Journal of the Korea Academia-Industrial cooperation Society
Vol. 22, No. 1 pp. 595-602, 2021

https://doi.org/10.5762/KAIS.2021.22.1.595
ISSN 1975-4701 / eISSN 2288-4688

# 정보 보안 제재성과 위협 인식, 분위기 인식이 준수 행동 의도성에 미치는 영향 분석: 전망 관점과 목표 지향 관점을 중심으로

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

# Analysis of The Effects of Information Security Policy Sanction, Perceived Threat, and Perception of Information Security Climate on Compliance Behavioral Intention: Focursing on Prospect and Goal Orientation

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

**요 약** 본 연구의 목적은 정보 보안 제재성, 위협 인식, 분위기 인식이 준수 행동 의도성에 미치는 효과를 이해하는 것이다. 연구 방법은 전망 관점과 목표 지향 관점의 교차설계로 구조화되었고, 정보 보안 과정은 정보 보안 제재성, 위협 인식, 분위기 인식, 준수 행동 의도성의 네 가지 변수로 측정되었다. 연구 진행은 전망 관점과 목표 지향 관점을 측정 후, 네 가지 변인을 측정하는 과정으로 구성되어 있다. 연구 결과, 전망 관점은 분위기 인식에 유의미한 영향을 미치고 있었으며, 이득 조건의 영향력이 손해 조건보다 더 큰 것으로 나타났다. 목표 지향 관점은 정보 보안 제재성, 위협 인식, 준수 행동 의도성에 유의미한 영향을 미치고 있었으며, 성장 조건의 영향력이 안정 조건보다 더 큰 것으로 나타났다. 전망 관점과 목표 지향 관점은 준수 행동 의도성에 대하여 상호작용 효과가 발생하였다. 결과적으로 도출한 연구 모형은 측정변인으로 구조화된 복합 매개모형으로 탐색되었다. 아울러, 논의점은 이러한 결과를 기반으로 정보 보안에 적합한 시사점을 포함하고 있다.

**Abstract** This study evaluates the impact of an information security policy sanction, a perceived threat, and the perception of the information security climate on a compliance behavioral intention. The research method was structured with a cross-sectional study design for the prospect and goal orientation. The variables used in the analysis are information security policy sanction, perceived threat, perception of information security climate, and compliance behavioral intention. Progress in this research consists of measuring the prospect and goal orientation, and then measuring the four variables. As a result, the prospect had a significant effect on the perception of the information security climate, and it was found that the influence of the gain-based condition was greater than the loss-based condition. Goal orientation had a significant effect on the information security policy sanction, the perceived threat, and the compliance behavioral intention, and the influence of the development-based condition was greater than the stability-based condition. Both prospect and goal orientation had an interactive effect on the compliance behavioral intention. The exploration model was verified as a mediation model. In addition, the discussion includes the appropriate implications for information security based on these research results.

**Keywords :** Prospect Theory, Goal Orientation Theory, Information Security Policy Sanction, Perceived Threat, Perception of Information Security Climate, Compliance Behavioral Intention

이 논문은 2018년 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2018R1D1A1B07050305)
*Corresponding Author : In-Ho Hwang(Kookmin Univ.)
email: hwanginho@kookmin.ac.kr
Received November 5, 2020 Revised December 1, 2020
Accepted January 8, 2021 Published January 31, 2021

## 1. 서론

정보 보안은 현대인의 일상 활동을 중심으로 산업적 정보와 관련되는 업무환경에서 분명히 발생할 수 있는 사고의 위험을 감안해야 하는 문제이며, 전반적인 활동 영역에서 정보문화의 관점이 적용된다고 해석할 수 있다. 연구적 영역은 보통 보안 장비를 통제하는 차원과 인간 요소를 개선하는 영역으로 분류할 수 있다. 대부분 연구들은 보안 기술을 통제하는 보안기술 차원을 접하기 때문에, 바이러스 백신이나 인증절차와 같은 측면에서 연관된 논문들이 확산되고 있다.

그렇지만, 근래에 인간의 요소에 의한 정보 보안 정책 관점의 연구 영역에 주목해야 한다는 목소리가 높아지고 있다[2-5]. 이 문제는 실제로 보안정책 시스템을 운영하는 당사자 관점의 요소들에 의해 발생하는 보안 정책 사고 건수가 점점 증가하고 있기 때문이다. 따라서 본 연구의 주제는 인간 요소의 영역을 향상시키는 측면의 실증적 필요성을 제안하며, 중요한 관련 변인들을 구조화하여 정보 보안 과정에 미치는 효과성을 탐색하고자 한다.

