Journal of Digital Convergence
Vol. 19. No. 2, pp. 105-115, 2021

ISSN 2713-6434 / eISSN 2713-6442
https://doi.org/10.14400/JDC.2021.19.2.105

개인 대처와 조직 동질성 문화에 따른 정보보안 준수 차이 분석

황인호
국민대학교 교양대학 조교수

Analysis of Differences in Information Security Compliance according to Individual Coping and Organizational Homogeneity Culture

In-ho Hwang
Assistant Professor, Department of General Education, Kookmin University

요 약 연구 목적은 탐색적 관점에서 개인 대처와 조직 동질성 문화의 차이에 따른 조직 구성원의 정보보안 준수에 미치는 영향을 확인하는 것이다. 연구는 개인 대처(업무 중심, 감정 중심)과 조직 동질성 문화(동질성, 이질성)으로 집단을 구분하였으며, 교차설계를 통한 각 집단별 정보보안의 차이를 확인하고, 정보보안 준수 선행요인과 정보보안 준수의도간의 이중매개 모델을 제시하였다. 연구 대상은 정보보안 정책을 보유한 조직에 근무하는 직장인을 대상으로 하였으며, SPSS 21.0을 통해 일변량 분석 및 위계적 회귀분석을 실시하였다.
연구 결과, 대처 차원은 감정 중심이 업무 중심보다 정보보안 관련 평균이 높았으며, 동질성 문화 차원은 동질성이 이질성보다 정보보안 관련 평균이 높았다. 또한, 정보보안 인식과 준수의도간의 영향 관계를 사회적 영향과 정보보안 관여도가 완전 매개효과를 갖는 것을 확인하였다. 연구 시사점은 조직 문화 차원에 따른 개인의 의사결정 유형의 정보보안 준수의 차이를 확인하였고, 정보보안 준수의도를 높이기 위한 방안을 제시하였다. 즉, 결과는 조직과 개인 특성별 차별화된 정보보안 준수 모델 정립의 방향을 제시한다.

주제어 : 대처, 동질성 문화, 정보보안 인식, 사회적 영향, 정보보안 관여도, 준수의도

Abstract The purpose of this study is to present the effect of differences in individual coping and organizational homogeneity culture on information security compliance from an exploratory perspective. The study divided groups into individual coping (task-oriented, emotion-oriented) and organizational homogeneity culture (homogeneity, heterogeneity), confirms the difference in information security for each group through cross-design and presents a multiple mediation model between information security factors.
As a result of the study, in the coping dimension, the average of the security compliance factors was higher in the emotion-oriented than the task-oriented, and in the homogeneity culture dimension, the average of the security compliance factors was higher in the homogeneity than the heterogeneity. Additionally, social influence and involvement had a multiple mediation effect on the relationship between information security awareness and compliance intention. The implications of this study were to confirm the difference in the effect of individual decision-making styles on security compliance according to the organizational culture differences. The results suggest the necessity of applying a customized information security compliance model for each organization and individual characteristics.

Key Words : Coping, Homogeneity Culture, Information Security Awareness, Social Influence, Security Involvement, Compliance Intention

*This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education(NRF-2020S1A5A8040463)
*Corresponding Author : Inho Hwang(hwanginho@kookmin.ac.kr)
Received December 16, 2020 Revised January 31, 2021
Accepted February 20, 2021 Published February 28, 2021

1. 서론

정보 자산 보호가 조직의 중요한 활동으로 인식되면서, 조직들은 정보보안 관련 기술 및 정책 도입에 투자를 높이고 있다. 전 세계적으로 정보보안 기술 시장은 연평균 10% 이상 성장하고 있으며, 글로벌 기업을 중심으로 정보보안 관련 국제 표준을 확보하기 위한 노력을 진행하고 있다[1].

하지만, 정보보안 사고는 줄어들지 않고 있다. Verizon[2020] 보고서는 조직의 정보보안 사고는 큰 문제가 발생했을 때 드러나는 경향이 있는 것을 확인했으며, 발생한 정보보안 사고의 2/3는 멀웨어, 해킹, 바이러스, 소셜 침입 등 기술적 접근을 통해서 이루어졌으며, 나머지 1/3 사고는 조직 내부자 또는 파트너에 의한 정보 노출로서 발생한 것으로 제시하고 있다[2].

이에, 조직들은 기술적 침입에 대해 보안 기술의 엄격한 적용을 통해 해결하고 있으며, 내부자 또는 파트너에 의한 정보 사고는 보안 정책을 적용함으로써 예방하고자 하고 있다[3]. 하지만, 조직 내부자들의 보안 위협은 조직이 모든 내부자들을 통제 및 관리할 수 없는 상황이고, 정보시스템의 발전에 따른 정보공유가 더욱 활성화되는 현재의 상황들을 감안하면 결코 간과할 수 없는 부분이다.

이에, 조직원의 보안 준수와 관련된 선행연구들은 보안 정책 준수 확대 방안에 대하여 구성원들의 심리적 행동 준수 관점에서 접근하고 있다. 선행연구들은 범죄학, 심리학, 사회학 등에서 적용되던 계획된 행동이론, 제재이론, 합리적 선택이론, 동기 이론 등을 정보보안 분야에 적용하여, 조직과 개인간의 관계에서 보안 동기 향상을 위한 방안을 제시하고 있다[4-8]. 즉, 조직의 정보보안 관련 특성과 개인의 동기는 심리적으로 연계되어 있어, 개인의 정보보안 준수 행동 향상을 위해서는 조직의 보안 관련 정책 및 분위기 등을 고려하여 개인의 보안 동기 향상을 위한 방안을 마련하는 것의 필요성을 제시하였다는 측면에서 높은 시사점을 가진다.

조직과 개인간의 관계에서 개인 특정 행동은 조직의 환경적 특성을 기반으로 개인의 의사결정을 통해 실행된다[5]. 즉, 정보보안 관점에서, 개인이 조직에서 요구한 수준의 보안 정책에 대한 준수행동을 하는 과정은 조직에서 부여한 정보보안 환경적 특성과 자신에게 미치는 영향을 복합적으로 고려하여 준수의도 또는 행동으로 발현된다[4]. 따라서, 개인을 둘러싼 환경적 특징에 따라 개인의 행동 원인을 찾는 것이 중요한 관점이 되며, 개인의 정보보안 준수 행동으로 이어지도록 한다. 특히, 조직만의 특정한 문화적 구조는 개인의 행동에 밀접한 영향을 미친다[7].

이에, 본 연구는 탐색적 관점에서 조직의 문화적 특성과 개인의 문제 대처 유형에 대한 집단적 차이에 의해 정보보안 선행 요인과 준수의도의 차이와 각 요인간의 영향 관계를 확인하고자 한다. 세부적으로 사회문화 심리학 분야에서 적용되는 조직의 문화적 분류 요인인 동질성 문화(동질성-이질성)와 개인의 특정 문제에 대한 대처 유형(업무 중심 대처-감정 중심 대처) 집단, 즉 교차 설계를 통한 4개의 집단에 따라 정보보안 준수 선행 요인(정보보안 정책 인식-사회적 영향-정보보안 관여도)과 정보보안 준수의도의 차이를 찾고자 한다. 즉, 다음 연구질문 1을 탐색적으로 제시하고 연구 설계 및 검증을 하고자 한다.

