정보보안정책의 특성이 구성원들의 보안정책 준수 행위에 미치는 영향에 관한 연구

임명성*

The Effect of Characteristics of Information Security Policy on Security Policy Compliance Intention of Employees

Myung-Seong Yim*

요 약 보안정책의 두 가지 구성요소는 내용과 형식이다. 지금까지 보안 정책 내용에 대한 연구는 폭 넓게 수행되어온 반면, 보안 정책의 형식에 대해서는 관련연구가 매우 부족한 실정이다. 형식이 보안정책의 성공을 결정하는 중요한 요인이기 때문에 어떻게 보안 정책의 형식을 작성할 것인가는 매우 중요하다. 따라서 본 연구의 목적은 보안 정책의 형식과 조직 구성원들의 보안 정책 준수간의 관계를 규명하는 것이다. 분석결과 보안정책의 형식은 보안준수태도, 주관적 규범, 인지된 행위 통제, 그리고 인지된 보안정책 준수비용에 유의한 영향을 미치는 것으로 나타났으며, 보안정책 준수태도와 주관적 규범은 지속적 보안준수 의도에 유의한 영향을 미치는 것으로 나타났다.

주제어 : 보안정책, 정책준수, 정책 내용, 정책 형식, 계획된 행위 이론

Abstract There are two elements of security policy that can have a bearing on its effectiveness: content and form. While the content of the security policy has been investigated extensively in the most of the previous studies, there is very little literature on the form of the security policy. Since the form of the policy influences its success, it is important to understand how to articulate the form of a security policy. Thus, the aim of this study is to investigate the relationship between security form and policy compliance of employees. Research results find that dimensions of security form have effect on attitude towards security compliance, subjective norm, perceived behavioral control, and perceived response costs, and besides attitude towards security compliance and subjective norm have an effect on persistent security compliance intention. The conclusions and implications are discussed.

Key Words : Security Policy, Policy Compliance, Policy Content, Policy Form, Theory of Planned Behavior

1. 서 론

오늘날의 많은 조직들은 정보보안 정책 위배로 인해 매년 최소 1회 이상의 보안 침해 사고에 직면하고 있다[42]. 따라서 정보시스템 보안 정책을 따르도록 조직 구성원들을 독려하는 것은 많은 조직들이 직면한 주요 도전과제이다[41].

정보 보안 정책은 조직 내 보안을 위해 사용되는 중요한 도구 중 하나이다[18]. D′Arcy and Hovav(2007)의 연구에 따르면 여러 보안 대책 중(예, 보안 정책, 보인 인식 프로그램, 컴퓨터 모니터링, 예방 소프트웨어) 구성원들이 보안 정책을 가장 잘 인식하고 있는 것으로 나타났다(7점 만점에 5.23). 이는 이미 많은 조직들이 보안 대책 중 보안정책을 가장 중요하게 인식하고 이를 구현하고 있기 때문이라는 것을 알 수 있다.

정보보안 정책은 조직 내 정보보안을 위한 방향성을 제시해주는 문서이자[23], 조직 내 구성원들이 정보시스템을 오용하지 않도록 하기 위해서 정보시스템 자원에

*삼육대학교 경영학과 조교수
논문접수: 2012년 11월 14일, 1차 수정을 거쳐, 심사완료: 2012년 11월 30일

대한 적절한 사용법을 기술한 문서이다[12]. 따라서 보안 정책은 조직의 목표와 신념, 현재의 통제규정, 그리고 구성원들의 책무에 대한 내용들이 포함될 뿐만 아니라, 조직의 정보시스템 자원에 대한 허용된 접근과 관련된 세부적인 가이드라인을 제공해 준다[12]. 이를 위해 정보보안 정책은 실무적으로 실행가능해야 하고, 강제성이 있어야 하며, 조직 전반에 걸쳐 정보 자산을 사용하는 모든 구성원들에게 전달되어야 한다[23]. 하지만 보안정책은 통상적으로 조직의 모든 수준에서 비효과적이며 불필요하고 심지어는 강제성이 결여되어 있다고 비판받아오고 있다[18].

일반적으로 보안정책이 다양한 보안 관련 경험과 경력이 있는 책임자에 의해 수립되는 경우는 많지 않다. 또한 정책을 개발한 경험조차 없는 경우가 비일비재하다. 많은 경우 회사의 보안 정책은 다른 조직의 보안 정책을 참고하거나, 국제 표준협회인 ISO가 제시한 ISO 17799와 같은 , 공공 원천(예, BS7799, ISO17799, ISO/IEC PDTR 13335-1, COBIT, GASSP, etc.)에서 제공하는 표준안을 기반으로 하거나[12], 심지어는 인터넷에서 공유되는 자료를 참고하여 작성하는 경우도 있다[23]. 하지만 이러한 자료의 경우 필수적인 권장사항(best practices)만을 포함하고 있기에 이를 그대로 수용하는 것은 적절치 못하다. 또한 보안 정책이라는 것은 조직뿐만 아니라 산업에 따라서도 달라질 수 있기 때문에 조직의 특성을 고려하지 않고 표준만 따르는 것은 여러 문제를 야기할 수 있다.

기존 연구에서는 보안 정책이 정보시스템의 오용을 억제할 수 있는 중요한 요소라고 주장한 연구가 있는 반면[25], 다른 연구는 보안 정책이 제한적 효과만 발휘한다고 주장하였다[39]. Lee and Lee(2002)는 보안 정책 미준수 시 발생할 수 있는 처벌에 대해 기술하며 처벌에 대한 위협을 증가시켰음에도 불구하고 여전히 많은 미국기업에서 보안사고가 발생하고 있다고 주장하였다. 반면 Foltz et al.(2008)은 보안정책이 업무환경에서 부적합한 자원의 접근을 억제시킴과 동시에 해당 정책의 침해는 강력한 처벌이 수반됨을 구성원들에게 인지시킴으로써 조직 내에서 매우 중요한 역할을 한다고 주장하였다.

이러한 불일치의 원인중 하나는 같은 보안정책이라도 사용자들의 인식(users′ perceptions)에 따라 다르게 작용하기 때문이다[25]. 따라서 억제 메커니즘으로써 보안정책의 성공여부는 결국 조직 구성원들의 행위(actions)와 인지(awareness)에 달려 있다[12].

