http://dx.doi.org/10.14400/JDC.2016.14.4.209

# 조직 구성원의 정보보안정책 준수행동에 대한 연구 : 수정된 Triandis 모델의 적용

김대진*, 황인호**, 김진수***
중앙대학교 경영경제대학 시간강사*, (사)한국창업경영연구원 책임연구원**, 중앙대학교 경영경제대학 경영학부 교수***

# A Study on Employee's Compliance Behavior towards Information Security Policy : A Modified Triandis Model

**Dae-Jin Kim*, In-Ho Hwang**, Jin-Soo Kim*****
**Lecture, College of Business and Economics, Chung-Ang University***
**Researcher, Korea Entrepreneurship & Management Institute****
**Professor, College of Business and Economics, Chung-Ang University*****

**요 약** 조직은 정보보안정책을 제공하고 이를 준수하기 위한 교육 및 지원 등 지속적인 노력을 하고 있으나, 조직 구성원의 보안 미준수에 따른 사고는 끊이지 않고 있다. 본 연구는 조직 구성원의 정보보안정책 준수행동에 영향을 주는 요인들을 Triandis 모델을 적용하여 규명하였으며, 요인들간의 영향 관계를 구조방정식모델링 기법인 PLS(Partial Least Squares)를 통해 살펴보았다. 가설검증 결과 조직은 정보보안정책과 이를 지원하는 촉진조건을 통해 구성원의 정보보안정책 준수의도 및 행동을 유도할 수 있으며, 조직의 정보보안정책에 대한 구성원의 기대가치, 습관 및 감정이 중요함을 증명하였다. 본 연구는 Triandis 모델을 정보보안 분야에 적용하여 분석하고, 구성원의 정보보안 행동에 대한 방향성을 제시하였다는 점에 의의가 있다. 그리고 본 연구 결과를 통해 조직의 정보보안정책 수립 및 구성원의 준수행동을 높이기 위한 방안을 제공할 수 있을 것이다.

**주제어** : 정보보안정책, Triandis 모델, 사회적 요인, 개인 인지 요인, 준수의도, 준수행동

**Abstract** Although organizations are providing information security policy, education and support to guide their employees in security policy compliance, accidents by non-compliance is still a never ending problem to organizations. This study investigates the factors that influence employees' information security policy compliance behavior using elements of Triandis model. We analyzed the relationships among Triandis model's factors using PLS( Partial Least Squares). The result of the hypothesis tests shows that organization can induce individual's information security policy compliance intention and behavior by information security policy and facilitating conditions that support it, and proves the importance of members' expected value, habit and affect about information security compliance. This study is significant in a way that it applies Triandis model in the field of information security, and presents direction for members' information security behavior, and will be able to provide measures to establish organization's information security policy and increase members' compliance behavior.

**Key Words :** Information Security Policy, Triandis Model, Social Factor, Individual Cognitive Factor, Compliance Intention, Compliance Behavior

Received 1 March 2016, Revised 25 March 2016
Accepted 20 April 2016, Published 28 April 2016
Corresponding Author: In-Ho Hwang
(Korea Entrepreneurship & Management Institute)
Email: hwanginho@nate.com

ISSN: 1738-1916

## 1. 서론

조직은 정보보안정책(Information Security Policy)을 제공하고, 구성원들의 준수 행동 제고를 위한 교육 및 지원 등을 아끼지 않고 있다. 그러나 구성원들의 보안 미준수에 따른 사건 및 사고는 끊이지 않고 있다[1,2]. 전 세계적으로, 보안 사고의 10.6%가 조직 정보시스템에 접근이 가능한 조직 구성원에 의해서 발생하고 있으며, 조직 구성원들은 누구나 잠재적 범죄자가 될 수 있다. 또한, 2014년에 비해 보안 위협 접근 방식을 비교 하면, 해킹 또는 네트워크 취약점에 의해 발생하는 피해는 상대적으로 낮아졌지만, 정보에 대한 물리적 접근이나 자신의 특권을 오용 또는 남용함으로써 보안 사고를 일으킨 사례는 늘어나고 있다[3]. 조직은 정보보안정책 준수 대상인 구성원들이 정보보안정책을 준수하는데 영향을 미치는 요인들을 고려해야 한다.

기존 정보보안정책 준수 관련 연구는 조직의 보안정책이 준수 태도 및 의도에 미치는 영향 분석 등을 중심으로 다루어져 왔다[2,4,5,6]. 결과변수가 주로 개인의 준수 태도 및 행동 의도에 맞추어져 있으며, 실제 준수 행동에 영향을 미치는 요인들에 대한 분석이 미흡하다[7]. 또한 기존 준수 태도 및 행동 의도에 대한 연구로는 조직 구성원의 실제 보안 준수행동에 영향을 미치는 다양한 요인들을 제시하기 어렵다.

정보보안에 있어서 조직과 구성원은 상호 간에 교환관계가 성립하는 관계이다[8,9]. 이에, 조직은 구성원에게 조직이 요구하는 수준에 맞는 정보보안 활동을 수행하길 요구하고, 구성원은 자신의 제한된 정보를 기반으로 의사결정을 하게 된다[10,11]. 또한, 구성원의 정보보안에 대한 의사결정 및 행동에 따라서 조직의 정보보안 수준이 결정된다[12]. 즉, 조직은 조직을 구성하는 개개인의 집합이며, 하나의 사회성을 띄는 집단이기 때문에[13], 조직의 입장에서 정보보안정책의 실효성을 제대로 파악하기 어렵다.

이에 본 연구에서는 첫째, 개인 및 조직 관점의 요인들이 구성원들의 정보보안정책 준수의도 및 실제 준수행동에 미치는 영향력을 찾고자 한다. Triandis(1980) 제시한 개인 및 조직 관점 요인들과 정보보안정책 준수의도 및 행동 간의 영향관계를 분석하여, 조직 구성원들의 정보보안정책 준수에 영향을 미치는 요인들을 제시하고자 한다[14]. 둘째, 정보보안정책 준수행동에 직접적으로 영향을 주는 선행 요인을 찾고자 한다. Triandis(1980) 등의 선행 연구를 기반으로 습관 및 촉진조건이 실제 준수행동에 영향을 미치는 직접적인 요인으로 판단하였으며[14], 영향관계를 증명하고자 한다.

## 2. 이론적 배경

### 2.1 조직의 정보보안

조직 내 정보보안 사고는 언제 어디서든 누군가가 조직의 정보시스템에 접근이 가능하면 발생할 가능성이 있다[15]. 조직의 정보시스템에 접근이 가능한 구성원은 직종과 무관하게 정보 노출 사고를 일으킬 수 있으며, 부주의로 조직의 정보자원을 노출시킬 수도 있다[16].

