https://doi.org/10.5392/JKCA.2021.21.04.153

정보보안 준수에 부정적 영향을 미치는 걱정 완화에 대한 연구

A Study on the Mitigation of Anxiety that Negatively Affect Information Security Compliance

황인호
국민대학교 교양대학

Inho Hwang(hwanginho@kookmin.ac.kr)

요약

연구 목적은 조직 구성원의 정보보안 준수의도에 긍정적, 부정적 영향을 주는 선행요인을 찾는 것이다. 세부적으로, 연구는 준수의도에 부정적 영향을 미치는 걱정을 감소시키기 위한 선행 요인을 찾고, 걱정과 준수의도 간의 부정적 관계를 피드백이 조절하는 것을 확인하고자 한다. 설문 대상은 정보보안 정책을 보유한 조직에 근무하는 직장인을 대상으로 하였으며, 구조방정식모델링을 기반으로 주효과 분석과 조절효과 분석을 실시한다.

연구 결과, 걱정은 준수의도에 부정적 영향을 미쳤으며, 경영진의 지원을 통해 높아진 조직문화가 걱정을 감소시키는 것을 확인하였다. 또한, 피드백이 걱정과 준수의도간의 부정적 영향 관계를 조절하는 것을 확인하였다. 연구의 시사점은 정보보안 기술 도입을 통해 발생한 걱정의 부정적 영향을 찾았고, 걱정을 완화하기 위한 방안을 제시하였다. 즉, 연구는 조직 내부의 정보보안 수준 향상을 위해 고려해야 할 전략 방향을 제시한다.

■ 중심어 : | 준수의도 | 걱정 | 경영층지원 | 조직문화 | 피드백 |

Abstract

The purpose of this study is to find precedent factors that positively and negatively affect the information security compliance intention. In detail, the study finds precedent factors to reduce anxiety that negatively affects compliance intentions, and confirms that feedback moderates the negative relationship between anxiety and compliance intention. The questionnaire was targeted at office workers working in organizations with information security policies, and research hypothesis verification was conducted through structural equation modeling to analyze main effects and moderation effects. As a result of the study, anxiety had a negative effect on the compliance intention, and the organizational culture that was raised through management support reduced anxiety of employees. In addition, feedback mitigated the negative impact relationship between anxiety and compliance intention. The implications of this study were to suggest a direction to mitigate the anxiety of the employees of the organization through the introduction and operation of information security technology.

■ keyword : | Compliance Intention | Anxiety | Top Management Support | Organizational Culture | Feedback |

* 이 논문은 2020년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구입니다(NRF-2020S1A5A8040463)

접수일자 : 2020년 12월 09일
심사완료일 : 2021년 01월 18일
수정일자 : 2021년 01월 18일
교신저자 : 황인호, e-mail : hwanginho@kookmin.ac.kr

I. 서론

전 세계적으로 정보보안에 대한 관심이 높아지면서, 조직들의 정보 자산 관리를 위한 투자는 지속적으로 증가하고 있다. 실제로, 글로벌 정보보안 기술 시장의 현황을 살펴보면, 매년 10% 이상 성장하고 있으며, 2024년에는 1,747억 달러에 달할 것으로 예측된다[1]. 또한, 조직의 정보 가치 보호를 위한 인증인 ISO국제 표준 등에 인증을 확보하는 등, 조직들은 대내·외적으로 정보보안을 위한 노력을 하고 있다[2].

하지만, 정보보안 사고는 결코 감소되지 않고 있다. Verizon[2020]은 정보보안 사고는 기업가치를 크게 감소시키는 요인이기 때문에, 조직은 사고가 발생하더라고 감추길 바라는 경향이 있어, 알려진 사고보다 훨씬 많은 정보보안 사고가 발생했을 것으로 예측하고 있다[2]. 그들에 따르면, 조직에 발생하는 보안 사고의 유형을 살펴보면, 해킹, 바이러스, 멀웨어 등 외부의 침입을 통해 발생하는 사고가 매년 전체의 60~70%를 차지하는 것으로 나타났으며, 내부자(insider)에 의한 사고는 20~30%를 차지하는 것으로 나타났다[3]. 정보시스템에 대한 침입 위협은 조직의 엄격한 보안기술의 도입 및 운영을 통해 해결할 수 있으나, 내부자에 의한 보안 위협은 개인의 준수 행동을 높임으로써 해결이 가능하다. 하지만, 개인에게 요구하는 보안 준수행동은 정보공유 시스템이 발전할수록, 외부와의 정보 연계 가능성이 높아질수록 지키기 어려워진다[4]. 즉, 정보기술의 지식공유 목표는 정보보안과 상충되는 면이 있기때문에, 조직원들의 보안 미준수 위협 요인은 지속적으로 발생할 가능성이 높다.

개인의 보안 준수와 관련된 선행연구들은 정보보안 준수에 영향을 주는 개인의 긍정적 동기 형성에 초점을 맞추어 다양한 선행 요인을 제시해왔다. 특히, 사회학, 범죄학, 심리학 등에서 적용하던 이론인 합리적선택이론, 제재이론, 보호동기이론, 계획된 행동이론 등을 연계하여 정보보안 분야에 이론적 적용 및 관련 정보보안 선행 요인의 확장을 추구해왔다[5-8]. 즉, 선행연구들은 조직과 개인간의 관계에서 개인의 행동 동기는 조직이 부여하는 환경 및 보안 특성, 특정한 교육 등 노력 요인 등을 통해서 높아질 수 있다고 보았다. 또한, 개인이 특정한 목표에 대한 의사결정 방식에 따른 행동의 차이 등을 제시함으로써, 내부자의 정보보안 준수 향상 방안을 찾았다는 점에서 높은 시사점을 가진다.

하지만, 조직 내 엄격한 정책 및 기술의 도입은 실제로 업무에 적용해야 하는 조직원에게 불만 등을 발현시키는 요인인데, 정보보안은 빠르게 변화하는 외부 환경에 대응하기 위하여 지속적으로 정책 및 기술 수준을 향상시켜야 하는 부담감을 가진다. 이렇듯, 정보보안 정책의 엄격성과 개인의 부담감은 동시에 발생 하여 개인이 보안 준수를 회피하게 만드는 요인이 된다[9,10]. 하지만, 스트레스와 같이 정보보안 미준수 원인과 완화하기 위한 선행조건 관련 연구는 최근에야 연구가 되기 시작하여, 관련 연구가 부족한 실정이다.

본 연구는 정보보안 준수에 부정적 영향을 주는 요인을 제시하고, 해당 요인을 감소시키거나, 영향을 완화할 수 있는 선행 조건을 제시하는 것을 목적으로 한다. 세부적으로, 부정적 영향요인으로 개인의 정보보안에 대한 걱정을 제시하였으며, 조직 차원의 개선 요인인 경영층 지원, 조직 문화가 걱정을 감소시키는 것을 확인하고자 한다. 더불어, 정보보안 피드백 요인을 적용하여, 준수의도에 미치는 부정적 & 긍정적 영향 요인을 조절하는지를 확인하고자 한다.