조직원들에게 인지되는 보안 정책의 요소는 내용(content)과 형식(form)이다[18]. 기존 연구의 핵심은 어떠한 내용이 보안 정책에 포함되어야 하는지였다. 그러나 보안 정책이 소수의 수립자에 의해 작성되는 반면 정책 수용자는 모든 구성원이기 때문에 내용뿐만 아니라 수용자에게 보여지는 형식도 중요하게 고려되어야 하는 요소이다. 즉 어떠한 내용이 포함되어 있느냐 뿐만 아니라 쓰여진 정책이 읽기 쉽고 이해하기 쉽고 따르기 쉬운지 여부도 중요하다. 예를 들어 보안 정책이 어려운 전문용어로 쓰여진 경우 이를 이해하는데 어려움이 따르면 보안정책을 수용하기 보다는 거부할 가능성이 높아진다. 따라서 본 연구는 보안 정책의 내용이 아니라 조직 구성원들에게 직접적으로 보여지는 보안정책의 형식이 조직원들의 보안정책 준수에 어떠한 영향을 미치는지 실증분석을 통해 살펴보고자 한다. 본 연구의 함의는 보안정책의 형식이 왜 중요한지 그리고 왜 보안정책의 준수가 제대로 실현되고 있지 않는지를 설명할 수 있는 하나의 이유를 설명해 준다는데 의의가 있다.

본 연구의 구성은 2장에서는 보안정책의 구성요소와 관련 가설을 제시하고, 3장에서는 실증 분석을 통해 가설을 검정한다. 마지막으로 4장에서는 분석결과를 기반으로 결론을 제시한다.

2. 본 론

보안 정책을 구성하는 두 가지 구성요소(elements)는 내용(content)과 형식(form)이다[18]. 하지만 그 동안 많은 조직에서는 보안정책의 내용 개발에만 관심을 두어왔다.

내용 측면에서 정보보안 정책은 정보시스템 보안 목적, 전략, 그리고 다른 정책들이 고려되어야 한다[26]. 따라서 보안 정책에는 다음의 세 가지 내용이 포함된다. 첫째, 보안 전략(strategy)이다[14]. 보안 전략은 상위 수준의 보안 총괄 계획을 나타내며, 경영 목표, 이해관계자, 정책의 범위, 정책의 목적 등이 포함된다[6][37]. 다음으로 정책(policy)이다. 정책은 중간 레벨의 정보보안 방법을 포함한다[6][37]. 또한 정책에서는 정책 근거, 가이드라인, 보안 행위 강화 메커니즘 등이 결합된 상황 특화적(issue-specific) 정책을 제공한다. 마지막으로 운영절차(operating procedures)가 있다. 운영절차에서는 하위 수준에서 다양한 시스템에서의 보안 정책을 구현할 수 있

는 구체적인 실행활동들이 기술되어 있다[6][37].

이처럼 보안 정책의 내용(content)에 대한 연구의 진척수준과는 다르게 형식(form)에 대한 연구는 여전히 초기단계이다. 하지만 보안 정책이란 어떤 내용을 쓸 것인가도 중요하지만 어떻게 쓸 것인가도 중요하다.

일반적으로 보안 정책은 다양한 국제 기준, 산업 기준, 정부 가이드라인 등을 참고하여 내부 전문가들이 수립하게 된다. 따라서 전문가나 의사결정자에 의해서 작성되는 보안 정책은 정책을 따라야 하는 구성원들의 목소리가 반영되기 쉽지 않으며, 정책 수립자와 수용자가 동일한 위치에 있지 않기 때문에 보는 시각도 다르기 때문에 이와 같은 상호 이해가 전제되지 않은 상태에서 수립자의 입장에서 모든 문서가 작성될 가능성이 높다. 따라서 정책 수용자의 입장에서 보안정책의 효과성을 측정하는 것은 매우 중요하다. 이전 연구의 경우 대부분이 보안정책의 내용에 치중한 나머지 보안정책의 또 다른 효과성 지표인 형식에 대해서는 고려하지 않았다. 따라서 형식을 기반으로 보안 정책을 구성원들이 평가하도록 하여 현재의 보안 현실에 대해 평가해 볼 필요가 있다.

Goel and Chengalur-Smith(2010)는 효과적인 보안 정책(effective security policies)을 위해 요구되는 세 가지 차원을 제시하였다: 명확성, 깊이, 간결성. 비록 이 세 가지 차원이 효과적인 보안 정책의 전부를 대변할 수는 없을 지라도 이 세 가지 차원은 정책의 효과성을 위해 필요한 요소이다[18].

명확성(Clarity)은 이해력(comprehension)이라고도 하며 보안 정책이 모호하지 않고 이해하기 쉬운지 여부를 나타낸다[18]. 잘 작성된 보안정책은 읽기 쉬워야 하며, 내용이 이해하기 쉬워야 한다[18]. 정보보안 정책은 내용이 명확해야 하고 조직 내 모든 구성원들이 이해하기 쉬워야 한다[23]. 뿐만 아니라 비전문가도 이해하기 어려운 기술적인 용어를 최대한 피해야 한다[23].

깊이(Breadth)는 완성도(completeness)와 깊이(depth), 즉 정책의 범위(scope, range, coverage)를 나타낸다[18]. 보안 정책이 명확하고 이해하기 쉬워야 할 뿐만 아니라 보안 정책은 현실적이어야 한다[23]. 또한 보안 정책은 주기적인 검토와 수정이 필요하다[23]. 기술환경의 주요 변화나 기술적 요구사항의 변화가 발생할 경우 보안 정책도 이를 반영하여 변경되어야 한다[23]. 단, 너무 잦은 변화는 정책을 따라야 하는 구성원들로 하여금 오히려 혼란을 가중시킬 수 있기 때문에 수정 주기에 대한 신중한 판단이 요구된다.

H1a. 보안정책의 깊이/명확성은 보안정책 지속적 준수 태도에 정의 영향을 미칠 것이다.

H1b. 보안정책의 깊이/명확성은 주관적 규범에 정의 영향을 미칠 것이다.

H1c. 보안정책의 깊이/명확성은 인지된 행위통제에 정의 영향을 미칠 것이다.

H1d. 보안정책의 깊이/명확성은 인지된 보안정책 준수비용에 부의 영향을 미칠 것이다.

간결성(Brevity)은 작성된 보안 정책의 장황한지(verbosity) 여부를 나타낸다[18]. 정보보안 정책은 짧고 읽기 쉬워야 한다[23]. 일반적으로 정보보안 정책은 1페이지에서 5페이지 사이가 읽기 좋은 형태이다. 만약 정책이 너무 길게 작성된다면, 조직 내 구성원들은 보안정책을 읽기 꺼려할 수 있다[23]. 또한 잘 작성된 보안 정책은 중복(redundancy), 장황함(wordiness), 전문용어(jargon)의 과도한 사용, 문장의 애매함(evasiveness), 완곡어법(circumlocution)의 사용이 적어야 한다[18].

H2a. 보안정책의 간결성은 보안정책 지속적 준수 태도에 부의 영향을 미칠 것이다.

H2b. 보안정책의 간결성은 주관적 규범에 부의 영향을 미칠 것이다.

H2c. 보안정책의 간결성은 인지된 행위통제에 부의 영향을 미칠 것이다.

H2d. 보안정책의 간결성은 인지된 보안정책 준수비용에 정의 영향을 미칠 것이다.

