Journal of the Korea Industrial Information Systems Research Vol.26 No.3, Jun. 2021 :23-39
http://dx.doi.org/10.9723/jksiis.2021.26.3.023 ISSN:1229-3741

정보보안 동기, 조직 신뢰가 정보보안 준수에 미치는 영향: 업무향상초점의 조절효과 분석+

(The Influence of Security Motivation and Organization Trust on Information Security Compliance: Focusing on Moderation Effects of Work Promotion Focus)

황 인 호[1], 허 성 호[2]*
(Inho Hwang and Sungho Hu)

요 약 정보보안에 대한 투자가 지속적으로 증가하고 있지만, 조직 내부의 보안 위협은 감소하지 않고 있다. 연구 목적은 조직원의 정보보안 준수의도를 높이기 위한 방향을 제시하는 것이다. 세부적으로, 연구는 정보보안 동기와 조직 신뢰가 정보보안 준수의도에 미치는 긍정적인 영향을 제시하고, 업무 향상초점의 조절효과를 확인한다. 연구 모델 및 가설 검증은 구조방정식 모델링을 통해 실시하며, 정량적 검증을 위하여 정보보안 정책을 도입한 조직의 조직원들에게 설문을 실시하였다. 가설 검증 결과, 정보보안 처벌, 가치 일치가 조직 신뢰를 통해 정보보안 준수의도에 긍정적 영향을 미치며, 업무 향상 초점이 처벌, 가치 일치, 조직 신뢰와 준수의도간의 영향 관계에 조절 효과가 있음을 확인하였다. 연구는 내부자의 정보보안 준수 수준 향상을 위한 조직의 노력 요인을 세부적으로 제시하였다는 측면에서 학술적, 실무적 시사점을 가진다.

핵심주제어: 정보보안 준수의도, 처벌, 가치 일치, 조직 신뢰, 업무 향상 초점

Abstract Investment of organization in information security is increasing, but information security threats within the organization are not decreasing. The purpose of this study is to suggest a direction to increase the information security compliance intention of employees. In detail, the study presents the positive effects of security motivation and organization trust on the information security compliance intention, and presents the moderating effect of work promotion focus. Research model and hypothesis verification are confirmed through structural equation modeling and the study conducted a questionnaire technique to the employees of the organization applying the information security policy for quantitative verification. As a result, information security punishment and value congruence had a positive affect on the compliance intention by mediating organization trust. In addition, work promotion focus had a moderating effect on the positive relationship between the precedent factors on the compliance intention. The research has academic and practical implications from the viewpoint of presenting the factors of the organization's efforts to improve the level of information security compliance by insiders.

Keywords: Information Security Compliance Intention, Punishment, Value Congruence, Organization Trust, Work Promotion Focus

* Corresponding Author: powerrcy@hanmail.net
+ 이 논문은 2018년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2018R1D1A1B07050305)
Manuscript received February 15, 2021 / revised April 14, 2021 / accepted May 24, 2021
1) 국민대학교 교양대학, 제1저자
2) 중앙대학교 심리학과, 제2저자, 교신저자

1. 서 론

정보보안이 조직의 중요한 자원으로 인식되면서, 세계적으로 조직들은 정보를 보호하기 위한 다각적인 노력을 하고 있다. 특히, 조직들은 정보보안 관련 국제 표준 인증을 받거나, 개인 정보 보호 등의 국가 차원의 법적 문제 해결을 위한 내부 정책 및 기술 도입 등을 시도하고 있다. 전 세계의 정보보안 시장은 보안 솔루션 시장을 중심으로 지속적으로 성장해왔는데, 2019년 세계 보안 시장의 규모는 1,565억 달러에 달하며 연평균성장률(CAGR)이 10%에 달할 정도로 규모가 커지고 있다(Grandviewresearch, 2019).

조직들의 정보보안에 대한 투자의 증가에도 불구하고 정보보안 사고는 감소하지 않고 있다. Verizon(2020) 보고서에 따르면, 정보보안 사고는 조직에게 있어 숨기고 싶은 사건이기 때문에 드러나지 않는 경우가 많음에도 불구하고 조직의 정보보안 사고는 증가하고 있는 것으로 나타났다. 또한, 매년 발생한 전 세계 정보보안 사고의 약 60~70%는 해킹과 같이 기술적 침입을 통해 발생하고 있으며, 약 20~30%의 사고는 조직 내부자의 노출로 발생하고 있음을 밝히고 있다. 발생한 보안 사고는 정보 노출 피해를 입은 해당 조직만 금전적, 비금전적 손실을 받는 것이 아닌, 해당 정보와 관계된 이해관계자(고객, 파트너, 정부 등) 모두 추가적인 피해를 받는 측면이 있어, 정보보안에 대한 투자뿐만 아니라, 지속적인 운영·관리가 중요하다(Hwang et al., 2017). 이중 조직 내부의 정보보안 관리 및 통제는 기술 도입보다 더욱 어려운 문제이다. West(2008)는 내부자의 정보보안 사고가 다분히 개인의 심리적인 관점에 의해서 발생하며, 보안 문제 발생 시 조직에게 들키지 않도록 노력하는 경향을 보이는 측면이 강하기 때문이라고 보았다. 즉, 조직 차원에서 구성원의 정보보안 관련 심리적 측면을 개선함으로써, 구성원들의 자발적인 준수 행동을 이끌어야 하기 때문이다(Boss et al., 2015).

조직 내부자 관점에서 접근하고 있는 정보보안 선행연구들은 조직과 개인의 관계에서 개인의 준수 행동을 높이기 위한 다양한 관점의 선행 요인을 제시하는 측면을 강화하고 있다. 대표적으로 보호동기이론(protection motivation theory)과 합리적 선택이론(rational choice theory), 제재이론(deterrence theory) 등과 같은 범죄학, 사회학 등에서 적용되던 이론들을 정보보안 분야에 적용함으로써, 구성원의 정보보안 준수 행동 수준을 높이는 방안을 제시해왔다(D'Arcy et al., 2009; Buglurcu et al., 2010; Guo et al., 2011; Boss et al., 2015; Safa and von Solms, 2016). 이와 같은 선행연구들은 조직이 구축한 정보보안 동기적 요인이 개인의 보안 관련 의지 또는 행동에 직접적인 영향을 미치는 것을 확인하였다는 높은 시사점을 가진다.

조직 환경과 개인 심리 사이의 관계에서 발생 가능한 이슈와 조직 및 개인의 성과와 관련된 연구들을 살펴보면, 개인을 둘러싼 특정 환경 또는 조직 문화적 특성(분위기 등)에 따라서 개인의 행동 동기 수준의 차이가 발생하며(Son, 2011), 특히, 조직에 대한 신뢰 형성이 개인 차원의 만족, 성과 달성에 높은 영향을 주고 있음을 확인하고 있다(Mayer et al., 1995; Agarwal, 2013). 하지만, 정보보안 분야에서 개인의 조직 신뢰 형성을 위한 선행 조건에 대한 결과를 아직까지 제시하지 못하고 있어, 정보보안과 관련된 인식이 어떻게 신뢰 형성에 영향을 주는지 확인할 필요가 있다.

또한, 특히 심리학, 교육학 등에서는 특정 행동에 대한 개인의 행동 결정은 동기적 측면 이외, 개인이 실행하고자 하는 의사결정 방식에 의해서 달라질 수 있다고 보고 있다(Keller, 2006; Neubert et al., 2008). 하지만, 조직 내에서 보상의 관점보다 처벌의 관점에서 적용되고 있는 정보보안 정책이 개인의 행동 결정 방식에 의해 어떻게 반영되는지를 다양한 관점에서 확인하지 못하고 있다.

본 연구는 개인의 정보보안 관련 유형별 동기(외재적 동기, 내재적 동기)가 정보보안 준수의도에 미치는 영향에 있어, 조직 신뢰를 통한 긍정적 영향 관계를 확인하고자 한다. 더불어, 개인이 인지한 정보보안 동기 및 신뢰의 보안 준수에 대한 긍정적 영향에 있어, 개인의 의사결정 방식인 업무 향상 초점이 미치는 긍정적 영향을

확인함으로써, 정보보안 준수를 위한 선행 요인들의 영향 관계 및 의미를 제시하고자 한다.

연구 결과는 정보보안 관련 유형별 동기가 신뢰를 통해 준수의도에 미치는 영향과 개인 의사결정 방식에 따른 영향의 차이를 확인함으로써, 개인의 정보보안 준수 관련 의사결정을 하는 조건을 다각적으로 제시한다는 측면에서 시사점을 가진다.

2. 이론적 배경

2.1 정보보안 동기

동기는 조직의 비전, 행동 목표 등이 구성원의 실제 행동으로 이어지도록 하는 행동 원천을 의미한다(Pinder, 1998). 정보보안 분야에서 구성원들의 보안 동기는 조직이 체계화한 보안 목표와 체계를 따르도록 하는 요인이며, 개인의 부정적 또는 긍정적 행동 결과를 설명할 수 있는 요인이다(Safa and von Solms, 2016).

