조직 내부자의 정보보안 준수 향상에 대한 연구

A Study on Improving Information Security Compliance of Organization Insider

황인호[1*]

In-Ho Hwang[1*]

〈Abstract〉

The expansion of information sharing activities using online can increase the threat of information exposure by increasing the diversity of approaches to information within an organization. The purpose of this study is to present conditions for improving the information security compliance intention of insiders to improve the level of information security within the organization. In detail, the study applies the theory of planned behavior that clearly explains the cause of an individual's behavior and proposes a way to increase the compliance intention by integrating the social control theory and goal-setting theory. The study presented research models and hypotheses based on previous studies, collected samples by applying a questionnaire technique, and tested hypotheses through structural equation modeling. As a result, information security attitude, subjective norms, and self-efficacy had a positive influence on the intention to comply. Also, attachment, commitment, and involvement, which are the factors of social control theory, formed a positive attitude toward information security. Goal difficulty and goal specificity, which are the factors of goal setting theory, formed a positive self-efficacy. The study presents academic and practical implications in terms of suggesting a method of improving the information security compliance intention of employees.

Keywords : Compliance Intention, Theory of Planned Behavior, Social Control Theory, Goal-Setting Theory

1* 정회원, 교신저자, 국민대학교 교양대학 조교수 1* Assistant Professor of Collage of General Education
E-mail: hwanginho@kookmin.ac.kr

1. 서 론

세계적으로 발생하고 있는 코로나19 사태는 많은 조직과 구성원들의 행동 방식을 변화시키고 있다. IT 업체들은 빠르게 온라인 미팅 및 업무 공유와 관련된 기술을 출시하고 있으며, 조직들은 해당 기술들을 업무에 적용하면서 코로나19 초반에 겪던 업무 효율성 문제는 많이 감소하였다. 하지만, 온라인 기반 업무 공유와 같은 효율성 확대 관점의 기술 도입은 내부자에 의한 정보 노출 가능성을 높일 수 있다. 예를 들어, 재택 근무는 개인이 조직의 정보시스템 화면을 보다 쉽게 타인에게 보여줄 수 있으며, 온라인 미팅 시 악의적인 외부 해킹 프로그램들의 침입이 가능하다[1]. 다시 말해, 온라인 기반의 정보 공유 환경이 확대되면서, 내부자의 정보 자원 노출 위협은 커질 수 있으며 대처방안을 마련하는 것이 필요하다[2].

내부자의 정보보안 위협 문제에 대한 해결책으로 선행연구들은 개인들의 심리적 관점의 접근을 중요시하여, 조직이 접근해야 할 전략적 방향을 제시해왔다. 대표적으로 개인은 이성적으로 조직이 요구하는 정보보안 행동에 대한 분석(이익, 비용 분석)을 통해 해당 행동에 대한 의사결정을 하므로, 정보보안 관련 정보를 명확하게 제공해야 한다는 합리적 선택이론 중심의 정보보안 연구[3], 개인이 정보보안 미준수 시 발생할 위협, 공포 등을 명확하게 인식하고 조직 지원 및 개인의 역량 등으로 대처 방법을 인지하고 있을 때, 정보보안 준수 행동은 높아지기 때문에 조직 차원의 정보보안 대처 방법을 제공해야 한다는 보호동기이론 중심의 정보보안 연구[4,5], 개인의 정보보안 행동은 외재적 동기(조직의 보상, 제재 등)와 내재적 동기(가치 일치, 조직 일치 등)에 의해 결정되기 때문에 동기 향상을 위한 조직의 노력이 필요하다는 동기이론 기반의 연구[6] 등이 있다. 선행연구들은 범죄학 등 타 분야에서 중점적으로 활용되던 이론들을 정보보안 분야에 적용하여, 다양한 개인의 보안 행동 원인을 제시해온 측면에서 시사점을 가진다.

최근에는 대표적인 개인행동에 대한 예측 모델인 계획된 행동이론(theory of planned behavior)을 적용하여[7-10], 정보보안 관련 행동의도 및 보안 행동의 구성요인을 강화하는 선행 조건을 제시한 연구들이 제시되고 있다. 계획된 행동이론은 행동의 예측성 관점에서 매우 높은 적합성을 보이기 때문에, 정보보안 상황에서 내부자의 행동을 예측할 수 있다는 관점에서 중요성이 높다.

본 연구는 조직 내부자들의 잠재적인 정보보안 행동 수준을 높이기 위한 조건으로 계획된 행동이론의 구성요인을 적용하고, 각 요인을 강화하기 위한 상황적 조건을 제시하고자 한다. 특히, 연구는 행동 결정에 있어 개인의 성향과 조직의 노력 요인을 복합적으로 살펴본다. 즉, 연구는 개인의 조직에 대한 믿음 및 행동을 결정하는데 높은 설명력을 보이는 사회통제이론(social control theory)을 적용하여, 개인의 정보보안 태도를 높이는 방안을 제언하고자 한다. 또한, 조직이 개인에게 집단의 목표를 어떻게 제시할 때, 개인이 성취감을 느끼고 행동으로 이어지는지를 설명하는 목표설정이론(goal setting theory)을 적용하여, 자기효능감에 영향을 주는 보안 환경적 측면의 방향을 제시하고자 한다. 즉, 본 연구는 정보보안에 대한 개인의 동기적 측면과 조직의 지원 측면을 함께 고려함으로써, 조직 내부의 보안 행동 향상 방안을 제시하고자 한다.

2. 이론적 배경

2.1 정보보안 준수의도

조직 내부의 정보보안 사고는 시간, 장소와 관계없이 조직 내 정보시스템에 접근 가능한 사람이면 누구나 일으킬 수 있다. 실제로, 전 세계 정보보안 사고 비율 중 내부자의 사고는 매년 전체 사고의 20~30%를 유지하고 있으며, 사무직, 엔지니어 등 정보관리자가 아닌 내부자들이 정보 노출 사고를 일으키고 있음을 감안 하면[11], 내부자에 의한 정보보안 노출 위협을 낮추기 위한 행동이 필요한 상황이다.

