Journal of the Korea Convergence Society
Vol. 12. No. 1, pp. 211-218, 2021

ISSN 2233-4890 / eISSN 2713-6353
https://doi.org/10.15207/JKCS.2021.12.1.211

정보보안 의식과 대처 효능감, 준수의향이 정보보안 행동에 미치는 영향분석: 가용성 차원과 문화 차원을 중심으로

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

Analysis of the effects of Information Security Awareness, Response Efficacy, and Compliance Behavioral Intention on Information Security Behavior: Focursing on Availability and Culture

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 연구는 정보보안의 연구 중 인간 요소를 다루는 분야의 필요성이 제기되어 융합연구 설계방안을 구성하였다. 본 연구의 목적은 정보보안의 측면이 보안 정책과 연관되는 인지과정에 미치는 효과성을 검정하는 것이다. 연구 방법은 가용성 차원과 문화 차원의 교차설계로 구성되었고, 정보보안 과정은 정보보안 의식, 대처 효능감, 준수의향, 정보보안 행동의 네 가지 변인으로 측정되었다. 연구 결과, 가용성 차원은 대처 효능감에 유의미한 영향을 미치고 있었으며, 사례 중심 조건의 영향력이 통계중심 조건보다 더 큰 것으로 나타났다. 문화 차원은 정보보안 의식, 대처 효능감, 준수의향, 정보보안 행동에 유의미한 영향을 미치고 있었으며, 동질성 조건의 영향력이 다양성 조건보다 더 큰 것으로 나타났다. 결과적으로 제시한 연구 모형은 측정변인으로 재구성된 다원적 매개모형으로 검증되었다. 아울러, 논의는 개인 요소와 조직 특성을 고려한 정보보안 전략의 필요성에 대하여 기술하고 있다.

주제어 : 가용성 이론, 문화 이론, 정보보안 의식, 대처 효능감, 준수의향, 정보보안 행동

Abstract This study is composed of a convergence research design plan as the necessity of information security field dealing with human factors are raised. The purpose of this study is to analyze the effectiveness of the aspect of information security on the cognitive process related to security policy. The research method consisted of the cross-design of the availability dimension and the culture dimension, and the information security process was measured with information security awareness, response efficacy, compliance behavioral intention, and information security behavior. As a result of the study, the dimension of availability had a significant effect on response efficacy, and it was found that the influence of the case-based condition was greater than that of the statistics-based condition. The cultural dimension had a significant effect on information security awareness, response efficacy, compliance behavioral intention, and information security behavior, and the influence of the homogeneity condition was found to be greater than that of the diversity condition. The proposed research model was verified as a multiple mediation model reconstructed with measurement variables. In addition, the discussion describes the necessity of an information security strategy in consideration of individual factors and organizational characteristics.

Key Words : Availability theory, Culture theory, Information security awareness, Response efficacy, Compliance behavioral intention, Information security behavior

*This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (NRF-2018R1D1A1B07050305).
*Corresponding Author : In-ho Hwang(hwanginho@kookmin.ac.kr)
Received November 4, 2020 Revised December 30, 2020
Accepted January 20, 2021 Published January 28, 2021

1. 서론

최근 정보보안 연구는 산업환경의 변화와 더불어 고도화된 스마트워크 개념이 조직문화에 도입되어 확산되면서, 조직의 내부 구성원에 의한 정보보안 위협 사건사고의 비율이 늘어나고 있는 실정이다[1]. 예컨대, 고도의 기술 장비들이 도입되고 이 장비들을 활용하여 업무의 생산성을 향상시키지만, 조직구성원들의 핵심 정보가 노출 될 수 있는 채널과 공간 역시 증가하면서 위험접근 허용 건수가 증가하고 있다[2-4]. 이러한 이유 때문에, 조직을 이루는 구성원들에 의한 정보보안 사건사고의 발생 가능성이 적지 않은 것으로 분석된다[1-3].

