

정보보안 정책준수에 대한 메타분석: 계획된 행동이론을 중심으로

김종기¹, 모건^{2*}

¹부산대학교 경영학과 교수, ²부산대학교 경영학과 조교수

Meta-analysis of Information Security Policy Compliance Based on Theory of Planned Behavior

Jongki Kim¹, Jian Mou^{2*}

¹Professor, Dept. of Business Administration, Pusan National University

²Assistant Professor, Dept. of Business Administration, Pusan National University

요약 정보기술의 발전에 따라 정보보안의 중요성이 갈수록 커지고 있다. 정보보안의 근본적인 방향을 제시하고 조직 구성원이 따라야 하는 규정과 지침을 다루는 보안정책은 보안관리의 핵심적인 요소이며, 조직 구성원의 보안정책 준수에 영향을 미치는 다양한 요인에 대한 연구들이 다수 수행되었다. 이들 연구는 다양한 이론적 기반으로 수행되었으며, 여러 문헌연구에 따르면 계획된 행동이론이 가장 빈번하게 사용되었다. 본 연구는 기존의 다양한 연구결과를 정량적으로 종합하는 메타분석 기법 중의 하나인 TSSEM을 적용하여 정보보안 정책준수 행동에 영향을 미치는 요인을 계획된 행동이론을 기반으로 실증분석한 연구들을 대상으로 분석하였다. 분석결과 계획된 행동이론의 행동의도를 설명하는 세 가지 요인인 태도, 주관적 규범 및 인지된 행동통제 모두 유의한 영향을 미쳤으며, 구조방정식 모형의 전반적인 적합도도 만족스럽게 나타났다.

주제어 : 보안정책, 정책준수, 계획된 행동이론, 메타분석, TSSEM

Abstract With widespread use of information technologies the importance of information security has been heightened. Security policies which deal with fundamental direction of information security are critical elements of information security management. Numerous studies have been conducted on users' intention to comply security policies. They were based on various theoretical foundations and the theory of planned behavior(TPB) was the most frequently used. This research employed one of the quantitatively synthesizing meta-analytic techniques called Two-Stage Structural Equation Modeling to investigate factors influencing information security policy compliance behavior based on TPB. Analysis results indicated that all three factors of TPB were significantly influencing the behavioral intention. Moreover, the overall fit indices of structural model exhibited satisfactory level.

Key Words : Security Policy, Policy Compliance, Theory of Planned Behavior, Meta-Analysis, TSSEM

*This work was supported by a 2-Year Research Grant of Pusan National University.

*Corresponding Author : Jian Mou(jian.mou@pusan.ac.kr)

Received October 6, 2020

Revised October 22, 2020

Accepted November 20, 2020

Published November 28, 2020

1. 서론

정보시스템에 대한 의존도가 갈수록 커지면서 정보보안은 조직에서 가장 중요한 활동 중의 하나로 간주된다. 해커나 자연재해와 같은 외부요인은 기업의 정보자원에 대한 중대한 보안위협이기는 하나 내부직원의 보안상 위협한 행동이 보다 더 큰 위협으로 간주된다[1]. 다수의 연구에 따르면 보안사고의 50% 이상이 내부직원의 고의나 실수로 인하여 발생한다고 일관되게 보고되고 있다[2].

정보보안정책은 내부자와 관련된 위협을 다루는 근본적인 접근법으로서, 보안사고의 예방과 탐지 및 대응을 위하여 정보자원 사용자의 책임과 역할을 명시한다[3]. 조직 구성원의 정보보안 정책준수는 조직의 보안을 유지하기 위한 가장 핵심적인 행동이다. 이에 따라 정보보안 정책준수 행위에 영향을 미치는 요인을 설명하는 많은 연구들이 수행되었다.

이들 연구는 다양한 이론적 기반을 두고 있는데, 그 중에서 억제이론(Deterrence Theory; DT), 보호동기이론(Protection Motivation Theory; PMT), 기술수용모형(Technology Acceptance Theory; TAM), 그리고 합리적 행동이론(Theory of Reasoned Action; TRA)과 이의 확장인 계획된 행동이론(Theory of Planned Behavior; TPB) 등이 빈번하게 적용되었다[2-6]. 본 연구는 이들 이론 중에서 가장 자주 적용된 이론인 TRA/TPB 기반의 실증연구를 대상으로 정보보안 정책준수에 대한 메타분석을 수행한다. 메타분석은 다양한 연구결과들을 통합하는데 유용한 정량적인 분석기법이다.

보안정책에 대한 기존 연구의 대부분은 Cram et al.[3]과 같이 대체로 서술적 분석에 그치거나, 계량적 분석을 시도한 경우라도 Cram et al.[6]과 같이 각각의 상관관계나 경로계수 또는 회귀계수와 같은 개별 효과크기에 대한 메타분석에 머무르고 있다. 본 연구는 개별 경로계수의 유의성을 평가할 수 있을 뿐만 아니라 연구모형 전체의 적합성을 분석할 수 있는 구조방정식 모형을 이용하여 메타분석을 수행하는 TSSEM (Two-Stage Structural Equation Modeling) 기법[7]을 적용하여 TPB 기반의 정보보안정책 준수행동에 관한 연구들을 대상으로 메타분석을 수행한다.

