

침해 경험 및 정보보호 인식이 정보보호 행동에 미치는 영향에 대한 연구 : 이중 프로세스 이론을 중심으로*

김창일** · 허덕원*** · 이혜민**** · 성욱준*****

요약

본 연구의 목적은 정보침해 경험이 정보보호 활동에 직관적으로 미치는 영향과 정보보호 인식을 통해 분석적으로 미치는 영향을 이중 프로세스 이론(Dual Process Theory)을 통해 분석하는데 있다. 이를 위해 Baron & Kenny 매개 회귀분석을 사용하였으며 그 분석결과는 다음과 같다. 첫째, 정보침해 경험은 정보보호 활동에 긍정적인 영향을 미치는 것으로 분석되었다. 둘째, 정보보호 인식은 정보침해 경험과 정보보호 활동 간의 관계를 매개하는 것으로 분석되었다. 셋째, 정보침해 경험이 정보보호 활동에 직접적으로 주는 영향과 인식을 매개하여 주는 간접적 영향의 효과는 모두 정(+)의 효과를 주는 것으로 분석되었다. 또한 정보침해 경험이 정보보호 활동에 주는 직접적 영향은 인식을 매개하여 정보보호 활동에 주는 간접적 영향에 비해 상대적으로 큰 것으로 분석되었다. 해당 분석결과를 바탕으로 정보보안 활동이 제고 될 수 있도록 하는 주기적 정보보안 교육 및 캠페인 정책이 필요함을 제안하였다.

주제어 : 정보침해 경험, 정보보호 인식, 정보보호 활동, 이중 프로세스 이론

A Study on the Influence of Victimization Experience and Awareness on Cyber Security Behavior – Focusing on Dual Process Theory*

Kim, Chang-Il** · Heo, Deok-Won*** · Lee, Hye-Min**** · Sung, Wook-Joon*****

Abstract

The purpose of this study is to investigate the direct effect of victimization experience on cyber security behavior and the indirect effect of information protection awareness through the Dual Process Theory. Baron & Kenny regression analysis was conducted and the results are as follows - first, victimization experience has a positive effect on cyber security behavior; second, the relationship between victimization experience and cyber security behavior is mediated by cyber security awareness; and third, the direct effect of victimization experience on cyber security behavior and the indirect mediating effect of cyber security awareness are both positive (+). The direct effect of victimization experience on cyber security behavior is analyzed to be relatively large compared to the indirect effect that cyber security awareness has on cyber security behavior.

Based on these results, It is suggested that periodic cyber security education and campaign policies are needed to enhance cyber security behavior.

Keywords : victimization experience, cyber security awareness, cyber security behavior, dual process theory

Received Feb 10, 2019; Revised Mar 15, 2019; Accepted Mar 18, 2019

* This study was supported by the Research Program funded by the SeoulTech(Seoul National University of Science and Technology).

** First Author, Graduated student. Graduate school of public policy and information technology, Seoul national university of science and technology (kyci@naver.com)

*** Graduated student. Graduate school of public policy and information technology, Seoul national university of science and technology (deokza@naver.com)

**** Graduated student. Graduate school of public policy and information technology, Seoul national university of science and technology (93lhm@hanmail.net)

***** Corresponding Author, Assistant professor, Graduate school of public policy and information technology, Seoul national university of science and technology (wjsung@seoultech.ac.kr)

I. 서론

4차 산업혁명 시대 급변하는 인터넷 환경에 따라 새로운 기술이 끊임없이 등장하고 있으며 이러한 새로운 기술과 빅데이터를 결합한 플랫폼 및 서비스가 고도화되고 있다. 이러한 기술과 서비스 고도화에 따라 악성코드, 정보유출 등의 정보침해사고는 어느 한 영역의 개별적인 피해가 아닌 한순간에 광범위한 피해를 주기도 한다.

대표적인 예로 2011년 네이트 데이터베이스에 저장된 가입자 3,500만 명 전원의 아이디, 비밀번호, 이름, 주민등록번호, 연락처 등의 개인정보가 유출되는 사건이 있었다. 또한 2013년 3월 20일에는 6.25 사이버 공격으로 국내 주요 언론사와 금융권의 전산망이 악성코드에 감염 후 다운되는 사태가 발생하여 10일 동안 언론사 및 금융사 6개사의 전산 마비로 인해 상당한 재산상 피해를 보았다. 이러한 정보 침해의 피해는 현재까지 지속적으로 증가하고 있는 추세이고 최근에는 IoT, 인공지능, 자율주행 등 다양한 기술이 개발됨에 따라 그 피해의 영역이 한정적·국지적으로 끝나는 것이 아니라 생명까지 위협할 수 있는 중대한 위협이 되었으며, 이를 사전에 예방하거나 빠른 대응을 수행하기 위한 정보보호의 중요성도 점점 더 커지고 있다.

그렇다면 정보보호 활동은 어떠한 요인의 영향을 받아 증진될 수 있을까? 정보보호 활동과 관련된 많은 선행연구들을 살펴보면 정보보호 활동에 미치는 중요한 영향으로 침해경험 또는 정보보호 인식을 언급하고 있다. 하지만 이와 같은 영향 분석은 각 연구에서 독립적으로 이루어질 뿐 종합적인 영향 관계를 분석한 선행연구는 없었다.

따라서 본 연구는 기존에 이루어지지 않은 정보침해 경험, 정보보호 인식, 정보보호 활동 간의 종합적인 영향 관계를 분석하기 위해 첫 번째 침해경험, 정보보호 인식, 정보보호 활동을 모두 고려하였을 때 이들 간의 관계는 어떠한지 두 번째, 정보침해 경험에서 정보보

호 활동으로 이어지는 과정은 인식을 거치지 않고 바로 영향을 미치는지 아니면 개인의 침해사고경험이 정보보호 인식에 영향을 미치고 정보보호 인식의 매개효과를 통해 정보보호 활동에 영향을 미치는지를 살펴보고자 한다. 이와 같은 경험, 인식, 행동 간 영향 관계를 잘 설명해줄 수 있는 이론은 행동경제학의 이중 프로세스 이론(Dual Process Theory)이다. 이중 프로세스 이론에서의 인간은 두 가지 정보 처리 시스템, 직감적, 연상적, 자동적, 감정적, 병렬 처리, 신속, 노력이 들지 않는 등의 특성을 가진 'System1'과 분석적, 통제적, 규칙 지배적, 직렬 처리, 노력을 필요로 하는 특징을 가지고 있는 'System2'를 통해 정보처리가 동시에 이루어진다고 설명한다.

본 연구에서는 이와 같은 이중 프로세스 이론을 적용하여 개인의 침해경험 및 정보보호 인식이 어떻게 정보보호 활동으로 이어지는지에 대해 분석하고자 한다. 개인의 침해경험과 정보보호 활동, 그리고 이 둘을 매개하는 정보보호 인식의 관계를 분석하여 과연 침해경험과 정보보호 활동의 사이에는 이중 프로세스 이론이 정의하는 인간의 사고 방법 중 어떠한 방식에 의해 이루어지는지에 대해서 살펴보고 그 분석결과에 따라 정부가 정책적으로 정보보호 활동을 장려하기 위해 취할 수 있는 방안에 대해서 고찰해 보고자 한다. 본 연구에서는 해당 분석을 위해 2017년 정보보호 실태조사(개인)의 데이터를 활용하였다.

II. 이론적 배경과 선행연구의 검토

본 연구에서는 개인의 침해사고 경험과 정보보호 인식, 정보보호 활동의 관계를 이중 프로세스 이론을 통해 살펴보고자 하며, 해당 모형을 통해 실증하고자 하는 내용은 다음과 같다.

첫 번째, System1의 직접적 사고절차를 통해 개인의 침해사고가 직접적으로 정보보호 활동에 영향을 미치는지 살펴보고자 한다. 두 번째, System2의 분석적 사고절차를 통해 개인의 침해경험이 정보보호 인식에

영향을 주고 이 인식이 다시 정보보호 활동에 영향을 주는지에 대해서 살펴보고자 한다. 마지막으로 이러한 두 가지 System의 영향 중 어떠한 효과가 큰지에 대해 살펴보고자 한다.

위 세 가지 분석을 위해 우선 각 변수의 이론적 정의와 이중 프로세스 이론의 정의에 대해서 살펴보고 마지막으로 이와 관련된 선행연구를 검토하여, 본 연구에서의 적용 방안을 마련코자 한다.

