Journal of Digital Convergence
Vol. 18. No. 12, pp. 217-229, 2020

ISSN 2713-6434 / eISSN 2713-6442
https://doi.org/10.14400/JDC.2020.18.12.217

정보보안 회피행동 완화에 대한 연구: 정보보안 관련 목표설정, 공정성, 신뢰의 관점을 중심으로

황인호
국민대학교 교양대학 조교수

A Study on the Mitigation of Information Security Avoid Behavior: From Goal Setting, Justice, Trust perspective

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

요 약 세계적으로, 정보보호는 조직의 필수적인 관리 조건이 되고 있으며, 조직들은 정보보안을 위하여 높은 수준의 자원을 지속적으로 투자하고 있다. 조직 내부자들의 보안 위협은 감소하지 않고 있어, 정보보안 행동 준수를 위한 관심이 필요한 상황이다. 본 연구의 목적은 조직원들의 보안 회피 행동의 원인인 역할갈등을 완화시키기 위한 선행 요인을 제시하는 것이다.

연구는 정보보안 정책을 보유한 조직에서 근무하는 조직원을 대상으로 설문을 실시하였으며, 383개의 표본을 활용하여 구조방정식모델링을 통한 가설 검증을 하였다. 가설 검증 결과, 역할갈등이 회피행동을 증가시키는 것으로 나타났으며, 목표 난이도와 세밀성, 공정성, 신뢰가 역할갈등을 완화하는 것으로 나타났다. 특히, 공정성은 신뢰를 통해 역할갈등과 회피 행동 감소에 영향을 주는 것으로 나타났다. 연구 결과는 조직원의 정보보안 회피행동 원인과 완화 요인을 제시함으로써, 정보보안 수준 향상을 위한 정보보안 전략 수립에 영향을 줄 것으로 판단한다.

주제어 : 정보보안 회피행동, 목표설정, 조직공정성, 신뢰, 역할갈등

Abstract Globally, information protection of organization has become an essential management factor, and organizations continue to invest high-level resources for information security. Security threats from insiders are not decreasing. The purpose of this study is to present the antecedence factors to mitigate the role conflict that is the cause of the security avoid behavior.

For the study, a survey was conducted for employees of organizations with information security policies, and structural equation modeling was conducted using a total of 383 samples for hypothesis verification. As a result of the analysis, role conflict increased avoid behavior, and goal difficulty, goal specificity, justice, and trust mitigated role conflict. In particular, justice influenced the reduction of role conflict and avoid behavior through trust. The implications were to present the causes and mitigation factors for avoid behavior of employee, and it is judged that it will help the organization to establish a security strategy.

Key Words : Information security avoid behavior, Goal setting, Organizational justice, Trust, Role conflict

*This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea(NRF-2018S1A5A8027420)
*Corresponding Author : Inho Hwang(hwanginho@kookmin.ac.kr)
Received September 18, 2020 Revised October 13, 2020
Accepted December 20, 2020 Published December 28, 2020

1. 서론

전 세계적으로, 정보보안은 조직에게 매우 중요한 요인으로 인식되고 있다. 이에 따라, 국내 정보보안 관련 시장은 매년 4~5% 이상 지속적으로 성장해왔으며, 2020년 현재 물리 보안 시장과 사이버 보안 시장을 통합한 전체 보안 시장 규모는 약 6조 원에 이르고 있다[1]. 해외의 경우, 연평균 10% 성장하고 있어, 성장성이 국내보다 높은 것으로 나타나고 있는데, 이와 같은 시장 변화는 증가하는 사이버범죄 등 각종 보안 위협에 대응하기 위한 신기술 활용이 필요해졌기 때문이다[2]. 즉, 정보보안 기술은 빠르게 변화하고 있으며, 조직은 IT 및 각종 보안 기술에 대한 투자를 통해 조직 내외의 보안 위협에 대응하고자 하고 있다[3].

정보보안 사고 유형을 살펴보면, 조직 내부-외부, 인간-비인간 관점의 차원으로 분석이 가능하다[4]. 조직 외부-인간, 조직 내부-비인간의 경우, 해킹에 의한 접근 등으로서 최근의 보안 기술로 해결하기 위한 수단이 존재한다. 조직 외부-비인간은 자연재해로 물리적 보안 센터의 파괴 등의 문제이며 불가항력에 가까운 부분이다. 반면, 조직 내부-인간의 보안 사고는 조직 시스템에 접근 가능한 내부자(직원, 협력업체 파트너 등)로부터 발생할 수 있는 보안 위협으로, 이러한 유형의 정보보안 사고는 감소하지 않고 있다. 실제로, 전 세계 보안 사고의 20~30%가 매년 내부자에 의해 지속적으로 발생하고 있는 실정이다[5].

여러 선행연구들은 조직구성원 또는 파트너와 같이 조직 정보시스템에 접근 가능한 내부자들의 정보보안 사고 원인을 개인의 심리적 관점에서 발생한다고 보고 있다. 조직구성원에게 있어 정보보안 준수 행동은 우선적으로 지켜야할 성과 목표가 아니고 개인이 실행한 정보보안 행동 결과에 대한 정보를 언제든 숨길 수 있기 때문에, 정보보안을 지키지 않을 가능성이 언제든 존재하며, 이에 대한 해결은 심리적 관점에서 개인의 보안 준수문제에 접근해야 한다는 것이다[6]. 즉, 조직에서 도입한 기술 및 정책, 규정 등을 실제로 실행에 옮겨야하는 조직원들은 엄격한 보안 규칙을 지키지 않더라도 들키지만 않는다면 문제가 없다는 생각을 할 수 있기때문에, 자발적인 준수 행동을 위한 동기를 형성시켜주는 것이 필요하다[7]. 선행연구들이 제시하는 조직원들의 정보보안 준수 행동 방향은 개인에게 형성된 보안 동기 등 심리적 측면을 긍정적으로 변화시키는데 있다고 본다. 특히, 선행연구들은 계획된 행동이론(theory of planned behavior)[8], 합리적선택이론(Rational choice theory)[9], 동기이론(motivation theory)[10], 억제이론(deterrence theory)[11] 등과 같은 범죄학, 사회학, 심리학 등의 이론 등을 보안 분야에 도입 또는 결합을 통해 개인의 긍정적 보안 행동 동기 향상을 위한 요인들을 제시하고 있다.

최근 몇몇의 연구는 정보보안 관련 긍정적 행동의 선행 요인이 아닌, 엄격한 정보보안 기술 및 정책은 반대로 개인의 부정적 행동을 유발할 수 있다는 관점을 제기하고 있다[12, 13]. 정보보안에 대한 조직의 대처가 엄격한 수준의 정책 및 기술 도입일 경우, 실행자인 조직원들은 보안 관련 엄격한 활동 요구로 인한 업무 상 스트레스를 받게 되며, 회피 등의 부정적인 행동으로 이어진다는 것이다. 현재까지 정보보안으로 인한 기술적 업무적 스트레스에 대한 대처 관련 연구는 스트레스 발생 유형을 제시하는 등 탐색적 연구관점에서 접근하고 있어, 스트레스 발생을 완화하기 위한 대안 수립을 위한 선행 조건에 대한 연구는 매우 부족한 상황이다.

따라서, 본 연구의 목적은 정보보안 관련 업무 스트레스와 정보보안 회피행동과의 영향 관계를 찾고, 업무 스트레스를 완화하기 위한 조직 차원의 대응 요인을 제시하는 것이다. 세부적으로, 정보보안으로 인하여 발생한 역할갈등이 정보보안 회피 행동에 미치는 영향을 파악하고, 역할갈등을 완화하기 위한 요인으로서 목표설정이론을 적용하여 보안관련 목표의 구체성, 난이도를 제시하고, 조직공정성과 신뢰와의 관계를 통해, 역할갈등 완화 방향을 제시하고자 한다.

이를 통해, 연구는 선행연구에서 제시하지 못했던 정보보안 부정적 행동 원인인 조직원의 정보보안 회피행동에 영향을 주는 선행 조건을 제시함으로서, 조직 차원에서 개인들의 보안 회피행동 최소화를 위한 조직 정보보안 목표 설정 방향, 신뢰 향상 등의 접근 전략을 수립하는데 도움을 줄 것으로 판단한다.

