

## 초등학생들의 정보보호실천에 영향을 미치는 요인\*

최 승 재,<sup>1†</sup> 김 형 열,<sup>2</sup> 김 태 성<sup>2‡</sup>  
<sup>1</sup>한국교원대학교, <sup>2</sup>충북대학교

### Factors Affecting Information Security Practice of Elementary School Students\*

Seung-Jae Choi,<sup>1†</sup> Hyeong-Yeol Kim,<sup>2</sup> Tae-Sung Kim<sup>2‡</sup>  
<sup>1</sup>Korea National University of Education, <sup>2</sup>Chungbuk National University

#### 요 약

정보보호에 대한 인식이 부족한 학생들의 경우 쉽게 자신의 정보를 타인에게 알려주거나, 죄의식 없이 남의 정보를 가져다 이용하는 일이 발생하고 있다. 사이버 범죄로부터 학생들을 보호하고 예방하기 위해서는 정보보호교육이 필요하지만, 국내 정보 교과과정에는 구체적인 정보보호 관련 내용이 별도로 없고 학교나 교사 재량으로 네티켓 교육을 실시하는 정도에 그치고 있다. 본 연구의 목적은 초등학생들의 정보보호실천에 영향을 미치는 요인들을 찾는 것이다. 실증분석을 위하여 초등학생들이 이해하기 쉬운 정보보호 어휘로 구성된 설문지로 조사를 실시하였고, 수집된 자료는 PLS(Partial Least Square, PLS)를 이용하여 측정모형 및 구조모형 검정을 실시하였다. 연구 결과, 정보윤리인식과 정보보호인식이 정보보호실천에 정(+ )의 영향을 미치는 것으로 확인되었다. 본 연구 결과는 초등학생의 정보보호실천에 필요한 구체적인 정보보호 교육내용을 선정하는데 도움을 줄 것으로 기대한다.

#### ABSTRACT

If students are not aware of the information security, they easily let others know their information or they use others' information with no sense of guilt. The information security education is necessary to protect and prevent students from cyber crime. However, South Korea's information curriculum has no specific information security education course and it has led a school or teacher to teach contents of information ethics superficially. The purpose of this paper is to find the factors affecting the information security practice of the elementary school students. For an empirical analysis, questionnaire survey was conducted and the Partial Least Square(PLS) was used to analyze the research model. The analysis results show that the information ethics awareness and the information security awareness have a positive impact on the information security practice. The results of this study are expected to help choose the specific information security curriculum required for the information security practice of elementary school students.

**Keywords:** Information Security Education, Information Ethics, Information Security Awareness, Information Security Practice, Elementary School Students

## I. 서 론

최근 정보통신 기술이 발전하면서 인터넷과 스마트폰 보급이 전 연령층을 대상으로 빠른 속도로 확산되고 있다. 한국인터넷진흥원의 인터넷이용실태조사에 따르면 각각 3~9세 인터넷 이용자의 인터넷 이용률이 78.8%, 10대 청소년 인터넷 이용자의 인터넷 이용률은 99.7%에 달하며[1], 모바일인터넷이용실태조사에 따르면 6~9세에 모바일인터넷을 처음 시작한 이용자의 비율이 2011년부터 2014년까지 각각 0.7%, 17.2%, 45.7%, 36.4%로 증가하는 추세이다[2]. 방송통신위원회의 사이버 폭력 실태에 따르면 초등학생의 7%가 사이버폭력 가해 경험이 있으며, 사이버폭력 가해이유에 대해 가장 많이 응답한 항목이 '상대방 행동에 보복하기 위해서', '상대방이 싫어서, 상대방에게 화가 나서', '재미나 장난으로, 스트레스 해소를 위해'이었으며 각각의 가해 이유 비율은 46.9%, 28.4%, 16.0%로 나타났다[3]. 특히 정보보호에 대한 인식이 부족한 학생들의 경우 해킹 등을 이용하여 타인의 정보를 탈취하거나 본인의 정보 역시 아무렇지 않게 노출하고 있어 심각한 사회문제가 되고 있다. 이러한 이유로 사이버 범죄로부터 학생들을 보호하고 학생들 스스로 정보보호인식과 실천능력을 기르기 위해서 초등학교에서부터 교육이 필요하다.

그러나 2009 개정 교육과정에서 별도의 정보보호 교육 내용이 정규교과에 존재하지 않음은 물론, 초·중등학교 정보통신기술교육 운영지침마저 폐지되면서 2007 개정 교육과정 시에 연간 총 200여 시간의 정보 교육이 2009 개정 교육과정에서는 연간 총 100여 시간의 창의적 체험 활동에 속하면서 축소되어 운영되거나, 전혀 실시하지 않는 학교도 존재하는 실정이다[4]. 이러한 환경에서 초등학교 교사는 정보보호 교육을 하기에 앞서 정규 교과가 따로 없기 때문에 무엇을 가르쳐야 하는 지에 대한 어려움이 존재한다. 이에 따라, 초등학생들의 정보보호교육에 대해 논의하기 위해서는 이전에 교육 학술기관과 국내의 교육과정에서 제시한 초등학생의 정보보호 교육내용을 파악하고, 각 내용에 대하여 현재 초등학생들의 정보보호 수준을 파악하여야 하며, 무엇을 가르쳐야 학생들이 정보보호 활동을 실천 할지에 대해 생각해 보아야 한다. 도출한 내용을 토대로 초등학생의 정보보호실천을 위하여 배워야 할 교육 내용은 무엇이며, 초등학생의 정보보호 수준이 얼마나 되는지를 실증적

으로 분석하여 초등학생을 대상으로 한 정보보호교육에 대한 필요성을 인식시키는 데 목적이 있다.

이상의 목적을 수행하기 위하여 국내외에 초등학생을 대상으로 시행되고 있는 정보보호 관련 교육과정을 조사하여 분류하고, 이를 기반으로 초등학생이 이해하기 쉬운 어휘 검사의 형태로 설문지를 구성하여 응답받았다. 정보보호교육 지역 센터(고려대학교, 충남대학교, 부산대학교)가 위치한 권역(수도권, 충청권, 영남권)에 거주하는 초등학생을 대상으로 설문지 192부를 수집하였고 구조 방정식 모형을 사용하여 분석하였다. 분석결과, 정보윤리인식과 정보보호 인식은 초등학생의 정보보호실천에 긍정적인 영향을 미치는 것으로 나타났다.