즉, 2020년 정보보안에 관한 보안 침해 보고서를 보면, 정보보안 관련 사고는 발생하더라도 공개되는 경우가 적은 특성이 있으며, 실제적으로 전 세계적에서는 매우 높은 수준으로 지속인 증가 추세로 나타나는 것으로 밝혀졌다[4]. 구체적으로는, 조직의 정보보안 사건은 매년 60~70% 정도가 해킹 및 멀웨어 등과 같은 외부 요소의 침입에 의해 발생하고 있으며, 상대적으로 조직 내부의 구성원에 의한 사건은 매년 20~30% 정도로 발생되는 것으로 집계되었다. 그리고 2019년의 경우 사고 유형들 중에 20% 이상은 권한이 부여된 사용자(user)의 잘못된 오용(misuse)에 인해 발생하는 것으로 밝혀졌으며, 이 보안 사고들 중에 30% 이상은 조직의 내부 구성원들에 의한 사고인 것으로 밝혀졌다[4]. 하지만, 기존의 연구들은 대다수 기술적인 영역에만 치중하고 있으며, 인간 요소에 대한 영역을 까다롭다는 이유로 상대적으로 연구 진행이 부족한 것이 사실이다[1-4]. 이에, 본 연구의 관점은 이러한 연구영역에 초점을 맞추어 기존의 연구와 차별성을 가진다고 할 수 있다.

결과적으로, 산업 안전 환경의 측면에서 조직이 소유하는 정보의 가치가 조직과 그 구성원의 중요한 자산을 의미하는 시대가 되면서, 다양한 산업 조직들은 필사적으로 자기 조직의 핵심 정보를 지키기 위해 많은 노력을 기울이는 상황으로 변화되었다[5]. 이는, 전세계적으로 정보보안과 관련되는 시장성은 2005년부터 2019년까지 대략 30배 이상으로 증가세를 보였고, 2022년에는 1,330억 달러 규모를 훌쩍 넘어 설 것으로 예상하고 있다[4,5].

정보보안은 오늘날 일상 활동을 중심으로 산업 정보를 접하는 실무를 수행할 때, 절대적으로 검토해야 하는 필수적 정보문화의 개념으로 접근할 수 있다[6]. 연구의 영역은 보편적으로 보안 시스템을 다루는 관점과 인간 요소를 보완하는 관점으로 비교할 수 있다. 앞서 언급한 대로, 많은 연구는 시스템을 통제하는 기술보안 영역을 처리하기 때문에, 자료 검열 같은 차원에서 주요 논문들이 나타나고 있다[6,7].

그런데, 근래 들어 인간 요소들에 해당하는 정보보안 정책 관점의 연구 내용에 인식해야 한다는 요청이 늘어나고 있다[2-4]. 그 이유는 결과적으로 보안정책 시스템을 사용하는 당사자 특성에 의해 발생하는 보안 사건 사례가 계속해서 많아지고 있기 때문이다[8]. 그래서 본 연구의 과정에서는 인간의 요소를 향상시키는 측면의 연구 필요성을 주장하며, 주요한 핵심 관련 요소를 설정하여 정보보안 과정에 가해지는 효과성을 검증하고자 한다.

2. 이론적 배경

2.1 의사결정 구조

인간의 의사결정 구조는 크게 내적 차원과 외적 차원으로 구분할 수 있다. 내적 차원은 내부의 특성으로 인해 의사결정이 이루어지는 경향을 의미하며, 외적 차원은 외부의 특성으로 인해 의사결정이 이루어지는 경향을 의미한다[9,10]. 예를 들어, 정보보안의 맥락에서도 개인의 입장에서 정보보안을 고려하여 그에 준하는 행동을 실천하는 경우가 있으며, 개인이 속한 조직에서 요구하는 정보보안의 행동 지침과 같은 요소의 영향을 받아 정보보안을 고려하는 행동을 하는 경우도 있을 것이다.

개인의 내적 차원의 특성들은 다양하며, 정보보안의 관점에서는 논리적 의사결정구조보다 휴리스틱 의사결정 구조의 적합성을 더 크게 평가하고 있다[10]. 왜냐하면, 담당자의 입장에서는 보안과 업무의 효율성이 일부 상반되는 특성을 가졌고, 기술이 개발되면서 정보보안의 이러한 딜레마적인 요소가 증가하고 있기 때문이다. 가용성 차원은 이러한 휴리스틱의 관점을 반영한 개념이라고 할 수 있으며, 정보보안의 맥락에서 볼 때, 개인의 내적 차원으로 규정할 수 있다[11].

개인의 외적 차원의 특성은 조직문화의 특성으로 설명할 수 있다[10]. 즉, 조직이 추구하는 문화적 측면을 고려하였을 때, 조직문화는 조직에 속해 있는 다양한 개인들에게 영향을 미치게 된다. 정보보안의 조건에서 조직의 입장에서는 반드시 강조할 수밖에 없는 운영방침이지만, 개인 수준의 행동을 모두 통제하기는 불가능하다. 따라서 자연스럽게 조직문화를 조성하여 조직의 구성원들에게 정보보안 행동을 유도하는 전략을 개발하게 되었다. 정보

보안의 조직문화는 차원의 개념으로 접근하는 것이 일반적이며, 다양성과 동질성 추구 관점은 가장 대표적인 문화 차원의 하나라고 할 수 있다[12].