1. 정보보호 관련 개념

1) 정보침해 경험

정보침해 경험은 시스템의 기밀성(Confidentiality), 무결성(Integrity) 또는 가용성(Availability)을 해치는 컴퓨터 및 네트워크 공격에 대한 경험을 의미한다. Moon and Kim(2017)은 정보침해를 정보에 대한 위협으로서 허락되지 않은 접근이나 수정, 노출, 혹은 훼손, 파괴 등으로 정의하였고 Chung(2013)은 정보침해 경험을 물리적 공격과 기술적 공격, 두 가지 유형으로 나누어 설명하며 해킹, 크래킹, 트로이목마, 취약점 공격, 구조적 공격, 사용자 도용, 서비스방해 공격, 피드백, 시스템위장, 컴퓨터 바이러스, 논리파괴 폭탄 및 기타 물리적인 침해를 세부적 유형으로 나열하였다. 본 연구에서는 이와 같은 선행연구들을 검토하여 정보침해 경험을 PC를 통해 개인정보 유출 및 사생활 침해 경험 사례, 악성코드 감염 등으로 인한 피해사례로 나누고 이 중 몇 가지 사례를 경험했는지 측정을 통해 정보침해 경험 정도를 살펴보고자 한다.

2) 정보보호 인식

인식은 정보보호 분야뿐만 아니라 사회과학 내 사회인지, 심리학, 의학 등 다양한 학문 분야에서 관심을 가지고 지속적으로 연구가 이루어져 왔다. 인식은 개인의 자각이라고 정의되며, 특정 대상에 대한 관심 증대는 인식의 중요한 요인이다. 이를 통해 인식의 구체적 사례인 정보보호 인식은 정보보호에 대한 개인

의 자각 및 정보보호 활동에 대한 관심도라고 정의할 수 있다. Cavulsoglu, et al.(2009)은 정보보호 인식을 조직 구성원들의 정보보호에 대한 지식과 정보보호 정책에 대한 인식 정도라고 정의하였고(Choi, et al., 2016; Lee, et al., 2016), Choi, et al.(2008)은 정보보호 인식을 조직구성원의 정보보안에 대한 일반적 지식과 그들 조직의 정보보안정책에 대한 인식 정도로 정의하였다. 본 연구에서는 이와 같은 선행연구의 정의들을 검토하여 정보보호 인식을 정보보호 중요성 인식의 정도로 측정하고자 한다.

3) 정보보호 활동

정보보호활동(Cyber Security Behavior)이란 여러 가지 위협으로부터 정보의 기밀성, 무결성, 가용성을 유지하기 위해 행하는 전반적 활동을 의미한다. 이와 같은 정보보호의 활동은 첫째, 관리적 보안으로 정보보호에 대한 지침 및 절차를 설정하고 이를 관리 감독하는 활동. 둘째, 기술적 보안으로 보안 위협 상황을 제거하기 위해 정보보호 시스템을 구축하고 운영하는 활동. 셋째, 시스템적 보안으로 허가되지 않은 정보 자산 시설 접근 및 사용을 차단하고 모니터링 하는 활동이 있다(Moon, 2017). 또한 한국정보통신기술협회(TTA)의 정보통신용어사전에서는 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적·기술적 수단 또는 그러한 수단으로 이루어지는 행위로서 정보보호 활동을 정의하였다.

본 연구에서는 이와 같은 선행연구의 정보보호 활동의 정의를 검토하여 정보보안 행동의 정도를 PC 패스워드 설정 빈도로 측정하고자 한다.

2. 이중 프로세스 이론(Dual Process Theory)의 개념 및 의의

이중 프로세스 이론은 인간의 사고가 두 가지 방식으로 이루어지는 것을 다루는 이론으로 행동경계

학, 심리학 등의 영역에서 널리 사용되고 있는 개념이다(Evans, 2008; Kahneman, 2011; Sloman, 1996; E. R. Smith & DeCoster, 2000; Stanovich, 2011; Park, 2016 재인용). 이중 프로세스 이론은 인간의 사고를 크게 System1과 System2로 나눈다. System1은 직관적 사고이며, 이는 의식적 사고 과정을 거치지 않고 행동을 결정하게 되는 방식을 말한다. System2는 의식적으로 정보를 분석하고 활용하여 해결 전략을 만들어나가는 방식을 말한다. System1의 직관적 사고에 따른 행동은 보통 인간의 본능에 의해 반응하게 되지만, System2에서의 의식적 사고과정이 반복됨에 따라 체득되어 발현될 수도 있음을 언급하고 있다. 이와 같은 이중 프로세스 이론으로 바라본 두 가지 인간의 사고의 특징은 아래 <표 1>과 같다.

3. 이중 프로세스 이론(Dual Process Theory)에 따른 선행연구 검토

정보침해 경험과 정보보호 활동, 정보보호 인식을 중심으로 하는 다양한 선행연구들은 주로 보호동기이론, 건강신념이론, 자극반응이론과 같은 개인 및 조직 내 행동이론에 근거하여 경험-인식, 인식-활동, 경험-활동 간 유의성을 개별적으로 검증하고 이에 대한 시사점을 도출하는 연구나, 특정 조직 내 정보보안과 관

련된 변수들을 검증하는 연구가 주를 이루고 있다. 본 연구에서는 파편화 되어 있는 정보보호 경험, 인식, 활동 간의 관계를 이중 프로세스 이론에서 제기하고 있는 두 가지 사고 유형(System1, System2)에 근거하여 종합적으로 분석하고자 하며 이를 위해 System1, System2 경로에 따라 선행연구를 살펴보고자 한다.

1) System1: 침해경험과 정보보호 활동에 대한 선행 연구

정보침해 경험이 정보보호 활동에 끼치는 영향에 대한 선행연구는 사이버보안 공간에서의 범죄 및 일탈로 인한 피해 경험이 예방 활동에 미치는 영향, 대학 내 연구정보보호 보안에 관한 연구, 인터넷 이용자의 정보보안침해 경험이 정보보안 행동에 끼치는 영향에 대해 수행한 연구 등이 있다.

기존의 많은 연구들은 정보보호 행위에 미치는 주된 요소로서 인식을 언급하고 있으나 정보침해 경험이 정보보호 행위에 직접 미치는 영향을 분석한 연구에서는 이와 같은 인식을 거치지 않고 경험이 정보보호 행위에 직접적으로 영향을 준다는 점을 실증적으로 분석하였다. 또한 기존의 건강신념모형, 기술수용모델 등 정보보호와 관련된 연구에서 활용되는 이론들이 경험의 역할을 간과하고 있다는 점을 지적한 연구도 일부 있었다(Kim, et al., 2013; Lee, et al., 2018; Kim,

<표 1> 이중 프로세스 이론의 두 가지 사고과정
<Table 1> Two Thinking Processes in Dual Process Theory

| Thinking Process | System 1 | System 2 |
|------------------|--|---|
| Attribute | Fast High capacity Parallel Nonconscious Biased response Contextualized Automatic Associative Experience-based decision making Independent of cognitive ability | Slow Capacity limited Serial Conscious Normative response Abstract Controlled Rule-based Consequential decision making Correlated with cognitive ability |

source: (Frankish & Evans(2009); Evans & Stanovich(2013); Park, 2016 재인용).

2010; Park, et al., 2010; Chou & Wister, 2007; Mattson, 1999; Sherman, et al., 2008; Cline, et al., 2004; Rodriguez-Reimann, 2004; Rutten & Iannotti, 2003).

2) System2: 침해경험, 정보보호 인식, 정보보호 활동에 대한 선행연구

(1) 침해경험과 정보보호 인식에 대한 선행연구

경험과 인식에 대한 연구는 정보보호 분야 외에도 교육학, 심리학, 언론학 등 다양한 분야에서 이루어져 왔으나 분야의 다양성과 비교해 그 선행연구의 수는 많지 않은 편이다. 정보의 침해경험이 정보보호 인식에 어떠한 영향을 미치는지 살펴보는 연구에서는 주로 개인의 침해경험이 정보보호 중요성 인식, 정보보호정책 필요 인식, 정보보호 태도 등에 미치는 영향을 분석하고 있다(Kim, et al., 2013; Kim, et al., 2016; Lee, 2009; Lee, 2002).

개인의 보안 관련 침해경험과 정보보호 인식에 관한 연구는 주로 정보보안 관련 사고를 진·간접적으로 경험한 사람이 경험하지 않은 사람보다 상대적으로 정보보호 인식이 높은 것으로 나타났다(Choi & Chae, 2016; Kim, et al., 2016; Lee, 2009; Lee, 2002).

정보의 침해경험이 정보보호 인식에 미치는 영향 연구 외에 경험과 인식 간의 관계를 분석하는 연구로 범위를 넓혀도 개인의 침해 경험은 관련된 인식에 영향을 준다고 언급하고 있다(Kim, 2018; Koo, 2016; Kim, et al., 2016; Park, et al., 2011; Kim, et al., 2013, Hwang, 2006).

반면, 경험이 인식에 미치는 영향을 기각하는 연구도 있었다. Park, et al.(2011)은 기술수용모델, 역제이론, 통제이론을 바탕으로 기업의 정보보호 활동을 위한 조직 구성원들의 태도와 주요 영향 요인을 분석한 결과 보안과 관련된 직접적 경험 및 간접적 경험이 조직 구성원 태도에 직접적이고 긍정적 영향을 미치지

않는다는 결론을 보였다.