인간에 의해 발생하는 사고(Human Error)에 대해 다루는 경우 인간 행위에 대한 이해가 필요하다. 그동안 이를 위해 여러 가지 접근법이 존재하였으나 정보보안 상황에서 인간의 행위를 설명하기 위해 가장 많이 사용된 것은 Fishbein and Ajzen(1975)에 의해 소개된 합리적 행위 이론(Theory of Reasoned Action)으로 정보시스템 보안 정황에서 성공적으로 응용되어왔다[5]. 합리적 행위이론은 인간이 어떠한 행위를 수행하거나 수행하지 않는 행위의도가 실제 행위의 매개역할을 함을 제안하였다[27]. 본 모형은 행위 의도에 영향을 미치는 두 가지 요인에 대해 소개하였는데 하나는 행위에 대한 태도(attitude)와 다른 하나는 주관적 규범(subjective norm)이다. 태도

란 행위가 좋은지 혹은 바쁜지에 대한 판단을 말한다[1]. 만약 행위의 결과가 긍정적이라고 인식될 경우 개인은 긍정적 태도를 형성하게 된다[40]. 주관적 규범은 개인이 특정한 행위를 수행하거나 하지 않는데 영향을 미치는 사회적 압력에 대한 영향을 말한다[1]. 따라서 주관적 규범은 개인의 사회적 울타리 안에서 자신에게 영향을 미치는 사람들에 의해 특정한 행위가 수용되고 독려될지 여부를 결정한다. 따라서 자신의 주변인들이 특정한 행위가 긍정적이라고 고려할 경우 개인은 그들의 긍정적 사회적 규범을 수용하게 된다[40].

Ajzen(1991)은 이후 계획된 행위 이론(Theory of Planned Behavior)을 소개하였는데 본 인론에서는 기존의 합리적 행위이론에서 개인의 행의 의도에 직접적 영향을 미치는 제 3의 요인인 인지된 행위 통제(perceived behavioral control)를 제안하였다. 인지된 행위 통제란 주어진 행위를 수행할 수 있는 능력 수준에 대한 개인의 기대, 필요 자원을 가지고 있는지 여부, 직면한 장벽을 극복할 수 있는 능력 등을 말한다[2]. 따라서 행위에 대한 충분한 통제 능력이 있다고 믿고 있는 개인의 경우 자신의 의도를 실현할 가능성이 높다[40].

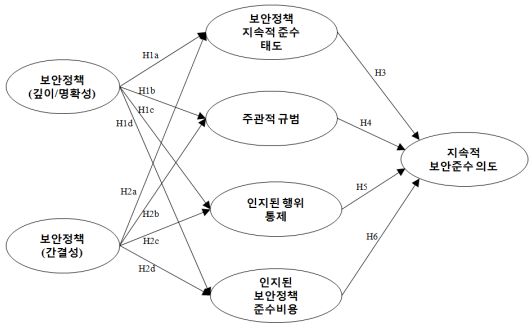
기존 학자들은 정보보안 관련 연구에서 계획된 행위 이론이 윤리적/비윤리적 행위를 예측하는데 합리적 행위 이론보다 더 유용하다고 주장하였다. Chang(1998)은 이 두 가지 사회 심리학 이론을 비윤리적 행위를 예측하는데 적용해보았다. 그는 연구결과에서 계획된 행위 이론이 합리적 행위이론보다 더 비윤리적 행위를 예측하는데 적합하다고 제시하였다. Loch and Conger(1996)도 합리적 행위이론을 활용하여 윤리적 의사결정 과정을 설명하고자 하였으나 그들은 결국 합리적 행위이론이 윤리적 의사결정을 설명하기에는 부족하다는 것을 실증분석을 통해 제시하였다. 다른 연구자들 역시 동일한 결론에 도달하였다[34][35]. 따라서 본 연구에서는 계획된 행위 이론을 사용하여 정보보안 정책 준수의도를 설명하고자 하였다. 하지만 본 이론은 윤리적 행위를 위해 개발된 것은 아니기 때문에[5], 정보보안관련 연구모형의 설명력을 향상시키기 위해 관련 변수의 포함이 필요하다. 따라서 본 연구에서는 인지된 보안 정책 준수비용을 포함하였다.

보안 정책 준수비용(Response Costs)이란 조직의 정보보안 정책을 준수하기 않을 경우 개인에게 기대되는 긍정적 결과(positive outcomes)를 말한다. 개인은 정보보안 정책을 준수함에 있어서 시간과 비용절감이라는 비용이 발생한다. Herath and Rao(2009)는 구성원들이 보안 정책을 준수하지 않는 이유 중 하나는 불편함을 초래하기 때문이라고 주장하였다. Chan et al.(2005)은 구성원들이 보안정책을 준수하는 것은 업무생산성과의 상충관계가 발생할 수 있다고 주장하였다. 따라서 다음의 가설을 제시할 수 있다.

H3. 보안정책 지속적 준수태도는 지속적 보안준수 의도에 정의 영향을 미칠 것이다.
H4. 주관적 규범은 지속적 보안준수 의도에 정의 영향을 미칠 것이다.
H5. 인지된 행위 통제는 지속적 보안준수 의도에 정의 영향을 미칠 것이다.
H6. 인지된 보안정책 준수비용은 지속적 보안준수 의도에 정의 영향을 미칠 것이다.

지금까지 제시한 가설을 중심으로 연구모형을 도식화하면 <그림 1>과 같다.

연구모형에서 정보보안 정책의 효과성을 나타내는 세 가지 차원을 깊이/명확성, 간결성 등 두 개의 외생변수로 구성하였다. Goel and Chengalur-Smith(2010)의 연구에서 처음 제시된 세 가지 차원은 서로 구분된다고 제시되었으나 실증분석 결과 세 가지 차원으로 보기에는 다소 무리가 있는 것으로 나타났다. 이들의 연구 결과에 따르면 탐색적 요인분석에서는 세 가지 차원이 구분되기는 하였으나 상관관계 분석에서 깊이와 명확성이 부의 상관관계가 존재하였고 이에 대한 충분한 설명이 부족하였다. 또한 본 연구에서도 Pretest에서 세 가지 차원을 모두 측정하였으나 깊이와 명확성이 하나의 요인으로 도출되었다. 따라서 이들 차원간의 명확한 구분이 쉽지 않기 때문에 이를 Pretest 결과를 기준으로 하나의 외생변수로 구성하였다.



[그림 1] 연구모형

3. 분 석

본 연구는 설문 조사법을 활용하여 데이터를 수집하였다. 수집된 데이터에 대한 기초 통계량 분석은 SPSS v19를 활용하였고 측정모형(measurement model)과 구조모형(structural model)에 대한 분석은 AMOS v19를 활용하였다.