2.2 정보보안 과정

조직 내에서 정보보안의 과정을 개선하기 위해서는 가장 기본적으로 인간의 의식적인 수준에서 정보보안을 제대로 인식하는 것이 중요하다. 왜냐하면 이 영역은 인간의 기저에서 시작되는 동기의 원천을 자극하기 때문이다. 정보보안 의식이 강조되는 것은 바로 이러한 이유 때문이다. 이에, 조직이 정보보안 정책을 마련하고 실행하는 과정에서 가장 먼저 기대하는 것은 개인의 정보보안 의식을 개선하는 효과성일 것이다[13,14].

조직의 정보보안 정책은 단지 정보보안 의식을 개선하는 것으로 끝나지 않는다. 실제적인 정보보안 행위로 영향력을 이어 나가기 위해서는 주도성향의 대처 효능감과 동조성향의 준수의향이 개선되어야 한다[15,16]. 이것은 정보보안 행동 요소에 영향을 주는 가장 근접 요인이며, 궁극적으로 조직원의 정보보안 행동을 개선시키기 위한 유용한 요인이라고 할 수 있다.

아울러, 정보보안의 행위준수 수준에서 정보보안 정책의 효과성을 검증하는 것은 매우 중요하다. 보편적인 태도-행동 일관성 이론의 관점에서도 정보보안의 효과성을 검증하기 위해서는 행위수준에서 나타나는 평가의 결과를 준거로 삼는 것이 매우 적합하다는 의견이 지배적이다[17]. 이러한 점들을 근거로 가설을 설정하였다.

따라서 본 연구에서는 정보보안의 정책으로 인해 기대할 수 있는 정보보안의 효과를 검증할 것이며, 정보보안 의식, 대처 효능감, 준수의향, 정보보안 행동의 변수를 측정하여 설명구조에 적합한 연구모형을 제시하고자 한다.

3. 연구방법

3.1 연구대상

본 연구는 정보보안의 영역 중에 인간의 행동 요소를 다루는 연구 분야이다. 참여자들은 일반적으로 정보보안 정책의 영향과 관련 있는 과업을 관여하고 있으며, 어느 정도 보안 정책의 특성을 파악하고 있는 성인 대상자이다. 자료를 수집하는 과정에서 남성 184명(평균 연령 29.08세), 여성 155명(평균 연령 27.73세), 총 339명(평균 연령 28.46세)의 자료를 무선적으로 수집하였으며, 최종 339개의 자료를 분석에 활용하였다.

3.2 측정도구

본 연구 과정에서 개인 요소에 해당하는 가용성 이론의 관점(Availability Theory)과 조직 요소에 해당하는 문화 이론의 관점(Culture Theory), 두 가지 차원으로 구분하여 교차설계모형(cross over design)을 확인하였다[11,12]. 정보보안 과정을 분석하기 위하여 정보보안 의식(Information Security Awareness), 대처 효능감(Response Efficacy), 준수의향(Compliance Behavioral Intention), 정보보안 행동(Information Security Behavior)으로 구성된 변인들을 측정하였으며, 측정한 변인들의 인과적 논리를 적용하여 차이검증, 다원변량분석, 모형검증에 활용하였다. 아울러, 모든 분석에는 SPSS 26.0을 사용하였다.

3.2.1 가용성 차원과 문화 차원

가용성 차원은 개인들이 가지는 의사결정의 중심 단서가 통계적 자료인지 혹은 특정 사례 자료인지를 선택하도록 되어 있고, 문화 차원은 조직들이 가지는 문화적 선호 특성이 다양성 혹은 동질성을 추구하는지를 선택하도록 되어 있다.

3.2.2 정보보안 의식(Information Security Awareness)

정보보안 의식은 정보보안을 지키고자 하는 인식 성향의 정도를 의미한다[13]. 본 연구에 적용한 설문 도구는 3개의 문항으로 재구성된 측정 도구이며, 연구의 상황에 맞게 수정하여 개인 설문지로 완성하였다. 측정은 7점 리커트로 만들어진 양적 척도를 적용하였으며, 이 측정 변수의 신뢰도 Chrombach' α는 .70 이다.

