가 매우 높은 것으로 나타났다(Tenenhaus et al., 2005).

PLS 분석을 통해 경로계수와 경로계수의 유의성을 검증하였다. 이를 위해 전체표본을 이용하여 구조모형에 대한 경로계수를 구하고, PLS에서 제공하는 부스트랩 방식을 이용하여 경로계수의 t-값을 산출하였다.



<Figure 3> Analysis Results

〈Table 5〉 Results of Hypotheses Test

Hypothesis		p-Value	t-Value	Result
H1	Perceived Vulnerability → Attitude	0.020	0.328	Reject
H2	Perceived Severity → Attitude	0.508	6.832	Adopt
H3	Information Security Education → Perceived Behavioral Control	0.233	3.848	Adopt
H4	Subjective Norm → Intention of Behavior	0.275	4.054	Adopt
H5	Attitude → Intention of Behavior	0.144	2.03	Adopt
H6	Perceived Behavioral Control → Intention of Behavior	0.383	7.073	Adopt
H7	Intention of Behavior → Information Security Practice	0.557	8.350	Adopt
H8	Perceived Behavioral Control → Information Security Practice	0.213	3.316	Adopt

구조모형의 경로분석은 Smart PLS의 Bootstrapping 방식에서 제공하는 t-값을 통해 통계적 유의성을 검증할 수 있다. H1을 제외한 8개 가설의 경로계수 t-값이 1.96보다 크게 나타나 H2-H8 가설의 경우 경로가 유의성을 가진다고 나타났다(〈Table 5〉 참조).

5. 결론 및 시사점

본 연구는 청소년의 정보보호 실천에 대한 요인을 알아보는데 그 목적이 있다. 문헌연구를 바탕으로 청소년의 정보보호 실천에 영향을 미치는 요인에 대하여도 출하였으며, 정보보호 실천에 영향을 미치는 요인에 대하여 확인하기 위해 연구 모델을 구성하고 설문조사를 실시하였다. 설문조사는 현재 중·고등학교에 재학 중인 학생들을 대상으로 실시하여, 총 143부를 회수하고 Smart PLS 2.0으로 118부를 분석하였다. 주요 분석 결과는 다음과 같다. 인지된 취약성은 태도에 영향을 미치지 않았지만, 인지된 심각성은 태도에 영향을 미치는 것으로 나타났으며, 정보보호 교육은 인지된 행동통제에 영향을 미치는 것으로 나타났다. 주관적 규범, 태도, 인지된 행동통제는 행동의도에 영향을 미치는 것으로 나타났다. 행동의도와 인지된 행동통제는 정보보호 실천에 영향을 미치는 것으로 나타났다.

청소년의 정보보호 실천에 영향을 미치는 요인에 대한 분석을 통해 다음과 같은 시사점을 도출하였다. 첫째, 청소년들의 정보보호 위협에 대한 인지된 심각성은 정보보호 태도에 영향을 미치는 것으로 나타났지만, 인지된 취약성은 정보보호 태도에 영향을 미치지 않는 것으로 나타났다. 보안 위협이 발생할 경우 수반되는 피해에 대하여는 인식하고 있지만, 직접적으로 태도를 형성하지 않는 것으로 해석할 수 있다. 청소년

들도 정보 자산이 위협으로부터 취약할수록 정보를 더욱 보호해야 한다는 인식을 함양할 수 있도록 정보보호 교육이 정보 제공자로서 역할을 수행해야 한다. 둘째, 정보보호 교육이 인지된 행동통제에 영향을 미치는 것으로 나타났다. 청소년의 정보보호와 관련된 인지된 행동통제는 개인정보를 보호하기 위해 능숙하게 정보보호 관련 조치를 취할 수 있는 능력을 말한다. 본 연구에서는 정보보호 교육은 인지된 행동통제에 영향을 미치는 것으로 나타나므로 정보보호 교육은 중요하며 정보 교과에 필요한 요소라 할 수 있다.

연구의 한계점 및 향후 연구방향은 다음과 같다. 첫째, 본 연구의 실증분석을 위하여 사용된 데이터는 중·고등학교 학생들을 대상으로 진행하였으나, 고등학생의 비율이 80%에 가까워 연구결과를 청소년으로 일반화하기에는 한계가 있다. 둘째, 정보 교과는 2018년부터 중학생을 대상으로 필수적으로 교육되고 있다. 이렇듯 정보기술 활용 능력이 향상됨에 따라 초등학교 고학년 역시 정보통신기술을 활용하고 있다. 이에 따라 청소년을 초등학교 고학년, 중학생, 고등학생으로 세분화하여 청소년 대상의 정보보호 교육이 정보보호 실천이 미치는 영향에 대하여 비교 연구함으로써 청소년의 정보보호에 대하여 상세하게 연구할 필요가 있다. 또한 청소년 대상의 정보보호 교육의 효과를 직접적으로 검증하기 위해서는 교육 전·후로 실험하여 측정하는 방식의 연구가 필요하다.