내부자들의 정보보안 준수 행동은 준수의도가 형성될 때 가능하다[2]. 정보보안 준수의도(compliance intention)는 조직이 보유한 핵심 정보 자원들을 보존하고 외부 또는 내부의 위협으로부터 보호하고자 하는 개인 의지의 수준으로서[3,12], 조직이 요구하는 수준의 정보 관리 및 보호를 위한 노력을 하겠다는 의지를 의미한다[13]. 본 연구는 행동 및 행동의도에 대한 예측력에 높은 정합성을 보이는 계획된 행동이론을 정보보안 분야에 적용하되, 계획된 행동이론의 구성요소를 높일 수 있는 조건을 확인함으로써, 의도 향상 방안을 제시하고자 한다.

2.2 계획된 행동이론

계획된 행동이론은 합리적 관점을 통해 행동이 결정되며, 행동을 결정하는 선행 조건은 행동에 대한 믿음을 통해 형성된 태도, 외부의 상황에 대한 믿음을 통해 형성된 주관적 규범, 그리고 통제에 대한 믿음을 통해 형성된 인지된 행동 통제로 구성되어 있다는 이론이다[9]. 즉, 계획된 행동이론은 개인의 행동 또는 행동 의도는 관련 상황에 대한 행동 태도와 개인을 둘러싼 환경적 특성에 대한 인식, 그리고 문제를 통제할 수 있다는 인식으로 결정되는 것을 상세히 설명하였기 때문에, 조직과 개인간의 관계에서 개인의 행동 원인을 상세히 설명하고, 높은 예측력을 제시하였다는 측면에서 높은 시사점을 가지고 있다[14].

계획된 행동이론을 정보보안 분야에 적용한 선행연구들은 조직 내 개인의 정보보안 준수의도에 영향을 주는 조건인 태도, 자기효능감, 주관적 규범 등에 긍정적 영향을 주는 선행 요인을 다각적 관점에서 제시하고 있다. 정보보안 분야에 보호동기이론과 계획된 행동이론을 접목하여, 정보보안 위협에 대한 인식과 대처 인식, 그리고 계획된 행동이론의 구성요인이 정보보안 준수 행동에 미치는 영향을 확인한 연구[7,14], 동기이론과 계획된 행동이론을 접목하여, 내재적, 외재적 동기가 태도에 미치는 긍정적 영향을 통해 준수행동 향상 방향을 제시한 연구가 대표적이다[15].

본 연구는 선행연구를 기반으로 행동의도에 영향을 주는 구성요인으로 태도, 자기효능감, 그리고, 주관적 규범을 적용한다.

태도(attitude)는 본인의 과거 경험을 통해 형성되는 해당 대상에 관한 호의성으로서[16], 태도의 대상은 본인을 둘러싼 집단적 환경일 수도 있으며, 특정한 사건과 같은 개별적 특성에 대한 관점일 수도 있다[14]. 정보보안과 관련하여 태도는 조직 또는 자신이 겪었던 경험에 기반하여 형성된 정보보안에 대한 호의적인 믿음이기 때문에, 긍정적인 태도가 형성된 사람은 조직이 요구하는 정보보안 관련 행동을 따르려는 경향을 보인다[15].

주관적 규범(subjective norm)은 정보보안 분야에서 사회적 규범 또는 사회적 영향 등으로 적용되는 요인으로, 조직의 정보보안 관련 환경적 조건에 기반하여 형성된 주관적 조직 문화에 대한

내재화 수준으로 정의된다[17]. 즉, 주관적 규범은 개인의 환경적 존재인 조직에서 구축한 정보보안 규범적 특성에 대하여 구성원과 함께 하려는 생각의 수준으로, 조직 내 모든 사람이 정보보안을 준수하고 본인도 조직 구성원으로서 함께 하고자 마음을 먹을 때, 조직이 추구하는 정보보안 관련 행동을 수행한다는 관점이다[15]. 따라서, 주관적 규범이 높은 개인은 조직을 위한 행동을 하려는 경향을 보이기 때문에 긍정적 행동의도를 보인다.

자기효능감(self-efficacy)은 자신에게 주어진 대상의 특정 문제를 통제하거나, 목표를 달성할 수 있다고 판단하는 평가 수준으로서[16], 당사자 해당 문제에 대하여 외부적인 압력이나 요구사항을 기준으로 의사결정을 하는 것이 아니라, 스스로 문제를 어떻게 통제하고 관리할 것인지를 판단하는 수준이기 때문에, 행동의도에 높은 영향을 주는 조건이다[14]. 정보보안 관점에서 자기효능감은 정보보안 기술관점에서 기술 활용성에 대한 통제 및 행동 가능성을 설명하기 위해 적용되거나[10], 정보보안 전반에 걸친 문화 또는 정책 적용 관점에서 적용되는 등 다양한 측면에서 활용되고 있다[8]. 즉, 계획된 행동이론의 구성요소인 태도, 자기효능감, 그리고 주관적 규범은 정보보안 준수의도를 높이는 선행요인이며, 연구가설은 다음과 같다.

H1: 정보보안 태도는 정보보안 준수의도에 양(+)의 영향을 준다.

H2: 정보보안 주관적 규범은 정보보안 준수의도에 양(+)의 영향을 준다.

H3: 정보보안 자기효능감은 정보보안 준수의도에 양(+)의 영향을 준다.

2.3 사회통제이론

사회통제이론은 사회, 조직, 특정 집단에서 개인의 해당 집단에 대한 긍정적 또는 부정적 행동 원인을 제시하는 이론이다[18]. 대표적으로, 사회통제이론은 긍정적 관점에서 집단에 대한 개인의 바람직한 행동 원인이 무엇인지를 설명하고, 집단에서 범죄 등 부정적 행동을 저지르는 원인이 무엇인지를 설명한다[19]. 즉, 사회통제이론은 개인의 주변 사람 또는 주변 집단의 속성에 초점을 맞추고 있으며, 속성간의 동일성 또는 유대감이 형성될 때 집단에 적합한 행동을 보인다는 관점이다[20].