## 2. 이론적 배경

### 2.1 의사결정 구조

인간의 합리적 의사결정(decision making) 과정은 기본적으로 개인 차원과 환경 차원으로 나눌 수 있다[6,7]. 개인 차원은 개인의 기질적 기반으로 인하여 인지적인 의사결정이 처리되는 경향성을 의미하며, 환경 차원은 집단적 특성으로 인하여 합리적인 의사결정이 처리되는 경향성을 의미한다. 예를 들자면, 보안정책 운영의 장면에서도 개인의 기준에서 보안 정책 운영을 고려하여 여기에 해당하는 보안행동을 실시하는 경우가 나타날 수 있으며, 개인이 소속된 조직에서 강조하는 정보 보안 정책의 준수 행동 규정과 같은 특정 제도의 영향력을 받아 조직의 기준에서 인정되는 정보 보안 정책 운영을 고려하여 여기에 해당하는 보안행동을 실시하는 경우도 있다.

인간이 갖는 개인 차원의 내용들은 여러 가지이며, 보안 정책의 영역에서는 논리적 의사결정 구조보다 휴리스틱 의사결정 활용성을 더 좋게 해석하고 있다. 그 이유는 담당자의 관점에서는 정보 보안 준수와 실무적 쟁점에서 몇 가지의 대립하는 현상이 생겨나고, 정보 보안 기술이 향상되면서 보안 정책의 이 같은 딜레마적인 사건이 늘어나고 있기 때문이다. 전망 관점은 이러한 휴리스틱 범례를 도입한 자극 요소라고 정의할 수 있으며, 정보 보안 운영의 차원에서 검토할 때, 인간 요소의 개인 차원으로 설명할 수 있다[8,9].

환경 차원의 영역들은 대부분 조직문화의 특성으로 설명할 수 있다. 즉, 조직이 주도하는 문화적 특성을 고려할 때, 조직문화는 그 조직에 소속되어 있는 수많은 구성원들에게 영향을 미친다. 하지만, 정보 보안 운영의 맥락에서 조직이 어쩔 수 없이 강요할 수밖에 없는 규정이라고 할지라도 개인 구성원 수준의 행동을 쉽게 개입하기는 불가능하다. 이런 상황에서 조직은 자연스럽게 조직문화를 수립하여 구성원들에게 보안에 적합한 준수 행동을 육성하는 운영방식을 마련할 수 있다. 보안정책 관점의 조직문화는 집단 분위기의 개념으로 접근하는 것이 일반적이며, 안정과 성장으로 분류하는 접근법은 매우 중요한 문화차원의 한 예라고 할 수 있다[10,11].

### 2.2 정보 보안의 동기 자극 과정

공동체 조직 관점에서 볼 때, 보안정책 운영의 효율성을 향상하기 위해서는 일차적으로 조직원의 의식적인 부분에서 정보 보안의 의미를 정확하게 지각하는 것이 중요한 관건이다. 왜냐하면 이 영역은 행동 수행의 깊은 곳에서 생성되는 동기의 원천을 자극하기 때문이다. 정보 보안 제재성이 강조되는 분위기는 즉 이러한 특성 때문이다. 이에, 공동체가 정보 보안 주요 정책을 마련하고 수행하는 과정에서 가장 기본적으로 기대하는 효과는 구성원의 정보 보안 제재성을 보완하는 것이다[12].

조직이 수립한 정보 보안의 쟁점은 정보 보안 제재성을 높이는 것으로 끝나지 않는다. 실용적인 정보 보안의 실천행동으로 체계적인 파급효과를 확보하기 위해서는 자기중심반응의 위협 인식과 조직중심반응의 분위기 인식이 촉진되어야 한다[13,14]. 이것은 세부적인 정보 보안 실천행동으로 영향을 끼치게 하는 매우 밀접한 변수이며, 통합적으로 그 조직에서 관여하는 개인의 정보 보안 준수행동 수준을 개선시키기 상당히 유익한 정보 보안 요인이라고 해석할 수 있다[15].

한편, 정보 보안의 준수행동 과정에서 정보 보안 관련 정책의 실용적인 효과성을 검증하는 것은 매우 필요하다[15]. 인간의 태도와 행동 전반을 분석하는 통상적인 기대가치 이론의 측면에서도 조직이 추진하는 정보 보안 정책의 본질적인 실효성을 규명하기 위해 의도 및 행동 차원에서 나타나는 평가 결과를 바탕으로 설명하는 것이 적당하다는 입장이 지배적이다.

따라서 본 연구 과정에서는 정보 보안의 관련 정책으

로 기대할 수 있는 실용적인 파급효과를 평가하기 위해 공동체 조직이 시행하는 실질적인 정보 보안 과정에서 나타나는 현실적 사실들을 토대로 정보 보안 운영의 현실적인 효과를 검증할 것이다. 정보 보안 운영의 효과는 정보 보안 제재성, 위협 인식, 분위기 인식, 그리고 준수 행동 의도성으로 구분된 변수를 응용하여 측정할 것이며, 연구 결과들을 통합하여 연구방안에 적합한 탐색모형을 도출하고자 한다.