RQ 1. 조직의 동질성-이질성 문화와 개인의 대처 방식의 차이는 조직원의 정보보안 준수 선행요인과 준수의도에 어떤 차이를 가지는가?

또한, 연구는 제시한 정보보안 준수 선행요인과 준수의도간의 영향관계를 찾고자 한다. 이에, 정보보안 인식이 정보보안 준수의도에 미치는 영향에 있어 사회적 영향과 정보보안 관여도의 이중매개효과가 있을 것으로 판단하고, 평행다중매개모델을 설계한다. 즉, 다음 연구질문 2를 제시하고 영향관계를 검증하고자 한다.

RQ 2. 조직원의 정보보안에 대한 인식은 정보보안 준수의도에 어떻게 영향을 미치는가?

2. 이론적 배경

2.1 대처

대처(coping)는 개인의 외부 환경적 문제 및 요구수준에 대하여 대응하고 관리하기 위해 대응하는 개인의 행동 수준으로서[9], 조직과 개인간의 관계에서, 대처는 조직의 요구사항에 대한 개인의 의사결정의 방식에 대한 개념이다[10]. 즉, 개인은 특정 문제 해결을 위하여 자신만의 대응 방식을 보유하며, 대처 유형별 다른 형태 및 방법으로 문제를 받아들이고 해결하고자 한다.

대처 유형은 2가지로 일반적으로 구분한다[11]. 첫째, 업무중심 대처(task-oriented coping)이다. 업무중심 대처는 자신에게 주어진 문제에 대한 해결에 있어, 문제 원인을 합리적으로 파악하고 업무적 관점에서 해결하고자 하는 성향을 의미한다. 둘째, 감정중심 대처

(emotion-oriented coping)이다. 감정중심 대처는 문제에 대하여 경험하는 자신의 정서를 조정함으로써 문제에 대처하려는 성향을 의미한다.

정보보안 관점에서, 개인의 대처는 정보보안에 의해 발생하는 부정적 측면을 대처하는 개인의 동기적 성향을 설명하기 위해 적용되고 있다[12]. 정보보안 기술 및 정책에 의해 발현된 부정적 특성인 스트레스는 대처 유형에 따라 다른 방식과 수준으로 준수의도에 영향을 주기 때문에, 개인의 대처 방식을 이해하는 것이 필요하다[13]. 본 연구는 개인의 문제 대처 방식으로 업무대처-감정대처로 구분하여, 집단별 정보보안 준수에 미치는 영향의 차이를 확인한다.

2.2 동질성 문화

조직 문화(organizational culture)는 조직의 역사, 비전 및 목표, 분위기 등 구성원들간에 공통적으로 보유하고 있는 목적, 신념, 습관 등 집단 내 특성을 지칭한다[7]. 일반적으로 조직 문화 형성은 집단을 구성하는 구성원들의 공통된 행동 및 사고 방식으로 구축되지만, 한번 구축된 조직 문화는 조직원들의 행동 방식을 다시 결정하도록 요구하는 현상을 가지기 때문에, 조직원의 특정 행동을 결정하는 중요한 선행 조건이다[14].

특정 집단의 문화를 결정하는 요인은 다양하게 제시되고 있지만, 사회문화 심리학에서는 집단 간의 특정 가치를 공유하고 있는 동질성-이질성에 따른 문화의 차이가 존재함을 제시하고 있다[15]. 동질성(homogeneity)은 서로 동일한 성질의 특성을 보유하고 공유하고 있는 수준을 의미하며, 이질성(heterogeneity)은 서로 상이한 성질의 특성을 보유 또는 부분을 가지고 있는 수준을 의미한다. 대표적으로, 우리나라의 경우, 남북한의 문화적 이질성과 동질성 유형에 따라 구성원 조직적 특성 및 개인들의 갈등과 단합 방향을 설명한다[16]. 본 연구는 동일한 조직 문화를 공유하고 있는 수준을 기반으로 동질성과 이질성으로 구분하여, 집단별 정보보안 준수에 미치는 영향의 차이를 확인한다.

2.3 정보보안 인식

정보보안 인식(information security awareness)은 조직 내 보안 활동에 대한 일반적인 이해 수준으로 정의되며[4], 정보 자산 보호의 필요성과 노출 시 발생가능한 조직 및 개인에 대한 위협 및 예상되는 피해 등에 대하여 전체적으로 이해하고 있는 수준을 말한다[7].

조직에서 개인이 가지는 정보보안에 대한 전반적인 인식은 조직 환경적 특성과 개인 성향에 따라 다르게 인식된다. 특히, 개인의 위험감수성, 개방성 등 개인별 성향에 따라, 또는 조직 내·외부 환경적 상황에 따라 인식 수준을 달리하는 경향이 있다[17]. 하지만, 조직은 정보보안 관련 교육 활동(세미나, 워크숍 등), 홍보 캠페인 등을 통해 개인의 보안 인식을 높일 수 있다[18]. 개인이 보유한 정보보안 인식이 중요한 이유는 정보보안 관련 동기를 형성하고, 행동 의지로 발현되기 위해서는 우선적으로 관련된 상황을 이해하고 인식하는 것이 우선되어야 하며, 인식 수준이 높아질수록 긍정적 행동으로 이어지기 때문이다[4].

2.4 사회적 영향

사회적 영향(social influence)은 정보보안과 관련된 조직의 상황에 따라 구축된 특수한 문화에 대한 개인의 내재화된 영향 수준으로서[5], 정보보안과 관련된 조직의 분위기, 구성원들의 행동이 개인에게 반영되어 행동으로 이어지도록 돕는 선행요인이다[19].

개인의 정보보안 준수행동은 주변 환경으로부터 확보된 다양한 정보로부터 긍정적인 보안 동기가 형성될 때 높아지는데, 조직 차원의 보안 정책, 시스템와 같은 외적 요인과 보안 문화와 같은 내적 요인을 복합적으로 받아들여 자신만의 동기를 형성시킨다. 이때, 사회적 영향은 자신을 둘러싼 보안적 특성과 주변의 행동을 복합적으로 받아들여 형성되기 때문에, 동일시 관점에서 준수의도를 높이는 효과를 제시한다[7,8].

2.5 정보보안 관여도

관여도는 특정한 주제나 활동에 대해 개인이 소비하는 시간, 노력 등을 통해 형성된 관심의 수준으로서, 대상에 대한 관심이 높으면 확보한 정보의 양이 많아져 행동에 영향을 준다[20]. 즉, 관여도는 대상에 대한 관심 및 보유한 지식의 수준으로 설명할 수 있으며, 관여도가 높으면 자신의 생각대로 행동할 가능성이 높다.