표본 수집을 위해 ITSMF(Information Technology Service Management Forum) Korea의 회원사의 CIO를 대상으로 미리 사전에 본 설문에 대한 목적을 설명한 뒤 설문에 참여의사를 문의하였으며, 참여 의사를 밝힌 관계자를 중심으로 설문을 배포하였다. 핵심 관계자는 설문 배포과정에서 자사 내 각 부서에 설문이 최대한 고르게 배포되도록 하였다. 배포된 설문은 우편과 이메일을 통해 수집되었다. ITSMF Korea는 IT 서비스 관리와 관련되어 유일하게 국제적으로 인정되는 독립조직인 ITSMF의 한국지사로 회원제에 의해 운영되는 비영리단체이다.

설문은 31개의 기업에 약 300부가 배포되었으며 이 중 273부가 회수되었다(회수율 91%). 이중 결측치(missing value)를 포함하고 있는 9부를 제외하고 총 264부를 최종 분석에 사용하였다.

〈표 1〉 응답자 특성 분석

구분	세부구분	빈도	비율(%)
성별	남성	192	72.7
	여성	70	26.5
	무응답	2	0.8
연령	18-24	2	0.8
	25-34	115	43.6
	35-44	119	45.1
	45-54	28	10.6
교육수준	고등학교 졸업	2	0.8
	2년제 대학 졸업	15	5.7
	4년제 대학 졸업	175	66.3
	석사	59	22.3
	박사	8	3.0
	무응답	5	1.9
현 직장 근속 년수(평균)		6.7152년	
직위	상위 관리자	9	3.4
	기술직	60	22.7
	관리직/사무직	92	34.8
	중간 관리자	64	24.2
	전문직	31	11.7
	무응답	8	3.0
	합계	264	100%

3.1 요인분석

요인분석의 목적은 공통요인(common factor)을 식별하는 것이기 때문에 모든 요인 즉, 각각의 요인들의 공통분산(common variance)과 고유분산(unique variance)을 고려하는 주성분분석을 요인분석이라 보기 어렵다[11][24]. 하지만 요인분석 절차상에서 몇 개의 요인을 최종요인으로 보유해야 하는가에 대한 문제점이 있다. 이를 선택할 수 있는 여러 가지 기준이 있으나 가장 많이 사용되는 방법은 고유값(eigenvalue)>1 초과기준이다[20][21].

카이저 준거(Kaiser's Criterion)는 고유치 최소 1을 갖는 요인들을 결정하는 기준으로 오직 주성분석에서만 사용된다[24]. 따라서 주성분분석을 탐색적 요인분석을 위해 사용하기도 한다. 따라서 본 연구에서는 주성분분석을 통해 요인구조를 탐색하였다.

탐색적 요인분석을 위해 필요한 표본에 대한 기준은 크게 두 가지로 구분되는데 하나는 질적 기준과 다른 하나는 양적 기준이다. 질적 기준으로는 KMO(Kaiser-Meyer-Olkin Measure)의 표본적합성과 Bartlett의 구형성이 있다. 이 두 지표는 모두 수집된 데이터가 요인분석을 수행하기에 적합한 상관관계 행렬을 도출할 수 있는지를 평가하는 질적 평가 기법이다. 일반적 기준에 따르면 KMO는 0.7이상 되어야 하며 Bartlett의 구형성은 유의해야 한다[19]. 본 연구의 경우 KMO가 0.897로 나타났으며, Bartlett의 구형성은 유의하게 나타났다($p<0.000$). 양적 기준으로 논의된 요인 분석을 위한 필요 표본 수(N)로 50은 매우 열악한 수준, 100은 열악한 수준, 200은 적정한 수준, 300은 좋은 수준, 500은 매우 좋은 수준, 1,000은 훌륭한 수준이다[21]. 본 연구에서 요인분석을 위해 사용한 표본 수는 264개로 적정 수준인 200이상으로 요인분석에 무리가 없는 것으로 판단할 수 있다.

많은 경우 표본 수에 대한 기준에 치중할 경우 변수의 공통성(h^2), 요인적재값의 정도와 같은 데이터의 특성에 대해 간과하기 쉽다[19]. 따라서 이에 대한 고려가 반드시 수반되어야 한다. 경험적 기준에 따르면 요인 적재값은 0.5이상 되어야 한다[11][19][21][24]. 본 연구에서는 최소값이 0.539로 나타나 이 기준을 충족하고 있는 것으로 나타났다. 또한 본 기준에 따라 요인을 추출한 결과 총 7개의 요인이 도출되었다. 또한 도출된 각각의 요인들의 공통성(communality = h^2)은 최소 0.519로 모든 항목이 최소 50%이상의 설명력을 가지고 있는 것으로 나타났다[19].