## 3. 연구방법

### 3.1 연구대상

본 연구 과정은 정보 보안의 영역 중에 인간행동과 관련된 요소에 관심을 두는 연구라고 할 수 있으며, 연구참여자는 대부분 정보 보안 정책의 영향과 관계있는 실무를 시행하고 있으며 어느 정도 정보 보안 정책의 특성을 이해하고 있는 성인이다. 자료수집 과정에서는 남성 174명(평균 연령 28.38세), 여성 140명(평균 연령 28.11세), 총 314명(평균 연령 28.26세)의 자료를 무작위로 수집하였으며, 총 314개의 데이터를 분석 과정에 사용하였다.

연구대상자들의 직업은 공무원 85명(27.1%), 은행원 85명(27.1%), 일반사무직 65명(20.7%), 전문가 54명(17.2%), 개인사업자 및 기타 25명(8.0%) 의 비율로 나타났다. 이들의 활동 중에 정보 보안과 관련되는 영역은 뉴스 자료 107건(34.1%), sns 활동 73건(23.2%), 이메일 활동 70건(22.3%), 거래승인 38건(12.1%), 분석자료 26건(8.3%) 의 비율로 나타났다.

### 3.2 측정도구

본 연구 과정에서는 내부적 차원에 해당하는 전망이론의 개념(prospect Theory)과 외부적 차원에 해당하는 목표지향이론의 개념(Goal Orientation Theory), 두 개의 차원으로 분리하여 교차방안(cross over design)을 평가하였다. 정보 보안의 동기 자극 과정을 평가하기 위해 정보 보안 제재성(Information Security Policy Sanction), 위협 인식(Perceived Threat), 분위기 인식(Perception of Information Security Climate), 준수 행동 의도성(Compliance Behavioral Intention)으로 구성된 변인들을 측정하였으며, 변인 간의 논리적 성향을 적용하여 차이검증, 다변량분석, 연구모형 탐색에 활용하였다. 아울러, 분석 과정에서는 SPSS 26.0을 사용했다.

#### 3.2.1 전망 관점과 목표 지향 관점

전망 관점은 전망이론의 영역에 해당하며, 개별 개인이 선호하는 의사결정 절차의 핵심 단서가 손해의 내용인지 그게 아니면 이득의 내용인지를 코딩한 변수이다. 측정은 양분척도를 활용하여 단 문항(“여러분은 다음 중 어느 특성에 더 큰 비중을 두고 의사결정을 내립니까?”)으로 특정하였다. 목표 지향 관점은 목표지향이론의 영역에 해당하며, 조직문화가 선호하는 의사결정 절차의 핵심 단서가 안정과 관련된 내용인지 그게 아니면 성장과 관련된 내용인지를 코딩한 변수이다. 측정은 양분척도를 활용하여 단 문항(“여러분이 소속되어 있는 조직문화는 다음 중 어느 특성을 더 강조합니까?”)으로 특정하였다.

#### 3.2.2 정보 보안 제재성(Information Security Policy Sanction)

정보 보안 제재성의 개념은 조직의 정보 보안 정책이 갖는 제재성의 내용을 의미한다[12]. 자료 수집에 적용한 설문 도구는 4개의 질문으로 이루어진 태도 측정 변수이며, 연구의 상황에 맞게 보강하여 조사 설문지로 제작하였다. 척도의 크기는 7점 리커트 방식(7-Likert)의 척도를 적용하였고, 이 측정도구의 문항간 신뢰도 Chrombach' $\alpha$는 .82 인 것으로 나타났다.

#### 3.2.3 위협 인식(Perceived Threat)

위협 인식의 개념은 개인이 인식하는 정보 보안의 위협을 의미한다[16]. 자료 수집에 적용한 설문 도구는 6개의 질문으로 이루어진 태도 측정 변수이며, 연구의 상황에 맞게 보강하여 조사 설문지로 제작하였다. 척도의 크기는 7점 리커트 방식(7-Likert)의 척도를 적용하였고, 이 측정도구의 문항간 신뢰도 Chrombach' $\alpha$는 .86 인 것으로 나타났다.

#### 3.2.4 분위기 인식(Perception of Information Security Climate)

분위기 인식의 개념은 개인이 조직적 분위기를 반영하여 정보 보안의 위협을 인식하는 내용을 의미한다[13]. 자료 수집에 적용한 설문 도구는 4개의 질문으로 이루어진 태도 측정 변수이며, 연구의 상황에 맞게 보강하여 조사 설문지로 제작하였다. 척도의 크기는 7점 리커트 방식(7-Likert)의 척도를 적용하였고, 이 측정도구의 문항간 신뢰도 Chrombach' $\alpha$는 .87 인 것으로 나타났다.