정보보안 분야에서도 관여도는 개인의 행동에 영향을 주는 선행 조건으로 적용되고 있다. 정보보안 관여도는 조직이 구축한 정보보안 정책, 기술 등에 대하여 경험하고, 참여하고자 하는 수준으로서[8], 관여도가 형성되면, 정보보안 관련 준수 행동을 높일 뿐만 아니라[8], 조직에 도입한 기술에 의해 발생할 수 있는 부정적 영향인 스트레스를 완화할 수 있어[21], 조직의 요구에 대한 긍정적

행동을 높일 수 있는 중요한 선행 조건이다.

2.6 정보보안 준수의도

조직 구성원의 정보보안 수준 향상은 조직 전체의 정보보안 목표 달성에 중요한 선행조건이다. 하지만, 조직과 개인간의 관계는 대리인 문제에 직면한다. 정보보안 행동 정보에 대한 개인과 조직간의 정보 불균형은, 개인을 도덕적 해이에 빠지게 할 수 있으며, 조직은 역선택을 할 수 있다[22]. 따라서, 정보보안 행동은 개인의 심리적 선택에 크게 의존할 수 밖에 없으며, 개인의 행동 동기를 높이는 활동을 요구한다. 정보보안 준수의도는 조직의 정보자원을 개인 스스로가 보호하고자 하는 의도로서[4], 형성된 준수의도는 보안 행동으로 이어진다. 이에, 정보보안과 관련된 올바른 행동 정보를 제공함으로써, 개인이 올바르게 행동할 수 있도록 가치를 부여하거나[7], 개인 주변의 동료들의 보안 행동을 유발하는 문화형성을 통해 개인의 보안 행동 의지를 확보하도록 하는 것이 필요하다[23]. 본 연구는 정보보안 준수의도에 영향을 주는 선행요인으로 정보보안 인식, 사회적 영향, 그리고 정보보안 관여도를 제시하여 상호간의 영향 관계를 확인한다.

3. 연구 방법

3.1 연구 설계

본 연구는 두 가지 관점의 연구 분석을 실시한다.

첫째, 교차설계를 실시하여, 정보보안 준수 선행요인과 준수의도에 대한 집단간 차이를 확인한다. 즉, 개인 대처 차원(업무 중심-감정 중심), 조직 문화(동질성 문화-이질성 문화) 차원에 따라, 구성된 집단별 정보보안 준수 선행 요인(정보보안 인식, 사회적 영향, 그리고 정보보안 관여도)과 준수의도에 대한 차이 수준을 파악하고자 한다.

둘째, 이중매개효과 설계를 실시하여, 정보보안 요인간의 영향관계를 확인한다. 즉, 정보보안 인식과 준수의도간의 영향관계를 사회적 영향과 정보보안 관여도가 매개하는 영향관계를 파악하고자 한다.

3.2 연구 대상

본 연구는 연구 목적에 대한 검증을 위하여, 정보보안 정책 및 기술을 도입한 조직에서 근무하는 근로자들을 대상으로 설문을 실시하여, 응답 당시의 응답자의 정보보안에 인지에 대한 생각 수준을 측정하여, 정량적 분석을 실시한다. 다만, 응답자 중 IT 관리 또는 보안 부서에서 근무하는 응답자는 설문 대상에서 제외하였는데, 해당 근로자들의 목적은 정보보안 기술 및 정책을 조직 전체에 배포하고 활용하도록 하는 것이어서, 본 연구의 목적인 일반 근로자의 업무에 보안을 적용하는 방향을 찾는 것과 상이하여 제외하였다.

설문은 대학 내 재직자 전형 중 경영학 및 심리학과에 다니는 학생 중, 정보보안 정책을 보유한 조직에서 근무하는 사람들에게 온라인 및 오프라인으로 배포하였으며, 응답 전 연구의 목적과 통계 분석에 대한 내용을 사전에 학생들에게 전달하고 응답을 허가한 사람들만 설문에 응답하도록 하였다. 총 489부를 회수하였으며, 응답에 문제가 있는 설문을 제외하고, 459개의 표본을 분석에 적용하였다.

3.3 측정 도구

설문은 선행연구를 검토하여, 본 연구의 목적에 맞게 수정 및 보완하여 설문 항목을 작성하였다. 설문 응답은 명목척도로 구성된 집단을 구분하는 2개 요인(대처, 동질성)과 등간척도(7점 척도)로 구성된 개인의 정보보안 인지 및 준수를 질문하는 4개 요인(정보보안 인식, 사회적 영향, 정보보안 관여도, 준수의도)으로 구성된다.

집단 구분 요인인 대처(coping)는 “주어진 특정한 문제에 대해 대처하는 개인의 인지된 행동 유형”으로 정의하며[Endler and Parker, 1994], 나는 “문제 해결에 집중” 또는 “감정적 대처에 집중” 2개의 명목척도로 구분하여 선택하도록 하였다. 동질성 문화(homogeneity)는 “동일한 특성을 보유하고 있는 문화 유형”으로 정의하며[15], 우리 조직은 “다양성을 중요하게 생각” 또는 “동일성을 중요하게 생각” 2개의 명목척도로 구분하여 선택하도록 하였다. 정보보안 인식은 “조직의 보안 위협 및 행동 필요성에 대한 인식의 수준”으로 정의하며[4], 선행연구를 기반으로 “전반적으로 잠재적인 보안 위협을 알고 있음”, “잠재적인 보안문제의 비용을 충분히 알고 있음”, “정보보안에 대한 우려와 일반적인 위험을 이해”의 3가지 항목으로 구성하였다. 사회적 영향은 “정보보안 조직 문화 및 환경이 개인에게 영향을 주는 보안 인식 수준”으로 정의하며[8], 선행 연구를 기반으로 “보안 정책은 동료에게 중요”, “동료들의 보안행동이 나에게 영향”, “보안 문화는 행동에 영향”의 3가지 항목으로 구성하였다. 정보보안 관여도는 “정보보안 경험 및 정보를 기반으로 조직 내 보안 활동에 참여하는 수준”으로 정의하며[24], 선행연구를 기반으로 “나는 업무에 정보보안을 적용하는데

관심이 있음", "보안 경험은 보안 위협을 평가하는데 도움", "보안 경험은 보안 행동에 도움"의 3가지 항목으로 구성하였다. 정보보안 준수의도는 "조직 내 보안 위협을 인지하고 정보자산을 보호하고자 하는 행동의도"로 정의하며[6], 선행 연구를 기반으로 "나는 지속적으로 보안 정책을 따를 것", "나는 정보자산 보호를 위하여 보안 정책을 따를 것", "업무 수행 시, 보안 규정 및 절차를 이행할 것"의 3가지 항목으로 구성하였다.

3.4 연구가설

정보보안 준수 선행요인과 준수의도간의 영향관계를 확인하고자 한 연구모형은 정보보안 인식과 준수의도 관계에 사회적 영향과 관여도가 매개효과를 가진다는 개념으로써, 각 연구모델<Fig. 1>의 영향관계에 대한 연구가설을 제시한다.