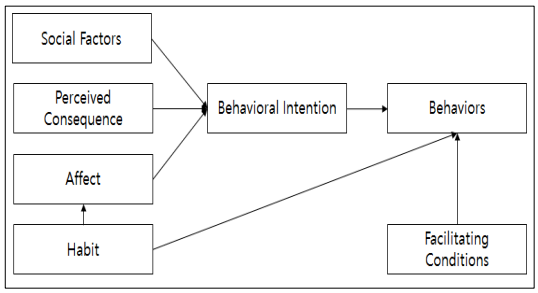
조직은 구성원의 정보보안 노출의 위험성 및 무의식적인 정보보안 노출을 줄이기 위한 교육 프로그램을 제공하며[17], 정보보안 활동의 중요성 등을 홍보하고 있다. 그럼에도 불구하고, 구성원의 정보보안 준수의도 및 행동에 대한 불확실성은 줄어들지 않고 있다[18]. West(2008)는 조직과 구성원의 정보보안 목표가 다르고, 구성원 자신은 보안 위험에 덜 노출 될 것이라는 인식, 그리고 구성원들과의 보안 행동 비교 등을 그 이유로 제시하였다[16]. 결과적으로 조직은 구성원의 보안 준수활동에 영향을 미치는 요인들을 찾고, 지원 체계를 갖춤으로써 보다 효과적인 정보보안 활동을 지원할 수 있다.

### 2.2 Triandis model

Triandis 모델은 1971년에 처음 제안되고, 이후 다양한 분야에서 인간행동을 설명·예측하기 위한 주요 모형으로 활용되고 있다. 이 모델은 행동에 대한 인간의 감정을 중시하고, 행동에 대한 기대 가치와 사회적 요인 등을 토대로 복합적인 인간의 사회적 행동을 예측하고 설명하는데 매우 유용한 이론적 모형으로 평가받고 있다[19].

Triandis 모형은 개인 인지 요인인 지각된 결과와 감정 요인, 그리고 사회적 요인 등은 행동의도를 매개로 실제 행동에 대한 영향을 분석하는 모형이다. 그리고 환경적 요인인 촉진조건과 습관은 실제 행동에 직접적으로 영향을 미친다고 가정한다[14,20]. 또한 인간의 행동은 감정과 지각된 결과, 그리고 사회·환경적 요인 등이 복합적

으로 발현된다는 점을 강조한다. 그러므로 Triandis 모델은 구성원들의 정보보안 준수의도 및 행동에 영향을 미치는 복합적인 요인들에 대한 고려가 가능하다[14]. 정보보안 관점에서 Triandis 모델은 조직과 구성원들의 고려요인들과 영향관계를 제시하기 때문에, 구성원의 정보보안 활동을 통제 및 관리하는 조직에게 유용한 의미를 줄 수 있다.




[Fig. 1] Triandis model(1980)

#### 2.2.1 준수의도

Triandis 모델에서, 행동의도(behavioral intention)는 행동을 위한 의도적인 계획(conscious plan)을 의미한다[14]. 정보보안 분야에서 행동의도는 준수의도(compliance intention)로 볼 수 있다. 정보보안 준수의도는 잠재적 보안 피해로부터 조직의 정보 및 기술 자원을 보호하기 위한 구성원의 의도로 정의된다[15,21]. 구성원의 정보보안 준수의도는 조직이 요구하는 수준의 정보보안정책에 대한 준수의지가 발생할 경우 실제 행동으로 전환된다[22]. 즉, 구성원의 정보보안 준수의도는 자발적인 보안 활동을 위한 구성원의 의지이기 때문에, 조직이 요구하는 정보보안 수준을 달성하기 위해서는 구성원 스스로의 노력이 필요하다. 본 연구에서는 구성원의 정보보안 준수의도와 준수행동간의 관계에 대하여 다음과 같은 가설을 제시한다.

H1 : 조직 구성원의 정보보안정책 준수의도는 준수행동에 정(+)의 영향을 미칠 것이다.

#### 2.2.2 습관

Triandis 모델에서, 습관(habit)은 주어진 환경에 대한 상황-행동의 순서(situation-behavior sequences)가 자동화된 개인적인 측면으로 정의할 수 있다[14]. 본 연구에서 습관은 정보보안 정책에 대한 상황-행동의 순서가 자동화된 개인적인 측면으로 정의할 수 있다. Triandis는 행동에 영향을 미치는 요인으로 의도보다 습관이 더 중요함을 강조하였다[23]. 습관은 장기적으로 실제 행동을 증가시키는 반면, 행동의도는 감소시키는 것으로 나타났다[24].

또한 습관은 개인의 경험과 주어진 역할을 수행할 수 있는 능력과 관련이 있으며, 주어진 상황에 대한 개인의 감정 반응에 영향을 준다[24,25]. 조직 구성원이 업무를 수행하면서 정보보안정책 준수 습관을 형성하기 위해서는 노력이 필요하며, 이에 대한 긍정·부정 등의 다양한 감정이 형성된다. 본 연구에서는 구성원의 습관과 정보보안 준수행동 및 구성원의 감정 간의 관계에 대하여 다음과 같은 가설을 제시한다.

H2a : 조직 구성원의 정보보안정책 준수 습관은 준수행동에 정(+)의 영향을 미칠 것이다.

H2b : 조직 구성원의 정보보안정책 준수 습관은 감정에 정(+)의 영향을 미칠 것이다.

#### 2.2.3 감정

Triandis 모델에서, 감정(affect)은 개인의 본능, 직관 및 감정에 의해 무의식(unconscious) 프로세스를 기반으로 특정 상황에 대한 정서적 또는 감정적인 반응이다. 즉, 특정 상황에 대한 즐거움, 흥분, 기쁨, 우울함, 싫음 등과 같은 개인의 감정적인 측면을 의미한다[14]. 구성원은 업무를 수행하며 자연스럽게 다양한 감정을 경험하며, 감정은 의사결정 과정에 중요한 영향을 미칠 것이다[26]. Triandis는 개인이 가끔은 상황을 정확하게 인지하지 못하고, 자신의 감정에 의존하여 의사결정에 도달한다고 주장하였다[14]. 조직 구성원은 정보보안정책을 준수하는 과정에서 다양한 감정을 경험하게 된다. 본 연구에서는 구성원의 감정과 준수의도간의 관계에 대하여 다음과 같은 가설을 제시한다.