〈표 2〉 요인분석 결과

	주성분분석							h^2	확인적 요인 분석				
	1	2	3	4	5	6	7		λ	표준오차	t값	p값	R^2
SPE1	**.831**	.083	.179	.065	-.025	.048	.017	.737	0.802	0.055	16.92	.000***	0.643
SPE2	**.834**	.156	.179	.053	-.041	.093	-.014	.765	0.785	0.054	16.243	.000***	0.616
SPE3	**.837**	.144	.183	.153	-.055	.158	.106	.818	0.868	0.052	19.696	.000***	0.753
SPE4	**.848**	.180	.129	.032	-.096	.083	.015	.786	0.82	0.052	17.601	.000***	0.673
SPE5	**.836**	.172	.127	.036	-.110	.103	-.003	.768	0.822	0.053	17.379	.000***	0.676
SPE6	**.792**	.166	.176	.122	-.088	.093	.058	.721	0.858	0.049	19.393	.000***	0.737
SPE7	**.765**	.206	.061	.271	-.053	.124	.147	.744	0.871	0.049	19.94	.000***	0.758
SPE8	**.795**	.170	.174	.163	-.138	.074	.185	.777	0.879	-	-	-	0.773
SPE9	.177	-.031	.110	.056	.035	-.028	**.830**	.739	0.785	0.107	11.753	.000***	0.616
SPE10	.139	.098	-.002	.094	.103	.103	**.873**	.822	0.941	0.116	12.368	.000***	0.886
SPE11	-.002	.058	-.043	-.062	.181	-.015	**.879**	.814	0.801	0.081	15.401	.000***	0.642
SPE12	.021	.077	-.044	-.067	.152	.034	**.808**	.690	0.692	-	-	-	0.479
PB1	-.099	.012	-.079	-.113	**.685**	-.075	.124	.519	0.561	0.057	10.251	.000***	0.315
PB2	-.073	-.025	-.047	-.042	**.908**	-.056	.074	.844	0.858	0.045	21.057	.000***	0.736
PB3	-.109	-.003	-.015	-.104	**.910**	.002	.059	.855	0.87	0.043	21.829	.000***	0.756
PB4	-.055	-.012	-.052	-.018	**.922**	-.062	.106	.872	0.963	0.038	28.399	.000***	0.928
PB5	-.099	-.010	-.075	-.023	**.872**	-.109	.108	.800	0.916	-	-	-	0.839
APC1	.165	.119	.487	**.548**	-.079	.376	-.022	.727	0.744	-	-	-	0.554
APC2	.145	.065	.421	**.539**	-.038	.390	-.043	.648	0.743	0.052	18.878	.000***	0.553
APC5	.133	.006	.257	**.844**	-.086	.191	.023	.841	0.859	0.066	18.005	.000***	0.737
APC6	.136	.025	.142	**.884**	-.060	.183	.020	.859	0.904	0.083	15.385	.000***	0.817
APC7	.161	.032	.293	**.826**	-.092	.254	.017	.869	0.963	0.075	16.649	.000***	0.928
APC8	.155	.030	.208	**.854**	-.093	.243	-.022	.865	0.917	0.074	16.15	.000***	0.841
SN1	.205	.025	**.817**	.243	-.026	.230	-.018	.823	0.822	-	-	-	0.675
SN2	.198	.118	**.851**	.263	-.040	.208	-.010	.892	0.89	0.033	30.811	.000***	0.792
SN3	.272	.208	**.800**	.234	-.087	.210	.036	.865	0.927	0.057	19.625	.000***	0.859
SN4	.274	.193	**.828**	.209	-.113	.195	.020	.893	0.945	0.056	20.291	.000***	0.892
SN5	.311	.162	**.779**	.260	-.107	.215	.011	.856	0.933	0.053	19.849	.000***	0.871
PBC1	.174	**.664**	.340	.101	-.029	.155	.055	.625	0.569	-	-	-	0.324
PBC2	.134	**.673**	.341	.122	-.065	.143	.090	.635	0.575	0.054	18.683	.000***	0.331
PBC3	.043	**.743**	.132	.026	-.080	.107	.202	.630	0.639	0.139	8.536	.000***	0.408
PBC4	.134	**.905**	-.033	-.016	.017	.030	.022	.840	0.881	0.163	10.337	.000***	0.776
PBC5	.120	**.912**	.002	-.028	.037	.005	-.008	.849	0.962	0.174	10.755	.000***	0.926
PBC6	.113	**.913**	.048	-.026	.049	.019	-.003	.851	0.958	0.167	10.772	.000***	0.918
PBC7	.258	**.829**	.015	.063	-.004	-.032	-.042	.761	0.804	0.157	9.824	.000***	0.646
PBC8	.262	**.830**	.070	.033	-.005	.012	-.003	.764	0.812	0.165	9.883	.000***	0.659
PCI1	.161	.114	.301	.275	-.100	**.826**	.042	.899	0.939	-	-	-	0.881
PCI2	.171	.064	.288	.300	-.096	**.832**	.042	.910	0.957	0.029	34.229	.000***	0.916
PCI3	.173	.064	.261	.315	-.098	**.843**	.050	.924	0.887	0.035	26.351	.000***	0.786
PCI4	.169	.089	.212	.287	-.101	**.855**	.014	.905	0.847	0.04	23.213	.000***	0.718
고유값	13.554	5.425	4.011	3.348	2.364	1.667	1.432		SPEa	SPEb	PB	APC	SN	PBC	PCI
설명분산	33.884	13.562	10.027	8.370	5.911	4.168	3.581	AVE	.694	.656	.715	.738	.818	.623	.825
누적분산	33.884	47.446	57.473	65.843	71.754	75.922	79.503	α	.952	.887	.925	.939	.962	.939	.968
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.							897	CR	.941	.883	.924	.944	.957	.927	.950
Bartlett's Test of Sphericity				Approx. Chi-Square			11905.116		Extraction Method: Principal Component Analysis.						
				Degree of Freedom			780		Rotation Method: Varimax with Kaiser Normalization.						
				Significance			.000		Rotation converged in 6 iterations.						

Note. SPEa: 보안정책(깊이/명확성), SPEb: 보안정책(간결성), PB: 인지된 보안정책 준수비용, APC: 보안정책지속적 준수태도, SN: 주관적 규범, PBC: 인지된 행위통제, PCI: 지속적 보안준수 의도

Note. ***$t_{0.001}$=3.291

Note. h^2 = communality

적절한 수준의 신뢰성을 가지고 있지 못하는 변수들은 의미있는 요인을 형성할 가능성이 낮다[24]. 따라서 신뢰성에 대한 평가가 필요하다. 본 연구에서는 신뢰성 평가를 위해 가장 많이 사용되는 방법인 내적 일관성(internal consistency)을 평가하는 Cronbach' α를 확인하였는데 일반적 기준에 따르면 새로이 개발된 지표의 경우 0.6이상 되어야 만족할 만한 수준이라 볼 수 있다[31]. <표 2>에 나타나 있듯이 Cronbach' α의 최소값이 0.887로 나타나 위의 기준을 충족하고 있다. 또한 내적 일관성을 평가하는 또 다른 기준인 복합신뢰성(CR, Composite Reliability)을 평가하여 신뢰성을 평가하였는데, 본 값도 최소값이 0.883으로 나타나 측정지표들이 신뢰성이 있다

〈표 3〉 상관관계 분석

	Mean	Std. Dev	편상관관계 분석 및 공통방법 분석 검정						상관관계 분석						
			SPEa	SPEb	PB	APC	SN	PBC	SPEa	SPEb	PB	APC	SN	PBC	PCI
SPEa	4.4242	1.22637	.952				대각선 값은		.833						
SPEb	3.8750	1.15195	.165	.887			Cronbahc'sα 임		.168**	.810					
PB	3.5614	1.32924	-.192	.224	.925				-.199**	.221**	.845				
APC	5.8283	1.00410	.375	.022	-.197	.939			.382**	.025	-.202**	.859			
SN	5.4159	1.18901	.496	.048	-.190	.639	.962		.499**	.050	-.193**	.641**	.905		
PBC	4.0710	1.23072	.389	.116	-.043	.172	.329	.939	.393**	.118	-.047	.177**	.332**	.790	
PCI	5.7462	1.15277	.372	.071	-.208	.661	.595	.218	.380**	.074	-.213**	.664**	.597**	.223**	.909
r			.135	.031	-.064	.091	.065	.066	**. Correlation is significant at the 0.01 level (2-tailed).						
r^			.372	.071	-.208	.661	.595	.218	대각선 값은 AVE의 제곱근 값을 나타냄						

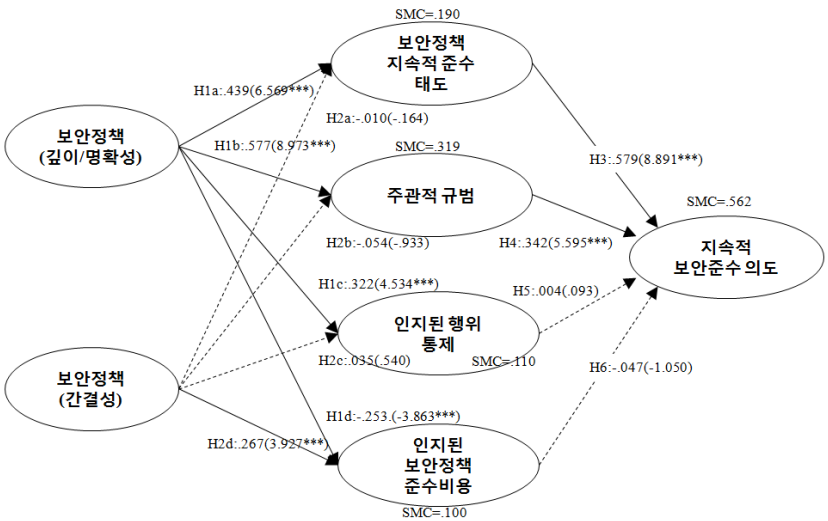
고 볼 수 있다.

