https://doi.org/10.32431/kace.2020.23.1.006

보안정책에 대한 편향적 사고가 보안준수 행동에 미치는 영향

허준† · 안성진††

요 약

보안사고 예방을 위한 많은 노력에도 불구하고 조직구성원의 보안행동과 연관된 정보유출, 랜섬웨어 등 치명적 보안사고 피해는 해마다 늘어나고 있다. 이 연구에서는 보안사고의 주요한 원인인 조직원의 보안정책 준수의 관점에서, 보안정책 준수에 영향을 주는 요인으로 편향적 사고를 제시하고 다음을 검증하였다. 첫째, 보안정책에 대한 편향적사고가 보안정책준수 태도에 주는 영향을 검증한다. 둘째, 경영진의 참여, 지각된 위험성, 교육 및 처벌이 편향적 사고를 증가 또는 감소시키는 조절 효과를 검증한다. 마지막으로, 보안정책준수 태도가 준수행동에 유의미한 영향을 주는 지 검증하였다. 이를 위해 157명을 대상으로 설문조사를 실시하고 연구모형 및 구조방정식 통계적 분석, 적합성 분석을 실시하였다. 연구결과 편향적 사고는 정보보안 정책준수 태도에 부정적 영향을 주는 것으로 나타났다. 또한 정보보안 정책준수 태도는 정책준수 행동을 증가시키는 것으로 분석되었다. 한편, 조직원 개인이 정보보안에 대한 위험성을 높게 지각할수록 편향적 사고를 감소시키는 조절효과가 있었으나, 경영진의 참여, 교육 및 처벌은 조절효과가 없는 것으로 나타났다. 향후, 연구결과는 내부조직원에 의한 보안사고 대처방안에 시사점을 줄 것으로 기대된다.

주제어 : 편향적 사고, 정보보안 정책준수, 경영진 참여, 보안교육, 처벌

Effects of Biased Awareness of Security Policies on Security Compliance Behavior

Jun Heo† · Seongjin Ahn††

ABSTRACT

From the perspective of compliance with security policies by members of the organization, which is a major cause of security incidents, this study presented biased thinking as factors that affect compliance with security policies and verified the following: First, the impact of biased thinking on security policies on compliance with security policies is verified. Second, the participation of management, perceived risk, education and punishment of management will verify the adjustment effect of increasing or decreasing biased thinking. Finally, we have verified that compliance attitudes have a significant impact on compliance behavior. To this end, 157 people were surveyed, statistical analysis of research models and structural equations, and conformity analysis were conducted. Studies have shown that biased thinking has a negative effect on the attitude of compliance with information security. In addition, it was analyzed that the attitude of compliance with information security policy increases policy compliance behavior. On the other hand, the higher the perceived risk of information security, the lower the bias was the adjustment effect, but management's participation, education and punishment were found to have no adjustment effect.

Keywords : Biased thinking, Security policy, CEO, Security education, Punishment

†정 회 원: 성균관대학교 교과교육학과 컴퓨터교육 전공 박사수료
††종신회원: 성균관대학교 컴퓨터교육학과 교수(교신저자)
논문접수: 2019년 11월 17일, 심사완료: 2019년 12월 19일, 게재확정: 2019년 12월 24일

1. 서론

정보보호체계인증, 취약점 진단, 모의해킹 등 많은 기업들의 보안위협 제거를 위한 노력에도 불구하고, 비교적 정보보안수준이 높은 대기업, 금융업 등에서도 정보보안 사고는 끊임없이 발생하고 있다. 특히, 심각한 정보유출 사고 5건 중 1건은 부주의한 내부직원에 의해 발생하고, 기업의 42%는 가장 큰 기밀정보 유출이 직원에 의해 발생하며, 피해액도 중소기업의 경우 평균 9,313만원, 대기업 9억 5,934만원에 달하고 있다[1]. 또한 실제 침해사고 중 내부자(34%), 협력업체(2%)가 직접 연루되어 있으며, 내부자가 의도하지 않았더라도 내부직원의 부주의를 악용하는 사회공학 공격이 33%, 인증된 사용자의 잘못된 사용 15%, 악성코드 감염 28%로 나타나는 등 간접적으로도 내부자의 행위가 원인되는 침해사고도 66%에 이르고 있으며, 보안사고 중 71%는 금전적인 동기에서 발생하고 있다[2].

조직에서 정보보안 정책, 기술 등에 투자와 관심이 높아지면 관리와 통제가 용이해지지만 조직원은 추가적인 보안요구사항에 심리적인 저항을 느끼게 된다[3]. 정보보안 정책 준수에 스트레스를 느끼는 정도가 높아지면 조직원의 정보보안 준수의도가 낮아지게 된다[4]. 조직원들은 정보보안 정책준수 행동에 따르는 추가적인 요구사항, 기존 업무패턴과의 충돌, 단기적 편리성 추구, 단기적 금전적인 이익 등 다양한 원인으로 정보보안 정책준수에 비이성적이며, 감정적인 편향적 사고를 보이고 이는 정보보안 정책준수 태도 및 행동에 영향을 줄 수 있으며 보안사고의 위험을 높인다. 사회심리학자 카너먼은 ‘우리는 살아가면서 수많은 상황에서 지적인 능력을 통해 합리적·이성적 사고를 하고 문제를 해결할 수 있는 존재라고 믿어 왔으나 인간의 이성은 탈 합리적이다’ 라고 하였다. 진화론적으로는 인간은 생존을 위해 인지처리과정이 느린 이성적사고 보다는 인지처리과정이 빠른 직관과 감성에 기대어 생각하고 판단할 때가 많다[5]. 즉 직관은 별다른 노력이 필요 없지만 이성은 별도의 노력과 논리 같은 형식이 필요하다[6]. 생존을 위해 주변 환경을 더 빨리 이해하고 예측하고 설명할 수 있었던 이러한 능력이 인간은 동물의 수준을 넘어서 수준 높은 삶을 가능하게 하였으나 그에 따른 부정적인 효과도 많이 생기게 되었고, 합리적이고 오류가 없는 판단과 결정보다는 반대로 비논리적인 오류가 있는 한쪽으로 치우친 판단과 결정을 할 수 있게 된 것이다[7]. 정보보안 정책 준수의 영역에서 살펴보면 정보보안 정책준수를 하지 않고 있음에도 이를 합리화하거나 옳다고 생각하여 보안준수행동에 영향을 주는 것이다.