사회통제이론에서 개인과 집단 간의 유대감을 설명하는 대표적인 세부 요인은 애착, 몰입, 관여가 있다. 애착(attachment)은 개인이 타인 또는 집단에 가지는 애정과 존중을 의미한다[21]. 즉 애착은 조직에 대한 가치를 식별하는 선행 조건으로서, 조직에 대한 애착이 형성된 개인은 조직이 본인과 동일한 관점에 존재하는 집단으로 판단하여, 조직과 동일시하고자 하는 경향을 보인다[15].

몰입(commitment)은 조직의 목표를 달성하기 위해 필요한 개인의 노력 수준을 의미한다[13]. 특정 집단에 대해 몰입하는 사람은 대상의 목표에 대한 이해를 위하여 지속적인 노력과 시간을 투자하기 때문에, 자연스럽게 지식을 형성하게 되어 긍정적 태도를 형성한다. 조직 몰입은 조직의 목표 달성을 위한 노력, 약속, 지원 등을 포함한다. 따라서, 조직 몰입이 형성된 사람들은 조직이 부여한 규칙을 어길 위험을 감수하지 않고 자신이 지금까지 노력한 것을 보존하고자 한다[15].

관여(involvement)는 누군가가 조직의 특정 활동이나 주제에 관여하는 시간 및 노력의 양을 의미한다[13]. 즉, 관여는 개인과 관여 대상 간에 관계의 깊이를 의미하는데, 높은 수준의 관여는 대상에 대한 의미가 깊어져 쉽게 참여 대상에 대해 취했던 태도나 행동을 변화하지 못한다[21]. 조직 내 특정 활동에 대한 지속적인 관여는 활동의 행

동 절차에 대한 이해도가 높이기 때문에, 긍정적인 태도를 형성한다[22].

사회통제이론의 세부 요인인 애착, 몰입, 그리고 관여는 개인의 태도 형성에 영향을 준다. 집단에 대한 소속감 또는 일체감과 관련된 애착, 몰입, 그리고 관여가 높을 경우, 해당 집단에 대한 긍정적 또는 부정적 행동 태도를 형성시키고, 조직이 추구하는 목표에 대한 행동의도를 가지게 된다[13,14]. 또한, Lee et al.[2004]은 내부자의 정보보안 통제 의도에 영향을 주는 조건으로서 제재이론과 사회통제이론을 적용하였으며, 사회통제이론의 구성요인 중 관여와 규범이 행동 통제 의도에 긍정적 영향을 주는 것을 확인하였다[22]. 즉, 조직이 요구하는 정보보안에 대한 명확한 태도 형성을 위해서는 사회통제이론의 애착, 몰입, 관여가 중요한 영향을 미칠 것으로 판단하며, 연구가설을 제시한다.

H4: 정보보안 애착은 정보보안 태도에 양(+)의 영향을 준다.

H5: 정보보안 몰입은 정보보안 태도에 양(+)의 영향을 준다.

H6: 정보보안 관여는 정보보안 태도에 양(+)의 영향을 준다.

2.4 목표설정이론

사람은 합리적인 행동을 보인다는 가정을 기반으로, 자신 또는 집단이 부여한 목표 달성을 위해 행동한다는 이론이 목표설정이론이다[23]. 즉, 목표는 개인이 추구하는 목적 및 방향일 수 있으며, 자신이 속한 집단의 비전 또는 조직이 자신에게 부여한 업무적 목표일 수 있다. 따라서, 개인에게 있어서 목표는 대상별 특성별 다양하게 제시되며, 개인은 주어진 목표 달성을 위하여 합리적인 의사결정을 통해 단계별로 노력한다는 관점이다[24].

목표설정이론에 따르면, 주어진 목표 달성을 위해 더욱 노력하고 결과로 나타나기 위해서는 난이도와 구체성이라는 2가지 조건이 필요하다. 목표 난이도(goal difficulty)는 개인이 달성해야 할 목표의 수준이 달성은 가능하나 현재에는 무척 어려운 수준의 상태를 의미하며, 목표 구체성(goal specificity)은 달성해야 할 목표를 달성할 수 있도록 매우 구체적인 상태를 의미한다[23,25]. 즉, 목표 난이도는 개인이 쉽게 달성할 수 있는 수준의 목표가 아니라, 지속적인 노력을 동반해야 해결 및 달성할 수 있는 목표의 수준이며, 목표 구체성은 개인이 이해할 수 있고 단계별 조금씩 성취감을 가질 수 있는 구체적으로 분류된 목표의 단계를 의미한다[25].

조직이 도입한 정책 미션을 명확하게 제시하는 것은 구성원의 행동 방향을 결정하기 때문에, 조직 차원의 방향성을 제시하는 것이 무엇보다 중요하다. Lowry et al.[2015]은 조직의 특정 활동이 구성원들의 행동으로 이어지도록 하기 위해서는 경영층의 관심과 활동에 대한 강력한 의지의 선언이 필요하다고 보았으며, 정보보안 또한 마찬가지로 보았다[26]. 즉, 정보보안 정책 방향이 구성원들의 준수 행동으로 이어지기 위해서는 정확하게 조직이 추구하는 보안 목표를 이해하고, 어떻게 행동해야 하는가를 인지하고 있는 것이 매우 중요하며, 정보보안 정책 미션 선언 및 지원이 개인의 행동 의도로 이어진다고 하였다[26].

단계별 맞춤형 목표 설정은 개인의 자기효능감을 높여 행동으로 이어진다. Locke and Latham [1990]은 일찍이 개인의 성과에 대한 동기 형성 과정을 설명하면서, 개인에게 명확하게 할당된 목표(목표의 난이도가 높으며, 단계별 달성 가능한 목표를 제시)는 개인이 스스로 문제에 대한 통제를 하고 행동을 할 수 있다는 믿음의 관점인 자기효능감에 영향을 주어 개인의 목표를 형성시켜 조

직 성과로 이어진다고 하였으며[27], Wright[2004]는 조직의 목표 구체성이 개인의 목표 구체성을 높이고 업무 동기를 형성시키지만, 너무 엄격한 목표에 대한 강제성을 부여 시, 개인이 달성 가능한 목표 난이도를 넘겨 자기효능감에 부정적 영향을 준다고 하였다[24]. 즉, 개인에게 부여된 정보보안 정책의 목표 난이도와 구체성이 자기효능감에 긍정적 영향을 줄 것으로 판단하며, 연구가설을 제시한다.