동기이론(motivation theory)에 따르면 동기 원인과 유형은 다양하게 분류될 수 있으나, 대표적으로 외재적 동기(extrinsic motivation)와 내재적 동기(intrinsic motivation)로 구분된다(Son, 2011).

외재적 동기는 개인의 외부 환경으로부터 특정한 보상을 얻거나 피해를 최소화하기 위하여 받아들이는 동기를 의미한다(Herath and Rao, 2009). 정보보안 관점에서 대표적으로 적용되는 외재적 동기는 처벌(punishment)이 있다. 처벌은 강등, 평판 상실, 견책, 금전적 또는 비금전적 패널티, 개인에게 불리한 언급 등을 포함하는 유형 또는 무형적 제재를 의미한다(Son, 2011). 정보보안 관점에서 처벌은 직접적이고, 단기적인 관점에서 개인의 특정 행동을 억제하는 효과를 가진다. 특히, 처벌의 강도와 개인의 문제적 행동이 반드시 처벌로 이어지도록 조직 차원의 정보를 제공할 때, 정보보안 준수 행동으로 이어지게 된다. 일반적으로, 조직들은 빠르게 내부의 정보보안 수준을 높이기 위하여, 정보보안 정책 내 처벌 관련 항목을 제시하고 조직원에게 정책 또는 규정을 따르도록 강조한다(Herath and Rao, 2009).

내재적 동기는 개인의 도덕적 믿음 또는 타인과 다른 자신에게 형성된 규범 및 규칙을 통해 특정 행동이 구현된다는 개념이다. 즉, 내재적 동기는 보상과 같은 외적 특성 및 압력에 굴하지 않고 관심이나 즐거움 등에서 비롯된 동기를 의미한다(safa and von Solms, 2016). 내재적 동기는 간접적이고, 중기적인 관점의 동기이지만, 한번 형성되면 특정 활동에 대하여 긍정적인 인식을 기반으로 성취하려는 성향을 가지고 있어 중요성이 높다(Bulgurcu et al., 2010) 정보보안 관점에서 대표적으로 적용되는 내재적 동기는 가치 일치(value congruence)가 있다. 가치 일치는 조직과 개인이 보유한 가치가 유사한 수준을 의미한다(Chatman, 1989). 정보보안과 관련하여 조직원은 조직보다 정보보안에 대한 가치를 잘 알지 못하기 때문에, 조직이 추구하고자 하는 정보보안 이슈에 대하여 행동하지 않으려는 경향을 보인다(West, 2008). 따라서, 정보보안 준수를 통해 개인이 확보할 수 있는 가치를 명확하게 인지시켜줄 때, 개인은 자신의 이익 달성을 위하여 보안 행동을 할 가능성이 높아진다(Son, 2011). 본 연구는 정보보안 관련 동기를 외재적 동기(처벌)와 내재적 동기(가치 일치)로 구분하고, 신뢰를 통하여 정보보안 준수의도에 미치는 영향을 확인하고자 한다.

2.2 조직 신뢰

신뢰는 개인 간 또는 집단 내 구성원 간의 상호 친밀성을 가지고 긍정적인 관점의 믿음을 보유한 수준으로서(Nachmias, 1985), 자신이 특정 관점에 대하여 통제 또는 관리하지 않더라도, 대상 스스로 관련 행동을 할 것이라는 기대를 의미한다(Mayer et al. 1995). 즉, 상대방에 대한 신의의 수준이기 때문에, 특정 행동 또는 목표에 대하여 자신과 비슷한 행동 또는 긍정적 행동을 할 것이라고 믿는 심리적 상태이다(Gillespie and Dietz, 2009). 특히, 조직 신뢰는 조직 내 구성원이 조직의 바람직한 목표에 대하여 긍정적 행동을 할 것이라는 믿음으로서, 상대방의 행동이 조직에 도움이 될 것이라는 믿음

을 의미한다(Agarwal, 2013). 한번 형성된 신뢰는 조직 구성원 간에 믿음을 형성시켜 특정 목표에 대하여 최선의 이익을 추구하도록 돕는 요인이지만, 한번 깨어진 신뢰는 구성원 간에 불안한 상태를 유지하고 불확실성을 높이는 요인으로 작용하여 조직 성과까지 부정적인 결과를 도출시킬 수 있다. 따라서, 신뢰 형성과 더불어 신뢰를 유지하기 위한 노력이 함께 이어지는 것이 중요하다(Gillespie and Dietz, 2009).

정보보안과 관련하여 조직 신뢰는 조직이 구축한 보안 규정, 정책 등에 대한 개인의 믿음이 형성될 때 발생한다(Lowry et al., 2015). 또한, 정보 보안과 관련된 조직에 대한 신뢰 형성은 조직에서 구축한 정보보안 체계가 자신과 구성원에게 최선의 이익이라고 믿고, 행동하도록 하는 조건이다(Hwang, 2020). 즉, 정보보안에 대한 신뢰를 형성한 개인은 조직이 도입한 정보보안 정책, 기술 등이 조직 전체뿐 아니라, 당사자의 이익에 도움이 될 것이라 믿기 때문에, 조직의 보안 목표를 따르려는 행동을 보인다. 따라서, 조직은 구성원에게 조직 신뢰 형성을 위하여 노력함으로써, 구성원들이 조직의 보안 활동에 대한 긍정적인 인식을 할 수 있도록 돕는 것이 필요하다.

2.3 업무 향상 초점

조절초점이론(regulatory focus theory)은 개인에게 근본적으로 다른 행동 욕구를 제공하는 동기적 지향 요인(향상 초점과 예방 초점)이 있다고 본다(Higgins, 1997). 즉, 사람은 특정 문제 및 이슈에 대한 처리에 있어 특정한 동기적 관점을 가지고 있어, 행동 방식의 차이를 가진다(Keller, 2006). 향상 초점(promotion focus) 관련 동기적 관점을 가진 사람은 “이상(ideal)” 관점의 목표를 가지고 성취에 대한 필요성을 충족시키기 위한 노력을 보이는 반면, 예방초점(prevention focus) 관련 동기적 관점을 가진 사람은 “의무(ought)” 관점의 목표를 가지고, 보호를 위한 행동을 하는 경향이 있다(Gino and Margolis, 2011).

조직에서 개인별 상이한 조절초점은 특정 문제에 대하여 행동하려는 방식의 차이를 가지기 때문에, 조직 프로세스에 대해 유형별 다른 접근 방식을 취한다. Neubert et al.(2008)은 조직 업무와 관련된 개인의 조절초점을 업무조절초점(work regulatory focus)으로 구분하였으며, 업무 향상 초점과 업무 예방 초점 2가지로 유형화하였다. 업무 향상 초점은 문제가 가지는 긍정적인 측면을 강화하고, 업무 예방 초점은 문제를 키우지 않도록 부정적인 측면을 최소화하는 측면을 강화하는 경향이 있다(Neubert et al., 2008). 즉, 조직에서 개인은 업무 수행에 있어서도 해결 방식에 대한 차이가 존재한다.

정보보안과 관련하여 조절초점은 정보보안 관련 규칙에 대한 행동에 있어 각기 다른 형태 접근 방식을 취하는데, 정보보안을 추가적으로 자신의 업무에 적용하는 상황 발생 시, 향상 초점을 보유한 사람은 보안적 가치를 긍정적으로 바라보고 목표 달성을 이상적으로 하는 경향이 있으며, 예방 초점을 보유한 사람은 보안은 최소한의 행동 가치로 판단하여, 목표 달성을 조직이 요구하는 수준에 한정하는 경향이 있다(Burns, 2021). 하지만, Hwang and Cha(2018)는 조직이 구축한 정보보안 기술에 대한 대응은 향상초점 관점을 가진 개인에게 높게 발생하고, 스트레스를 감소시켜 준수의도에 영향을 주는 것을 확인하였기 때문에, 본 연구에서는 업무 향상 초점을 활용하여 보안 동기, 조직 신뢰가 준수의도 향상에 미치는 영향을 찾는다.

2.4 정보보안 준수의도

내부자에 의한 정보보안 사고는 당사자의 직업과 관련 없이, 조직의 정보시스템에 접근이 가능하면 발생 가능하다. 실제 정보 노출 사고를 일으킨 당사자의 직업은 사무직, 엔지니어, 영업직 등 다양한 것으로 나타나고 있다(Verizon, 2020). 즉, 내부자에 의한 정보보안 준수는 심리적 관점에서 접근하여, 긍정적 행동을 높이기 위한 노력을 통해 해결할 수 있다(Hwang et al., 2017).