H3 : 조직의 정보보안정책에 대한 구성원의 감정은 준수의도에 정(+)의 영향을 미칠 것이다.

#### 2.2.4 기대가치

Triandis 모델에서, 지각된 결과(perceived consequence)는 특정 대상이나 행동을 통해 지각되는 가치이다. 지각

된 결과는 인지적 측면을 포함한 행동의 결과가 수반하게 될 잠재적인 성과와 이로움을 줄 가능성에 대한 개인의 기대를 의미한다[14,19,26,27]. 정보보안정책 준수에 따른 지각된 결과는 구성원 개인측면에서 직접적으로 확인하는데 어려움이 있으며, 또한 선행연구에서 제시하는 단기·장기적 결과 측정이 어렵다. 그러므로 Triandis 초기 연구에서 제시된 가치측면에서 접근하는 것이 타당하며, 본 연구에서 지각된 결과를 기대가치(expected value)로 구성하였다. 기대가치는 정보보안정책 준수행동에 대한 기대 정도로 정의하여 측정하였다. 본 연구에서는 구성원의 기대가치와 준수의도간의 관계에 대하여 다음과 같은 가설을 제시한다.

H4 : 조직의 정보보안정책에 대한 구성원의 기대가치는 준수의도에 정(+)의 영향을 미칠 것이다.

#### 2.2.5 보안 정책

Triandis 모델에서, 사회적 요인(social factor)은 개인의 행동 의지 및 행동에 영향을 미치는 개인의 준거집단으로부터 받는 사회적 압력을 의미한다[28]. 조직의 정보보안 환경에서 사회적 요인은 구성원이 준수해야 할 정보보안정책으로 생각할 수 있으며, 구성원에게 정보보안 행동을 요구하기 위해서는 조직이 요구하는 정보보안 행동 수칙 및 수준을 명확하게 제공하는 것이 필요하다[29,30,31]. Lee et al.(2004)는 정보보안정책이 구성원의 보안 준수의도를 높이고 남용(misuse)을 줄일 수 있는 선행요인이라고 하였으며, 조직에 맞는 정보보안정책 수립은 조직의 정보보안 활동에 영향을 줄 것으로 판단된다[32].

본 연구에서 정보보안정책은 ISO/IEC 17799(2000), ISO 27001(2013) 국제 표준에서 제시한 설문문항을 기반으로 구성하였다[33]. 그러나 ISO에서 제시한 설문문항들은 정보보안 관리자에게 조직의 정보보안 관련 의견을 조사하기 위한 설문문항들로 구성되어 있어, 정보보안 관리자가 아닌 구성원들이 설문에 응답하기에 어려움이 있다. 그러므로 제시된 34개의 설문문항 중 구성원들이 응답 가능한 16개 문항으로 재구성하였으며, 설문 응답은 Yes/No로 진행하였다. 이후 구조방정식 분석을 위하여 Yes로 응답한 개수를 7점 리커드 척도로 변환하여 분석에 사용하였다[34]. 본 연구에서는 조직의 정보보안정책과 구성원의 준수의도간의 관계에 대하여 다음과 같은 가설을 제시한다.

H5 : 조직의 정보보안정책은 구성원의 준수의도에 정(+)의 영향을 미칠 것이다.

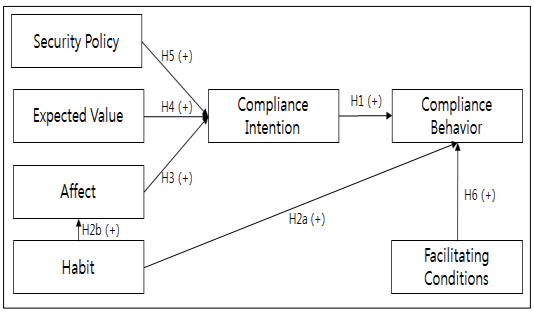
#### 2.2.6 촉진조건

Triandis 모델에서, 촉진조건(facilitating conditions)은 개인의 특정 행동을 보다 용이하게 만들어주는 외적 환경요인으로 객관적인 요소에 해당한다[14]. 개인의 행동의도가 높다고 하더라도 어떠한 객관적 방해물이 존재한다면 행동이 이루어질 수 없기 때문에 촉진조건의 고려는 매우 중요하다[19,25]. 정보보안 분야에서 촉진조건은 정보보안 준수를 용이하게 만들어주는 외적 환경요인으로 정의할 수 있다. 즉, 촉진조건은 정보보안정책 준수행동에 긍정적인 영향을 미친다고 가정할 수 있다. 부족한 촉진조건은 구성원들의 정보보안정책 내용 확인을 어렵게 할 것이다. 이는 정보보안정책 준수행동에 영향을 미치며, 결국 준수행동의 가능성을 낮출 것이다[35]. 본 연구에서는 조직의 촉진조건과 구성원의 정보보안 준수행동간의 관계에 대하여 다음과 같은 가설을 제시한다.

H6 : 조직의 촉진조건은 구성원의 준수행동에 정(+)의 영향을 미칠 것이다.

## 3. 연구 모델 및 방법

### 3.1 연구 모델




[Fig. 2] Research Model and Proposed Hypotheses

본 연구는 복합적인 인간의 행동을 예측하는데 활용

된 Triandis 모델을 기반으로 조직의 정보보안 활동에 영향을 미치는 요인들을 개인 및 조직 관점을 고려한 통합 관점에서 접근하여, 조직과 조직원의 효과적인 정보보안 활동을 하기 위한 조건 및 방안을 제시하고자 한다. 본 연구의 목적에 기반한 연구 모델은 [Fig. 2]와 같다.

### 3.2 데이터 측정 방법 및 수집

본 연구에 사용된 측정변수들은 관련 선행연구를 통하여 다항목 지표들로 구성하여 측정하였다 <Table 1>. 각 측정 변수들은 7점 리커트 척도를 사용하여 구성하였다.