(2) 정보보호 인식과 정보보호 활동에 대한 선행연구

개인의 정보보호 인식이 정보보호 활동에 미치는 영향은 보호동기이론, 건강신념모델, 합리적 행동이론 등 다양한 행동이론(프레임워크)을 통해 분석되어 왔다. 정보보호 인식은 주로 프라이버시 보호 인식, 정보보안 정책 인식, 정보보호 중요성 인식 등의 세부 설문을 통해 측정되었으며 정보보호 활동은 패스워드 설정 행동, 보안제품 활용 행동, 개인정보 제공주의 행동 등의 세부 설문을 통해 측정되었다. 이와 같은 정보보호 인식이 정보보호 활동에 미치는 영향을 분석한 연구들의 결과를 살펴보면 정보보안 인식과 정보보호 활동 간 관계는 유의미한 관계를 가지고 있다는 점이 지속적으로 언급되어 왔으며, 행위이론/계획행동이론(TRA/TPB)나 기술수용모델(TAM)을 근거로 정보보안의 행동은 인지된 신념 또는 생각이 선행되어야 이루어질 수 있다고 주장한다(Kim, et al., 2011; Son, et al., 2015; Kim, et al., 2016; Park, 2015; Ha, et al., 2013; Choi, 2017; Choi & Che, 2016; Choi, S. J., et al, 2016; Choi, S. Y., et al, 2016; Choi & Kang, 2016; Lim, 2018; Lee, 2008; Layton, 2005).

3) 정보보호 인식과 정보보호 활동에 미치는 기타요인

정보보호 인식과 정보보호 활동에 미치는 기타 영향요인을 살펴보면 주로 인구사회학적요인이 주를 이루고 있다. 정보보호 인식과 정보보호 활동에 미치는 인구사회학적 요인 중 많이 언급된 요인은 성별, 연령, 최종학력, 소속, 직책, 전공, 조직 규모, 업종, 소득 등이 있다(Park, 2015; Park, et al., 2010; Choi, 2017; Park, et al., 2011, Lee, et al., 2018). 이와 같은 선행연구들을 바탕으로 본 연구에서는 정보보호 인식과 정보보호 활동에 미치는 기타 영향 요인으로 월 가구소득, 성별, 연령, 학력, 직업유무, 지역을 설정하고 이를 통제한 후 분석을 진행하고자 한다.

4. 선행연구와의 차별성

기존의 인터넷상 개인의 침해사고 경험과 정보보호 중요성 인식 및 활동에 관련한 선행연구들은 각각 경험과 인식, 인식과 활동, 경험과 활동 간의 관계와 영향력에 대해서는 다루고는 있지만 이와 같은 요인 간의 관계들을 종합적으로 다루고 있는 연구는 거의 전무한 편이다.

본 연구에서는 이와 같은 정보 침해경험과 정보보호 인식, 정보보호 활동 간의 관계를 종합적으로 분석하고 있다는 점에서 그 의의가 있으며 이와 같은 경험, 인식, 활동 간의 관계를 정보보호 분야에서 기존에 사용되지 않은 행동경제학 분야의 이중 프로세스 이론 모형을 사용하여 변수 간 관계를 분석했다는 점에서 그 의미가 있다. 또한 분석의 신뢰성 증진을 위해 한국 인터넷진흥원(KISA)의 국가승인통계 자료(2017년도 정보보호 실태조사)를 사용하여 분석을 진행하였다.

호 활동을 설정하였으며 통제변수는 기존 선행연구를 통해 산출한 요인들인 월 가구 소득, 성별, 연령, 학력, 직업유무, 지역으로 설정하였다. 본 연구에서는 개인의 침해사고 경험이 정보보호 예방활동에 미치는 영향이 이중 프로세스 이론에 따라 직관적으로 이루어지는 System1에 의해 이루어지는지 혹은 인식을 통하여 이루어지는 System2에 의해 이루어지는지 살펴보고자 한다. 이와 관련한 본 연구의 분석내용은 다음과 같다.

첫 번째, 개인의 침해사고 경험은 정보보호 활동에 어떠한 영향을 미치는지 살펴보고자 한다. 두 번째, 정보보호 인식은 개인의 침해사고 경험과 정보보호 예방활동 간 관계를 매개하는지 살펴보고자 한다. 세 번째, System1에 의한 침해사고 경험의 정보보호 예방활동에 대한 직접적 영향 방향과 System2에 의한 인식을 매개한 간접적 영향 방향은 동일한지 그리고 어느 경로의 효과가 더 큰지에 대해서 살펴보고자 한다.

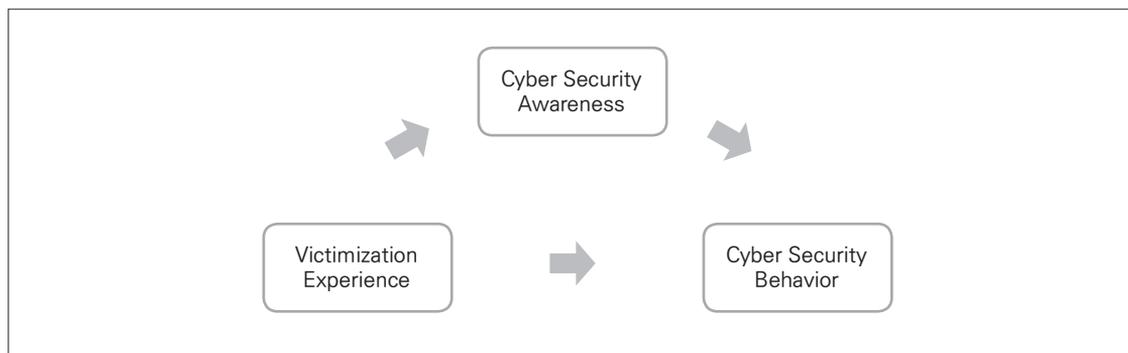
Ⅲ. 연구 분석틀 및 가설

1. 연구 분석틀

본 연구의 분석틀은 아래와 같다. 독립변수로 침해 경험, 매개변수로 정보보호 인식, 종속변수로 정보보

2. 연구문제 및 연구가설

기존의 선행연구에서 개인의 침해경험과 정보보호 인식에 대한 관계 분석, 정보보호 인식과 정보보호 활동에 대한 관계 분석, 침해경험과 정보보호 활동에 대한 관계 분석은 각각 독립적으로 연구가 진행되어 왔



〈그림 1〉 연구분석틀
 〈Fig. 1〉 Research and Analysis Framework

다. 하지만 이러한 정보 침해, 정보보호 인식, 정보보호 행동 간의 관계가 종합적으로 이어진 연구는 드물며 정보보호 외 일반적인 침해 경험, 보호 인식, 보호 행동 간 관계분석 연구로 그 범위를 확장해도 이들 간의 관계를 종합적으로 살펴본 연구는 적은 편이다.

이중 프로세스 이론은 정보 침해, 정보보호 인식, 정보보호 행동 간의 관계에 대해 그 사고의 과정을 종합적으로 고려할 수 있다. 이중 프로세스 이론에 따르면 침해 경험이 정보보호 활동에 영향을 미치는 사고의 과정은 직접적 사고방식의 System1과 인식을 거쳐 분석적으로 이루어지는 사고방식의 System2로 구성되어 있다.

그렇다면 과연 정보침해 경험에 의한 정보보호 활동은 System1에 따라 이루어지는지, 혹은 System2를 통해 이루어지는지, System1과 System2 사고절차 영향의 방향은 동일한지, 두 사고절차가 모두 이루어진다면 과연 어떠한 사고방식의 영향이 강한지에 대해서 살펴보고자 한다. 이와 같은 문제의식에 따라 본 연구는 아래와 같이 세 가지 연구문제를 제시하고 한다.

첫째, 개인의 침해사고 경험과 정보보호 예방활동 간의 관계를 분석한 연구들은 주로 피해 경험의 인지와 정보보호 활동 간의 관계를 분석하고 있다(Kim, et al., 2013; Lee, et al., 2018; Kim, 2010; Park, et al., 2010; Chou & Wister, 2007; Mattson, 1999; Sherman, et al., 2008; Cline, et al., 2004; Rodriguez-Reimann, 2004; Rutten & Iannotti, 2003). 이를 통해 얻은 연구문제는 “개인의 정보 침해 사고 경험은 정보보호 활동에 영향을 미치는가?”이다. 인간의 사고 절차 중 System1로 인한 직관적 의사결정은 정보보호 활동에 긍정적인 효과를 미칠 수 있을 것이다.

연구가설 1: 개인의 침해사고 경험은 정보보호 활동에 유의한 정(+)의 영향을 미칠 것이다.

