Journal of Convergence for Information Technology
Vol. 10. No. 12, pp. 91-99, 2020
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2020.10.12.091

정보보안 정책 인식과 정보보안 관여성, 준수 의도성이 정보보안 행동에 미치는 영향 분석: 보상 차원과 공정성 차원을 중심으로

허성호[1], 황인호[2*]
[1]중앙대학교 심리학과 강사, [2]국민대학교 교양대학 조교수

Analysis of the Effects of Information Security Policy Awareness, Information Security Involvement, and Compliance Behavioral Intention on Information Security behavior : Focursing on Reward and Fairness

Sung-ho Hu[1], In-ho Hwang[2*]
[1]Lecturer, Department of Psychology, Chung-Ang University
[2]Assistant Professor, Department of General Education, Kookmin University

요 약 본 연구의 목적은 정보보안 정책 인식, 정보보안 관여성, 준수 의도성이 정보보안 행동에 미치는 영향력을 분석하는 것이다. 연구 방법은 보상 차원과 공정성 차원의 교차설계로 구성되었고, 조직적인 차원의 정책이 개인의 의사결정 수준에서 발생하는 정보처리 단계를 통해 정보보안 준수의도로 나타나는 과정에 주안점을 두었다. 연구 결과, 보상 차원은 준수 의도성에 유의미한 영향을 미치고 있었으며, 심리적 조건의 영향력이 물질적 조건보다 더 큰 것으로 나타났다. 공정성 차원은 정보보안 정책 인식, 정보보안 관여성, 정보보안 행동에 유의미한 영향을 미치고 있었으며, 형평성 조건의 영향력이 동등성 조건보다 더 큰 것으로 나타났다. 결과적으로 도출한 결과 모형은 측정변인으로 재구성된 복합 매개모형으로 확인되었고, 개인과 조직의 문화적 환경에 의한 시너지 관점에서 필요한 연구 방향을 논의하였다.

주제어 : 개인유의성, 조직수단성, 정보보안 정책 인식, 정보보안 관여성, 준수 의도성, 정보보안 행동

Abstract The aim of this study to assess the effect of information security policy awareness, information security involvement, compliance behavioral intention on information security behavior The research method is composed of a cross-sectional design of reward and fairness. This paper focuses on the process of organizational policy on the information security compliance intention in the individual decision-making process. As a result, the reward had a significant effect on compliance behavioral intention, and it was found that influence of the psychological reward-based condition was greater than the material reward-based condition. The fairness had a significant effect on information security policy awareness, information security involvement, information security behavior, and it was found that influence of the equity-based condition was greater than the equality-based condition. The exploration model was verified as a multiple mediation model. In addition, the discussion presented the necessary research direction from the perspective of synergy by the cultural environment of individuals and organizations.

Key Words : Valence, Instrumentality, Information security policy awareness, Information security involvement, Compliance behavioral intention, Information security behavior

* This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2018R1D1A1B07050305)

*Corresponding Author : In Ho Hwang(hwanginho@kookmin.ac.kr)

Received November 7, 2020
Revised December 6, 2020
Accepted December 20, 2020
Published December 28, 2020

1. 서론

최근 Covid 19와 같은 주변환경의 변화와 더불어 스마트워크 개념이 산업조직에 도입되어 확산되기 시작하면서, 조직의 내부자에 의한 정보보안 사건사고의 위협은 더욱 늘어나고 있는 실정이다[1-3]. 즉, 휴대 기술 디바이스 도입 및 활용을 통한 업무의 생산성 향상 추구는 조직구성원들의 핵심 정보 접근을 더욱 다양한 채널과 공간을 활용하여 근접하도록 허용하고 있기때문에, 조직의 구성원들에 의한 보안 사고 위협의 가능성이 적지 않은 것으로 사료된다[3-5].

2020년 정보보안 침해 보고서에 의하면, 정보보안 사고는 특성상 발생하더라도 잘 드러나지 않는 경향성이 있으며, 실질적으로는 전 세계적으로 매우 높은 수준으로 지속인 발생건 수가 증가하고 있는 것으로 나타났다[6]. 구체적으로는, 조직의 보안 사고가 매년 60~70% 정도가 해킹이나 멀웨어 등과 같은 외부의 침입 요소에 인해 발생하고 있으며, 조직 내부자에 의한 사고는 매년 20~30% 정도 발생하는 것으로 나타났다. 실제, 2019년의 경우 정보보안 사고 유형 중에 20% 이상이 권한이 부여된 사용자(user)의 오용(misuse)에 인해 발생한 것으로 나타났으며, 정보보안 사고 중에 30% 이상은 내부자에 인한 사고인 것으로 나타났다[6].

결과적으로, 산업 조직에서 보유한 정보의 가치가 조직의 중요한 자산의 의미하는 시대가 되면서, 산업 조직들은 필연적으로 자사의 핵심 정보를 보호하기 위해 다양한 노력을 기울이는 상황으로 접어들었다[7]. 실제로, 전세계적으로 나타나는 정보보안에 관련되는 시장성은 지난 2005년부터 2019년까지 약 30배 이상으로 성장하였고, 2022년에는 1,330억 달러를 훨씬 넘어 설것으로 추정하고 있다[6,7].