2. 이론적 배경

2.1 정보보안 회피 행동

조직 내부자에 의한 정보보안 사고는 지속적으로 발생하고 있다[5]. 정보시스템을 통한 업무 효율성 향상 및 성과 확보를 위한 조직 차원의 노력이 강조될수록 정보보안 사고 발생가능성은 높아진다[14]. 즉, 조직 내외부에서 정보시스템에 접근 권한이 부여된 이해관계자가 많아질수록 정보 노출 가능성은 높아진다. 실제로, 정보보안

사고 중 내부자에 의해 정보 오용(misuse)으로 발생한 사건은 전체 정보보안 사고의 14%를 차지하고 있는 것으로 나타났다[5]. 조직구성원의 정보 접근에 있어 오용은 자신에게 부여된 권한을 적절하게 사용하지 않거나, 업무의 신속한 처리 등을 위하여 정보보안 데이터 보호 절차를 무시 또는 축약하는 경우, 그리고, 자신에게 허가되지 않은 보안 등급의 정보를 무의식적 또는 의식적으로 활용하는 등의 문제이다. 이러한 문제는 단순히 조직의 정보 노출 사고에 의하여 기업에게 피해를 주는 것뿐 아니라, 노출 정보와 관련된 사람, 기업 등에게 2차 피해를 입힐 수 있는 여지가 있어 데이터 오용 사고 감소를 위한 노력이 필요한 상황이다.

이처럼, 악의적이지 않으나, 정보보안 준수 정책, 규정을 지키지 않고 회피하고자 하는 행동을 회피행동(avoidance behavior)이라 한다[15]. Chen and Zahedi[2016]은 정보보안 회피행동을 “자신에게 부여된 기술, 정책 등에 의해 구축된 부정적이고 민감한 환경 또는 상황을 회피하는 행동”으로 정의하였으며[16], Liang and Xue[2010]은 “조직에서 요구하는 규정 또는 정책을 여러 가지 이유로 회피하는 행동”으로 정의하였다[17]. 즉, 회피행동은 현재의 정보보안 관련 어려운 상황이 발생했을 때나 향후 발생될 문제를 모른척하기 위한 행동이기 때문에, 정보보안 관련 회피행동의 개인적 원인을 파악하고, 이를 완화하기 위한 조직 차원의 방향을 제시하는 것이 필요하다.

2.2 정보보안 관련 역할갈등

특정 상황에 대한 조직 환경은 조직원에게 업무 효율성 증대, 성과 목표 달성 등 긍정적인 영향을 미칠뿐 아니라, 불만족 및 이직의도와 같은 부정적인 영향을 미칠 수도 있다[18]. 조직환경과 개인간의 관계를 보다 체계적으로 설명하는 개념이 조직-개인 적합성(person-environment fit)이다[19]. 조직-개인 적합성은 조직의 환경과 개인 사이에는 특정 상황에 대한 평형성이 유지된다는 개념이다. 평형성이 유지되면 개인은 조직에 만족하게 되고 보다 이타적인 행동을 하는 반면, 조직과 개인간의 평형성이 깨지게 될 경우 개인에게 스트레스, 긴장 등을 유발시킨다[20]. 즉, 개인의 스트레스는 조직의 환경적 특성이 자신이 생각하는 관점과 어긋나기 시작할 때부터 발생되며 지속될 경우 육체적, 정신적 문제를 발생시켜 조직에 불이익을 가져올 수 있는 요인이 된다. 업무 스트레스는 개인의 업무과제 및 목표 달성 과정에 있어, 둘러싼 특정한 상황의 변화 또는 갈등을 발생시키는 환경이 지속될 때 발생한다[18]. 업무 스트레스는 업무 환경에 대한 개인의 심리적, 생리적 관점에서의 인지 또는 느낌으로서[21], 업무의 양 및 강도 등에 의해 개인이 보유한 역량의 한계가 발생 시, 업무적 스트레스가 발생된다.

역할갈등은 대표적인 업무 스트레스 요인으로서, 조직으로부터 받은 업무의 수준 및 목표, 진행 절차 등에서 개인이 생각하는 수준과 차이가 발생하는 상황을 지칭한다[22]. 즉, 특정한 상황에서 조직의 업무적 요구사항이 과도하여 요구사항 실행에 대한 개념적 차이가 발생할 때 업무과정에서 개인이 수행해야 할 역할의 차이가 발생하며, 개인은 스트레스를 받게 된다[12].

정보보안 분야는 역할갈등이 자주 발생할 수 있는 영역이다. 정보보안은 첫째, 개인의 관점이 아닌 조직 전체의 관점에서 기술 및 정책을 고려하는 분야이고, 둘째, 외부 위협 대응을 위하여 보안 정책 및 기술이 자주 변경됨에 따라, 개인에게 요구하는 정보보안 규정이 추가적으로 발생될 가능성이 높은 분야이기 때문이다[23]. 예를 들어, 특정 상황에서 파트너와 정보 공동 생성 및 공유, 그리고 변경 등의 문서화 작업이 필요할 때, 업무의 효율성 달성을 위해서는 정보보안 규칙을 지키는 것보다 빠르게 정보를 제공하고 변경하는 것이 좋은 상황이 발생할 수 있다. 하지만, 엄격한 정보보안을 위하여 문서 관리자의 사전 검토, 승인 등의 절차가 필요해지며, 이러한 절차들은 개인 성과 달성에 어려움을 겪게 하는 부정적인 상황이 될 수 있다.

정보보안 관련 역할갈등은 개인의 보안 준수 행동에 부정적인 영향을 주는 요인이다. Hwang and Cha[2018]는 기술스트레스와 행동간의 관계가 정보보안 분야에도 적용될 것으로 판단하고, 정보보안 관련 기술스트레스-업무스트레스, 그리고 준수의도간의 부정적 관계가 있음을 확인하였다[12]. 특히, 보안 관련 업무스트레스의 부분 매개효과가 있음을 확인하였다[12]. D’Arcy et al.[2014]은 시나리오 기법을 통해 정보보안 관련 스트레스가 미준수의도를 높이는 것을 확인하였다[23]. 즉, 정보보안 관련 업무스트레스는 미준수 행동을 높이는 선행 조건이다[24]. 이에 따라, 업무 스트레스인 역할갈등은 조직원의 정보보안 관련 회피행동을 높이는데 영향을 줄 것으로 판단하고 다음의 연구가설을 제시한다.

H1: 정보보안 관련 역할갈등은 정보보안 회피행동을 높일 것이다.

2.3 정보보안 신뢰

신뢰는 이해당사자들간에 있어 상호간에 대한 긍정적이고 친밀성 있는 믿음 수준으로서[25], 본인이 이해관계에 있는 상대방을 관리 또는 통제하지 않더라도, 상대방이 스스로 관련된 중요 행동을 할 것이라는 기대이며[26], 상대방이 자신에게 보여지는 신의의 수준[27]으로 정의하고 있다. 즉, 신뢰는 이해관계에 있는 사람들간에 긍정적 행동을 할 것이라는 믿음을 가지고 있는 심리적 상태로 정의할 수 있다.

조직신뢰는 구성원의 조직에 대한 믿음으로서, 제도적으로 조직구성원간에 형성된 긍정적 관계에 의해, 상대방의 행동을 믿으려고 하는 수준으로 정의할 수 있다[28]. 조직으로 부터 신뢰를 받는다고 생각하는 개인은 조직에 대한 특정의 신념을 구성하게 되며, 조직은 최선의 이익을 위해 행동할 것이라 믿음을 가지게 되어 조직 관점에 이익이 되는 행동을 취한다[28]. 반대로, 신뢰는 형성하기도 어렵지만, 상호간의 신뢰가 훼손되면 상대방을 믿지 못하는 상황이 지속적으로 유지되어 부정적 행동으로 이어지게 된다. 특히 조직과 개인간의 관계에서 신뢰가 깨질 경우 신뢰 복구는 더욱 어렵다[27]. 조직 내 제도 및 관행에 따른 업무 절차 등에서 갈등의 요인이 발생하여 구성원들의 신뢰를 상실한다면, 경영진의 더 많은 노력에도 신뢰 개선은 어려워진다[29]. 따라서, 조직 차원의 지속적인 신뢰 확보를 위한 노력이 필요하다.