H7: 정보보안 정책 목표 난이도는 정보보안 자기효능감에 양(+)의 영향을 준다.

H8: 정보보안 정책 목표 구체성은 정보보안 자기효능감에 양(+)의 영향을 준다.

3. 연구 모델 및 방법

3.1 연구 모델

연구의 목적은 조직 내부자들의 정보보안 행동 향상 방안을 제시하는 것이다. 선행연구를 기반으로 도출한 연구 모델은 Fig. 1과 같다.

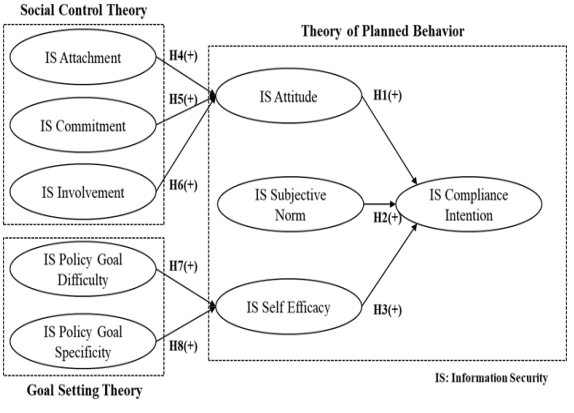

Fig. 1 Research Model and Proposed Hypotheses

3.2 데이터 측정 방법 및 수집

연구 모델의 요인들은 계획된 행동이론, 사회통제이론, 목표설정이론의 세부 요인들로 구성되어 있으며, 정보보안 또는 정보기술 분야에 적용되었던 요인들의 설문 문항을 중심으로 정보보안 특성에 맞추어 변경하여 7점 척도로 적용하였다.

정보보안 준수의도는 조직 정보 자산을 보호하기 위하여 행동할 것이라는 의지 수준으로서 선행연구를 통해, “조직의 정보 시스템 접속 시 보안 정책을 따를 것”, “업무 수행 시 보안 절차를 따를 것”, “보안 정책을 따를 것이라는 태도에 확신을 가짐”과 같은 3개 문항을 적용하였다[12].

계획된 행동이론은 태도, 주관적 규범, 자기효능감으로 구성된다. 태도는 정보보안 준수에 대한 방향 수준을 의미하며, 선행연구를 통해 “보안 기술&방법을 채택하는 것은 중요”, “보안 기술&방법을 채택하는 것은 혜택이 있음”, “보안 기술&방법을 채택하는 것은 도움이 됨”의 3개 문항을 적용하였다[15]. 주관적 규범은 구성원들의 조직의 정보보안 요구사항을 준수해야한다고 생각하는 수준으로서, 선행연구를 통해 “나의 동료들은 내가 정보보안 요구사항을 준수해야한다고 생각”, “임직원은 내가 정보보안 요구사항을 준수해야한다고 생각”, “보안 관리자들은 내가 정보보안 요구사항을 준수해야 한다고 생각”의 3개 문항을 적용하였다[3]. 자기효능감은 정보보안 실행에 대한 기대와 신념의 수준으로서 선행연구를 통해 “사전에 도움을 받을 수 있다면, 나는 정보보안을 쉽게 적용할 수 있을 것”, “정보보안 어려움이 발생 시 다른 사람을 부를 수 있다면, 나는 정보보안을 쉽게 적용할 수 있을 것”, “정보보안 시작 시 도움을 받을 수 있다면, 나는 정보보안을 쉽게 적용할 수 있을 것”, “충분한 시간이 있다면, 나는 정보보안을 쉽게 적용할 수 있을 것”의 4개 문항을 적용

하였다[3].

사회통제이론은 애착, 몰입, 관여로 구성되어 있으며, 조직의 정보보안 활동에 대한 개인 차원에서 참여하고자 하는 요인들이다. 애착은 조직의 정보보안 가치에 대하여 일치하고자 하는 수준으로, 선행연구를 통해 “정보보안 위협에 대한 조직의 우려는 나에게 중요함”, “나는 조직의 정보자산을 보호하기 위해 노력하고 싶음”, “조직의 보안 문제가 나의 문제임”의 3개 문항을 적용하였다[13]. 몰입은 조직의 정보보안 목표를 지원하기 위해 소비하는 개인의 노력 수준으로, 선행 연구를 통해 “나는 조직의 정보 자산을 보호하기 위하여 최선을 다하고 있음”, “나는 정보보안을 위태롭게 하는 부정행위를 방지하기 위하여 노력하고 있음”, “나는 정보보안 실수를 피하기 위해 정보보안 정책을 준수할 것”의 3개 문항을 적용하였다[13]. 관여는 정보보안 활동에 참여하고자 하는 수준으로, 선행연구를 통해 “나는 정보보안 활동에 적극적으로 참여함”, “나는 잘못된 행동을 피하기 위해 조직의 정보보안 정책에 참여함”, “나는 정보보안 활동에 참여하는 것을 가치 있게 생각함”의 3개 문항을 적용하였다[13].

목표설정이론의 세부 요인은 목표 난이도와 목표 구체성으로 구성되어 있으며, 조직이 구축한 정보보안 정책의 목표가 개인에게 받아들여지는 수준에 대한 구성을 의미한다. 목표 구체성은 선행연구를 통해 “조직의 정보보안 목표를 명확하게 설명할 수 있음”, “조직의 정보보안 방향성을 이해하고 있음”, “조직은 명확한 보안 목표를 가지고 있음”의 3개 문항을 적용하였다[24]. 목표 난이도는 선행연구를 통해 “조직 보안 목표 달성은 많은 노력을 필요로 함”, “정보보안 달성은 높은 수준의 기술과 지식을 요구”, “보안 목표는 매우 높은 수준을 요구”의 3개 문항을 적용하였다[24].