반면, 조직의 구성원들이 정보보안 준수 행동을 개선하기 위해서는 개인의 심리적 결정 과정에서 이루어지기 때문에, 개인을 둘러싼 다양한 조직 내부의 환경적 특성의 영향을 받게 된다[8]. 즉, 조직구성원의 정보보안 준수 행동에 긍정적인 영향을 주는 조직 환경 요인이 있을 수 있으며, 개인은 자신에게 주어진 다양한 특성을 종합적으로 고려하여 보안 행동 수준을 결정할 것이다. 하지만, 정보보안 준수의도에 영향을 주는 조직의 환경적 특성이나 구조를 제시하는 것이 중요함에도 불구하고 지금까지 조직 구성원의 정보보안 준수의도와 관련된 연구들은 동기 형성에 기여하는 기술적 요소에 초점을 맞추고 있어서 조직차원에서 고민해야 할 개인 중심의 정보보안 요소 및 지원체계에 대한 연구는 매우 부족한 상황이다.

정보보안은 인간의 일상 활동을 비롯하여 특정한 정보를 다루는 업무를 관여할 때, 분명히 감안해야 하는 필수적인 정보문화의 관점으로 이해할 수 있다[8]. 연구 관련 차원은 보편적으로 보안 기술을 수립하는 측면과 인간의 요소를 개선하는 차원으로 구분할 수 있다. 많은 연구 쟁점은 보안 설정을 제한하는 보안의 기술 영역을 처리하기 때문에, 인증절차 같은 측면에서 관련 내용들이 팽창하고 있다.

그렇지만, 근래 들어 인간 요소의 특성에 의한 정보보안 정책 관점의 사례에 관심을 두어야 한다는 의견이 높아지고 있다[1,2]. 그 까닭은 결과적으로 시스템을 활용하는 당사자 변인에 의해 일어나는 보안 정책 사고 내용이 꾸준히 확산되고 있기 때문이다. 이러한 측면에서 본 연구 수행에서는 인간 요소의 영역을 조절하는 관점의 연구적 필요성을 제시하며, 주요한 핵심 관련 변인을 구조화하여 정보보안 과정에 관여하는 영향을 분석하고자 한다.

2. 이론적 배경

조직구성원 관점에서 정보보안에 대한 여러 가지 선행 연구들을 보면 인간의 심리적 관점에서 개인 수준의 정보보안 특성을 고려해야 한다고 강조하고 있다. 예를 들어, 일반억제이론(general deterrence theory)은 조직의 보상성과 개인의 정보보안 미준수 성향에 대하여 명확한 제재를 보여주는 것은 정보보안 준수 행동에 큰 영향을 준다는 연구 결과를 제시하고 있으며[9], 예방동기이론(protection motivation theory)은 보상성과 정보보안 준수 의도성을 강화시키기 위해 명확한 공포 자극의 메시지가 개인의 태도 및 행동에 영향을 주는 결과를 바탕으로 다양한 확장형 연구가 병행되는 분위기를 조성하였다[10]. 또한, 계획된 행동이론(theory of planned behavior)과 공정성이론(justice theory)을 응용하여 조직구성원이 정보보안을 준수해야 하는 개인 수준의 행동 원천 소재를 찾는 연구가 진행되었다[11,12]. 최근에는 스트레스에 관한 연구적 관점이 증가하면서 정보기술의 측면인 기술스트레스 특성이 정보보안 분야에 적용되는 연구들이 나타나고 있다[12,13]. 이와 같은 선행연구들을 보면, 조직의 구성

원들이 정보보안 준수 행동을 향상시킬 수 있는 주요 요인들을 다양한 이론을 통해 개인의 측면에서 조직의 업무 환경에 적합한 전략을 제시하였다는 공통된 시사점을 가진다.

2.1 의사결정 구조

인지적 의사결정 특성은 보통 내부적 영역과 외부적 영역으로 구분해 볼 수 있다[14,15]. 내부적 영역은 사람의 성격적 특질로 인해 주도적인 의사결정이 나타나는 경향을 가리키며, 외부적 영역은 문화적 특질로 인해 주도적인 의사결정이 나타나는 경향을 의미한다. 예를 들자면, 보안 정책 운영의 측면에서도 개인의 입장에서 보안 정책 운영을 참작하여 그에 타당한 보안 행동을 실천하는 경우가 있으며, 개인이 속해 있는 공동체에서 지시하는 보안 정책 관점의 행동 지침과 같은 특정 제도의 영향을 받아 조직의 입장에서 보안 정책 운영을 참작하여 그에 타당한 보안 행동을 실천하는 경우도 나타날 수 있다.

인간이 갖는 내부적 영역의 특징들은 다양할 수 있으며, 보안 정책의 장면에서는 실증적 의사결정 과정보다 휴리스틱 의사결정 적절성을 더 타당하게 분석하고 있다. 왜냐하면, 담당자의 측면에서는 정보보안 준수와 직무의 상호작용 측면에서 어느 정도 병행할 수 없는 특성이 발생하고, 정보보안 기술이 확대되면서 보안 정책의 이런 특성의 딜레마적인 문제가 증대되고 있기 때문이다. 보상 차원은 이런 휴리스틱 특성을 응용한 변수라고 이해할 수 있고, 정보보안의 측면에서 파악할 때, 인간요소의 내부적 영역으로 설명할 수 있다[14-16].