조직 신뢰는 구성원들의 협력, 이타적 행동 등을 증진시켜 조직 성과에 직, 간접적인 영향을 주는 선행 요인이다. 즉, 조직을 신뢰하는 조직원은 조직이 자신을 돌보고 있다고 믿기 때문에, 조직에 대해 유익하게 행동할 가능성이 높다. Mayer et al.[1995]는 신뢰를 능력, 호의성, 그리고 무결성으로 세분화하였으며, 개인에게 형성된 신뢰는 상호간의 관계의 위험을 감소시켜 긍정적 결과를 발생시킨다고 하였으며[26], Top et al.[2015]는 병원 조직에 대한 구성원들의 몰입을 높이기 위해서는 리더십과 조직 신뢰가 선행되어야 가능하다고 보았다[30]. 나아가, 신뢰는 개인의 조직에 대한 믿음의 형성이기 때문에, 이타적 행동을 하고자 하는 조직시민행동에 긍정적인 영향을 주어 조직의 성장에 영향을 준다[31].

정보보안 관점에서, 정보보안 정책에 대한 신뢰는 조직의 보안 활동이 조직 및 개인에게 최선의 이익을 위한 추구하는 행동 요구수준이라고 판단하도록 돕는다[32]. Lowry et al.[2015]는 정보보안 정책, 정보보안 교육, 훈련 시스템, 그리고 조직 커뮤니케이션에 의한 변화 인지가 컴퓨터 남용에 미치는 영향을 파악하였으며, 보안 관련 조직 신뢰가 매개효과를 가지는 것을 확인하였다[32]. 즉, 보안 관련 조직 신뢰의 형성은 조직의 보안 환경 구축 및 조직의 지속적인 보안 정보 제공 활동을 통해 형성되고, 형성된 신뢰는 컴퓨터 남용을 완화한다는 것이다. 즉, 정보보안 관련 신뢰는 구성원의 부정적 행동을 완화시키는 것으로 판단하고 다음의 연구가설을 제시한다.

H2: 정보보안 관련 신뢰는 정보보안 회피행동을 완화할 것이다.

조직에 대한 긍정적 신뢰는 조직의 행동이 현재 상황에서 옳은 선택이라는 관점을 가지도록 돕기 때문에, 스트레스를 감소시키는 효과를 가진다. Guinot et al.[2014]은 조직 업무에서 대인간의 신뢰와 업무스트레스, 그리고 직업 만족도간의 관계성을 연구하였다[33]. 그들은 조직 내 구성원들간에 형성된 높은 신뢰성은 조직 및 구성원에 대한 믿음을 높여, 업무스트레스를 감소시키고, 직업 만족도를 높이는 것을 확인하였다[33]. Top and Tekingunduz[2018]은 병원 조직의 업무 스트레스 완화에 대한 연구에서, 조직 공정성과 조직신뢰를 선행 완화요인으로 제시하였다[34]. 특히, 그들은 신뢰를 인지기반 신뢰와 영향기반 신뢰로 구분하였으며, 각 구분된 신뢰가 업무 스트레스를 완화하는 것을 확인하였다. 즉, 선행연구를 기반으로 정보보안 신뢰가 보안 관련 역할갈등을 완화할 것으로 판단하고, 다음의 연구가설을 제시한다.

H3: 정보보안 관련 신뢰는 정보보안 역할갈등을 완화할 것이다.

2.4 정보보안 관련 목표설정

목표설정이론(goal setting theory)은 개인들이 합리적으로 행동한다는 가정하에, 정해진 목표를 달성하기 위하여 노력한다는 동기이론이다[35]. 목표는 조직 내 개인의 업무 관련 행동을 변화시키고, 나아가 조직 성과를 높이는 동기이다. Wright[2004]는 조직에서 조직원들의 업무 동기 형성은 업무 단위의 목표 난이도와 목표 구체성이 형성될 때 업무 동기를 형성시킨다고 하였으며[36], Prichard et al.[1988]은 업무 목표 설정은 개인의 행동을 결정짓지만, 개인 단위가 아니라 조직 차원의 특정한 목표가 설정되면 조직 전체의 성과가 높아진다고 하였다[37].

목표설정이론의 세부 요인을 살펴보면, 목표의 구체성

(specificity)과 목표의 난이도(difficulty)가 있다[35]. 목표의 구체성은 행동의 목표 또는 목적을 명확하게 이해하고 행동할 수 있도록 목표가 구체적인 상태를 의미하며[38], 목표 난이도는 목표 이행 대상자가 현실적으로는 목표 달성은 가능하지만, 행동하기 어려운 수준을 의미한다[39]. 즉, 목표설정이론은 개인 또는 조직 차원의 목표가 보다 구체적이고 보다 도전적인 수준을 가지고 있을 때, 높은 성과를 달성할 수 있는 동기를 부여한다는 관점이다. 즉, 목표 설정 시, 현재 할 수 있는 수준보다 어렵지만, 달성을 위한 보다 세밀한 단계별 목표 수준을 가질수록 목표를 설정한 대상의 직무 수준 및 성과는 더욱 높아질 수 있다[40].

정보보안 관점에서도 조직차원의 명확한 정보보안 목표 설정은 조직구성원들의 보안 행동에 긍정적인 영향을 미친다. 내부자의 정보보안 준수는 구성원들의 보안 준수 문화 및 분위기가 형성되어야 하는데, 정보보안 목표가 설정되고, 구체적인 목표 실행 방향 등이 지속적으로 제시된다면 개개인의 준수 행동에 긍정적인 영향을 미친다는 것이다[41]. Koskosas[2008]는 정보보안 운영 및 관리 체계 향상을 위해서 물리적 정보보안 목표 설정과 보안 시스템 관점의 목표 설정을 구분하여 접근하는 것이 필요하다고 보았다[42]. 정보보안과 관련된 물리적 기기에 대한 운영 목표 설정은 개인의 접근 권한 등을 명확하게 하고 관리 체계를 제시하며 시스템에 대한 목표 설정은 정보시스템 접근 권한 및 책임을 명확하게 제시하기 때문에, 조직구성원들의 정보보안 행동 및 성과를 체계화할 수 있다[42].

목표 설정은 업무 스트레스를 완화시키는 선행 요인이다. Quick[1979]은 조직 내 구성원들은 각자 업무 목표가 설정되어 있으며, 업무 목표 달성을 위해서는 자연스럽게 업무 관련 스트레스가 발생할 수 밖에 없다고 하였다[43]. 하지만, 주어진 업무 목표의 난이도가 높아서 업무 목표 달성을 위해 구성원들이 어렵게 목표 성과를 달성하고자 할 때, 그리고 업무 목표가 명확하여 어려운 목표 성과에 대한 이행 단계를 이해하고 있을 때, 업무 스트레스를 감소시킬 수 있다고 하였다[43]. Lee and Schuler[1980]은 조직 구성원의 업무스트레스 관리를 위한 목표설정과 리더십의 조건에 대한 연구에서, 개인 목표의 구체성과 난이도가 업무스트레스를 감소시켜 업무 만족도 및 성과에 긍정적인 영향을 가져온다고 하였다[44]. 즉, 정보보안 관점에서 목표의 설정(구체성, 난이도)이 정보보안에 의한 역할갈등을 감소시킬 것으로 판단하며, 다음의 연구가설을 제시한다.

H4: 정보보안 관련 목표 구체성은 정보보안 관련 역할갈등을 완화할 것이다.

H5: 정보보안 관련 목표 난이도는 정보보안 관련 역할갈등을 완화할 것이다.