내부자의 정보보안 준수 행동의 방향은 최종적으로 형성된 개인의 정보보안 준수의도를 통

해서 결정된다(Kim et al., 2018; Park, 2019). 정보보안 준수의도는 연구자별 조금씩 차이가 있으나, 조직이 보호하고자 하는 정보에 대하여, 발생 가능한 위협을 파악하고, 개인 스스로가 해당 정보를 보호하고 관리하고자 하는 의지로 정의된다(Bulgurcu et al., 2010; Vance et al., 2012). 즉, 준수의도는 자발적이고 능동적인 관점에서 조직의 보안 준수를 위한 행동을 하려는 인식 수준이기 때문에, 행동에 직접적인 영향을 주는 요인이다. 따라서, 조직은 내부자의 정보보안 준수 수준을 높이기 위하여, 정보보안 준수의도 향상을 위한 노력을 해야 한다.

이에, 본 연구는 정보보안 동기(처벌, 가치 일치), 조직 신뢰, 그리고, 행동에 대한 동기인 향상 초점이 준수의도에 미치는 영향 관계를 확인하고자 한다.

3. 연구 모델 및 가설 설정

3.1 연구 모델

본 연구는 정보보안 동기 유형(외재적 동기, 내재적 동기)이 보안 정책에 대한 신뢰 형성을 통해 조직원의 정보보안 준수의도에 어떻게 영향을 주고, 개인의 의사결정 유형에 따라 차이가 있는지를 알아보고자 한다. 이에 다음의 연구 모델을 제시한다(Fig. 1).

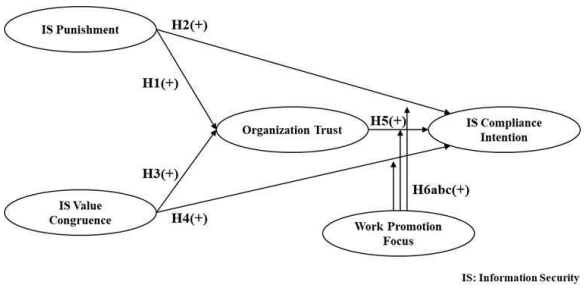

Fig. 1 Research Model and Proposed Hypotheses

3.2 연구 가설

3.2.1 처벌과 신뢰와의 관계

조직 신뢰는 개인이 조직에 대한 긍정적 관점의 믿음을 보유한 상태를 의미한다. 조직은 특정한 상황에 직면한 구성원이 긍정적 행동을 하도록 하기 위해서는 조직의 행동에 대한 긍정적 믿음을 가질 수 있는 자극을 주는 것이 필요하다(Gillespie and Dietz, 2009). 즉, 개인이 조직에 대한 신뢰 형성을 위해서는 신뢰 동기 형성을 위한 동인을 제공하여야 한다. van der Werff et al.(2019)은 신뢰 의사결정을 위한 프레임워크를 제시하였는데, 개인의 신뢰 관련 동기 형성은 동기 동인이 필요하며, 외재적 동기, 내재적 동기, 그리고 통제된 외재적 동기를 함께 확보해야 신뢰를 형성할 수 있다고 하였다. Mulder et al.(2009)은 제재가 도덕적 판단에 긍정적인 영향을 미치는데, 제재의 심각성 수준과 도덕적 판단간에 신뢰가 강화효과를 가지는 것을 확인하였다. 즉, 처벌은 신뢰와 긍정적인 관계를 가지고 있으며, 신뢰 형성을 위해서는 외재적 동기가 선행되어야 한다. 따라서, 외재적 동기인 처벌이 조직 신뢰에 긍정적인 영향을 미칠 것으로 판단하고, 다음의 연구 가설을 제시한다.

H1: 정보보안 처벌은 조직 신뢰에 긍정적 영향을 준다.

3.2.2 처벌과 준수의도와의 관계

대표적인 외재적 동기 요인인 정보보안 처벌은 조직원의 정보보안 관련 경각심을 높여 준수의도에 긍정적인 영향을 준다. 특히, 정보보안 관련 처벌이 조직 구성원의 직위와 상황에 관계없이 명확하게 처리되고, 처벌의 수위가 높아질 경우, 구성원들은 제재에 의해 본인이 감당해야 할 책임 및 비용이 증가하여 조직이 요구하는 보안 행동을 하려고 한다(D'Arcy et al., 2009). Buglurcu et al.(2010)은 개인의 정보보안 관련 의사결정은 혜택과 비용 관점의 합리적 선택에 의해 결정되는데, 처벌은 미준수 행동에 대한 개인의 비용 관점이기 때문에, 미준수 행동에 의한 비용과 준수 행동에 대한 혜택을 비교해서 준수의도로 이어진다고 보았다. 또한, 조직원이 소속되어 있는 조직 단위, 부서 단위, 그리고 개인 단위의 처벌 유형별, 개인의 정보보안 준수의도에 영향을 준다(Guo and Yuan, 2012). 즉,

선행연구를 기반으로 본 연구는 다음과 같은 연구 가설을 제시한다.

H2: 정보보안 처벌은 정보보안 준수의도에 긍정적 영향을 준다.

3.2.3 가치 일치와 신뢰와의 관계

조직 또는 개인에 대한 신뢰가 형성되기 위해서는 이해당사자간의 동일한 목표 또는 가치를 형성시키는 것이 필요하다(Cazier et al., 2007). 조직과 개인간의 신뢰는 상호간에 대한 긍정적인 방향성을 가진 믿음이기 때문에(Agarwal, 2013), 조직이 추구하는 비전과 목표가 본인과 일치하지 않을 경우, 조직에 대한 믿음을 형성하기 어렵다. Cazier et al.(2007)은 e-비즈니스에서 기업의 정보 공개에 대한 소비자의 믿음 형성은 해당 기업의 가치와 자신과 일치할 때 발생한다고 보았으며, 가치 일치가 신뢰를 높이는 것을 확인하였다. 또한, 개인과 조직 리더와의 신뢰의 형성은 리더가 보유한 가치의 방향을 인식하고 본인과 일치한다고 판단될 때 발생하고 높아진다(Lau et al., 2007). 따라서, 내재적 동기인 가치 일치는 조직 신뢰에 긍정적 영향을 미칠 것으로 판단하고, 다음의 연구 가설을 제시한다.

H3: 정보보안 가치 일치는 조직 신뢰에 긍정적 영향을 준다.

3.2.4 가치 일치와 준수의도와의 관계

가치 일치는 조직을 포함한 이해당사자의 비전, 목표를 이해하고, 추구하는 방향이 동일하다고 판단하는 수준이기 때문에, 가치 일치가 높은 사람은 조직이 요구하는 행동 수준이 본인의 목표와 동일하다고 판단하여 긍정적인 행동하려는 경향을 보인다(Kristof-Brown et al., 2005). 정보보안 정책이 비록 개인의 직접적인 업무 목표는 아니지만, 가치 일치가 높은 사람은 조직의 정보 가치를 이해하고 보호하기 위한 노력을 하고자 한다(Safa and von Solms, 2016). 즉, 정보보안과 관련하여 조직이 추구하는 정보보호 가치를 이해하고, 본인의 업무와 연관성을 발견한 개인은 정보보안을 준수할 가능성이 높다(Son, 2011). 따라서, 조직과 정보보안 관련 가치가 조직과 일치한 사람은 정보보안 요구 수준을 따를 것으로 판단하며, 다음의 연구 가설을 제시한다.

H4: 정보보안 가치 일치는 정보보안 준수의도에 긍정적 영향을 준다.

3.2.5 조직 신뢰와 준수의도와의 관계

조직에 대한 구성원들의 신뢰는 보완적인 관점으로서, 개인은 조직의 특정 활동 체계의 적정성을 판단하고 개인에게 이익이 되는지를 확인함으로써 신뢰를 형성하게 된다(Mayer et al., 1995). 즉, 조직은 개인의 신뢰를 확보하기 위한 노력을 통해, 구성원들의 믿음을 가지게 되며, 개인은 신뢰를 기반으로 조직의 요구 수준을 달성하고자 한다(Gillespie and Dietz, 2009).

정보보안 정책에 대한 조직 신뢰는 조직의 정보보안 정책의 수준이 조직 전체의 이익이 될 뿐만 아니라, 관련 행동 시 개인에게 피해가 없음을 인지될 때 확보되며, 조직에 대한 신뢰 형성은 개인의 정보보안 관련 행동으로 이어진다(Lowry et al., 2015). Hwang(2020)은 조직이 추구하는 정보보안 활동에 대한 신뢰가 형성될 때, 정보보안 회피 행동을 감소시키는 것을 확인하였다. 즉, 정보보안 정책에 대한 신뢰 형성은 정보보안 준수의도를 높이는 선행 조건이다. 이에 연구는 선행연구를 기반으로 다음의 연구 가설을 제시한다.

H4: 조직 신뢰는 정보보안 준수의도에 긍정적 영향을 준다.