3.2 공통방법오류

독립변수와 종속변수를 하나의 도구로 측정하였기 때문에 수집된 데이터가 공통방법오류(Common Method Bias)의 영향에서 자유로울 수 없다. 따라서 세 가지 방법을 통해 공통방법오류 여부를 측정하였다. 첫째, Harman의 일요인(Harman's One-factor test) 검정을 실시하여 데이터 내 분산의 대부분이 하나의 요인에 의해 설명되는지 여부를 분석해 보았다[33].

<표 2>에서 볼 수 있듯이 요인회전 전 탐색적 요인분석에서 총 설명력은 75.922로 요인분석이 갖아야 할 설명력인 75%이상을 나타내고 있으며[38], 가장 많은 설명력을 차지하는 요인의 설명분산은 33.884로 절반이하로 상대적으로 높지 않게 나타났다. 다음으로 잠재변수간 상관관계 계수 높은 경우(0.9이상) 공통방법오류의 단서가 되는데[32] <표 3>에 나타나 있듯이 가장 높은 상관관계 계수가 0.664로 높은 수준은 아니기 때문에 공통방법오류의 문제가 심각하지 않은 것으로 볼 수 있다[30]. 주의할 것은 잠재변수간의 상관관계 계수(r)가 0.7이상[7] 혹은 0.8이상[4] 될 경우 다중공선성(multi-collinearity)의 문제가 발생할 수 있다. 이미 언급한 바와 같이 가장 높은 상관관계 계수가 0.664로 이 기준을 초과는 값이 관측되지 않기 때문에 다중공선성의 문제도 심각하지 않은 것으로 볼 수 있다.

마지막으로 최근 많은 연구에서 공통방법오류의 문제를 사후적으로 분석하기 위해 사용하는 Lindell and Whitney(2001)의 마커 변수 검정법을 사용하였다. Lindell and Whitney(2001)의 마커 변수 검정은 모형의 주요 잠재 변수간의 상관관계를 조정하기 위해 이론적으



χ^2=1429.214(df=709, p<0.001), χ^2/df=2.016, GFI=0.795, RMSEA=0.062, NFI=0.887, NNFI=0.933, CFI=0.940, AGFI=0.763, PGFI=0.688, PNFI=0.807, PCFI=0.854

[그림 2] 구조모형분석결과

〈표 4〉 가설검정 결과

	β	Std. Error	t-value	p value	Support
H1a. 보안정책의 깊이/명확성 → 보안정책 지속적 준수 태도 (+)	0.439	0.042	6.569	0.000***	지지
H1b. 보안정책의 깊이/명확성 → 주관적 규범 (+)	0.577	0.056	8.973	0.000***	지지
H1c. 보안정책의 깊이/명확성 → 인지된 행위 통제 (+)	0.322	0.045	4.534	0.000***	지지
H1d. 보안정책의 깊이/명확성 → 인지된 보안정책 준수비용 (-)	-0.253	0.074	-3.863	0.000***	지지
H2a. 보안정책의 간결성 → 보안정책 지속적 준수 태도 (-)	-0.01	0.056	-0.164	0.869	기각
H2b. 보안정책의 간결성 → 주관적 규범 (-)	-0.054	0.072	-0.933	0.351	기각
H2c. 보안정책의 간결성 → 인지된 행위 통제 (-)	0.035	0.059	0.54	0.59	기각
H2d. 보안정책의 간결성 → 인지된 보안정책 준수비용 (+)	0.267	0.11	3.927	0.000***	지지
H3. 보안정책 지속적 준수태도 → 지속적 보안준수 의도 (+)	0.579	0.082	8.891	0.000***	지지
H4. 주관적 규범 → 지속적 보안준수 의도 (+)	0.342	0.056	5.595	0.000***	지지
H5. 인지된 행위 통제 → 지속적 보안준수 의도 (+)	0.004	0.057	0.093	0.926	기각
H6. 인지된 보안정책 준수비용 → 지속적 보안준수 의도 (+)	-0.047	0.032	-1.05	0.294	기각

*$t_{0.05}$=1.960, **$t_{0.01}$=2.576, ***$t_{0.001}$=3.291

로 관련성이 낮은 마커 변수를 사용하는 방법이다. 마커 변수가 연구에서 제시한 다른 주요 잠재변수와 이론적으로 관련성이 낮아야 하는 이유는, 높은 상관관계는 공통 방법 편의에 의한 오염으로 발생하기 때문이다. 본 연구에서는 다른 변수와의 이론적 연관성이 매우 적은 변수인 외부활동 선호도(α= 0.95)를 마커 변수로 사용하였다. <표 3>에 나타나있듯이 주요 잠재변수간의 평균 상관관계 계수는 낮았으며 유의하지도 않았기 때문에 공통 방법 편의의 증거를 찾아 볼 수 없었다.

3.3 측정모형 분석

다음으로 평균분산추출(Average Variance Extracted, AVE)을 평가하여 집중 타당성(convergent validity)을 검증하였는데, 일반적 기준에 의하면 모든 값이 0.5이상이 되어야 한다[17]. 본 연구의 경우 최소값이 0.623으로 나타나 잠재개념에 의해 설명되는 분산이 50%이상 되는 것을 확인할 수 있다.

다음으로 AVE의 제곱근 값과 구성개념들 간의 상관관계 계수를 비교하여 판별타당성(discriminant validity) 검증을 수행하였다. <표 3>에 나타난 바와 같이 모든 AVE 제곱근 값이 구성개념간의 상관관계 계수보다 높게 나타나 각 구성개념이 구별됨을 알 수 있다. 이러한 결과를 통해 개념 타당성(construct validity)도 확보되었다고 볼 수 있다. 일반적으로 표준 요인 적재치가 0.5 이상이고, AVE값이 0.5이상이며, 이 값이 구성개념간의 상관관계 계수의 제곱 값 보다 크며, 복합신뢰성이 0.7이상일 경우 개념 타당성이 존재한다고 볼 수 있다[36].