2.5 정보보안 관련 조직공정성

조직공정성(organization justice)은 조직구성원에 대한 조직 차원에서 형성된 공정함에 대한 수준이면서, 행동 반응을 의미한다[45]. 조직공정성 이론의 기본적 가정은 개인의 특정 행동 및 결과의 만족 수준 등을 판단할 때, 상황별 상대적 공정성을 기반으로 행동에 대한 의미 및 가치를 부여한다는 것이다[46]. 즉, 조직에서 개인들의 행동 및 결과에 대한 평가는 주변과 자신을 비교하여 관련 정보의 확보, 행동의 절차, 그리고 결과에 대한 판단 수준 등을 복합적으로 고려하고, 과정과 결과의 피드백이 적절하다고 판단했을 때 공정하다는 것이다[47]. 공정성은 초기에는 결과 분배의 관점에서 공정성을 설명하다가, 최근에는 사전 정보 제공, 상호작용 관계, 그리고 행동의 절차까지 다양한 관점까지 확대되고 있다. 하지만, 공통적인 것은 공정성에 대한 판단 기준은 상대적인 것으로서, 공정성을 판단하는 당사자들은 특정 행동에 대한 비교 대상과의 상대적 비교를 통해 공정하다고 판단하며, 이성적 판단과 더불어 개인의 감정 등을 포함하여 판단한다고 본다[46].

조직공정성은 조직 구성원의 긍정적 마인드를 형성하도록 할 뿐아니라, 주어진 목표에 대한 능동적 행동과 성과를 달성하는데 도움을 준다[46]. 특히, 조직공정성은 조직 내 개인 차원의 결과변수인 조직 만족도 또는 조직 시민행동과 같은 긍정적이고 이타적인 행동을 할 수 있도록 돕는 선행요인으로서 가치를 가진다[48]. 뿐만 아니라, 조직공정성은 개인들의 조직에 대한 평가를 보다 긍정적으로 하고, 결과에 대한 보상 수준까지 기대하도록 하기 때문에, 업무 수준을 높이고, 특정 목표에 대한 능동적인 행동을 하도록 돕기 때문에, 조직 성장에 긍정적 영향을 준다[49].

정보보안 관점에서도 조직 공정성은 조직에 구축된 정보보안 목표 달성에 도움을 주는 선행 요인이다. 특히, 조직 공정성은 정보보안 미준수 행동 결과에 대한 조직 차원의 제재와 연계되어 준수의도를 높이는 선행 조건으로 활용된다. Xue et al.[2011]은 제재에 대한 조직원의 인지된 공정성은 미준수 행동에 의해 제재를 받을 상황에 이르게 될 경우, 제재 기대 수준을 높여 자신에게 직접적인 피해를 줄 수 있다는 것을 제기하고 관련 관계를 증명

하였다[50].

더불어, 정보보안 관련 조직공정성은 업무 스트레스를 완화하는 요인이다. 정보보안과 관련하여 조직공정성은 조직원에게 제공되는 정보의 공정성, 업무 절차에서 정보보안을 적용하는 과정의 공정성, 그리고 보안 업무 결과에 대한 제재 및 보상에 대한 동등한 평가 및 제공을 하는 것을 의미한다[51]. 즉, 정보보안 준수 행동에 영향을 주는 사전 정보, 상호작용, 예상되는 결과가 공정하다면, 정보보안 준수 당사자가 준수 행동 또는 미준수 행동으로 피해를 본다는 생각을 적게 할 수 있기 때문에 스트레스를 감소시킬 수 있다[52]. Hwang and Ahn[2019]은 정보보안과 관련하여 규정 등 행동 정보를 사전에 제공하고, 정보보안 준수 과정이 적합하고, 그리고 준수 결과가 공정하다면 정보보안 관련된 업무로 인한 스트레스(역할갈등 및 업무과부하)를 완화할 수 있음을 증명하였다[24]. 또한, Cho et al.[2019]은 정보보호 인력의 업무 스트레스와 이직의도에 미치는 영향관계를 조직공정성이 조절하는 것을 제시하였다[53]. 즉, 정보보안 관련 조직공정성은 정보보안 관련 역할갈등을 완화할 것으로 판단하고 다음의 연구가설을 제시한다.

H6: 정보보안 관련 조직공정성은 역할갈등에 음(−)의 영향을 미칠 것이다.

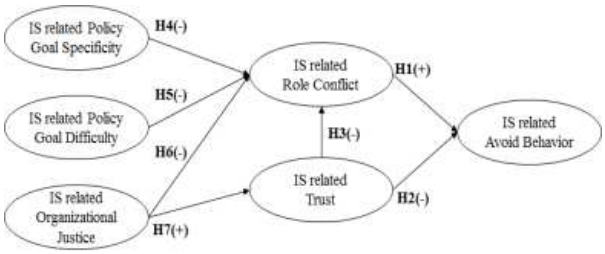
조직공정성은 신뢰를 높이는 선행요인이다. 조직에서 신뢰는 훼손되면 구성원들에게 지속적으로 부정적 인식을 주게 되고, 이후 신뢰를 다시 형성시키는 것은 매우 어렵다[27]. 따라서, 조직은 처음부터 조직을 저버리지 않도록 구성원들이 믿음을 가질 수 있도록 하는 것이 필요하다. 조직공정성은 자신과 비교가 되는 대상간의 지원 및 결과에 대한 수준이 공정한지에 대한 상대적 비교 수준이기 때문에, 조직원이 공정하다고 판단할 때 조직에 대한 믿음이 생기게 된다[49]. 실제로, Wong et al.[2006]은 신뢰를 상급자에 대한 신뢰, 조직에 대한 신뢰 두 가지 유형으로 보고, 상호작용 공정성, 절차공정성, 분배공정성과의 연관성을 확인하였다[48]. 분석 결과, 분배공정성과 절차공정성은 조직 차원의 신뢰에 영향을 주는 요인으로, 상호작용 공정성은 상급자에 대한 신뢰를 형성시키는 선행 조건임을 확인하였다[48]. 또한, Zeinabadi and Salehi[2011]은 사회적교환이론을 적용하여, 절차공정성과 신뢰, 직업 만족도간의 관계를 확인하였는데, 절차공정성은 조직의 신뢰를 높여 개인의 직업만족도를 높이는 것을 확인하였다[49]. 정보보안 분야에서도 조직공정성은 조직 신뢰를 높이는 요인이라고 판단하며, 다음의 연구가설을 제시한다.

H7: 정보보안 관련 조직공정성은 정보보안 관련 신뢰를 높일 것이다.

3. 연구 모델 및 방법

3.1 연구 모델

본 연구는 조직원의 정보보안 회피 행동에 영향을 주는 보안 관련 역할갈등을 감소시키기 위한 조직 차원의 노력요인을 제시함으로써, 내부자들의 정보보안 준수 수준을 높이는 것을 목적으로 한다. 역할갈등 완화 요인으로서 보안 정책 목표 설정, 조직 공정성, 그리고 신뢰 요인을 제시하였으며, 관련 연구모델은 다음 Fig. 1과 같다.



IS: Information security

Fig. 1. Research Model and Proposed Hypotheses

3.2 데이터 측정 방법 및 수집

조직 내부의 정보보안 회피행동 감소라는 연구 목적에 맞는 실증 분석을 위하여, 정보보안 기술 및 정책을 도입하고 있는 조직에서 근무하는 일반 근로자들을 대상으로, 설문지 기법으로 데이터를 확보하고, 구조방정식 모델링을 통하여 가설을 검증하였다.

설문지 개발은 연구 모델에 적용한 요인 및 관련 이론에 대한 선행 연구를 중심으로 다항목 기반의 설문 항목들을 검토하였으며, 7점 리커트 척도를 기반으로 정보보안 분야에 맞게 재구성하였다. 이후, 요인들의 설문 구성에 대한 타당성 확보를 위하여, 정보보안 정책 및 관련 기술을 도입하고 있는 기업에서 근무하는 대학원 학생 10명으로 부터 설문 항목 검토를 실시하였으며, 내용타당성이 있다고 판단하여 본 설문을 실시하였다.