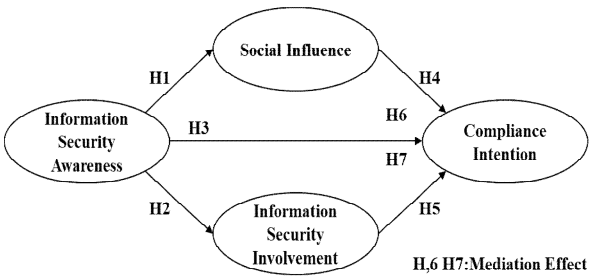

Fig. 1. Research Model

3.4.1 정보보안 인식 관련 연구가설

정보보안 인식은 조직에서 구성원들이 정보보안 행동 위해 필요한 상황에 대한 이해, 필요성 등을 인지하는 요인이다. 즉, 정보보안 인식이 형성되어야 개인의 보안 관련 동기 및 행동으로 전이될 수 있다[4].

첫째, 정보보안 인식은 사회적 영향에 영향을 주는 요인이다. 개인이 조직의 보안 분위기 또는 주변 사람들의 행동을 이해하고 받아들이기 위해서는 조직의 전체적인 보안 상황을 인지하고 있어야 한다[3]. 즉, 정보보안 인식은 정보보안 준수 또는 미준수에 대한 예상되는 결과, 주변의 위협 등을 이해하고 있는 수준이기 때문에[7], 주변의 보안 행동으로 인해 내재화된 개념인 사회적 영향에 우선적으로 영향을 준다[4]. 따라서, 다음과 같은 연구가설을 제시한다.

H1 : 정보보안 인식은 사회적 영향에 긍정적 영향을 줄 것이다.

둘째, 정보보안 인식은 개인의 정보보안 관여도에 영향을 주는 요인이다. 정보보안 관여도는 조직이 추구하는 정보보안에 대하여 이해하고, 참여하고자 하는 수준[24]으로서, 관여도가 형성되기 위해서는 관련 대상에 대한 정보를 보다 많이 확보하고, 자신의 것으로 개념화시켜야 한다[20]. 따라서, 정보보안에 대한 전체적인 인지 개념인 정보보안 인식은 정보보안 관여도에 긍정적인 영향을 미칠 것으로 판단하며, 다음과 같은 연구가설을 제시한다.

H2 : 정보보안 인식이 정보보안 관여도에 긍정적 영향을 줄 것이다.

셋째, 정보보안 인식은 정보보안 준수의도에 영향을 주는 요인이다. Flores and Ekstedt[2016]는 보안 관련 조직 문화를 통해 형성된 개인의 정보보안 인식은 보안 관련 행동의 내적 믿음을 향상시켜 준수의도를 높인다고 하였으며[7], Bulgurcu et al.[2010]은 개인의 보안 관련 합리적 선택은 사전에 형성된 정보보안 인식에 기반한다고 하였다[4]. 따라서, 정보보안 인식이 개인의 정보보안 준수의도를 높이는 요인으로 판단하며, 다음과 같은 연구가설을 제시한다.

H3 : 정보보안 인식은 정보보안 준수의도에 긍정적 영향을 줄 것이다.

3.4.2 사회적 영향 관련 연구가설

사회적 영향은 개인을 둘러싼 조직 및 집단적 특성 및 행동에 의해 영향을 받아 내재화된 개념으로서, 정보보안 준수의도에 영향을 주는 요인이다[19]. Safa et al.[19]은 제재와 예방이론을 연계하여 정보보안 위협을 완화하기 위한 선행 조건을 제시하였으며, 개인을 둘러싼 조직 차원의 조건에 의해 형성된 사회적 영향이 개인의 준수의도를 높이는 요인이라고 하였다. 또한, Flores and Ekstedt[2016]은 정보보안 조직구조가 개인 내적 보안 믿음에 영향을 주며 준수의도를 높인다고 하였는데, 보안 믿음을 자기효능감, 태도, 규범으로 제시하였다[7]. 이에 따라 다음의 연구가설을 제시한다.

H4 : 사회적 영향은 정보보안 준수의도에 긍정적 영향을 줄 것이다.

3.4.3 정보보안 관여도 관련 연구가설

정보보안 관여도는 정보보안 준수의도를 높이는 선행요인이다. 정보보안 관여도는 정보자산 보호에 대한 개인의 관심 수준이기 때문에, 개인에게 확보된 보안관련 정

보를 기반으로 업무에 보안 활동을 접목시키도록 돕는 요인이다[6]. 관여도는 긍정적 행동 수준을 높이는데, Safa et al.[2019]은 내부자의 보안 실수 행동의 감소에 대한 태도 형성에 정보보안 관련 관여도가 영향을 준다고 하였다[8]. 또한, Tarafdar et al.[2007]은 기술 관여도가 조직 내 기술스트레스로 인한 부정적 영향을 완화하는 매커니즘이라고 하였다[21]. 따라서, 다음과 같은 연구가설을 제시한다.

H5 : 정보보안 관여도는 정보보안 준수의도에 긍정적 영향을 줄 것이다.

3.4.4 매개효과 관련 연구가설

정보보안과 관련하여 환경적으로 준수를 위한 구조가 명확하고, 체계적으로 구축될 경우, 조직에 대한 개인의 믿음을 형성시켜 조직이 요구하는 수준 달성을 위한 의지를 높이는 효과를 가진다[19]. 이 때, 정보보안 인식은 조직의 보안 환경 구조에 의해 형성되어 개인의 내적 믿음 요인을 높이는데 영향을 준다[7]. 또한, 개인 차원에서의 보안 행동의 필요성 인식은 조직의 환경적 특성에 기반하며, 조직의 보안 행동에 의해 높아지는 요인인 사회적 영향을 높여 준수의도에 긍정적 영향을 준다[25]. 따라서, 다음과 같은 연구가설을 제시한다.

H6 : 정보보안 인식이 정보보안 준수의도에 미치는 영향에 있어서 사회적 영향의 매개효과가 있을 것이다.

조직의 정보보안 정책, 기술 등 조직원이 업무 중 준수해야할 규칙 및 방식은 개인의 정보보안 인식 수준을 높여 준수의도에 영향을 준다. 정보보안 관련 형성된 인식은 정보보안에 대한 관여도 수준을 높이고[20], 형성된 보안에 대한 관여는 준수의도를 높이는데 일조한다[8]. 즉, 정보보안 인식은 정보보안에 관여하도록 하고, 정보보안 요구 수준을 달성하기 위한 의도 형성에 도움을 준다. 따라서, 다음과 같은 연구가설을 제시한다.

H7 : 정보보안 인식이 정보보안 준수의도에 미치는 영향에 있어서 보안 관여도의 매개효과가 있을 것이다.

4. 연구 결과

4.1 기초통계

분석에 적용된 459개의 표본의 기초 통계분석을 집단별 실시한 결과는 다음 Table 1과 같다.