연구의 결과는 정보보안 정책&기술로 인한 걱정을 완화시키기 위한 조직의 보안 노력 요인을 제시함으로써, 내부자의 정보보안 준수 수준 향상을 위한 방향을 제시할 수 있을 것으로 판단한다.

II. 이론적 배경

1. 최고경영층 지원

조직의 특정 활동에 대한 최고경영층의 관심과 지원은 구성원들의 관련 활동에 대한 행동을 높이는 주요 선행 조건이다[11]. 특히, 조직 내 새로운 기술 또는 정책 등을 채택하고 도입하기 위한 투자를 하는 경우, 조직 구성원들이 명확하게 접근 방향을 이해하고, 행동할 수 있도록 리더의 역할이 매우 강조된다. 경영진의 관심은 같은 맥락으로서, 특정 목표 달성을 위한 기술 및 정책 도입과 같은 조직 내 새로운 무엇인가를 적용할

때는 항상 내부의 갈등이 발현되는데, 경영진의 의지와 관심, 그리고 명확한 정보의 제공 활동은 구성원들의 행동을 조직이 요구하는 방향으로 유도할 수 있다[12].

정보보안 분야 또한 경영진의 지원(top management support)이 매우 중요한 분야이다. 정보보안은 조직 내 새로운 기술 및 규정을 도입하여 기존 정보 공유활동을 제어하고 정보자산을 보호하는 것이 목적이기 때문에, 구성원들의 업무에 추가적인 보안 활동을 요구한다[13]. 특히, 정보보안은 모든 구성원이 지켜야 하는 규칙이기 때문에, 조직 차원에서 정보보안 관련 목표를 제시하고 장기적 관점에서 기술 투자를 진행하게 된다. 조직의 보안 목표를 달성하기 위한 경영층의 지원은 경영층 주도의 정보보안 미팅 실시, 정보보안 캠페인 활동 운영, 관련 정보 제공을 위한 교육 등을 실시 등이 있다. 이를 통해, 구성원들이 능동적으로 정보보안을 준수하도록 조직 차원의 보안 문화 확대를 위한 노력을 한다[14][15].

2. 조직 문화

조직 문화(organizational culture)는 특정 조직만의 공유된 언어, 행동의미, 패러다임 등으로 표현되는 구성원들이 가치판단을 할 수 있도록 돕는 틀을 의미한다[16]. 즉, 조직 문화는 조직 내 구성원들의 공통된 행동의미이기 때문에, 구성원들의 행동 결과로서 나타나는 틀이며, 조직 문화가 형성된 이후에는 구성원의 행동에 직간접적으로 영향을 주는 선행 조건이 된다[17]. 또한, 조직 문화는 유사 업종, 산업의 조직이라도 다른 차원의 행동적 특성을 발현시킬 가능성이 높아 조직만의 특성을 설명하는 기준점이 된다[18].

정보보안 분야에서도 조직 문화는 조직을 구분하고, 구성원들의 보안 행동을 결정하는 중요한 환경적 조건이다. Knapp et al.[2009]은 정보보안 조직 문화를 구성원들의 보안 행동이 조직의 보안 요구수준 및 목표를 반영하여 올바르게 나타나는 정도로 정의하였다[19]. 즉, 정보보안에 대한 조직 문화의 형성은 개인들의 보안 목표에 대한 올바른 행동 수준을 높여 조직의 보안 관리 수준을 향상시키는 중요한 조건이다[17]. 따라서, 조직은 조직원의 능동적인 보안 행동달성을 위해서, 조직 내 보안 분위기 형성을 위한 노력이 필요하다[18].

3. 걱정

걱정(anxiety)은 개인의 내적 동기(intrinsic motivation) 중 목적 행동에 부정적 영향을 형성시키는 요인이다[13]. 특히, 걱정은 정보시스템과 같이 갑작스럽게 또는 지속적으로 조직의 체계를 변화시키는 환경변화에서 개인이 적응하는가에 대한 부분을 설명하는 요인이다. 즉, 걱정은 정보시스템 등 특정 기술 등을 활용함에 있어 개인에게 발생하는 두려움 또는 우려 사항의 집합 수준으로 정의된다[20].

조직의 환경 또는 특정 대상에 대한 개인의 걱정 수준의 증가는 목표 행동에 대한 회피와 같은 형태의 결과로 발현된다[21]. 즉, 걱정은 정보보안 관련 정책, 기술을 자신에게 적용하기 두려운 상황이기 때문에, 정보보안에 대한 태도, 행동 등을 감소시켜, 조직 내부의 보안 위협을 높이는 요인이 된다[13]. 따라서, 조직은 정보보안 기술 도입에 있어, 조직원의 걱정을 최소화하기 위한 노력을 함께 수행하는 것이 필요하다.

4. 피드백

피드백(feedback)은 개인의 행동에 대해 결과, 평가 등 정보를 제공하는 것을 의미한다[22]. 조직에서 개인은 자신의 행동에 대해 주변으로부터 공식적, 비공식적으로 피드백을 받으며, 피드백으로부터 개선 활동 정보를 취득하고 지식화한다[23]. 즉, 피드백은 개인을 평가하며, 개인의 행동을 유도하는 매커니즘으로써, 조직은 피드백을 통해 조직의 목표에 대해 실행할 수 있는 지식 형성 및 행동으로 옮겨질 수 있도록 한다[24].

정보보안 분야에서 피드백은 개인의 정보보안 활동이 업무 수행 과정에서 적용되는지를 판단하고, 결과 및 개선 방향을 제공하는 활동이기 때문에, 개인의 정보보안 행동에 대한 명확한 방향을 확보하도록 보조하는 역할을 한다[25]. 따라서, 조직이 정보보안 목표를 달성하기 위해서는 다양한 방법을 통해 개인의 보안 행동 절차와 결과에 대하여 정보를 제공하고 스스로 지식화할 수 있도록 돕는 것이 필요하다.

5. 준수의도

조직 내부자들의 정보 노출 사고는 구성원의 직무와 관련 없이 정보시스템에 접근이 가능한 사람이면 발생

시킬 수 있다. 실제로, 정보 노출 사고를 일으킨 개인의 직무 유형은 IT 부서 이외에도 임원, 기술자, 사무직 등 다양하게 나타나고 있다[3]. 내부자들의 정보보안 수준을 높이기 위해서는 정보보안 준수의 필요성을 인지시켜 자발적인 보안 행동을 수행하도록 유도하는 것이 필요하다[13].

다시말해, 조직 구성원들의 정보 보호를 위해서는 정보보안 준수의도를 향상시키는 것이 필요하다. 정보보안 준수의도(information security compliance intention)는 조직 내 잠재적으로 발생가능한 정보 자원 노출 위협으로부터 보호하기 위한 구성원의 행동의지로 정의된다[5]. 즉, 정보보안 준수의도는 조직의 중요 정보자원을 보호하고자 하는 개인의 의지 수준이기 때문에, 준수의도가 높아지면 조직 내부의 보안 위협을 감소시킬 수 있다.