둘째, 개인의 침해사고 경험과 정보보호 인식 간

의 관계를 분석한 연구에 따르면 기존의 많은 연구들은 주로 건강신념모델 또는 보호동기이론을 모델로 하여 개인의 침해 경험과 정보보호 인식 관계에 대한 영향을 분석하였다(Koo, 2016; Kim, et al., 2016; Lee, 2009, Park, et al., 2011; Kim, et al., 2013; Lee, 2002). 또한 정보보호 활동 영향요인에 대한 선행연구 중 정보보호 인식은 정보보호 활동에 영향을 미치는 요인 중 가장 많이 고려되는 요인 중 하나이다(Kim, et al., 2011; Son, 2015; Park, 2015; Ha, et al., 2013; Choi, et al, 2016; Choi & Che, 2016; Choi, S. J., et al., 2016; Choi, S. Y., et al, 2016; Choi & Kang, 2016; Lim, 2018; Lee, 2008; Noh, J. & Seo, J., 2016). 따라서 이와 같은 선행연구들의 경향을 통해 얻은 연구문제는 “정보보호 중요성 인식은 개인의 침해사고 경험과 정보보호 예방활동 간의 관계를 매개하는가?”이다. 인간의 사고 절차 중 System2로 인한 분석적 의사결정은 개인의 침해사고 경험이 직접적으로 정보보호 활동에 영향을 미치지 않고 정보보호 중요성 인식을 경유하여 정보보호 활동에 긍정적 효과를 미칠 수 있을 것이다.

연구가설 2: 정보보호 중요성 인식은 개인의 침해사고 경험과 정보보호 예방활동 간 관계를 매개할 것이다.

셋째, 개인의 경험이 활동에 영향을 미치는 절차에 대한 모형으로 이중 프로세스 이론(Dual Process Theory) 모형을 사용하고자 한다. 이중 프로세스 이론은 직관적 사고인 System1과 분석적 사고인 System2가 가끔 그 사고의 영향의 방향이 다를 수도 있으며 그 크기가 다를 수도 있다고 설명하고 있다(Ma, 2016; Park, 2016). 이와 같은 연구들을 바탕으로 도출한 연구문제는 “개인의 침해사고 경험이 정보보호 활동에 미치는 영향의 방향은 System1과 System2가 동일한가? 또한 System1과 System2 중 어떠한 영향 크기가 더 클 것인가?”이다. 침해로 인한

정보보호 활동은 인식을 통해서 진행되기보다 침해 인 System1이 영향의 크기가 클 것이라는 가설을 바
 에 대해 직관적 반응으로 이루어지는 System1 위주 탕으로 하고 있다.
 로 이루어져 분석적 사고인 System2에 비해 직관적

〈표 2〉 정보보호 활동 영향 변수 정리
 〈Table 2〉 Variables and Operational Definitions

| Division | Variable Name | Contents | Variable Measurement |
|----------------------|--------------------------|---|--|
| Dependent variable | Cyber Security Behavior | Password setting frequency when using PC Case 1: CMOS Login Case 2: When logging in to the operating system (Windows, etc.) Case 3: Turning off screen protection Case 4: When setting up shared files and folders Case 5: When Saving Critical Data Files Case 6: When accessing backup data | 1. No case 2. One case 3. Two cases 4. Three cases 5. Four cases 6. Five cases 7. Six cases |
| Independent variable | Victimization Experience | Victimization Experience case Case 1: Damage caused by malicious code infection Case 2: Leaking Personal Information and Invading Privacy | 1. No experience case 2. One case of damage 3. Two cases of damage |
| Mediating variable | Cyber Security Awareness | How important is it for information security? | Importance Level 1. Very low 2. Low 3. Average 4. High 5. Very high |
| Control Variable | Demographic Factor | Monthly household income | 1. Less than 2 million won 2. 2~3 million won 3. 3~4 million won 4. 4~5 million won 5. More than 5 million won |
| | | Gender | 0. male 1. female |
| | | Age | 1. 12 ~ 19 2. 20s 3. 30s 4. 40s 5. 50s |
| | | Educational Background | 0. Below high school graduation 1. College students or higher degrees |
| | | Employment | 0. Not employed 1. Employed |
| | | Region | 0. Metropolitan areas 1. Non-metropolitan areas |

- 연구가설 3-1: 침해 경험으로 인한 정보보호 활동에 있어 System2 사고절차와 System1 사고절차 영향의 방향은 같을 것이다.
- 연구가설 3-2: 침해 경험으로 인한 정보보호 활동에 있어 System2 사고절차에 비해 System1 사고절차 영향의 크기가 상대적으로 더 클 것이다.

3. 주요변수의 측정 정리

본 연구에서는 설문조사 데이터를 통해 이중 프로세스 이론에서 바라보고 있는 인간의 사고절차 중 하나로서 직관적 방식인 System1과 분석적 방식인 System2가 정보침해 경험, 정보보호 활동, 정보보호 인식 간 어떻게 작용하는지를 살펴보는데 그 목적이 있다. System1에 의하면 정보침해 경험은 정보보호의 인식 과정 없이 직접적으로 정보보호 활동에 영향을 미칠 것이며 System2에 의하면 정보침해 경험은 정보보호 인식이라는 과정을 통해 정보보호 활동에 영향을 미칠 것이다. 기존연구에서는 정보침해 경험, 정보보호 인식, 정보보호 활동 간의 단편적인 영향을 분석한 연구 위주로 진행되었으며, 이와 같은 영향들을 종합적으로 분석한 연구는 없었다. 따라서 본 연구의 독립변수, 매개변수, 종속변수, 통제변수의 구성요소 및 측정방법을 자세히 살펴보면 다음과 같다.

첫 번째 독립변수인 침해의 경험 여부는 정보침해 경험을 최근 1년간 경험 여부로 편성하고자 한다. 두 번째 종속변수인 정보보호 활동은 상황별 패스워드 설정 빈도로 편성하고자 한다. 세 번째 매개변수인 정보보호 인식은 정보보호 중요성 인식의 정도로 편성하고자 한다. 네 번째 통제변수인 인구사회학적 요인은 월 가구소득, 성별, 연령, 학력, 직업유무, 지역으로 편성하고자 한다.

본 연구에서는 1년마다 조사가 진행되는 2017년 정보보호 실태조사 데이터를 사용한다. 해당 조사의 모집단은 2017년도 8월~9월 현재 최근 1개월 이내

인터넷이용자 만12~59세 인원이며, 가구방문 면접조사를 통해 조사가 이루어졌다. 표본설계는 다단계층화 추출법(Multi-stage Stratified sampling)을 통해 이루어졌으며, 표본의 크기는 총 4,000명이다. 영향변수, 종속변수, 통제변수 모두 본 정보보호 실태조사에서 작성된 자료를 통해 도출하고자 한다.

4. 분석방법

본 연구에서는 다중회귀분석을 활용한 매개효과 검증절차로 Baron and Kenny(1986) 방식으로 매개효과를 측정한다. 이와 같은 매개효과는 다음과 같은 네 가지 조건을 만족하여야 한다. 첫째, 독립변수가 종속변수에 유의미하게 영향을 미쳐야 한다. 둘째, 독립변수는 매개변수에 유의미하게 영향을 미쳐야 한다. 셋째, 매개변수는 종속변수에 유의미하게 영향을 미쳐야 한다. 넷째, 매개변수가 통제된 상황에서 독립변수가 단독으로 종속변수에 미치는 영향에 비해 매개변수가 포함됐을 시에 독립변수의 효과가 줄어들어야 한다. 본 연구에서는 Baron and Kenny 매개회귀분석을 통해 개인의 침해사고 경험이 정보보호 인식과 정보보호 예방활동에 어떠한 영향을 미치는지에 대해 알아보고자 하며 개인의 침해사고 경험과 정보보호와 예방 활동 간 관계를 정보보호 인식이 어떻게 매개하는지 살펴보고자 한다.

IV. 분석결과

1. 기술통계

종속변수인 비밀번호(패스워드) 사례별 설정 빈도는 최소 0점에서 6점의 분포를 보이며, 평균은 1.66점이다. 비밀번호(패스워드) 사례별 설정 빈도가 6점대(6개 사례에서 비밀번호 설정)인 사람은 총 138명(3.5%)이었으며 5점대(5개 사례에서 비밀번호 설정)인 사람은 총 133명(3.3%), 4점대(4개 사례에서 비밀번호 설정)인 사람은 총 318명(8%), 3점대(3개 사례

에서 비밀번호 설정인 사람은 총 542명(13.6%), 2점대(2개 사례에서 비밀번호 설정)인 사람은 총 738명(18.5%), 1점대(1개 사례에서 비밀번호 설정)인 사람은 총 773명(19.3%), 0점대(설정하지 않음)인 사람은 총 1,358명이었다. 분석에 사용된 주요 설명변수에 대한 기술통계량은 아래 <표 3>과 같다.