#### 3.2.5 준수 행동 의도성(Compliance Behavioral Intention)

준수 행동 의도성의 개념은 정보 보안행동을 할 것이라는 직접적인 행동의도성에 관한 내용을 의미한다[15]. 자료 수집에 적용한 설문 도구는 4개의 질문으로 이루어진 태도 측정 변수이며, 연구의 상황에 맞게 보강하여 조사 설문지로 제작하였다. 척도의 크기는 7점 리커트 방식(7-Likert)의 척도를 적용하였고, 이 측정도구의 문항간 신뢰도 Chrombach' $\alpha$는 .72 인 것으로 나타났다.

## 4. 연구결과

### 4.1 기초 통계 분석 결과

Table 1. Participants distribution

| prospect | goal orientation | sex | | total |
|---|---|---|---|---|
| | | male | female | |
| loss | stability | 58(54.21%) | 49(45.79%) | 107(100.00%) |
| | development | 26(48.15%) | 28(51.85%) | 54(100.00%) |
| | total | 84(52.17%) | 77(47.83%) | 161(100.00%) |
| gain | stability | 42(62.69%) | 25(37.31%) | 67(100.00%) |
| | development | 48(55.81%) | 38(44.19%) | 86(100.00%) |
| | total | 90(58.82%) | 63(41.18%) | 153(100.00%) |
| total | stability | 100(57.47%) | 74(42.53%) | 174(100.00%) |
| | development | 74(52.86%) | 66(47.14%) | 140(100.00%) |
| | total | 174(55.41%) | 140(44.59%) | 314(100.00%) |

본 연구의 대상자 분포 성향을 전망 관점, 목표 지향 관점, 그리고 성별의 세 가지 단위로 분류하여 분포 특성을 확인했다. 전망 관점의 범주에서 2.55% 정도 분포의 차이가 있었고, 목표 지향 관점의 범주에서 10.83% 정도 분포의 차이가 있었고, 성별의 범주에서 10.83% 정도 분포의 차이가 있었다. 결과적으로, 분류된 분포의 비율을 고려했을 때, 문제가 될 만한 편향이 발생되지 않았다고 판단할 수 있다.

### 4.2 교차설계 분석 결과

본 분석 과정은 연구참가자들이 응답 반응을 응용하여 전망 관점과 목표 지향 관점이 교차 설계의 구조 내에서 정보 보안의 동기 자극 과정을 검증하기 위해 ANOVA 기법을 반영하였다. 결과적으로 전망 관점과 목표 지향 관점의 교차설계방안에서 교차모형이 정보 보안 제재성, 위협 인식, 분위기 인식, 준수 행동 의도성에 미치는 효과성을 검증하였다.

첫째, 전망 관점(prospect), 목표 지향 관점(goal orientation) 변인이 정보 보안 제재성(Information Security Policy Sanction)에 미치는 영향을 변량분석으로 검증하였고(전망 관점(2)×목표 지향 관점(2)), 그 결과는 다음과 같다.

전망 관점 변인에서 손해 집단(M = 5.45)이 이득 집단(M = 5.84)보다 정보 보안 제재성의 평균이 더 낮은 것으로 나타났다. 그리고 전망 관점 변인이 정보 보안 제재성 변인에 미치는 영향력($F(1, 310) = 6.67$, $p < 0.05$)은 통계적으로 유의한 것으로 나타났다.

목표 지향 관점 변인에서 안정 집단(M = 5.42)이 성장 집단(M = 5.92)보다 정보 보안 제재성의 평균이 더 낮은 것으로 나타났다. 그리고 목표 지향 관점 변인이 정보 보안 제재성 변인에 미치는 영향력($F(1, 310) = 15.04$, $p < 0.01$)은 통계적으로 유의한 것으로 나타났다.

전망 관점 변인과 목표 지향 관점 변인의 상호작용($F(1, 310) = 0.03$, n.s.)은 통계적으로 유의하지 않은 것으로 나타났다.

Table 2. ANOVA of Information Security Policy Sanction

| variables | Mean | | SS | df | MS | F |
|---|---|---|---|---|---|---|
| prospect(P) | loss | 5.45 | 6.12 | 1 | 6.12 | 6.67* |
| | gain | 5.84 | | | | |
| goal orientation(G) | stability | 5.42 | 13.80 | 1 | 13.80 | 15.04** |
| | development | 5.92 | | | | |
| P × G | - | | 0.03 | 1 | 0.03 | 0.03 |

* $p < 0.05$, ** $p < 0.01$

둘째, 전망 관점, 목표 지향 관점 변인이 위협 인식(Perceived Threat)에 미치는 영향을 변량분석으로 검증하였고, 그 결과는 다음과 같다.