선행연구에서는 조직원의 보안정책 미준수의 위험과 정책 준수에 따른 효용이 높을수록 정보보안 정책 준수 의도가 높다는 보호동기관련 연구[8]와 정보보안 정책 이행의무 수준이 높아질수록 보안정책 준수의도가 높아진다는 억제이론이 있다(General Deterrence Theory). 정보보안 정책에 대한 경영진의 참여와 신뢰가 정보보안 준수태도에 중요한 연관이 있고 교육과 처벌이 유의미한 조절효과가 있다[9]. 정보보안 정책에 따른 업무 스트레스로 정보보안 준수의도가 낮아진다는 연구가 있다[4]. 이러한 선행연구들은 조직이 정보보안에 대해 경영진의 참여, 교육, 처벌 등의 효과성에 초점을 두거나, 조직원의 보호동기가 높고, 정보보안 정책 의무수준이 높아질수록 정보보안 정책 준수의도가 높아진다는 점을 검증하였으나, 본래적인 인간의 심리적인 편향적 사고에 기인한 감성적, 비이성적인 판단과 결정이 정보보안 정책 준수에 미치는 측면을 설명하고 있지 않다.

이 연구에서는 정보보안정책준수라는 판단과 결정을 하는 동안 정보보안 정책 준수에 영향을 미치는 편향적 사고 유형을 제시하고, 실제 미치는 긍정적, 부정적 영향을 검증하여 조직원의 편향적 사고를 관리의 필요성을 제시하고자 한다. 연구의 목적을 달성하기 위하여 다음과 같이 연구를 진행하였다. 첫째, 선행연구를 통해 인간의 편향적 사고 유형 가운데 정보보안 정책준수와 관련된 유형을 제시하고 정보보안 정책준수 태도에 미치는 영향을 검증한다. 둘째 정보보안 정책준수 태도가 행동에 미치는 영향을 검증한다. 마지막으로 경영진참여, 보호동기 요인(지각된 위험성), 교육 및 처벌의 편향적 사고에 대한 조절효과를 분석하여, 조직원의 편향적 사고가 정보보안 정책 준수에 미치는 영향을 줄이기 위한 방향성을 제시한다.

2. 이론적 배경

2.1 보안정책 준수태도 및 준수행동

조직은 보안 사고를 줄이기 위해 노력을 하고 있지만, 조직원의 정보보안에 대한 태도와 행동을 인위적으로 모두 통제할 수 없다. 따라서 조직원이 정보보안 정책에 대한 긍정적인 태도 갖고 이를 준수하는 행동을 하도록 관심과 노력을 기울여야 한다. 사회심리학에서는 태도와 행동의 관계를 많이 연구하고 있다. 태도는 '개인이 어떤 일이나 상황 따위를 대하는 마음가짐, 또는 그 마음가짐이 드러난 자세'를 의미한다. 또한 개인의 태도는 어떤 상황에 대해 긍정적 또는 부정적인 반응하는 감정이라고 정의할 수 있다[10]. 태도와 행동은 높은 상관관계가 있으며, 태도는 행동을 결정하는 중요 요소로서 연구하고 이를 발전시켜 합리적 행동이론을 제시하고 있다[11]. 한편 보안태도는 조직원이 정보보안에 대한 위험을 인식하고 행동하는 것이다[12]. 즉, 보안정책 준수에 대한 태도와 행동은 정보보안 위협에 대한 조직원의 조직의 자산을 지키려는 의지이다.

2.2 편향적 사고

심리학의 이중인지과정 이론의 핵심은 '인간은 이성과 분석을 중시하는 사고체계와 감성과 직관을 중시하는 사고체계를 지녔고, 특정 상황에서 이 중에 어떤 사고체계의 영향을 받느냐에 따라 전혀 다른 결과가 나온다.' 라고 한다[6]. Daniel Kahneman의 연구에 따르면 이중인지과정이론 연구를 종합하여 직관을 제1체계로 이성을 제2체계로 나누어 설명한다. 직관은 자동으로 활성화되는 빠른 인지 처리과정이라면, 이성은 느리고 의식적인 처리 과정이다. 즉 직관은 별다른 노력이 필요하지 않지만 이성은 별도의 노력과 논리 같은 형식이 필요하다[6].

인간은 진화의 과정에서 더 빨리 현상을 파악, 예측하고, 반응하기 위한 수단으로 해석 프레임, 인지적 틀을 발달시켰다. 이러한 능력이 인간을 다른 동물의 삶보다 높은 수준의 삶을 살게 했지만 부정적인 효과로 각종 왜곡된 편향적 사고를 하게 하였다[7]. 최근 연구결과에 따르면 인간은 논리적으로 합리적인 사고를 하는 것이 아니라 여러 가지 편향적인 주먹구구식 직관적 사고를 하는 것으로 밝혀지고 있다.(Daniel Kahneman) Daniel Kahneman의 연구에 따르면, 인간은 수많은 편향적 사고(75개의편향, 21개의 사회적 편향, 49개의 기억오류, 총145개)를 하며 인지적 편향과 오류에 살고 있지만 '나는 논리적으로, 합리적으로 사고하는 사람이며, 나의판단과 결정은 늘 합리적, 이성적이며, 내주장 내 생각은 옳다'라고 믿고 산다고 하였다.

사회심리학자 카너먼은 '우리는 살아가면서 수많은 상황에서 지적인 능력을 통해 합리적·이성적 사고를 하고 문제를 해결할 수 있는 존재라고 믿어왔으나 인간의 이성은 탈 합리적이다' 라고 하였다. 진화론적으로는 인간은 생존을 위해 인지처리과정이 느린 이성적사고 보다는 인지처리과정이 빠른 직관과 감성에 기대어 생각하고 판단할 때가 많다[5]. 즉 직관은 별다른 노력이 필요 없지만 이성은 별도의 노력과 논리 같은 형식이 필요하다[6]. 생존을 위해 주변 환경을 더 빨리 이해하고 예측하고 설명할 수 있었던 이러한 능력이 인간은 동물의 수준을 넘어서 수준 높은 삶을 가능하게 하였으나 그에 따른 부정적인 효과도 많이 생기게 되었고, 합리적이고 오류가 없는 판단과 결정보다는 반대로 비논리적인 오류가 있는 한쪽으로 치우친 판단과 결정을 할 수 있게 된 것이다[7].

2.3 경영진 역할, 보호동기, 교육 및 처벌

Puhakainen & Siponen은 경영진이 보안 사고에 참여하여 보안사고 수습 및 정보보호 활동을 촉진하는 등 실질적으로 관여한 이후에는, 조직의 구성원들의 정보보안정책 준수 의지가 긍정적으로 변화된다고 하였다[13]. 또한 경영진의 참여는 조직구성원에 영향을 주고 따라서 정보보안정책 준수 의지에도 영향이 있다고 하였다[14].

Rogers(1975)는 개인이 지각하는 위협요인과 위험한 상황에서의 대처과정을 보호동기 이론으로 정리하였다[15]. 본 연구는 정보보안정책 준수 태도에 중요한 영향을 미치는 요인이 될 것으로 기대되는 지각된 위험성을 조절 변수로 선택하였다. 선행

연구에 의해 지각된 위험성은 개인이 지각하는 위협요인으로서 인지되는 위협의 크기를 나타낸다. Herath et al.(2009)은 지각된 위험성은 조직원에게 정보보안정책을 실천 의지에 영향을 줄 수 있음을 제시하고 정보보안정책 준수 행동을 위한 태도와 인과관계가 있음을 설명 하였다.