3.2.6 업무 향상 초점의 조절효과

업무 향상 초점은 개인의 스트레스 상황, 즉 개인을 둘러싼 환경이 요구하는 특정 이슈에 대해 대처하는 개인의 성향 중 이상적이고 긍정적인 부분을 높게 평가하여 해결하고자 하는 성향을 의미한다(Gino and Margolis, 2011). 정보보안 관련하여 업무 향상 초점을 보유한 사람은 엄격한 정보보안 정책에 의해 발생 가능한 부정적 영향에 저항하고, 정보보안 정책 및 기술이 가지는 긍정적인 측면을 중점적으로 고려하는 성향을 가진다(Hwang and Cha, 2018). 또한, Liang et al.(2013)은 조직의 정보시스템 활용에 대한 개인들의 동기 요인인 보상 기대는 준수의도를 높이며, 향상 초점이 높은 사람이 낮은 사

람보다 보상 기대의 준수의도에 미치는 영향이 더욱 높은 것을 확인하였다. 즉, 업무에 대한 향상 초점이 높은 개인은 정보보호를 위해 구축한 정책에 대한 처벌(외재적 동기), 기대가치(내재적 동기)에 대한 긍정적인 측면을 중점적으로 고려하고, 보안 준수의도를 높게 가질 것으로 판단하며, 다음의 연구 가설을 제시한다.

H5a: 업무 향상초점은 정보보안 처벌과 준수의도간의 긍정적인 영향 관계를 조절한다.

H5b: 업무 향상초점은 정보보안 가치 일치와 준수의도간의 긍정적인 영향 관계를 조절한다.

더불어, Chang et al.(2019)은 소비자들의 전자상거래 구매의도에 있어, 커뮤니티와 소비자의 조절초점의 유사성을 검토하였는데, 조절초점 적합성 수준 높아질수록 구매의도에 긍정적인 영향을 주는 것을 확인하였다. 특히, SNS에 대한 신뢰가 조절초점과 구매의도간의 긍정적 관계를 조절하는 것을 확인하였다. 즉, 긍정적인 믿음의 형태인 신뢰와 이상적인 관점의 목표를 지향하는 향상 초점간에는 높은 상관관계를 가지고 있는 것으로 판단하며, 정보보안 분야에도 적용될 것으로 판단한다. 즉, 신뢰와 준수의도간의 긍정적인 영향 관계를 향상 초점이 조절할 것으로 판단하고 다음의 연구 가설을 제시한다.

H5c: 업무 향상 초점은 조직 신뢰와 준수의도간의 긍정적인 영향 관계를 조절한다.

3.3 데이터 측정 방법 및 수집

가설검증은 구조방정식모델링 분석을 통해 확인하고자 하며, SPSS 21.0과 AMOS 22.0을 분석에 적용한다. 이에 연구는 설문지 확보를 통한 정량 데이터를 확보하였다. 연구모델에 적용된 요인은 총 5개(정보보안 처벌, 정보보안 가치 일치, 조직 신뢰, 정보보안 준수의도, 그리고 업무 향상 초점)이며, 각 요인의 설문 항목들은 선행연구를 통해 도출하였으며, 정보보안 특성에 맞추어 질문을 재구성하였으며, 7점 리커트 척도를 적용하였다.

정보보안 처벌은 “정보보안 정책 위반에 대한 엄격하고 명시적인 처벌 수준”으로 정의하며(Guo et al., 2011), 선행연구를 통해 “조직은 직원의 보안 위반행위에 대해 엄격하게 처벌함”, “정보보안 정책 위반 시 처벌받을 가능성 있음”, “조직은 정보보안 정책 위반에 대한 처벌을 명시적으로 제시함”과 같이 3개 항목을 설문에 적용하였다.

정보보안 가치 일치는 “조직의 정보보안 가치가 나와 일치하는 수준”으로 정의되며(Son, 2011), 선행연구를 통해 “나의 가치와 조직의 정보보안 가치가 매우 비슷함”, “조직의 정보보안 의미는 나에게 중요함”, “조직의 정보보안 목표 가치를 이해하는 것에 동의함”과 같이 3개 항목을 설문에 적용하였다.

조직 신뢰는 “조직의 행동 및 지원에 대한 믿음 수준”으로 정의하며, Agarwal(2013) 연구를 기반으로 “조직은 약속을 지키기 위한 노력을 함”, “조직은 의사결정 시 구성원들의 의견을 고려함”, “나는 조직의 결정에 기꺼이 따를 것”과 같이 3개 항목을 설문에 적용하였다.

정보보안 준수의도는 “조직 정보 위협을 방지하기 위해, 정보보안을 준수하고자 하는 의지 수준”으로 정의하며, Chen et al.(2012)의 연구를 통해, “나는 조직의 보안 정책을 지속으로 따를 것”, “조직의 정보 보호를 위해 보안 정책을 준수할 것”, “업무 수행할 때마다 정보보안 절차를 준수할 것”과 같이 3개의 항목을 설문에 적용하였다.

업무 향상 초점은 “업무 대한 긍정적이고 열정적으로 참여하고자 하는 경향 수준”으로 정의하며, Neubert et al.(2008)의 연구를 통해 “나는 열망을 성취하는 방법을 찾기 위하여 많은 시간을 할애”, “ 업무에 대한 우선순위는 내가 열망하는 바를 보여줌”, “조직에서 내가 가진 희망가 열망을 통해 동기를 부여받고 있음”, “성장에 대한 목표를 극대화하기 위한 기회 포착을 노력을 하고 있음”, “직장에서 성공하기 위하여 위험을 무릅쓰는 경향이 있음”과 같이 5개의 항목을 설문에 적용하였다.

설문 대상은 IT 보안 기준을 적용하고, 조직 차원에서 정보보안 정책을 적용하고 있는 조직에 근무하는 근로자들을 대상으로 하였다. 특히, 현재 직책에서 일상적으로 정보보안 기술 및 정

책을 업무에 적용해야 하는 부서의 근로자를 대상으로 하였다. 설문 조사는 대학에서 주말에 경영학을 배우고 있는 직장인에게 오프라인 설문으로 실시하였다. 직장인들 중 설문 대상에 부합한 사람들만 응답하도록 하되, 설문의 목적과 통계 활용에 대한 방향을 사전에 전달하고 설문에 동의한 사람들만 응답하도록 하였다. 설문 결과 총 314개의 유효 표본을 확보하였으며, 해당 표본을 분석에 활용하였다. 표본의 인구통계학적 특성은 Table 1과 같다.

Table 1 Demographic Characteristics

Demographic Categories		Frequency	%
Total		314	100.0
Industry	Manufacture	61	19.4
	Service	253	80.6
Gender	Male	174	55.4
	Female	140	44.6
Age	under 30	86	27.4
	31~40	127	40.4
	41~50	91	29.0
	over 50	10	3.2
Job Position	Staff	133	42.4
	Assistant Manager	81	25.8
	Manager	49	15.6
	General Manager	51	16.2

4. 연구 결과

4.1 신뢰성 및 타당성 분석

연구는 다 항목 기반의 설문지 기법을 통해 정량 데이터를 확보하고, 구조방정식 모델링을 통해 가설 검증을 하므로, 요인의 구성 적절성에 대한 신뢰성과 타당성 분석을 한다.

우선 다 항목에 대한 요인의 일관성을 확인하기 위하여 신뢰성 분석을 하였다. 신뢰성 분석은 SPSS 21.0을 활용하여 탐색적 요인분석과 cornbach's α를 확인함으로써 요인이 일관성을 가지는지를 확인한다. 분석에 활용한 5개 요인은 총 17개 항목으로 구성되는데, 탐색적 요인분석 결과 1개 항목(PF2)을 제거하고 16개의 항목을 활용하였으며, 모든 요인의 cornbach's α가 신뢰성 요구 수준인 0.7을 넘어서(Nunnally, 1978), 신뢰성 문제는 없는 것으로 나타났다(Table 2).

더불어, 구조모델에 적용할 요인의 타당성 분석을 하였다. 타당성 분석은 집중 타당성, 판별 타당성 분석을 실시한다. 집중 타당성은 다 항목 요인이 일정하게 구성되어 있는지를 확인하는 기법이며, CR(contstruct reliability)과 AVE (average variance extracted)를 통해 적정성을 확인한다. 판별 타당성은 복수 요인간의 차이가 분명하게 존재하는지를 확인하는 기법으로 상관계수와 AVE값을 비교하여 확인한다.

타당성 분석을 위하여, AMOS 22.0을 활용하여 확인적 요인분석을 실시하였다. 확인적 요인분석에 적용한 모델의 적합성을 확인한 결과 모든 값이 구조방정식 적합성 요구사항에 적합한 것으로 나타났다(χ^2/df = 1.341, GFI = 0.957, AGFI = 0.936, CFI = 0.995, NFI = 0.981, RMSEA = 0.033). 집중 타당성에서 CR의 기준은 0.7 이상의 값을 요구하며, AVE의 기준은 0.5 이상의 값을 요구한다(Wixom and Watson, 2001). 분석 결과 CR과 AVE 모두 요구 기준을 확보한 것으로 나타났다(Table 2).