Ⅲ. 연구 모델 및 가설설정

1. 연구모델

본 연구는 조직 내부자들의 정보보안 준수의도에 부정적 영향을 주는 요인(정보보안 걱정)에 대한 완화를 위한 선행 요인을 제시하고, 긍정적 영향(경영층 지원, 보안 문화)을 주는 요인에 대한 강화를 위한 방안을 제시하는 것을 목적으로 한다. 연구 모델은 다음 [그림 1]과 같다.

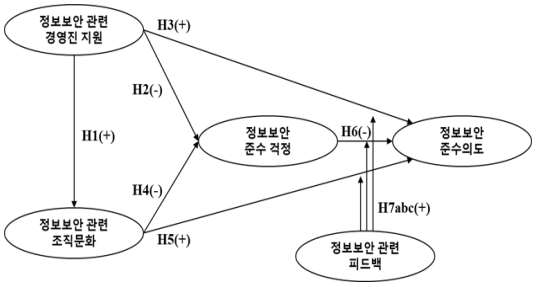

그림 1. 연구모델

2. 연구가설

2.1 최고 경영진 지원 관련 연구가설

정보보안 정책 및 기술 관련된 정보가 조직 내 모든 구성원들에게 스며들고, 구성원들의 보안 준수 목표를 위한 행동을 유도하기 위해서는 경영진의 지원이 무엇보다 중요하다[13].

특히, 정보보안에 대한 경영진의 관심 및 지원은 조직 내 보안 활동 문화를 형성하도록 하는 선행 요인다. 경영진의 리더십은 상향식으로 조직 구성원들이 특정 목표에 대한 행동 방향을 제시하는 선행 요인이기 때문에[26], 엄격한 정보보안 정책 및 기술이 조직에 도입될 때 발생가능한 구성원들의 반발을 최소화하고 행동하는 문화로 만들기 위해서는 경영층이 선도적으로 행동하는 모습이 필요하다[18]. 즉, 경영층의 지원은 조직의 정보보안 분위기 및 행동 문화를 형성하도록 돕는 요인이며, 선행연구를 통하여 다음의 연구가설을 제시한다.

H1. 정보보안 관련 경영진 지원은 정보보안 관련 조직 문화에 긍정적 영향을 줄 것이다.

또한, 정보보안 관련 경영진의 관심 및 참여는 조직 구성원들의 정보보안 관련 걱정을 완화시킨다. 정보보안 관련 기술 도입은 구성원에게 새로운 기술을 이해하고 지식화하도록 요구하기 때문에, 적정한 보안 행동에 대한 걱정을 발현시킬 가능성이 높다[13]. 보안 관련 걱정을 완화시키기 위해서는 정보보안 활동 관련 캠페인, 회의, 정보 제공 등의 활동이 필요한데 경영진의 관심과 지원이 높을 때 더욱 활발하게 발생할 수 있다[19]. 즉, 정보보안에 대한 경영진의 지원은 개인의 보안 준수 걱정을 완화할 것으로 판단하며, 다음의 연구가설을 제시한다.

H2. 정보보안 관련 경영진 지원은 정보보안 준수 걱정에 부정적 영향을 줄 것이다.

마지막으로, 정보보안에 대한 경영진 지원은 조직원의 정보보안 준수에 직접적인 영향을 주는 선행 요인이다. 정보보안 활동에 대한 경영진의 능동적인 참여는 구성원에게 정보보안의 필요성을 인식시키고, 긍정적인 동기를 형성한다[15]. 또한, 경영진의 정보보안에 대한 관심은 조직과 일치하고자 하는 구성원들에게 긍정적

영향을 주어 준수의도를 높인다[27]. 즉, 정보보안에 대한 경영진의 지원은 개인의 보안 준수의도를 높일 것으로 판단하며, 다음의 연구가설을 제시한다.

H3. 정보보안 관련 경영진 지원은 정보보안 준수의도에 긍정적 영향을 줄 것이다.

2.2 정보보안 조직 문화 관련 연구가설

조직 내 정보보안 관련 능동적 행동 분위기 등 문화를 형성하는 것은 구성원들에 대한 정보보안 목표를 제시할 뿐만 아니라 조직과 일체화하려는 개인의 행동을 조직이 요구하는 수준으로 높일 수 있는 중요한 선행조건이다. 특히, 조직에 형성된 조직 문화와 일치하는 사람은 조직 내에서 자신의 위치를 긍정적으로 인식하고, 요구 행동을 하려는 경향이 있는데, 특히 특정 분야에 대한 긍정적인 조직 문화는 개인의 스트레스를 감소시켜 조직 내 개인의 번아웃(burnout)을 최소화할 수 있는 요인이다[28]. Lansisalmi et al.[2000]은 조직 내 개인의 스트레스는 복합적으로 나타나게 되는데, 조직과 일치하려는 가치를 가진 개인은 스트레스를 최소화할 수 있다고 보았다[29]. 선행연구를 기반으로 보안 관련 조직 문화형성은 개인의 정보보안 걱정을 완화할 것으로 판단하며, 다음의 연구가설을 제시한다.

H4. 정보보안 관련 조직 문화는 정보보안 준수 걱정에 부정적 영향을 줄 것이다.

또한, 정보보안 문화의 형성은 조직원의 준수의도 향상에 영향을 주는 선행 요인이다. Chang et al.[2007]은 정보보안 조직 분위기 등 문화를 형성시키기 위한 조직 차원의 노력은 조직원들의 행동 정보를 사전에 제공하는 것이 필연적이기 때문에 지식형성에 도움을 준다고 하였으며[30], Hwang et al.[2016]은 조직 내 실천적인 보안 문화의 형성은 개인의 보안 지식 형성에 영향을 주고 지속적인 준수의도를 높인다고 하였다[18]. 선행연구를 기반으로 정보보안 조직 문화의 형성은 개인의 보안 준수의도에 긍정적 영향을 줄것으로 판단하고 다음의 연구가설을 제시한다.

H5. 정보보안 관련 조직 문화는 정보보안 준수의도에 긍정적 영향을 줄 것이다.

2.3 정보보안 걱정 관련 연구가설

조직 구성원들의 특정 기술에 대한 걱정은 개인의 회피행동을 발현할 뿐 아니라, 조직의 성과에 부정적인 영향을 준다. 정보보안에서 걱정은 도입된 보안 기술의 자신의 업무에 적용의 어려움, 규정에 대한 불명확한 이해 등 복합적으로 발생되는데, 이러한 걱정 수준이 높아질수록 정보보안 위협 요인은 높아지며, 정보보안 준수의도에 부정적 영향을 미치게 된다[12][31]. 즉, 선행연구를 기반으로 정보보안 관련 걱정은 개인의 보안 준수의도에 부정적 영향을 줄 것으로 판단하고 다음의 연구가설을 제시한다.

H6. 정보보안 준수 걱정은 정보보안 준수의도에 부정적 영향을 줄 것이다.