개인의 외부적 영역의 특징들은 조직문화의 맥락에서 접근할 수 있다. 즉, 집단이 추구하는 문화적 측면을 고려하였을 때, 조직문화는 조직 집단에 관여하는 수많은 개인 구성원들에게 영향을 미칠 수 있다. 하지만, 보안 정책 운영의 조건에서 집단이 당연히 강조할 수밖에 없는 규정이라고 할 지라도 개인 수준의 준수행동을 전부 통제하기는 매우 힘들다. 그러므로 조직단체는 전략적으로 조직문화를 조성하여 개별 구성원들에게 정보보안 준수행위를 이끌어 내는 해결책을 검토하게 되었다. 정보보안의 조직문화는 조직 상황의 개념으로 접근하는 것이 적절하며, 동등성과 형평성으로 구분하는 접근방식은 상당히 의미 있는 문화차원의 사례라고 볼 수 있다[17].

2.2 정보보안 동기화 과정

조직 관점에서 정보보안 정책의 효과를 개선하기 위해서는 가장 일차적으로 조직원의 내재적인 단계에서 정보보안의 정책을 명확하게 지각하는 것이 필요하다. 왜냐하면 이 단계는 행동 수행의 깊은 곳에서 비롯되는 동기의 요소를 자극하기 때문이다. 정보보안 정책 인식이 언급되는 경향성은 곧 이러한 이유 때문이다. 그렇기 때문에, 집단이 정보보안 운영 정책을 준비하고 실시하는 절차 속에서 우선 일차적으로 기대하는 효과는 조직 구성원의 정보보안 정책 인식을 향상시키는 것이다[18].

조직이 수립한 보안 정책의 핵심은 단지 정보보안 정책 인식을 높이는 것으로 끝난 것이 아니다. 실질적인 정보보안의 준수행동으로 단계적인 영향력을 확보하기 위해서는 개인추구성향의 정보보안 관여성과 준수 의도성이 개선되어야 한다[19,20]. 이것은 실질적인 정보보안 준수행동으로 주된 영향을 끼치는 꾀 인접한 매개 요소이며, 전체적으로 그 조직에서 활동하는 조직원의 정보보안 행동수준을 개선시키는데 필요한 정보보안의 변인이라고 볼 수 있다[9-11,19,20].

아울러, 정보보안의 태도와 행동 단계에서 정보보안 관련 정책의 실제적인 영향력을 평가하는 작업은 아주 결정적이다. 조직 구성원의 태도와 행동 전반을 설명하는 통상적인 정보보안 관련 이론의 측면에서도 조직이 주도하는 정보보안 정책의 핵심적인 실효성을 밝히기 위해서는 의도성 및 행위 수준에서 확인되는 분석적 결과들을 근거로 입증하는 것이 매우 적당하다는 입장이 대다수이다[21].

따라서 본 탐색 연구에서는 정보보안의 핵심 정책으로 기대할 수 있는 실제적인 확산 효과를 분석하기 위해 조직이 실시하는 현실적인 정보보안 절차 속에서 드러나는 평정 결과 자료를 기준으로 정보보안 정책의 핵심적인 효과를 규명할 것이다. 정보보안 정책의 효과는 정보보안 정책 인식, 정보보안 관여성, 준수 의도성, 그리고 정보보안 행동으로 작성된 문항들을 활용하여 측정할 것이며, 연구 결과를 융합하여 설명구조에 적합한 분석모형을 검증하고자 한다.

3. 연구방법

3.1 연구대상

본 연구에서는 정보보안 정책에서 인간의 행동 요소에 관심을 가지는 조사 연구이며, 연구대상자들은 일상적으로 보안 관련 정책의 영향권에 있는 직무를 진행하고 있으며, 적어도 보안 정책 운영의 개념을 인식하고 있는 성인이다. 자료를 모으는 절차에서 남성 154명(평균 연령 29.54세), 여성 167명(평균 연령 27.78세), 총 321명(평균 연령 28.63세)의 자료를 무작위 방식으로 수집하였으며, 최종적으로 321개의 자료를 연구분석에 응용하였다.

3.2 측정도구

본 연구에서는 내부적 영역에 해당하는 개인유의성의 개념(Valence)과 외부적 영역에 해당하는 조직수단성의 개념(Instrumentality), 두 차원으로 분류하여 교차방안(cross over design)을 검증하였다. 정보보안의 동기화 과정을 분석하기 위해 정보보안 정책 인식(Information Security Policy Awareness), 정보보안 관여성(Information Security Involvement), 준수의도성(Compliance Behavioral Intention), 정보보안 행동(Information Security Behavior)으로 구성된 변인들을 측정했고, 변인 간의 상호적 특징을 감안하여 평균차이검증, 일반선형 변량분석, 모형검증에 사용하였다. 아울러, 분석 과저에서는 SPSS 26.0을 사용했다.

3.2.1 보상 차원과 공정성 차원

보상 차원은 개인유의성의 개념에 해당하며, 개인들이 지향하는 의사결정 절차의 핵심적인 단서가 물질적의 내용인지 또는 심리적의 내용인지를 입력한 변수이다. 공정성 차원은 조직수단성의 개념에 해당하며, 조직문화의 특성이 지향하는 의사결정 절차의 핵심적인 단서가 동등성과 관련된 내용인지 또는 형평성과 관련된 내용인지를 입력한 변수이다.