Table 1. Participants Distribution

Coping	Organization Homogeneity	sex		Job Position			Total
		male	female	under Manager	Manager	Over Manager	
Task coping	Heterogeneity	78	62	56	46	38	140
	Homogeneity	45	41	49	20	17	86
	total	123	103	105	66	55	226
Emotion coping	Heterogeneity	33	47	55	19	6	80
	Homogeneity	80	73	118	25	10	153
	total	113	120	173	44	16	233
total	Heterogeneity	111	109	111	65	44	220
	Homogeneity	125	114	167	45	27	239
	total	236	223	278	110	71	459

업무 중심 대처 유형은 226개, 감정 중심 대처 유형은 233개였으며, 이질성 중심 문화는 220개, 동질성 중심 문화는 239개로 집단별 비슷한 규모의 표본적 특성을 가지고 있었다. 성별로 구분 시, 남성 236개, 여성 223개를 중심으로 집단 간 유사한 비율로 성별 특성을 가지고 있는 것으로 나타났으며, 직위로 구분 시, 대리 이하 278개, 과장 110개, 차장 이상 71개로 응답자들의 직위는 대리 이하가 가장 많았으나, 일반적인 조직의 특성을 고려 시 표본은 대표성을 가질 수 있는 것으로 판단 한다.

4.2 교차분석

본 장은 개인 성향인 대처(업무중심-감정중심) 유형과 조직 문화 유형인 동질성(동질성-이질성) 집단 별 개인의 정보보안 준수 선행요인과 준수의도에 미치는 영향의 차이가 있는지를 확인하기 위하여, 교차설계(cross-over design)을 통해 집단간 차이 및 영향 수준을 분석한다.

교차분석을 실시하기 전, 정보보안 인식, 사회적영향, 보안 관여도, 준수의도에 대하여 탐색적 요인분석과 신뢰성 분석을 Table 2와 같이 실시하였다. 연구는 SPSS 21.0을 활용하여 cormbach's α를 분석하였으며, 신뢰성 요구사항인 0.7을 넘은 것으로 나타났다[26].

또한, Harman의 단일요인기법을 통한 공통방법편의(common method bias)수준 분석을 실시하였다. 본 방법은 탐색적 요인분석을 실시하여, 회전 전 해(unrotated solution) 내 하나의 지배요인(one dominant factor)를 확인하는 것으로, SPSS 21.0을 통

Table 2. Exploratory Factor Analysis

construct	1	2	3	4	Crombach' α
ISA1	.048	.083	**.836**	.194	0.799
ISA2	.220	.061	**.835**	−.023	
ISA3	.153	.133	**.761**	.301	
SI1	**.797**	.130	.148	.115	0.803
SI2	**.819**	.109	.135	.160	
SI3	**.812**	.171	.114	.161	
ISI1	.107	**.843**	.158	.116	0.820
ISI2	.191	**.790**	.136	.300	
ISI3	.131	**.833**	−.004	.088	
CI1	.256	.128	.265	**.701**	0.729
CI2	.222	.157	.191	**.772**	
CI3	.033	.165	.026	**.777**	
* ISA(Information Security Awareness), SI(Social Influence), ISI(Information Security Involvement), CI(Compliance Intention)					

한 분석 결과 가장 많은 설명력을 가진 설명분산은 37.710으로 나타나, 공통방법편의 문제는 낮은 것으로 판단된다[26].

교차분석은 SPSS 21.0의 일변량 분석으로 검증하였다. 첫째, 대처유형과 조직 동질성 변인이 정보보안 인식에 미치는 영향의 차이 검증을 실시하였다. 대처유형별 정보보안 인식 평균을 분석한 결과, 감정중심 대처(M = 4.95)가 업무중심 대처(M = 4.95)보다 높은 평균을 가지는 것으로 나타났으며, 대처 요인이 정보보안 인식에 미치는 영향은 통계적으로 유의하지 않은 것으로 나타났다(F(1, 455), n.s.). 동질성의 정보보안 인식 평균을 분석한 결과 동질성 문화(M = 5.10)가 이질성 문화(M = 4.78)보다 높은 평균을 가지는 것으로 나타났으며, 동질성이 정보보안 인식에 미치는 영향은 통계적으로 유의한 것으로 나타났다(F(1, 455), p < 0.01). 또한, 정보보안 인식에 대한 대처와 동질성간의 상호작용효과는 통계적으로 유의한 것으로 나타났다(F(1, 455), p < 0.05).

Table 3. ANOVA of Information Security Awareness

variables	SS	df	MS	F
Coping (C)	1.48	1	1.48	1.17
Homogeneity (H)	13.34	1	13.34	10.52**
C × H	6.08	1	6.08	4.79*

* p < 0.05, ** p < 0.01

대처유형과 동질성 유형이 정보보안 인식에 미치는 집단별 상호작용효과를 확인하기 위하여 그래프로 표현한 결과<Fig. 2>, 업무중심 유형의 집단에서는 동질성, 이질성과 관계없이 정보보안 인식에 미치는 영향이 높았으나, 감정 중심 유형의 집단에서는 이질성 집단이 동질성 집단보다 정보보안 인식이 낮은 수준인 것으로 나타났다. 즉, 감정 중심 집단에서는 동질성 조직 문화에서 높게 정보보안 인식을 하는 것으로 나타났다.

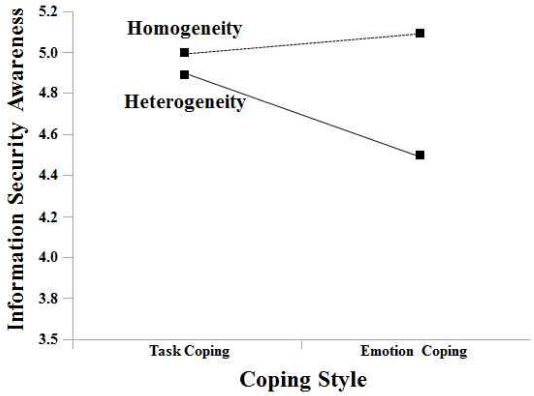

Fig. 2. Interaction Effect of IS Awareness

둘째, 대처유형과 조직 동질성 변인이 사회적 영향에 미치는 영향의 차이 검증을 실시하였다. 대처유형별 사회적 영향 평균을 분석한 결과, 감정중심 대처(M = 5.37)가 업무중심 대처(M = 5.21)보다 높은 평균을 가지는 것으로 나타났으며, 대처 요인이 사회적 영향에 미치는 영향은 통계적으로 유의하지 않은 것으로 나타났다(F(1, 455), n.s.). 동질성의 사회적 영향 평균을 분석한 결과 동질성 문화(M = 5.57)가 이질성 문화(M = 4.99)보다 높은 평균을 가지는 것으로 나타났으며, 동질성이 사회적 영향에 미치는 영향은 통계적으로 유의한 것으로 나타났다(F(1, 455), p < 0.01) <표 6>. 또한, 사회적 영향에 대한 대처와 동질성간의 상호작용효과는 통계적으로 유의한 것으로 나타났다(F(1, 455), p < 0.05).