전망 관점 변인에서 손해 집단(M = 5.10)이 이득 집단(M = 5.47)보다 위협 인식의 평균이 더 낮은 것으로 나타났다. 그리고 전망 관점 변인이 위협 인식 변인에 미치는 영향력($F(1, 310) = 6.94$, $p < 0.01$)은 통계적으로 유의한 것으로 나타났다.

목표 지향 관점 변인에서 안정 집단(M = 5.18)이 성장 집단(M = 5.40)보다 위협 인식의 평균이 더 낮은 것으로 나타났다. 그러나 목표 지향 관점 변인이 위협 인식 변인에 미치는 영향력($F(1, 310) = 1.35$, n.s.)은 통계적으로 유의하지 않은 것으로 나타났다.

전망 관점 변인과 목표 지향 관점 변인의 상호작용(F(1, 310) = 0.56, n.s.)은 통계적으로 유의하지 않은 것으로 나타났다.

Table 3. ANOVA of Perceived Threat

| variables | Mean | | SS | df | MS | F |
|---|---|---|---|---|---|---|
| prospect(P) | loss | 5.10 | 7.99 | 1 | 7.99 | 6.94** |
| | gain | 5.47 | | | | |
| goal orientation(G) | stability | 5.18 | 1.56 | 1 | 1.56 | 1.35 |
| | development | 5.40 | | | | |
| P × G | - | | 0.64 | 1 | 0.64 | 0.56 |

** p < 0.01

셋째, 전망 관점, 목표 지향 관점 변인이 분위기 인식(Perception of Information Security Climate)에 미치는 영향을 변량분석으로 검증하였고, 그 결과는 다음과 같다.

전망 관점 변인에서 손해 집단(M = 5.22)이 이득 집단(M = 5.67)보다 분위기 인식의 평균이 더 낮은 것으로 나타났다. 그리고 전망 관점 변인이 분위기 인식 변인에 미치는 영향력(F(1, 310) = 5.79, p < 0.05)은 통계적으로 유의한 것으로 나타났다.

목표 지향 관점 변인에서 안정 집단(M = 5.25)이 성장 집단(M = 5.67)보다 분위기 인식의 평균이 더 낮은 것으로 나타났다. 그리고 목표 지향 관점 변인이 분위기 인식 변인에 미치는 영향력(F(1, 310) = 4.07, p < 0.05)은 통계적으로 유의한 것으로 나타났다.

전망 관점 변인과 목표 지향 관점 변인의 상호작용(F(1, 310) = 0.95, n.s.)은 통계적으로 유의하지 않은 것으로 나타났다.

Table 4. ANOVA of Perception of Information Security Climate

| variables | Mean | | SS | df | MS | F |
|---|---|---|---|---|---|---|
| prospect(P) | loss | 5.22 | 11.24 | 1 | 11.24 | 5.79* |
| | gain | 5.67 | | | | |
| goal orientation(G) | stability | 5.25 | 7.91 | 1 | 7.91 | 4.07* |
| | development | 5.67 | | | | |
| P × G | - | | 1.84 | 1 | 1.84 | 0.95 |

* p < 0.05

넷째, 전망 관점, 목표 지향 관점 변인이 준수 행동 의도성(Compliance Behavioral Intention)에 미치는 영향을 변량분석으로 검증하였고, 결과는 다음과 같다.

전망 관점 변인에서 손해 집단(M = 4.99)이 이득 집단(M = 5.36)보다 준수 행동 의도성의 평균이 더 낮은 것으로 나타났다. 그리고 전망 관점 변인이 준수 행동 의도성 변인에 미치는 영향력(F(1, 310) = 7.99, p < 0.01)은 통계적으로 유의한 것으로 나타났다.

목표 지향 관점 변인에서 안정 집단(M = 5.07)이 성장 집단(M = 5.30)보다 준수 행동 의도성의 평균이 더 낮은 것으로 나타났다. 그러나 목표 지향 관점 변인이 준수 행동 의도성 변인에 미치는 영향력(F(1, 310) = 1.27, n.s.)은 통계적으로 유의하지 않은 것으로 나타났다.

Table 5. ANOVA of Compliance Behavioral Intention

| variables | Mean | | SS | df | MS | F |
|---|---|---|---|---|---|---|
| prospect(P) | loss | 4.99 | 10.10 | 1 | 10.10 | 7.99** |
| | gain | 5.36 | | | | |
| goal orientation(G) | stability | 5.07 | 1.60 | 1 | 1.60 | 1.27 |
| | development | 5.30 | | | | |
| P × G | - | | 7.94 | 1 | 7.94 | 6.29* |

* p < 0.05, ** p < 0.01

전망 관점 변인과 목표 지향 관점 변인의 상호작용(F(1, 310) = 6.29, p < 0.05)은 통계적으로 유의한 것으로 나타났다.