3.2.2 정보보안 정책 인식(Information Security Policy Awareness)

정보보안 정책 인식의 변수는 조직이 마련한 정보보안 정책에 대하여 인식하고 있는 정도를 뜻한다[12]. 자료 수집에 활용한 측정 도구는 7개의 질문으로 재구성된 태도 측정 변수이며, 연구 조건에 맞게 보강하여 조사 설문지로 제작하였다. 척도의 크기는 7점 리커트 방식으로 사용했으며, 이 측정도구의 문항간 신뢰도(Chrombach' α)는 .74 로 나타났다.

3.2.3 정보보안 관여성(Information Security Involvement)

정보보안 관여성의 변수는 정보보안 정책에 대하여 주도적으로 관여하고자 하는 의지의 정도를 뜻한다[10]. 자료 수집에 활용한 측정 도구는 6개의 질문으로 재구성된 태도 측정 변수이며, 연구 조건에 맞게 보강하여 조사 설문지로 제작하였다. 척도의 크기는 7점 리커트 방식으로 사용했으며, 이 측정도구의 문항간 신뢰도(Chrombach' α)는 .86 로 나타났다.

3.2.4 준수 의도성(Compliance Behavioral Intention)

준수 의도성의 변수는 조직이 추진하는 정보보안 정책에 대하여 얼마나 동조하여 수용할 것인가의 정도를 뜻한다[9]. 자료 수집에 활용한 측정 도구는 4개의 질문으로 재구성된 태도 측정 변수이며, 연구 조건에 맞게 보강하여 조사 설문지로 제작하였다. 척도의 크기는 7점 리커트 방식으로 사용했으며, 이 측정도구의 문항간 신뢰도(Chrombach' α)는 .71 로 나타났다.

3.2.5 정보보안 행동(Information Security Behavior)

정보보안 행동은 정보보안 행동의 변수는 실제로 조직 환경에서 실천하는 구체적인 수준의 정보보안 행동의 정도를 뜻하며, 비밀번호 관리, 업데이트 패치, 안티바이러스 프로그램 사용, usb 사용 관리, 쿠키 처리, 스팸메일 처리, 호환성 웹페이지 관리의 7가지 행동으로 구성되어 있다[11]. 자료 수집에 활용한 측정 도구는 7개의 질문으로 재구성된 태도 측정 변수이며, 연구 조건에 맞게 보강하여 조사 설문지로 제작하였다. 척도의 크기는 7점 리커트 방식으로 사용했으며, 이 측정도구의 문항간 신뢰도(Chrombach' α)는 .86 로 나타났다.

3.3 연구 모델 및 가설

본 연구에서 분석에 초점을 맞춘 모형은 정보에서는 연구모형으로 매개모형을 제시하였고, 위계적 회귀분석을 통해 효과성을 검증하였고(Fig 1),

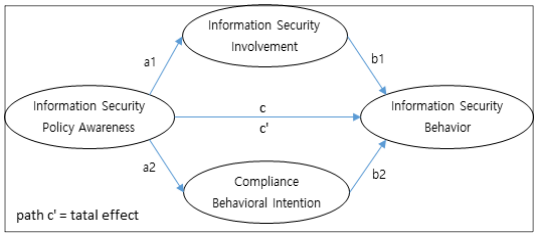

Fig. 1. research model

지금까지의 내용을 종합하여 본 연구는 다음과 같은 가설을 수립하였다.

H1 : 정보보안 정책 인식이 높을수록 정보보안 관여성이 높을 것이다.

H2 : 정보보안 정책 인식이 높을수록 준수 의도성이 높을 것이다.

H3 : 정보보안 정책 인식이 높을수록 정보보안 행동이 향상될 것이다.

H4 : 정보보안 관여성이 높을수록 정보보안 행동이 향상될 것이다.

H5 : 준수 의도성이 높을수록 정보보안 행동이 향상될 것이다.

4. 연구결과

4.1 기초 통계 분석 결과

본 연구의 대상자 성향을 보상 차원, 공정성 차원, 그리고 성별의 세 가지 범주로 분류하여 분포 성향을 확인하였다. 보상 차원의 범주에서 0.31% 정도 분포의 차이가 있었고, 공정성 차원의 범주에서 17.76% 정도 분포의 차이가 있었고, 성별의 범주에서 4.05% 정도 분포의 차이가 있었다. 따라서 각 분포의 비율을 고려했을 때, 치명적인 편향이 확인되지 않았다고 할 수 있다.

Table 1. participants distribution

reward	fairness	sex		total
		male	female	
material	equality	39(42.39%)	53(57.61%)	92(100.00%)
	equity	42(60.87%)	27(39.13%)	69(100.00%)
	total	81(50.31%)	80(49.69%)	161(100.00%)
psychological	equality	17(42.50%)	23(57.50%)	40(100.00%)
	equity	56(46.67%)	64(53.33%)	120(100.00%)
	total	73(45.63%)	87(54.38%)	160(100.00%)
total	equality	56(42.42%)	76(57.58%)	132(100.00%)
	equity	98(51.85%)	91(48.15%)	189(100.00%)
	total	154(47.98%)	167(52.02%)	321(100.00%)

연구대상자들의 학력은 고졸 이하 20명(6.2%), 대졸 이하 241(73.2%), 대학원졸 이하 66명(20.6%)이었다. 직업은 공무원 87명(27.1%), 은행원 84명(26.2%), 일반사무직 74명(23.1%), 전문가 46명(14.3%), 개인사업자 및 기타 30명(9.3%) 의 비율로 나타났다. 이들의 활동 중에 정보 보안과 관련되는 영역은 정보 수집 자료 103건(32.1%), 이메일 활동 77건(24.0%), sns 활동 72건(22.4%), 거래정보 40건(12.5%), 보고서자료 29건(9.0%)의 비율로 나타났다.