2.4 정보보안 관련 피드백

정보보안 관련 조직 차원의 피드백 활동은 개인의 보안 준수행동에 직접적 또는 간접적으로 긍정적 영향을 미친다. 정보보안 피드백은 개인의 보안 수행 과정 및 결과에 대한 정보를 제공하는 활동이기 때문에 조직이 요구하는 보안 행동 수준에 대하여 명확하게 알 수 있도록 돕는 요인이다. 이러한 활동의 결과는 개인의 정보보안 준수 행동을 높이는 결과로 나타난다. D'Arcy et al.[2009]은 정보보안 미준수 행동을 완화하는 제재 유형과 조직의 시스템적 접근에 대한 연구를 실시하였으며, 조직 차원의 모니터링 및 정보 제공은 개인의 제재 수준을 명확하게 인식시킴으로써 미준수 행동을 감소시킬 수 있다고 하였다[32]. 또한, Hwang[2020]은 정보보안 업무스트레스와 준수의도간의 부정적 관계를 정보보안 피드백 활동이 완화시키는 요인임을 확인하였다[25]. 즉, 선행연구를 기반으로 정보보안 피드백 활동이 정보보안 준수의도에 긍정적 영향을 미치는 요인(경영진 지원, 조직문화)과 부정적 영향을 미치는 요인(걱정)에 조절 효과를 가질 것으로 판단하고, 다음의 연구가설을 제시한다.

H7a. 정보보안 관련 피드백은 경영진지원과 준수의도간의 영향관계를 조절할 것이다.
H7b. 정보보안 관련 피드백은 조직 문화와 준수의도간의 영향관계를 조절할 것이다.
H7c. 정보보안 관련 피드백은 준수 걱정과 준수의도간의 영향관계를 조절할 것이다.

3. 데이터 측정 도구 및 수집

연구 가설 검증은 설문지 기법을 실시하여 적정 설문대상에 대한 응답을 확보하고, 구조방정식모델링을 통해 정량적 분석을 실시한다. 연구 가설에 적용한 요인들의 설문항목은 조직 및 심리학 분야 등에서 활용한 선행연구를 기반으로 정보보안 특성에 맞게 재구성하여 활용하였다.

정보보안 경영진지원은 정보보안 수준 향상을 위한 경영진의 참여 및 노력 정도로 정의[27]하며, "경영진의 정보보안 관련 미팅 참여", "경영진의 정보보안 의사결정에 참여", "경영진의 정보보안 활동에 참여", "보안 시스템 적용을 위한 지원"과 같이 4개 요인으로 구성하였다. 정보보안 보안 문화는 조직의 보안 요구사항이 구성원의 의식과 행동에 반영되어 나타나는 정도로 정의하며[19], "구성원의 정보보안 중요성 인지", "조직 내 보안가치가 중요", "보안 환경이 정보보안에 적합하도록 설계", "업무 수행 시 정보보안 적용", "정보보안은 조직 내 핵심 규범"과 같이 5개 요인으로 구성하였다. 보안 준수 걱정은 정보보안 요구수준에 대한 적정행동에 대한 불안감으로 정의[21]하며, "정보보안은 다소 위협적", "정보보안 행동이 불안", "보안 관련 실수에 대한 염려로 정보보안 관련 행동이 불안"과 같이 3개의 요인으로 구성하였다. 준수의도는 조직 내 정보 보호를 위하여 행동하고자 하는 의지로 정의하며[7], "정보보안에 대한 지속적인 지킴", "조직의 정보를 지속적으로 보호할 가능성이 높음", "업무에 정보보안 규정 및 절차를 준수"와 같이 3개 요인으로 구성하였다. 정보보안 피드백은 정보보안 행동 결과에 대한 정보 제공의 수준으로 정의하며[22], "정보보안에 대한 평가는 업무 개선에 도움", "정보보안 규정준수 개선을 위해 다른 사람들로부터 정보를 제공 받음", "정보보안 준수에 대한 강정과 약점에 대한 유용한 평가를 받음"과 같이 3개의 요인으로 구성하였다.

설문 대상은 정보보안 정책 및 시스템을 도입하여 업무에 적용하고 있는 조직에 근무하고 있는 직장인들을 대상으로 한다. 이중 IT부서, 보안 부서 등은 대상에서 제외하였는데, 본 연구는 일반 업무에서 보안 규정을 준수하도록 돕는 요인을 도출하는데 목적이 있으며, 해당 부서들은 보안 준수가 목표이기 때문에 목적이 다르다고 판단했기 때문이다.

설문은 대학 내 재직자 전형으로 경영학과에 다니는 직장인들에게 실시하였다. 설문은 해당학과들의 수업시간 전, 후에 오프라인으로 실시하였는데, 사전에 관련 설문 목적과 통계 사용의 방식에 대한 정보를 제공하고, 응답을 거절한 사람들을 제외하고 샘플을 확보하였다. 전체 총 450부를 출력하여 배포하였으며, 398부를 회수하였다. 그리고 응답에 문제가 있는 20부를 제외한 378부를 분석 표본으로 활용하였다.

Ⅳ. 가설 검증

1. 기초 통계

표본의 인구통계적 특성은 여성이 56.3%로 남성보다 많았고, 나이는 30대가 40.7%로 가장 많았으며, 직급은 사원급이 38.1%로 가장 많게 나타났다. 각 구분 항목이 차이가 높지 않아 분석에 문제가 없다고 판단하고 연구가설 분석에 적용한다.

표 1. 기초 통계

구분		빈도	%
합계		378	100.0
성별	남성	165	43.7
	여성	213	56.3
나이	〈 30	98	25.9
	31~40	154	40.7
	41~50	107	28.3
	〉 50	19	5.0
직급	사원	144	38.1
	대리	77	20.4
	과장	74	19.6
	차장 이상	83	22.0

2. 신뢰성 및 타당성 분석

본 연구는 다항목 중심의 요인에 대한 설문을 통해 요인간의 관계를 확인하기 때문에, 개별 요인들의 신뢰

성과 타당성 분석을 실시한다.

신뢰성은 요인의 일관성을 확인하기 위한 기법으로서, 본 연구는 SPSS 21.0을 통해 탐색적 요인분석 및 크론바하 알파 값을 통해 신뢰성을 확인한다. 선행연구는 크론바하 알파 값이 0.7이상일 경우 신뢰성이 존재한다고 판단한다 [33], 연구 모델에 적용한 5개 요인의 구성항목은 총 18개로, 신뢰성에 문제가 있는 5개 항목을 제외한 13개의 요인을 분석한 결과, 크론바하 알파 값이 가장 낮은 요인은 걱정(0.859)으로 신뢰성을 확보하였다.