2. 계획된 행동 이론과 정보보안 정책준수

2.1 계획된 행동 이론

TV 시청, 선거 투표, 헌혈 등 사람이 행하는 대부분의 행위는 그러한 행위를 하기 원하는 경우에 쉽게 수행할 수 있다. 인간의 행동을 이해하기 위해서는 의도를 결정하는 요인을 식별할 필요가 있는데, TRA는 사람의 의도는 개인적인 요인과 사회적 영향의 두 가지 요인에 의해서 결정된다고 주장한다. 개인적 요인은 어떤 행위의 수행에 대한 개인의 긍정적인 또는 부정적인 평가이며, 이 요인을 행동에 대한 태도(attitude)라고 부른다. 두 번째 요인은 어떤 행동의 수행 여부에 대한 사회적 압력의 인식이며, 이를 주관적 규범(subjective norm)이라고 한다[8]. TRA는 인간이 분별 있게 행동한다는 가정을 전제로 하며, 획득 가능한 정보를 기반으로 명시적으로나 묵시적으로 그들의 행동이 미치는 영향을 고려한다.

TPB는 TRA와 더불어 인간의 사회적 행동을 예측하는 사회인지이론 중에서 대표적인 모형으로서 가장 빈번하게 언급되고 가장 광범위하게 적용되고 있는 모형이다[9]. TPB는 단순하고 간결하며 적용하기가 쉬우며 다양한 영역에 적용 가능하다. 안전벨트 착용, 도덕적 행동, 치과치료, 대학의 수업출석, 학업 성취도, 체중감량 등과 같은 다양한 분야에서 의도와 행동의 예측에 성공적으로 적용되었다[10]. TPB는 다음의 Fig. 1과 같이 구성된다.

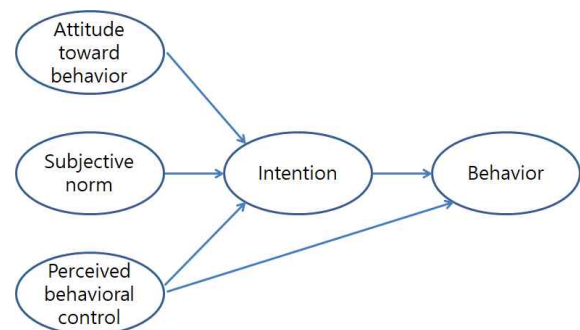


Fig. 1. Theory of Planned Behavior

TPB는 Fishbein & Ajzen[8]의 TRA를 확장한 이론이며, 행동에 대한 불완전한 자발적 통제(volitional control)라는 한계를 다루기 위해 고안되었다[11]. TRA와 같이 TPB의 중심요인은 특정한 행위를 수행하는 개인의 의도이다. 의도는 행동에 영향을 미치는 동기적 요인이며, 그러한 행동을 수행하기 위하여 사람들이 얼마나 열심히 시도할 의사가 있는지를 나타낸다. 일반적으로 행동을 수행할 의도가 강할수록 그 행동의 성과를 거둘 가능성이 크다. 그러나 TRA는 행동이 자의적인 통제에 있을 경우에만 행동의도가 행동으로 이어진다고 본다[9].

행동 의도는 어떤 행동을 시도하고자 하는 의도로 해석되는데, 의도된 행동의 성공적인 수행은 그것을 방해하는 다양한 요인에 대한 통제에 달려 있다. 엄밀하게 보면, 의도는 실제 행동이 아니라 행동을 수행하고자 하는 시도를 예측할 뿐이다. 따라서 정확하게 예측하기 위해서는 의도를 평가해야 할 뿐만 아니라 그러한 행동에 대한 통제를 얼마나 행사할 수 있는지에 대하여 추정할 필요도 있다[12]. 이러한 인지된 행동 통제(perceived behavioral control)에 대한 관점은 Bandura[13]의 인지된 자기효능감(perceived self-efficacy) 개념과 매우 유사하다[11].

의도가 행동을 예측하는지 여부는 부분적으로 개인의 통제를 넘어서는 요인들에 달려있다. 즉, 의도와 행동의 관계의 강도는 행동에 대한 실제 통제에 의해 조절된다. 방법론적인 문제를 제외한다면 의도와 행동 사이의 낮은 관련성은 합리적 행동의 한계를 보여주는 하나의 징표이다[9].

2.2 정보보안 정책준수

정보보안 정책은 조직 구성원이 조직의 정보보안 목표를 달성하기 위하여 준수해야 하는 원칙, 규정과 지침을 포함한다. 정보보안 정책의 목적은 정보보안에 대한 관리의 지향점이 무엇인지를 설명하는데 있으며, 정보자원의 허용되는 사용방법, 정보보안의 책임과 의무, 정보보안 정책위반에 대한 처벌, 다양한 유형의 직원들이 이수해야 하는 교육훈련 등을 포함한다[4].