〈Table 1〉 Questionnaire

| Constructs | | Items | Source |
|---|---|---|---|
| Security Policy (Yes/No Question) | SP1 | Organization has clearly definable rules and responsibilities for information security. | [33] |
| | SP2 | Organization has a written form of information security policy. | |
| | SP3 | Organization has a system that when a third party(outsider) approaches the information system, the approval from senior management positions is required. | |
| | SP4 | Organization provides measures to store, use, delete, and back up data. | |
| | SP5 | Organizations has an immediate reporting system for the security incidents. | |
| | SP6 | Organization requires a personal PC to be logged off or locked when away. | |
| | SP7 | Organization has an official disciplinary process for when information security policy or process is violated. | |
| | SP8 | Organization holds a security product or related assets for information security. | |
| | SP9 | Organization has physical procedures(security access gates, etc) for information security. | |
| | SP10 | Organization has outsider control procedures for information security. | |
| | SP11 | Organization conducts a regular information system check for information security. | |
| | SP12 | Organization has a system for solving problems in the event of an accident. | |
| | SP13 | Organization has its information system protected by information security policy and firewall technology. | |
| | SP14 | Organization's information system has an authentication process for users. | |
| | SP15 | Organization's information system controls via user account registration and the access control policies. | |
| | SP16 | Organization monitors information security violation situation and the contents. | |
| Expected Value | EV1 | I work complying information security policy and it has positive effect on my work performance. | [26], [27] |
| | EV2 | I work complying information security policy and it can increase quality of my work result. | |
| | EV3 | I work complying information security policy and it can increase the efficiency of my work performance. | |
| | EV4 | I work complying information security policy and it can make a lot of performance effect with the same efforts. | |
| Affect | Aff1 | It is smart to do the work complying information security policy. | [24] |
| | Aff2 | It is a pleasure to do the work complying information security policy. | |
| | Aff3 | It is boring to do the work complying information security policy.(reverse) | |
| | Aff4 | It feels good to do the work complying information security policy. | |
| | Aff5 | It is unsatisfactory to do the work complying information security policy.(reverse) | |
| Habit | Hab1 | I always comply information security policy. | [24] |
| | Hab2 | I definitely comply information security policy. | |
| | Hab3 | Before complying information security policy, I don't think twice.(dropped) | |
| | Hab4 | It is natural to comply information security policy. | |
| Facilitating Conditions | FC1 | Immediate managers make up regular meetings related to information security. | [26] |
| | FC2 | There is a personnel(or organization) supporting when there are difficulties regarding the organization's information security policy compliance. | |
| | FC3 | It is possible to get education related to information security policy. | |
| | FC4 | There are many difficulties(time, expertise, interaction, etc) complying information security policy in organization. (dropped) | |
| Compliance Intention | CI1 | I will continue to follow our organization's information security policy. | [29] |
| | CI2 | I am likely to continue to follow the organization's information system security policy to protect information systems of our organization.(dropped) | |
| | CI3 | I will comply with information security policy each time I connect to our company's information system. | |
| | CI4 | I will observe information security process every time I do the work. | |
| | CI5 | I feel confident about my attitude to comply with the organization's information security policy.(dropped) | |
| Compliance Behavior | CB1 | I comply the information security policy.(dropped) | [30] |
| | CB2 | I recommend complying the information security policy to others.(dropped) | |
| | CB3 | I help others comply the information security policy. | |
| | CB4 | I use the information security equipment(system) which is necessary to perform the work. | |
| | CB5 | I comply the correct information security procedures while performing the work. | |

정보보안정책 보유 기업의 구성원 및 관련 전공 대학원생 등 20명을 대상으로 사전 설문을 실시하여 설문 문항을 수정·보완하였다. 본 설문은 정보보안정책을 보유한 기업의 구성원을 대상으로 실시하였다. 설문 수집은 2014년 5월 한달 동안 직접 방문 및 이메일로 설문을 실시하였다. 총 526개의 설문이 수집되었으며, 오류 응답 설문 65개를 제외한 461개의 설문 응답을 분석하였다 <Table 2>.

〈Table 2〉 Demographic Characteristics

| Demographic Categories | | | Frequency | | % |
|---|---|---|---|---|---|
| Total | | | 461 | | 100.0 |
| Gender | Male | | 237 | | 51.4 |
| | Female | | 224 | | 48.6 |
| Age | < 30 | | 118 | | 25.6 |
| | 31~40 | | 178 | | 38.6 |
| | 41~50 | | 132 | | 28.6 |
| | > 50 | | 33 | | 7.2 |
| Type of Industry | Manufacture | Chemical | 31 | 136 | 29.5 |
| | | Motor Vehicles | 44 | | |
| | | Electronic | 17 | | |
| | | Other | 44 | | |
| | Service | Information | 24 | 325 | 70.5 |
| | | Finance | 249 | | |
| | | Business Support | 15 | | |
| | | Other | 37 | | |
| Job Tenure | < 5 years | | 141 | | 30.6 |
| | 5~10 years | | 91 | | 19.7 |
| | 11~15 years | | 82 | | 17.8 |
| | 16~20 years | | 56 | | 12.1 |
| | > 21 years | | 91 | | 19.7 |
| Job Position | Staff | | 158 | | 34.3 |
| | Assistant Manager | | 93 | | 20.2 |
| | Manager | | 88 | | 19.1 |
| | General Manager | | 106 | | 23.0 |
| | Executive | | 16 | | 3.5 |

## 4. 가설 검증

### 4.1 신뢰성 및 타당성 분석

본 연구에서는 측정변수의 신뢰성 및 타당성 분석을 실시하였다. 분석은 SPSS 21.0과 SmartPLS 2.0을 활용하였으며, 부트스트랩(bootstrap) 복원 횟수는 3,000으로 설정하였다.

<Table 3>에 나타난 것처럼, 측정변수의 Cronbach's α 값과 Composite Reliability 값은 0.7이상이고, AVE (Average Variance Extracted) 값이 0.5이상으로 충분히 신뢰성을 확보한 것으로 나타났다[36]. 또한 측정문항의 요인 적재량이 0.5이상이며, 각 요인의 t 값이 2.576 이상으로 나타나 유의수준 1%에서 모두 유의하므로 집중 타당성이 있는 것으로 평가할 수 있다. <Table 4>와 같이, 각 구성요소의 AVE 제곱근 값은 종과 횡의 구성개념간 상관계수값 보다 커서 판별 타당성이 존재한다고 할 수 있다[37,38].