## II. 이론적 배경

### 2.1 정보보호 교육과정

Table 1. Transition of Information-related Curriculum

Curriculum	Elementary School
5th('87~'92)	- Computer practice
6th('92~'00)	- Handling, managing and writing using computer - Computer training as an extra-curricula activity
7th('98~'10)	- Handling and using the computer
2007 revision ('09~'14)	- Characteristics of information equipment - Characteristics and ethics of cyberspace - Internet and information
2009 revision ('13~)	- Life and information - Life and electricity/electronics

#### 2.1.1 국내의 초등학교 정보보호분야 교육현황

우리나라 초등학교에서 컴퓨터 교육이 처음 시작된 것은 제5차 교육과정부터이다. 제5차 교육과정에서 초등학교의 경우 컴퓨터 활용영역과 쓰임새에 대한 내용이 실과 과목에 실리게 되었다. 제6차 교육과정에서는 컴퓨터 다루기, 관리하기, 컴퓨터로 글쓰기가 초등학교 실과 과목에 포함되었

고, 학교장 재량시간을 이용하여 컴퓨터 교육을 실시할 수 있도록 하였다. 마찬가지로 제7차 교육과정에서도 컴퓨터 다루기, 관리하기, 컴퓨터로 글쓰기가 초등학교 실과 과목에 포함되었다. 2007 개정 교육과정에서는 정보기기 특성, 사이버 공간의 특성 및 윤리, 인터넷과 정보가 실과 과목에 포함되었다. 2009 개정 교육과정에서는 초등학교 5학년과 6학년 실과 과목에 생활과 정보, 생활과 전기·전자 한 단원씩 포함되었다[4, 5].

2.1.2 국내 비정규교과 정보보호분야 교육현황

교육부(Ministry of Education, MOE)에서는 국민 공통 기본 교육과정에서 특별 활동 시간이나 재량 활동시간 등을 활용하여 정보통신 기술에 관한 소양 교육을 실시할 수 있도록 도움을 주고자 초·중등학교 정보통신기술 교육 운영지침을 마련하였다. 그러나 2009 개정 교육과정에서는 초·중등학교 정보통신 교육 운영지침을 삭제하여 현재 운영되고 있지 않다[6].

한국인터넷진흥원(Korea Internet and Security Agency, KISA)에서도 학생들이 함께 참여할 수 있는 인터넷윤리 및 정보보호교육 사업을 추진하고 있다. KISA 홈페이지를 통해 초·중학생들의 정보윤리인식과 정보보호인식 개선 함양을 위해 스스로 참여할 수 있는 교육 서비스를 제공하고 있으며, 정보보호기술 온라인학습장에서 주니어 정보보호 교육을 실시하고 있다[7].

그밖에도 한국교육학술정보원(Korea Education and Research Information Service, KERIS), 한국정보화진흥원(National Information Society Agency, NIA), 서울특별시교육청(Seoul Metropolitan Office of Education, SMOE)과 같은 여러 학술 기관에서 정보 교육 및 정보보호 교육 지도 자료를 마련하고 있다[8, 9, 10].

2.1.3 해외의 정보보호분야 교육현황

미국의 정보 교육 과정은 통합 교과 형태로 운영되고 있으며 국제교육기술협회(The International Society for Technology in Education, ISTE)와 미국 컴퓨터 학회(Association for Computing Machinery, ACM)에서 표준을 지원하고 있다. 이 표준을 각

주 정부에서 교육청 구 단위 그대로 채택하거나 수정하여 표준을 만든다. ACM과 미국 정보과학 교사협회(Computer Science Teachers Association, CSTA)에서 2011년에 개정된 CSTA K-12 Computer Science Standards 의 정보과학 교육과정의 내용은 크게 전산적사고, 협력, 프로그래밍, 컴퓨터통신, 정보생활의 5가지 영역으로 나뉜다[11].

영국은 컴퓨터 과목이 기초 교과에 포함되어 있기 때문에 초·중등 학교에서 필수로 운영하고 있다. 영국 교육부(Department for Education, DE)의 컴퓨터 교육 목적은 컴퓨터를 활용하여 학생들이 변화하는 세계를 창의력과 컴퓨팅 사고를 가지고 이해하기 위함이다. 기술, 과학, 수학 등과 관련성이 많은 컴퓨터 교육을 통해 학생들이 컴퓨터를 이해하고 컴퓨터 지식을 활용할 수 있도록 하고자 한다[12].

인도의 컴퓨터 교육과정(Computer Masti

Table 2. Extra-curricula Information Security Education

Institution	Contents of Education
MOE	<ul style="list-style-type: none"> <li>- Life of the information society</li> <li>- Understanding on information appliances</li> <li>- Understanding of information processing</li> <li>- Sharing of processed information</li> <li>- Overall activities</li> </ul>
KISA	<ul style="list-style-type: none"> <li>- Information security for youths</li> <li>- Internet use guide for youths</li> <li>- Information security during online games</li> <li>- Making a safe pc</li> <li>- Understanding of I-PIN</li> </ul>
KERIS	<ul style="list-style-type: none"> <li>- Overview of information security</li> <li>- Sound information life</li> <li>- Problems and measures in information society</li> </ul>
NIA	<ul style="list-style-type: none"> <li>- Copyright and privacy</li> <li>- Computer skills for preventing unsound information</li> <li>- Internet addiction</li> <li>- Internet etiquette</li> </ul>
SMOE	<ul style="list-style-type: none"> <li>- Understanding of information society</li> <li>- Protecting my information</li> <li>- Protecting others' information</li> </ul>

Curriculum, CMC)은 1~4학년을 대상으로 주당 1시간, 5~8학년을 대상으로는 주당 2시간에 걸쳐 컴퓨터 교육을 진행하도록 하고 있다. 교육 내용은 개념, 사용기술, 사회적 측면 세 가지 영역으로 구성되어 있다. 이 중에서 정보보호교육과 관련된 내용은 사회적 측면에 포함되어 있다[13].

## 2.2 인지행동 이론

인지행동 이론은 인지이론과 행동주의 이론을 통합한 이론으로 인간의 인지 또는 사고가 인간의 행동과 정서에 영향을 준다는 전제에서 인지나 인지 과정을 변화시키기 위해 인지적 기법과 행동적 기법을 함께 적용하는 것이다. 인지행동 이론은 사람이 무엇을 어떻게 생각하는 지가 행동과 정서에 어떠한 영향을 미치는지에 관하여 초점을 두었다. 인간은 인지와 환경, 그리고 개인적인 영향력 사이에서 끊임없이 상호작용을 하며 행동한다. 즉, 환경적 요인이 개인의 행동에 영향을 미치고, 환경적 요인을 인지한 개인은 또다시 환경적 요인을 형성하게 되는 상호결정론적인 입장에서 설명하고 있다.

인지행동 이론가인 Ellis(1962)는 인간의 신념이나 생각 중에서 인지적인 면들이 행동과 정서에 큰 영향을 미친다고 주장하였다[14]. 환경적으로 선행사건이 일어난 후에 사람은 선행사건을 인지하고 이를 바탕으로 행동과 감정이 나타난다는 것이다. Ellis의 이론은 A-B-C이론이라고 불린다. 선행 사건을 뜻하는 Activation Event(A), 신념이나 사고를 뜻하는 Belief System(B), 결과를 뜻하는 Consequence(C)이다.