3.2.3 대처 효능감(Response Efficacy)

대처 효능감은 위협으로 작용하는 보안문제에 대하여 스스로 얼마나 잘 해결하는지에 대한 정도이다[18]. 본 연구에 적용한 설문 도구는 4개의 문항으로 재구성된 측정 도구이며, 연구의 상황에 맞게 수정하여 개인 설문지로 완성하였다. 측정은 7점 리커트로 만들어진 양적 척도를 적용하였으며, 이 측정 변수의 신뢰도 Chrombach' α는 .82 이다.

3.2.4 준수의향(Compliance Behavioral Intention)

준수의향은 정보보안정책에 대하여 동조하여 지킬 의도를 가지는가의 정도를 의미한다([16]. 본 연구에 적용한 설문 도구는 4개의 문항으로 재구성된 측정 도구이며,

연구의 상황에 맞게 수정하여 개인 설문지로 완성하였다. 측정은 7점 리커트로 만들어진 양적 척도를 적용하였으며, 이 측정 변수의 신뢰도 Chrombach' α는 .72 이다.

3.2.4 정보보안 행동(Information Security Behavior)

정보보안 행동은 비밀번호 관리, 업데이트 패치, 안티바이러스 프로그램 사용, usb 사용 관리, 쿠키 처리, 스팸메일 처리, 호환성 웹페이지 관리의 7가지 행동으로 구성되어 있다[17]. 본 연구에 적용한 설문 도구는 7개의 문항으로 재구성된 측정 도구이며, 연구의 상황에 맞게 수정하여 개인 설문지로 완성하였다. 측정은 7점 리커트로 만들어진 양적 척도를 적용하였으며, 이 측정 변수의 신뢰도 Chrombach' α는 .86 이다.

3.3 연구 모형 및 가설

본 분석 과정에서는 복합적 이중 매개모형을 연구모형으로 제시하였고, 위계적 회귀분석을 통해 계수의 적합성을 검증하고, 매개효과를 검증하였다(Fig. 1 참조).

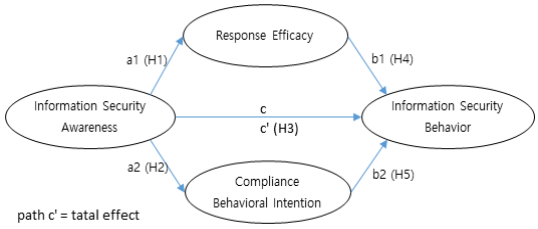

Fig. 1. research model

가설을 도출하는 과정에서 앞서 언급한 정보보안 의식이 정보보안의 행동을 야기하는 매우 중요한 변인으로 작용할 수 있다는 점에 주목하여 주요 가설로 선정하였다(H3). 이 과정에서 대처 효능감의 개념과 준수의향의 개념이 중재하는 가능성을 고려하여 최종 5개의 가설을 수립하였다. 즉, 정보보안 의식이 높은 사람은 일반적으로 정보보안 행동을 실천할 가능성이 높은데, 그 이유는 대처 효능감으로 인한 자신의 행동에 대한 확신감이 반영되었기 때문이라고 할 수 있다[15,16]. 이에, 정보보안 의식이 높은 사람은 대처 효능감이 높을 가능성이 있으며(H1), 대처 효능감이 높은 사람은 궁극적으로 정보보안 행동을 수행할 가능성이 높다고 판단된다(H4). 마찬가지로, 의식과 행동을 매개하는 주요 변인으로는 태도변수가 일반적이다. 그리고 정보보안 의식이 정보보안 행동으로 이어지는 과정에서 준수의향은 중요한 태도변수가 될 수 있다[10,12]. 따라서 정보보안 의식이높은 사람은 준수의향이 높을 가능성이 있으며(H2), 준수의향이 높은 사람은 궁극적으로 정보보안 행동을 수행할 가능성이 높다고 할 수 있다(H5).

H1 : 정보보안 의식이 높을수록 대처 효능감이 높을 것이다.
H2 : 정보보안 의식이 높을수록 준수의향이 높을 것이다.
H3 : 정보보안 의식이 높을수록 정보보안 행동이 향상될 것이다.
H4 : 대처 효능감이 높을수록 정보보안 행동이 향상될 것이다.
H5 : 준수의향이 높을수록 정보보안 행동이 향상될 것이다.