교육훈련은 조직원이 보안정책을 스스로 따르도록 하는 내적 동기와 실행 능력을 부여할 수 있는 조직의 활용 수단이다[16]. Straub(1990)과 Siponen et al.(2007)은 조직구성원에 대한 제재 및 처벌은 정보보안 정책 준수 행동을 증가시키는데 영향을 미치는 것으로 주장하였다[17][18].

3. 연구설계 및 방법론

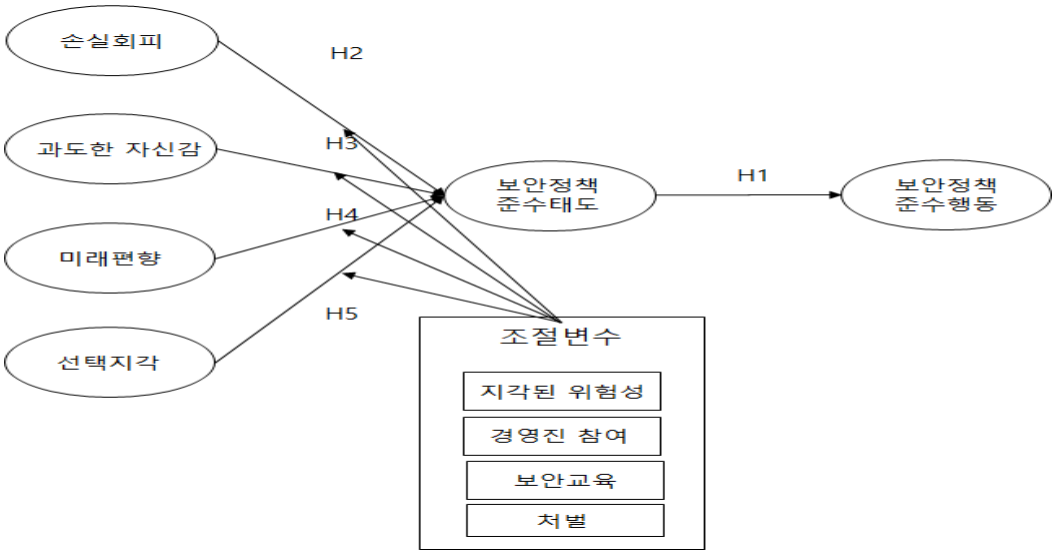
3.1 변수정의 및 측정

정보보안 정책준수와 관련된 편향적 사고 요인은 선행연구에서 손실혐오, 과도한 자신감, 미래가치 폄하, 선택적 지각으로 구성하였다. 편향적 사고 요인은 이남석(2013, 인지편향사전)의 연구를 통해서 세부 요인 및 측정항목을 제시하였다. 손실혐오는 “손실을 보는 상황에서는 이를 벗어나기 위해 작은 확률에도 매달리는 위험을 감수하는 것”으로 정의하였으며, 3개의 항목을 적용한다. 과도한 자신감은 “자신의 능력, 상태, 통제력, 일의 범위, 성과 등을 과대평가하는 경향”으로 정의하였으며, 3개의 항목을 적용한다. 과도한 미래가치 폄하는 “시간상으로 더 먼 미래의 것은 상대적으로 가치를 폄하하는 현상”으로 정의하였으며, 3개의 항목을 적용한다. 선택적 지각은 “자신의 신념이나 생각과 일치하거나 자기에게 유리한 것만 선택적으로 받아들여 처리하려는 경향”으로 정의하였으며, 3개의 항목을 적용한다.

정보보안 태도 및 행동 요인은 Ajzen(1991, 2002) 의 연구[19][20]를 통해서 요인의 개념 및 측정항목을 제시하였다. 정보보안 준수 태도는 “정보보안정책 준수에 대한 개인의 긍정적 또는 부정적 판단 또는 인식”으로 정의하고 5개 항목을 적용하였다.

종속변수인 정보보안 정책준수 행동은 “정보보안정책에 의한 정보자산 활용과 비밀을 유지하고, 잠재적 보안사고로부터 정보자산 보호할 책무를 이행”으로 정의하였으며 4개의 항목을 적용한다.

마지막으로 조절효과 검증을 위한 경영진 참여는 “정보보안정책에 관한 경영진의 분명한 비전, 목표 수립 및 추진 방향 제시”으로 정의하고 Liang et al.(2007), Jarvenppa & Ives(1991), Hu et al.(2012)를 통해서 3개 항목을 적용하였다. 보호동기의 지각된 위험성은 “정보보안정책 위반에 따른 지각된 정보 보안 위협 심각성”으로 정의하고 Vance & Siponen(2012), Siponen et al.(2010),



[그림 1] 연구 모형

Ifinedo(2012)를 통해서 3개 항목을 적용하였다. 교육훈련은 “정보보안정책 준수 의무 중요성과 필요성 인식 교육 및 정보보안 정책 이행 직무능력 향상 훈련”으로 정의하고 Puhkainen & Siponen(2010)을 통해 2개 항목을 적용하였다. 처벌은 “정보보안 정책 미준수에 따른 제재벌칙에 대한 가능성 또는 확실성 및 가해지는 제재 벌칙에 대한 심각성”으로 정의하고 Son(2011)을 통해 3개 항목을 적용하였다. 구조방정식에서 경로분석을 위해 잠재변수별 3개 이상의 관측변수를 갖도록 권고하고 있다

연구가설 검증을 위한 10개의 요인에 대한 세부측정항목들은 정보보안 정책준수라는 이 연구과제에 적합하도록 추가적인 수정을 하였다. 최종적으로 32개의 항목을 설문으로 활용하였으며 모든 변수들은 5점 리커트 척도를 사용하였다.(1점 전혀그렇지 않다 - 5점 매우 그렇다). 2019년 4월부터 5월까지 191명을 대상으로 설문을 배포하였으며, 총 173개의 응답결과가 수집되었다. 이중 불성실한 응답으로 판단되는 16개를 제외하고 157개의 응답을 분석에 사용하였다. 응답결과의 통계학적 특징은 <표 1> 과 같다.

3.2 연구모형 설계 및 연구가설

이 연구는 정보보안 정책준수 관련 조직원의 편향적사고(손실혐오, 과도한자신감, 미래가치폄하, 선택적 지각)와 정보보안 정책준수 태도와의 관계, 경영진의 참여, 지각된 위험성, 교육 및 처벌의 편향적 사고에 대한 조절효과를 검증과 정책준수 태도와 정책준수 행동과의 관계를 검증한다. 이에 편향적 사고 및 보안 정책준수 태도, 행동과 관련된 선행 연구들을 참고하여 연구모형 [그림 1] 및 가설검증에 필요한 10개의 요인을 제시하였다.