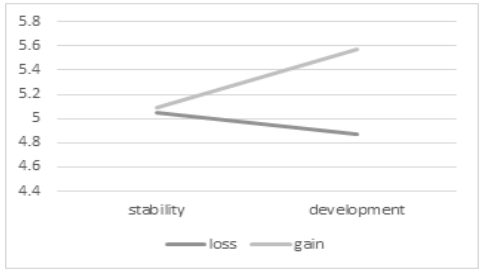


Fig. 1. Interaction of Compliance Behavioral Intention

## 4.3 연구모형 분석 결과

본 분석 과정에서는 매개모형을 제시하였고, 위계적 회귀분석과 Sobel 검증을 실시하여 매개효과 및 모형을 검증하였다(Fig 2).

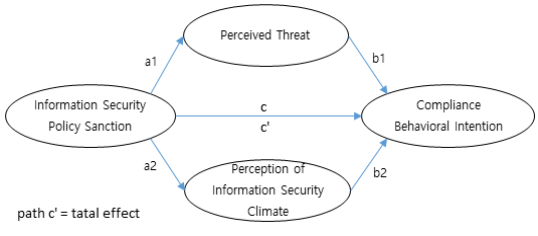


Fig. 2. Research model

우선, 정보 보안 제재성이 위협 인식을 거쳐 준수 행동 의도성을 설명하는 매개모형을 검증하였다. 정보 보안 제재성이 준수 행동 의도성에 미치는 전체적인 영향력은 통계적으로 유의한 것으로 나타났으며(경로 c'; $\beta$ = 0.19, p 〈 0.01), 정보 보안 제재성이 위협 인식에 미치는 영향력(경로 a1; $\beta$ = 0.44, p 〈 0.01)과 위협 인식이 준수 행동 의도성에 미치는 직접적인 영향력(경로 b1; $\beta$ = 0.22, p 〈 0.01)은 모두 통계적으로 유의한 것으로 나타났다. 그리고 정보 보안 제재성이 준수 행동 의도성에 미치는 직접적인 영향력은 통계적으로 유의하지 않은 것으로 나타났다(경로 c; $\beta$ = 0.02, n.s.).

Table 6. Hierarchical regression analysis of mediation model

| step | | path | beta |
|---|---|---|---|
| 0 step( c′ path) | | ISPS→CBI | 0.19** |
| 1-1 step( a path) | a1 | ISPS→PT | 0.44** |
| | a2 | ISPS→PISC | 0.24** |
| 1-2 step( b path) | b1 | PT→CBI | 0.22** |
| | b2 | PISC→CBI | 0.29** |
| 2 step( c path) | | ISPS→CBI | 0.02 |

※ Information Security Policy Sanction : ISPS, Perceived Threat : PT, Perception of Information Security Climate : PISC, Compliance Behavioral Intention : CBI

두 번째로, 정보 보안 제재성이 분위기 인식을 거쳐 준수 행동 의도성을 설명하는 매개모형을 검증하였다. 정보 보안 제재성이 준수 행동 의도성에 미치는 전체적인 영향력은 동일하며, 정보 보안 제재성이 분위기 인식에 미치는 영향력(경로 a2; $\beta$ = 0.24, p 〈 0.01)과 분위기 인식이 준수 행동 의도성에 미치는 직접적인 영향력(경로 b2; $\beta$ = 0.29, p 〈 0.01)은 모두 통계적으로 유의한 것으로 나타났다. 그리고 정보 보안 제재성이 준수 행동 의도성에 미치는 직접적인 영향력 또한 동일하다.

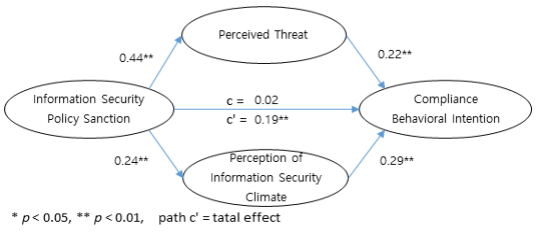


Fig. 3. Multiple process mediation model

아울러, 두 가지 경로로 구조화된 다원 매개효과의 유효성을 검증하기 위해 Sobel 검증을 실시하였고, 그 결과 매개효과가 통계적으로 유의한 것으로 나타났다(Z = 1.65, p 〈 .05).

따라서 본 연구모형은 이중 복합모형으로 설명할 수 있으며, 정보 보안 제재성이 준수 행동 의도성으로 이어지는 과정에서 위협 인식과 분위기 인식이 매개하는 역할을 하고 있다는 것을 확인할 수 있다.