4. 연구결과

4.1 기초 통계 분석 결과

본 연구의 참여자 특성을 가용성 차원, 문화 차원, 그리고 성별의 세 가지 차원으로 분류하여 분포 특성을 확인했다. 가용성 차원의 범주에서 11.50% 정도 분포의 차이가 있었고, 문화 차원의 범주에서 1.47% 정도 분포의 차이가 있었고, 성별의 범주에서 8.55% 정도 분포의 차이가 있었다. 따라서 분포의 비율에서 편향의 우려가 심각하지는 않다고 판단내릴 수 있다.

Table 1. participants distribution

availability	culture	sex		total
		male	female	
statistics	diversity	55(52.88%)	49(47.12%)	104(100.00%)
	homogeneity	46(54.12%)	39(45.88%)	85(100.00%)
	total	101(53.44%)	88(46.56%)	189(100.00%)
case	below	37(54.41%)	31(45.59%)	68(100.00%)
	above	46(56.10%)	36(43.90%)	82(100.00%)
	total	83(55.33%)	67(44.67%)	150(100.00%)
total	below	92(53.49%)	80(46.51%)	172(100.00%)
	above	92(55.09%)	75(44.91%)	167(100.00%)
	total	184(54.28%)	155(45.72%)	339(100.00%)

4.2 교차분석 결과

본 분석의 과정에서는 연구참여자들이 응답한 자료를

적용하여 가용성 차원과 문화 차원이 교차되어 혼합된 구조 내에서 정보보안과 관련되는 삶의 일상에 대하여 어떻게 영향을 미치는지를 확인하기 위해 변량분석 기법을 활용하였다. 다시 말하면, 가용성 차원과 문화 차원의 교차설계방안에서 교차방안이 정보보안 의식, 대처 효능감, 준수의향, 정보보안 행동에 미치는 영향을 검증하였다.

첫째, 가용성 차원(availability), 문화 차원(culture) 변인이 정보보안 의식(Information Security Awareness)에 미치는 영향을 변량분석으로 검증하였고(가용성 차원(2)×문화 차원(2)), 그 결과는 다음과 같다.

가용성 차원 변인에서 통계중심 집단(M = 5.94)이 사례중심 집단(M = 6.04)보다 정보보안 의식의 평균이 더 낮은 것으로 나타났다. 그러나 가용성 차원 변인이 정보보안 의식 변인에 미치는 영향력(F(1, 335) = 0.75, n.s.)은 통계적으로 유의하지 않은 것으로 나타났다.

문화 차원 변인에서 다양성 집단(M = 5.88)이 동질성 집단(M = 6.09)보다 정보보안 의식의 평균이 더 낮은 것으로 나타났다. 그리고 문화 차원 변인이 정보보안 의식 변인에 미치는 영향력(F(1, 335) = 6.20, p 〈 0.05)은 통계적으로 유의한 것으로 나타났다.

가용성 차원 변인과 문화 차원 변인의 상호작용(F(1, 335) = 2.83, n.s.)은 통계적으로 유의하지 않은 것으로 나타났다.

Table 2. ANOVA of Information Security Awareness

variables	SS	df	MS	F
availability(A)	0.51	1	0.51	0.75
culture(C)	4.22	1	4.22	6.20*
A × C	1.92	1	1.92	2.83

* p 〈 0.05

둘째, 가용성 차원, 문화 차원 변인이 대처 효능감(Response Efficacy)에 미치는 영향을 변량분석으로 검증하였고, 그 결과는 다음과 같다.

가용성 차원 변인에서 통계중심 집단(M = 5.02)이 사례중심 집단(M = 5.35)보다 대처 효능감의 평균이 더 낮은 것으로 나타났다. 그리고 가용성 차원 변인이 대처 효능감 변인에 미치는 영향력(F(1, 335) = 5.95, p 〈 0.05)은 통계적으로 유의한 것으로 나타났다.

문화 차원 변인에서 다양성 집단(M = 4.89)이 동질성 집단(M = 5.44)보다 대처 효능감의 평균이 더 낮은 것으로 나타났다. 그리고 문화 차원 변인이 대처 효능감 변인에 미치는 영향력(F(1, 335) = 21.82, p 〈 0.01)은 통계적으로 유의한 것으로 나타났다.

가용성 차원 변인과 문화 차원 변인의 상호작용(F(1, 335) = 0.55, n.s.)은 통계적으로 유의하지 않은 것으로 나타났다.