Table 2 Result for Construct Validity and Reliability

Construct	Item	Factor Loading	Cronbach's α	CR	AVE
IS Punishment	IP1	0.896	0.971	0.936	0.831
	IP2	0.903			
	IP3	0.893			
IS Value Congruence	IVC1	0.833	0.930	0.892	0.734
	IVC2	0.849			
	IVC3	0.811			
Organization Trust	OT1	0.800	0.951	0.904	0.759
	OT2	0.803			
	OT3	0.817			
Compliance Intention	CI1	0.827	0.940	0.962	0.894
	CI2	0.827			
	CI3	0.818			
Promotion Focus	PF1	0.802	0.895	0.868	0.687
	PF3	0.848			
	PF4	0.862			
	PF5	0.876			

CR(construct reliability)
AVE(average variance extracted)

판별 타당성 분석은 요인들의 상관계수와 AVE값의 제곱근을 비교하여 확인하며, AVE 값의 제곱근이 상관계수보다 높을 때, 판별 타당성을 확보하였다고 본다(Fornell and Lacker, 1981). 분석 결과는 모든 요인의 상관계수보다 AVE 제곱근 값이 높은 것으로 나타나 판별 타당성을 확보하였다(Table 3)

Table 3 Result for Discriminant Validity

Construct	1	2	3	4	5
IS Punishment	***0.912***				
IS Value Congruence	.453**	***0.857***			
Organization Trust	.579**	.635**	***0.871***		
Compliance Intention	.502**	.644**	.676**	***0.946***	
Promotion Focus	.475**	.502**	.520**	.577**	***0.829***

Note: Values in bold type along the diagonal indicate the square root of the AVE
**: p < 0.01

마지막으로, 연구는 설문지 기법을 통해 데이터를 확인하였기 때문에 독립 변수와 종속 변수 간의 동일한 상황적 문제가 발생할 수 있다. 이에 공통방법편의(common method bias) 분석을 추가로 실시하였다. Podsakoff et al.(2003)은 공통방법편의 문제를 제시하면서, 다각적 관점의 해결 방법을 제시하였다. 본 연구는 대표적으로 적용하고 있는 싱글 공통방법편의 분석 기법을 적용한다. 본 방법은 기존 구조모델과 단일요인을 추가적으로 반영한 구조모델의 설문 항목들의 변화량을 비교하여 분석하는 기법이다. 우선 기존 구조모델의 적합성(χ^2/df = 1.341, GFI = 0.957, AGFI = 0.936, CFI = 0.995, NFI = 0.981, RMSEA = 0.033)과, 단일 요인을 추가한 구조모델의 적합성(χ^2/df = 1.217, GFI = 0.968, AGFI = 0.940, CFI = 0.997, NFI = 0.986, RMSEA = 0.026)은 모두 요구사항을 충족한 것으로 나타났으며, 두 개의 구조모델의 항목들의 차이 값을 비교한 결과 0.2 이하로 나타나, 공통방법편의 문제는 낮은 것으로 나타났다.

4.2 주 효과 분석

주 효과 분석은 조절 효과를 제외한 요인들간의 영향 관계를 확인하는 단계로서, 구조모델의 적합성, 경로 분석(β), 그리고 결정계수 분석(R^2)을 실시하여 분석 결과를 확인한다.

첫째, 구조모델의 적합성 검증을 실시한다. 적합성 분석 결과는 χ^2/df = 1.268, GFI = 0.968, AGFI = 0.948, CFI = 0.997, NFI = 0.988, RMSEA = 0.029로 나타나, 구조방정식 요구 적합성을 충족하였다.

둘째, 경로 분석을 실시하였으며, 결과는 Fig. 2, Table 4와 같다.

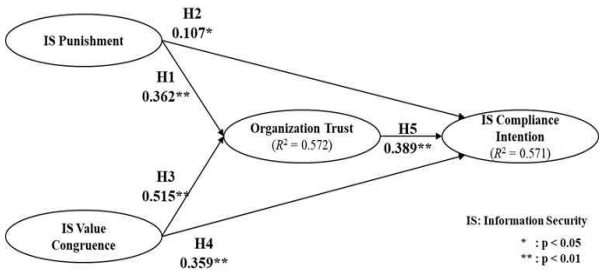

Fig. 2 Results of the Structural Model

Table 4 Summary of Hypothesis Tests

	Path	Coefficient	t-value	Results
H1	IP → OT	0.362	7.595**	Support
H2	IP → CI	0.107	2.125*	Support
H3	IVC → OT	0.515	10.305**	Support
H4	IVC → CI	0.359	6.148**	Support
H5	OT → CI	0.389	6.000**	Support

IP(IS punishment), IVC(IS value congruence), OT(organization trust), CI(compliance intention)
**: p < 0.01, *: p < 0.05

가설 1은 정보보안 처벌이 조직 신뢰에 긍정적 영향을 준다는 것으로, 경로계수(β) 확인 결과 통계적으로 유의한 것으로 나타났다(H1: β

= 0.362, p<0.01). 이러한 결과는 개인을 둘러싼 환경 중 외재적 동기 요인이 조직 신뢰에 긍정적인 영향을 주어 행동으로 이어진다는 선행연구(van der Werff et al., 2019)와 유사하며, 관련 요인 간의 관계가 정보보안 분야에서도 적용됨을 의미한다. 즉, 정보보안의 정책 실행에 있어 중요한 단기적 동기 요인인 처벌이 명확하고 반드시 적용된다는 관점을 명확하게 인지하고 있을 때, 개인은 정보보안 분야에서도 조직 신뢰를 형성할 수 있음을 의미한다. 따라서, 조직은 정보보안 정책의 적용 정보를 조직원에게 분명하게 인식시켜주기 위한 노력을 하는 것이 필요하다.

가설 2는 정보보안 처벌이 정보보안 준수의도에 긍정적 영향을 준다는 것으로, 경로계수(β) 확인 결과 통계적으로 유의한 것으로 나타났다(H2: β = 0.107, p<0.05). 이러한 결과는 제재의 심각성과 명확성이 구성원의 보안 준수의지를 향상 시키고, 부정적 행동을 감소시킨다는 정보보안 분야의 선행연구(Guo et al., 2011)와 동일한 결과이다. 즉, 내부의 정보보안 요구 수준을 달성시키기 위해서는 구성원의 자발적인 준수의도 형성이 중요하며, 정보보안에 대한 처벌 수준이 엄격할수록 구성원은 본인의 피해를 최소화하기 위한 노력을 한다. 따라서, 조직은 내부 보안 피해 최소화를 위해 보안 규정의 실행력을 확인시켜주는 것이 필요하다.

가설 3은 정보보안 가치 일치가 조직 신뢰에 긍정적 영향을 준다는 것으로, 경로계수(β) 확인 결과 통계적으로 유의한 것으로 나타났다(H3: β = 0.515, p<0.01). 이러한 결과는 개인에게 형성된 내재적 동기가 조직 신뢰를 형성시켜 긍정적인 행동을 유발한다는 선행연구(van der Werff et al., 2019)와 유사하며, 요인 간의 관계가 정보보안 분야에서도 적용됨을 의미한다. 즉, 조직이 추구하는 정보보호를 위한 가치가 본인의 행동 가치와 일치된다고 판단할 경우, 조직에 대한 신뢰가 형성됨을 의미한다. 따라서, 조직은 신뢰를 형성시키기 위해, 정보보안의 필요성을 조직과 구성원 모두에게 필요한 상황임을 인지시키는 활동을 하는 것이 필요하다.

가설 4는 정보보안 가치 일치가 정보보안 준수의도에 긍정적 영향을 준다는 것으로, 경로계수(β) 확인 결과 통계적으로 유의한 것으로 나타났다(H4: β = 0.359, p<0.01). 이러한 결과는 정보보안 필요성의 의미를 형성할 때, 긍정적인 보안 행동으로 이어진다는 정보보안 분야의 선행연구(Son, 2011)와 동일한 결과이다. 즉, 정보보안 활동의 가치가 조직에서 본인의 역할 및 목표임을 인식할 때, 자발적인 정보보안 준수 행동으로 이어지는 것을 의미한다. 따라서, 개인 정보보안 준수 수준을 향상시키기 위해서는 조직 차원에서 정보보안 준수의 필요성과 추구 목표, 그리고 업무 내 정보보안 절차 등을 명확하게 구성원에게 인식시켜주는 노력이 필요하다.

가설 5는 조직 신뢰가 정보보안 준수의도에 긍정적 영향을 준다는 것으로, 경로계수(β) 확인 결과 통계적으로 유의한 것으로 나타났다(H5: β = 0.389, p<0.01). 이러한 결과는 조직에 대한 신뢰가 정보보안 이슈에 대한 회피 행동을 감소시킨다는 선행연구(Hwang, 2020)와 유사한 결과이다. 즉, 조직 신뢰는 조직 행동의 적절성과 명확성에 의해서 형성된 개인의 믿음 수준이기 때문에, 조직에 대한 믿음이 견고할수록 정보보안이 조직과 본인에게 필요한 부분임을 인지하는 것을 의미한다. 따라서, 조직은 정보보안 준수의도 향상을 위해서 구성원들이 조직에 대한 믿음을 견고히 할 수 있도록 하고, 특히 정보보안 정책의 수행과 관리가 명확하고, 보안 준수의 가치가 모든 구성원에게 필요한 요인임을 제시하는 것이 필요하다.