Fig.1.에서와 같이 본 연구에서는 선행 사건인 정보보호윤리(A) 교육을 통해서 정보보호인식(B)을 개선하고 그 결과 정보보호실천(C)을 하는 행동 결과를 일으킨다고 가정하였다. 따라서 이러한 가정을 바탕으로 정보윤리인식, 정보보호인식, 정보보호실천 요인에 인지행동 이론을 접목시켜 요인간의 관계를 분석하고자 한다.

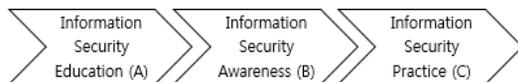


Fig. 1. A-B-C Model

## 2.3 정보윤리인식

### 2.3.1 정보윤리인식의 개념

윤리는 도덕적인 상황이나 문제에 직면했을 때 이러한 것을 해결하기 위해서 선과 악, 옳고 그름을 구분하는 원칙을 말한다[15]. 윤리는 옳고 그름에 대하여 사회적 행동과 태도로 나타나게 되며 실제로 사회 조직이나 집단에서의 규칙으로 나타난다. 이러한 규칙은 개인의 행동을 규제하기도 한다. 특히 최근에 정보화 시대에서는 정보윤리인식이라는 개념이 이론적으로 정립되었다. 정보윤리인식은 정보 사회에서의 행동이나 규범 체계로서 개인 또는 사회구성원들의 행동과 태도의 옳고 그름을 판단하게 해주고 윤리적인 것과 비윤리적인 것으로 나눠 주는 기준이라고 볼 수 있다.

### 2.3.2 정보윤리인식 관련 선행연구

Laudon(1995)은 정보화 사회에서 적용되는 윤리적인 문제들을 정보에 대한 권리와 의무, 지식소유권, 책무와 통제, 시스템의 품질, 삶의 질 이렇게 다섯 가지로 보았다[16].

Rubin(1994)은 정보화 사회에서 여러 가지의 유혹들이 사람의 도덕적 판단을 훼손시킨다고 보았다. 정보 기술 발달이 초래한 속도의 유혹, 프라이버시와 익명성의 유혹, 국제적 범위의 유혹, 파괴력의 유혹이 있다. 앞서 말한 유혹들로 인하여 새로운 문제점이 생기고 윤리에 대한 새로운 시각들이 생겨났다[17].

Johnson(1994)은 정보윤리의 변화를 전혀 새롭게 보거나 아주 전통적인 것처럼 볼 것이 아니라 정보윤리에 관한 의사결정이 새로움과 전통적인 것을 혼합하여 인식 할 것을 주장하였다. 대표적인 예로 예전부터 다뤄왔던 소유권에 정보기술 요인이 추가된 지식재산권이 있다. 이에 더하여 Johnson은 정보화 사회의 윤리 문제를 직업윤리, 지식재산권, 프라이버시, 컴퓨터 범죄와 남용, 해커 윤리, 책임, 사회적 의미 등으로 분류하였다.

정보 통신에 대한 의존도가 점점 증가하면서 발생하는 윤리적 문제들에 대하여 깊은 관심을 가질 필요가 있다. 따라서 본 연구에서는 정보의 역기능 방지, 사이버 범죄로부터 유혹 방지는 물론 스스로 정보를 보호함에 있어서 정보윤리인식은 정보보호실천의 기본이 되며, 정보보호실천에 영향을 미친다고 보았다.

## 2.4 정보보호인식

### 2.4.1 정보보호인식의 개념

인식이란 개념은 정보 시스템 인식 분야뿐만 아니라 사회 과학에서의 사회 인지, 심리학, 의학 등 다방면의 학문 분야에서 관심을 가지고 연구되어 왔다. 인식은 개인의 자각이라고 정의될 수 있으며, 어떠한 것에 관심이 증가하는 것도 인식의 주요 구성요인 중 하나로 여겨진다. 사람들은 직면하는 환경에 대해 위협하는 활동들을 인지함으로써, 일관된 목표를 향해 업무를 조정해나갈 수 있다[18].

정보보호인식은 정보보호에 대한 개인의 자각 및 정보보호활동에 대한 관심도라고 할 수 있다[18]. Cavulsoglu 외(2009)의 연구에서 정보보호에 대한 인식은 조직 구성원들의 정보보호에 대한 일반적 지식과 조직 내의 정보보호정책에 대한 인식 정도라고 정의하였다[23].

### 2.4.2 정보보호인식 관련 선행연구

정보보호실천에 있어 정보보호인식 제고가 무엇보다 중요하다고 많은 선행연구에서 주장하고 있다.

Choi 외(2008)는 정보보호인식이야말로 조직 전체의 정보 자산을 책임져줄 정보보호 성과에 대한 핵심 지표이며, 여러 보안 위협으로부터 정보 시스템을 성공적으로 보호할 수 있도록 해주는 가장 결정적인 요인으로 보았다[18]. 따라서 조직의 정보 자산을 보호하기 위해서는 정보보호인식을 가장 중요하게 고려해야 한다고 주장하였다.

Siponen(2000)은 정보보호인식이 증가됨에 따라 사용자들이 정보 유출 등과 관련된 실수를 줄이게 될 것이고 사용자 관점에서의 보안 기술 및 절차에 대하여 효율적으로 운영하게 될 것이라고 주장하였다[19].

Solms(2001)은 회사나 조직에서 정보 자산을 보호하기 위해서 정보보호에 관련된 많은 기술들을 구현하고 이에 대한 투자를 증가시키더라도 조직 구성원들이 정보보호에 대한 인식이 부족하다면 이러한 기술 투자들은 효과가 없을 것이라고 주장하였다[20].

Chen 외(2008)은 현 시대에는 기술적 보안 솔루션과 더불어 정보자산 보호의 가장 중요한 요인은 사람이라 주장하였다. 그 중 정보보호인식은 사람을 측정하기 위한 한 요인이다. 보안 위협은 사용자의

정보보호인식 부족과 행동의 부주의로 인하여 일어난 게 되므로 성공적인 정보보호를 위해서는 정보보호 인식이 다른 기술적인 요인들보다 더 중요 할 수도 있다는 것이다[21].

Nosworthy(2000)는 정보보호 실패가 정보보호 인식 부족, 정보보호 자원 할당 부족, 정보보호 교육 및 훈련 부족 때문이라고 하였다. 따라서 정보보호를 위해서는 정보보호인식을 제고할 수 있는 교육과 훈련이 필요하다고 하였다[22].

Rezgui와 Marks(2008)는 탐색적 연구를 통해서 정보보호인식을 제고하기 위해서는 정보보호교육이 중요하다고 주장하였다. 학습된 환경에서 정보보호인식이 더욱 촉진된다는 것이다[23].