다음으로 독립변수들에 대한 다중공선성의 가능성을 살펴보았다. 독립변수의 다중공선성은 공차한계(tolerance)와 VIF(Variance Inflation Factor) 값으로 분석하였다. 일반적으로 공차한계가 0.1 이하, VIF가 4 이상일 때 다

〈Table 3〉 Result for Construct Validity and Reliability

| Construct | Item | Mean | SD | Factor Loading | t-ststistic | Cronbach's Alpha | Composite Reliability | AVE |
|---|---|---|---|---|---|---|---|---|
| Security Policy | SP | 6.57 | 1.103 | 1.000 | 127.863 | 1.000 | 1.000 | 1.000 |
| Expected Value | EV1 | 4.727 | 1.681 | 0.949 | 60.379 | 0.964 | 0.974 | 0.903 |
| | EV2 | 4.690 | 1.726 | 0.948 | 58.334 | | | |
| | EV3 | 4.512 | 1.754 | 0.967 | 55.231 | | | |
| | EV4 | 4.464 | 1.729 | 0.936 | 55.447 | | | |
| Affect | Aff1 | 5.25 | 1.570 | 0.841 | 71.867 | 0.915 | 0.936 | 0.745 |
| | Aff2 | 4.349 | 1.591 | 0.893 | 58.684 | | | |
| | Aff3(R) | 4.855 | 1.570 | 0.845 | 66.408 | | | |
| | Aff4 | 4.423 | 1.580 | 0.894 | 60.100 | | | |
| | Aff5(R) | 4.896 | 1.627 | 0.840 | 64.627 | | | |
| Habit | Hab1 | 5.913 | 1.357 | 0.956 | 93.591 | 0.946 | 0.966 | 0.903 |
| | Hab2 | 6.002 | 1.352 | 0.970 | 95.310 | | | |
| | Hab4 | 5.866 | 1.380 | 0.925 | 91.278 | | | |
| Facilitating Conditions | FC1 | 4.618 | 1.886 | 0.857 | 52.566 | 0.882 | 0.927 | 0.809 |
| | FC2 | 5.579 | 1.649 | 0.906 | 72.658 | | | |
| | FC3 | 5.423 | 1.688 | 0.935 | 68.984 | | | |
| Compliance Intention | CI1 | 6.197 | 1.158 | 0.954 | 114.890 | 0.959 | 0.973 | 0.924 |
| | CI3 | 6.275 | 1.115 | 0.970 | 120.830 | | | |
| | CI4 | 6.265 | 1.089 | 0.959 | 123.493 | | | |
| Compliance Behavior | CB3 | 6.030 | 1.194 | 0.948 | 108.458 | 0.949 | 0.967 | 0.908 |
| | CB4 | 6.161 | 1.242 | 0.947 | 106.459 | | | |
| | CB5 | 6.158 | 1.134 | 0.963 | 116.611 | | | |

중공선성이 존재한다고 판단한다[39]. 측정결과 보안정책(tolerance = 0.976, VIF = 1.025), 기대가치(tolerance = 0.466, VIF = 2.146), 그리고 감정(tolerance = 0.468, VIF = 2.173) 모두 조건에 충족하여, 다중공선성 문제가 없음을 알 수 있다.

### 4.2 동일방법편의 검증

본 연구에서 사용된 데이터가 동일시점에 동일한 측정대상으로부터 자기보고 방법을 통해 측정되었다는 점에서 동일방법편의(common methods bias)가 발생했을 가능성이 있다[40]. 이에, 본 연구에서는 두 가지 검증을 실시하였다. 첫째, 일반적인 방법으로 구성요인들에 대한 상관관계 분석을 실시하여 값이 0.9 이상이면 동일방법편의가 존재한다고 판단할 수 있다[41]. <Table 4>에서 상관관계 분석을 통해 0.9 이상의 값은 확인되지 않았으므로, 동일방법편의 관련 문제는 없는 것으로 확인되었다. 둘째, 보다 엄격하게 동일방법편의를 진단하기 위해 Podsakoff et al.(2003)가 제안한 '비측정 단일 동일방법요인'을 Liang et al.(2007)이 PLS에 적용한 방법으로 분석하였다[42,43]. PLS 모델로 동일방법편의를 분석하기 위해서 방법변수에 모든 주요 구성변수의 측정변수들을 포함하고, 주요 구성변수와 방법변수에 의해 설명되는 분산을 계산하여 <Table 5>와 같이 제시하였다[43,44].

〈Table 4〉 Result for Discriminant Validity

| Constructs | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| 1. Security Policy | 1.000 | | | | | | |
| 2. Expected Value | 0.153 | 0.950 | | | | | |
| 3. Affect | 0.146 | 0.731 | 0.863 | | | | |
| 4. Habit | 0.395 | 0.377 | 0.412 | 0.950 | | | |
| 5. Facilitating Conditions | 0.499 | 0.366 | 0.398 | 0.644 | 0.900 | | |
| 6. Compliance Intention | 0.408 | 0.418 | 0.404 | 0.793 | 0.540 | 0.961 | |
| 7. Compliance Behavior | 0.447 | 0.423 | 0.370 | 0.772 | 0.589 | 0.855 | 0.953 |

Note: Values in bold type along the diagonal indicate the square root of the AVE

〈Table 5〉 Common Method Bias Analysis

| Constructs | Indicator | Substantive Factor Loading(R1) | $(R1)^2$ | Method Factor Loading(R2) | $(R2)^2$ |
|---|---|---|---|---|---|
| Security Policy | SP1 | 0.448*** | 0.200 | 0.000 | 0.000 |
| Expected Value | EV1 | 0.715*** | 0.512 | 0.061** | 0.004 |
| | EV2 | 0.698*** | 0.488 | 0.024 | 0.001 |
| | EV3 | 0.685*** | 0.469 | -0.045** | 0.002 |
| | EV4 | 0.666*** | 0.444 | -0.040* | 0.002 |
| Affect | Aff1 | 0.692*** | 0.478 | 0.232*** | 0.054 |
| | Aff2 | 0.639*** | 0.408 | -0.013 | 0.000 |
| | Aff3(R) | 0.588*** | 0.345 | -0.054 | 0.003 |
| | Aff4 | 0.632*** | 0.399 | -0.033 | 0.001 |
| | Aff5(R) | 0.552*** | 0.305 | -0.124*** | 0.015 |
| Habit | Hab1 | 0.779*** | 0.607 | -0.064** | 0.004 |
| | Hab2 | 0.805*** | 0.649 | -0.012 | 0.000 |
| | Hab4 | 0.792*** | 0.627 | 0.077* | 0.006 |
| Facilitating Conditions | FC1 | 0.636*** | 0.404 | 0.032 | 0.001 |
| | FC2 | 0.648*** | 0.420 | -0.021 | 0.000 |
| | FC3 | 0.673*** | 0.453 | -0.009 | 0.000 |
| Compliance Intention | CI1 | 0.819*** | 0.671 | 0.052** | 0.003 |
| | CI3 | 0.810*** | 0.656 | -0.028 | 0.001 |
| | CI4 | 0.802*** | 0.644 | -0.024 | 0.001 |
| Compliance Behavior | CB3 | 0.813*** | 0.661 | 0.050 | 0.002 |
| | CB4 | 0.791*** | 0.625 | -0.024 | 0.001 |
| | CB5 | 0.804*** | 0.647 | -0.026 | 0.001 |
| Average | | 0.704 | 0.505 | 0.001 | 0.005 |

분석결과 측정변수들의 설명된 평균 분산은 0.505이며, 방법기반 평균 분산은 0.005이다. 실제요인 평균 분산과 방법요인 평균 분산의 비율은 약 110:1이다. 또한 대부분의 방법요인 적재량도 유의하지 않고, 방법요인 분산의 규모가 작고 무의미하므로, 본 연구에서는 동일방법편의에 따른 문제는 심각하지 않다고 볼 수 있다.