3.2.1 보안정책 준수태도 및 준수행동

선행연구에서 태도와 행동은 높은 상관관계가 있음을 제시하였다. 따라서 정보보안 정책에 대한 긍정적인 보안정책 준수태도는 보안 정책 준수행동을 증가시킬 것으로 판단되며, 다음과 같은 연구가설을 제시한다.

H1 : 정보보안 정책 준수 태도가 정보보안 정책 준수 행동에 양(+)의 영향을 미칠 것이다.

3.2.2 편향적 사고

편향적 사고를 정보보안 정책 준수의 영역에서 살펴보면 정보보안 정책준수를 하지 않고 있음에도 이를 합리화하거나 옳다고 생각하는 경향이다. 이 연구에서는 선행연구를 통해 도출된 145개의 편향사고 유형 중 조직원들이 정보보안정책을 받아들이고 행동하는 결정을 하는데 영향을 줄 수 있을 것으로 판단되는 4가지 편향적 사고 유형을 선별하였다. 첫째는 손실혐오(Loss Aversion)는 같은 수준이라도 얻은 것의 가치보다 잃은 것의 가치를 훨씬 크게 느끼며, 손실을 보는 상황에서는 이를 벗

<표 1> 응답자 특성 분석

구분		빈도	%
성별	남성	132	84.1
	여성	25	15.9
연령	20~29	50	31.8
	30~39	81	51.6
	40~49	26	16.6
기업형태	중소기업	77	49.0
	중견기업	24	15.3
	대기업	9	5.7
	공공기관	41	26.1
	기타	6	3.8
직급	사원	52	33.1
	대리	51	32.5
	과장	34	21.7
	차장 이상	20	12.8

어나기 위해 작은 확률에도 매달리는 위험을 감수하는 것으로 정의된다(Daniel Kahneman). 즉 조직원이나, 협력업체 직원 중에 자신에게 다양한 사유로 금전적인 손해가 발생하여 심리적으로 위축된 상황일 때 이를 벗어나기 위해서 조직의 정보보안 정책을 위반해서라도 자신이 지득한 회사정보를 유용하여 이직, 불법거래 등을 시도하려는 성향을 의미한다. 둘째 과도한 자신감(Overconfidence Bias)은 자신의 능력, 상태, 통제력, 일의 범위, 성과 등을 과대평가하는 현상으로 정의된다. 즉 조직원이나 관련 협력업체 직원이 자신은 조직의 정보보안 시스템과 정책을 잘 알고 있고, 이를 우회할 수 있다고 확신하여 정보보안 정책을 위반하여도 아무런 책임을 지지 않아도 된다고 확신하는 성향을 의미한다. 셋째, 과도한 미래가치 폄하(Hyperbolic Discounting)은 시간상으로 더 먼 미래의 것은 상대적으로 가치를 폄하하는 현상으로 정의된다. 즉 조직원이나 관련 협력업체 직원이 정보보안 정책을 준수함으로써 장기적으로 보안사고 감소와 조직의 성장에 기여하고, 개인적으로도 혜택을 누릴 수 있다고 여기는 것보다 정보보안 정책을 위반함으로 얻는 업무상 편리함을 추구하는 성향을 의미한다. 넷째, 선택적 지각(Selective Perception)은 외부정보를 객관적으로 있는 그대로 받아들여 처리하는 것이 아니라, 자신의 신념이나 생각과 일치하거나 자기에게 유리한 것만 선택적으로 받아들여 처리하려는 현상으로 정의된다. 즉 조직원이나 관련 협력업체 직원이 조직의 정보보안 정책을 지키는 것은 자신이 수행하는 업무에 전혀 도움이 되지 않을 것이라고 확신하는 경향을 의미한다.

이러한 편향적 사고의 경향이 높을수록 정보보안 준수 태도에 영향을 줄 것이라고 판단되며 다음과 같은 연구 가설을 제시한다.

H2 : 편향적 사고 손실혐오가 정보보안 정책준수 태도에 영향을 미칠 것이다.

H3 : 편향적 사고 과도한자심감은 정보보안 정책준수 태도에 영향을 미칠 것이다.

H4 : 편향적 사고 과도한 미래가치 폄하는 정보보안 정책준수 태도에 영향을 미칠 것이다.

H5 : 편향적 사고 선택적 지각은 정보보안 정책준수 태도에 영향을 미칠 것이다.

3.2.3 경영진 역할, 보호동기, 교육 및 처벌

앞에서 살펴본 선행연구에 의하여 경영진의 역할, 지각된 위험성, 교육 및 처벌이 정보보호 정책준수에 영향을 줄 수 있음을 설명하였다. 따라서 다음과 같은 연구 가설을 제시한다.

H6 : 경영진의 참여는 편향적사고가 정보보호 정책준수를 위한 태도에 미치는 영향강도를 긍정적으로 조절할 것이다.

H7 : 지각된 위험성은 편향적사고가 정보보호 정책준수를 위한 태도에 미치는 영향강도를 긍정적으로 조절할 것이다.

H8 : 교육 및 처벌은 편향적사고가 정보보호 정책준수를 위한 태도에 미치는 영향강도를 긍정적으로 조절할 것이다.

4. 실증분석

4.1 신뢰성 검정

이 연구의 연구가설 검증을 위해 AMOS 18.0을 사용하고, 연구모델의 적정성검증으로 신뢰성과 타당성검증을 실시하였다. 이를 위해 확인적 요인분석 실시 후 모델 적합도가 기준치 이상 도출되면 신뢰성과 타당성 검증에 활용할 수 있다. 확인적 요인분석의 모델 적합도는 <표 2>에 나타난바와 같이 전반적으로 수용가능 한 수준으로 도출 되었다.

신뢰성은 측정요인의 관측변수들이 동질적인 변수들로 구성되어 있는지 확인하는 과정이며, 내적일관성을 이용하여 측정한다. 내적일관성은 크론바 알파 값을 이용하여 내적 일관성을 측정한다. Nunnally(1978)는 활용가능(0.6～0.7), 적절(0.7～0.9), 우수(0.9이상) 로 제시하였다.

이 연구의 신뢰성 분석 결과 내적 일관성을 <표 3>와 같이 확보하고 있는 것으로 나타났다.