설문 항목은 다음과 같은 선행연구를 기반으로 도출하였다. 첫째, 결과변수인 정보보안 회피행동은 Chen and Zahadi[2016]의 연구를 기반으로 3개 항목을 도출하였으며[16], 예를 들어 “정보보안 정책 위반 상황 발생 시,

지켜야 할 정보보안 관련 행동에 대한 회피한다"와 같은 항목을 구성하였다. 둘째, 정보보안 관련 역할갈등은 Tarafdar et al.[2007]의 연구를 기반으로 4개 항목을 도출하였으며[21], 예를 들어, "종종 보안 정책 때문에 내가 한 더 나은 판단에 반대되는 것을 하도록 요청 받는다" 와 같은 항목을 구성하였다. 셋째, 신뢰는 Agarwal[2013]의 연구를 기반으로 5개 항목을 도출하였으며[28], 예를 들어 "우리 회사는 약속을 지키기 위한 노력을 한다"와 같은 항목을 구성하였다. 넷째, 목표 구체성과 난이도는 Wright[2004]의 연구를 기반으로 각각 3개 항목들을 도출하였으며[36], "우리 회사는 명확하고 잘 정의된 정보보안 목표를 가지고 있다", "우리 회사의 정보보안 목표는 매우 도전적이다"와 같은 항목을 구성하였다. 마지막으로, 정보보안 공정성은 Ambrose and Schminke[2009]의 연구 기반으로 4개의 항목을 도출하였으며[54], "전반적으로, 나는 정보보안과 관련하여 공정한 대우를 받고 있다"와 같은 항목을 구성하였다. 이렇게 도출된 설문 항목은 22개이다.

설문 대상은 일반 근로자들을 대상으로 하되, 전산 팀 또는 정보보안 부서에서 근무하고 있는 근로자들은 제외하였는데, 이유는 해당 부서의 근로자들은 업무 목표가 IT 기술 또는 보안 정책 준수에 있기 때문에, 일반 업무를 보는 근로자들과 성과가 다르기 때문에 제외하였다.

설문은 대학의 사회교육원에서 주말에 경영학 수업을 듣는 학생들에게 총 500부를 배포하였으며, 설문은 사전에 설문에 대한 동의를 얻은 후 설문지를 배포하고 다시 한번 설문 목표와 데이터 활용에 대한 방법에 대한 설명을 한 후 설문에 응답하고자 하는 사람들만 대상으로 확보하였다. 총 433부를 확보하였으며, 이 중 설문에 문제가 있는 데이터를 제외하고 총 383개의 표본을 분석에 활용하였다. 표본의 인구통계학적 특성은 Table 1.과 같다.

Table 1. Demographic Characteristics of Sample

Demographic Categories of Sample		Frequency	%
Age	≤ 30	109	28
	31-40	125	32
	41-50	109	28
	≥ 51	40	10
Gender	Male	235	61
	Female	148	38
Type of Industry	Manufacturer	74	19
	Service	309	80
Job Position	Staff	123	32
	Assistant Manager	102	26
	Manager	115	30
	General Manager	43	11
Total		383	100

4. 가설 검증

4.1 신뢰성 및 타당성 분석

연구 가설 검증은 AMOS 22.0를 활용하여 변수들간의 상호 연관관계를 분석함으로써 관계성을 찾는다. 이를 위하여, 요인에 대한 신뢰성과 타당성 분석을 실시하였다. 신뢰성은 SPSS 21.0를 활용하여 크롬바하알파 값을 분석함으로써 확인하며, 22개의 세부 설문항목을 탐색적 요인분석을 실시하였다. 각 요인들의 신뢰도가 가장 낮은 요인은 목표 구체성(0.890)으로, 신뢰도 요구사항인 0.7 이상을 확보한 것으로 나타났다[55]. 타당성은 AMOS 22.0을 활용하여 확인적 요인분석을 실시하여, 변수 내 설문항목 간, 변수 간 차이가 있는지 확인한다. 우선 확인적 요인분석을 위한 모델링한 결과에 대한 모델의 적합도 분석을 실시하였으며, 적합도는 구조모형의 적합도 항목을 다각적으로 살펴보았다. 결과는 χ^2/df = 1.798, GFI = 0.923, AGFI = 0.9, CFI = 0.981, NFI = 0.958, RMSEA = 0.046와 같이 나타나, 선행연구의 요구수준을 달성하였다[56]. 변수 내 항목간의 타당성 적정성 기준은 개념신뢰도(contruct reliability) 0.8이상을 요구하며, 평균분산추출(average variance extracted) 0.5이상의 값들을 요구한다. 분석 결과 개념신뢰도와 평균분산추출 모두 요구사항에 적합한 것으로 나타났다.

Table 2. Result for Construct Validity and Reliability

Construct	Item	Factor Loading	Cronbach's Alpha	CR	AVE
Goal Difficulty	GD1	0.829	0.923	0.888	0.725
	GD2	0.841			
	GD3	0.738			
Goal Specificity	GS1	0.827	0.890	0.828	0.617
	GS2	0.855			
	GS3	0.777			
Organization Justice	OJ1	0.762	0.943	0.910	0.718
	OJ2	0.765			
	OJ3	0.767			
	OJ4	0.760			
Role Conflict	RC1	0.760	0.932	0.883	0.653
	RC2	0.782			
	RC3	0.763			
	RC4	0.759			
Trust	Trust1	0.822	0.941	0.912	0.675
	Trust2	0.846			
	Trust3	0.852			
	Trust4	0.814			
	Trust5	0.789			
Avoid Behavior	AB1	0.819	0.918	0.905	0.762
	AB2	0.920			
	AB3	0.877			

그리고, 변수간의 차별성에 대한 분석을 위하여 판별타당성(discriminant validity) 분석을 실시하였다. 판별

타당성은 요인들의 상관계수 값과 평균분산추출의 제곱근 값을 비교하되, 평균분산추출값이 클 때 판별타당성이 있다고 보는데[57], 요구사항에 적합한 것으로 나타났다. Table 3. 또한, 일변량 정상성 확인을 위하여, 개별 변인들의 왜도(skewness)와 첨도(kurtosis)를 확인하였다. 왜도는 절대값 2이하, 첨도는 절대값 4이하를 요구하는데[58], 개별변인들의 값이 요구사항에 적합한 것으로 나타나 정상분포를 하는 것으로 판단하였다. Table 3는 변수 평균값에 대한 왜도와 첨도를 제시한다.

Table 3. Result for Discriminant Validity

Constructs	1	2	3	4	5	6
Goal Difficulty	***0.852***					
Goal Specificity	0.47**	***0.785***				
Organization Justice	0.68**	0.59**	***0.847***			
Role Conflict	−0.65**	−0.58**	−0.67**	***0.808***		
Trust	.056**	0.46**	0.61**	−0.61**	***0.821***	
Avoid Behavior	−0.45**	−0.33**	−0.46**	0.45**	−0.43**	***0.873***
Skewness	−0.812	−0.744	−0.947	1.090	−0.985	−0.953
Kurtosis	0.662	0.559	0.979	1.215	1.431	1.349

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

또한, 다항목 설문에서 발생될 수 있는 공통방법편의(common method bias)문제를 확인하였다. 공통방법편의 확인은 단일방법요인 접근법(single method factor approaches)를 통해 실시하였다[59]. 본 접근법은 확인적 요인분석에서 단일 요인을 추가로 적용 전과 후의 측정 변인들의 추정치 변화량을 측정한다. 분석 결과 변인들의 추정치의 변화량이 최대 0.25보다 작은 것으로 나타나, 공통방법편의 문제가 낮은 것으로 판단되어 구조모형 평가를 실시한다.

4.2 구조모형 평가

변수의 신뢰성과 타당성에 문제가 없는 것으로 나타나, 연구 모델 및 가설에 대한 검증을 실시한다. 구조방정식모델링은 3가지 절차를 통해 검증 한다.

첫째, 구조모형의 적합도를 확인한다. 연구 모델을 구조적으로 제시하고 적합도를 확인하였으며, 결과는 χ^2/df = 1.9, GFI = 0.918, AGFI = 0.896, CFI = 0.978, NFI = 0.954, RMSEA = 0.049로 나타나 구조방정식모델링 요구수준을 종합적으로 상회하는 것으로 나타났다[56].

둘째, 구조모형의 요인간의 경로계수(β)를 파악함으로써 연구가설의 연관 관계를 확인한다. 가설 검정 결과는 다음 Fig. 2와 Table 4.와 같다.