Eminağaoğlu 외(2009)는 회사 직원 2,900명을 대상으로 암호 사용 등과 같은 정보보호 교육과 함께 캠페인 프로젝트를 12개월에 걸쳐 실시한 뒤 통계적으로 분석하였다. 그 결과 정보보호인식 교육 그리고 교육 관련 캠페인이 긍정적이고 효과적인 결과를 가져온다는 것을 확인하였다[27].

Hagen 외(2011)는 회사 직원들을 대상으로 이터닝 학습 일주일 전과 이터닝 학습 후 8개월 뒤 두 차례 걸쳐 설문조사를 실시하였고, 설문조사에서는 직원들의 지식과 태도, 두 가지를 평가하였다[25]. 평가 결과, 정보보호인식과 정보보호실천 개선을 목표로 하는 이터닝 학습 도구가 장기적으로 효과가 있음을 확인하였다.

정보보호인식에 대한 연구 분석 결과, 정보보호인식과 정보보호실천 활동과의 관계에 대한 연구가 주를 이루고 있었다. 정보보호실천을 위한 정보보호인식을 높여주는 교육과 훈련의 중요성을 강조하는 연구가 많았고, 정보보호교육이 효과적이라는 것을 많은 연구에서 보여주었다. 본 연구에서는 선행연구 결과를 통하여 초등학생을 대상으로 적절한 교육 내용과 교육 방법을 개발하여 정보보호인식을 높여주면 정보보호실천 개선에 도움이 됨을 확인하고자 한다.

## III. 연구모형 및 가설

### 3.1 연구모형

본 연구는 이상에서 언급한 초등학생들의 정보보호실천에 영향을 주는 요인들 사이의 관계를 분석하기 위해 Fig.2.와 같은 모형을 제시하고 분석하였다.

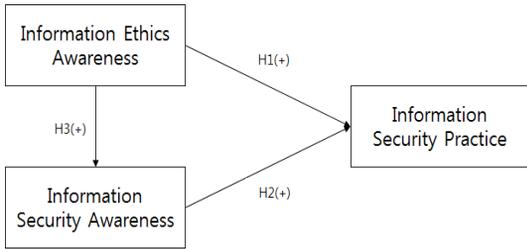


Fig. 2. Research Model

정보윤리인식(Information Ethics Awareness)는 정보 사회에서의 행동과 태도의 옳고 그름을 판단하고 윤리적인 것과 비윤리적인 것으로 나눠 주는 기준이며, 정보보호인식(Information Security Awareness)는 정보보호에 대한 개인의 자각 및 정보보호활동에 대한 관심도이다. 정보보호실천(Information Security Practice)는 정보보호에 대하여 인식에 그치는 것이 아니라 정보보호활동을 직접 수행하고 실천하는 것이다.

## 3.2 연구가설

### 3.2.1 정보윤리인식과 정보보호실천 가설

정보윤리인식교육의 부재로 정보사회의 역기능이 발생하기도 한다. 역기능을 줄이기 위해선 정보윤리인식교육을 통한 정보윤리인식 확립이 중요하다. Bulgurcu 외(2009)는 '정보보안정책 준수에 있어 정보보호인식과 지각된 공정성의 역할'이라는 실증연구를 하였다[26]. 연구결과, 정보보호인식과 지각된 공정성이 조직의 정보보호정책과 규칙을 따르는 태도에 영향을 미치는 역할을 함을 증명하였다. 따라서 본 연구에서는 정보윤리인식이 정보보호실천에 영향을 미치는지를 측정하기 위하여 다음과 같이 가설을 설정하였다.

H1(+): 정보윤리인식(Information Ethics Awareness, IEA)은 정보보호실천 (Information Security Practice, ISP)에 정(+의 영향을 미칠 것이다.

### 3.2.2 정보보호인식과 정보보호실천 가설

Choi 외(2008)는 정보보호인식과 정보보호실천 사이에 관계가 있음을 증명하였다[18].

Eminagaoglu 외(2009) 또한 조직 구성원을 대상으로 정보보호인식을 증가시키기 위한 정보보호교육과 캠페인을 1년에 걸쳐 실시한 뒤 정보보호활동이 개선되었음을 확인하였다[27]. Kruger 외(2010)는 대학생들을 대상으로 정보보호인식 수준과 정보보호실천에 대한 질문들로 설문지 구성하여 정보보호인식 수준이 높은 학생이 정보보호실천을 잘한다는 결론을 도출하고, 정보보호인식과 정보보호실천 간의 관련성을 증명하였다[32]. 따라서 본 연구에서는 정보보호인식이 정보보호실천에 영향을 미치는지를 측정하기 위하여 다음과 같이 가설을 설정하였다.

H2(+): 정보보호인식(Information Security Awareness, ISA)은 정보보호실천에 정(+의 영향을 미칠 것이다.

### 3.2.3 정보윤리인식과 정보보호인식 가설

Johnson(1994)은 정보윤리에 대한 의사 결정은 전혀 새로운 것이 아니며 또한 고전적인 것도 아니라고 하였다. 새로운 것과 고전적인 것이 혼합된 것으로 인식할 것을 주장하였다[18]. 이러한 측면에서 지식재산권의 경우도 전통적인 저작권과 지식 정보가 혼합된 것으로 정보윤리도 전통적인 윤리 개념과 새로운 정보통신 개념이 함께 쓰인다고 말하였다. 직업윤리, 지식재산권, 프라이버시, 컴퓨터 범죄, 컴퓨터 남용, 해커 윤리 등으로 분류하여 정보윤리인식과 정보보호인식 간의 관계가 혼합되어 있음을 설명하였다. Grover(1993)는 정보에 관한 문화, 정책, 규범이 정보의 유형과 함께 정보 처리자의 인식과 태도에 영향을 미칠 수 있으며 결과적으로는 정보 처리자의 행위에도 영향을 미칠 수 있다고 주장하였다[28]. 따라서 본 연구에서는 정보윤리인식이 정보보호인식에 영향을 미치는지를 측정하기 위하여 다음과 같이 가설을 설정하였다.

H3(+): 정보윤리인식은 정보보호인식에 정(+의 영향을 미칠 것이다.