2. Baron & Kenny 매개-회귀분석

이중프로세스 모형을 통해 개인의 침해경험과 정보 보호 활동 간의 관계를 침해경험과 정보보호 활동의 직접적 사고 절차로 바라보는 System1과 침해경험을 통해 정보보호 인식에 변화가 오고 이러한 변화를 통

<표 3> 주요 설명변수 및 비밀번호 설정 사례 분포
<Table 3> Key Explanatory Variables and Distribution of Password Setting Cases

| Variable Name | Variable Measurement | Frequency | Ratio(%) | Frequency of Password Setting Cases | |
|--------------------------------|------------------------------------|-----------|----------|-------------------------------------|--------------------|
| | | | | Average | Standard Deviation |
| Victimization Experience Count | No experience | 3,660 | 91.5% | 1.59 | 1.638 |
| | 1 case experience | 255 | 6.4% | 2.30 | 1.727 |
| | 2 case experience | 85 | 2.1% | 2.57 | 1.499 |
| Monthly Household Income | Less than 2 million won | 155 | 3.9% | 1.19 | 1.575 |
| | 2~3 million won | 603 | 15.1% | 1.43 | 1.537 |
| | 3~4 million won | 1298 | 32.5% | 1.60 | 1.590 |
| | 4~5 million won | 1089 | 27.2% | 1.73 | 1.683 |
| | More than 5 million won | 855 | 21.4% | 1.89 | 1.768 |
| Gender | Male | 2,038 | 50.9% | 1.83 | 1.632 |
| | Female | 1,962 | 49.1% | 1.47 | 1.659 |
| Age | 12 ~ 19 | 652 | 16.3% | 1.74 | 1.620 |
| | 20s | 782 | 19.6% | 2.14 | 1.717 |
| | 30s | 827 | 20.7% | 1.99 | 1.647 |
| | 40s | 888 | 22.2% | 1.48 | 1.603 |
| | 50s | 851 | 21.3% | 1.01 | 1.436 |
| Educational Background | Below high school graduation | 493 | 12.3% | 1.55 | 1.554 |
| | College students or higher degrees | 3,507 | 87.7% | 1.66 | 1.669 |
| Employment | Not employed | 1,577 | 39.4% | 1.55 | 1.601 |
| | Employed | 2,423 | 60.6% | 1.72 | 1.686 |
| Region | National capital region | 1,278 | 32% | 1.82 | 1.750 |
| | Non-National capital region | 2,722 | 68% | 1.58 | 1.603 |

해 정보보호 활동의 변화가 이루어지는 분석적 사고 절차로 바라보는 System2의 영향력을 각각 살펴보기 위해 Baron & Kenny 매개-회귀분석을 사용하였다. 첫 번째로 <표 4>는 개인의 침해경험이 정보보호 중요성 인식에 미치는 영향력에 관한 다중회귀분석 결과이다.

개인의 침해경험이 정보보호 활동에 직접 미치는 System1의 영향과 <표 4>의 결과와 연결하여 정보보호 인식을 통해 정보보호 활동에 간접적으로 미치는 System2의 영향을 분석한 결과는 <표 5>와 같다.

위의 분석결과를 통해 매개효과의 유의성을 살펴보기 위해서는 Baron and Kenny가 언급한 매개효과가 성립하기 위한 네 가지 조건을 살펴보아야 한다.

첫 번째, 독립변수와 종속변수 간 유의미한 영향은

β 값 0.101 P-value 값 0.001미만으로 유의미하게 분석되었다. 두 번째, 독립변수와 매개변수 간 유의미한 영향은 β 값 0.047 P-value 값 0.01미만으로 유의미하게 분석되었다. 세 번째 매개변수와 종속변수 간 유의미한 영향은 β 값 0.062 P-value 값 0.001미만으로 유의미하게 분석되었다. 마지막으로 네 번째 매개변수가 통제된 상황에서 독립변수가 단독으로 종속변수에 미치는 β 값인 0.104에 비해 매개변수가 포함됐을 시에 β 값이 0.101로 줄어들었다.

이와 같은 분석결과로 보건대, 정보보호 인식은 개인의 침해 경험과 정보보호 활동을 유의미하게 매개하는 것으로 볼 수 있으며, 동시에 이러한 효과는 매개변수를 거치지 않고도 직접적으로 정보보호 행동에 유의한 영향을 미치는 간접매개 효과라는 것을 확인할 수

<표 4> 개인의 침해경험이 정보보호 중요성 인식에 미치는 영향력에 관한 다중회귀분석 결과

<Table 4> Multiple Regression Analysis Results on the Impact of Victimization Experience on Cyber Security Awareness

| Division | | Cyber Security Awareness | | | |
|----------------------|--|--------------------------|----------|-----------|----------|
| | | Model 1 | | Model 2 | |
| | | b | β | b | β |
| Control Variable | Employment (Reference Group: Not employed) | .086*** | .069*** | .087*** | .069*** |
| | Gender(Reference Group: Male) | .016 | .013 | .019 | .016 |
| | Age | -.036*** | -.080*** | -.034*** | -.076*** |
| | Monthly Household Income | .051*** | .092*** | .053*** | .094*** |
| | Educational Background | .097* | .052* | .090* | .048* |
| | Region(Reference Group: National capital region) | .082*** | .062*** | .090 | .068 |
| Independent Variable | Victimization Experience | | | .078** | .047** |
| Constant | | 100.998*** | | 99.706*** | |
| R^2 | | .018 | | .021 | |
| Adjusted R^2 | | .017 | | .019 | |
| F | | 12.514*** | | 12.006*** | |

* p<0.05 ** p<0.01 *** p<0.001

Dependent Variable : Cyber Security Awareness

〈표 5〉 정보보호 중요성 인식의 매개효과에 관한 다중회귀분석 결과
 (Table 5) Multiple Regression Analysis Results on the Mediating Effect of Cyber Security Awareness

| Division | | Cyber Security Behavior | | | | | |
|----------------------|--|-------------------------|----------|------------|----------|------------|----------|
| | | Model 1 | | Model 2 | | Model 3 | |
| | | b | β | b | β | b | β |
| Control Variable | Employment(Reference Group: Not employed) | .287*** | .085*** | .289*** | .085*** | .274*** | .081*** |
| | Gender (Reference Group: Male) | -.280*** | -.085*** | -.261*** | -.079*** | -.264*** | -.080*** |
| | Age | -.382*** | -.319*** | -.372*** | -.310*** | -.366*** | -.305*** |
| | Monthly Household Income | .122*** | .081*** | .129*** | .086*** | .121*** | .080*** |
| | Educational Background | .816*** | .162*** | .770*** | .153*** | .755*** | .150*** |
| | Region(Reference Group: National capital region) | -.157** | -.044** | -.108* | -.030* | -.123* | -.035* |
| Independent Variable | Victimization Experience | | | .465*** | .104*** | .452*** | .101*** |
| Mediating Variable | Cyber Security Awareness | | | | | .166*** | .062*** |
| Constant | | 17.577*** | | 16.556*** | | 5.444*** | |
| R^2 | | .090 | | .101 | | .104 | |
| Adjusted R^2 | | .089 | | .099 | | .103 | |
| F | | 65.900*** | | 63.8206*** | | 58.1286*** | |

* p<0.05 ** p<0.01 *** p<0.001

Dependent Variable : Cyber Security Behavior

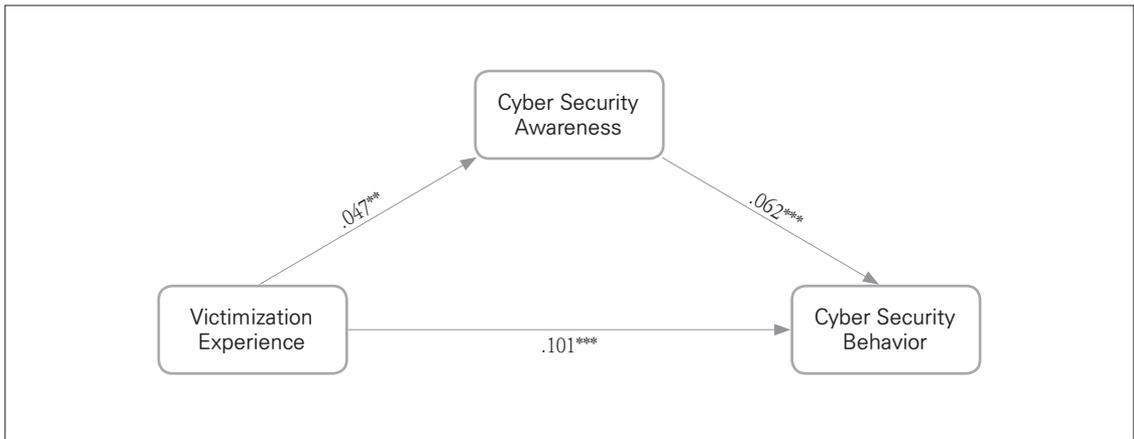
있다. 본 연구 모형에서 인과적 과정을 표준화 계수를 반영하여 그림으로 도해하면 〈그림 2〉와 같다.