정보보안정책이 매우 광범위한 수준으로 작성되기 때문에 일반적으로 표준, 지침, 절차 등으로 세분화되어 개발된다. 시스템을 보다 안전하게 사용하도록 기술과 방법을 표준과 지침으로 구체화한다. 절차는 보안 관련한 업무를 수행하기 위하여 준수해야 하는 더욱 세밀한 단계를 지칭한다. 다양한 유형의 정책을 프로그램 정책, 주제 중심 정책, 그리고 시스템 중심 정책으로 구분할 수 있다[14].

프로그램 정책은 보안에 대한 전략적 방향을 설정하고 보안전략의 구현을 위하여 자원을 할당함으로써 조직의 정보보안 프로그램을 구현하는 역할을 한다. 주제 중심 정책은 인터넷 접근, 이메일 프라이버시, 자가 기기 사용, 소셜 미디어 등과 같이 현재의 관심사항에 대한 구체적인 지침을 제공한다. 시스템 중심 정책은 특정 시스템을 어떻게 사용할 지에 대한 정보와 지침을 제공한다.

정보시스템 보안에 관련된 연구 중에서 조직 차원의

보안정책의 형성, 구현 및 효과에 대한 상당한 연구가 진행되었다. 보안정책 관련 연구의 분류와 더불어 Guo[15], Karlsson et al.[16], Lebek et al.[5] 등과 같이 정보보안에 대한 인식, 문화와 보안정책에 대한 준수와 같은 보다 세부적인 주제를 다루는 문헌연구들이 수행되었다. 특히, 직원의 정보보안정책 준수와 관련하여 정책준수 행동의 분류[15], 이의 선행요인에 대한 메타분석[4], 방법론 및 연구주제에 대한 논의[1]와 같은 연구가 수행되는 등 학계의 많은 관심을 끄는 주제가 되었다.

Cram et al.[3]은 34개 학술지에서 총 114편의 보안정책 관련 논문을 체계적인 문헌검토를 통하여 선별하였다. 이들 연구를 기반으로 10개의 고유한 연구개념과 이들 사이의 다섯 가지의 핵심적인 관계를 도출하였으며, 기존 연구들이 다루지 못한 이슈들을 고려하여 향후 연구를 위한 연구 프레임워크를 제시하였다.

3. 계획된 행동이론과 정보보안 정책준수에 대한 메타분석 선행연구

3.1 체계적 문헌 분석과 메타분석

연구분야를 불문하고 시간이 흐름에 따라 연구들이 축적되면서 상이한 연구결과를 종합적으로 분석할 필요가 있다. 1990년대 이전에 주로 사용되었던 서술적 분석(narrative review)에는 편의적 표본추출, 연구에 대한 서술적 설명, 기술통계 등의 기법이 활용된다. 이 방법은 객관성과 투명성이 결여되어 있으며, 분석대상의 연구가 많아지면 연구결과를 종합하기가 어렵다는 문제점이 있다[17].

체계적 문헌 분석(systematic literature review)과 메타분석(meta-analysis)은 서술적 분석의 문제를 극복하기 위하여 사용되었으며, 기존의 연구결과를 체계적이고 종합적으로 분석하여 투명하고 재현가능한 결과를 얻을 수 있도록 고안되었다[17]. 체계적 문헌 분석은 정성적인 또는 정량적인 연구들을 정성적으로 종합하는 방법이라고 본다면 메타분석은 정량적인 연구결과들을 정량적으로 통합하는데 초점을 둔다[18]. 메타분석은 여러 연구결과를 종합하기 위하여 평균차이, 상관관계수, 승산비 등과 같은 효과크기(effect size)를 사용하는 통계적 방법이며, 개별 연구에 비하여 높은 정교성과 정확한 추정치를 가진다[19].

3.2 계획된 행동이론의 메타분석

TPB가 광범위한 영역에서 적용됨에 따라 이를 기반으로 한 많은 연구가 수행되었고, 이에 따라 다수의 메타분석 연구가 수행되었다. Armitage & Conner[20]는 TPB 이론에 기반한 실증연구 185편을 분석하여 TPB 이론을 구성하는 요인들의 영향력을 분석하였으며, Steinmetz et al.[21]은 TPB 이론을 기반으로 행동변화를 유발하기 위한 개입의 효과를 메타분석하기 위하여 82편의 연구를 분석하였다.

TPB 이론을 특정한 연구주제에 적용한 연구들을 메타분석한 연구도 있다. 예를 들어, 16편의 실증연구를 바탕으로 지속가능한 음식소비행동의 선행요인을 TPB 이론을 기반으로 메타분석을 수행한 연구[22], 모유수유 행동의 예측에 대한 10편의 연구를 대상으로 TPB 이론의 적용가능성과 효과성을 분석[23], 음주행동을 설명하는 TPB 기반의 연구 28편을 이용하여 TPB 모형의 변수들과 음주의도 및 음주행동과의 관계를 메타분석[24], TPB와 TAM을 결합한 연구모형을 근간으로 모바일 커머스 수용에 대한 53편의 논문을 메타분석한 연구[25] 등이 있다.