< 표 2 > 확인적 요인분석 적합도 결과

	절대적합지수				증분적합지수			
	CMIN/DF	GFI	AGFI	RMSEA	NFI	TLI	CFI	IFI
적합도	1.687	0.848	0.802	0.066	0.868	0.930	0.941	0.942
요구사항	1.0~2.0	>0.9	>0.9	0.05~0.08	>0.9	>0.9	>0.9	>0.9

< 표 3 > 신뢰도 및 집중 타당성 분석 결과

구분	측정문항	표준화계수	Cronbach's Alpha	AVE	CR
손실회피	손실1	0.867	0.896	0.746	0.898
	손실2	0.924			
	손실3	0.807			
미래편향	미래1	0.876	0.802	0.574	0.798
	미래2	0.816			
	미래4	0.596			
선택지각	선택1	0.839	0.669	0.522	0.751
	선택2	0.745			
	선택4	0.392			
과도자신감	과도1	0.818	0.873	0.576	0.844
	과도2	0.725			
	과도3	0.840			
	과도4	0.805			
태도	태도1	0.851	0.940	0.878	0.973
	태도2	0.901			
	태도3	0.837			
	태도4	0.905			
	태도5	0.872			
행동	행동1	0.721	0.869	0.755	0.925
	행동2	0.759			
	행동3	0.833			
	행동4	0.871			

< 표 4 > 판별타당성 검증 결과

구분	1	2	3	4	5	AVE
손실회피(p^2)	1					0.746
미래편향(p^2)	0.642(.412)**	1				0.574
선택지각(p^2)	0.441(.194)**	0.556(.309)**	1			0.522
과도한자신감(p^2)	0.495(.245)**	0.561(.315)**	0.241(.058)	1		0.576
태도(p^2)	-0.405(.164)**	-0.476(.227)**	-0.497(.247)**	-0.052(.003)	1	0.878
행동(p^2)	-0.418(.175)**	-0.489(.239)**	-0.488(.238)**	-0.262(.069)**	0.592(.350)*	0.755

< 표 5 > 구조방정식 적합도

	절대적합지수				증분적합지수			
	CMIN/DF	GFI	AGFI	RMSEA	NFI	TLI	CFI	IFI
적합도	1.672	0.845	0.801	0.066	0.868	0.931	0.941	0.942
요구사항	1.0~2.0	>0.9	>0.9	0.05~0.08	>0.9	>0.9	>0.9	>0.9

4.2 타당성 검정

타당성 분석은 측정요인들이 서로 다른 개념으로 구성되어 있는지 확인하는 분석이며 집중타당성과 판별타당성으로 검정한다.

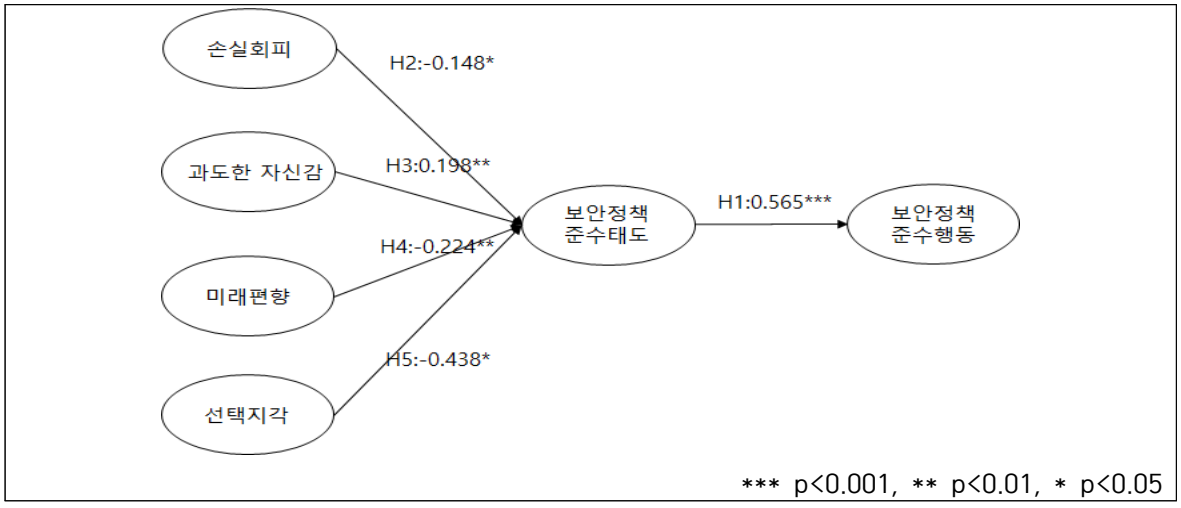
집중타당성은 측정요인의 관측변수들의 일치성 정도이며, 확인적 요인분석 결과 평균분산추출(AVE:Average Variance Extracted)와 개념신뢰도(CR:Construct Reliability)를 사용하여 검증한다. 평균분산추출은 0.5이상, 개념신뢰도는 0.7이상이면 적합하다고 판별한다.(Wixom and Watson, 2001). 각 요구사항에 대한 분석결과 <표 3>과 같이 적합 기준치를 상회하는 것으로 도출되었다.

판별타당성은 검증은 측정요인들의 결정계수 값과 평균분산추출 값을 비교하여 검증한다(Formell and Lacker, 1981). 일반적으로 두 요인사이의 평균분산추출값이 각 요인의 결정계수(r^2) 값보다 크면 판별타당성이 확보된 것으로 판단한다. 분석결과 판별타당성 확보의 요구사항을 <표 4>과 같이 만족하는 것으로 나타났다.

5. 연구결과

5.1 연구모형 분석 및 고찰

측정모형에 대해 변수들의 인과관계를 AMOS 18.0을 활용하여 구조방정식 모델링을 적용하여 분석하였다. 우선, 연구모형의 적합성에 대한 검증을 실시하여, 연구모형이 연구표본과 적합하게 합치되는 가에 대한 적절성 여부를 살펴보았다. 연구모형의 적합성은 절대적합지수, 증분적합지수 등으로 판단할 수 있다. 연구모형의 적합도는 <표 5>에 나타난 바와 같이 전반적으로 수용가능 한 수준으로 도출 되었다. 연구가설의 검증을 위하여 AMOS 프로그램을 활용하여 각각의 변수간 관계분석을 통하여 [그림 2], <표 6>과 같이 연구가설을 검증하였다. 첫째 정보보안 정책 준수 태도가 정보보안 정책준수 행동에 양(+)의 영향을 미친다는 가설은 채택되었다(β=0.565, p<0.001). 정보보안 정책준수에 대한 긍정적인 태도가 높을수록 정보보안 정책 준수 행동도 높아져 조직의 정보보안 수준을 높인다는 것이며 태도가 행동에 영향을 준다는 선행연구와 같은 결과이다[11]. 둘째, 조직원 편향적 사고의 손실혐오 정도는 정보보안 정책 준수 태도에 영향을 미친다는 가설은 채택되었다(β=-0.148, p<0.039). 조직원이 자신의 금적적인 손실이 발생되거나 예상될 때 정보보안 정책을 위반하면서 이를 회피하고자 하는 정도가 높을수록 정보보안 정책준수 태도는 낮아진다는 것이다. 셋째, 조직원 편향적 사고의 과도한 자신감 정도는 정보보안 정책 준수 태도에 영향을 미친다는 가설은 채택되었다(β=0.198, p<0.002). 조직원이 정보보안 정책의