Table 4. ANOVA of Social Influence

variables	SS	df	MS	F
Coping (C)	0.02	1	0.02	0.01
Homogeneity (H)	35.97	1	35.97	34.18**
C × H	5.74	1	5.74	5.45*

* p < 0.05, ** p < 0.01

대처유형과 동질성 유형이 사회적 영향에 미치는 집단별 상호작용효과를 확인하기 위하여 그래프로 표현한 결과<Fig. 3>, 업무중심 유형의 집단에서는 동질성, 이질성과 관계없이 정보보안 인식에 미치는 영향이 높았으나,

감정 중심 유형의 집단에서는 이질성 집단이 동질성 집단보다 정보보안 인식이 낮은 수준인 것으로 나타났다. 즉, 감정 중심 집단에서는 동질성 조직 문화에서 높은 사회적 영향 인식을 하는 것으로 나타났다.

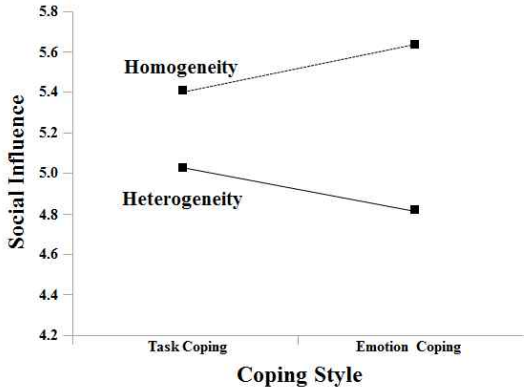

Fig. 3. Interaction Effect of Social Influence

셋째, 대처유형과 조직 동질성 변인이 정보보안 관여도에 미치는 영향의 차이 검증을 실시하였다. 대처유형별 보안 관여도 평균을 분석한 결과, 감정중심 대처(M = 4.39)가 업무중심 대처(M = 4.33)보다 높은 평균을 가지는 것으로 나타났으며, 대처 요인이 보안 관여도에 미치는 영향은 통계적으로 유의하지 않은 것으로 나타났다(F(1, 455), n.s.). 동질성의 보안 관여도 평균을 분석한 결과 동질성 문화(M = 4.62)가 이질성 문화(M = 4.08)보다 높은 평균을 가지는 것으로 나타났으며, 동질성이 보안 관여도에 미치는 영향은 통계적으로 유의한 것으로 나타났다(F(1, 455), p < 0.01). 또한, 보안 관여도에 대한 대처와 동질성간의 상호작용효과는 통계적으로 유의하지 않은 것으로 나타났다(F(1, 455), n.s.).

Table 5. ANOVA of Security Involvement

variables	SS	df	MS	F
Coping (C)	1.05	1	1.05	0.74
Homogeneity (H)	34.85	1	34.85	24.55**
C × H	1.87	1	1.87	1.32

* p < 0.05, ** p < 0.01

마지막으로, 대처유형과 조직 동질성 변인이 준수의도에 미치는 영향의 차이 검증을 실시하였다. 대처유형별 준수의도의 평균을 분석한 결과, 감정중심 대처(M = 5.26)가 업무중심 대처(M = 4.95)보다 높은 평균을 가지는 것으로 나타났으며, 대처 요인이 준수의도에 미치는 영향은 통계적으로 유의하지 않은 것으로 나타났다(F(1, 455), n.s.). 동질성의 준수의도 평균을 분석한 결과 동질성 문화(M = 5.92)가 이질성 문화(M = 4.22)보다 높은 평균을 가지는 것으로 나타났으며, 동질성이 준수의도에 미치는 영향은 통계적으로 유의한 것으로 나타났다(F(1, 455), p < 0.01). 또한, 준수의도에 대한 대처와 동질성간의 상호작용효과는 통계적으로 유의하지 않은 것으로 나타났다(F(1, 455), n.s.).

Table 6. ANOVA of Compliance Intention

variables	SS	df	MS	F
Coping (C)	2.95	1	2.95	4.59
Homogeneity (H)	321.52	1	321.52	501.16**
C × H	0.58	1	0.58	0.90

* p < 0.05, ** p < 0.01

교차설계 분석 결과는 조직 동질성 문화와 개인 대처 유형에 따라, 정보보안 준수 요인에 미치는 영향의 차이가 있음을 확인하였다. 전체적으로, 대처 유형 중 감정중심 대처가 업무중심 대처보다 평균이 높았으나, 영향의 차이는 없는 것으로 나타나 개인의 대처 유형에 따른 정보보안 준수 인식에 미치는 영향 차이는 낮은 것으로 판단된다. 하지만, 정보보안 분야에서는 개인의 감정에 따른 영향이 높기 때문에, 감정적 대처를 하는 사람에게는 조직과 개인간의 정서적 유대감을 높이는 정보제공이 필요하다고 판단된다.

또한, 동질성 문화에서 동질성 집단이 이질성 집단보다 정보보안 인식 요인 평균이 높았으며, 전체적으로 집단간 차이가 있는 것을 확인하였다. 즉, 정보보안 관련 행동은 동일한 특성을 중요시 여기는 집단에서 높게 나타나는 것을 의미하기 때문에, 이질적 집단보다 정보보안 수준이 높아진다고 판단된다.

마지막으로, 대처-동질성간의 상호작용효과는 정보보안 인식과 사회적 영향에 나타났는데, 업무중심 대처 보다는 감정중심 대처에서 동질성-이질성 집단 평균 차이가 높았다. 즉, 조직과 동일시하는 감정적 대응 집단에서 정보보안의 중요성을 높게 인식하기 때문에, 동질성 유형의 조직은 개인의 보안에 대한 정서적 접근을 하는 것이 필요하다.

4.3 연구모델 분석

본 연구에서 제시한 이중매개모델은 SPSS 21.0의 위계적 회귀분석을 통해 실시하며, 이중매개효과에 대한 확

인은 Process 3.1을 통해 Table 7과 같이 확인한다.