설문 대상은 정보보안 정책을 업무에 적용하고 있는 조직원으로서, 보안 부서에 근무하는 조직원은 일반 업무를 보는 조직원과 부서의 목표가 다르기 때문에 제외하였다. 보안 부서의 목표는 조직 구성원의 보안 준수에 있으며, 일반 직원들의 목표는 자신에게 부여된 업무 성과달성에 있으며, 보안은 추가적인 행동 개념이기 때문이다. 설문은 직장에 다니면서, 학교생활을 하는 재직자 전형의 경영학과 학생들을 대상으로 하였으며, 설문 전 조직이 정보보안 정책을 운영하고 있는지를 확인하고, 설문의 목표와 통계 활용의 방식에 대하여 정확하게 전달한 후, 정책을 모르거나 설문에 부담을 가진 사람을 제외하고 설문을 실시하였다. 2019년 12월 동안 설문을 실시하였으며, 유효 표본 318개를 확보하였다. 분석에 적용한 표본 318개의 특성은 Table 1과 같다.

Table 1. Demographic Characteristics

인구 통계 구분		빈도	%
성별	남성	176	55.3
	여성	142	44.7
산업	제조업	65	20.4
	서비스업	253	79.6
직위	사원	134	42.1
	대리	82	25.8
	과장	50	15.7
	차, 부장 이상	52	16.4
전체		318	100.0

4. 가설 검증

4.1 신뢰성 및 타당성 분석

연구 모델에 적용한 요인들은 다 항목 기반의 설문 문항으로 구성되어 있으므로, 요인들의 신뢰

Table 2. Result for Validity and Reliability

변수	항목	크론바흐 알파	개념 신뢰도	평균분산 추출
애착	ISA 1 ISA 2 ISA 3	0.931	0.893	0.735
몰입	ISC 1 ISC 2 ISC 3	0.895	0.864	0.680
관여	ISI 1 ISI 2 ISI 3	0.904	0.821	0.604
목표 난이도	GD 1 GD 2 GD 3	0.892	0.861	0.756
목표 구체성	GS 1 GS 2	0.918	0.819	0.602
태도	Atti 1 Atti 2 Atti 3	0.940	0.900	0.750
주관적 규범	SN 1 SN 2 SN 3	0.934	0.905	0.759
자기효능감	SE 1 SE 3 SE 4	0.947	0.926	0.807
준수의도	CI 1 CI 2 CI 3	0.961	0.948	0.859

성 및 타당성을 분석한다(Table 2).

신뢰성 분석은 SPSS 21.0을 적용하였으며, 탐색적 요인분석과 크론바흐 알파 분석을 통해 확인한다. 연구 모델에 적용된 9개 요인은 총 28개의 항목으로 구성되어 있다. 탐색적 요인분석 결과 항목간에 문제를 보인 2개 항목(GS3, SE2)을 제외한 9개 요인(26개 항목)에 대한 크론바흐 알파 분석을 실시하였으며, 모든 요인들은 선행 연구가 요구한 0.7 이상을 만족하였다[28].

타당성 분석은 AMOS 22.0을 적용하여 확인적 요인분석을 실시하고, 요인 내 문항간의 일치성(집중 타당성)과 요인간의 차별성(판별 타당성)을 확인한다. 확인적 요인분석 관련 구조 모델에 대한 적합성을 파악한 결과는 χ^2/df = 1.526, GFI = 0.916, AGFI = 0.888, CFI = 0.984, NFI = 0.954, RMSEA = 0.041과 같이 나타났다. 즉, 결과는 구조 모델에 대한 적합성 요구사항보다 높은 것으로 나타나[29], 집중타당성과 판별타당성 분석을 하였다. 집중 타당성은 개념신뢰도(0.7 이상 요구)와 평균분산추출(0.5 이상 요구)을 적용한다[30]. 개념신뢰도와 평균분산추출 확인 결과 집중 타당성 요구사항보다 높은 것으로 나타났다(Table 2).

또한, 연구는 판별타당성 분석을 실시하였다.

Table 3. Result for Discriminant Validity

변수	1	2	3	4	5	6	7	8	9
애착	***0.77***	·	·	·	·	·	·	·	·
몰입	.54**	***0.83***	·	·	·	·	·	·	·
관여	.59**	.53**	***0.78***	·	·	·	·	·	·
목표 난이도	.54**	.53**	.66**	***0.86***	·	·	·	·	·
목표 구체성	.58**	.56**	.70**	.67**	***0.87***	·	·	·	·
태도	.63**	.59**	.62**	.54**	.56**	***0.87***	·	·	·
주관적 규범	.53**	.37**	.54**	.53**	.50**	.52**	***0.87***	·	·
자기효능감	.71**	.56**	.65**	.59**	.64**	.65**	.55**	***0.89***	·
준수의도	.61**	.43**	.62**	.55**	.56**	.65**	.54**	.64**	***0.92***

Note: 볼드체는 AVE의 제곱근
**: p 〈 0.01

판별타당성은 평균분산추출 값과 적용 요인의 상관계수 값을 비교하여 확인한다. 선행연구는 평균분산추출의 제곱근이 전체 상관계수 값보다 크면 판별타당성이 존재한다고 판단한다[30]. 분석 결과는 판별타당성을 확보한 것으로 나타났다(Table 3).

다만, 상관계수 분석 결과 요인간의 상관계수가 다소 높은 것으로 나타나 다중공선성 분석을 실시하였다. 다중공선성은 SPSS 21.0의 VIP를 통해 확인하였으며, 결과 변수인 정보보안 준수의도에 대하여 선행 요인들의 다중공선성을 확인한 결과 애착(2.393), 몰입(1.863), 관여(2.816), 목표 난이도(2.248), 목표구체성(2.721), 태도(2.332), 주관적 규범(1.712), 자기효능감(2.727)로 나타나 다중공선성 문제는 낮은 것으로 판단되었다.

4.2 구조 모형 평가

연구 모델에 대한 구조모형 평가는 3단계로 진행한다. 첫째, 구조 모델의 적합성을 분석한다. 둘째, 연구 가설간의 경로 분석(β)을 통해 가설 검증을 실시한다. 셋째, 선행 변수의 결과변수에 미치는 영향력 검증(R^2)을 실시한다.