[그림 2] 구조모형 분석 결과

< 표 6 > 연구모형 가설검증 결과 요약

	가설경로	경로계수	C.R.(t)	검증결과
H1	보안정책 준수태도 → 보안정책 준수행동	0.565	6.558***	채택
H2	손실회피 → 보안정책 준수태도	-0.148	-2.066*	채택
H3	과도한 자신감 → 보안정책 준수태도	0.198	3.095**	채택
H4	미래편향 → 보안정책 준수태도	-0.224	-2.780**	채택
H5	선택지각 → 보안정책 준수태도	-0.438	-2.428*	채택

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

기술적 내용에 대해 잘알고 있고, 자신은 이를 우회할 수 있다는 확신이 높을수록 정보보안 정책준수의 태도가 높아진다는 것이다. 넷째, 조직원 편향적 사고의 미래가치편향 정도는 정보보안 정책준수 태도에 영향을 미친다는 가설은 채택되었다(β=-0.224, p<0.05). 조직원이 정보보안 정책을 준수함으로 미래에 발생되는 긍정적인 효과보다는 현재 자신의 업무 불편함의 정도에 더 민감할수록 정보보안 정책 준수 태도는 낮아진다는 것이다. 다섯째, 조직원의 편향적 사고의 선택지각 정도는 정보보안 정책 준수 태도에 영향을 미친다는 가설은 채택되었다(β=-0.438, p<0.015). 조직원이 조직의 정보보안 정책이 자신과는 상관이 없는 일로 여기는 정도가 높을수록 정보보안 정책 준수태도는 낮아진다는 것을 의미한다.

연구결과를 고찰하여 보면, 첫째 정보보안 정책준수 태도가 정보보안 정책준수 행동에 긍정적 영향을 주는 요인임을 증명하였다(H1). 조직원은 피고용인으로 정보 보유 수준 등의 차이로 조직과의 관계에서 대리인 문제가 발생할 수밖에 없다[21]. 따라서 조직의 정보보안사고 예방을 위해서는 근본적으로 조직원의 자발적인 정보보안 정책준수 행동이 가장 중요하다. 관련된 사회심리학의 많은 연구에서 태도가 행동에 영향을 주는 요인임을 고려하여, 이 연구에서는 조직원의 정보보안 정책준수 태도가 긍정적이면 정보보안 정책준수 행동을 증가시키는 것을 증명하였다. 이는 조직원이 기업에서 준수해야 하는 정보보안 정책에 대해 편향적으로 또는 부정적으로 인식하고 있는 경우 정보보안 준수행동으로 이어지기 어려우며 정보보안 사고 예방, 보안 수준제고라는 목표를 달성하기 어려움을 의미한다. 따라서 조직은 정보보안 정책준수를 요구할 때 조직원이 긍정적인 태도로 받아들일 수 있도록 다양한 접근방식을 고려하는 전략이 필요함을 나타낸다.

둘째, 조직원의 편향적 사고유형(손실혐오, 과도한 자신감, 미래가치폄하, 선택적 지각)이 정보보안 정책준수 태도에 영향을 미치는 것을 증명하였다(H2,H3,H4,H5). 조직에서 정보보안에 대한 투자와 관심은 높아지지만 내부조직원의 부주의 또는 악의적인 행동에 의한 정보유출 등의 정보보안 사고는 지속적으로 발생한다. 이는 조직원의 정보보안 정책준수에 대한 편향적 사고인 비이성적인 행동 또는 부정적인 태도로 인해 정보보안의 정책의 불이행의 사각지대가 발생하고 사고로 이어지는 확률이 낮지 않음을 의미한다. 이 연구에서는 조직원의 비이성적인 행동 요인인 편향적 사고 유형을 관련 선행연구로부터 도출하여 정보보안 정책준수에 적용하여 관련성이 있음을 검증하였다. 편향적 사고(손실혐오, 과도한 미래가치폄하, 선택적 지각) 유형은 조직의 정보보안 정책준수 태도에 부정적인 영향을 주어 결과적으로 정보보안 정책준수 행동을 감소시키는 것으로 검증되었다. 편향적사고(과도한 자신감)은 조직의 정보보안 정책준수 태도에 긍정적인 영향을 주어 결과적으로 정보보안 정책준수 행동을 증가시키는 것으로 검증 되었다. 따라서 이 연구는 정보보안 준수태도 및 행동에 부정적·긍정적 영향을 주는 조직원의 심리적 요인인 편향적 사고의 유형을 제시·검증하고 부정적인 영향을 주는 편향적 사고 요인을 감소시키고 긍정적인 영향을 주는 요인을 증가시키기 위한 연구의 방향을 제시한 것에 의의가 있다. 실무적으로 조직은 정보보호 수준제고를 위한 정책 수립 및 지속투자에 만족하는 것을 넘어 조직원의 편향적 사고(손실혐오, 과도한 미래