타당성은 다항목 요인들의 일정한 구성으로 나타나며(집중타당성), 요인들간의 차별성(판별타당성)을 가지는지를 확인하는 기법으로 AMOS 22.0의 확인적 요인분석을 실시하여 확인한다. 집중타당성 분석은 개념신뢰도(CR: construct reliability)와 평균분산추출(AVE: average variance extracted)을 통해 분석하며, 선행연구에 따르면 개념신뢰도는 0.7이상을 요구하며, 평균분산추출은 0.5이상을 요구한다[34]. 확인적 요인분석을 위해 구조방정식모델링을 실시한 결과, 모델 적합성은 x^2/df = 2.244, GFI = 0.962, AGFI = 0.920, NFI = 0.976, CFI = 0.986, RMSEA = 0.057로 나타나 적합성이 확보되었으며, 각 요인들은 요구사항보다 높게 나타나 집중타당성을 확보하였다[표 2].

표 2. 구성요인의 신뢰성 및 타당성 분석 결과

변수	항목	요인 적재량	크론바하 알파	CR	AVE
경영진 지원	경영진2 경영진3 경영진4	.907 .902 .883	.961	.927	.810
보안 문화	문화2 문화4 문화5	.819 .824 .835	.945	.892	.734
걱정	걱정2 걱정3	.915 .927	.859	.729	.575
준수의도	의도1 의도2 의도3	.874 .865 .868	.958	.945	.851
피드백	피드백1 피드백3	.946 .946	.911	.749	.599

또한, 연구는 각 요인들간의 차별성을 확보하였는지를 확인하기 위하여 판별타당성 분석을 실시한다. 판별타당성은 각 요인들의 상관계수와 평균분산추출을 비교하여 확인한다. 세부적으로 평균분산추출의 제곱근 값이 상관계수보다 크면 판별타당성이 존재한다고 보며[35], 분석결과는 판별타당성을 확보하였다[표 3].

표 3. 판별타당성 분석 결과

변수	1	2	3	4	5
경영진지원	***0.900***				
보안문화	.570**	***0.857***			
걱정	.208**	.298**	***0.759***		
준수의도	.435**	.639**	.300**	***0.923***	
피드백	.226**	.338**	.071	.189**	***0.774***

Note: 볼드체는 AVE의 제곱근 값임
**: p 〈 0.01

연구는 설문지 기법을 통해 독립변수과 종속변수를 동일한 시점에 확보하였기 때문에, 공통방법편의(common method bias)의 가능성을 확인한다. 공통방법편의 분석 기법은 다양하게 제시되고 있으나, 본 연구는 단일공통방법편의 방법(single common method analysis)을 적용하여 분석한다. 본 방법은 확인적 구조모델에 단일 요인을 추가로 적용하기 전과 적용한 후를 비교하여 측정 도구 값의 변화량을 통해 확인한다[36]. 분석 결과, 공동요인 적용 전과 적용 후의 측정 도구의 차이가 가장 큰 요인이 0.3이하로 나타나 공통방법편의는 크게 높지 않다고 판단하여 가설검증을 실시한다.

3. 주효과 검증

주효과 검증은 구조방정식모델링을 통해 모형간의 경로를 검정하기 때문에, 구조모델의 적합성 검증, 경로(β) 검증, 그리고, 영향력(R^2) 검증의 절차를 통해 확인한다. 첫째, 구조모델의 적합성 검증을 실시한 결과는 x^2/df = 2.755, GFI = 0.934, AGFI = 0.900, NFI = 0.962, CFI = 0.976, RMSEA = 0.068로 나타나, 적합성을 확보하였다. 둘째, 연구 가설간의 경로계수(β) 검증을 통해 가설 검정을 실시한다[그림 2][표 4].

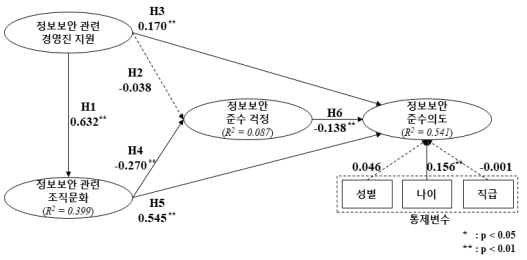

그림 2. 주효과 검증 결과

연구 가설 1은 정보보안 관련 경영진 지원이 조직문화에 긍정적 영향을 준다는 것으로, 분석 결과 경영진의 지원이 높아질수록 정보보안 조직 문화가 높아지는 것으로 나타났다(H1: β= 0.632, p〈0.01). 연구 가설 2는 정보보안 관련 경영진 지원이 정보보안 준수 걱정에 부정적 영향을 준다는 것으로, 분석 결과 경영진의 지원은 개인의 정보보안 준수 걱정에 영향을 주지 않는 것으로 나타났다(H2: β= -0.038, n.s.). 연구 가설 3은 정보보안 관련 경영진 지원이 개인의 준수의도에 긍정적 영향을 준다는 것으로, 분석 결과 경영진의 지원이 높아질수록 정보보안 준수의도가 높아지는 것으로 나타났다(H3: β= 0.170, p〈0.01). 연구 가설 4는 정보보안 관련 조직 문화가 개인의 보안 준수 걱정에 부정적 영향을 준다는 것으로, 분석 결과 조직 문화 수준이 높아질수록 정보보안 걱정을 감소시키는 것으로 나타났다(H4: β= -0.270, p〈0.01). 연구 가설 5는 정보보안 관련 조직문화가 준수의도에 긍정적 영향을 준다는 것으로, 분석 결과 조직 문화 수준이 높아질수록 준수의도를 높이는 것으로 나타났다(H5: β= 0.545, p〈0.01). 연구 가설 6은 정보보안 관련 준수 걱정이 준수의도에 부정적 영향을 준다는 것으로, 분석 결과 준수 걱정이 커질수록 정보보안 준수의도가 낮아지는 것으로 나타났다(H6: β= -0.138, p〈0.01).

표 4. 주효과 분석 결과

경로		추정치	t-값	결과
H1	경영진지원 → 조직문화	0.632	13.781**	지지
H2	경영진지원 → 준수 걱정	-0.038	-0.531	미지지
H3	경영진 지원 → 준수의도	0.170	3.380**	지지
H4	조직 문화 → 준수 걱정	-0.270	-3.566**	지지
H5	조직 문화 → 준수의도	0.545	10.235**	지지
H6	준수 걱정 → 준수의도	-0.138	-3.252**	지지

**: p 〈 0.01

마지막으로, 각 요인들이 결과변수에 미치는 영향력을 확인하기 위하여, 결정계수(R^2)를 확인하였다. 경영진지원은 조직문화에 39.9%의 영향력이 있는 것으로 나타났으며, 조직문화는 준수 걱정에 8.7%의 영향력이 있는 것으로 나타났다. 경영진지원, 조직문화, 그리고 준수 걱정은 준수의도에 54.1%의 영향력이 있는 것으로 나타났다.