References

- [1] Albrechtsen, E., "A qualitative study of users' view on information security", *Computers and Security*, Vol. 26, No. 4, 2007,

- pp. 276-289.
- [2] Arachchilage, N. A. G. and Love, S., "Security awareness of computer users : A phishing threat avoidance perspective", *Computers in Human Behavior*, Vol. 38, 2014, pp. 304-312.
- [3] Ajzen, I., "The theory of planned behavior", *Organizational Behavior and Human Decision Processes*, Vol. 50, No. 2, 1991, pp. 179-211.
- [4] Ajzen, I., "Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior", *Journal of Applied Social Psychology*, Vol. 32, No. 4, 2002, pp. 665-683.
- [5] Bandura, A., "Self-efficacy : toward a unifying theory of behavioral change", *Psychological Review*, Vol. 84, No. 2, 1977, pp. 191-215.
- [6] Boannews, "Information security technology I've been teaching so well...?", 2016. 01. 22.
- [7] Bulgurcu, B., Cavusoglu, H., and Benbasat, I., "Roles of information security awareness and perceived fairness in information security policy compliance", *AMCIS 2009 Proceedings*, Vol. 419, 2009.
- [8] 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.
- [9] Chin, W. W. and Gopal, A., "Adoption intention in GSS : relative importance of beliefs", *ACM SigMIS Database*, Vol. 26, No. 2-3, 1995, pp. 42-64.
- [10] Chin, W. W., "The partial least squares approach to structural equation modeling", *Modern Methods for Business Research*, Vol. 295, No. 2, 1998, pp. 295-336.
- [11] Choi, S. J., Kim, H. Y., and Kim, T. Y., "Factors Affecting Information Security Practice of Elementary School Students", *Journal of The Korea Institute of Information Security and Cryptology*, Vol. 26, No. 2, 2016, pp. 449-461.
- [12] CSTA, CSTA K-12 Computer Science Standards, 2016.
- [13] Department for Education, The National Curriculum in England : Framework Document, 2014, England.
- [14] Falk, R. F. and Miller, N. B., *A Primer for Soft Modeling*. University of Akron Press, 1992.
- [15] Fishbein, M. and Ajzen, I., *Belief, Attitude, Intention and Behavior : An Introduction to Theory and Research*, Addison-Wesley, Reading, MA, 1975.
- [16] Fornell, C. and Larcker, D. F., "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, Vol. 18, No. 1, 1981, pp. 39-50.
- [17] Herath, T. and Rao, H. R., "Encouraging information security behaviors in organizations : Role of penalties, pressures and perceived effectiveness", *Decision Support Systems*, Vol. 47, No. 2, 2009, pp. 154-165.
- [18] Ifinedo, P., "Understanding information systems security policy compliance : An integration of the theory of planned behavior and the protection motivation theory", *Computers and Security*, Vol. 31, No. 1, 2012, pp. 83-95.
- [19] Ifinedo, P., "Information systems security policy compliance : An empirical study of the effects of socialisation, influence, and cognition", *Information and Management*, Vol. 51, No. 1, 2014, pp. 69-79.
- [20] Jung, J. J. and Youn, S. C., "A Study