<표 7> 조절 효과 검증 결과

변수	모형	R	R 제곱	수정된 R 제곱	추정값의 표준오차	통계량 변화량					Durbin-Watson
						R 제곱 변화량	F 변화량	df1	df2	유의확률 F 변화량	
손실혐오	**손실혐오**	**.392a**	**.153**	**.148**	**.55604**	**.153**	**28.105**	**1**	**155**	**.000**	
	지각된위험성	**.589b**	**.347**	**.339**	**.48982**	**.194**	**45.740**	**1**	**154**	**.000**	
	손실혐오×지각된위험성	**.603c**	**.364**	**.351**	**.48513**	**.017**	**3.991**	**1**	**153**	**.048**	**1.879**
미래가치편향	**미래가치편향**	**.399a**	**.160**	**.154**	**.55404**	**.160**	**29.429**	**1**	**155**	**.000**	
	지각된위험성	**.595b**	**.354**	**.346**	**.48713**	**.195**	**46.503**	**1**	**154**	**.000**	
	미래가치편향×지각된위험성	**.611c**	**.373**	**.361**	**.48161**	**.019**	**4.554**	**1**	**153**	**.034**	**1.799**
선택적지각	**선택적지각**	**.393a**	**.155**	**.149**	**.55567**	**.155**	**28.347**	**1**	**155**	**.000**	
	지각된위험성	**.584b**	**.341**	**.333**	**.49201**	**.187**	**43.707**	**1**	**154**	**.000**	
	선택적지각×지각된위험성	**.606c**	**.368**	**.355**	**.48367**	**.026**	**6.360**	**1**	**153**	**.013**	**1.808**
과도한자신감	과도한자신감	.050a	.002	-.004	.60360	.002	.386	1	155	.536	
	지각된위험성	.567b	.321	.312	.49960	.319	72.252	1	154	.000	
	과도한자신감×지각된위험성	.569c	.324	.311	.50015	.003	.662	1	153	.417	1.887
손실혐오	손실혐오	.392a	.153	.148	.55604	.153	28.105	1	155	.000	
	경영진참여	.420b	.176	.165	.55032	.023	4.241	1	154	.041	
	손실혐오×경영진참여	.428c	.183	.167	.54966	.007	1.370	1	153	.244	1.916
미래가치편향	미래가치편향	.399a	.160	.154	.55404	.160	29.429	1	155	.000	
	경영진참여	.429b	.184	.174	.54764	.025	4.645	1	154	.033	
	미래가치편향x경영진참여	.429c	.184	.168	.54940	.000	.013	1	153	.909	1.969
선택적지각	선택적지각	.393a	.155	.149	.55567	.155	28.347	1	155	.000	
	경영진참여	.440b	.194	.183	.54440	.039	7.484	1	154	.007	
	선택적지각x경영진참여	.441c	.194	.178	.54602	.000	.089	1	153	.766	1.948
과도한자신감	과도한자신감	.050a	.002	-.004	.60360	.002	.386	1	155	.536	
	경영진참여	.221b	.049	.036	.59134	.046	7.497	1	154	.007	
	과도한자신감x경영진참여	.225c	.051	.032	.59264	.002	.324	1	153	.570	2.035
손실혐오	손실혐오	.392a	.153	.148	.55604	.153	28.105	1	155	.000	
	보안교육	.435b	.189	.179	.54593	.036	6.795	1	154	.010	
	손실혐오x보안교육	.437c	.191	.175	.54715	.002	.316	1	153	.575	1.815
미래가치편향	미래가치편향	.399a	.160	.154	.55404	.160	29.429	1	155	.000	
	보안교육	.444b	.197	.186	.54337	.037	7.146	1	154	.008	
	미래가치편향x보안교육	.445c	.198	.182	.54472	.001	.239	1	153	.626	1.886
선택적지각	선택적지각	.393a	.155	.149	.55567	.155	28.347	1	155	.000	
	보안교육	.440b	.194	.183	.54436	.039	7.512	1	154	.007	
	선택적지각x보안교육	.447c	.200	.184	.54406	.006	1.170	1	153	.281	1.875
과도한자신감	과도한자신감	.050a	.002	-.004	.60360	.002	.386	1	155	.536	
	보안교육	.291b	.085	.073	.58000	.082	13.874	1	154	.000	
	과도한자신감x보안교육	.323c	.104	.087	.57563	.020	3.344	1	153	.069	1.947
손실혐오	손실혐오	.392a	.153	.148	.55604	.153	28.105	1	155	.000	
	처벌	.398b	.159	.148	.55616	.005	.933	1	154	.336	
	손실혐오x처벌	.406c	.165	.149	.55583	.006	1.186	1	153	.278	1.860
미래가치편향	미래가치편향	.399a	.160	.154	.55404	.160	29.429	1	155	.000	
	처벌	.414b	.171	.161	.55190	.012	2.204	1	154	.140	
	미래가치편향x처벌	.414c	.171	.155	.55370	.000	.002	1	153	.963	1.981
선택적지각	선택적지각	.393a	.155	.149	.55567	.155	28.347	1	155	.000	
	처벌	.433b	.187	.177	.54656	.033	6.214	1	154	.014	
	선택적지각x처벌	.475c	.226	.211	.53523	.038	7.586	1	153	.007	1.893
과도한자신감	과도한자신감	.050a	.002	-.004	.60360	.002	.386	1	155	.536	
	처벌	.193b	.037	.025	.59491	.035	5.563	1	154	.020	
	과도한자신감x처벌	.221c	.049	.030	.59327	.011	1.849	1	153	.176	2.094

가치폄하, 선택적 지각)에 대한 이해도를 높이고 이를 감소시킬 수 있는 전략적인 접근이 필요함을 의미하며 다양한 방식의 체계적인 지원을 할 필요가 있다. 한편, 편향적사고(과도한 자신감)은 정보보안 정책준수 태도에 긍정적인 영향을 주므로 조직원이 정보보안 정책, 보안 기술 등의 지식에 자발적인 관심을 갖도록 유도하여 조직원 스스로 회사의 보안 정책 및 기술에 잘 알고 있다고 확신을 갖도록 정보보안 교육 등을 지원할 필요가 있다.

5.2 조절효과 분석 및 고찰

이 연구는 경영진의 참여, 보호동기의 지각된 위험성, 교육 및 처벌이 조직원의 편향적 사고(손실혐오, 미래가치편향, 선택적 지각, 과도한자신감)와 정보보안 정책준수 태도와의 관계에서 조절효과를 <표 7>과 같이 가질 것으로 판단하여 검증하였다.

조절효과 검증결과 손실혐오, 미래가치편향, 선택적 지각이 정보보안 정책준수 태도에 미치는 영향에 대한 지각된 위험성의 조절효과의 결과 R제곱이 순차적으로 증가하였으며, 유의확률F변화량 결과 값이 유의수준 0.05보다 작으므로 지각된 위험성은 정보보안 정책준수 태도에 미치는 영향에 대한 강도에 유의미한 조절효과가 있는 것으로 나타났다. 그러나 과도한 자신감에 대한 지각된 위험성의 조절 효과는 유의확률F변화량 결과값이 0.05보다 크므로 조절효과는 없는 것으로 나타났다. 따라서 지각된 위험성은 편향적사고가 정보보호 정책준수를 위한 태도에 미치는 영향강도를 긍정적으로 조절할 것이라는 가설은 과도한 자신감을 제외하고 채택되었다. 한편 편향적 사고의 4가지 유형, 손실혐오, 미래가치편향, 선택적 지각, 과도한 자신감에 대한 경영진의 참여, 보안교육의 조절효과는 유의확률F변화량 결과 값이 모두 0.05보다 크므로 조절효과는 없는 것으로 나타났다. 따라서 경영진의 참여는 편향적사고가 정보보호 정책준수를 위한 태도에 미치는 영향강도를 긍정적으로 조절할 것이라는 가설은 기각되었다. 또한 교육 및 처벌은 편향적사고가 정보보호 정책준수를 위한 태도에 미치는 영향강도를 긍정적으로 조절할 것이라는 가설도 기각되었다.

조절효과를 고찰하여 보면, 조직원의 편향적 사고유형(손실혐오, 미래가치폄하, 선택적 지각)이 정보보안 정책준수 태도에 영향을 미치는데 있어, 보호동기의 지각된 위험성이 영향력을 긍정적으로 조절함을 증명하였다(H6). 선행 연구에서는 경영진의 참여, 교육 및 처벌이 정보보안 정책 준수에 영향을 미치는 것으로 나타났으나 이 연구에서는 조절변수로서 편향적 사고에 유의미한 영향을 미치는 조절효과가 나타나지 않았다. 즉 조직원의 정보보안 정책준수 태도에 영향을 주는 편향적 사고를 긍정적으로 완화시키기 위해서는 일반적인 관점에서의 경영진의 참여, 교육, 처벌의 효과가 없음을 의미한다. 다만 조직원이 지각된 위험성(정보보안정책 준수에 대한 조직에서의 중요성 인지와, 정보보안정책 미준수 또는 위반에 따른 조직내부에서의 정보보안 문제에 대한 심각성 인지, 개인의 보안문제 심각성 인지) 을 인지할 수 있도록 경영진의 참여와, 교육, 처벌 등의 정보보안 정책이 효과적으로 이루어질 수 있다면 편향적 사고를 감소시키는 요인으로 작용할 수 있을 것으로 판단된다. 따라서 조직원의 정보보안 정책준수 태도에 부정적인 영향을 주는 편향적 사고를 감소시킬 수 있는 조직차원의 모든 노력은 조직원이 보안사고에 대한 위험성을 개인이 인지할 수 있도록 초점을 맞추는 게 핵심임을 제시한다.