주 효과 검증 결과 개인의 정보보안 준수의도에 영향을 미치는 요인으로 조직 경영진의 보안에 대한 지원과 조직 문화 형성이 높은 영향을 미치는 것으로 나타났으나, 정보보안에 대한 걱정이 지속될 경우 준수의도를 감소시키기 때문에, 조직 관점에서 개인의 정보보안 준수에 대한 걱정을 완화하기 위한 노력을 해야함을 시사한다. 개인의 보안 걱정을 완화하는 요인은 경영진지원을 거쳐 형성된 조직문화로 나타났다. 즉, 정보보안 준수와 관련된 조직 문화가 형성되어 개인의 준수 환경을 자연스럽게 만들어줄 때, 개인의 보안에 대한 걱정은 감소할 수 있음을 의미한다.

4. 조절효과 검증

연구 가설 7a, 7b, 7c는 개인의 정보보안 행동에 대한 조직차원의 피드백 활동이 개인의 준수의도에 영향을 주는 요인(경영층지원, 조직문화, 걱정)에 조절효과를 가지는지를 확인한다. 조절효과 검증은 구조방정식 모델링을 통해서 상호작용효과 분석을 실시하여 확인하고자 하며, 엄격한 조절효과 검증 모델인 Lin et al.[2010]이 제시한 기법을 적용하여 분석하였다[37]. 분석 결과는 [표 5]와 같다.

표 5. 조절효과 분석 결과

경로		추정치	t-값	결과
H7a	경영진 → 준수의도	0.547	11.539**	미지지
	피드백 → 준수의도	0.052	1.095	
	경영진x피드백 → 준수의도	0.038	1.47	

H7b	조직문화 → 준수의도	0.729	16.8**	지지
	피드백 → 준수의도	-0.037	-0.899	
	조직문화x피드백 → 준수의도	0.141	3.764**	
H7c	걱정 → 준수의도	-0.323	-6.032**	지지
	피드백 → 준수의도	0.182	3.32**	
	걱정x피드백 → 준수의도	0.093	2.254*	

* p < 0.05, ** p < 0.01

첫째, 피드백이 경영진지원과 준수의도간의 긍정적 영향관계를 조절할 것인지를 확인한 결과, 상호작용효과가 기각되어, 피드백의 조절효과는 발생하지 않은 것으로 나타났다.

둘째, 피드백이 조직문화와 준수의도간의 긍정적 영향 관계를 조절할 것인지를 확인한 결과, 상호작용 효과가 있는 것으로 나타났다. 보다 상세한 조절 효과를 확인하기 위하여, 그래프로 표현한 결과는 [그림 3]과 같다. 피드백이 높은 집단에서 조직 문화가 준수의도에 미치는 영향이 낮은 집단보다 높은 것으로 나타났다. 즉, 피드백은 조직 문화가 준수의도에 미치는 긍정적 영향에 강화 효과를 가진다.

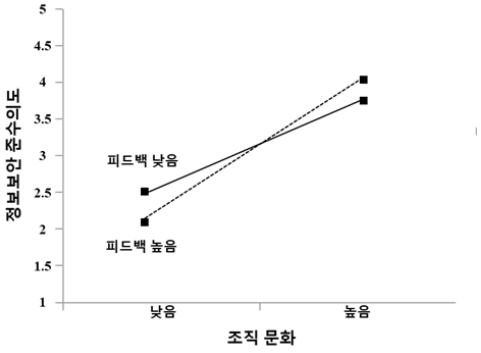

그림 3. 피드백의 조직문화-준수의도에 미치는 영향

셋째, 피드백이 걱정과 준수의도간의 부정적 영향 관계를 조절하는지를 확인한 결과, 상호작용 효과가 있는 것으로 나타났으며, [그림 4]와 같이 나타났다. 피드백이 높은 집단이 낮은 집단보다 걱정이 준수의도에 미치는 부정적 영향을 완화하는 것으로 나타났다. 즉, 피드백은 걱정과 준수의도간의 부정적 관계에 완화 효과를 가지는 것을 확인하였다.

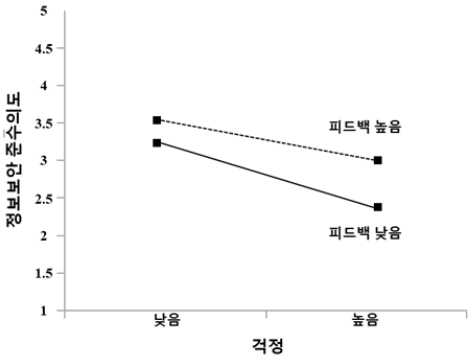

그림 4. 피드백의 준수걱정-준수의도에 미치는 영향

V. 결론

1. 연구 요약

연구는 조직구성원들의 정보보안 준수 걱정이 준수의도에 부정적 영향을 미치고, 걱정을 완화하기 위한 조직 차원의 다각적 행동 요인을 제시하였다. 세부적으로, 조직 행동 관점(경영층지원, 조직 문화, 피드백)과 개인 동기 관점(준수 걱정)을 제시하였으며, 각 영향 관계를 확인하고자 하였다.

연구 가설 확인을 위해, 정보보안 정책 및 기술을 조직에서 적용하고 있는 직장인들을 대상으로 설문을 실시하여, 표본을 확보하였으며, 구조방정식모델링을 통해 연구가설을 검증하였다.

분석 결과는 개인의 정보보안 걱정이 준수의도에 부정적 영향을 미치는 것을 확인하였다. 반면, 경영층의 지원과 조직 문화가 긍정적 영향을 주었으며, 특히, 조직 문화는 걱정을 완화하는 것을 확인하였다. 또한, 조직 차원의 정보보안에 대한 피드백 활동이 조직 문화와 개인의 걱정의 영향을 조절하는 것을 확인하였다.

2. 연구 시사점 및 한계점

본 연구는 다음 관점의 학술적, 실무적 시사점을 가진다. 첫째, 조직 내 정보보안 행동 수준 향상에 부정적 영향을 주는 개인 동기 요인으로 정보보안 준수 걱정을 제시하고 준수의도에 부정적 영향을 미치는 것을 확인하였다. 정보보안 준수 관련 선행연구들은 개인들의 인

지 향상을 위한 동기적 요인을 중점적으로 제시함으로써, 정보보안 준수의도 수준을 높이기 위한 방향을 도출하였으나, 조직 내 개인이 가지는 정보보안 준수 걱정과 같은 부정적 요인을 다각적으로 제시하지 못하였다. 이에 연구는 정보보안 준수 걱정이 준수의도에 부정적 영향을 미치는 것을 확인함으로써, 정보보안 부정적 요인을 학술적 관점에서 제시하였다. 또한, 실무적 관점에서 개인의 정보보안 미준수 원인을 제시하였다. 정보보안 정책과 기술의 준수는 개인에게 새로운 정보를 확보하고 지식을 형성하도록 강요하는 분야이기 때문에, 개인은 정보보안 준수 행동이 적절한지에 대한 걱정을 할 수 있고, 걱정 수준이 높아질수록 관련 행동을 회피하려는 경향을 보인다. 따라서, 실무적 관점에서 조직은 개인에게 충분한 시간과 정보를 제공하는 등의 보안 관련 지원 노력을 실시함으로써 걱정 수준을 낮추기 위한 활동을 할 필요성을 제시하였다.