Table 3. ANOVA of Response Efficacy

variables	SS	df	MS	F
availability(A)	6.42	1	6.42	5.95*
culture(C)	23.54	1	23.54	21.82**
A × C	0.60	1	0.60	0.55

* p 〈 0.05, ** p 〈 0.01

셋째, 가용성 차원, 문화 차원 변인이 준수의향(Compliance Behavioral Intention)에 미치는 영향을 변량분석으로 검증하였고, 그 결과는 다음과 같다.

가용성 차원 변인에서 통계중심 집단(M = 5.01)이 사례중심 집단(M = 5.18)보다 준수의향의 평균이 더 낮은 것으로 나타났다. 그러나 가용성 차원 변인이 준수의향 변인에 미치는 영향력(F(1, 335) = 0.02, n.s.)은 통계적으로 유의하지 않은 것으로 나타났다.

문화 차원 변인에서 다양성 집단(M = 4.24)이 동질성 집단(M = 5.95)보다 준수의향의 평균이 더 낮은 것으로 나타났다. 그리고 문화 차원 변인이 준수의향 변인에 미치는 영향력(F(1, 335) = 364.37, p 〈 0.01)은 통계적으로 유의한 것으로 나타났다.

가용성 차원 변인과 문화 차원 변인의 상호작용(F(1, 335) = 0.17, n.s.)은 통계적으로 유의하지 않은 것으로 나타났다.

Table 4. ANOVA of Compliance Behavioral Intention

variables	SS	df	MS	F
availability(A)	0.01	1	0.01	0.02
culture(C)	242.50	1	242.50	364.37**
A × C	0.11	1	0.11	0.17

** p 〈 0.01

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

가용성 차원 변인에서 통계중심 집단(M = 5.44)이 사례중심 집단(M = 5.62)보다 정보보안 행동의 평균이 더 낮은 것으로 나타났다. 그러나 가용성 차원 변인이 정보보안 행동 변인에 미치는 영향력(F(1, 335) = 1.44, n.s.)

은 통계적으로 유의하지 않은 것으로 나타났다.

문화 차원 변인에서 다양성 집단(M = 5.21)이 동질성 집단(M = 5.84)보다 정보보안 행동의 평균이 더 낮은 것으로 나타났다. 그리고 문화 차원 변인이 정보보안 행동 변인에 미치는 영향력(F(1, 335) = 37.49, p 〈 0.01)은 통계적으로 유의한 것으로 나타났다.

가용성 차원 변인과 문화 차원 변인의 상호작용(F(1, 335) = 1.07, n.s.)은 통계적으로 유의하지 않은 것으로 나타났다.

Table 5. ANOVA of Information Security Behavior

variables	SS	df	MS	F
availability(A)	1.25	1	1.25	1.44
culture(C)	32.54	1	32.54	37.49**
A × C	0.92	1	0.92	1.07

** p 〈 0.01

4.2 연구모형 분석 결과

우선, 정보보안 의식이 대처 효능감을 거쳐 정보보안 행동을 설명하는 매개모형을 검증하였다. 정보보안 의식이 정보보안 행동에 미치는 총체적인 영향력은 통계적으로 매우 유의한 것으로 나타났으며(경로 c'; β = 3.97, p 〈 0.01; 가설 3 채택), 정보보안 의식이 대처 효능감에 미치는 영향력(경로 a1; β = 5.42, p 〈 0.01; 가설 1 채택)과 대처 효능감이 정보보안 행동에 미치는 직접적인 차원의 영향력(경로 b1; β = 9.99, p 〈 0.01; 가설 4 채택)은 모두 통계적으로 유의한 것으로 나타났다. 그리고 정보보안 의식이 정보보안 행동에 미치는 직접적인 영향력은 통계적으로 유의하지 않은 것으로 나타났다(경로 c; β = 0.63, n.s.).

두번째로, 정보보안 의식이 준수의향을 거쳐 정보보안 행동을 설명하는 매개모형을 검증하였다. 정보보안 의식이 정보보안 행동에 미치는 전체적인 영향력은 동일하며, 정보보안 의식이 준수의향에 미치는 영향력(경로 a2; β = 3.25, p 〈 0.01; 가설 2 채택)과 준수의향이 정보보안 행동에 미치는 직접적인 영향력(경로 b2; β = 6.91, p 〈 0.01; 가설 5 채택)은 모두 통계적으로 유의한 것으로 나타났다. 그리고 정보보안 의식이 정보보안 행동에 미치는 직접적인 영향력 또한 동일하다.