첫째, 연구 모델의 적합성 분석을 실시하였다. 분석 결과 적합성은 x^2/df = 2.494, GFI = 0.886, AGFI = 0.856, CFI = 0.962, NFI = 0.932, RMSEA = 0.060와 같이 나타났다. 비록 GFI가 요구사항보다 조금 낮고, RMSEA가 요구사항보다 조금 높으나, 정보 기술 분야에서 충분히 적용되는 수준으로 판단되고, 종합적으로 판단하는 구조방정식 모델링의 특성을 감안하여 분석을 계속 진행하였다.

둘째, 연구가설의 경로분석(β)을 실시하였다. 가설 검증 결과는 Fig. 2, Table 4와 같다. 연구가설 1은 태도가 정보보안 준수의도에 긍정적 영향을 미친다는 것으로서, 경로 분석 결과는 통계적으로 유의하였다(H1: β= 0.394, p<0.01). 연구가설 2는 주관적 규범이 정보보안 준수의도에 긍정적 영향을 미친다는 것으로서, 경로 분석 결과는 통계적으로 유의하였다(H2: β= 0.378, p<0.01). 연구가설 3은 자기효능감이 정보보안 준수의도에 긍정적 영향을 미친다는 것으로서, 경로 분석 결과는 통계적으로 유의하였다(H3: β= 0.185, p<0.01). 연구가설 4는 정보보안 애착이 태도에 긍정적 영향을 미친다는 것으로서, 경로 분석 결과는 통계적으로 유의하였다(H4: β= 0.282, p<0.01). 연구가설 5는 정보보안 몰입이 태도에 긍정적 영향을 미친다는 것으로서, 경로 분석 결과는 통계적으로 유의하였다(H5: β= 0.247, p<0.01). 연구가설 6은 정보보안 관여가 태도에 긍정적 영향을 미친다는 것으로서, 경로 분석 결과는 통계적으로 유의하였다(H5: β= 0.247, p<0.01). 연구가설 7은 정보보안 정책 목표 난이도가 자기효능감에 긍정적 영향을 미친다는 것으로서, 경로 분석 결과는 통계적으로 유의하였다(H7: β= 0.402, p<0.01). 그리고, 연구가설 8은 정보보안 정책 목표 구체성이 자기효능감에 긍정적 영향을 미친다는 것으로서, 경로 분석 결과는 통계적으로 유의하였다(H8: β= 0.383, p<0.01).

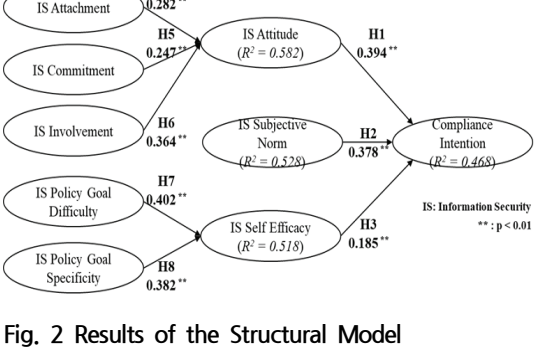

Fig. 2 Results of the Structural Model

Table 4. Summary of Hypothesis Tests

	경로	경로계수	t-값	결과
H 1	태도 → 준수의도	0.394	7.576**	채택
H 2	주관적규범 → 준수의도	0.378	7.339**	채택
H 3	자기효능감 → 준수의도	0.185	4.100**	채택
H 4	애착 → 태도	0.282	4.748**	채택
H 5	몰입 → 태도	0.247	4.251**	채택
H 6	관여→ 태도	0.364	5.968**	채택
H 7	목표난이도 → 자기효능감	0.402	5.975**	채택
H 8	목표구체성 → 자기효능감	0.383	5.76**	채택

** $p < 0.01$

마지막으로, 선행변수의 결과변수에 대한 영향력 검증(R^2)을 하였다. 태도, 주관적 규범, 자기효능감은 준수의도에 46.8%의 영향을 가지는 것으로 나타났으며, 애착, 몰입, 관여는 태도에 58.2%의 영향을 가지는 것으로 나타났다. 마지막으로 목표 난이도와 목표 구체성은 자기효능감에 51.8%의 영향을 가지는 것으로 나타났다.

5. 결 론

코로나 19라는 바이러스의 침입은 전 세계적으로 개인 및 조직에게 사람 간의 연계를 최소화하도록 요구하고 있다. 이에 대한 대처로서 많은 조직은 재택근무 및 온라인 기반의 업무를 추진하고 있다. 하지만, 구성원의 정보시스템에 대한 접근 방식의 다양성과 정보 접근 권한의 약화는 내부의 정보보안 위협을 높일 수 있어, 내부자들의 정보보안 준수 수준 향상을 위한 노력이 더욱 필요한 시점이다. 본 연구는 인간의 행동 예측력에 대한 설명력이 높은 계획된 행동이론을 정보보안에 적용하고, 정보보안 준수의도에 영향을 주는 구성요소인 태도와 자기효능감을 높이기 위한 선행 조건을 제시하는 것에 초점을 두었으며, 사회통제이론을 정보보안 분야에 적용하여 정보보안 태도에 미치는 영향을 살펴보고, 목표설정이론을 정보보안 분야에 적용하여, 조직이 구축한 정보보안 정책에 대한 목표설정이 개인의 자기효능감에 미치는 영향을 살펴보았다.

본 연구가 가지는 학술적 시사점은 다음과 같다. 첫째, 본 연구는 개인의 행동의도 또는 행동에 대한 대표적인 예측 모델인 계획된 행동이론을 접목하여, 개인의 준수의도를 높이는 선행요인을 재확인하였다. 세부적으로, 정보보안 태도, 정보보안 주관적 규범, 그리고 정보보안 자기효능감이 정보보안 준수의도에 미치는 긍정적 영향을 확인하였으며(R^2 = 46.8%), 모든 구성요인이 개인의 준수 행동의 선행 요인인 준수의도에 긍정적 영향을 미치는 것을 확인하였다. 즉, 연구는 학술적 관점에서 조직 구성원의 정보보안 준수 행동에 영향을 주는 요인을 계획된 행동이론의 세부 요인을 적용하여 확인하였다는 측면에서 시사점을 가진다.