둘째, 조직의 정보보안 준수 노력 활동이 개인의 준수의도에 긍정적 영향을 미치는 것을 확인하였다. 연구는 조직의 정보보안 준수 노력 요인으로 경영층 지원과 조직 문화 형성을 제시하였다. 학술적 관점에서 결과는 경영층지원이 조직문화에 영향을 주며, 각각의 요인이 개인의 정보보안 준수의도에 긍정적 영향을 주는 선행요인임을 확인하였기 때문에, 조직 정보보안 행동 요인의 선행 연구로서의 학술적 시사점을 가진다. 또한, 실무적 관점에서 정보보안 활동은 조직 전체가 수행해야 할 활동이기 때문에, 상향식 관점에서 경영층이 보안 관련 활동을 능동적으로 실행해야 함을 확인하였으며, 특히 조직의 정보보안 문화를 형성하는데 기여하는 것을 확인하였다. 즉, 조직이 정보보안 준수 활동을 능동적으로 하는 것이 개인의 정보보안 준수의도에 긍정적 영향을 주며, 특히 경영층의 지원을 통해 조직 보안 준수 분위기를 형성시키는 것이 필요함을 시사점으로 제시하였다.

셋째, 개인의 정보보안 관련 준수 걱정을 완화하기 위해 조직이 취해야 할 노력 요인(경영층지원, 조직문화, 피드백)을 확인하였다. 결과는 조직문화가 보안을 준수하는 형태로 형성될수록 개인의 정보보안에 대한 걱정을 완화하는 것을 확인하였으며, 개인 보안 행동에 대한 피드백 활동이 걱정의 준수의도에 미치는 부정적 영향을 감소시키는 것을 확인하였다. 학술적 관점에서, 정보보안 준수에 부정적 영향을 미치는 요인을 완화하기 위한 요인을 도출하였다는 측면에서 학술적 시사점을 가진다. 또한, 실무적 관점에서, 정보보안 관련 개인의 걱정을 형성시키지 않도록 하기 위해서는 조직 보안 문화가 개인의 환경으로서 구축되어야 함을 제시하였으며, 형성된 걱정은 피드백 활동으로 감소시킬 수 있음을 확인하였다는 측면에서 실무적 시사점을 가진다.

넷째, 조직의 정보보안 관련 조직 문화가 정보보안 준수의도에 미치는 긍정적 영향을 피드백 활동이 강화하는 것을 확인하였다. 학술적 관점에서 정보보안 피드백 활동의 강화 효과를 검증하였기 때문에, 관련 연구의 선행연구로서의 가치를 가질 것으로 판단하며, 실무적 관점에서 조직의 정보보안 준수 활동 분위기가 보다 강화되기 위해서는 개인의 보안 행동에 대한 지속적인 피드백을 통해 개인이 행동 정보를 지식화할 수 있도록 지원하는 것이 필요함을 제시하였다.

본 연구는 조직 내부의 정보보안 수준 향상을 위한 구성원의 보안 준수의도에 미치는 영향요인을 다각적으로 제시하였다는 측면에서 시사점을 가지지만, 다음의 연구적 한계점을 가진다. 첫째, 연구는 연구 목적 달성을 위하여 정보보안 정책을 보유한 직장인에게 설문을 통해 양적 검증을 실시하였다. 하지만, 조직의 정보보안 지원(경영층 지원, 조직 문화, 피드백) 활동에 대하여 응답 당시 개인의 인지 수준에 의해서 판단하도록 하였기 때문에, 실제 해당 조직의 정보보안 수준을 명확하게 알 수 없다는 한계점을 가진다. 따라서, 향후 연구에서는 조직의 보안특성 및 수준을 명확하게 판단할 수 있는 기준(예, ISO 도입 및 적용 등)을 제시하여 개인의 행동을 측정한다면 높은 현실적 시사점을 가질 수 있을 것으로 판단한다.

둘째, 연구는 설문의 특성 상 조직의 특성을 배제하고 정보보안 정책 및 기술을 도입한 조직에 대한 개인의 인지 수준 측정을 실시하였다. 하지만, 조직과 개인과의 관계는 조직의 특성에 따라, 개인의 의사결정 성향 등에 따라 다르게 나타날 수 있다. 즉, 집합주의-개인주의, 안정지향 조직-성장지향 조직, 외향성-내향성 등 조직의 다각적 특성과 이성지향-감성지향 등 개인의 의사결정적 특성 등에 따라 다르게 정보보안 행동의 차

이가 발생할 것으로 판단한다.

셋째, 본 연구는 정보보안 정책을 보유한 조직의 근로자에게 설문을 하였으나, 조직의 업종별 특성별 생각의 차이가 있을 것으로 판단한다. 특히, 영업부서와 내근직 부서와 같은 행동의 차이가 발생하는 조직에서의 정보보안에 대한 관심은 차이가 발생할 것으로 판단한다. 향후 연구에서는 이와 같은 집단별 특성 분석을 통해, 집단 유형별 정보보안 준수 행동 영향요인을 제시한다면, 보다 실무적 시사점을 제시할 수 있을 것으로 판단한다.

참 고 문 헌

[1] Grand View Research,.Cyber Security Market Size, Share & Trends Analysis Report By Component, By Security Type, By Solution, By Service, By Deployment, By Organization, By Application, By Region, And Segment Forecasts, 2020 - 2027, 2020.

[2] M. Noh, "The Relationship Analysis of Online Security, Social Network Service, and Smartphone Expenses," Journal of the Korea Contents Association, Vol.19, No.1, pp.648-659, 2018.
DOI : 10.5392/JKCA.2019.19.01.648.

[3] Verizon, *2020 Data Breach Investigations Report,* 2020.

[4] R. West, "The Psychology of Security," Communications of the ACM, Vol.51, No.4, pp.34-40, 2008. DOI : 10.1145/1330311.1330320.

[5] B. Bulgurcu, H. Cavusoglu, and 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.

[6] K. H. Guo, Y. Yuan, N. P. Archer, and C. E. Connelly, "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model," Journal of Management Information Systems, Vol.28, No.2, pp.203-236, 2011.
DOI : 10.2753/MIS0742-1222280208.

[7] Y. Chen, K. Ramamurthy, and K. W. Wen, "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?," Journal of Management Information Systems, Vol.29, No.3, pp.157-188, 2010.

[8] T. Sommestad, H. Karlzén, and J. Hallberg, "The Sufficiency of the Theory of Planned Behavior for Explaining Information Security Policy Compliance," Information & Computer Security, Vol.23, No.2, pp.200-217, 2015.
DOI : 10.1108/ICS-04-2014-0025.

[9] J. D'Arcy and P. L. The, "Predicting Employee Information Security Policy Compliance on a Daily Basis: The Interplay of Security-related Stress, Emotions, and Neutralization," Information & Management, Vol.56, No.7, pp.103151, 2019.
DOI : 10.1016/j.im.2019.02.006.