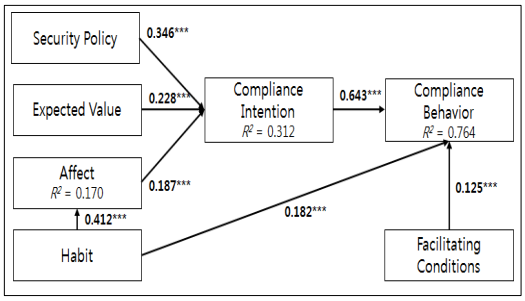
### 4.3 구조모형 평가

구조모형에 대한 적합도는 구조모형의 통계추정량을 나타내는 Redundancy값이 양수일 때 적합도가 있는 것으로 평가하며, 내생변수의 $R^2$ 값이 0.26 이상이면 적합도가 '상', 0.13~0.26 미만이면 '중', 0.02~0.13 미만이면 '하'로 평가한다[45]. 그리고 전체 적합도(goodness of fit)은 $R^2$ 값의 평균값과 공통성(communality)의 평균값의 곱을 제곱근한 값으로 평가하는데, 0.36 이상이면 '상', 0.25~0.36 미만이면 '중', 0.1~0.25 미만이면 '하'로 평가한다[46]. 본 연구에서는 Redundancy 값이 모두 양의 값이며, 내생변수의 $R^2$ 값은 감정(0.170), 준수의도(0.312), 준수행동(0.764) 적합도가 있는 것으로 평가된다. 전체

적합도는 0.606으로 구조모형의 적합성이 존재하는 것으로 나타났다.

### 4.4 가설 검증

구조모형 경로간의 인과관계는 [Fig. 3], <Table 6>의 경로계수 값과 t-값으로 유의성을 평가하였다.




[Fig. 3] Results of the Structural Model

첫째, 구성원의 정보보안정책 준수의도는 준수행동에 정(+)의 영향을 미친다는 가설은 채택되었다($\beta$=0.643, p<0.01). 이러한 결과는 정보보안 준수의도가 준수행동을 증가시킨다는 선행연구와 같은 결과이다[15,21]. 즉, 구성원의 정보보안 준수의도는 자발적인 보안 활동을 위한 개인의 의지이기 때문에, 조직이 요구하는 정보보안 수준을 달성하기 위해서는 구성원의 정보보안 준수의도를 지속적으로 높이기 위한 노력을 하는 것이 필요하다.

둘째, 구성원의 정보보안정책 준수 습관은 준수행동에 정(+)의 영향을 미친다는 가설은 채택되었다($\beta$=0.182, p<0.01). 또한 구성원의 정보보안정책 준수 습관은 정보보안정책에 대한 감정형성에 정(+)의 영향을 미친다는 가설은 채택되었다($\beta$=0.412, p<0.01). 개인의 습관은 감정 및 준수행동에 영향을 주는 요인으로, 정보보안정책 미준수 행동을 예방하는 중요한 요인이다. 그러므로 조직은 구성원들이 보안에 대한 관심을 가지고 능동적으로 정보보안 준수행동을 습관화 할 수 있도록 지속적인 지원을 하는 것이 필요하다.

셋째, 조직의 정보보안정책에 대한 구성원의 바람직한 감정형성은 준수의도에 정(+)의 영향을 미친다는 가설은 채택되었다($\beta$=0.187, p<0.01). 조직은 구성원의 정보보안정책에 대한 감정이 긍정적으로 형성되도록 지속적인 커뮤니케이션을 통하여, 구성원이 요구하는 보안에 대한 관점을 이해하고 지원하는 것이 필요하다.

넷째, 조직의 정보보안정책에 대한 구성원의 기대가치는 준수의도에 정(+)의 영향을 미친다는 가설은 채택되었다($\beta$=0.228, p<0.01). 조직은 구성원들이 정보보안정책에 대한 인지 및 기대 수준을 높일 수 있도록 정보보안의 중요성을 알리며, 정보보안정책을 준수하며 업무를 수행하는 구성원들을 지원을 하는 것이 필요하다.

다섯째, 조직의 정보보안정책은 구성원의 준수의도에 정(+)의 영향을 미친다는 가설은 채택되었다($\beta$=0.346, p<0.01). 이러한 결과는 정보보안정책이 명확하게 규정되어 있을수록 조직의 정보보안 준수행동을 높인다는 선행연구와 같은 결과이다[18]. 조직이 구성원에게 정보보안 준수행동을 요구하기 위해서는 조직의 보안정책을 명확하고 이해하기 쉽게 구조화하는 것이 필요하다.

마지막으로, 조직의 촉진조건은 구성원의 정보보안정책 준수행동에 정(+)의 영향을 미친다는 가설은 채택되었다($\beta$=0.125, p<0.01). 조직은 구성원의 정보보안정책 준수를 위해 지원 조직 및 관련 교육 등의 체계가 필요하다. 따라서 촉진조건을 조직 및 구성원들의 특성을 고려하여 구성하는 것이 필요하다.

〈Table 6〉 Summary of Hypothesis Tests

| Hypothesis | Path | Coefficient | S.E. | t-value | Results |
|---|---|---|---|---|---|
| H1 | Compliance Intention → Compliance Behavior | 0.643*** | 0.062 | 10.383 | Support |
| H2a | Habit → Compliance Behavior | 0.182*** | 0.067 | 2.728 | Support |
| H2b | Habit → Affect | 0.412*** | 0.035 | 11.867 | Support |
| H3 | Affect → Compliance Intention | 0.187*** | 0.064 | 2.934 | Support |
| H4 | Expected Value → Compliance Intention | 0.228*** | 0.069 | 3.329 | Support |
| H5 | Security Policy → Compliance Intention | 0.346*** | 0.051 | 6.833 | Support |
| H6 | Facilitating Conditions → Compliance Behavior | 0.125*** | 0.037 | 3.332 | Support |

***: p < 0.01

## 5. 결론

본 연구는 Triandis 모델을 정보보안 분야에 적용함으로써, 구성원들의 정보보안정책 준수의도 및 행동에 영향을 미치는 요인들을 분석하고, 정보보안 행동에 대한 방향성을 제시하였다. 조직은 정보보안정책과 이를 지원하는 촉진조건을 통해 구성원의 준수의도 및 행동을 유도할 수 있음을 증명하였다. 또한 구성원의 준수의도 및 행동을 유도하기 위해서는 정보보안정책에 대한 구성원들의 기대가치, 습관 및 감정이 중요함을 증명하였다.