## IV. 연구방법

### 4.1 데이터 수집 및 표본특성

본 연구의 실증 분석을 위해 초등학교 고학년생(4

Table 3. Profile of Sample

Category	Items	Frequency	Ratio (%)
Gender	male	102	53.1
	female	90	46.9
Grade	4	45	23.4
	5	103	53.6
	6	44	22.9
Region	Capital	45	23.4
	Chungcheong	41	21.4
	Yeongnam	106	55.2
Total		192	100

학년, 5학년, 6학년)을 표본으로 하였다. 초등학교 고학년생을 표본으로 선정할 이유는 본 연구의 설문지 항목의 수준이 초등학교 저학년생 보다는 고학년생에게 적합하다고 판단되기 때문이다. 데이터 수집을 위하여 2014년 9월 25일부터 11월 22일까지 약 두 달간 정보보호교육 지역 센터(고려대학교, 충남대학교, 부산대학교)가 있는 3개 권역(수도권, 충청권, 영남권)에 거주하는 초등학교생을 대상으로 설문조사를 진행하였다. 설문지 220부를 배포하였으며, 그 중에서 성실하게 응답한 192부를 확보하였다.

다음의 Table 3.에서는 수집된 표본을 이용하여 응답대상자의 성별, 인구, 지역과 관련된 인구통계학적 특성을 알아보기 위하여 빈도분석을 실시하여 정리한 것이다. 응답자의 남녀비율은 남자 102명(53.1%), 여자 90명(46.9%)으로 남성의 비율이 높았으며, 학년별로는 5학년 103명(53.6%), 4학년 45명(23.4%), 6학년 44명(22.9%) 순으로 5학년 학생의 비율이 높게 나타났다. 권역별로는 영남권 106명(55.2%), 수도권 45명(23.4%), 충청권 41명(21.4%) 순으로 영남권에 거주하는 초등학교생의 비율이 높게 나타났다.

## 4.2 측정척도 개발

### 4.2.1 초등학교 정보보호어휘 연구문항

본 연구의 목적을 달성하기 위해 기존의 국내외 초등학교 교육과정과 초등학교생을 대상으로 하는 정부 산하 학술기관의 지침서에서 제시하고 있는 교육 내용을 신뢰성과 타당성이 검증된 측정 항목들 토대로 연구문항을 구성하였다. 연구 대상이 초등학교생이기 때문에 용어 형식의 문항을 선택하였다.

글의 이해는 해독, 정보처리 속도와 단어 재인,

추론, 배경 지식 및 상위인지 등과 같은 여러 가지 인지 능력에 의해서 이루어진다. 해독이란 시각적으로 제시된 글자를 보고 말소리로 바꾸는 기술을 뜻하며, 재인이란 심성 어휘집에 접근하여 단어의 의미를 이해하는 처리 기술을 의미한다. 해독과 재인 과정이 정확하고 빠르고 자동적으로 이루어지면 능숙한 독자로 발전할 수 있다[29]. 학령기 어린이가 익숙한 짧은 단어를 재인하기 위해서 약 0.5초 정도 걸리고 성인은 약 0.25초가 걸린다. 그 이유는 학령기 어린이는 성인에 비해 먼저 시각적이고 청각적인 수준에서 단어를 자동처리하기 때문이다. 따라서 학령기 어린이를 대상으로 하는 설문지를 일반인 대상으로 하는 설문지 형식과 동일하게 할 수가 없다. 정보보호 전반에 대한 내용을 다 묻기에는 많은 시간이 소요될 것은 물론 초등학교생들이 이해하고 응답하기 힘들기 때문이다[30].

용어검사 형식에 대해서는 Kruger 외(2010)의 연구에서 대학생을 대상으로 보안 어휘 검사와 보안 활동 간의 타당성을 검증하였다. 첫 번째 섹션에서는 응답자의 행동을 평가하는 어휘 검사를 실시하였고, 두 번째 섹션에서는 보안 활동을 수행 할 수 있는 지에 대하여 검사를 실시하였다. 분석 결과의 한 예를 들면 강력한 비밀번호(Strong Password)가 무엇인지 모르는 응답자는 비밀번호를 매우 간단하게 설정하였다. Kruger 등은 두 섹션 간의 연관성을 검증하면서 보안 어휘 검사의 타당성을 입증하였다[31].

따라서 검증된 바 있는 보안 용어 형식으로 초등학교생의 글 이해 수준을 고려한 정보보호 어휘들을 응답자에게 물음으로써 단어를 통한 정보보호에 대한 포괄적인 개념 이해정도를 확인하고자 한다. 구성 개념 용어는 각 교육 기관에서 초등학교생을 대상으로 정보보호 교육 지도 자료를 제공한 내용에서 발췌하였으며, 용어의 빈도를 고려하여 정보윤리인식, 정보보호인식, 정보보호실천이라는 3가지 개념으로 용어를 정리하여 나누었다(Table 4).

### 4.2.2 설문지 구성

본 연구의 설문지는 초등학교생 대상의 정보보호 교육 자료를 바탕으로 초등학교생의 언어 수준을 고려한 이해하기 쉬운 용어로 구성되어 있다. 설문지는 네 개 부분으로 구성되어 있다. 첫 번째 섹션은 성별, 나이, 사는 지역과 같은 설문대상의 기본적인 정보를

Table 4. Elements of Questionnaire Design

Construct	Items	Reference								Counts
		MOE	KISA	KERIS	NIA	SOME	CSTA	NCE	CMC	
IEA	IEA1	O	O	O	X	O	O	X	O	6
	IEA2	X	O	O	X	O	X	X	O	4
	IEA3	O	X	X	O	O	O	X	O	5
	IEA4	X	O	O	O	O	X	O	X	5
	IEA5	O	O	O	O	O	O	O	X	7
ISA	ISA1	X	O	O	X	O	O	O	X	5
	ISA2	O	O	O	O	O	X	O	X	6
	ISA3	O	O	O	O	X	X	X	O	5
	ISA4	X	X	X	X	O	X	X	X	1
	ISA5	O	X	X	X	X	X	X	X	1
	ISA6	O	O	X	O	O	X	X	X	4
	ISA7	X	O	X	X	X	X	X	X	1
	ISA8	X	O	X	X	X	X	X	X	1
ISP	ISP1	X	O	O	O	O	O	O	X	6
	ISP2	X	O	X	X	X	X	X	X	1
	ISP3	X	O	O	X	X	X	X	O	3
	ISP4	O	O	X	O	O	X	X	X	4
	ISP5	X	X	O	X	X	O	X	X	2
	ISP6	X	O	X	X	X	X	O	O	3
	ISP7	O	O	O	O	X	X	X	O	5

수집하였다. 두 번째 섹션에서부터는 설문지 측정에 사용되는 변수들로 구성하였다. 독립변수인 정보윤리 인식에 대한 응답자의 이해 정도를 측정하기 위하여 사이버 폭력(IEA1), 악성 댓글(IEA2), 인터넷 중독(IEA3), 불법 사이트(IEA4), 불법 다운로드(IEA5)에 관한 항목을 선정하였다. 세 번째 섹션은 매개변수인 정보보호인식에 대한 응답자의 이해 정도를 측정하기 위하여 해킹(ISA1), 바이러스(ISA2), 스팸(ISA3), 피싱(ISA4), 암호화(ISA5), 개인정보 유출(ISA6), 주민등록번호 도용(ISA7), 아이핀(ISA8)에 관한 항목을 선정하였다. 끝으로 네 번째 섹션은 정보보호실천에 대한 응답자의 이해 정도를 측정하기 위하여 정품 프로그램 사용(ISP1), 백신 프로그램 설치 및 사용(ISP2), 사이트 비밀번호 관리(ISP3), 개인정보 피해 예방(ISP4), 정보보호 법률 확인(ISP5), 온라인 의사소통 시 정보 보안(ISP6), 스팸 신고 및 차단(ISP7)에 관한 항목을 선정하였다. 선정된 설문항목들은 리커트(Likert) 7점 척도(1:전혀 모른다, 4:보통이다, 7:매우 잘 안다)를 사용하여 측정하였다(Table 4).