[10] I. Hwang and O. Cha, "Examining Technostress Creators and Role Stress as Potential Threats to Employees' Information Security Compliance," Computers in Human Behavior, Vol.81, pp.282-293, 2018.
DOI : 10.1016/j.chb.2017.12.022.

[11] A. R. Said, H. Abdullah, J. Uli, and Z. A. Mohamed, "Relationship between Organizational Characteristics and Information Security Knowledge Management Implementation," Procedia-Social and Behavioral Sciences, Vol.123, No.20, pp.433-443, 2014.
DOI : 10.1016/j.sbspro.2014.01.1442

[12] V. L. Mitchell, "Knowledge Integration and Information Technology Project Performance," MIS Quarterly, Vol.30, No.4, pp.919-939, 2006.
DOI : 10.2307/25148759

[13] I. Hwang, D. Kim, T. Kim, and S. Kim, "Why not Comply with Information Security? An Empirical Approach for the Causes of Non-compliance," Online Information Review, Vol.41, No.1, pp.1-17, 2017.
DOI : 10.1108/OIR-11-2015-0358.

[14] T. Kim, "Situation Analysis and Education Plan of Security Ethics for Training College

Students Majoring in Information Security," Journal of the Korea Contents Association, Vol.17, No.4, pp.596-605, 2017.
DOI : 10.5392/JKCA.2017.17.04.596.

[15] I. Hwang, R. Wakefield, S. Kim, and T. Kim, "Security Awareness: The First Step in Information Security Compliance Behavior," Journal of Computer Information Systems, pp.1-12. 2019. DOI: 10.1080/08874417.2019.1650676.

[16] N. J. Adler and M. Jelinek, "Is "Organization Culture" Culture Bound?," Human Resource Management, Vol.25, No.1, pp.73-90, 1986,

[17] S. Ernest Chang and C. S. Lin, "Exploring Organizational Culture for Information Security Management," Industrial Management & Data Systems, Vol.107, No.3, pp.438-458, 2007.
DOI: 10.1108/02635570710734316.

[18] I. Hwang, D. Kim, T. Kim, and J. Kim, "The Study about Security Compliance Intention and Knowledge of Employee based on Security Culture of Organization," Information Systems Review, Vol.18, No.1, pp.1-23, 2016.
DOI : 10.14329/isr.2016.18.1.001.

[19] K. J. Knapp, R. F. Morris, T. E. Marshall, and T. A. Byrd, "Information Security Policy: An Organizational-level Process Model," Computers & Security, Vol.28, No.7, pp.493-508, 2009.
DOI : 10.1016/j.cose.2009.07.001.

[20] M. R. Simonson, M. Maurer, M. Montag-Torardi, and M. Whitaker, "Development of a Standardized Test of Computer Literacy and a Computer Anxiety Index," Journal of Educational Computing Research, Vol.3, No.2, pp.231-247, 1987.

[21] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User Acceptance of Information Technology: Toward a Unified View," MIS Quarterly, Vol.27, No.3, pp.425-478, 2003.

[22] B. E. Wright, "The Role of Work Context in Work Motivation: A Public Sector Application of Goal and Social Cognitive Theories," Journal of Public Administration Research and Theory, Vol.14, No.1, pp.59-78, 2004.
DOI : 10.1093/jopart/muh004.

[23] M. C. Andrews and K. M. Kacmar, "Confirmation and Extension of the Sources of Feedback Scale in Service-based Organizations," The Journal of Business Communication, Vol.38, No.2, pp.206-226, 2001.
DOI : 10.1177/002194360103800204

[24] B. McAfee, V. Quarstein, and A. Ardalan, "The Effect of Discretion, Outcome Feedback, and Process Feedback on Employee Job Satisfaction," Industrial Management & Data Systems, Vol.95, No.5, pp.7-12, 1995.
DOI : 10.1108/02635579510088128.

[25] I. Hwang, "A Study on Mitigation of Information Security Related Work Stress," Journal of Convergence for Information Technology, Vol.10, No.9, pp.123-135, 2020.

[26] Y. Kim and M. Jung, "Interrelationship between leadership, Organizational Culture and Organizational Commitment," Journal of the Korea Contents Association, Vol.12, No.12, pp. 201-211, 2012.
DOI : 10.5392/JKCA.2012.12.12.201.

[27] A. Kankanhalli, H. H. Teo, B. C. Tan, and K. Wei, "An Integrative Study of Information Systems Security Effectiveness," International Journal of Information Management, Vol.23, No.2, pp.139-154, 2003.
DOI: 10.1016/S0268-4012(02)00105-6.

[28] E. S. Williams, L. B. Manwell, T. R. Konrad, and M. Linzer, "The Relationship of Organizational Culture, Stress, Satisfaction, and Burnout with Physician-reported Error and Suboptimal Patient Care: Results from the MEMO Study," Health Care Management Review, Vol.32, No.3, pp.203-212, 2007.
DOI: 10.1097/01.HMR.0000281626.28363.59.

[29] H. Lansisalmi, J. M. Peiro, and M. Kivimaki IV, "Collective Stress and Coping in the Context of Organizational Culture," European Journal of Work and Organizational Psychology, Vol.9, No.4, pp.527-559, 2000.

DOI : 10.1080/13594320050203120.
[30] S. E. Chang and C. S. Lin, "Exploring Organizational Culture for Information Security Management," Industrial Management & Data System, Vol.106, No.3, pp.438-458, 2007. DOI : 10.1108/02635570710734316.
[31] W. S. Brown, "Ontological Security, Existential Anxiety and Workplace Privacy," Journal of Business Ethics, Vol.23, No.1, pp.61-65, 2000. DOI: 10.1023/A:1006223027879.
[32] J. D'Arcy, A. Hovav, and D. Galletta, "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach," Information Systems Research, Vol.20, No.1, pp.79-98, 2009. DOI : 10.1287/isre.1070.0160.
[33] J. C. Nunnally, *Psychometric Theory* (2nd ed.), New York: McGraw-Hill. 1978.
[34] B. H. Wixom and H. J. Watson, "An Empirical Investigation of the Factors Affecting Data Warehousing Success," MIS Quarterly, Vol.25, No.1, pp.17-41, 2001. DOI : 10.2307/3250957.
[35] C. Fornell and D. F. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," Journal of Marketing Research, Vol.18, No.1, pp.39-50, 1981. DOI: 10.2307/3151312.
[36] P. M. Podsakoff, S. B. MacKenzie, J. Y. Lee, and N. P. Podsakoff, "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," Journal of Applied Psychology, Vol.88, No.5, pp.879-903, 2003. DOI : 10.1037/0021-9010.88.5.879.
[37] G. C. Lin, Z. Wen, H. W. Marsh, and H. S. Lin, "Structural Equation Models of Latent Interactions: Clarification of Orthogonalizing and Double-mean-centering Strategies," Structural Equation Modeling, Vol.17, No.3, pp. 374-391, 2010. DOI : 10.1080/10705511.2010.488999.

저 자 소 개

황 인 호(Inho 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