지식경영 분야에서 획득한 지식을 다른 사람에게 전파하는 지식공유 행동을 설명하기 위한 연구에서 TPB가 널리 활용되고 있다. Nguyen et al.[26]은 지식공유에 적용된 TPB 이론에 대한 메타분석을 수행하기 위하여 체계적 문헌검토를 통하여 26편의 연구를 선정하여 MASEM을 이용하여 분석하였다. 분석 결과 태도, 인지된 행동통제 및 주관적 규범의 순으로 행동의도에 대하여 영향을 미치는 것으로 나타났으며, 집단주의적 문화, 1인당 GDP로 측정된 경제규모 그리고 정보기술 지원과 같은 조절변수를 확인하였다.

Lebek et al.[5]은 직원의 정보시스템 보안 행위를 설명하는데 사용된 이론을 조사하기 위하여 체계적인 문헌검토를 수행하여 113편의 논문을 선정하였으며, 이를 바탕으로 54개의 이론을 식별하였다. 다양한 이론들 중에서 TRA/TPB에 기반한 연구가 27편(23.9%), GDT가 17편(15.1%), PMT가 10편(8.9%), TAM이 7편(6.2%)의 순으로 적용되었다.

3.3 정보보안 정책준수에 대한 메타분석

Balozian & Leidner[2]는 상위 25개의 정보시스템 학술지에 게재된 67편의 정보시스템 보안정책 준수에 관련된 논문을 분석하였는데, GDT에 기반한 연구가 32%

로 가장 많았고, TPB가 18%, TRA가 18%, PMT가 14%를 차지하였다. TPB가 TRA의 확장이라는 관점에서 보면 TPB/TRA 이론 기반의 연구가 정보보안 정책준수 행동을 설명하는데 가장 널리 사용되고 있음을 알 수 있다.

정보보안 분야에서 Sommestad et al.[4]은 정보보안 정책준수에 영향을 미치는 요인을 찾기 위하여 체계적 문헌검토를 통하여 29개의 연구를 선정하였다. 분석 결과 61개의 변수가 식별되었는데, 40개의 변수는 하나의 연구에서만 사용되었다. 또한 정책준수 행위에 대한 각 변수의 설명력이 상당히 낮으며, 연구에 사용된 이론들 중에서도 충분한 설명력을 보이는 것은 없었다.

Cram et al.[6]은 정보보안 정책의 준수에 대한 선행요인을 메타분석하였다. 95편의 연구를 바탕으로 401개의 독립변수를 17개의 범주로 구분하고, 각 범주에 대하여 정보보안 정책준수와의 관계를 분석하였다. 이 연구에 포함된 선행연구들은 다양한 이론적 기반을 가지고 있는데, 그 중에서 TRA/TPB, DT, PMT의 순서로 가장 널리 사용되었다.

Moody et al.[27]은 정보보안 정책준수 행동을 설명하는 11개의 주요 이론과 27개의 연구개념을 검토하여 통합된 연구모형을 제안하고 실증적으로 분석하였다. Sommestad & Hallberg[28]는 TPB를 기반으로 한 정보보안 정책 준수에 대한 16편의 실증연구를 분석하여 TPB 이론의 설명력을 검증하고 다양한 연구결과를 합리적으로 설명할 수 있는 방안을 모색하였다.

Milicevic & Goeken[29]은 정보보안 정책의 준수에 대한 체계적 문헌검토를 통하여 354편의 논문을 선별하여 정책준수에 대한 행동의도에 영향을 미치는 요인들을 종합한 모형을 도출하였다. 이들 요인 중에서 TPB 모형을 구성하는 요인에 대하여 메타분석을 수행하여 인지된 행동통제와 태도 요인의 유의한 영향력을 확인하였으나 주관적 규범 요인은 행동의도에 대하여 전반적으로 유의하지 않다고 분석되었다.

4. 분석과 토의

4.1 데이터

일반적으로 구조방정식 모형의 분석에는 공분산 행렬의 사용을 선호하나, TASSEM을 포함하여 MASEM을 이용한 메타분석에서는 상관관계 행렬이 더 선호된다. 만약 메타분석 대상 연구들 간에 동일한 척도가 사용되었다면

공분산 행렬도 사용할 수 있다[30]. 본 연구에서는 Cram et al.[6]이 메타분석에서 사용한 연구 중에서 TRA/TPB를 기반으로 한 연구를 분석에 포함하였다.

Cram et al.[6]은 PRISMA(PREFERRED Reporting Items for Systematic reviews and Meta-Analyses) 가이드라인에 따라 자료를 수집하였다. 먼저, 자료의 탐색은 ABI/Inform, ACM Digital Library, Business Source Premier, 그리고 JSTOR와 같은 데이터베이스에서 “security policy,” “cybersecurity policy,” “information security policy,” “cybersecurity policy,” “information security policy,” “security compliance,” “security policy violation,” “security policy noncompliance,” “computer abuse,” “information systems misuse”와 같은 키워드로 검색하여 1,698편의 논문을 식별하였다.

출판편향을 최소화하기 위한 목적으로 학술대회 발표 논문을 연구에 포함하기 위하여 ICIS, AMCIS, ECIS 등을 포함하는 AIS 전자도서관을 검색하여 149편의 논문을 추가하였다. 또한, 학위논문을 검색하기 위하여 ProQuest 학위논문 데이터베이스에서 925편의 연구를 찾았다. 초기 검색된 논문 중에서 실증연구와 보안정책 준수를 종속변수로 사용한 연구, 메타분석을 수행하기 위한 충분한 통계자료가 포함된 논문이라는 기준을 적용하여 95편의 연구를 선별하였다.