둘째, 본 연구는 개인의 정보보안 태도 형성을 위해 필요한 선제 조건을 사회통제이론을 접목하여 연관 관계를 확인하였다. 사회통제이론은 개인과 집단 간의 관계에서 집단이 요구하는 관습, 또는 특정한 행동에 대한 긍정적 또는 부정적 행동 원인을 설명하는 대표적인 이론으로서, 본 연구는

개인의 정보보안 애착, 정보보안 몰입, 그리고 정보보안 관여가 높아질 때, 정보보안에 대한 호의성의 개념인 태도를 형성하여(R^2 = 58.2%), 긍정적인 정보보안 준수의도를 보이는 것을 확인하였다. 즉, 연구는 학술적 관점에서 사회학, 교육학 등에서 적용되던 사회통제이론을 정보보안 분야에 적용하여, 개인의 정보보안 태도에 영향을 주는 선행요인임을 제시하였다는 측면에서 시사점을 가진다.

마지막으로, 본 연구는 정보보안을 통제할 수 있다고 판단하는 개념인 자기효능감 형성에 필요한 선행 요인을 목표설정이론을 접목하여 제시하였으며, 연관 관계를 확인하였다. 목표설정이론은 합리적인 의사결정 역량을 기본가정으로 특정 목표를 어떻게 제시하고 받아들일 때보다 높은 수준의 성과를 도출할 수 있는지에 대한 관점의 이론으로서, 목표가 지금보다 달성하기 어려운 난이도로 구성되어 있고, 단계별 구체적으로 이행할 수 있을 때 성과로 이어진다는 개념이다. 본 연구는 정보보안 정책에 대한 목표를 제시하고, 개인이 받아들일 때, 자기효능감을 형성시켜(R^2 = 51.8%), 긍정적인 정보보안 준수의도로 나타나는 것을 확인하였다. 즉, 연구는 학술적 관점에서 계획된 행동이론 중 자기효능감 수준을 높이는 선행요인으로 목표설정이론을 적용하여 높은 긍정적 영향 관계를 확인하였다는 측면에서 시사점을 가진다.

본 연구의 실무적 시사점은 다음과 같다.

첫째, 본 연구는 구성원의 정보보안 준수는 조직이 무작정 요구한다고 해서 행동으로 이어지는 것이 아니라, 본인의 행동에 대한 타당성을 확립했을 때 가능하다는 관점에서, 계획된 행동이론을 정보보안에 적용하였다. 특히, 자신의 경험을 통해 확보한 정보보안에 대한 호의적인 믿음인 태도의 형성, 조직의 정보보안 문화에 내재하고자 하는 믿음인 주관적 규범의 형성, 그리고 정보보안 문제 등에 스스로 대처하고 통제할 수 있다고 판단하는 자기효능감이 복합적으로 형성될 때, 스스로 정보보안 준수의지를 가지고 행동으로 이어지는 것을 확인하였다. 따라서, 조직은 구성원이 정보보안에 대한 좋은 경험과 호의성을 가질 수 있도록 하고, 정보보안에 대한 조직 차원의 문화 형성을 통해 구성원이 조직 일체감을 가지고 행동할 수 있도록 환경을 구축하고, 스스로 통제할 수 있도록 관련 정보를 제공하는 것이 필요하다. 즉, 연구는 실무적 관점에서 조직 구성원의 정보보안 준수의도를 높이는 선행 조건을 제시하고 방향을 제시하였다는 측면에서 시사점을 가진다.

둘째, 본 연구는 개인의 정보보안에 대한 호의성의 개념인 태도를 형성에 필요한 선제 조건을 제시하였다. 조직과 개인간의 유대감이 태도 형성에 중요한 선행 조건이라고 한 사회통제이론을 접목하여, 정보보안 애착, 몰입, 그리고 관여가 태도를 높이는 조건임을 제시하고 결과를 확인하였다. 따라서, 조직은 구성원이 조직 또는 조직이 추구하는 보안 활동과 같은 특정한 행동 방향에 있어, 애착을 가질 수 있도록 관련 정보를 제공하고, 몰입을 할 수 있는 시간적 여유를 제공하고, 정보보안 정책 개발 및 운영에 있어서 구성원들의 참여를 자연스럽게 유도하는 활동을 하는 것이 필요하다. 즉, 연구는 실무적 관점에서 준수의도를 높이는 태도 형성에 영향을 주는 조건을 제시하고 조직이 추구해야 할 방향을 제시하였다는 측면에서 시사점을 가진다.

마지막으로, 본 연구는 개인이 정보보안 관련 행동을 하는데 중요한 행동 통제에 대한 인식 수준인 자기효능감을 형성시키기 위한 조건을 제시하였다. 특히 정보보안 정책에 대한 목표설정 방식에 따라, 개인이 받아들이는 정보의 수준, 그리고 합리적 판단 방식이 달라진다는 목표설정이론의 자기효능감에 대한 영향 관계를 정보보안 분야

에 접목시켰다. 따라서, 조직은 정보보안 정책에 대한 목표를 조직원이 달성하기 어려운 수준으로 상향하되, 조금씩 달성할 수 있는 단계적, 구체적인 목표를 제시하고 구성원들이 이해할 수 있도록 지원하는 것이 필요하다. 즉, 연구는 실무적 관점에서 조직 차원의 정보보안 목표 선언과 지원이 개인의 준수행동에 미치는 영향을 확인하고 방향성을 제시하였다는 측면에서 시사점을 가진다.