4.2 교차분석 결과

본 분석에서는 연구참여 대상자들이 응답 자료를 응용하여 보상 차원과 공정성 차원이 혼합된 상태에서 정보보안의 동기화 과정을 탐색하기 위해 변량분석(ANOVA) 기법을 응용하였다. 다시 말한다면, 보상 차원과 공정성 차원의 교차설계방안에서 교차방안이 정보보안 정책 인식, 정보보안 관여성, 준수 의도성, 정보보안 행동에 미치는 효과성을 탐색적으로 확인하였다.

첫째, 보상 차원(reward), 공정성 차원(fairness) 변인이 정보보안 정책 인식(Information Security Policy Awareness)에 미치는 영향을 변량분석으로 검증하였고(보상 차원(2)×공정성 차원(2)), 그 결과는 다음과 같다.

보상 차원 변인에서 물질적 집단(M = 5.69)이 심리적 집단(M = 5.84)보다 정보보안 정책 인식의 평균이 더 낮은 것으로 나타났다. 그러나 보상 차원 변인이 정보보안 정책 인식 변인에 미치는 영향력($F(1, 317) = 0.47$, n.s.)은 통계적으로 유의하지 않은 것으로 나타났다.

공정성 차원 변인에서 동등성 집단(M = 5.6)이 형평성 집단(M = 5.88)보다 정보보안 정책 인식의 평균이 더 낮은 것으로 나타났다. 그리고 공정성 차원 변인이 정보보안 정책 인식 변인에 미치는 영향력($F(1, 317) = 5.41$, $p < 0.05$)은 통계적으로 유의한 것으로 나타났다.

보상 차원 변인과 공정성 차원 변인의 상호작용($F(1, 317) = 0.00$, n.s.)은 통계적으로 유의하지 않은 것으로 나타났다.

Table 2. ANOVA of Information Security Policy Awareness

variables	SS	df	MS	F
reward(R)	0.39	1	0.39	0.47
fairness(F)	4.49	1	4.49	5.41*
R × F	0.00	1	0.00	0.00

* p 〈 0.05

둘째, 정보보안 관여성(Information Security Involvement)에 미치는 영향을 변량분석으로 검증하였고, 그 결과는 다음과 같다.

보상 차원 변인에서 물질적 집단(M = 4.27)이 심리적 집단(M = 4.34)보다 정보보안 관여성의 평균이 더 낮은 것으로 나타났다. 그러나 보상 차원 변인이 정보보안 관여성 변인에 미치는 영향력(F(1, 317) = 0.27, n.s.)은 통계적으로 유의하지 않은 것으로 나타났다.

공정성 차원 변인에서 동등성 집단(M = 4.05)이 형평성 집단(M = 4.49)보다 정보보안 관여성의 평균이 더 낮은 것으로 나타났다. 그리고 공정성 차원 변인이 정보보안 관여성 변인에 미치는 영향력(F(1, 317) = 10.12, p 〈 0.01)은 통계적으로 유의한 것으로 나타났다.

보상 차원 변인과 공정성 차원 변인의 상호작용(F(1, 317) = 0.01, n.s.)은 통계적으로 유의하지 않은 것으로 나타났다.

Table 3. ANOVA of Information Security Involvement

variables	SS	df	MS	F
reward(R)	0.39	1	0.39	0.27
fairness(F)	14.67	1	14.67	10.12**
R × F	0.01	1	0.01	0.01

** p 〈 0.01

셋째, 준수 의도성(Compliance Behavioral Intention)에 미치는 영향을 변량분석으로 검증하였고, 그 결과는 다음과 같다.

보상 차원 변인에서 물질적 집단(M = 4.90)이 심리적 집단(M = 5.29)보다 준수 의도성의 평균이 더 낮은 것으로 나타났다. 그리고 보상 차원 변인이 준수 의도성 변인에 미치는 영향력(F(1, 317) = 6.45, p 〈 0.05)은 통계적으로 유의한 것으로 나타났다.

공정성 차원 변인에서 동등성 집단(M = 5)이 형평성 집단(M = 5.16)보다 준수 의도성의 평균이 더 낮은 것으로 나타났다. 그러나 공정성 차원 변인이 준수 의도성 변인에 미치는 영향력(F(1, 317) = 0.16, n.s.)은 통계적으로 유의하지 않은 것으로 나타났다.

보상 차원 변인과 공정성 차원 변인의 상호작용(F(1, 317) = 1.21, n.s.)은 통계적으로 유의하지 않은 것으로 나타났다.