3.4 구조모형 분석

마지막으로 수립된 가설검정을 위해 구조모형을 분석하였다. 검정 전에 수집된 데이터와 모형간의 적합성을 평가하기 위해 모형 적합도(Model Fit Indices)를 평가하였다. 일반적으로 모형적합도 분석을 위해 20여 가지 이상의 지표들이 개발되었으며, 절대적인 지표는 존재하지 않는다. 그렇기 때문에 모든 기준이 충족되어야 하는 것은 아니다. <그림 2>에 제시한 바와 같이 대부분의 기준이 선행연구에서 제안한 기준에 근사하거나 상회하기 때문에 연구모형을 검정하는데 문제가 없다고 판단된다.

검정 결과를 정리하면 다음과 같다. 첫째, 보안정책의 깊이/명확성은 보안정책 지속적 준수태도(β=0.439, p<0.001), 주관적 규범(β=0.577, p<0.001), 인지된 행위통제(β=0.322, p<0.001), 인지된 보안정책 준수비용(β=-0.253, p<0.001)에 유의한 영향을 미치는 것으로 나타났다.

다음으로 보안정책의 간결성은 인지된 보안정책 준수비용에만 유의한 영향을 미치는 것으로 나타났다(β=0.267, p<0.001). 반면 보안정책의 간결성은 보안정책 지속적 준수태도(β=-0.01), 주관적 규범(β=-0.054), 인지된 행위통제(β=0.035)에 통계적으로 유의한 영향을 미치지 않는 것으로 나타났다.

다음으로 계획된 행위이론에서 제시한 행위 의도에 영향을 미치는 선행요인 중 보안정책 지속적 준수태도(β=0.579, p<0.001)와 주관적 규범(β=0.342, p<0.001)만 지속적 보안준수 의도에 유의한 영향을 미치는 것으로 나타났다. 반면 인지된 행위 통제(β=0.004)와 인지된 보안정책 준수비용(β=-0.047)은 지속적 보안준수 의도에 통계적으로 아무런 영향을 미치지 않는 것으로 나타났다.

이는 기존 연구에서 제시한 바와 같이 계획된 행위이론(TPB)보다는 합리적 행위 이론(TRA)이 본 연구에서는 더 적합하다는 것을 알 수 있다.

4. 결 론

본 연구는 그동안 논의되지 않았던 보안정책의 형식이 보안정책 준수에 미치는 영향을 살펴보고자 수행되었다. 보안 정책의 성공을 결정하는 요인은 보안 정책의 내용과 형식이다. 내용이란 무엇이 쓰여야 하는지와 관련된 것이고 형식이란 어떻게 읽혀지겠는가와 관련된다.

그동안의 연구는 내용과 관련되었으나 보안 정책을 준수해야 하는 구성원들의 입장에서는 자신들이 읽게 되는 보안정책의 형식도 매우 중요한 요소 중 하나이다. 따라서 형식에 대한 연구가 필요하다.

분석결과 보안정책의 깊이/명확성은 보안정책 지속적 준수태도, 주관적 규범, 인지된 행위 통제, 인지된 보안정책 준수비용에 유의한 영향을 미치는 것으로 나타났다. 이는 기업의 보안 정책이 모호하지 않고 이해하기 쉬운 경우 그리고 정책의 내용이 현실적이고 포괄적인 경우 보안 정책의 준수태도를 유도할 수 있다는 것을 말해준다. 또한 이 경우 보안 정책이 모든 구성원들에게 널리 인지되기 때문에 주변인들이 정보보안의 중요성에 대해 보다 쉽게 인지하게 된다. 뿐만 아니라 개인이 보안정책을 제대로 인지할 경우 보안 상황을 인지하고 통제할 수 있는 능력이 있다고 느끼는 것으로 나타났다. 마지막으로 개인이 보안 정책에 대해 인지하고 있을 경우 보안 정책을 준사하는 것이 비용이 아니라 자신이 속한 조직을 위해 필요한 행위라는 것을 인지하는 것으로 나타났다.

다음으로 보안 정책의 간결성 인지된 보안 정책준수 비용에 유의한 영향을 미치는 것으로 나타났다. 이는 보안 정책이 조직 구성원들에게 제대로 인지될 경우와는 반대로 보안 정책이 불필요하게 길거나, 장황하거나 반복적인 어구로 쓰여 있을 경우 조직원들이 보안 정책을 제대로 인지하지 못하여 보안 정책을 준수하는 행위가 업무의 생산성과 상충관계가 있다고 인식하는 것을 알 수 있다.

마지막으로 보안 정책 준수의도에 영향을 미치는 요인은 보안정책 준수태도와 주관적 규범으로 나타났다. 보안 정책을 준수하는 것이 기업에 긍정적인 결과를 유발할 것이라고 판단될 경우, 그리고 주변인들이 보안 정책을 준수하는 것을 중요하게 생각할 경우 보안정책을 준수할 의도가 발생한다는 것을 알 수 있다. 이는 기존 연구에서 주장한 계획된 행위 이론보다는 그동안 유용성이 낮다고 판단한 합리적 행위 이론이 더 적합하다는 것을 알 수 있다.

따라서 기업 입장에서 보안 정책을 수립할 경우 정책을 준수하는 구성원들이 읽기 쉽고, 이해하기 쉬운 반면 보안 행위를 실행하기 위해 필요한 구체적인 내용을 포함하고 있을 경우 보안 정책의 준수를 유발할 수 있다는 것을 알 수 있다. 뿐만 아니라 보안 정책을 내용 중심이 아니라 내용과 형식이 정책 준수자의 입장에서 작성되어야 궁극적으로 의도한 보안정책의 목적을 달성할 수 있음을 알 수 있다.

본 연구는 이상과 같은 실증적 의미가 있음에도 불구하고 다음의 한계점도 존재한다. 첫째는 본 연구가 설문지법을 사용함과 동시에 결과 변수와 영향변수를 한 시점에 동일한 응답자에게 응답하도록 함에 따라 공통방법오류의 문제가 발생할 가능성이 있다. 물론 사후적 분석기법을 통해 공통방법오류 존재여부를 평가하였지만 완전한 해결책은 되지 않는다. 이를 완전히 해결하기 위해서는 결과변수와 원인변수에 대해 구분하고 각각 다른 응답자를 대상으로 데이터를 수집해야 한다. 다음으로 보안은 다양한 통제 변수에 의해 영향을 받을 수 있다. 예를 들어 직급이나, 성별이나, 업무 형태나 연령 등에 의해 영향을 받을 수 있다. 따라서 이에 대한 추가적인 고려가 필요하다. 마지막으로 선행 연구에서는 보안 정책이 세 가지 차원으로 구분된다고 하였으나 본 연구에서는 두 개의 차원으로만 구분되었다. 선행 연구에서는 세 가지 차원 간에 음의 상관이 존재하기 때문이라 하였으나 본 연구에서는 두 개의 차원이 하나로 나타나는 결과를 보였다. 따라서 그 이유에 대해 규명하는 것도 매우 의미가 있을 것으로 판단된다.

참 고 문 헌

[1] Ajzen, I., & Fishbein, M. (1980). Understanding Attitudes and Predicting Social Behavior, Englewood Cliff, NJ: Prentice-Hall.