6. 결론

이 연구는 조직에서 정보보안 정책 시행시 조직원의 정보보안 정책에 대한 태도가 정보보안 정책준수 행동에 영향을 준다는 것을 검증하고, 조직원의 비논리적인 편향적 사고 패턴과 정보보안 정책준수 태도와 관계를 검증하는 것을 목적으로 한다. 태도와 행동관련 이론과 편향적 사고 이론의 사회심리학의 선행연구를 기반으로 정보보안 정책 준수 태도가 정책준수 행동을 증가시키는 것을 제시하였다. 또한 편향적 사고 유형(손실혐오, 과도한자신감, 미래가치폄하, 선택적지각)이 정보보안 정책준수 태도에 영향을 미칠 것으로 가설을 제시하였다. 연구결과는 사회심리학의 선행연구 결과를 정보보안 분야로 확장하여, 기존 정보보안 수준제고를 위한 여러 연구에서 다루지 않았던 조직원의 정보보안 준수 행동의 유발요인으로서 편향적 사고라는

새로운 관점을 추가 보완함으로써 특장점을 가진다.

이 연구는 다음과 같은 한계점도 존재하며, 향후 연구에서 보완될 필요성이 있다. 첫째, 이 연구에서는 조직원의 심리학적 요인인 편향적 사고가 정보보안 준수태도에 미치는 영향을 검증하여 실무적인 시사점을 제시하였다. 또한 편향적 사고를 감소시킨 요인으로 지각된 위험성에 대해서 검증되었으나, 경영진의 참여, 교육 및 처벌이 지각된 위험성을 증가시키는 방향으로 이루어진다면 정보보안 정책 준수 태도에 영향을 줄 수 있다는 영향관계는 검증하지 못하였다. 둘째, 정보보안 정책준수 태도에 영향을 주는 요인으로 다른 선행연구에서는 다양한 관점의 요인을 제시하고 있다. Inho Hwang(2017)은 보안관련 업무 스트레스가 정보보안준수의도에 영향을 주고, 스트레스는 정보보안활용촉진, 기술지원, 참여촉진으로 감소함을 제시하였다[4]. 신혁(2018)은 경영진의 참여와 보호동기가 정보보안 정책준수 태도에 영향을 줌을 제시하였다[9]. 따라서 향후 추가 연구에서는 정보보안 준수태도에 영향을 주는 추가적인 요인들을 제시하는 것이 필요하다.

참 고 문 헌

[1] Kaspersky Lab(2017), Foolproof Employee Security Checklist

[2] Verizon(2019), Data Breach Investigations Report

[3] D'Arcy, J., Herath, T., & Shoss, M. K. (2014), "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective", Journal of Management Information Systems, 31(2), 285-318.

[4] 황인호 · 김승욱(2017), 조직원의 정보보안 관련 업무 스트레스에 대한 억제 및 업무 대처에 관한 연구-금융비즈니스를 중심으로

[5] Tversky, A., & Kahneman, D.(1986). Rational choice and the framing of decisions. *Journl of Business,* S251~s258.

[6] 이남석 · 이정모(2013), 누구나 빠지는 생각의 함정 인지편향사전

[7] 이정모(2012), 인지과학

[8] Ifinedo, P., (2012). Understanding information sustems security policy compliance:An integration of the theory of planned theory and protection motivation theory. *Computers and Security. 31,* 83-95.

[9] 신혁(2018), 계획행동 요인을 매개로 경영진 역할과 보호동기가 정보보안정책 준수에 미치는 영향.

[10] Ajzen, I. & Fishbein, M. (1997). Attitude-Behavior Relation: A Theoretical Analysis and Review of Empirical Research. *Psychological Bulletin, 84*(5), 888-918.

[11] Ajzen, I., and Fishbein, M. (1977). Attitude-Behavior Relations: A theoritical analysis and review of empirical research. *Psychological Bulletin, 84*(5), 888-918.

[12] 강다연 · 장명희. (2012). 해운항만조직 구성원들의 정보보안정책 준수에 영향을 미치는 요인. **한국항만경제학회지 28**(1), 2012, 1-23.

[13] Puhakainen, P., and Siponen, M. (2010). Improving employees' colpliance through information systems security training: An action research study. *MIS Quarterly, 34*(1), 757-778.

[14] Liang, H., Saraf, H., Hu, Q., and Xue, Y. (2007). Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quarterly, 31*(1), 59-87.

[15] Rogers, R. W. (1975). A protection Motivation Theory of fear appeals and attitude change 1. *The Journal of Psychology, 91*(1), 93-114.

[16] Siponen, P. (2000), A concepyual foundation for organizational information security awareness, *Information Management & Computer Security, 8*(1), 31-41.

[17] Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3). 255-276.

[18] Siponen, M., Pahnila, S., and Mahmood, A. (2007). Employees' adherence to

information security policies: An empirical study. *IFIP International Federation for Information Processing. 232*, 133-144.

[19] Ajzen, I. (2002). Constructing a TpB questionnaire: Conceptual and Methodological considerations, *au.edu.tw, 17*, 1-14.

[20] Ajzen, I. (1991). The theory of planned behavior, *Organizational Behavior and Human Decision Processes, 50*, pp.179-211.

[21] West, R. (2008). The Psychology of Security. *Communications of the ACM, 51*(4), 34-40.

허 준

2002 아주대학교
정보 및 컴퓨터 공학과(공학사)
2004 한양대학교
경영정보시스템(경영학 석사)
2015 성균관대학교 교과교육학과 컴퓨터교육
(교육학 박사수료)
2005~현재 한국인터넷진흥원 수석연구원
관심분야: 정보보안, 컴퓨터교육, 정보윤리
E-Mail: herjune@kisa.or.kr

안 성 진

1988 성균관대학교 정보공학과(학사)
1990 성균관대학교 정보공학과(석사)
1998 성균관대학교 정보공학과(박사)
1990~1995 KIST/SERI 연구원
1996 정보통신기술사
1999~현재 성균관대학교 컴퓨터교육과 교수
관심분야 : SW교육, 정보윤리, 정보보안
E-Mail: sjahn@skku.edu