아울러, 두 가지 경로로 구조화된 이중 매개효과의 유효성을 검증하기 위해 Sobel 검증을 실시하였고, 그 결과 매개효과가 통계적으로 유의한 것으로 나타났다(Z = 1.95, p 〈 .05).

Table 6. Hierarchical regression analysis of mediation model

step		path	beta
0 step(c′ path)		ISA→ISB	0.21**
1-1 step(a path)	a1	ISA→RE	0.28**
	a2	ISA→CBI	0.17**
1-2 step(b path)	b1	RE→ISB	0.46**
	b2	CBI→ISB	0.31**
2 step(c path)		ISA→ISB	0.03

※ Information Security Awareness : ISA, Response Efficacy : RE, Compliance Behavioral Intention : CBI, Information Security Behavior : ISB

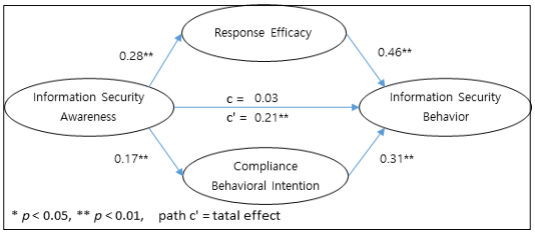

Fig. 2. dual process mediation model

따라서 본 연구모형은 이중 복합모형으로 설명할 수 있으며, 정보보안 의식이 정보보안 행동으로 이어지는 과정에서 대처 효능감과 준수의향이 매개하는 역할을 하고 있는 것을 확인할 수 있다.

5. 결론

첫째, 분석된 결과에서 전반적으로 가용성 차원의 실효성이 확인되었는데, 가용성 차원을 이루고 있는 요소들 중 사례중심 요소의 효과성이 더 우수하다는 확실한 결과를 밝혀냈다. 이러한 점으로 미루어, 조직 내 훈련 영역에서 사례중심 요소의 내용을 적용한다면, 보안 정책들의 운영 규정을 개선하는데 커다란 계기가 될 수가 있을 것이다. 한 예로, 정보보안 규정을 수립하는 입장에서 가용성 차원에 관한 핵심 개념을 응용하여 구체적인 정책에 제작할 수 있다면, 외적인 범위에서 다루기 어려웠던 보안 정책의 맹점에 대하여 책임감 있게 처리할 수 있을 것이라고 판단된다. 또한, 이러한 연구적 결과는 정보보안에 있어서 가용성 차원의 중요성을 밝힌 예전의 연구적 입장과 유사하다[19].

둘째, 문화 차원의 검증 결과에서도 유사한 영향력이 밝혀졌는데 유의미한 차이로 동질성 요소가 다양성 요소

보다 효율이 더 큰 사실로 확인되었다. 이런 사실을 가지고 인적관리 정책에 응용하면, 보안 정책의 관리 운영을 고도화시키는데 꾀 커다란 긍정적 효과를 확신할 수 있다고 보여 진다[20,21]. 또한, 정보보안 정책을 규정하는 입장에서 문화 차원에 관한 주된 단서를 구체적인 정책에 반영하여 완성할 수 있다면, 환경적인 부분에서 다룰 수 없었던 정보보안 정책의 미비점에 대하여 성공적으로 해결할 수 있다고 판단된다. 아울러, 이러한 연구 결과는 보안 정책 운영에 있어서 문화 차원의 적합성을 강조한 이전의 학술적 관점과 비슷하다.

셋째, 학술적인 관점에서 이 연구에서의 접근은 이전의 보안 관련 정책 연구와 비교하면, 사용통제 기술과 관련 있는 기능적 특성의 제재 방식에 초점을 맞춘 연구 방안이 아닌, 컴퓨터를 사용하는 인간의 요소를 조절하는 관점에 중점을 두고 있다는 점에서 연구적 차별성을 가진다. 결국 효과적인 기능으로 설계된 정보보안 기술을 적용하여 정보보안 정책에 타당한 적용 방식으로 정보보안 시스템에 응용하더라도, 관련자가 보안 정책을 많은 부분 준수하지 않는다면 매우 치명적인 보안 사고를 일으킬 수도 있다. 그래서 정보보안이 중요한 조직이나 단체에서는 본 연구 과정이 주목하는 인간 요소에 해당하는 보안 전략 관련 특성을 적용하여 원활히 정보보안 습관을 보완할 수 있는 가치 있는 조치 분위기를 확보해야 할 것으로 사료된다.