Table 4. ANOVA of Compliance Behavioral Intention

variables	SS	df	MS	F
reward(R)	8.03	1	8.03	6.45*
fairness(F)	0.19	1	0.19	0.16
R × F	1.50	1	1.50	1.21

* p 〈 0.05

넷째, 정보보안 행동(Information Security Behavior)에 미치는 영향을 변량분석으로 검증하였고, 그 결과는 다음과 같다.

보상 차원 변인에서 물질적 집단(M = 5.41)이 심리적 집단(M = 5.67)보다 정보보안 행동의 평균이 더 낮은 것으로 나타났다. 그러나 보상 차원 변인이 정보보안 행동 변인에 미치는 영향력(F(1, 317) = 0.73, n.s.)은 통계적으로 유의하지 않은 것으로 나타났다.

공정성 차원 변인에서 동등성 집단(M = 5.27)이 형평성 집단(M = 5.73)보다 정보보안 행동의 평균이 더 낮은 것으로 나타났다. 그리고 공정성 차원 변인이 정보보안 행동 변인에 미치는 영향력(F(1, 317) = 14.18, p 〈 0.01)은 통계적으로 유의한 것으로 나타났다.

보상 차원 변인과 공정성 차원 변인의 상호작용(F(1, 317) = 1.21, n.s.)은 통계적으로 유의하지 않은 것으로 나타났다.

Table 5. ANOVA of Information Security Behavior

variables	SS	df	MS	F
reward(R)	0.68	1	0.68	0.73
fairness(F)	13.16	1	13.16	14.18**
R × F	1.12	1	1.12	1.21

** p 〈 0.01

4.2 연구모형 분석 결과

우선, 정보보안 정책 인식이 정보보안 관여성을 거쳐 정보보안 행동을 설명하는 매개모형을 검증하였다. 정보보안 정책 인식이 정보보안 행동에 미치는 전체적인 영향력은 통계적으로 유의한 것으로 나타났으며(경로 c'; β = 0.24, p 〈 0.01; 가설 3 채택), 정보보안 정책 인식이 정보보안 관여성에 미치는 영향력(경로 a1; β =

0.25, p 〈 0.01; 가설 1 채택)과 정보보안 관여성이 정보보안 행동에 미치는 직접적인 영향력(경로 b1; β = 0.33, p 〈 0.01; 가설 4 채택)은 모두 통계적으로 유의한 것으로 나타났다. 또한, 정보보안 정책 인식이 정보보안 행동에 미치는 직접적인 영향력은 통계적으로 유의하지 않은 것으로 나타났다(경로 c; β = 0.06, n.s.).

두번째로, 정보보안 정책 인식이 준수 의도성을 거쳐 정보보안 행동을 설명하는 매개모형을 검증하였다. 정보보안 정책 인식이 정보보안 행동에 미치는 전체적인 영향력은 동일하며, 정보보안 정책 인식이 준수 의도성에 미치는 영향력(경로 a2; β = 0.3, p 〈 0.01; 가설 2 채택)과 준수 의도성이 정보보안 행동에 미치는 직접적인 영향력(경로 b2; β = 0.33, p 〈 0.01; 가설 5 채택)은 모두 통계적으로 유의한 것으로 나타났다. 또한, 정보보안 정책 인식이 정보보안 행동에 미치는 직접적인 영향력 또한 동일하다. 다중공선성을 검증하기 위해 해당경로에 대하여 각각 VIF 값을 산출하였고, 모두 공선성이 나타나지 않았다(b1=1.14, b2=1.19, c=1.12).

Table 6. Hierarchical regression analysis of mediation model

step		path	beta	가설
0 step(c′ path)		ISPA→ISB	0.24**	채택
1-1 step(a path)	a1	ISPA→ISI	0.25**	채택
	a2	ISPA→CBI	0.30**	채택
1-2 step(b path)	b1	ISI→ISB	0.33**	채택
	b2	CBI→ISB	0.33**	채택
2 step(c path)		ISPA→ISB	0.06	-

※ Information Security Policy Awareness : ISPA, Information Security Involvement : ISI, Compliance Behavioral Intention : CBI, Information Security Behavior : ISB

아울러, 두 가지 경로로 구조화된 이중 매개효과의 유효성을 검증하기 위해 Sobel 검증을 실시하였고, 그 결과 매개효과가 통계적으로 유의한 것으로 나타났다 (Z = 1.92, p 〈 .05).

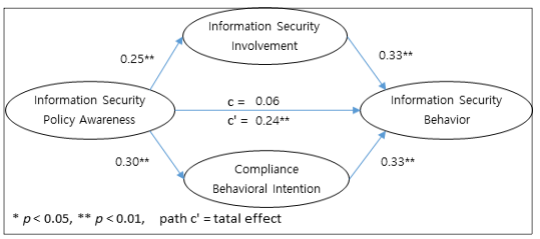

Fig. 2. Multiple process mediation model

따라서 본 연구모형은 이중 복합모형으로 설명할 수 있으며, 정보보안의식이 정보보안 행동으로 이어지는 과정에서 대처효능감과 준수의향이 매개하는 역할을 하고 있는 것을 확인할 수 있다. 아울러 다음의 몇 가지의 논의점을 추론할 수 있다.

첫째, 주효과 분석 결과에서 공정성 차원의 영향력이 정보보안 정책 인식, 정보보안 관여성, 정보보안 행동 특성을 유의미하게 향상시킨다는 결과들을 밝혀냈다. 그리고 지금 현재 등장하는 4차 산업혁명의 특정 분위기를 고려한다면 이 다음 우리 사회가 필요로 하는 다양한 정보문화 혁신 속에 인간이 있다는 핵심을 수용해야 한다.