그 중에서 모두 39편의 논문이 TRA/TPB에 기반한 것으로 분석되었다. 그러나, 그 중에서 D'Arcy & Lowry[31]의 연구에서는 상관관계 행렬이 보고되지 않았고, Lebek et al.[5]과 Shropshire et al.[32]의 연구모형에는 TRA나 TPB와 관련한 연구변수가 포함되어 있지 않아 제외되었다. 한편, Jenkins[33]는 두 개의 독립된 연구에서 세 개의 실험을 수행함에 따라 세 개의 상관관계 행렬 데이터가 본 연구에 포함되었다. 따라서, 모두 38개의 상관관계 행렬 데이터가 식별되었으며, 총 표본수는 10,626개이다.

일부 연구에서는 보안정책 준수와 상반되는 개념을 사용하기도 하였다. Chu et al.[34]에서는 오용 태도(misuse attitude)와 오용 의도(misuse intention)를 포함하고 있고, Guo et al.[35]은 악의적이지 않은 보안위반 의도(nonmalicious security violation intention)를 종속변수로 설정하였다. 위의 경우에 해당되는 연구변수의 상관관계를 역코딩(reverse coding)하여 분석에 사용하였다. Dugo[36]는 모든 변수를 정보보안 위반 행위(committing INFOSEC violation)에 대한 것으로 조

작적으로 정의하였고, Peace et al.[37]은 소프트웨어 불법복제 의도를 TPB 모형으로 설명하면서 종속변수인 불법복제 의도를 역척도(reversed scale)로 측정하였으므로 논문에 보고된 상관관계를 그대로 사용하였다.

4.2 데이터 분석 및 토의

본 연구에서는 Cheung and Chan[7]이 제안한 TSSEM을 적용하였다. TSSEM은 메타분석과 구조방정식 모형을 결합한 MASEM(Meta-Analytic Structural Equation Modeling)의 한 기법이다. MASEM을 분석하는 데는 OpenMx, Lisrel, Mplus, Lavaan 등 다양한 도구를 사용할 수 있는데, metaSEM이 TSSEM을 적용하는데 특히 유용하다[38]. metaSEM 패키지는 R 프로그래밍 언어 기반의 OpenMx 패키지를 근간으로 운영되며, TSSEM의 1단계 모형에서 자동적으로 변수 값, 표준편차 및 적합도지수의 추정을 고려함으로써 특히 유용하다[39].

TSSEM은 두 단계로 구분되어 수행되는데, 1단계에서는 통합된 상관관계 행렬(pooled correlation matrix)과 점근적 공분산 행렬(asymptotic covariance matrix)을 이용하여 메타분석에 포함된 연구들의 상관관계 행렬의 동질성(homogeneity)을 확인한다 [7]. 동질성이 있다면 2단계에서 고정효과모형(fixed effect model; FEM)을 이용하여 분석하고, 동질성이 없다고 판단되면 조절변수를 기준으로 동질성 있는 하위집단으로 나누어 분석하거나, 개별 연구 차원의 상관관계 계수의 분산을 고려하는 무선효과모형(random effect model; REM)을 적용한다[39].

1단계의 FEM 분석 결과 모든 상관관계 계수의 동질성 평가에 있어서 $\chi^2_{(166)}$ 값이 2183.19로서 p-값이 0.01보다 작으며, RMSEA 값이 0.2085로서 95% 신뢰구간이 0.2011에서 0.2167 사이에 있다. 동질성 분석에 있어서 RMSEA 값의 허용치는 0.08보다 작아야 한다[39]. 그 밖에 SRMR이 0.1762, TLI가 0.7157, CFI가 0.7256으로 전반적인 적합도 지표가 분석에 포함된 개별 연구들의 상관관계 계수의 동질성이 없는 것으로 나타났다.

무선효과 분석결과를 요약한 효과크기의 동질성에 대한 Q 통계치는 유의하게 나타났는데($Q_{(166)} = 1954.727$, $p < 0.01$), 이는 상관관계 행렬에 심각한 이질성이 있다는 것을 보여준다[40]. Table 1에 나타난 바와 같이 개별 상관관계 계수의 이질성 지표인 I^2 값이 0.89에서 0.95 사이에 있어 모든 상관관계 계수에 있어서 분산의 상당부분이 개별 연구 수준에 있음을 보여준다.