## V. 가설검증 및 분석결과

연구 모형과 가설을 검증하기 위해서 수집한 데이

터를 Smart PLS 2.0 프로그램으로 분석하였다. 부분최소자승법(Partial Least Square, PLS)은 이론적 구조 모형을 평가하고 측정 모형에 대한 평가를 동시에 할 수 있는 분석 도구이며, 측정 항목과 구성 개념 간의 관계가 원인과 결과인 모형을 분석하는 데 용이하다[32].

### 5.1 측정모형

본 연구의 목적은 초등학생의 정보보호실천에 영향을 미치는 요인에 관한 연구모형을 개발하고, 모형의 유효성을 검증하는 것이다. 따라서 잠재변수 및 측정항목의 내적일관성(Internal Consistency), 집중타당성(Convergent Validity), 판별타당성(Discriminant Validity) 검증을 요구한다.

내적일관성 검증을 위해 반영지표인 정보윤리인식, 정보보호인식, 정보보호실천을 대상으로 평균 분산추출(Average Variance Extracted, AVE)값과 복합신뢰도(Composite Reliability, CR), 그리고 측정 도구의 신뢰성을 확인하기 위한 크론바하알파(Cronbach's Alpha)계수를 측정하였다[33]. 측정치에 관한 일반적인 검증 기준은 AVE 값이 0.5이상, CR 값이 0.7이상이며 Cronbach's Alpha 계수가 0.7 이상으로 나타나면 측정 도구의

Table 5. Results of Reliability and Validity Tests

Construct	Items	Mean	S.D	Factor Loading	AVE	CR	Cronbach's Alpha
IEA	IEA1	5.94	1.12	0.749	0.638	0.924	0.904
	IEA2	6.09	1.19	0.781			
	IEA3	6.26	1.16	0.78			
	IEA4	5.02	1.96	0.818			
	IEA5	5.33	1.85	0.822			
ISA	ISA1	5.15	1.95	0.853	0.631	0.932	0.915
	ISA2	5.17	1.92	0.789			
	ISA3	5.19	2.01	0.819			
	ISA4	4.86	2.16	0.871			
	ISA5	4.77	2.01	0.734			
	ISA6	5.63	1.71	0.812			
	ISA7	4.85	2.04	0.790			
	ISA8	4.41	2.12	0.661			
ISP	ISP1	5.56	1.30	0.801	0.625	0.893	0.852
	ISP2	4.77	2.01	0.703			
	ISP3	5.35	1.44	0.867			
	ISP4	5.10	1.72	0.866			
	ISP5	4.71	1.50	0.680			
	ISP6	5.34	1.64	0.874			
	ISP7	5.51	1.70	0.775			

신뢰성이 확보되었다고 볼 수 있다[31]. PLS 분석 결과 AVE 값은 0.625~0.638, CR 값은 0.893~0.924, Cronbach's Alpha 계수는 0.852~0.915 사이에 분포되어 모두 기준치를 상회한 것으로 나타났다. 본 측정 모형의 신뢰성이 확보되었다고 볼 수 있으며 내적일관성이 검증되었다.

집중타당성은 개별 관측변수의 측정 항목에 대한 요인적재값(Factor Loading)과 t 값으로 검증하였다. PLS 분석에서는 탐색적 요인분석보다는 확인적 요인분석을 요구하는데, 요인적재값 값의 일반적인 기준은 0.5~0.95사이에 분포하면 유의하다고 보고 0.7이상이면 신뢰성이 있다고 판단한다. PLS 분석 결과 구성 개념의 요인적재값은 검증 기준치인 0.5~0.95사이에 분포된 것으로 유의성이 검증되었다. 따라서 Table 5.에서 보는 바와 같이 ISA8의 값 0.661을 제외한 모든 개별 관측변수 값이 0.7을 상회하기 때문에 집중타당성이 양호하다고 판단된다[34]. 또한 각 요인적재값이 다른 요인적재값보다 크기 때문에 모든 설문문항이 해당 기준을 충족하였으며 요인적재값의 t값은 유의수준 5%에서 모두 유의한 것으로 나타났다[36].

판별타당성은 구성 개념 간 상관계수 중에서 가장 큰 값과 AVE의 제곱근 값 중 가장 작은 값을 비교하여 AVE의 제곱근 값이 상관계수보다 큰 경우에 판별타당성이 있다고 판단된다[34]. PLS 분석결과

AVE의 제곱근 중 가장 작은 값 0.791이 가장 큰 상관계수 값 0.731을 상회하였다[Table 6]. 따라서 본 연구에서 사용된 개별 잠재변수 모두의 판별타당성이 존재하는 것으로 검증되었다.

이상으로 본 연구모형에서 사용된 구성 개념과 측정 문항에 대한 내적일관성, 집중타당성, 판별타당성을 검증한 결과 모든 기준 요건을 만족하였다. 따라서 본 모형에 대한 신뢰성과 타당성이 검증되었다.

Table 6. Results of Discriminant Validity

Construct	IEA	ISA	ISP
IEA	<b>0.791</b>		
ISA	0.731	<b>0.795</b>	
ISP	0.594	0.691	<b>0.798</b>

The correlation coefficients in the diagonal matrix are the square roots of AVE, respectively.