둘째, 분석된 결과를 기반하여 보안 정책의 방향을 강구하기 위해서는 보상 차원의 조건에서 예상할 수 있는 주요 성과를 밝히기 위해 준수 의도성 등에 해당하는 정보 관련 태도 보완 기법을 확립하는 것이 매우 중요하다점이 나타났다.

셋째, 정보보안 정책 인식은 정보보안 관여성과 준수 의도성의 다차원 구조의 매개모형을 통해 정보보안 행동에 효력을 작용하는 구조모형으로 밝혀졌다.

5. 결론

지금까지의 연구 결과를 토대로 학술적, 정책적, 교육적 논의점을 요약하면 다음과 같다.

첫째, 학술적으로 이 연구 과정의 관점은 기존 보안 관련 정책 접근 관점과 비교한다면, 보안 기술 체제와 관여되는 기능적 속성의 제재 관점에 주목한 연구라기보다 통제 설정을 활용하는 인간의 요소를 향상시키는 방안에 중점을 둔 연구라는 점에서 연구의 차별성을 찾는다. 예컨대, 탁월한 규격으로 설치된 보안 기술을 반영하여 정보보안에 해당하는 형태로 정보보안 시스템에 적용하더라도, 사람들이 정보보안 규정을 수용하지 않게 되면 아주 치명적인 위험을 발생시킬 수가 있다. 따라서 정보보안 정책이 필요한 집단에서는 본 연구 과정이 주안점을 두는 인간 요소의 정보보안 전략에 적합한 교육방식을 고려하여 문제없이 보안 행동 방식을 보강할 수 있도록 현실적인 대응 분위기를 확보해야 될 것으로 판단된다[2,23].

둘째, 정보보안의 정책적 측면에서 공정성 차원을 고려했을 때, 정보보안의 방향도 인간 요소의 전략이 적용된다면 일부 정보보안 정책 인식, 정보보안 관여성,

정보보안 행동 측면에서 두드러지는 변화들이 수용될 것이다. 이 결과들은 공정성 차원에 해당하는 개인 특성의 중요한 증거가 될 수 있다는 관점에서 명백한 현실적 가치를 제공한다. 고로 보안 체계에 있어서 구축 절차에는 공정성 차원을 응용하여 정보보안 정책 인식, 정보보안 관여성, 정보보안 행동을 강화할 수 있는 정책의 활용이 반드시 필요하다.

셋째, 이제, 4차 산업혁명의 변화로 나타나는 주요 특성을 참작한다면 앞으로의 한국의 미래 사회가 기대하는 다차원적인 정보문화 변혁 속에 우리가 있다는 중요한 사실을 직면해야 한다[24]. 따라서 보안 정책의 교육 방향도 인간 요소가 도입된 전략이 개발된다면 일부 준수 의도성 개념에서 확인되는 변화가 수용되어야 할 것이다[25]. 또한, 교육제도의 측면에서도 이 사실을 적용하여 추진한다면, 정보보안 정책 방안에 보상 차원을 고려하여 정책 체제를 재편성하여 준수 의도성을 강화할 수 있는 교육제도의 마련이 꼭 필요하다.

넷째, 연구모형을 토대로 정책제도의 방향을 고려한다면, 탐색구조의 상대적인 위상을 분리하여 비교하여 정보보안 관여성과 준수 의도성은 각자 '개인추구성향'과 '조직동조성향'의 측면으로 구분하여 설명하는 양분 특성에 주목해야 한다. 따라서, 매개효과의 모델에 부합하는 핵심 특성을 양분하여 정보보안 정책 운영에 도입해야 하며, 두 측면의 핵심 특성을 고려하여 기관의 상황에 적합한 보안 정책 체제를 구조적으로 적용하는 전략적 추진이 필요하다.

끝으로, 본 연구는 연구참여자의 독특한 개별적 특징을 생각하지 못한 점이 제한점이라고 말 할 수 있다. 동시에, 보안 정책 관련 연구 모형을 인간 요소의 관련 특성에 초점을 두고 조사를 실시하는 중 업종 성향을 숙고한다면, 더욱 타당한 연구적 가치를 도출할 수 있을 것이라고 평가된다[2]. 결론적으로, 현실타당성을 향상시키는 후속연구가 촉구되고, 다양한 인간 요소의 변인과 문화적 환경의 시너지 기능을 여러 가지 구조에서 검증하는 분석의 필요성을 제안한다.

REFERENCES

[1] B. Khan, K. S. Alghathbar, S. I. Nabi & M. K. Khan. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management, 5(26)*, 10862-10868. DOI : 10.5897/AJBM11.067

[2] R. W. Lee, I. H. Hwang & S. H. Hu. (2017). Exploratory research of information security strategy focused on human factors. *The Journal of General Education, 6*, 103-124.

[3] J. D'Arcy & P. L. Teh. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management*, *56(7)*, 103151. DOI : 10.1016/j.im.2019.02.006.