Table 1. Heterogeneity indices (based on the estimated Tau2)

Intercept1: I ² (Q statistic)	0.9440
Intercept2: I ² (Q statistic)	0.8964
Intercept3: I ² (Q statistic)	0.8933
Intercept4: I ² (Q statistic)	0.9207
Intercept5: I ² (Q statistic)	0.9508
Intercept6: I ² (Q statistic)	0.9459

TSSEM의 두 번째 단계에서는 구조모형을 분석하는데, metaSEM 패키지에서는 세 가지 유형의 행렬을 사용한다. 행렬 A는 구조모형의 회귀계수를 지정하며, 행렬 S는 분산과 공분산을, 그리고 행렬 F는 관찰변수와 잠재변수를 지정한다. 분석 결과 경로모형의 χ^2 는 유의하게 나타났다 ($\chi^2_{(3)} = 178.79, p < 0.01$). 그러나 RMSEA가 0.0743이며, 95% 신뢰구간은 0.0652와 0.0837로 나타났다으며, CFI가 0.8787임을 고려할 때 전반적인 구조모형의 적합도는 적절한 것으로 보인다. Table 2는 TPB 모형에서 각 경로의 추정치와 표준편차, 그리고 95% 신뢰구간과 z-값을 보여준다.

Table 2. Parameter estimates and 95% confidence intervals

Path	Estimate (Std.Err)	lbound	ubound	z-value
Attitude -> Intention	0.4741 (0.0285)	0.4183	0.5299	16.6594
Behavioral Control -> Intention	0.3472 (0.0448)	0.2594	0.4350	7.7492
Subjective Norm -> Intention	0.2803 (0.0442)	0.1937	0.3670	6.3381

메타분석 결과에 따르면 행동의도에 가장 영향을 많이 미치는 요인은 태도이며, 그 다음으로 행위통제이고, 주관적 규범이 가장 적은 영향을 미치는 것으로 나타났다. 이러한 본 연구의 분석결과는 TPB 이론을 바탕으로 지식공유에 대한 연구의 메타분석을 수행한 Nguyen et al.[26]의 연구결과와 일치하며, 이런 결과는 주관적 규범의 측정에 있어서 보다 정교한 조작적 정의와 타당성 높은 측정항목이 요구됨을 시사한다.

5. 결론

정보시스템을 기반으로 한 조직 운영이 보편화됨에 따

라 정보보안의 중요성이 더욱 커지고 있다. 조직 구성원의 정보보안정책 준수 여부는 효과적인 정보보안관리의 핵심요소이다. 정보보안정책에 대한 연구자들의 높은 관심은 방대한 연구결과로 이어지며, 그 중에서 다양한 이론적 기반을 바탕으로 보안정책의 준수에 영향을 미치는 요인들에 대한 많은 연구들이 실증분석을 수행하였다.

최근의 문헌검토 연구[2-6]에 따르면 여러 이론 중에서도 TRA/TPB 기반의 연구가 가장 빈번하게 수행되었다. 그러나 TRA/TPB가 매우 간단명료한 연구모형임에도 불구하고 다수의 연구에서 상이하거나 때로는 상충되는 분석결과가 도출되었다. 이에 따라 기존의 개별적인 연구결과들을 통합하여 분석하는 연구들이 수행되었다. 본 연구는 정보보안 정책준수에 대한 기존의 정성적인 분석이나 개별 효과크기에 대한 정량적인 메타분석에서 나아가 전체 연구모형의 전반적인 적합도를 평가할 수 있는 구조방정식모형을 메타분석에 접목한 MASEM 기법 중의 하나인 TSSEM을 적용하여 메타분석을 수행하였다.

Cram et al.[6]의 개별 효과크기에 대한 메타분석에서 사용한 데이터를 이용하여 분석한 결과 행동의도에 영향을 미치는 세 가지 요인, 즉 태도, 행위통제 및 주관적 규범 모두 유의한 영향을 미치는 것으로 나타났으며, 전반적인 모형 적합도도 만족스러운 수준이었다. 이러한 분석결과는 개별 요인의 유의성에 대한 이전의 연구결과와는 일치한다. 그러나 개별 효과크기를 대상으로 메타분석을 수행한 연구들에서 행동의도에 대한 개별 요인들의 전체 설명력이 부족하다는 관점[41]과는 다르다.

본 연구에서는 다음과 같은 한계와 이에 따른 향후 연구방향을 제안한다. 먼저, 본 연구의 분석에 포함된 36편의 연구 중에서 4편이 종속변수를 정책준수의도가 아닌 위반의도로 측정하였기 때문에 역코딩된 자료를 분석에 이용하였다. 긍정적인 행동과 부정적인 행동을 상반된 유형으로 간주하는 것은 매우 단순한 관점이며, 정책준수를 설명하는 요인이 정책위반을 설명할 수 있다고 볼 수 있는 근거가 충분하지 않다[15]. 대부분의 연구가 정책준수를 종속변수로 사용하고 있지만 향후 연구에서는 부정적인 행동과 긍정적인 행동을 구분하여 분석하거나 이를 조절변수로 적용하여 분석할 수 있을 것이다.

다음으로, 기존의 실증연구에서 한 가지 이론이 아니라 두세 가지 이론을 통합하여 적용한 경우가 많이 있었다. TRA/TPB 이외의 다른 요인들을 추가하여 메타분석을 수행할 수 있을 것이다. 또한, TRA/TPB 이외에 자주 적용된 이론인 DT, PMT, TAM 등을 각각 메타분석하여 비교할 수 있다.