본 연구는 PC 사용과 관련하여 개인의 침해 사고 경험이 향후 정보보호 활동에 미치는 영향에 대해서 분석하되, 행동경제학의 이중 프로세스 이론(Dual Process Theory)를 통해서 System1의 직접적 사고 방식, System2의 간접적 사고방식의 효과를 분해하여 분석하고 그 상대적 크기를 알아보는데 그 목적을 두고 있다. 〈그림 2〉에서 보듯이 개인의 침해 사고 경험은 매개변수인 정보보호 중요성 인식을 통하여 간접적으로 정보보호 활동에 영향을 미치는데, System1의

직접적 사고절차와 System2의 간접적 사고절차로 분해하면 다음 〈표 6〉과 같다. 첫 번째로 개인의 침해 경험이 매개변수인 정보보호의 중요성 인식을 통하여 간접적으로 정보보호 활동에 영향을 미치는 System2의 간접효과는 0.0029이다. 두 번째로 개인의 침해 경험이 매개변수를 거치지 않고 정보보호 활동에 직접 영향을 미치는 System1의 직접 효과는 0.101이다. 이 System1의 직접효과와 System2의 간접효과를 비교하면 직접효과(0.101)은 간접효과(0.0029) 보다 더 크다. 이로써 개인의 System1에 의한 직접효과가 가지는 상대적 비중이 간접 효과가 가지고 있는 상대적

〈표 6〉 개인의 침해 경험의 정보보호 행동에 대한 직접 및 간접 효과
 〈Table 6〉 Direct and Indirect Effect of Victimization Experience on Cyber Security Behavior

| Independent Variable | Direct Effect | Indirect Effect | | Dependent Variable |
|--------------------------|---------------|--------------------------|--------|-------------------------|
| | Size | Mediating Variable | Size | |
| Victimization Experience | .101 | Cyber Security Awareness | 0.0029 | Cyber Security Behavior |



***p<0.001, **p<0.01

〈그림 2〉 정보보호 중요성 인식의 매개모형 검증결과: 표준화 계수
 〈Fig. 2〉 Result of Mediating Model Test on Cyber Security Awareness; Standardized Regression Coefficient

비중에 비해 더 크므로 이를 연구문제3에 대한 답으로 삼을 수 있다.

3. 가설검증

측정모형을 검증한 다음, 본 연구에서 제시한 3가지의 가설검증을 실시하였다. 먼저 가설1, 가설2, 가설3의 검증은 Baron & Kenny의 매개회귀분석의 결과를 통해 각 가설에 대한 통계적 지지여부를 검증하였다.

분석결과 첫 번째, 이중 프로세스 이론(Dual Process Theory) 중 개인의 침해사고 경험이 정보보호 활동에 직접적으로 영향을 미치는 직접적 사고방식인 System1에 의해 미치는 효과가 정(+)의 영향일 것이라는 가설 1은 분석결과 베타 값이 0.101 p-value 값이 0.001

보다 작아 가설이 채택되었다.

두 번째, 이중 프로세스 이론(Dual Process Theory) 경로 중 System2에 의해 정보보호 인식이 개인의 침해사고 경험과 정보보호 활동 간의 관계를 매개할 것이라는 가설2는 분석결과 개인침해 경험과 정보보호 인식, 정보보호 인식과 정보보호 행동의 p-value 값이 각각 0.01, 0.001보다 작고 간접효과 값이 0.0029로 분석되어 가설이 채택되었다.

세 번째, 이중 프로세스 이론(Dual Process Theory) 경로 중 System1의 정보보호 활동에 대한 효과 방향과 System2의 효과 방향은 같을 것이라는 가설3-1과 System1, System2 사고방식 절차 중 직접적인 사고절차인 System1의 효과가 클 것이라는 가설 3-2는 직접효과 0.101, 정보보호 인식을 통한 간접효과

〈표 7〉 연구가설 검증표
 〈Table 7〉 Hypothesis Test Results

| Division | Contents | Adoption |
|----------------|---|-----------|
| Hypothesis 1 | Individuals' Victimization Experience will have a positive (+) effect on Cyber Security Behavior. | Supported |
| Hypothesis 2 | Cyber Security Awareness will mediate the relationship between Victimization Experience and Cyber Security Behavior. | Supported |
| Hypothesis 3-1 | Regarding Cyber Security Behavior, System 1 thinking process and System 2 thinking process will have the same direction of impacts. | Supported |
| Hypothesis 3-2 | System 1 thinking process impact will be relatively larger than System 2 thinking process impact. | Supported |

0.0029로 직접효과가 간접효과에 비해 더 큰 것으로 나타나 가설이 채택되었다. 해당사항을 〈표 7〉과 같이 정리하였다.

V. 결론

서론에서도 언급한 바와 같이 4차 산업혁명 시대의 도래에 따라 빅데이터 활용, IoT, 인공지능 등 새로운 기술이 급속히 발전하면서 정보보호의 중요성은 날이 더 커져가고 있다. 이에 따라 개인의 정보보호 활동을 증진시키기 위한 정부의 정책적 역할도 구체적으로 제시되어야 할 것이다.

본 연구에서는 이와 같은 개인의 침해 경험, 정보보호 인식, 정보보호 활동 간의 관계를 분석하고 해당 관계 분석을 통해 정부가 정책적으로 정보보호 활동을 증진 시킬 수 있는 방안에 대해 제안하고자 하였다. 연구결과 이중 프로세스 이론 모델 중 직관적인 사고인 System1을 통한 정보보호 활동이 상대적으로 강한 것을 확인하였으며, 이와 함께 System2도 작용하고 있는 것을 살펴 볼 수 있었다. 개인의 주된 정보보호 활동이 직관적 사고를 통해 이루어지지만 정보보호 중요성 인식을 통한 분석적 사고를 통해서도 정보보호 활동에 미치는 것으로 분석되었다. 이와 같은 분석 결과를 보았을 때 정부는 정보보호 활동을 증진시키기

위해 어떠한 노력을 진행하여야 할까? System1을 통한 정보보호 활동 증진은 그 영향력이 클 수 있겠지만 침해 사고를 경험한 후 행동하는 사후적 대응방안이라고 볼 수 있다. 하지만 최근 침해 사고가 발생했을 시에는 그 피해의 범위와 정도가 큰 경우 많아 이와 같은 사후적 대응방안에 비해 예방적 활동이 중요하다. 이중프로세스 이론에서는 이와 같은 System1의 직관적 사고도 System2의 인식적 사고를 지속적으로 반복하여 체득되었을 때 동일하게 이루어질 수 있다고 언급한다. 따라서 지속적 정보보호 교육 또는 정보보호 인식 제고 캠페인을 통해 정보보호에 대한 직관적 사고를 할 수 있도록 체득시켜 주는 정책적 노력이 필요하다(Um, M. & Kim, M., 2007). 이를 위한 정보보호 교육은 교육 대상자들에게 단순 지식을 일시적으로 전달하는 방식의 교육이 아니라 주기적이면서도 다양한 침해 사례를 경험, 학습할 수 있도록 하여야 한다. 정기적인 정보보호 교육을 실시하고 새롭게 생겨나는 위협에 대해서 지속적으로 인지시켜주며 교육 및 캠페인에서 전달한 위협 및 준수사항에 대해 모의 위협 상황을 만들어 줌으로써 교육대상자들의 정보보호에 대해 직관적 사고를 체득할 수 있도록 도와주어야 한다.

이상 개인의 침해경험이 정보보호 활동에 어떠한 절차를 통해 영향을 미치는지 이중 프로세스 이론을 통해 분석하고 정보보호 활동을 증진시키기 위한 정책적

방향에 대해서 이론적 고찰을 해보았다. 이와 같은 논의를 통해 추후 정부 및 관련 전문기관이 정보보호 활동 증진을 위한 정책(프로그램) 기획 및 집행 방향 설정을 함에 있어 학문적 시사점을 줄 수 있을 것이라 예상된다. 다만 본 연구를 진행함에 있어 가지고 있는 한계점은 연구의 분석 데이터로 2차 데이터를 사용함에 따라 매개변수를 한 가지 설문문항으로 측정하여 신뢰성 있는 설문 항목을 사용하지 못했다는 점과 정보보호 활동 증진을 위한 핵심적인 요소로 정보보호 교육, 캠페인을 제시하고 있으나 정보보호 예방 활동에 대한 해당 변수의 영향을 실증적으로 분석하지 못했다는 점에 있다. 따라서 향후에는 본 연구 정책적 제언에서 언급한 내용을 실증적으로 분석하기 위해 '정보보호 교육 및 캠페인이 정보보호 활동에 미치는 영향은 어떠한가?', '해당 교육 및 캠페인의 시행 빈도에 따라 정보보호 활동에 미치는 영향은 어떻게 달라지는가?'에 대한 연구물음을 가지고 후속연구가 이루어지길 기대해 본다.