[4] I. Hwang, R. Wakefield, S. Kim & T. Kim. (2019). Security awareness: The first step in information security compliance behavior. *Journal of Computer Information Systems*, 1-12. DOI : 10.1080/08874417.2019.1650676

[5] H. Lee & J. Kim. (2018). A convergence study on the structural relationships among emotional labor and work performance of information security professionals. *Journal of the Korea Convergence Society*, *9(1)*, 67-74. DOI : 10.15207/JKCS.2018.9.1.067.

[6] Verizon. (2020). *2020 data breach investigations report*.

[7] Grandviewresearch. (2019). *Cyber security market size, share & trends analysis report by component, by security type, by solution, by service, by deployment, by organization, by application, and segment* Forecasts, 2019 - 2025. https://www.globenewswire.com.

[8] L. Tredinnick. (2008). *Digital information culture: the individual and society in the digital age*, Amsterdam : Elsevier.

[9] M. I. Merhi & P. Ahluwalia. (2019). Examining the impact of deterrence factors and norms on resistance to information systems security. *Computers in Human Behavior*, *92*, 37-46. DOI : 10.1016/j.chb.2018.10.031

[10 P. Van Schaik, K. Renaud, C. Wilson, J. Jansen, & J. Onibokun. (2020). Risk as affect: The affect heuristic in cybersecurity. *Computers & Security, 90*, 101651.

[11] S. Aurigemma & T. Mattson, (2017). Deterrence and punishment experience impacts on ISP compliance attitudes. *Information and Computer Security*, *25(4)*, 421-436. DOI : 10.1108/ICS-11-2016-0089.

[12] J. Cho, J. Yoo & J. I. Lim. (2019). An Impact Analysis of Information Security Professional's Job Stress and Job Satisfaction to Turnover

Intention: Moderation of Organizational Justice. *The Journal of Society for e-Business Studies, 24(3)*, 143-161.

[13] A. P. Getman, O. G. Danilyan, A. P. Dzeban, Y. Y. Kalinovsky, & Y. A. Hetman. (2020). Information security in modern society: Sociocultural aspects. *Amazonia Investiga, 9(25)*, 6-14.

[14] J. G. Paolillo & S. J. Vitell. (2002). An empirical investigation of the influence of selected personal, organizational and moral intensity factors on ethical decision making. *Journal of Business Ethics, 35(1)*, 65-74.

[15] M. L. Foulds. (1971). Changes in locus of internal-external control: A growth group experience. Comparative Group Studies, 2(3), 293-300.
DOI : 10.1177/104649647100200303

[16] J. Cameron & W. D. Pierce. (1994). Reinforcement, reward, and intrinsic motivation: A meta-analysis. *Review of Educational research, 64(3)*, 363-423.
DOI : 10.3102/00346543064003363

[17] E. A. Mannix, M. A. Neale & G. B. Northcraft. (1995). Equity, equality, or need? The effects of organizational culture on the allocation of benefits and burdens. *Organizational Behavior and Human Decision Processes, 63(3)*, 276-286.

[18] M. Siponen, S. Pahnila & M. A. Mahmood. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43(2)*, 64-71.
DOI : 10.1109/MC.2010.35

[19] P. Ifinedo. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51(1)*, 69-79.
DOI : 10.1016/j.im.2013.10.001

[20] E. Albrechtsen. (2007). A qualitative study of users' view on information security. *Computers & Security, 26(4)*, 276-289.
DOI : 10.1016/j.cose.2006.11.004

[21] A. E. Howe, I. Ray, M. Roberts, M. Urbanska & Z. Byrne, (2012). *The psychology of security for the home computer user*. IEEE.

[22] B. Bulgurcu, H. Cavusoglu & I. Benbasat. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly, 34(3)*, 523-548.

[23] S. H. Hu. (2020). Analysis of the impact of military organization's safety culture on safety behavior: Focusing on the mediating effect of safety leadership. *Journal of Advances in Military Studies, 3(2)*, 63-81.
DOI : 10.37944/jams.v3i2.70

[24] S. H. Hu. (2020). A comparative study on job orientation between enterprises and job seekers: Focusing on the recruitment process. *Journal of Digital Convergence, 18(7)*, 85-92.

[25] N. S. Safa, C. Maple, T. Watson & R. Von Solms. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of information security and applications, 40*, 247-257.
DOI : 10.1016/j.jisa.2017.11.001

허 성 호(Sung-ho Hu) [종신회원]

- 2004년 2월 : 홍익대학교 신소재공학과(공학사)
- 2006년 2월 : 중앙대학교 심리학과(문학석사)
- 2012년 8월 : 중앙대학교 심리학과(문학박사)
- 2016년 3월 ~ 현재: 한양대학교 산업융합대학원 겸임교수
- 관심분야 : 정보문화, 융합연구, 정보격차, 정보보안, 공동체, 채용경향 분야 등
- E-Mail : powerrcy@hanmail.net

황 인 호(In-ho Hwang) [정회원]

- 2004년 8월 : 건국대학교 경영학과(경영학사)
- 2007년 6월 : 중앙대학교 경영학과(경영학석사)
- 2014년 2월 : 중앙대학교 경영학과(경영학박사)
- 2020년 9월 ~ 현재: 국민대학교 교양대학 조교수
- 관심분야 : IT 핵심성공요인, 디지털 콘텐츠, 정보보안 및 프라이버시 분야 등
- E-Mail : hwanginho@kookmin.ac.kr