## 5. 논의

첫째, 이 연구에서의 접근 방식은 지금까지 나타난 보안 정책 접근과 비교해서 볼 때, 컴퓨터 프로그램과 관련 있는 공학적 특성의 억제 관점에 주안점을 둔 연구적 설계가 아니며, 컴퓨터를 실행하는 인간 행동과 관련되는 인간 요소를 개선하는 차원에 중점을 두었다는 점에서 연구의 차별성을 가진다. 예를 들면, 뛰어난 사양으로 개발된 보안 프로그램 기술을 적용하여 보안 정책에 적합한 형태로 정보 보안 운영 체계에 적용하더라도, 관련자가 보안 규정을 준수하지 못한다면 매우 치명적인 위협을 일으킬 가능성이 있다[3,17]. 따라서 보안 정책이 강조되는 조직에서는 본 연구 과정에서 주안점을 두는 인간 요소 관점의 정보 보안 전략이 매우 유의한 정보가 될 수 있다. 이에 적합한 인간 요소의 관점을 활용하여 원만한 보안 행동을 보완할 수 있는 실제적인 적응 분위기를 갖추어야 할 것으로 판단된다.

둘째, 주효과 분석에서는 전망 관점의 영향력이 정보 보안 제재성, 위협 인식, 분위기 인식, 준수 행동 의도성 특성을 분명하게 개선시킨다는 사실을 확인했다. 그리고 지금 등장하는 4차 산업혁명의 특정 분위기를 고려한다면 앞으로 한국의 미래가 필요로 하는 다차원적인 융합 정보 변혁의 한 가운데 인간의 요소가 있다는 핵심을 직면해야 한다. 이러한 관점에서 보았을 때, 정보 보안의 정책방향도 인간 요소가 도입된 정보 보안 정책전략이 적용된다면 가능한 정보 보안 제재성, 위협 인식, 분위기 인식, 준수 행동 의도성 개념에서 나타나는 반응들이 수용될 것이다. 이러한 결과는 전망 관점에 해당하는 개인 특성의 정확한 지표가 될 수 있다는 점에서 분명한 교육적 함의를 갖는다[17]. 이에 정보 보안 체계에 있어서 개선 과정 속에는 전망 관점을 투영하여 정보 보안 제재성, 위협 인식, 분위기 인식, 준수 행동 의도성을 확보할 수 있는 정책 제도의 활성화가 필요하다.

셋째, 분석된 결과를 토대로 보안 정책의 방향성을 확

립하기 위해서는 목표 지향 관점의 조건에서 확신할 수 있는 주요 성과들을 탐색하기 위해 정보 보안 제재성, 분위기 인식 등을 포함하는 보안 태도 활성 방법을 추진하는 것이 요구된다. 또한, 등장하는 주된 변화의 분위기를 헤아려 본다면 이제 한국의 미래가 필요로 하는 다차원적 정보 변혁의 중심에 우리가 놓여 있다는 중요한 현실을 수용해야 한다. 따라서 정보 보안의 방향도 인간 중심 요소의 보안 전략이 적용된다면 최소한 정보 보안 제재성, 분위기 인식 개념에서 나타나는 변화가 수용될 것이다[18]. 이 결과들을 기반하여 제도적 방안을 유추한다면, 정보 보안 정책 체계 방안에 목표 지향 관점을 응용하여 정책 기반을 재정립하여 정보 보안 제재성, 분위기 인식을 강화할 수 있는 제도의 수립이 필요하다.

넷째, 준수 행동 의도성 변인에 대하여 전망 관점과 목표 지향 관점의 상호작용이 발생했는데, 이것은 어느 정도 주효과와 분리하여 설명할 수 있다. 이 분석에서 두 가지 요인의 단독 효과가 준수 행동 의도성에 미치는 분리된 영향만을 생각하여 보안 정책의 확립과정을 추진하는 것은 미흡한 방식이라고 비판받을 수 있다. 그 이유는 상호작용의 효과를 기반하여 경우에 따라 정책의 설정 방향을 확립하는 것이 방법적으로 맞기 때문이다. 결과적으로 합리적인 보안 정책 제도를 검토하고 수립하고자 한다면, 상호작용의 시너지를 고려하여 효과성을 넓힐 수 있는 실질적인 정책 사안을 설정해야 할 것이다.

다섯째, 정보 보안 제재성은 위협 인식과 분위기 인식의 다차원 구조로 이루어진 매개모형을 거쳐서 준수 행동 의도성에 영향을 미치는 것으로 검증되었다. 실제로 대응 구조의 상대적인 주효과의 위상을 분리한다면, 위협 인식과 분위기 인식은 각각 '자기중심반응'과 '조직중심반응'의 영역으로 나누어 해석할 수 있다[5]. 이에, 상호작용의 구조에 부합하는 개념을 분리 적용하여 정보 보안 정책 운영에 도입해야 하며, 이 두 가지의 의미를 활용하여 조직집단의 정황에 알맞은 보안 관련 정책을 유연하게 활용하는 전략이 요구된다.