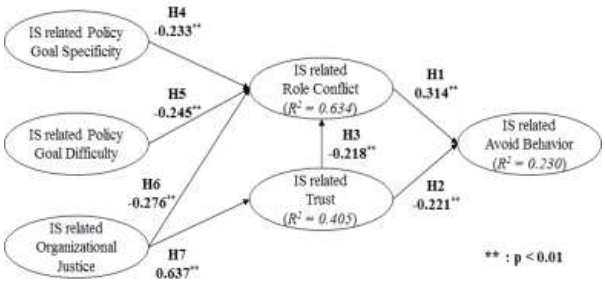


Fig. 2. Results of the Structural Model

Table 4. Summary of Hypothesis Tests

	Path	Coefficient	t−value	Results
H1	RC → AB	0.314	4.935**	Support
H2	Trust → AB	−0.221	−3.519**	Support
H3	Trust → RC	−0.218	−4.493**	Support
H4	GS → RC	−0.233	−4.628**	Support
H5	GD → RC	−0.245	−4.661**	Support
H6	OJ → RC	−0.276	−3.906**	Support
H7	OJ → Trust	0.637	12.789**	Support

**: $p < 0.01$
AB(Avoid Behavior), RC(Role Conflict), GS(Goal Specificity), GD(Goal Difficulty), OJ(Organization Justice)

연구가설 1은 정보보안 관련 역할갈등이 보안 회피행동을 높인다는 것으로, 분석 결과 경로간에 긍정적 영향관계에 있는 것을 확인하였다(H1: β= 4.935, p<0.01). 이러한 결과는 정보보안 관련 스트레스가 회피행동에 긍정적 영향을 미친다는 선행연구[24]의 연구와 일치한다. 즉, 정보보안 정책 및 기술 등의 도입으로 인하여, 개인의 업무에 차질 또는 갈등 문제가 발생될 경우 정보보안을 회피함으로써 문제를 해결하려는 경향이 있다는 것을 의미한다.

연구가설 2는 정보보안 관련 신뢰가 보안 회피행동을 완화한다는 것으로, 분석 결과 경로간에 부정적 영향 관계에 있는 것을 확인하였다(H1: β= −3.519, p<0.01). 이러한 결과는 신뢰가 정보보안 오남용을 감소시키는 선행조건이라는 선행연구[32]와 일치한다. 즉, 조직 내 보안절차 등에 대한 신뢰가 형성되면, 개인은 조직에서 요구하는 행동에 의미가 있다고 판단하기 때문에 회피행동을 감소시킬 수 있음을 의미한다.

연구가설 3은 정보보안 관련 신뢰가 역할갈등을 완화

한다는 것으로, 분석 결과 경로간에 부정적 영향 관계에 있는 것을 확인하였다(H1: β= −4.493, p<0.01). 이러한 결과는 병원 조직의 업무 스트레스 완화요인으로 신뢰를 제시한 선행연구[34]와 유사한 결과이다. 즉, 조직 내 새로운 정보보안이 도입되어 개인의 업무 절차 등에 문제를 제기하더라도 조직에 대한 신뢰가 형성되어 있다면, 개인은 조직 관점에서 접근하려는 경향이 있음을 의미하며, 신뢰의 형성이 필요함을 제시한다.

연구가설 4는 정보보안 목표 구체성이 역할갈등을 완화한다는 것으로, 분석 결과 경로간에 부정적 영향 관계에 있는 것을 확인하였다(H1: β= −4.628, p<0.01). 이러한 결과는 체계적인 목표 수립이 업무 스트레스를 감소시킨다는 선행연구[44]와 동일한 결과이다. 즉, 정보보안 정책 준수를 위한 구체적인 절차 및 목표를 제시할 경우, 수행 대상자는 목표달성에 어려움을 덜 겪기 때문에 갈등이 감소되는 것을 의미한다.

연구가설 5는 정보보안 목표 난이도가 역할갈등을 완화한다는 것으로, 분석 결과 경로간에 부정적 영향 관계에 있는 것을 확인하였다(H1: β= −4.661, p<0.01). 이러한 결과는 목표 난이도가 업무 스트레스와 부정적 상관관계에 있다는 선행연구[43]와 동일한 결과이다. 즉, 정보보안 정책 및 개인에게 주어진 목표가 달성가능하나 어렵게 되어 있다면, 준수 행동에 대한 욕구를 발생시키기 때문에 기존 업무와의 갈등을 감소시킬 수 있음을 의미한다. 즉, 연구가설 4와 5는 개인의 직무별 정보보안 목표를 제시하되, 기존 지키던 방식보다 엄격하되 단계별 지킬 수 있는 절차 및 방법을 제시할 때, 준수행동으로 이어질 수 있다는 것을 시사한다.

연구가설 6은 정보보안 공정성이 역할갈등을 완화한다는 것으로, 분석 결과 경로간에 부정적 영향 관계에 있는 것을 확인하였다(H1: β= −3.906, p<0.01). 이러한 결과는 분배, 절차, 상호작용 공정성이 업무 스트레스를 감소시킨다는 선행연구[24]와 동일한 결과이다. 즉, 개인에게 정보보안과 관련된 업무 과정, 결과 등 종합적인 수준이 공정하다고 판단되면, 준수의 필요성을 인지하게 되며 역할갈등을 감소시킨다는 것을 의미한다.

연구가설 7은 정보보안 관련 조직공정성이 정보보안 관련 조직 신뢰에 긍정적인 영향을 준다는 것으로, 분석 결과 경로간에 긍정적 영향 관계에 있는 것을 확인하였다(H1: β= 12.789, p<0.01). 이러한 결과는 조직 내 공정성과 신뢰간의 높은 상관관계를 제시한 선행연구[48]와 유사한 결과이다. 즉, 정보보안 관련 조직 공정성 수준이 높으면, 구성원들의 조직에 대한 믿음을 형성하며, 신뢰 수준으로 나타남을 의미한다.

셋째, 종속변수들의 결정 계수(R^2)를 분석함으로써, 선행요인에 대한 설명력을 제시한다. 회피행동은 역할갈등과 신뢰로부터 23%의 설명력을 가지는 것으로 나타났으며, 역할갈등은 목표 구체성, 목표 난이도, 조직 공정성, 그리고 신뢰로부터 63.4%의 설명력을 가지는 것으로 나타났다. 신뢰는 조직공정성으로부터 40.5%의 설명력을 가지는 것으로 나타났다.

5. 결론

5.1 연구의 요약

최근 조직 내 정보보안에 대한 관심이 높아지면서, 정보보안 기술 및 정책이 보다 엄격해지고 있다. 엄격한 수준의 보안 규제는 조직구성원의 보안 준수행동을 오히려 감소시킬 수 있어, 정보보안 관련된 업무 스트레스 감소를 위한 연구가 필요한 시점이다. 본 연구는 조직 내 구성원들의 정보보안 미준수 행동인 회피행동에 영향을 주는 스트레스 요인을 제시하고, 스트레스 완화를 위한 조직 차원의 노력 요인(조직 목표 설정, 조직공정성, 조직신뢰)을 제시하고자 하였다.

정보보안 스트레스와 회피행동을 완화시키기 위한 연구 모델에 대한 검증은 구조방정식모델링을 통해서 실시하였으며, 정보보안 정책 및 기술을 도입한 조직에서 근무하는 조직원을 대상으로 설문을 실시하였다.

연구가설 검증 결과, 조직원에게 형성된 정보보안 관련 스트레스인 역할갈등이 보안에 대한 회피 행동을 높이는 것을 확인하였고, 역할갈등을 완화하기 위한 조건으로서 정보보안 목표 구체성과 목표 난이도, 정보보안 조직 공정성과 신뢰가 영향을 주는 요인임을 확인하였다.