References

- Ahlan, A. R., Lubis, M. & Lubis, A. R. (2015). "Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures." *Procedia Computer Science*, 72, 361-373.
- Bae, J. (2016). "An Empirical Study on the Effect of Leakage Threat of Personal Information on Protective Behavior Intention in Big Data Environment: Based on Health Psychology Theory and Protection Motivation Theory." *The e-Business Studies*, 17(3), 191-208.
- {배재권 (2016). 빅데이터 환경에서 개인정보유출 위협이 정보보호 행위에 미치는 영향에 관한 연구. <e-비즈니스연구>, 17권 3호, 191-208.}
- Baron, R. M. & Kenny, D. A. (1986). "The moderator - mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations." *Journal of Personality and Social Psychology*, 51(6), 1173-1182.
- Choi, J. (2015). "An Empirical Study on the Relationship of Personal Optimistic Bias and Information Security Awareness and Behavior in the Activity of Information Ethic." Master's Thesis, Department of Management Information Systems, Seoul Venture University.
- {최종근 (2015). <정보윤리 활동에서 개인의 낙관적 편견과 정보보안 인식 및 정보보안 행위와의 관련성에 관한 실증연구>. 서울벤처대학원대학교 박사학위 논문.}
- Choi, J. & Che, M. (2016). "An empirical study on the relationship of personal optimistic bias and information security awareness and behavior in the activity of information ethics." *Journal of the Korea Academia-Industrial*, 17(5), 538~547.
- {최종근·채명신 (2016). 정보윤리 활동에서 개인의 낙관적 편견과 정보보안 인식 및 정보보안 행위와의 관련성에 관한 실증 연구. <한국산학기술학회논문지>, 17권 5호, 538-547.}
- Choi, M. (2017). "A study on the Influence of the Work Environment Characteristics of Coworking office on Information Security Awareness and Behavior." Master's Thesis, Department of Financial Information Security, Kookmin University.
- {최민혜 (2017). <코워킹 오피스 근무환경 특성이 개인의 정보보안인식 및 행동에 미치는 영향에 대한 연구>. 국민대학교 석사학위 논문.}
- Choi, N., Kim, D. J., Goo, J. & Whitmore, A. (2008). "Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action." *Information Management & Computer Security*, 16(5), 484-501.
- Choi, S., Kim, H. & Kim, T. (2016). "Factors Affecting Information Security Practice of Elementary School Students." *Journal of the Korea Institute of Information Security & Cryptology*, 26(2), 449-461.
- {최승재·김형열·김태성 (2016). "초등학생들의 정보보호실천에 영향을 미치는 요인." <정보보호학회논문지>, 26권 2호, 449-461.}
- Choi, S., Lim, D., Ko, I. & Moon, I. (2016). "Perception and Performance about Patients' Medical Information Protection in Allied Health College

- Students.” *The Journal of Korean Academic Society of Nursing Education*, 22(1), 83-95.
- {최선영·임도연·고일선·문인오 (2016). 보건계열 대학생의 환자 의료 정보 보호에 대한 인식과 수행. <한국간호교육학회지>, 22권 1호, 83-95.}
- Choi, Y. & Kang, H. (2016). “A Study on Dental Hygienist’ Knowledge, Awareness and Performance of Patient’s Personal Information Protection.” *Journal of the Korea Academia-Industrial cooperation Society*, 17(2), 416-426.
- {최예진·강현경 (2016). 환자 개인정보보호에 관한 치과위생사의 지식과 인식도 및 실천도에 관한 연구. <한국산학기술학회 논문지>, 17권 2호, 416-426.}
- Chou, P. H. B. & Wister, A. V. (2007). “From Cues to Action: Information Seeking and Exercise Self-care among Older Adults Managing Chronic Illness.” *Canadian Journal on Aging*, 24(4), 395-408.
- Cline, R. R., Farley, J. F., Hansen, R. A. & Schommer, J. C. (2004). “Osteoporosis Beliefs and Antiresorptive Medication Use.” 50, 196-208.
- Ha, S. & Kim, H. (2013). “The Effects of User’s Security Awareness on Password Security Behavior.” *Journal of Digital Contents Society*, 14(2), 179-189.
- {하상원·김형중 (2013). 정보보안의식이 패스워드 보안행동에 미치는 영향에 관한 연구. <한국디지털콘텐츠학회 논문지>, 14권 2호, 179-189.}
- Hwang, E. (2006). “The Mediating Effects of Self-Conscious Affects on Depression and Anxiety in Children’s Abusive Experience.” Master’s Thesis, Department of Child Welfare and Studies, Sookmyung Women’s University.
- {황은수 (2006). <아동의 학대경험이 우울과 불안에 영향을 미치는 자기인식정서의 매개효과>. 숙명여자대학교 석사학위 논문.}
- Jang, I. & Choi, B. (2014). “Analyzing the Privacy Leakage Prevention Behavior of Internet Users Based on Risk Perception and Efficacy Beliefs : Using Risk Perception Attitude Framework.” *The Journal of Society for e-Business Studies*, 19(3), 65-89.
- {장익진·최병구 (2014). 위험지각과 효능감에 따른 인터넷 사용자의 개인정보 유출 예방행위 분석 - 위험지각태고 프레임워크를 기반으로. <한국전자거래학회지>, 19권 3호, 65-89.}
- Jeon, J. (2018). “Analysis of motivational and psychological factors affecting information security perception of employees.” Master’s Thesis, Department of Security Convergence, Chung-AngUniversity.
- {전재찬 (2018). <조직 구성원의 정보보안인식에 영향을 미치는 동기 및 심리적인 요인 분석>. 중앙대학교 석사학위 논문.}
- Joung, Y. (2013). “Seeking for Component Parts of Information Security’s Legal Concept :Based on Analysis of Cases about Information Security.” *Public Law Journal*, 14(4), 209-243.
- {정연부 (2013). 정보보안 침해 사건 분석에 기초한 정보보안의 법적 개념 요소 도출. <공법학연구>, 14권 4호, 209-243.}
- Kim, H., Jeon, E. & Kim, S. (2016). “An Empirical Study of People’s Perceptions and Attitudes Toward Personal Information Disclosure Online : Focusing on ‘Psychological Reactance’ in the Big Data Age.” *Korean Journal of Communication & Information*, 80, 143-166.
- {김형지·전은식·김성태 (2016). 온라인상의 개인정보 노출에 대한 인식과 보호 태도 연구- 빅데이터 시대 개인정보 노출에 대한 심리적 반발에 주목하며. <한국언론정보학보>, 80호, 143-166.}
- Kim, J. (2010). “The Effects of victimized Experiences as Internal Cues to Action on Preventive Behavioral Intentions in Cyber Communication: Modifying Health Belief Model.” *Journal of Cybercommunication Academic Society*, 27(3), 5-46.
- {김준홍 (2010). 사이버 커뮤니케이션에서 행위단서로서 범 죄피해 경험이 피해 예방행동 의도에 미치는 영향 - 수정된 건강신념모형을 중심으로. <사이버커뮤니케이션학보>, 27권 3호, 5-46.}
- Kim, J. & Kang, D. (2008). “The Effects of Security Policies, Security Awareness and Individual Characteristics on Password Security Effectiveness.” *Journal of the Korea Institute of Information Security & Cryptology*, 18(4), 123-133.
- {김종기·강다연 (2008). 보안정책, 보안의식, 개인적 특성이