REFERENCES

- [1] R. Willison & M. Warkentin. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly*, 37(1), 1-20. DOI: 10.25300/misq/2013/37.1.01
- [2] P. Balozian & D. Leidner. (2017). Review of IS Security Policy Compliance: Toward the Building Blocks of an IS Security Theory. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, 48(3), 11-43. DOI: 10.1145/3130515.3130518
- [3] W. A. Cram, J. G. Proudfoot, & J. D'Arcy. (2017). Organizational Information Security Policies: A Review and Research Framework. *European Journal of Information Systems*, 26(6), 605-641. DOI: 10.1057/s41303-017-0059-9
- [4] T. Sommestad, J. Hallberg, K. Lundholm & J. Bengtsson. (2014). Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies. *Information Management & Computer Security*, 22(1), 42-75. DOI: 10.1108/imcs-08-2012-0045
- [5] B. Lebek, J. Uffen, M. Neumann, B. Hohler & M. Breitenr. (2014). Information Security Awareness and Behavior: A Theory-based Literature Review. *Management Research Review*, 37(12), 1049-1092. DOI: 10.1108/mrr-04-2013-0085
- [6] W. A. Cram, J. D'Arcy & J. G. Proudfoot (2019). Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. *MIS Quarterly*, 43(2), 525-554. DOI: 10.24251/hicss.2017.489
- [7] M. W. L. Cheung & W. Chan. (2005). Meta-Analytic Structural Equation Modeling: A Two-Stage Approach. *Psychological methods*, 10(1), 40-64. DOI: 10.1037/1082-989x.10.1.40
- [8] M. Fishbein & I. Ajzen. (1975). *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley.
- [9] I. Ajzen. (2011). The Theory of Planned Behaviour: Reactions and Reflections. *Psychology and Health*, 26(9), 1113-1127. DOI: 10.1080/08870446.2011.613995
- [10] L. Leone, M. Perugini & A. P. Ercolani. (1999). A comparison of three models of attitude-behavior relationships in the studying behavior domain. *European Journal of Social Psychology*, 29(2-3), 161-189. DOI: 10.1002/(SICI)1099-0992(199903/05)29:2/33.0
- [11] I. Ajzen. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211. DOI: 10.1016/0749-5978(91)90020-t
- [12] I. Ajzen. (1985). From Intentions to Actions: A Theory of Planned Behavior. In *Action control from Cognition to Behavior*(pp. 11-39). Springer, Berlin, Heidelberg.
- [13] A. Bandura. (1977). Self-Efficacy: Toward a Unifying Theory of Behavioral Change. *Psychological Review*, 84(2), 191-215. DOI: 10.1037/0033-295x.84.2.191
- [14] M. Nieves, K. Dempsey & V. Pillitteri. (2017). *An Introduction to Information Security* (NIST Special Publication 800-12 Rev. 1). National Institute of Standards and Technology.
- [15] K. H. Guo. (2013). Security-Related Behavior in Using Information Systems in the Workplace: A Review and Synthesis. *Computers and Security*, 32, 242-251. DOI: 10.1016/j.cose.2012.10.003
- [16] F. Karlsson, J. Åström & M. Karlsson. (2015). Information Security Culture-State-of-the-Art Review between 2000 and 2013. *Information and Computer Security*, 23(3), 246-285. DOI: 10.1108/ICS-05-2014-0033
- [17] S. Hwang.(2015). *Meta-Analysis Using R*, Hakjisa.
- [18] K. Yeon. (2018). Meta-analysis of the effects of TPM activity factors on Corporate performance. *Journal of Digital Convergence*, 16(2), 151-156. DOI: 10.14400/JDC.2018.16.2.151
- [19] B. Cho & J. Lee. (2018). A Meta Analysis on Effects of Flipped Learning in Korea. *Journal of Digital Convergence*, 16(3), 59-73. DOI: 10.14400/JDC.2018.16.3.059
- [20] C. J. Armitage & M. Conner. (2001). Efficacy of the Theory of Planned Behaviour: A Meta-Analytic Review. *British journal of social psychology*, 40(4), 471-499. DOI: 10.1348/014466601164939
- [21] H. Steinmetz, M. Knappstein, I. Ajzen, P. Schmidt & R. Kabst. (2016). How Effective are Behavior Change Interventions Based on the Theory of Planned Behavior?: A Three-Level Meta-Analysis. *Zeitschrift für Psychologie*, 224(3), 216-233. DOI: 10.1027/2151-2604/a000255
- [22] Y. Han & H. Hansen. (2012). Determinants of Sustainable Food Consumption: A Meta-Analysis Using a Traditional and a Structural Equation Modelling Approach. *International Journal of Psychological Studies*, 4(1), 22-45. DOI: 10.5539/ijps.v4n1p22
- [23] J. L. Guo, T. F. Wang, J. Y. Liao & C. M. Huang. (2016). Efficacy of the Theory of Planned Behavior in Predicting Breastfeeding: Meta-Analysis and Structural Equation Modeling. *Applied Nursing Research*, 29, 37-42. DOI: 10.1016/j.apnr.2015.03.016
- [24] R. Cooke, M. Dahdah, P. Norman & D. P. French. (2016). How Well Does the Theory of Planned Behaviour Predict Alcohol Consumption? A Systematic Review and Meta-Analysis. *Health Psychology Review*, 10(2), 148-167. DOI: 10.1080/17437199.2014.947547