5.2 연구의 시사점 및 향후 연구

본 연구는 다음과 같은 이론적, 실무적 시사점을 가진다. 첫째, 정보보안 미준수 행동 중 하나인 회피행동과 업무 스트레스와의 관계를 확인하였다. 회피행동은 개인이 의도하였으나, 조직에게 피해를 주지 않고 자신의 불리한 상황 등을 개선하기 위한 행동요인으로서, 장기적으로는 조직의 보안 문화에 나쁜 영향을 주어, 보안 수준을 떨어뜨릴 수 있는 조건이다. 정보보안 관련 역할갈등은 회피행동을 높이는 것을 확인하였는데, 이론적 관점에서 기술스트레스 또는 조직의 일반적 상황의 역할갈등이 정보보

안 분야에도 적용될 수 있음을 확인하였다는 측면에서 시사점을 가진다. 또한 실무적 관점에서, 나날이 엄격해지는 정보보안 정책 및 기술 수준에 의해 실제 업무에 적용해야하는 조직원의 관점에서 업무적 갈등은 지속적으로 발생할 가능성이 높은데, 실제로 역할갈등과 회피행동 간의 긍정적 관계가 있음을 확인하였다. 즉, 정보보안 도입으로 인해 개인에게 주어진 본연의 성과 달성 절차 등에 문제가 생길 경우, 역할갈등이 생길 수 있음을 제시하였다. 따라서, 조직은 정보보안 정책, 기술 도입이 개인의 업무 스트레스에 발생할 이슈를 사전에 고려함으로써, 회피행동을 최소화시키기 위한 방안을 마련하는 것이 필요하다.

둘째, 정보보안 관련 역할갈등을 완화시키기 위한 조직 차원의 노력 요인으로서 목표설정이론을 적용하였으며, 세부 요인인 목표 구체성과 목표 난이도가 역할갈등을 완화함을 확인하였다. 이론적 관점에서, 목표설절이론과 스트레스간의 관계를 정보보안 분야에 적용함으로써, 선행 연구로서의 가치를 가질 것으로 판단한다. 실무적 관점에서, 조직 차원에서 정보보안 관련 목표의 구체적인 제시와 보안 목표 수준의 적정성을 고려하여 정책을 마련할 때, 개인이 받아들이는 스트레스 수준이 변화할 수 있음을 확인하였다. 즉, 개인은 정보 보안 체계의 변화에 따라 발생하는 업무적 변화, 차이 등에 따라 갈등을 일으키지만, 사전에 주어진 보안 목표 수준에 의해 갈등을 감소시킬 수 있음을제시하였으며, 완화관계에 있음을 확인하였다. 따라서, 조직 차원의 보안 목표 수립 시 접근해야 할 방향성을 제시했다는 측면에서 시사점을 가진다.

셋째, 정보보안 관련 역할갈등 수준 완화요인으로서 조직 공정성을 제시하였으며, 조직 공정성의 직접적인 완화효과와 신뢰를 통해 완화 효과를 가지는 것을 확인하였다. 이론적 관점에서, 결과는 정보보안 분야에 공정성과 스트레스간의 완화관계를 제시하고, 신뢰를 통한 매개효과 관계가 있음을 추가적으로 확인하였다. 즉, 조직 공정성과 신뢰가 정보보안 역할갈등을 감소시키는 선행요인임을 제시한 것에서 시사점을 가진다. 실무적 관점에서, 개인에게 형성된 보안 절차 등에 의한 역할갈등으로 인하여 증가할 수 있는 회피행동의 개선은 조직과 개인 간의 관계가 긍정적이고 친밀한 수준을 지속적으로 유지할 때 가능하다는 것을 확인하였으며, 보안 관련 조직의 활동인 사전 정보제공, 보안 절차, 보안 행동 결과에 대한 공정한 수준이 높음을 인지될 때 역할갈등을 완화시킬 수 있음을 확인하였다. 따라서, 조직은 개인에게 보안 관련 불편함 등의 문제가 발생되기 전에, 신뢰를 형성시키는 것이 필요하며, 모든 조직 내 구성원들이 공정하게 보안 정책을 따르고 있음을 지속적으로 제시하는 것이 필요하다.

본 연구는 다음과 같은 연구적 한계점을 가지며, 향후 연구에서는 개선될 필요성이 있다. 첫째, 조직구성원들의 보안 회피행동 관련 부정적, 긍정적 원인을 제시하기 위하여, 정보보안 정책을 보유한 조직의 근로자들의 설문을 통해 분석을 실시하였다. 설문은 응답자의 설문 당시의 생각을 중심으로 개인 관점의 회피행동 수준과 조직이 제공하는 정책 목표, 조직 공정성 수준을 확인하였다. 즉, 설문은 당시의 조직에 대한 개인의 생각을 확인하였기 때문에, 실제 조직이 제공하는 보안 수준에 대한 정보를 명확하게 알 수 없다는 한계를 가진다. 향후 연구에서는 리커트 척도가 아닌 지표 등을 통해 조직 목표 수준, 공정성 수준 등을 명확하게 측정할 수 있는 방안을 마련하여, 개인의 행동의지와의 연계성을 함께 연구한다면 높은 시사점을 제시할 것으로 판단한다.

둘째, 연구는 설문의 범위를 정보보안 정책을 도입한 기업의 일반 부서의 근로자로 통제하였다. 하지만, 조직의 업종별, 조직원의 직무별 정보보안 정책 및 기술을 받아들이는 수준의 차이가 발생할 것으로 판단한다. 예를 들어, 연구 부서 생산 부서, 그리고 마케팅 부서 등 부서에서 가지고 있는 정보의 중요도는 차별성이 높을 것으로 판단된다. 정보의 중요도에 따라 보안 수준의 차이는 자명한 것이기 때문에, 관련된 스트레스의 차이는 높게 발생할 것으로 판단된다. 향후 연구에서는 정보 관리의 중요도 등 수준별 보안 정책에 대한 차별화된 연구를 실시한다면 보다 높은 시사점을 가질 것으로 판단한다.

셋째, 역할갈등요인을 정책 목표, 조직공정성, 신뢰를 제시하였으나, 각 요인별 세부적으로 받아들이는 수준의 차이가 발생할 것으로 판단한다. 공정성을 예를 들어 정보제공 단위, 절차 단위, 결과 단위별로 조직공정성에 대한 인지는 차이가 있다. 즉, 스트레스 완화를 위한 세분화된 분야별 선행 요인을 제시한다면 정보보안 분야에 스트레스 감소를 위한 전략 수립에 도움이 될 것으로 판단한다.

REFERENCES

[1] Security News. (2020). *2020 Security Market Report.*

[2] Grand View Research. (2020). *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.

[3] 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.

[4] K. D. Loch, H. H. Carr & M. E. Warkentin. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. *MIS Quarterly*, *16(2)*, 173-186. DOI : 10.2307/249574.

[5] Verizon. (2019). *2019 data breach investigations report*.

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

[7] J. Han & Y. Kim. (2015). Investigating of Psychological Factors Affecting Information Security Compliance Intention: Convergent Approach to Information Security and Organizational Citizenship Behavior. *Journal of Digital Convergence*, *13(8)*, 133-144.

[8] S. Aurigemma & T. Mattson. (2017). Deterrence and Punishment Experience Impacts on ISP Compliance Attitudes. *Information and Computer Security*, *25(4)*, 421-436.
DOI : 10.1108/ICS-11-2016-0089.

[9] 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.

[10] J. Y. Son. (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.

[11] 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.
DOI : 10.1016/j.future.2019.03.024.

[12] I. Hwang & O. Cha. (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.

[13] J. D'Arcy & P. L. Teh. (2019). Predicting Employee Information Security Policy Compliance on a Daily Basis: The Interplay of Security-related Stress, Emotions, and Neutralization. *Information & Management*, *56(7)*, 103151.
DOI : 10.1016/j.im.2019.02.006.

[14] 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.

[15] J. M. Stanton, K. R. Stam, P. Mastrangelo & J. Jolton. (2005). Analysis of End User Security Behaviors. *Computers and Security*, *24(2)*, 124-133.
DOI : 10.1016/j.cose.2004.07.001.

[16] Y. Chen & F. M. Zahedi. (2016). Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China. *MIS Quarterly*, 40(1), 205-222.

[17] H. Liang & Y. Xue. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems*, *11(7)*, 394-413.
DOI : 10.17705/1jais.00232

[18] 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.