마지막으로, 선행 변수가 결과 변수에 미치는 영향력을 확인하기 위하여 결정계수(R^2)를 확인하였다. 정보보안 처벌과 정보보안 가치 일치가 조직 신뢰에 미치는 영향력은 57.2%로 나타났으며, 정보보안 처벌과 정보보안 가치 일치, 그리고 조직 신뢰가 준수의도에 미치는 영향력은 57.1%로 나타났다.

4.3 조절 효과 분석

연구 가설 H6a, H6b, H6c는 업무향상초점이 정보보안 처벌, 정보보안 가치 일치, 그리고 조직 신뢰의 정보보안 준수의도에 미치는 긍정적

인 영향 관계를 조절한다는 것으로서, 본 연구는 조절변수 요인을 7점 리커트 척도로 확인하였다. 연속형 변수간의 구조방정식모델링을 통한 조절 효과 검증은 상호작용효과를 확인한다.

Table 5 Summary of Moderating Effect Tests

	Path	Coefficient	t-value	Results
H6a	IP→CI	0.266	5.151**	Support
	PF→CI	0.477	8.71**	
	IPxPF→CI	-0.199	-4.381**	
H6b	IVC→CI	0.494	9.841**	Support
	PF→CI	0.339	6.75**	
	IVCxPF→CI	-0.22	-5.387**	
H6c	OT→CI	0.528	10.432**	Support
	PF→CI	0.315	6.285**	
	OTxPF→CI	-0.17	-4.227**	

IP(IS punishment), IVC(IS value congruence),
OT(organization trust), CI(compliance intention)
PF(promotion focus)
**: $p < 0.01$

구조방정식모델링을 통한 상호작용효과 분석은 Little et al.(2006)이 제시한 엄격한 검증방법인 직교화접근법(orthogonalizing approach)을 적용하였다. 본 접근법은 상호작용항 도출에 있어, 비교 항목 전체를 곱한 항을 만들고, 비표준화 잔차를 추가 항목으로 도출하여 적용하는 기법이다. 분석 결과는 Table 5와 같다.

연구 가설 H6a는 정보보안 처벌과 정보보안 준수의도간의 영향 관계를 업무 향상 초점이 조절한다는 것으로, 분석 결과 상호작용 효과가 있는 것으로 나타났다. 이에, 각 요인 간의 영향 수준을 확인하기 위하여 그래프로 확인하였으며, Fig. 3과 같다. 분석 결과, 정보보안 제재가 높을 경우에는 업무 향상 초점 집단(고, 저)의 영향 차이가 높지 않으나, 정보보안 제재의 영향이 낮은 집단에서는 업무 향상 초점이 높은 집단이 낮은 집단보다 정보보안 준수의도에 높은 영향을 미치는 것을 확인할 수 있었다.

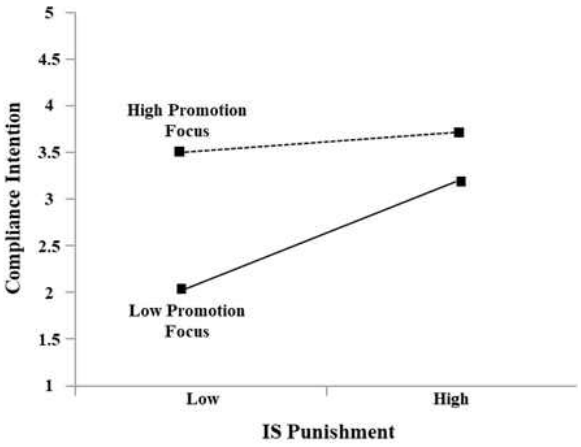

Fig. 3 Moderation Effect: Punishment x Promotion Focus

연구 가설 H6b는 정보보안 가치 일치와 정보보안 준수의도간의 영향 관계를 업무 향상 초점이 조절한다는 것으로, 분석 결과 상호작용 효과가 있는 것으로 나타났다. 이에, 각 요인 간의 영향 수준을 확인하기 위하여 그래프로 확인하였으며, Fig. 4와 같다. 분석 결과, 정보보안 가치 일치가 높을 경우에는 업무 향상 초점 집단(고, 저)의 영향 차이가 높지 않으나, 정보보안 가치 일치의 영향이 낮은 집단에서는 업무 향상 초점이 높은 집단이 낮은 집단보다 정보보안 준수의도에 높은 영향을 미치는 것을 확인할 수 있었다.

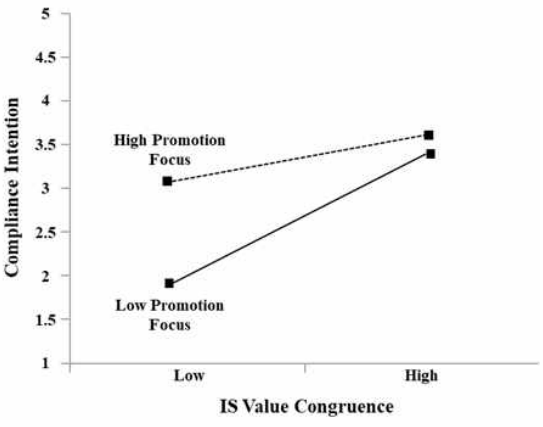

Fig. 4 Moderation Effect: Value Congruence x Promotion Focus

연구 가설 H6c는 조직 신뢰와 정보보안 준수의도간의 영향 관계를 업무 향상초점이 조절한다는 것으로, 분석 결과 상호작용 효과가 있는 것으로 나타났다. 이에, 각 요인 간의 영향 수준을 확인하기 위하여 그래프로 확인하였으며, Fig. 5와 같다. 분석 결과, 조직 신뢰가 높을 경우에는 업무 향상 초점 집단(고, 저)의 영향 차이가 높지 않으나, 조직 신뢰의 영향이 낮은 집단에서는 업무 향상 초점이 높은 집단이 낮은 집단보다 정보보안 준수의도에 높은 영향을 미치는 것을 확인할 수 있었다.

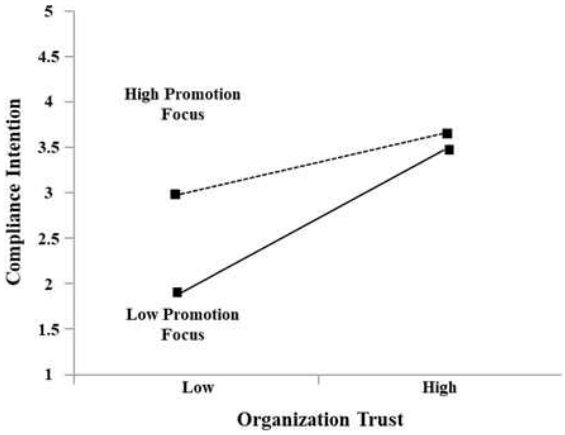

Fig. 5 Moderation Effect: Trust x Promotion Focus

4.4 매개 효과 분석

추가적으로, 본 연구는 조직 신뢰의 매개 효과를 확인하고자 한다. 구조방정식을 통한 매개효과 검증을 위해 Hoyle and Kenny(1999)의 매개 효과 분석 방법을 적용하였다. 본 방법은 독립변수와 종속변수간 분석이 문제 없을 때, 매개변수를 적용하고, 부트스트래핑 기법을 적용하여, 간접효과를 확인하는 기법이다. 연구는 부트스트래핑 1,000과 신뢰도 95%를 적용하였다.

Table 6 Summary of Mediating Effect Tests

	Path		Coefficient	t-value	Results
ISP → CI	step 1	ISP→CI	0.512	9.89**	Support
	step 2	ISP→CI	0.139	2.57**	
		ISP→OT	0.604	11.75**	
		OT→CI	0.617	10.75**	
	Step 2. Indirect Effects of ISP = 0.308**				
IVC → CI	step 1	IVC→CI	0.676	14.08**	Support
	step 2	IVC→CI	0.370	6.29**	
		IVC→OT	0.685	13.56**	
		OT→CI	0.447	7.56**	
	Step 2. Indirect Effects of IVC = 0.290**				

IP(IS punishment), IVC(IS value congruence), OT(organization trust), CI(compliance intention)
**: $p < 0.01$

분석 결과, 정보보안 처벌과 조직 신뢰, 그리고 준수의도간의 관계는 간접효과가 존재하고, 모든 요인이 유의한 것으로 나타나, 부분 매개 효과를 가지는 것으로 파악되었다. 정보보안 가치 일치와 조직 신뢰, 그리고 준수의도간의 관계 또한 부분 매개 효과를 가지는 것으로 나타났다.