넷째, 정책적인 방향을 고려한다면, 정보보안 의식은 대처 효능감과 준수의향의 복합 구조의 매개모형을 거쳐 정보보안 행동에 영향력을 주는 모형인 것으로 검증되었다. 실제로 대안적 모형의 상대적인 위상을 비교한다면, 대처 효능감과 준수의향은 각기 '주도성향'과 '동조성향'의 범주로 양분하여 이해할 수 있다. 따라서, 상호작용의 방안에 부합하는 특성을 구분하여 정보보안 체제 운영에 반영해야 하며, 이 두 가지의 의미를 참작하여 공동체의 정황에 타당한 정보보안의 정책을 구조적으로 반영하는 전략적 집행이 요구된다[22,23].

마지막으로, 본 연구에서는 연구지원자의 여러 가지 개별적 성향을 반영하지 못하였던 것이 한계점이라고 평가할 수 있다. 동시에, 정보보안 연구 설정을 인간의 요소에 쟁점을 두고 검증을 실행하는 중에 업무 차원을 참작한다면, 매우 타당한 연구성과를 달성할 수 있다고 여겨진다. 이에, 성과를 강화하는 후속 연구가 요구되고, 독특한 개인 요소의 변인과 조직적 특성의 상호작용 활동을 여러 가지 구조에서 확증하는 연구 분석의 필요성을 제의한다.

REFERENCES

[1] 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.

[2] 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

[3] 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.

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

[5] 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.

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

[7] A. AlHogail. (2015). Design and validation of information security culture framework. *Computers in human behavior, 49*, 567-575.
DOI : 10.1016/j.chb.2015.03.054

[8] 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

[9] 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

[10] S. A. Stumpf & M. London. (1981). Management promotions: Individual and organizational factors influencing the decision process. *Academy of Management Review, 6(4),* 539-549.

[11] A. Tversky & D. Kahneman. (1973). Availability: A heuristic for judging frequency and probability. *Cognitive psychology, 5(2),* 207-232.

[12] W. E. Watson, K. Kumar & L. K. Michaelsen. (1993). Cultural diversity's impact on interaction process and performance: Comparing homogeneous and diverse task groups. *Academy of management journal, 36(3),*

590-602.

[13] 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.

[14] 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

[15] M. Workman, W. H. Bommer & D. Straub. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in human behavior, 24(6),* 2799-2816.
DOI : 10.1016/j.chb.2008.04.005

[16] 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

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

[18] P. Ifinedo. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31(1),* 83-95.
DOI : 10.1016/j.cose.2011.10.007

[19] S. Z. ul Abdin, O. Farooq, N. Sultana & M. Farooq. (2017). The impact of heuristics on investment decision and performance: Exploring multiple mediation mechanisms. *Research in International Business and Finance, 42*, 674-688.
DOI : 10.1016/j.ribaf.2017.07.010

[20] I. H. Hwang & S. H. Hu. (2018). A Study on the Influence of Information Security Compliance Intention of Employee: Theory of Planned Behavior, Justice Theory, and Motivation Theory Applied. *Journal of Digital Convergence, 16(3),* 225-236.
DOI : 10.14400/JDC.2018.16.3.225

[21] I. H. Hwang & S. H. Hu. (2020). A study on the information security compliance and non-compliance causes of organization employees. *Journal of the Korea Convergence Society, 11(9),* 229-242.
DOI : 10.15207/JKCS.2020.11.9.229

[22] 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

[23] 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.

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
· 2020년 3월 ~ 현재: 블라인드 공채 채용심사 전문요원
· 관심분야 : 정보문화, 융합연구, 고령화, 빅데이터, 채용경향, 공동체 분야 등
· E-Mail : powerrcy@hanmail.net

황 인 호(In-ho Hwang) [종신회원]

· 2004년 8월 : 건국대학교 경영학과(경영학사)
· 2007년 6월 : 중앙대학교 경영학과(경영학석사)
· 2014년 2월 : 중앙대학교 경영학과(경영학박사)
· 2018년 7월 ~ 2020년 8월 : 한국산업기술대학교 창업교육센터 연구교수
· 2018년 9월 : 국민대학교 교양대학 조교수
· 관심분야 : IT 핵심성공요인, 디지털 콘텐츠, 정보보안 및 프라이버시 분야 등
· E-Mail : hwanginho@kookmin.ac.kr