Table 7. Hierarchical Regression Analysis of Mediation Model

step		path	beta	t-value
0 step	H3	ISA → CI	.230	5.04**
1-1 step	H1	ISA → SI	.421	9.93**
	H2	ISA → ISI	.300	6.71**
1-2 step	H4	SI → CI	.259	5.33**
	H5	ISI → CI	.214	4.62**
2 step	H3'	ISA → CI	.056	1.18

** p < 0.01
※ ISA(Information Security Awareness), SI(Social Influence), ISI(Information Security Involvement), CI(Compliance Intention)

첫째, 정보보안 인식이 사회적 영향을 거쳐 정보보안 준수의도에 미치는 영향을 설명하는 매개모형을 검증하였다. 정보보안 인식이 준수의도에 미치는 영향력은 유의한 것으로 나타났으며(H3 : β = 0.230, p < 0.01), 정보보안 인식이 사회적 영향에 미치는 영향력(H1 : β = 0.421, p < 0.01)과 사회적 영향이 준수의도에 미치는 영향력(H4 : β = 0.259, p < 0.01) 모두 통계적으로 유의한 것으로 나타났다. 하지만, 전체 요인에서 정보보안 인식이 준수의도에 미치는 영향은 유의하지 않은 것으로 나타났다(H3' : β = 0.056, n.s.),

둘째, 정보보안 인식이 정보보안 관여도를 거쳐 정보보안 준수의도에 미치는 영향을 설명하는 매개모형을 검증하였다. 정보보안 인식이 준수의도에 미치는 영향력은 유의한 것으로 나타났으며(H3 : β = 0.230, p < 0.01), 정보보안 인식이 정보보안 관여도에 미치는 영향력(H2 : β = 0.300, p < 0.01)과 정보보안 관여도가 준수의도에 미치는 영향력(H5 : β = 0.214, p < 0.01) 모두 통계적으로 유의한 것으로 나타났다. 하지만, 전체 요인에서 정보보안 인식이 준수의도에 미치는 영향은 유의하지 않은 것으로 나타났다(H3' : β = 0.056, n.s.).

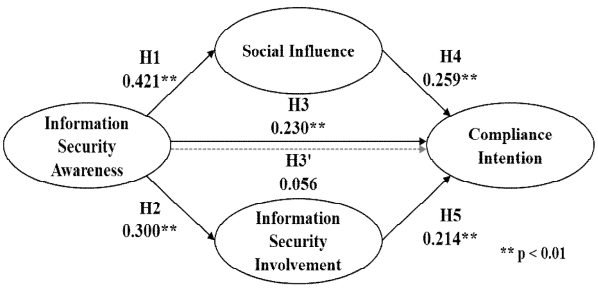

Fig. 4. Result of Multiple Mediator Model

두 개의 매개 경로에서 완전매개 효과가 존재하는 것으로 나타나, Process 3.1을 통해 이중매개효과가 존재하는지 확인하였다. 보안 인식과 준수의도간의 직접효과는 없는 것으로 나타났으며(t = 1.18, n.s.), 사회적 영향(H6)과 정보보안 관여도(H7)의 간접효과를 확인한 결과, 사회적 영향과 정보보안 관여도 모두 신뢰구간 사이에 '0'을 포함하지 않아 간접효과가 있는 것으로 나타났다. 즉, 평행다중매개모델(parallel multiple mediator model)이 형성된 것으로 나타났다.

Table 8. Indirect Effects of SI and ISI

		Effect	BootSE	BootLLCI	BootULCI
H6	SI	0.1120	0.0267	0.0603	0.1630
H7	ISI	0.0657	0.0177	0.0350	0.1630
	(CI)	−0.0463	0.0358	−0.1160	0.0240

※ SI(Social Influence), ISI(Information Security Involvement),

이중매개모델에 대한 영향관계를 분석한 결과, 정보보안 인식과 준수의도간의 영향관계에 사회적 영향과 정보보안 관여도가 각각 매개효과를 가지는 것을 확인하였다. 즉, 정보보안 준수의도에 미치는 개인의 동기는 조직에서 제공한 다양한 보안 관련 정보를 기반으로 형성된 정보보안 인식에 기반하는 것을 확인하였으며, 형성된 정보보안 인식은 조직 보안 환경에 의해 영향을 받는 요인인 사회적 영향과 개인의 정보보안 관여도에 영향을 줌으로써, 외적 측면과 내적 측면에서 정보보안 준수의도에 복합적인 영향을 주는 것을 확인하였다. 따라서, 조직은 개인의 정보보안 준수의도 향상이 사전적인 정보보안 인식에 기반함을 인지하고 관련 정보보안 정보들을 제공하는 것이 필요하다.

5. 결론

본 연구는 조직 동질성 문화와 개인 대처 유형에 따른 정보보안 준수 선행요인과 준수의도에 대한 인식 차이 검정과, 정보보안 준수요인들간의 영향관계를 확인함으로써, 정보보안 준수 수준 향상을 위한 차별화된 학술적 관점, 실무적 관점의 시사점을 제시한다.

첫째, 본 연구는 기존 선행연구에서 필요성을 제시했던 조직과 개인 특성에 따른 집단별 정보보안 준수 선행요인과 준수의도에 미치는 영향의 차이를 확인하였다는 측면에서 시사점을 가진다. 학술적 관점에서 조직원의 정

보보안 준수 관련 선행요인과 준수의도가 조직의 환경적 특성과 개인의 의사결정 관점에 의해서 차이가 나타난다는 것을 확인하였기 때문에, 향후 조직 문화 등 집단의 특성별 맞춤형 정보보안 지원 방향을 제시했다는 시사점을 가진다. 실무적 관점에서 결과는 조직의 정보보안 요구수준에 대한 개인의 행동은 자신을 둘러싼 외적 환경과 내적 동기에 의해서 결정되는 것을 확인하였기 때문에, 정보보안에 대한 집단별 특성에 맞는 차별화된 정보보안 준수 전략의 수립 필요성을 제시하였다는 시사점을 가진다.

둘째, 조직 문화를 구분하기 위해서 사회문화 심리학에서 주로 활용되던 동질성 요인을 적용하여, 조직 문화적 특성을 집단화하였다. 즉, 연구는 동질성 문화와 이질성 문화 집단에 따른 정보보안 준수 인식에 미치는 차이를 확인하였으며, 동질성 문화 집단이 이질성 문화 집단보다 정보보안 준수 선행요인과 준수의도에 대한 평균이 높은 것을 확인하였다. 학술적 관점에서 연구는 개인의 정보보안 관련 행동은 조직의 문화적 특성에 기인하는 것을 확인하였다. 특히 유사한 성향을 추구하는 집단인지를 설명하는 동질성 요인을 가진 조직 문화의 평균이 더 높음을 제시하였기 때문에, 정보보안에 영향을 주는 조직 문화의 선행 연구가 되었다고 판단된다. 실무적 관점에서 연구는 집단의 성격이 비슷한 집단에서 개인의 정보보안 준수 선행 요인과 준수의도의 평균이 높은 것을 확인하였기 때문에, 조직 문화적 성격에 맞는 보안 수행 전략의 수립의 필요성을 제시하였다.

셋째, 개인의 의사결정에 대한 행동 방식인 대처 유형 집단에 따라 정보보안 준수 선행요인과 준수의도에 대한 평균의 차이가 있음을 확인하였다. 비록, 정보보안 인식에 미치는 영향 차이는 기각되었지만, 감정 중심 대처가 업무 중심 대처보다 평균이 높았고, 정보보안 인식, 사회적 영향 요인에 대하여 대처 유형과 동질성 문화 유형에 의한 상호작용효과가 존재함을 확인하였다. 학술적 관점에서 연구는 개인의 대처가 동질성 문화와 연관 관계가 있음을 확인하였으며, 실무적 관점에서 감정 중심 대처의 사람들은 이질성 집단에서 동질성 집단보다 정보보안 인식과 사회적 영향을 적게 받는 것으로 나타나, 조직이 구성원을 위해 지향해야 할 방향을 제시하였다.