## 5.2 가설검증

본 연구에서 제시한 구조 모형의 계수를 측정하기 위하여 PLS 부스트래핑(Bootstrapping) 기법을 사용하여 Fig.3.과 같이 가설검증용 경로분석을 수행하였다. 분석결과 R<sup>2</sup>값이 모두 0.1을 상회하여 각 구성개념에 대한 분산설명력(explained variance)

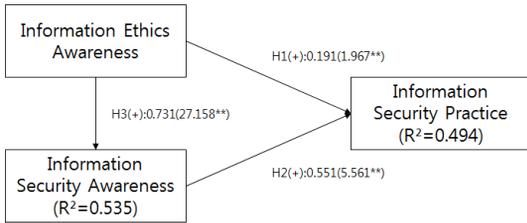


Fig. 3. Results of Path Analysis

Table 7. Analysis Results of Hypothesis Test

	Path	Coefficient	t-Value	Result
H1	IEA → ISP	0.191	1.967**	Accepted
H2	ISA → ISP	0.551	5.561**	Accepted
H3	IEA → ISA	0.731	27.158**	Accepted

이 충분한 것으로 해석된다[35]. Table 7.과 같이 모든 경로계수들은 통계적으로 유의수준 0.05에서 지지되어 가설이 채택되었다. 또한 구조 모형의 전체 적합도(Goodness of Fit, GoF)를 확인할 수 있는데, GoF 값은 공통성 평균과 R<sup>2</sup>평균의 기하평균을 사용하여 구할 수 있다[32]. 분석결과 Wetzels 외 (2009)가 제시한 GoF값 0.36보다 훨씬 상회한 0.57이 나왔다. 따라서 본 연구에서 제시한 모형의 GoF의 값은 상당히 높으므로 본 연구에서 사용된 모형에 대한 적합도는 충분한 것으로 해석된다[32].

본 연구의 가설을 검증한 결과는 다음과 같다 [Table 7]. 첫째, 정보윤리인식(IEA)이 정보보호실천(ISP)에 정(+)의 영향을 미칠 것으로 가정하였는데, 분석결과 경로계수 값은 0.191, t-값은 1.967로 유의하게 나타나 가설 H1(+)이 채택되었다. 둘째, 정보보호인식(ISA)이 정보보호실천(ISP)에 정(+)의 영향을 미칠 것으로 가정하였는데, 분석결과 경로계수 값은 0.551, t-값은 5.561으로 유의하게 나타나 가설 H2(+)가 채택되었다. 마지막으로 정보윤리인식(IEA)이 정보보호인식(ISA)에 정(+)의 영향을 미칠 것으로 가정하였는데, 분석결과 경로계수 값은 0.731, t-값은 27.158으로 유의하게 나타나 가설 H3(+)이 채택되었다.

따라서 정보보호실천을 위해서는 정보윤리인식과 정보보호인식이 유의한 영향을 미친다는 것을 확인할 수 있으며, 경로계수 비교를 통해 정보윤리인식 보다는 정보보호인식이 정보보호실천에 더 강한 영향을

미치는 것을 확인할 수 있다. 하지만 정보윤리인식이 정보보호인식에 영향을 미치지 때문에 초등학생의 정보보호실천을 위해서는 정보윤리인식 교육과 정보보호인식 교육 둘 다 필요하다고 말할 수 있다.

## VI. 결 론

### 6.1 연구결과의 요약

본 연구에서는 초등학생들의 정보윤리인식과 정보보호인식이 정보보호실천에 미치는 요인을 실증적으로 검증하였다. 이를 위해 국내외 정보교과와 학술기관의 정보보호교육 지침서들을 바탕으로 정보윤리인식, 정보보호인식, 정보보호실천 요인들을 추출하였다. 연구 모형을 개발함에 있어 정보윤리인식과 정보보호인식이 정보보호실천에 영향을 미치는지에 대해 규명하고자 인지행동 이론을 참고하였고, 설문지 개발에 있어 초등학생들의 특성을 고려한 언어발달이론을 활용하였다.

연구결과를 요약하면 다음과 같다. 첫째, 정보윤리인식은 정보보호실천에 정(+)의 영향을 미치는 것으로 나타났다. 둘째, 정보보호인식은 정보보호실천에 정(+)의 영향을 미치는 것으로 나타났다. 셋째, 정보윤리인식은 정보보호인식에 정(+)의 영향을 미치는 것으로 나타났다.

### 6.2 연구결과의 시사점

국내외 초등학생의 정보보호교육에 대한 연구가 부족한 실정이며, 정보보호실태 및 정보보호교육 방법에 관한 연구는 존재하나 초등학생을 대상으로 구체적으로 무엇으로 가르쳐야 학생들이 정보보호실천을 할지에 대한 교육 내용 중심의 연구는 거의 없었다. 학교 정규교과에도 정보보호교육내용이 없기에 정보보호 교육을 실시하고자 하는 교사들도 어떠한 내용을 가르쳐야 학생들이 정보보호실천을 할지에 대해 어려움이 있었으리라 본다.

이에 본 연구에서는 초등학생들의 정보윤리인식과 정보보호인식이 정보보호실천에 유의미한 영향을 미친다는 것을 검증하였다. 또한 초등학생들의 정보보호인식 수준과 실태를 파악함으로써 정보윤리인식과 정보보호인식을 높일 수 있는 정보보호교육의 필요성을 알 수 있다.

연구결과, 초등학생들은 정보윤리인식이 정보보호

실천에 19.1%, 정보보호인식이 정보보호실천에 55.1%, 정보윤리인식이 정보보호인식에 73.1% 영향을 미쳤다. 초등학교의 정보보호실천에 있어서 정보보호인식이 정보윤리인식보다 더 큰 영향력을 미친다. 따라서 초등학교들이 네티켓에 한정된 정보윤리 교육만 받는 것으로 마치는 것이 아닌, 정보보호에 관한 정보윤리인식과 더불어 정보보호인식 개선을 위한 교육을 받는다면 초등학교들의 정보보호실천에 도움을 줄 것으로 기대한다.

컴퓨터 교육의 경우 일반적인 방법 보다 교과목 특성과 교육 환경을 고려하여 교수 학습 방법을 선택하여야 한다. 일반적으로 교수 학습법은 크게 학생중심, 교수중심, 학습내용중심 교수방법으로 나누어지며 그 외에 다양한 교수법이 세부적으로 존재한다 [37]. 본 연구에서는 정보보호인식의 중요성을 확인했기에 개념 지도법 등의 학습 내용 중심 교수법을 활용하면 좋을 것이다. 또한 본 연구에서 통계적 방법으로 입증된 결과를 바탕으로 구체적인 초등학교 수준에서의 정보보호에 대한 개념적 인식을 할 수 있는 교육 방법을 개발하는데 도움을 줄 수 있을 것이다.

### 6.3 연구의 한계

본 연구에 필요한 자료를 수집함에 있어 표본의 집단적 편차가 크기 때문에 결과에 대하여 일반화하는 것이 다소 제한적이다. 또한 초등학교를 대상으로 하는 정보보호 교육과정이 따로 없기 때문에 측정 요인들을 선택함에 있어 한계가 있다. 따라서 향후 초등학교 관계자와 정보보호 전문가가 참여하여 초등학교의 개인적 인식 외에도 환경적인 요인과 같은 외부적 요소를 비롯하여 초등학교에 특화된 요인을 찾아 초등학교의 정보보호실천에 관하여 정기적인 조사를 실시한다면 의미 있는 결과를 얻을 것으로 기대한다.