5. 결 론

5.1 연구의 요약

최근 정보보안에 대한 관심이 증가하면서, 조직들은 정보에 대한 투자 및 정보 자원 관리를 위한 노력을 요구받고 있다. 이에 조직들은 엄격한 보안 정책과 기술 등을 도입함으로써, 정보 노출 위협을 감소시키고 있다. 하지만, 아직까지 내부자의 정보보안 준수에 대한 이슈가 해결되고 있지 않고 있다. 이에, 연구는 조직원의 정보보안 준수의도에 긍정적인 영향을 미치는 요인을 외재적 동기(처벌)와 내재적 동기(가치

일치), 그리고 조직 신뢰를 제시하고, 조직 신뢰의 영향 관계를 확인하고자 하였다. 더불어, 개인의 업무 향상 초점이 각 선행 요인의 준수의도에 미치는 영향을 어떻게 조절하는지를 확인하고자 하였다.

가설 검증은 구조방정식모델링을 적용하였으며, 정보보안 정책과 기술을 도입한 조직의 근로자들에게 설문을 진행하고 표본을 확보하였다. 분석 결과, 정보보안 처벌과 가치 일치가 조직 신뢰를 높이고, 조직 신뢰가 준수의도에 긍정적 영향을 미치는 것을 확인하였으며, 업무 향상 초점 요인이 처벌, 가치 일치, 그리고 조직 신뢰의 준수의도에 미치는 긍정적 영향을 조절하는 것을 확인하였다.

5.2 연구의 시사점

연구는 다음과 같은 관점에서 학술적 시사점을 가진다. 첫째, 조직과 개인의 관계에서 개인의 만족도 또는 조직의 성과와 같이 종속 변인에 중요한 영향을 주는 조직 신뢰가 정보보안 분야에 적용되어 준수의도를 높이는 요인임을 확인하였다. 즉, 조직이 추구하는 특정 활동에 대한 과정, 결과에 대한 복합적 믿음 요인인 조직 신뢰가 형성된 사람은 조직이 요구하는 보안 준수적 행동을 하려는 경향을 보임을 확인하였다. 즉, 조직 신뢰가 정보보안 분야에 적용되어, 행동에 영향을 주는 선행 요임을 증명하였다. 둘째, 조직 신뢰 향상에 있어, 개인에게 형성된 정보보안 유형별 동기가 영향을 주는 선행 조건임을 확인하였다. 즉, 연구는 정보보안 관련 외재적 동기(처벌)와 내재적 동기(가치 일치)가 조직에 대한 개인의 신뢰 형성에 영향을 주는지를 검증하였으며, 영향 관계에 있음을 확인하였다. 셋째, 조직 내 개인의 의사결정 유형인 업무 향상 초점이 준수의도에 긍정적 영향을 미치는 선행 요인들에게 조절 효과가 있음을 확인하였다. 특히, 처벌, 가치 일치, 조직 신뢰가 높은 집단이 향상 초점에 의한 준수의도에 미치는 영향이 낮은 집단과 큰 차별성은 없었으나, 처벌, 가치 일치, 그리고 조직 신뢰가 낮은 집단에서 업무 향상 초점이 준수의도에 높게 영향을 주는 것을 확인하였다.

즉, 본 연구는 학술적 관점에서 조직 신뢰가 정보보안 분야에 적용되어 준수에 영향을 주는 요인이며, 정보보안 동기 요인들이 조직 신뢰를 높이는 선행 조건이며, 그리고 업무 향상 초점을 통해 조절하여 적용됨을 확인하였다는 측면에서 높은 시사점을 가진다.

연구는 다음과 같은 관점에서 실무적 시사점을 가진다. 첫째, 정보보안 분야에 조직 신뢰가 가지는 긍정적 영향과 조직 신뢰를 높이기 위한 선행 조건을 확인하였다는 측면에서 실무적 시사점을 가진다. 즉, 개인의 보안 준수 행동은 심리적 관점에서 적용되는데, 조직의 행동 전반에 대한 믿음 수준인 신뢰가 형성될 경우, 구성원들의 행동은 조직이 요구하는 수준을 달성하려는 경향이 있다. 연구는 보안 분야에 적용하여, 내부자의 보안 행동에도 신뢰가 중요한 선행 조건임을 확인하였다. 더욱이, 조직 신뢰향상을 위해서는 개인에게 형성된 인지적 동기가 중요한데, 외재적 동기인 처벌과 내재적 동기인 기대 일치 모두 조직 신뢰를 높이는 요인임을 확인하였다. 따라서, 조직이 내부자의 정보보안 수준 향상을 위해서는 구성원들의 조직에 대한 믿음을 향상시키는 것이 중요하다. 즉, 연구는 조직이 정보보안 정책 적용의 일관성과 명확성을 통해 형성된 개인의 처벌 인지 측면과 정보보안 준수의 가치가 본인의 역할과 동일하다는 것을 인지시켜주는 측면을 지속적으로 강화할 필요를 제시한다.

둘째, 조직에서 개인 업무 이슈 해결에 있어 접근 유형인 업무 향상 초점이 준수의도에 미치는 선행 요인의 긍정적 효과를 조절하는 것을 확인한 측면에서 실무적 시사점을 가진다. 연구 결과, 업무 향상 초점은 준수의도에 긍정적 영향을 미치는 선행 요인(처벌, 가치 일치, 신뢰)의 영향이 낮은 집단에서 크게 영향을 주는 것을 확인하였다. 즉, 처벌 인식이 낮은 집단, 가치 일치 인식이 낮은 집단, 그리고 조직 신뢰가 낮은 집단에서, 이상적이고 목표지향적 관점에서 행동을 하려는 유형의 사람들은 높은 준수의도를 가지는 것을 확인하였다. 따라서, 연구는 개인의 의사결정 방식이 보다 목표지향적이고, 능동적으로 행동할 수 있도록 혁신성, 위험감수

성을 확보하기 위한 캠페인, 교육 등의 프로그램 등을 운영함으로써, 내부자들의 보안 수준을 향상시키는 것이 필요함을 실무적으로 제시하였다는 측면에서 높은 시사점을 가진다.

5.3 연구의 한계점

연구는 조직 구성원의 정보보안 수준 향상을 위한 선행 조건을 다각적인 관점에서 제시한 부분의 시사점을 가지나, 다음과 같은 연구의 한계점이 존재하며, 향후 연구에서는 추가로 검토할 필요가 있다. 첫째, 연구는 가설 검증을 위하여 설문 대상자에 대한 설문지 기법을 통해 응답 당시의 생각을 기반으로 인지 수준을 확인하였다. 하지만, 정보보안 처벌은 인지적 요인으로 확인할 수도 있지만, 정책 구축 수준과 같은 실제 적용 현황요인으로 확인하는 것이 더욱 정확할 수 있다. 또한, 가치 일치는 조직과 개인의 차이를 명확하게 확인하기 위하여, 설문을 다르게 구성하여 접근할 수 있다. 즉, 응답자의 구성을 다각화하거나, 실제 조직 데이터를 활용하여 분석한다면, 높은 시사점을 가질 수 있을 것으로 판단한다. 둘째, 연구는 조직에 대한 인식 요인을 확인하여 연구 가설을 검증하였다. 하지만, 조직문화에 대한 차이(예: 개인주의 조직, 집단주의 조직), 업종에 대한 차이(예: 서비스, 제조업 또는 IT 및 영업 중심 업종)는 정보보안에 대한 구성원의 인식 차이를 보여줄 것으로 판단한다. 따라서, 향후 연구에서는 조직의 다양한 특성에 따라 심도 있는 준수의도에 대한 영향요인을 제시한다면, 높은 시사점을 제공할 것으로 판단한다. 마지막으로, 본 연구는 개인의 의사결정 성향인 조절초점이론 중 향상 초점을 적용하여, 향상초점이 준수의도에 미치는 선행연구의 영향력을 조절하는 것을 확인하였다. 조절초점이론에 따르면, 예방 초점은 문제 해결관점에서 접근되기 때문에, 오히려 정보보안 관련 해결관점에 적절할 수 있다. 따라서, 조절초점이론의 세부 요인들을 복합적으로 적용하여, 개인 차원인을 제시한다면 보다 높은 시사점을 제시할 수 있을 것으로 판단한다.

References

Agarwal, V. (2013). Investigating the Convergent Validity of Organizational Trust. *Journal of Communication Management*, 17(1), 24-39. DOI : 10.1108/13632541311300133.

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D. and Polak, P. (2015). What Do Systems Users have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors, *MIS Quarterly*, 39(4), 837-864.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness, *MIS Quarterly*, 34(3), 523-548.

Burns, A. J. (2021). Protecting Organizational Information Assets: Exploring the Influence of Regulatory Focus on Rational Choices, In *Proceedings of the 54th Hawaii International Conference on System Sciences* (p. 5228).

Cazier, J. A., Shao, B. B. and Louis, R. D. S. (2007). Sharing Information and Building Trust through Value Congruence, *Information Systems Frontiers*, 9(5), 515-529. DOI : 10.1007/s10796-007-9051-6.