마지막으로, 연구는 정보보안 인식, 사회적 영향, 정보보안 관여도, 준수의도 간의 완전매개효과를 갖는 것을 확인하였다. 학술적 관점에서 연구는 개인에게 형성된 정보보안 준수의 필요성 및 위협과 같은 인식이 준수의도에 미치는 매커니즘을 제시하였다는 측면에서 시사점을 가진다. 또한, 실무적 관점에서 자발적인 보안 행동 향상을 위해서는 사회적 영향과 관여도에 영향을 주는 정보보안 인식 수준을 높이기 위한 전략이 필요함을 제시한다.

연구는 조직의 동질성 문화 유형과 개인의 문제 대처 요인을 활용하여 4개의 집단으로 구분하여, 정보보안 준수 인식 요인에 미치는 영향을 제시하였다는 측면에서 시사점을 가지지만, 다음과 같은 연구적 한계를 가진다. 첫째, 연구는 조직 특성, 개인 특성을 고려한 집단을 유형화하여 응답자가 설문 당시의 응답을 통해 구분하였다. 하지만, 조직의 문화적 특성의 경우 개인의 생각에 의존하였기 때문에 보다 객관적 측면에서 문화적 특성을 구분할 필요성이 있다. 예를 들어 동양의 집합주의, 서양의 개인주의 문화와 같이 명확하게 구분할 수 있는 집단 분석을 통해 결과의 보편성을 확보하는 것이 필요하다. 둘째, 연구는 개인의 의사결정 특성을 대처 유형으로 구분하였으나, 전망이론, 목표초점이론과 같이 개인의 의사결정에 도움을 주는 유형 이론이 다양하게 존재하기 때문에, 향후 연구에서는 보다 다양한 개인의 유형을 구분하여 분석하는 것이 필요하다. 마지막으로, 본 연구는 조직 차원의 업종, 개인의 직무 등을 구분하여 분석하지 않았는데, 제조업과 서비스업, 영업직 등 다양한 조건별 준수 행동에 미치는 영향의 차이를 분석한다면 보다 높은 현실적 시사점을 가질 것으로 판단한다.

REFERENCES

[1] *Security Type, By Solution, By Service, By Deployment, By Organization, By Application, By Region, And Segment Forecasts, 2020 - 2027*.

[2] Verizon. (2012). *2012 data breach investigations report*.

[3] I. Hwang & S. Kim. (2018). A Study on the Influence of Organizational Information Security Goal Setting and Justice on Security Policy Compliance Intention. *Journal of Digital Convergence*. *16(2)*, 117-126. DOI : 10.14400/JDC.2018.16.2.117.

[4] 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.

[5] A. C. Johnston & M. Warkentin. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, *34(3)*, 549-566, 2010. DOI : 10.2307/25750691

[6] 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.

[7] W. R. Flores & M. Ekstedt. (2016). Shaping Intention to Resist Social Engineering through Transformational Leadership, Information Security Culture and Awareness. *Computers & Security*, *59*, 26-44. DOI : 10.1016/j.cose.2016.01.004.

[8] N. S. Safa, C. Maple, S. Furnell, M. A. Azad, C. Perera, M. Dabbagh & M. Sookhak. (2019). Deterrence and Prevention-based Model to Mitigate Information Security insider Threats in Organisations. *Future Generation Computer Systems*, *97*, 587-597. 10.1016/j.future.2019.03.024

[9] J. E. Higgins & N. S. Endler. (1995). Coping, Life Stress, and Psychological and Somatic Distress. *European Journal of Personality*, *9(4)*, 253-270. DOI : 10.1002/per.2410090403

[10] H. Jang & S. Kim (2018), The Effects of Maladaptive Perfectionism and Stress Coping on Chronic Fatigue of Adolescent Athletes through Convergence. *Journal of Digital Convergence*, *16(1)*, 371-379.

[11] S. Folkman & R. S. Lazarus. (1985). If It Changes It Must Be a Process: Study of Emotion and Coping during Three Stages of a College Examination. *Journal of Personality and Social Psychology*, *48(1)*, 150-170.

[12] J. D'Arcy, T. Herath & M. K. Shoss. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*, *31(2)*, 285-318. DOI : 10.2753/MIS0742-1222310210.

[13] P. S. Galluch, V. Grover & J. B. Thatcher. (2015). Interrupting the Workplace: Examining Stressors in an Information Technology Context. *Journal of the Association for Information Systems*, *16(1)*, 1-47. DOI : 10.17705/1jais.00387.

[14] Q. Hu, T. Dinev, P. Hart & D. Cooke. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences*, *43(4)*, 615-660. DOI : 10.1111/j.1540-5915.2012.00361.x.

[15] K. M. Carley. (1995). Communication Technologies and their Effect on Cultural Homogeneity, Consensus, and the Diffusion of New Ideas. *Sociological Perspectives*, *38(4)*, 547-571. DOI: 10.2307/1389272.

[16] J. Chae & J. Lee. (2004). North Korea-South Korea Cultural Heterogeneity in Psychological Perspective: Focusing on the North Korean Defectors` Adaptation. *Korean Journal of Psychological and Social Issues*, *19(2)*, 79-101.

[17] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius & M. Pattinson. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior*, *69*, 151-156. DOI : 10.1016/j.chb.2016.11.065.

[18] E. H. Park, J. Kim & Y. S. Park. (2017). The Role of Information Security Learning and Individual Factors in Disclosing Patients' Health Information, *Computers & Security*, *65*, 64-76. DOI :10.1016/j.cose.2016.10.011.

[19] I. Hwang & H. Lee. (2016). The Employee's Information Security Policy Compliance Intention: Theory of Planned Behavior, Goal Setting Theory, and Deterrence theory Applied. *Journal of Digital Convergence*, *14(7)*, 155-166, DOI : 10.14400/JDC.2016.14.7.155.

[20] H. H. Chang & S. S. Chuang. (2011), Social Capital and Individual Motivations on Knowledge Sharing: Participant Involvement as a Moderator, Information & Management, 48(1), 9-18. DOI : 10.1016/j.im.2010.11.001.

[21] M. Tarafdar, Q. Tu, B. S. Ragu-Nathan & T. S. Ragu-Nathan. (2007). The Impact of Technostress on Role Stress and Productivity. *Journal of Management Information Systems, 24(1)*, 301-328. DOI : 10.2753/MIS0742-1222240109.

[22] R. West. (2008). The Psychology of Security. *Communications of the ACM*, *51(4)*, 34-40. DOI : 10.1145/1330311.1330320.

[23] I. Hwang & S. 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.

[24] 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.

[25] J. C. Nunnally. (1978). *Psychometric theory* (2nd ed.). New York: McGraw-Hill.

[26] P. Podsakoff, S. MacKenzie, J. Lee, and N. Podsakoff. (2003). Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies, *Journal of Applied Psychology*, *88(5)*, 879-903.

황 인 호(Hwang, In Ho) [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