본 연구는 다음과 같은 시사점을 제시한다. 첫째, 본 연구는 정보보안 분야에 Triandis 모델을 적용하였다. 조직에서 실행하는 정보보안정책의 결과는 구성원 행동으로 나타나기 때문에, 조직과 구성원들이 중요하게 고려하는 요인들을 파악하는 것이 필요하다. 따라서 Triandis 모델은 단순히 성과와 목표로서 구성원들의 정보보안정책 준수의도 및 행동을 요구하는 것이 아닌 구성원들의 능동적 참여를 위한 개인적 습관 및 감정 등을 고려한 접근이 필요함을 제시한다. 이론적으로 조직과 구성원들이 중요하게 고려하는 영향요인들에 대한 선행 연구를 수행하였으므로, 조직 지원 및 구성원 중요 가치를 기반으로 정보보안 연구를 수행하기 위한 가이드라인을 제시하였다. 실무적으로는 조직에서 제공하는 촉진조건과 같은 지원 이외 구성원의 습관 및 감정 등을 통해 내재화까지 고려하는 것이 필요함을 제시하였다.

둘째, Triandis 모델에서 제시하는 준수행동에 직접적인 관계를 갖는 촉진조건 및 습관에 대한 영향 관계를 확인하였다. 정보보안정책에 대한 구성원의 준수행동은 조직 지원 등의 객관적인 촉진조건과 직접적인 관계가 형성되면 준수행동이 더 높아진다. 또한 습관은 감정을 매개로 준수의도 및 행동과 영향관계를 형성하지만, 직접적인 관계가 형성되면 준수행동이 더 높아진다. 이론적으로 구성원들의 준수행동을 조직 및 개인 측면을 고려하여 직접적인 영향요인들에 대한 연구를 수행하였으며, 향후 구성원의 정보보안정책 준수행동 연구를 위한 가이드라인을 제시하였다. 실무적으로는 조직의 촉진조건과 구성원의 습관이 실제 정보보안정책 준수행동에 미치는 영향 관계를 확인하였으며, 정보보안 팀 및 부서에서 구성원들의 정보보안정책 준수행동을 위한 전략적 행동 수립을 위한 정보를 제공하였다.

본 연구는 다음과 같은 한계점을 가지고 있다. 첫째, 본 연구는 정보보안정책이 잘 수립되어 있는 대기업 및 금융권 위주로 설문을 수집하여, 기업 유형에 따른 특성 등을 반영하지 못하였다. 향후 설문 대상을 다양하게 하고, 더욱 많은 표본을 확보함으로써 통계적으로 보다 세분화하여 분석할 필요성이 있다.

둘째, 본 연구는 기존 Triandis 모델을 정보보안 분야에 적용한 연구로, 구성원들의 정보보안정책 준수의도 및 행동을 위한 조직의 노력 방향을 제시하였다. 향후 연구 시 실제 정보보안정책 준수행동을 위한 다각적 요인들을 제시함으로써, 조직이 수행해야 할 상세한 접근 방향을 제시하는 것이 필요할 것으로 판단된다.

## REFERENCES

[1] J. Han and Y. Kim, "Investigating of Psychological Factors Affecting Information Security Compliance Intention: Convergent Approach to Information Security and Organizational Citizenship Behavior", Journal of Digital Convergence, Vol. 13, No. 8, pp. 133-144, 2015.

[2] M. Yim, "A Path Way to Increase the Intention to Comply with Information Security Policy of Employees", Journal of Digital Convergence, Vol. 10, No. 10, pp. 119-128, 2012.

[3] Verizon, 2015 Data Breach Investigations Report, 2015.

[4] M. Yim and K. Han, "An Investigation of the Factors that Influence the Compliance to Information Security Policy : From Risk Compensation Theory", Journal of Digital Convergence, Vol. 11, No. 10, pp. 153-168, 2013.

[5] J. Do and J. Kim, "A Study on Critical Success Factors for Enterprise Security Collaboration", Journal of Digital Convergence, Vol. 12, No. 10, pp.235-242, 2014.

[6] M. Yim, "An Investigation of the Factors that Influence the Compliance to Information Security Policy: From Risk Compensation Theory", Journal of Digital Convergence, Vol. 11, No. 2, pp.19-32, 2013.

[7] T. Jeong, M. Yim and J. Lee, "A Development of Comprehensive Framework for Continuous Information Security", Journal of Digital Convergence, Vol. 10, No. 2, pp.1-10, 2012.

[8] R. M. Emerson, "Social Exchange Theory", Annual Review of Sociology, Vol. 2, pp. 335-362, 1976.

[9] L. D. Molm, "Structure, Action, and Outcomes: The Dynamics of Power in Social Exchange", American Sociological Review, Vol. 55, No. 3, pp. 427-447, 1990.

[10] C. A. Sims, "Implications of Rational Inattention", Journal of Monetary Economics, Vol. 50, No. 3, pp. 665-690, 2003.

[11] Q. Hu, Z. Xu, T. Dinev and H. Ling, "Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?", Communications of the ACM, Vol. 54, No. 6, pp. 54-60, 2011.

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

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

[14] H. C. Triandis, Values, Attitudes, and Interpersonal Behavior, in Nebraska Symposium on Motivation, 1979: Beliefs, Attitudes, and Values, Lincoln, NE: University of Nebraska Press, pp. 195-259, 1980.

[15] 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.

[16] R. West, "The Psychology of Security", Communications of the ACM, Vol. 51, No. 4, pp. 34-40, 2008.

[17] C. Park and M. Yim, "An Understanding of Impact of Security Countermeasures on Persistent Policy Compliance", Journal of Digital Convergence, Vol. 10, No. 4, pp. 23-35, 2012.

[18] J. D'Arcy, A. Hovav and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach", Information Systems Research, Vol. 20, No. 1, pp. 79-98, 2009.

[19] R. L. Thompson, C. H. Higgins and J. M. Howell, "Towards a Conceptual Model of Utilization", MIS Quarterly, Vol. 15, No. 1, pp. 125-43, 1991.