- 패스워드 보안효과에 미치는 영향. <정보보호학회논문지>, 18권 4호, 123-133.}
- Kim, J. & Lim, S. (2016). "A Preliminary Research on the Impact of Perception of Personal Information Leakage Incidents on the Behavior of Individual Information Management in the Mobile Banking Contexts." *Journal of the Korea Institute of Information Security & Cryptology*, 26(3), 735-744.
- {김정덕·임세현 (2016). 모바일 뱅킹 이용자의 개인정보 유출사고 인지가 개인정보관리 준수행동에 미치는 영향에 대한 사전 연구. <정보보호학회논문지>, 26권 3호, 735-744.}
- Kim, S. & Park, H. (2013). "An Analysis of Influence Factors on Privacy Protection Awareness and Protection Behavior and moderating Effect of Privacy Invasion Experience." *The Journal of Internet Electronic Commerce Research*, 13(4), 79-105.
- {김상현·박현선 (2013). 프라이버시 보호인식 및 보호행동의 도에 미치는 영향 요인과 프라이버시 침해경험의 조절효과에 관한 연구. <인터넷전자상거래연구>, 13권 4호, 79-105.}
- Kim, Y. (2018). "The Effects of Trust in Government, Disaster Experience, and Social Capital on Disaster Risk Perception: Focusing on Disaster Victims in Local Areas." Ph.D. Thesis, Department of Public Administration, Yonsei University.
- {김영주 (2018). <정부신뢰, 재난경험, 사회적 자본이 재난 위험인식에 미치는 영향-지역의 재난 피해자를 중심으로>. 연세대학교 박사학위 논문.}
- Koo, J. (2016). "Effects of Primary School Students' Human Rights Related Experience on Their Human Rights Awareness." *Theory and Research in Citizenship Education*, 48(3), 1-25.
- {구정화 (2016). 일상의 인권경험이 초등학생의 인권인식에 미치는 영향. <시민교육연구>, 48권 3호, 1-25.}
- Korea Internet & Security Agency (2018). *2017 Survey on Information security(Individual)*. Korea Internet & Security Agency.
- {한국인터넷진흥원 (2018). <2017년 정보보호실태조사 개인부문>. 한국인터넷진흥원.}
- Jang, I. & Choi, B. (2014). "Analyzing the Privacy Leakage Prevention Behavior of Internet Users Based on Risk Perception and Efficacy Beliefs : Using Risk Perception Attitude Framework." *The Journal of Society for e-Business Studies*, 19(3), 65-89.
- {장익진·최병구 (2014). 위험지각과 효능감에 따른 인터넷 사용자의 개인정보 유출 예방행위 분석 - 위험지각태고 프레임워크를 기반으로. <한국전자거래학회지>, 19권 3호, 65-89.}
- Jeon, J. (2018). "Analysis of motivational and psychological factors affecting information security perception of employees." Master's Thesis, Department of Security Convergence, Chung-Ang University.
- {전재찬 (2018). <조직 구성원의 정보보안인식에 영향을 미치는 동기 및 심리적인 요인 분석>. 중앙대학교 석사학위 논문.}
- Joung, Y. (2013). "Seeking for Component Parts of Information Security's Legal Concept :Based on Analysis of Cases about Information Security." *Public Law Journal*, 14(4), 209-243.
- {정연부 (2013). 정보보안 침해 사건 분석에 기초한 정보보안의 법적 개념 요소 도출. <공법학연구>, 14권 4호, 209-243.}
- Lebek, B., Uffen, J., Neumann, M., Hohler, B. & H. Breitner, M. (2014). "Information security awareness and behavior: a theory-based literature review." *Management Research Review*, 37(12), 1049-1092.
- Lee, H., Kho, H. Roh, E. & Han, K. (2018). "A Study on the Factors of Experience and Habit on Information Security Behavior of New Services-based on PMT and UTAUT2." *Journal of Digital Contents Society*, 19(1), 93-102.
- {이흥제·고형석·노은희·한경석 (2018). 경험 및 습관이 신규 서비스의 정보보호 행동에 미치는 요인에 대한 연구-보호동기이론과 UTAUT2을 중심으로. <한국디지털콘텐츠학회지논문지>, 19권 1호, 93-102.}
- Lee, M. (2002). "Articles: The Reactions to Cybercrime victimized: Testing a Generic Model." *Korean Journal of Victimology*, 10(2), 209-247.
- {이민식 (2002). 사이버 범죄 피해에 대한 반응: 일반모델의 검증. <피해자학연구>, 10권 2호, 207-247.}

- Lee, S. & Park, C. (2014) "A study of the User Privacy Protection Behavior in Online Environment: Based on Protection Motivation Theory." *Journal of Internet Computing and Services(JICS)*, 15(2), 59-71.
- {이상우·박찬욱 (2014). 인터넷상에서의 개인정보 보호행동에 관한 연구: 보호동기이론을 중심으로. <인터넷정보학회논문지>, 15권 2호, 59-71.}.
- Lee, T., Youn, Y. & Kim, H. (2016). "The Analysis of Information Security Awareness Using A Text Mining Approach." *Informatization policy*, 23(4), 76-94.
- {이태현·윤영주·김희웅 (2016). 텍스트 마이닝을 이용한 정보보호인식 분석 및 강화 방안 모색. <정보화정책>, 23권 4호, 76-94.}.
- Lee, Y. (2009). "A Study on Factors Influencing the Preventive Efforts toward Personal Information Privacy." Master's Thesis, Department of Business & Information Education, Sungkyunkwan University.
- {이윤선 (2009). <개인정보보호 예방활동의 영향요인 연구: 고등학생을 중심으로>. 성균관대학교 석사학위 논문.}.
- Lim, J. & Kwon, S. (2018). "An Experimental Study on the Effects of Risk Cognition of Personal Information and Self-Expression Information on Conation of Privacy Protection." *Journal of the Korea Institute of Information Security & Cryptology*, 28(3), 681-694.
- {임정호·권순동 (2018). SNS의 개인정보와 자기표현정보의 중요도 인지가 정보보호 행동의지에 미치는 영향에 관한 실험연구. <정보보호학회논문지>, 28권 3호, 681-694.}.
- Mattson, M. (1999). "Toward a Reconceptualization of Communication Cues to Action in the Health Belief Model: HIV Test Counseling." *Communication Monographs*, 66, 240-265.
- Mha, J. (2016). "Are consumers Really Reasonable Beings?: A Theoretical Approach of Applying Behavioral Economics to Advertising Researches." *Advertising Research*, 111, 101-131.
- {마정미 (2016). 소비자: 합리적인 존재인가: 행동경제학의 광고학 적용을 위한 개념적 연구. <광고연구>, 111호, 101-131.}.
- Moon, K. & Kim, S. (2017). "Relationship between Information Security Activities of Enterprise and Its Infringement : Mainly on the Effects of Information Security Awareness." *Journal of the Korea Institute of Information Security & Cryptology*, 27(4), 897-912.
- {문건웅·김승주 (2017). 기업의 정보보호 활동과 정보침해 사고 간의 관계 - 정보보호 인식의 매개효과를 중심으로. <정보보호학회논문지>, 27권 4호, 897-912.}.
- Noh, J. & Seo, J. (2016). "Information Security and Its Awareness in Local Governments." *Informatization policy*, 23(1), 20-37.
- {노재인·서진원 (2016). 지방자치단체의 정보보호 현황 및 인식의 변화 분석. <정보화정책>, 23권 1호, 20-37.}.
- Park, G. (2015). "A Study on the Determinants of the Internet Privacy Protection Behavior: Focused on the Net Users' Characteristics." Ph. D. Thesis, Department of Public Administration, Hanyang University.
- {박건우 (2015). <인터넷 개인정보 보호행동의 결정요인: 이용자의 특성을 중심으로>. 한양대학교 석사학위 논문.}.
- Park, I. Kim, S. & Seo, S. (2010). "Improving Research Information Security in Academic Institutes through the Analysis of Security Awareness and Activities." *Journal of the Korea Institute of Information Security & Cryptology*, 20(2), 91-108.
- {박일형·김성우·서승우 (2010). 보안 인지 및 실천 현황 분석을 통한 대학 연구정보보안 수준 제고 방안. <정보보호학회논문지>, 20권 2호, 91-108.}.
- Park, J., Kim, B. & Cho, S. (2011). "Primary Factors Affecting Corporate Employees' Attitudes Toward Information Security." *korean management review*, 40(4), 955-985.
- {박준경·김범수·조성우 (2011). 기업정보보호 활동을 위한 조직 구성원들의 태도와 주요 영향 요인. <경영학연구>, 40권 4호, 955-985.}.
- Park, Y. (2016). "A Dual-process Theoretical Interpretation of Decision making under Uncertainty." Ph. D. Thesis, Department of Psychology, Ajou University.

- {박영준 (2016). <불확실성 하의 의사결정 연구에 대한 이중 처리 이론적 해석>. 아주대학교 박사학위 논문.}.
- Pharm, H., Brennan, L. & Richardson, J. (2017) "Review of behavioral theories in security compliance and research challenges." *Proceedings of the Informing Science + Information Technology Education conference*, 65-76.
- Rodriguez-Reimann, cNicassio P, Reimann JO, Gallegos PI, Olmedo EL. (2004). "Acculturation and health beliefs of Mexican Americans regarding tuberculosis prevention." *J Immigr Health*, 6(2), 51-62.
- Rutten, L. J. F. & Iannotti, R. J. (2004). "Health Beliefs, Salience of Breast Cancer Family History, and Involvement with Breast Cancer Issues: Adherences to Annual Mammography Screening Recommendations." *Cancer Detection and Prevention*, 27, 353-359.
- Sherman, A. C., Pennington, J., Simonton, S., Latif, U., Arent, L. & Farley H. (2008). "Determinants of Participation in Cancer Support Groups: The Role of Health Beliefs." *International Journal of Behavioral Medicine*, 15, 92-100.
- Son, Y. (2015). "A Study on the Relationship between Cognition of personal information protection and Following protection Activities." Master's Thesis, Department of Security Management, Sangmyung University.
- {손영수 (2015). <개인정보보호 인지와 정보보호 활동에 대한 연구: 앤더슨의 행동모형을 기반으로>. 상명대학교 석사학위 논문.}.
- Um, M. & Kim, M. (2007). An Exploratory Study on Factors affecting Efforts for Information Protection in Cyber space. *Informatization policy*, 14(1), 125-143.
- {엄명용·김미량 (2007). 사이버공간에서 정보보호 예방활동에 영향을 미치는 요인에 관한 탐색적 연구. <정보화정책>, 14권 1호, 125-143.}.