하지만, 연구는 연구 범위 및 방식에 따른 한계점을 가지고 있으며, 향후 연구에서는 보완될 필요가 있다. 첫째, 본 연구는 계획된 행동이론, 사회통제이론, 그리고 목표설정이론을 접목하고 설문을 통해 영향 관계를 확인하였다. 하지만, 조직 관점 요인인 정보보안 정책 목표의 수준은 실제 상황과 개인의 인식 상황의 차이가 발생할 수 있다는 한계가 있다. 즉, 보다 객관적 관점의 보안 정책 구축 수준을 확인하는 것이 필요하다. 보안 관련 인증 확보 수준별 집단 간 분석과 정보보안 정책 구축 수준별 구성원의 목표에 대한 인식의 차이를 확인한다면, 현실적 시사점을 제시할 것으로 판단한다. 더불어, 산업 또는 조직 특성별 사이버 보안 지원 체계 및 행동 프레임워크를 명료하게 제시할 필요가 있다. 최근 공학 분야를 중심으로 정보보안 구성 체계 관련 프레임워크를 제시함으로써, 조직이 활용가능한 체계를 제시하고 있다[31]. 본 연구는 정보보안 관련 행동 체계를 제시하였기 때문에, 조직 내 구성원들의 행동 관련 적용 가능 프레임워크를 제시한다면 조직에 현실적으로 적용가능한 결과를 확보할 것으로 판단한다. 둘째, 연구는 개인의 정보보안 행동의도의 예측력 향상을 위한 방향을 이론간의 접목을 통해 도출하였으나, 개인차에 의한 행동의 차이는 고려하지 않았다. 즉, 문제에 대한 개인의 대처 방식에 대한 차이는 개인의 행동 원인을 연구하는 많은 선행연구들이 접근하는 주제로서, 향후 조직 구성원의 실질적 보안 행동수준 향상을 위해 개인차를 구분하고 영향 관계를 확인한다면 높은 현실적 시사점을 제시할 것이다.

참고문헌

[1] Verizon, Analyzing the COVID-19 data breach landscape, (2020).

[2] K. D. Loch, H. H. Carr, and M. E. Warkentin, “Threats to information systems: Today’s reality, yesterday’s understanding,” MIS Quarterly, vol. 16, no. 2, pp. 173-186, (1992).

[3] 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).

[4] H. L. Chou, and C. Chou, “An analysis of multiple factors relating to teachers’ problematic information security behavior,” Computers in Human Behavior, vol. 65, pp. 334-345, (2016).

[5] C. Posey, T. L. Roberts, and P. B. Lowry, “The impact of organizational commitment on insiders’ motivation to protect organizational information assets,” Journal of Management Information Systems, vol. 32, no. 4, pp. 179-214, (2015).

[6] J. Y. Son, “Out of fear or desire? Toward a better understanding of employees’ motivation to follow IS security policies,” Information & Management, vol. 48, no. 7, pp. 296-302, (2011).

[7] J. Cox, “Information systems user security: A structured model of the knowing–doing gap,” Computers in Human Behavior, vol. 28, no. 5, pp. 1849-1858, (2012).

[8] W. R. Flores, and M. Ekstedt, “Shaping intention to resist social engineering through transformational leadership, information security culture and awareness,” Computers & Security,

vol. 59, pp. 26-44, (2016).
[9] I. Hwang, and S. Hu, "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, vol. 16, no. 3, pp. 225-236, (2018).
[10] J. Zhang, B. J. Reithel, and H. Li, "Impact of perceived technical protection on security behaviors," Information Management & Computer Security, vol. 17, no. 4, pp. 330-340, (2009).
[11] Verizon, 2020 data breach investigations report, (2020).
[12] M. Siponen, S. Pahnila, and M. A. Mahmood, "Compliance with information security policies: An empirical investigation," Computer, vol. 43, no. 2, pp. 64-71, (2010).
[13] N. S. Safa, C. Maple, T. Watson, and R. Von Solms, "Motivation and opportunity based model to reduce information security insider threats in organisations," Journal of Information Security and Applications, vol. 40, pp. 247-257, (2018).
[14] 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).
[15] N. S. Safa, and R. Von Solms, "An information security knowledge sharing model in organizations," Computers in Human Behavior, vol. 57, pp. 442-451, (2016).
[16] I. Ajzen, "The theory of planned behavior," Organizational Behavior and Human Decision Processes, vol. 50, no. 2, pp. 179-211, (1991).
[17] A. C. Johnston, and M. Warkentin, "Fear appeals and information security behaviors: An empirical study," MIS Quarterly, vol. 34, no. 3, pp. 549-566, (2010).
[18] T. Hirschi, Causes of delinquency, University of California Press, (1969).
[19] G. B. Magklaras, and S. M. Furnell, "A preliminary model of end user sophistication for insider threat prediction in IT systems," Computers & Security, vol. 24, no. 5, pp. 371-380. (2005).
[20] G. S. Mesch, "Social bonds and Internet pornographic exposure among adolescents," Journal of Adolescence, vol. 32, no. 3, pp. 601-618, (2009).
[21] L. Cheng, Y. Li, W. Li, E. Holm, and Q. Zhai, "Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory," Computers & Security, vol. 39, pp. 447-459, (2013).
[22] S. M. Lee, S. G. Lee, and S. Yoo, "An integrative model of computer abuse based on social control and general deterrence theories," Information & Management, vol. 41, no. 6, pp. 707-718, (2004).
[23] E. A. Locke, and G. P. Latham, "New directions in goal setting theory," Current Directions in Psychological Science, vol. 15, no. 5, pp. 265–268, (2006).
[24] 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).
[25] R. Vollmeyer, B. D. Burns, and K. J. Holyoak, "The impact of goal specificity on strategy use and the acquisition of problem structure," Cognitive Science, vol. 20, no. 1, pp. 75-100, (1996).
[26] P. B. Lowry, C. Posey, R. B. J. Bennett, and T. L. Roberts, "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, vol. 25, no. 3, pp. 193-273, (2015).
[27] E. A. Locke, and G. P. Latham, "Work

motivation and satisfaction: Light at the end of the tunnel," Psychological Science, vol. 1, no. 4, pp. 240-246, (1990).
[28] J. C. Nunnally, Psychometric theory (2nd ed.). New York: McGraw-Hill, (1978).
[29] 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).
[30] 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).
[31] 김성민, 정혜선, 이용우, "프레임워크 기반 스마트시티 사이버 보안 메트릭스," 한국산업융합학회 논문집, 제23권, 제2호, pp. 333-341, (2020).

(접수: 2021.05.06. 수정: 2021.05.23. 게재확정: 2021.06.04.)