끝으로, 본 연구에서는 연구참여자들의 여러 가지 개인 특징을 참작하지 못하였던 것이 제한 요소라고 할 수 있다. 또한, 정보 보안 관련 연구를 인간 요소 관련 변인에 주안점을 두고 검증을 실시하는 가운데 업무 비중을 숙고한다면, 매우 타당성 있는 연구적 업적을 달성할 수 있을 것이라고 판단된다. 그리고 적절성을 높이는 후행 연구가 필요하고, 특정 개인 인식의 성향과 공동체적 특성의 상호성 효과를 특정 모델에서 확증하는 분석들의 추진 필요성을 제기한다.

## References


[1] L. Tredinnick, Digital information culture: the individual and society in the digital age, p.205, Amsterdam : Elsevier, 2008, pp.57-79.

[2] A. AlHogail, "Design and validation of information security culture framework", *Computers in human behavior*, Vol.49, pp.567-7575, Aug. 2015.
DOI : https://doi.org/10.1016/j.chb.2015.03.054

[3] B. Khan, K. S. Alghathbar, S. I. Nabi & M. K. Khan, "Effectiveness of information security awareness methods based on psychological theories", *African Journal of Business Management*, Vol.5, No.26, pp.10862-10868, 2011.

[4] S. H. Hu, "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*, Vol.3, No.2, pp.63-81, 2020.
DOI : https://doi.org/10.37944/jams.v3i2.70

[5] R. W. Lee, I. H. Hwang & S. H. Hu, "Exploratory research of information security strategy focused on human factors", *The Journal of General Education*, Vol.6, No.2, pp.103-124, 2017.

[6] M. L. Foulds, "Changes in locus of internal-external control: A growth group experience", *Comparative Group Studies*, Vol.2, No.3, pp.293-300, 1971.
DOI : https://doi.org/10.1177/104649647100200303

[7] S. A. Stumpf & M. London, "Management promotions: Individual and organizational factors influencing the decision process", *Academy of Management Review*, Vol.6, No.4, pp.539-549, 1981.

[8] D. Kahneman & A. Tversky, Prospect theory: An analysis of decision under risk, Handbook, World Scientific, Singapore, pp.99-127.

[9] H. Shefrin & M. Statman, "The contributions of Daniel kahneman and Amos tversky", *The Journal of Behavioral Finance*, Vol.4, No.2, pp.54-58, 2003.
DOI : https://doi.org/10.1207/S15427579JPFM0402_01

[10] D. VandeWalle, "Development and validation of a work domain goal orientation instrument", *Educational and psychological measurement*, Vol.57, No.6, pp.995-1015, 1997.
DOI : https://doi.org/10.1177/0013164497057006009

[11] R. R. Blake & J. S. Mouton, "Management by Grid® principles or situationalism: Which?", *Group and Organization Studies*, Vol.6, No.4, pp.439-455, 1981.

[12] B. Bulgurcu, H. Cavusoglu & I. Benbasat, "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS quarterly*, Vol.34, No.3, pp.523-548, 2010.

[13] M. Chan, I. Woon & A. Kankanhalli, "Perceptions of information security in the workplace: linking

information security climate to compliant behavior", *Journal of information privacy and security*, Vol.1, No.3, pp.18-41, 2005.

[14] M. Siponen, M. A. Mahmood & S. Pahnila, "Employees' adherence to information security policies: An exploratory field study", *Information and Management*, 51, No.2, pp.217-224, 2014.
DOI : https://doi.org/10.1016/j.im.2013.08.006

[15] P. Ifinedo, "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition", *Information and Management*, Vol.51, No.1, pp.69-79, 2014.
DOI : https://doi.org/10.1016/j.im.2013.10.001

[16] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory", *Computers and Security*, Vol.31, No.1, pp.83-95, 2012.
DOI : https://doi.org/10.1016/j.cose.2011.10.007

[17] Y. Zhao & M. Zhao, "WeChat Users' Information Protection Behavior Based on Prospect Theory", *International Journal of Information and Education Technology*, Vol.9, No.6, pp.390-395, 2019.
DOI : https://doi.org/10.18178/ijiet.2019.9.6.1233

[18] T. Sommestad, H. Karlzén & J. Hallberg, "The theory of planned behavior and information security policy compliance", *Journal of Computer Information Systems*, Vol.59, No.4, pp.344-353, 2019.
DOI : https://doi.org/10.1080/088744417.2017.1368421

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 : 중앙대학교 심리학과 강사

〈관심분야〉
정보보안, 문화, 공동체, 진로개발

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