- on the Improvement Policy of the Deterrent Effect in Accordance with the Trend of the Juvenile Cyber-Crime”, *Journal of Police*, Vol. 14, No. 1, 2014, pp. 53-80.
- [21] Kim, D. Y., “Verification of The prediction model on Participation behavior of Youth activity”, *Korea Youth Studies*, Vol. 24, No. 1, 2017, pp. 307-333.
- [22] Korea Education and Research Information Service, Analysis of Information Dysfunction Prevention Trend and Study on Improvement of Information and Communication Education, 2014.
- [23] Korea Information Society Development Institute, 4th Industrial Revolution and Changes in the Industrial Structure, 2016.
- [24] Korea Legislation Research Institute, Improvement of Personal Information Protection Law in the Era of the 4th Industrial Revolution 2017.
- [25] Lee, J. C. and Park, M. J., “The Prediction of Career Information-Seeking Behavior of Adolescents : An Application of the Theory of Planned Behavior”, *The Korean Journal of Counseling and Psychotherapy*, Vol. 20, No. 3, 2008, pp. 795-818.
- [26] Lee, Y. E. and Lee, H. N., “The effects of engineering design and science inquiry-based STEAM education program on middle school students’ interest in science, mathematics, technology, self-efficacy and career choice”, *Journal of Research in Curriculum and Instruction*, Vol. 18, 2014, pp. 513-540.
- [27] 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.
- [28] Ministry of Education, Ministry of Education Notification Notice No. 1992-11 Middle School Curriculum, 1992a.
- [29] Ministry of Education, Ministry of Education Notification No. 1992-19 High School Curriculum, 1992b.
- [30] Ministry of Education, Ministry of Education Notice No. 1997-15 [Separate 3] Middle School Curriculum, 1997a.
- [31] Ministry of Education, Ministry of Education Notice No. 1997-15 [Separate 4] High School Curriculum, 1997b.
- [32] Ministry of Education, Ministry of Education Notice No. 2015-74 [Separate 3] Middle School Curriculum, 2015a.
- [33] Ministry of Education, Ministry of Education notification 2015-74 [Separate 4] High school education course. 2015b.
- [34] Ministry of Science and ICT, 2017 Survey on the Internet Usage, 2018.
- [35] 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.
- [36] Park, C. O. and Lee, S. W., “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, 2014, pp. 59-71.
- [37] Police Cyber Bureau, Cyber Crime Statistics, 2018.
- [38] Rhee, H. S., Kim, C., and Ryu, Y. U., “Self-efficacy in information security : Its influence on end users’ information security practice behavior”, *Computers and Security*, Vol. 28, No. 8, 2009, pp. 816-826.
- [39] Safa, N. S., Von Solms, R., and Furnell, S., “Information security policy compliance model in organization”, *Computers*

- and Security*, Vol. 56, No. 5, 2016, pp. 70-82.
- [40] Shropshire, J., Warkentin, M., and Sharma, S., "Personality, attitudes, and intentions : Predicting initial adoption of information security behavior", *Computers and Security*, Vol. 49, No. 12, 2015, pp. 177-191.
- [41] Siponen, M. T., "A conceptual foundation for organizational information security awareness", *Information Management and Computer Security*, Vol. 8, No. 1, 2000, pp. 31-41.
- [42] Sung, E. S. and Na, S. I., "The Effects of the Integrated STEM Education on Science and Technology Subject Self-efficacy and Attitude toward Engineering in High School Students", *Korean Technology Education Association*, Vol. 12, No. 1, 2012, pp. 255-274.
- [43] Tenenhaus, M., Vinzi, V. E., Chatelin, Y. M., and Lauro, C., "PLS path modeling", *Computational Statistics & Data Analysis*, Vol. 48, No. 1, 2005, pp. 159-205.
- [44] Thompson, C. B., "Apoptosis in the pathogenesis and treatment of disease", *Science*, Vol. 267, No. 5203, 1995, pp. 1456-1462.
- [45] Vance, A., Siponen, M., and Pahlila, S., "Motivating IS security compliance : insights from habit and protection motivation theory", *Information and Management*, Vol. 49, No. 3-4, 2012, pp. 190-198.
- [46] Wang, P. A., "Information security knowledge and behavior : An adapted model of technology acceptance", In *Education Technology and Computer (ICETC), 2010 2nd International Conference on* (Vol. 2, pp. V2-364). IEEE, 2010.
- [47] Wetzels, M., Odekerken-Schröder, G., and Van Oppen, C., "Using PLS path modeling for assessing hierarchical construct models : Guidelines and empirical illustration", *MIS Quarterly*, Vol. 33, No. 1, 2009, pp. 177-195.

■ 저자소개



Min-Seong Kang

Min-Seong Kang has been working for Korea Standards Association Media since March 2019. He received master's degree from the Chungbuk National University. His main

research interests are information security, knowledge content management and technical management.



Tae-Sung Kim

Tae-Sung Kim has been working for Department of Management Information Systems at Chungbuk National University since September 2000.

He received his bachelor, master, and doctoral degrees in engineering from the Department of Management Science at KAIST in 1991, 1993 and 1997. He worked for ETRI as a Senior Researcher from February 1997 to August 2000. His research areas include telecommunications management, information privacy, information security economics. His recent research papers have appeared in international journals, such as European Journal of Operational Research, Journal of the Operations Research Society, Operations Research Letters, Stochastic Analysis and Applications and Journal of Intelligent Manufacturing.



Taek-Young Kim

Taek-Young Kim is a Doctoral Candidate in the Department of Management Information System at the Chungbuk National University in South Korea. He received ma-

ster's degree from Chungbuk National University. His main research interests are personal information breach, information security policy and ICT convergence.