- [25] L. Zhang, J. Zhu & Q. Liu. (2012). A Meta-Analysis of Mobile Commerce Adoption and the Moderating Effect of Culture. *Computers in Human Behavior*, 28, 1902-1911. DOI: 10.1016/j.chb.2012.05.008
- [26] T. M. Nguyen, P. T. Nham & V. N. V. Hoang. (2019). The Theory of Planned Behavior and Knowledge Sharing: A Systematic Review and Meta-Analytic Structural Equation Modelling. *VINE Journal of Information and Knowledge Management Systems*, 49(1), 76-94. DOI: 10.1108/VJKMS-10-2018-0086
- [27] G. D. Moody, M. Siponen & S. Pahlila. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly*, 42(1), 285-311. DOI: 10.25300/misq/2018/13853
- [28] T. Somestad & J. Hallberg. (2013, July). A Review of the Theory of Planned Behaviour in the Context of Information Security Policy Compliance. *IFIP International Information Security Conference* (pp. 257-271). Springer, Berlin, Heidelberg.
- [29] D. Milicevic & M. Goeken. (2013). Systematic Review and Meta-Analysis of IS Security Policy Compliance Research. First Steps Towards Evidence-Based Structuring of the IS Security Domain. *International Conference on Wirtschaftsinformatik*. (pp. 1067-81). Leipzig.
- [30] M. W. L. Cheung, K., Leung & K. Au. (2006). Evaluating Multilevel Models in Cross-Cultural Research: An Illustration with Social Axioms. *Journal of Cross-Cultural Psychology*, 37, 522-541. DOI: 10.1177/0022022106290476
- [31] J. D'Arcy & P. B. Lowry. (2019). Cognitive-Affective Drivers of Employees' Daily Compliance with Information Security Policies: A Multilevel, Longitudinal Study. *Information Systems Journal*, 29(1), 43-69. DOI: 10.1111/isj.12173
- [32] J. Shropshire, M. Warkentin & S. Sharma. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, 49, 177-191. DOI: 10.1016/j.cose.2015.01.002
- [33] J. L. Jenkins. (2013). *Alleviating Insider Threats: Mitigation Strategies and Detection Techniques*. unpublished doctoral dissertation, University of Arizona.
- [34] A. M. Chu, P. Y. Chau & M. K. So. (2015). Explaining the misuse of information systems resources in the workplace: A dual-process approach. *Journal of Business Ethics*, 131(1), 209-225. DOI: 10.1007/s10551-014-2250-4
- [35] K. Guo, Y. Yuan, N. Archer & C. Connelly. (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
- [36] T. M. Dugo. (2007). *The Insider Threat to Organizational Information Security: A Structural Model and Empirical Test*, unpublished doctoral dissertation, Auburn University.
- [37] A. G. Peace, D. F. Galletta & J. Y. Thong. (2003). Software Piracy in the Workplace: A Model and Empirical Test. *Journal of Management Information Systems*, 20(1), 153-177. DOI: 10.1080/07421222.2003.11045759
- [38] M. W. L. Cheung. (2015). metaSEM: An R Package for Meta-Analysis using Structural Equation Modeling. *Frontiers in Psychology*. 5, 1-7. DOI: 10.3389/fpsyg.2014.01521
- [39] S. Jak. (2015). *Meta-analytic Structural Equation Modelling*. New York: Springer. DOI: 10.1007/978-3-319-27174-3
- [40] M. Cho & H. Park. (2019). Convergence Study on the Effect of Music Mediation Program on Children with ADHD - Systematic Review and Meta-Analysis. *Journal of Digital Convergence*. 17(10), 497-507. DOI: 10.14400/JDC.2019.17.10.497
- [41] Y. Sohn & B. Lee. (2012). An Efficacy of Social Cognitive Behavior Model based on the Theory of Planned Behavior : A Meta-Analytic Review. *Korean Journal of Journalism & Communication Studies*. 56(6), 127-161. UCI: G704-000203.2012.56.6.007

김 중 기(Jongki Kim)

[정회원]



- 1987년 2월 : 부산대학교 경영학과(경영학사)
- 1988년 12월 : 미국 아칸소 주립대 경영대학원(경영학석사)
- 1992년 12월 : 미국 미시시피 주립대 경영학과(경영학박사)
- 1999년 3월 ~ 현재: 부산대학교 경영

학과 교수

- 관심분야 : 정보 프라이버시, 정보보안, 연구방법론, 메타분석

· E-Mail : jkkm1@pusan.ac.kr

모 건(Jian Mou)

[정회원]



- 2009년 8월 : 강원대학교 경영학과(경영학사)
- 2011년 8월 : 부산대학교 경영학과(경영학석사)
- 2015년 3월 : 남아공 University of the Witwatersrand (정보시스템학박사)

· 2020년 3월 ~ 현재 : 부산대학교 경영학과 조교수

- 관심분야 : social media, online human behavior, online security and privacy, HCI, meta-analysis

· E-Mail : jian.mou@pusan.ac.kr