이를 바탕으로 향후 연구에서는 본 연구에서 분류한 정보보호교육 내용을 토대로 초등학교에게 효과적인 정보보호 교수법에 대한 연구가 이루어지는 것이 바람직할 것이다. 따라서 초등학교의 정보보호교육에 대한 많은 학문적 연구와 자료들이 축적되어야 하며 이에 대한 후속 연구가 필요하다.

## References

- [1] Korea Internet and Security Agency, Internet Use Survey, 2014.
- [2] Korea Internet and Security Agency, Mobile Internet Use Survey, 2015.
- [3] Korea Communications Commission, Cyber Bullying Research, 2014.
- [4] Korea Association of Information Education, Elementary School Information Curriculum Contents System, 2014.
- [5] Education and Information Research Academy of Korea, Primary and Secondary Information Education, 2005.
- [6] Ministry of Education(South Korea), Information and Communication Technology Education Instructions, 2005.
- [7] Korea Internet and Security Agency, Online Learning of Junior Information Security, 2014.
- [8] Korea Education and Research Information Service, Primary and Secondary School Information Security Education Reinforcement Support, 2005.
- [9] National Information Society Agency, The Healthy Information Life, 2007.
- [10] The Seoul Metropolitan Office of Education, Information and Communication Ethics Education Instructional Materials for Elementary School Students, 2010.
- [11] CSTA, CSTA K-12 Computer Science Standard, 2011.
- [12] Department for Education(England), National Curriculum in England: Computing Programmes of Study, 2013.
- [13] Department of Computer Science and Engineering Indian Institute of Technology Bombay, Mumbai, CMC: A Model Computer Science Curriculum for K-12 School, 2013.
- [14] A. Ellis, "The revised ABC's of ration-

- al-emotive therapy(RET)," *Journal of Rational-Emotive and Cognitive-Behavior Therapy*, vol. 9, no. 3, pp. 139-172, 1991.
- [15] K.E. Goodpaster, "The concept of corporate responsibility," *Journal of Business Ethics*, vol. 2, no. 1, pp. 1-22, 1983.
- [16] K.C. Laudon, "Ethical concepts and information technology," *Communications of the ACM*, vol. 38, no. 12, pp. 33-39, 1995.
- [17] R. Rubin, *Moral Distancing and The Use of Information Technologies*, Computer Ethics Institute, Washington, DC, 1994.
- [18] D. Johnson, *Computer Ethics, The Philosophy of Computing and Information*, 1985.
- [19] N. Choi, D. Kim, J. Goo and A. Whitmore, "Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action," *Information Management and Computer Security*, vol. 16, no. 4, pp. 484-501, 2008.
- [20] M. Siponen, "A conceptual foundation for organizational information security awareness," *Information Management and Computer Security*, vol. 8, no. 1, pp. 31-44, 2000.
- [21] B.V. Solms, "Information security - A multidimensional discipline," *Computer and Security*, vol. 20, no. 6, pp. 504-508, 2001.
- [22] J. Nosworthy, "Implementing information security in the 21 st century - do you have the balancing factors?," *Computer and Security*, vol. 19, no. 4, pp. 337-347, 2000.
- [23] C. Chen., B. Medlin and R. Shaw, "A cross-cultural investigation of situational information security awareness programs," *Information Management and Computer Security*, vol. 16, no. 4, pp. 360-376, 2008.
- [24] Y. Rezgui and A. Marks, "Information security awareness in higher education: An exploratory study," *Computer and Security*, vol. 27, no. 7, pp. 241-253, 2008.
- [25] J. Hagen, E. Albrechtsen and S.O. Johnsen, "The long-term effects of information security e-learning on organizational learning," *Information Management and Computer Security*, vol. 19, no. 3, pp. 140-154, 2011.
- [26] B. Bulgurcu, H. Cavusoglu and I. Benbasat, "Roles of information security awareness and perceived fairness in information security policy compliance," *AMCIS 2009 Proceedings*, pp. 419, 2009.
- [27] M. Eminağaoğlu, E. Ucar and S. Eren, "The positive outcomes of information security awareness training in companies - A case study," *Information Security Technical Report*, vol. 14, no. 4, pp. 223-229, 2009.
- [28] S.L. Grover, "Lying, deceit, and subterfuge: A model of dishonesty in the workplace," *Organization Science*, vol. 4, no. 3, pp. 478-495, 1993.
- [29] K.E. Stanovich, "Matthew effects in reading: Some consequences of individual differences in the acquisition of literacy," *Reading Research Quarterly*, vol. 21, no. 4, pp. 360-407, 1986.
- [30] R.E. Owens Jr, *Language Development: An Introduction*, Pearson, 2015.
- [31] H. Kruger, L. Drevin and T. Steyn, "A vocabulary test to assess information security awareness," *Information Management and Computer Security*, vol. 18, no. 5, pp. 316-327, 2010.
- [32] M. Wetzel, G. Odekerken-Schröder and C. V. Oppen, "Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration," *MIS Quarterly*, vol. 33, no. 1, pp. 177-195, 2009.
- [33] J.C. Nunnally, *Psychological Theory*,

- McGraw-Hill, 1987.
- [34] C. Fornell and D.F. Larcker, "Two structural equation models with unobservable variables and measurement error," *Journal of Marketing Research*, vol. 18, no. 1, pp. 39-50, 1981.
- [35] R.F. Falk and N.B. Miller, *A Primer for Soft Modeling*, University of Akron Press, 1992.
- [36] D. Gefen and D. Straub, "A practical guide to factorial validity using pls-graph: tutorial and annotated example," *Communications of the Association for Information Systems*, vol. 16, no. 1, pp. 91-109, 2005.
- [37] T. Lee, *The Computer Curriculum Education Theory*, Ehan Publishing Company, 2006.

### 〈저자소개〉



최 승 재 (Seung-Jae Choi) 학생회원  
 2013년 2월: 한국교원대학교 컴퓨터교육과 학사  
 2015년 2월: 충북대학교 정보보호경영학과 석사  
 2015년 3월~현재: 한국교원대학교 컴퓨터교육과 박사과정  
 <관심분야> 정보통신과 정보보호 분야의 교육 및 정책



김 형 열 (Hyeong-Yeol Kim) 학생회원  
 2015년 2월: 한남대학교 경찰행정학과 학사  
 2015년 3월~현재 : 충북대학교 정보보호경영학과 석사과정  
 <관심분야> 정보보호관리체계, 정보보호영향평가, 정보보호투자 의사결정



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 및 학과장, 보안컨설팅연계전공 주임 교수, 일반대학원 정보보호경영전공 주임교수, 국가정보원 보안관리실태평가 자문 및 평가 위원, 금융보안원 금융보안컴플라이언스 자문위원, 전자정부 민관협력포럼 자문위원  
 <관심분야> 정보통신과 정보보호 분야의 경영 및 정책 의사결정