[20] M. K. Chang and W. Cheung, "Determinants of the Intention to Use Internet/WWW at Work: A Confirmatory Study", Information & Management, Vol. 39, No. 1, pp. 1-14, 2001.

[21] A. Vance, M. Siponen and S. Pahnila, "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory", Information & Management, Vol. 49, No. 3, pp. 190-198, 2012.

[22] Y. Chen, K. Ramamurthy and K. W. Wen, "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?", Journal of Management Information Systems, Vol. 29, No. 3, pp. 157-188, 2012.

[23] F. Bergeron, L. Raymond, S. Rivard and M. F. Gara, "Determinants of EIS Use: Testing a Behavioral Model", Decision Support Systems, Vol. 14, No. 2, pp. 131-46, 1995.

[24] M. Limayem, S. G. Hirt, "Force of Habit and Information Systems Usage: Theory and Initial Validation", Journal of Association for Information Systems, Vol. 4, pp. 65-97, 2003.

[25] C. Cheung and M. Limayem, "The Role of Habit in Information Systems Continuance: Examining the Evolving Relationship between Intention and Usage", Proceedings of the Twenty-Sixth International Conference on Information Systems, Las Vegas, pp. 471-482, 2005.

[26] M. K. Chang, W. Cheung, C. H. Cheng, and J. H. Yeung, "Understanding ERP System Adoption from the Users' Perspective", International Journal of Production Economics, Vol. 113, No. 2, pp. 928-942, 2008.

[27] W. Cheung, M. K. Chang and V. S. Lai, "Prediction of Internet and World Wide Web Usage at Work: A Test of an Extend Triandis Model", Decision

Support Systems, Vol. 30, No. 1, pp. 83-100, 2000.

[28] M. Fishbein and I. Ajzen, Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research, Reading, MA: Addison-Wesley Publishing Company, 1975.

[29] T. Herath and H. R. Rao, "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness", Decision Support Systems, Vol. 47, No. 2, pp. 154-165, 2009.

[30] 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.

[31] R. Von Solms, "Information Security Management: Why Standards are Important", Information Management & Computer Security, Vol. 7, No. 1, pp. 50-58, 1999.

[32] S. Lee, S. 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.

[33] C. T. Upfold and D. A. Sewry, "An Investigation of Information Security in Small and Medium Enterprises (SMEs) in the Eastern Cape", In: H. S. Venter, J. H. P. Eloff, L. Labuschagne, & M. M. Eloff (Eds.), Proceedings of the ISSA 2005 new knowledge today conference, 29 June - 1 July 2005, South Africa, Article 082, pp.1 - 17, 2005.

[34] J. G. Dawes, "Do Data Characteristics Change According to the Number of Scale Points Used? An Experiment Using 5 Point, 7 Point and 10 Point Scales", International Journal of Market Research, Vol. 51, No. 1, pp. 61-77. 2008.

[35] M. Siponen, S. Pahnila and A. Mahmood, "Factors Influencing Protection Motivation and IS Security Policy Compliance", Innovations in Information Technology, pp. 1-5, 2006.

[36] J. C. Nunnally, I. H. Bernstein, Psychometric Theory(3rd ed.), New York: McGraw-Hill, 1994.

[37] 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.

[38] M. Noh, K. Lee, S. Kim and G. Garrison, "Effect of Collectivism on Actual S-Commerce Use and the Moderating Effect of Price Consciousness", Journal of Electronic Commerce Research, Vol. 14, No. 3, pp. 244-260, 2013.

[39] R. E. Walpole, R. H. Myers, S. L. Myers, and K. Ye, Probability and Statistics for Engineers and Scientists (Vol. 5). New York: Macmillan, 1993.

[40] N. K. Malhotra, S. S. Kim and A. Patil, "Common Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research", Management Science, Vol. 52, No. 12, pp. 1865-1883, 2006.

[41] P. A. Pavlou and M. Fygenson, "Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior", MIS Quarterly, Vol. 30, No. 1, pp. 115-144, 2006.

[42] P. Podsakoff, S. MacKenzie, J. Lee and N. Podsakoff, "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies", Journal of Applied Psychology, Vol. 88, No. 5, pp. 879-903, 2003.

[43] H. Liang, N. Saraf, Q. Hu and Y. Xue, "Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top-Management", MIS Quarterly, Vol. 31, No. 1, pp. 59-87, 2007.

[44] L. J. Williams, J. R. Edwards and R. J. Vandenberg, "Recent Advances in Causal Modeling Methods for Organizational and Management Research", Journal of Management, Vol. 29, No. 6, pp. 903-936, 2003.

[45] W. W. Chin, "Issues and Opinion on Structural Equation Modeling", MIS Quarterly, Vol. 22, No. 1, pp. 52-104, 1998.

[46] M. Tenenhaus, V. E Vinzi, Y. M. Chatelin and C. Lauro, "PLS Path Modeling", Computational Statistics & Data Analysis, Vol. 48, No. 1, pp. 159-205, 2005.

**김 대 진(Kim, Dae Jin)**

- 2002년 2월 : 중앙대학교 경영학과 (경영학사)
- 2004년 8월 : 중앙대학교 경영학과 (경영학석사)
- 2011년 2월 : 중앙대학교 경영학과 (경영학박사)
- 2011년 3월 ~ 현재 : 중앙대학교 경영경제대학 시간강사
- 관심분야 : IT 수용, ICT 융합, 정보보안 및 프라이버시 분야 등
- E-Mail : yauchee@cau.ac.kr

**황 인 호(Hwang, In Ho)**

- 2004년 8월 : 건국대학교 경영학과 (경영학사)
- 2007년 6월 : 중앙대학교 경영학과 (경영학석사)
- 2014년 2월 : 중앙대학교 경영학과 (경영학박사)
- 2014년 3월 ~ 현재 : (사)한국창업경영연구원 정보전략 연구팀장
- 관심분야 : IT 핵심성공요인, 디지털 콘텐츠, 정보보안 및 프라이버시 분야 등
- E-Mail : hwanginho@nate.com

**김 진 수(Kim, Jin Soo)**

- 1982년 2월 : 연세대학교 상경대학 응용통계학과(경제학사)
- 1986년 2월 : 텍사스 주립대학 MBA(경영학석사)
- 1990년 2월 : 루이지애나 주립대학(LSU)(경영학박사)
- 1995년 3월 ~ 현재 : 중앙대학교 경영경제대학 경영학과 교수
- 관심분야 : ICT 융합 및 서비스전략, 비즈니스 모델, 빅데이터, 기업가정신과 혁신, 벤처기술창업 등
- E-Mail : sunny@cau.ac.kr