[19] R. Ayyagari, V. Grover & R. Purvis. (2011). Technostress: Technological Antecedents and Implications. *MIS Quarterly*, *35(4)*, 831-858.
DOI : 10.2307/41409963.

[20] K. J. Lauver & A. Kristof-Brown. (2001). Distinguishing between Employees' Perceptions of Person-Job and Person-Organization Fit. *Journal of Vocational Behavior*, *59(3)*, 454-470.
DOI : 10.1006/jvbe.2001.1807.

[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] M. Tarafdar, E. Bolman Pullins & T. S. Ragu-Nathan. (2014). Examining Impacts of Technostress on the Professional Salesperson's Behavioral Performance. *Journal of Personal Selling and Sales Management*, *34(1)*, 51-69.
DOI : 10.1080/08853134.2013.870184.

[23] 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.

[24] I. Hwang & S. Ahn. (2019). The Effect of Organizational Justice on Information Security-Related Role Stress and Negative Behaviors. *Journal of The Korea Society of Computer and Information*, *24(11)*, 87-98.
DOI: 10.9708/jksci.2019.24.11.087.

[25] D. Nachmias. (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.

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

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

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

[29] R. J. Lewicki, D. J. McAllister & R. J. Bies. (1998). Trust and Distrust: New Relationships and Realities. *Academy of Management Review*, *23(3)*, 438-458.
DOI : 10.5465/amr.1998.926620

[30] M. Top, M. Akdere & M. Tarcan. (2015). Examining Transformational Leadership, Job Satisfaction, Organizational Commitment and Organizational Trust in Turkish Hospitals: Public Servants Versus Private Sector Employees. *The International Journal of Human Resource Management*, *26(9)*, 1259-1282.
DOI : 10.1080/09585192.2014.939987.

[31] M. A. Krosgaard, S. E. Brodt & E. M. Whitener. (2002). Trust in the Face of Conflict: The Role of Managerial Trustworthy Behavior and Organizational Context. *Journal of Applied Psychology*, *87(2)*, 312-319.
DOI : 10.1037/0021-9010.87.2.312.

[32] P. B. Lowry, C. Posey, R. B. J. Bennett & T. L. Roberts. (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.

[33] J. Guinot, R. Chiva & V. Roca-Puig. (2014). Interpersonal Trust, Stress and Satisfaction at Work: An Empirical Study. *Personnel Review*, *43(1)*, 96-115.
DOI : 10.1108/PR-02-2012-0043.

[34] M. Top & S. Tekingunduz. (2018). The Effect of Organizational Justice and Trust on Job Stress in Hospital Organizations. *Journal of Nursing Scholarship*, *50(5)*, 558-566.
DOI : 10.1111/jnu.12419.

[35] E. A. Locke & G. P. Latham. (2006). New Directions in Goal Setting Theory. *Current Directions in Psychological Science*, *15(5)*, 265-268.
DOI: 10.1111/j.1467-8721.2006.00449.x.

[36] B. E. Wright. (2004). 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*, *14(1)*, 59-78.
DOI : 10.1093/jopart/muh004

[37] R. D. Pritchard, S. D. Jones, P. L. Roth, K. K. Stuebing & S. E. Ekeberg. (1988). Effects of Group Feedback, Goal Setting, and Incentives on Organizational Productivity. *Journal of Applied Psychology*, *73(2)*, 337-358.

[38] R. Vollmeyer, B. D. Burns & K. J. Holyoak. (1996). The Impact of Goal Specificity on Strategy Use and the Acquisition of Problem Structure. *Cognitive Science, 20(1)*, 75-100.
DOI : 10.1207/s15516709cog2001_3.

[39] J. M. Diefendorff & G. A. Seaton. (2015). *Work Motivation*. International Encyclopedia of the Social & Behavioral Sciences, 2nd edn. Elsevier, Oxford, 680-686.

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

[41] 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.

[42] I. Koskosas. (2008). Goal Setting and Trust in a Security Management Context. *Information Security Journal: A Global Perspective*, *17(3)*, 151-161.
DOI : 10.1080/19393550802290337.

[43] J. C. Quick. (1979). Dyadic Goal Setting and Role Stress: A Field study. *Academy of Management Journal*, *22(2)*, 241-252.
DOI : 10.5465/255587.

[44] C. Lee & R. S. Schuler. (1980). Goal Specificity and Difficulty and Leader Initiating Structure as Strategies for Managing Role Stress. *Journal of Management*, *6(2)*, 177-187.
DOI : 10.1177/014920638000600206.

[45] R. H. Moorman. (1991). Relationship between Organizational Justice and Organizational Citizenship Behaviors: Do Fairness Perceptions Influence Employee Citizenship?. *Journal of Applied Psychology*, *76(6)*, 845-855.
DOI : 10.1037/0021-9010.76.6.845.

[46] J. A. Colquitt. (2001). On the Dimensionality of Organizational Justice: A Construct Validation of a Measure. *Journal of Applied Psychology*, 86(3), 386-400.

[47] B. Meyer. (2001). Allocation Processes in Mergers and Acquisitions: An Organizational Justice Perspective. *British Journal of Management*, 12(1), 47-66.
DOI : 10.1111/1467-8551.00185.

[48] Y. T. Wong, H. Y. Ngo & C. S. Wong. (2006). Perceived Organizational Justice, Trust, and OCB: A Study of

Chinese Workers in Joint Ventures and State-owned Enterprises. *Journal of World Business*, *41(4)*, 344-355. DOI : 10.1016/j.jwb.2006.08.003.

[49] H. Zeinabadi & K. Salehi. (2011). Role of Procedural Justice, Trust, Job Satisfaction, and Organizational Commitment in Organizational Citizenship Behavior (OCB) of Teachers: Proposing a Modified Social Exchange Model. *Procedia-Social and Behavioral Sciences*, *29*, 1472-1481. DOI : 10.1016/j.sbspro.2011.11.387.

[50] Y. Xue, H. Liang & L. Wu. (2011). Punishment, Justice, and Compliance in Mandatory IT Settings. *Information Systems Research*, *22(2)*, 400-414. DOI : 10.1287/isre.1090.0266.

[51] K. A. Alshare, P. L. Lane & M. R. Lane. (2018). Information Security Policy Compliance: A Higher Education Case Study. *Information & Computer Security*. *26(1)*, 91-108, DOI : 10.1108/ICS-09-2016-0073.

[52] H. Li, R. Sarathy, J. Zhang & X. Luo. (2014). Exploring the Effects of Organizational Justice, Personal Ethics and Sanction on Internet Use Policy Compliance. *Information Systems Journal*, *24(6)*, 479-502. DOI : 10.1111/isj.12037.

[53] J. Cho, J. Yoo & J. Lim. (2019). An Impact Analysis of Information Security Professional's Job Stress and Job Satisfaction to Turnover Intention: Moderation of Organizational Justice. *Journal of Society for e-Business Studies*, *24(3)*, 143-161, DOI: 10.7838/jsebs.2019.24.3.143.

[54] M. L. Ambrose & M. Schminke. (2009). The Role of Overall Justice Judgments in Organizational Justice Research: A Test of Mediation. *Journal of Applied Psychology*, *94(2)*, 491-500. DOI : 10.1037/a0013203.

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

[56] B. H. Wixom & H. J. Watson. (2001). An Empirical Investigation of the Factors Affecting Data Warehousing Success, *MIS Quarterly*, *25*(1), 17-41. DOI : 10.2307/3250957.

[57] C. Fornell & D. F. Larcker. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error, *Journal of Marketing Research*, *18(1)*, 39-50. DOI: 10.1177/002224378101800104.

[58] S. G. West. J. F., Finch & P. J. Curran. (1995). *Structural Equation Models with Non-normal Variables: Problems and Remedies*. In R. H. Hoyl (Ed.). Structural Equation Modeling: Conceots, Issues, and Applications, pp. 56-75. Thousand Oaks, CA: Sage.

[59] P. M. Podsakoff, S. B. MacKenzie, J. Y. Lee & N. P. 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. DOI : 10.1037/0021-9010.88.5.879.

황 인 호(In-Ho Hwang) [정회원]

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