Chang, K. C., Hsu, Y. T., Hsu, C. L. and Sung, Y. K. (2019). Effect of Tangibilization Cues on Consumer Purchase Intention in the Social Media Context: Regulatory Focus Perspective and the Moderating Role of Perceived Trust, *Telematics and Informatics*, 44, Advance online publication.
DOI : 10.1016/j.tele.2019.101265

Chatman, J. A. (1989). Improving Interactional Organizational Research: A Model of Person-Organization Fit, *Academy of management Review*, 14(3), 333-349.
DOI : 10.5465/amr.1989.4279063.

Chen, Y., Ramamurthy, K. and Wen, K. W. (2012). Organizations' Information Security

Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems*, 29(3), 157-188. DOI : 10.2753/MIS0742-1222290305.

D'Arcy, J., Hovav, A. and Galletta, D. (2009). User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach, *Information Systems Research*, 20(1), 79-98. DOI : 10.1287/isre.1070.0160.

Fornell, C. and Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error, *Journal of Marketing Research*, 18(1), 39-50. DOI: 10.2307/3151312.

Gillespie, N. and Dietz, G. (2009). Trust Repair After an Organization-Level Failure, *Academy of Management Review*, 34(1), 127-145. DOI : 10.5465/amr.2009.35713319.

Gino, F. and Margolis, J. D. (2011). Bringing Ethics into Focus: How Regulatory Focus and Risk Preferences Influence (un) Ethical Behavior, *Organizational Behavior and Human Decision Processes*, 115(2), 145-156. DOI : 10.1016/j.obhdp.2011.01.006.

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.

Guo, K. H. and Yuan, Y. (2012). The Effects of Multilevel Sanctions on Information Security Violations: A Mediating Model, *Information & Management*, 49(6), 320-326. DOI : 10.1016/j.im.2012.08.001.

Guo, K. H., Yuan, Y., Archer, N. P. and Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model, *Journal of Management Information Systems*, 28(2), 203-236. DOI : 10.2753/MIS0742-1222280208.

Herath, T. and Rao, H. R. (2009). Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness, *Decision Support Systems*, 47(2), 154-165. DOI : 10.1016/j.dss.2009.02.005.

Higgins, E. T. (1997). Beyond Pleasure and Pain, *American Psychologist*, 52(12), 1280 - 1300. DOI : 10.1037/0003-066X.52.12.1280.

Hoyle, R. H. and Kenny, D. A., (1999). Sample Size, Reliability, and Tests of Statistical Mediation, *Statistical Strategies for Small Sample Research*, 1, 195-222.

Hwang, I. (2020). A Study on the Mitigation of Information Security Avoid Behavior: From Goal Setting, Justice, Trust perspective, *Journal of Digital Convergence*, 18(12), 217-229. DOI : 10.14400/JDC.2020.18.12.217.

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

Hwang, I., Kim, D., Kim, T. and Kim, S. (2017). Why Not Comply with Information Security? An Empirical Approach for the Causes of Non-compliance, *Online Information Review*, 41(1), 2-18. DOI : 10.1108/OIR-11-2015-0358.

Keller, P. A. (2006). Regulatory Focus and Efficacy of Health Messages, *Journal of Consumer Research*, 33(1), 109-114. DOI : 10.1086/504141.

Kim, J., Kim, K. and Park, H. (2018). The Impact of Family-Friendly Corporate Culture on Employees' Behavior, *Journal of the Korea Industrial Information Systems Research*. 23(2), 75-92. DOI : 10.9723/jksiis.2018.23.2.075.

Kristof-Brown, A. L., Zimmerman, R. D. and Johnson, E. C. (2005). Consequences of Individuals' Fit at Work: A Meta-Analysis of Person - Job, Person - Organization, Person - Group, and Person - Superior Fit, *Personnel psychology*, 58(2), 281-342. DOI : 10.1111/j.1744-6570.2005.00672.x.

Lau, D. C., Liu, J. and Fu, P. P. (2007). Feeling Trusted by Business Leaders in China: Antecedents and the Mediating Role of Value Congruence, *Asia Pacific Journal of Management*, 24(3), 321-340. DOI 10.1007/s10490-006-9026-z.

Liang, H., Xue, Y. and Wu, L. (2013). Ensuring Employees' it Compliance: Carrot or Stick?, *Information Systems Research*, 24(2), 279-294. DOI : 10.1287/isre.1120.0427.

Little, T. D., Bovaird, J. A. and Widaman, K. F. (2006). On the Merits of Orthogonalizing Powered and Product Terms: Implications for Modeling Interactions among Latent Variables, *Structural Equation Modeling*, 13(4), 497-519. DOI: 10.1207/s15328007sem1304_1.

Lowry, P. B., Posey, C., Bennett, R. B. J. and Roberts, T. L. (2015). Leveraging Fairness and Reactance Theories to Deter Reactive Computer Abuse Following Enhanced Organisational Information Security Policies: An Empirical Study of the Influence of Counterfactual Reasoning and Organisational Trust, *Information Systems Journal*, 25(3), 193-273. DOI : 10.1111/isj.12063.

Mayer, R. C., Davis, J. H. and Schoorman, F. D. (1995). An Integrative Model of Organizational Trust, *Academy of Management Review*, 20(3), 709-734. DOI : 10.5465/amr.1995.9508080335

Mulder, L. B., Verboon, P. and De Cremer, D. (2009). Sanctions and Moral Judgments: The Moderating Effect of Sanction Severity and Trust in Authorities, *European Journal of Social Psychology*, 39(2), 255-269. DOI : 10.1002/ejsp.506.

Nachmias, D. (1985). *Determinants of Trust within the Federal Bureaucracy.* In Rosenbloom, D. H. (Eds), Public Personnel Policy: The Politics of Civil Service, New York: Associated Faculty Press, Port Washington, 133-143.

Neubert, M. J., Kacmar, K. M., Carlson, D. S., Chonko, L. B. and Roberts, J. A. (2008). Regulatory Focus as a Mediator of the Influence of Initiating Structure and Servant Leadership on Employee Behavior, *Journal of Applied Psychology*, 93(6), 1220 - 1233. DOI : 10.1037/a0012695.

Nunnally, J. C. (1978). *Psychometric Theory* (2nd ed.), New York: McGraw-Hill.

Park, K. (2019). A Study on the Influence of the Perception of Personal Information Security of Youth on Security Attitude and Security Behavior, *Journal of the Korea Industrial Information Systems Research*, 24(4), 79-98. DOI : 10.9723/jksiis.2019.24.4.079.

Pinder, C. C. (1998), *Work Motivation in Organizational Behavior,* Upper Saddle River, NJ: Prentice Hall.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y. and Podsakoff, N. P. (2003). Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies, *Journal of Applied Psychology*, 88(5), 879-903. DOI : 10.1037/0021-9010.88.5.879.

Safa, N. S. and von Solms, R. (2016). An Information Security Knowledge Sharing Model in Organizations, *Computers in Human Behavior*, 57, 442-451. DOI : 10.1016/j.chb.2015.12.037.

Son, J. Y. (2011). Out of Fear or Desire? Toward a better Understanding of Employees' Motivation to Follow IS Security Policies, *Information & Management*, 48(7), 296-302.

DOI : 10.1016/j.im.2011.07.002.
van der Werff, L., Legood, A., Buckley, F., Weibel, A. and de Cremer, D. (2019). Trust Motivation: The Self-Regulatory Processes Underlying Trust Decisions, *Organizational Psychology Review*, 9(2-3), 99-123. DOI : 10.1177/2041386619873616.
Vance, A., Siponen, M. and Pahnila, S. (2012). Motivating IS Security compliance: Insights from Habit and Protection Motivation Theory, *Information & Management*, 49(3-4), 190-198. DOI : 10.1016/j.im.2012.04.002.
Verizon. (2020). Data Breach Investigations Report. https://enterprise.verizon.com/resources/reports/dbir.
West, R. (2008). The Psychology of Security, *Communications of the ACM*, 51(4), 34-40. DOI : 10.1145/1330311.1330320.
Wixom, B. H. and Watson, H. J. (2001). An Empirical Investigation of the Factors Affecting Data Warehousing Success, *MIS Quarterly*, 25(1), 17-41. DOI : 10.2307/3250957.

황 인 호 (Inho Hwang)
• 정회원
• 건국대학교 경영학과 경영학사
• 중앙대학교 경영학과 경영학석사
• 중앙대학교 경영학과 경영학박사
• 국민대학교 교양대학 조교수
• 관심분야: IT 핵심성공요인, 디지털 콘텐츠, 정보보안 및 프라이버시 분야 등

허 성 호(Sungho Hu)
• 정회원
• 중앙대학교 심리학과 문학석사
• 중앙대학교 심리학과 문학박사
• 중앙대학교 심리학과 강사
• 관심분야: 정보문화, 융합연구, 고령화, 빅데이터, 채용경향, 공동체 분야 등