[2] Ajzen, I. (1991). The Theory of Planned Behavior, Organizational Behavior and Human Decision

Processes, 50(2), 179-211.

[3] Bagozzi, R. P., & Yi, Y. (2012). Sepecification, Evaluation, and Interpretation of Structural Equation Models, Journal of the Academy of Marketing Science, 40, 8-24.

[4] Bagozzi, R. P., Yi. Y., & Phillips, L. W. (1991). Assessing Construct Validity in Organizational Research, Administrative Science Quarterly, 36(3), 421-458.

[5] Banerjee, D., Cronan, T. P., & Jones, T. W. (1998). Modeling IT Ethics: A Study in Situational Ethics, MIS Quarterly, 22(1), 31-59.

[6] Baskerville, R., & Siponen, M. (2002). An Information Security Meta-Policy for Emergent Organizations, Logistics Information Management, 15(5/6), 337-346.

[7] Cassel, C., Hackl, P., & Westlund, A. H. (1999). Robustness of Partial Least-Squares Method for Estimating Latent Variable Quality Structures, Journal of Applied Statistics, 26(4), 435-446.

[8] Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior, Journal of Information Privacy & Security, 1(3), 18-41.

[9] Chang, M. K. (1998). Predicting Unethical Behavior: A Comparison of the Theory of Reasoned Action and the Theory of Planned Behavior, Journal of Business Ethics, 1825-1834.

[10] Chin, W. (1998). Issues and Opinions on Structural Equation Modeling, MIS Quarterly, 22(1), vii-xvi.

[11] Costello, A. B., & Osborne, J. W. (2005). Best Practices in Exploratory Factor Analysis: Four Recommendations for Getting the Most from Your Analysis, Practical Assessment, Research & Evaluation, 10(7), 1-9.

[12] D'Arcy, J., & Hovav, A. (2007). Deterring Internal Information Systems Misuse, Communications of the ACM, 50(10), 113-117.

[13] Dhillon, G., & Backhouse, J. (1996). Risks in the Use of Information Technology Within Organizations, International Journal of Information Management, 16(1), 65-74.

[14] Dhillon, G. (1997). Managing Information Systems Security, MacMillan Press, London, England.

[15] Fishbein, M., & Ajzen, I. (1975). Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research, MA, Addison-Wesley.

[16] Foltz, C. B., Schwager, P. H., & Anderson, J. E. (2008). Why Users (Fail to) Read Computer Usage Policies, Industrial Management & Data Systems, 108(6), 701-712.

[17] Fornell, C., & Larcker, D. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error, Journal of Marketing Research, 18(1), 39-50.

[18] Goel, S., & Chengalur-Smith, I. N. (2010). Metrics for Characterizing the Form of Security Policies, Journal of Strategic Information Systems, 19, 281-295.

[19] Hair, Jr. J. F., Black, W. C., Babin, B. J., & Anderson, R. E.(2010). Multivariate Data Analysis, 7th ed., Upper Saddle River, NJ: Prentice Hall.

[20] Hayton, J. C., Allen, D. G., & Scarpello, V. (2004). Factor Retention Decisions in Exploratory Factor Analysis: A Tutorial on Parallel Analysis, Organizational Research Methods, 7(2), 191-205.

[21] Henson, R. K., & Roberts, J. K. (2006). Use of Exploratory Factor Analysis in Published Research: Common Errors and Some Comment on Improved Practice, Educational and Psychological Measurement, 66(3), 393-416.

[22] Herath, T., & Rao, H. R. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations, European Journal of Information Systems, 18(2), 106-125.

[23] Höne, K., & Eloff, J. H. P. (2002). Information Security Policy: What Do International Information Security Standards Say?, Computers & Security, 21(5), 402-409.

[24] Kahn, J. H. (2006). Factor Analysis in Counseling Psychology Research, Training, and Practice: Principles, Advances, and Applications, Counseling

Psychologist, 34(5), 684-718.

[25] Lee, J., & Lee Y. (2002). A Holistic Model of Computer Abuse within Organizations, Information Management & Computer Security, 10(2), 57-63.

[26] Lee, S. M., lee, S.-G., & Yoo, S. (2004). An Integrative Model of Compute Abuse Based on Social Control and General Deterrence Theories, Information and Management, 41(6), 707-718.

[27] Leonard, L. N. K., Cronan, T. P., & Kreie, J. (2004). What Influences IT Ethical Intentions- Planned Behavior, Reasoned Action, Perceived Importance, or Individual Characteristics?, Information and Management, 24, 177-187.

[28] Lindell, M. K., & Whitney, D. J. (2001). Accounting for Common Method Variance in Cross-Sectional Research Designs, Journal of Applied Psychology, 86(1), 114-121.

[29] Loch, K. D., & Conger, S. (1996). Evaluating Ethical Decision Maing and Computer Use, Communications of the ACM, 39(7), 74-83.

[30] Malhotra, N., Kim, S., & Patil, A. (2006). Common Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research, Management Science, 52(12), 1865-1883.

[31] Nunnally, J. C. (1967). Psychometric Theory, New York, NY: McGraw-Hill.

[32] Pavlou, P., Liang, H., & Xue, Y. (2007). Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective, MIS Quarterly, 31(1), 105-136.

[33] Podsakoff, P. M., MacKenzie, S. B., Lee, J., & Podsakoff, N. P. (2003). Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies, Journal of Applied Psychology, 88(5), 879-903.

[34] Randall, D. M. (1989). Taking Stock: Can the Theory of Reasoned Action Explain Unethical Conduct, Journal of Business Ethics, 8, 873-882.

[35] Randall, D. M., & Gibson, A. M. (1990). Methodology in Business Ethics: A Review and Critical Assessment, Journal of Business Ethics, 9, 457-471.

[36] Segars, A. H. (1997). Assessing the Unidimensionality of Measurement: A Paradigm and Illustration within the Context of Information Systems Research, Omega, 25(1), 107-121.

[37] Sterne, D. F. (1991). On the Buzzword 'Security Policy', Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, 219-230.

[38] Stevens, J. (1996). Applied Multivariate Statistics for the Social Sciences, 3rd ed., Mahwah, NJ: Lawrence Erlbaum.

[39] Straub, D. (1990). Effective IS Security: An Empirical Study, Information Systems Research, 1(3), 255-276.

[40] Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The Insider Threat to Information Systems and the Effectiveness of ISO17799, Computers & Security, 24, 472-484.

[41] Vance, A., & Siponen, M. (2012). IS Security Policy Violations: A Rational Coice Perspective, Journal of Organizational and End User Computing, 24(1), 21-41.

[42] Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory, Information & Management, 49, 190-198.

임 명 성

· 2002년 2월: 삼육대학교 경영정보학과(경영학사)
· 2004년 2월: 한국외국어대학교 경영정보대학원(MBA)
· 2011년 8월: 서강대학교 경영전문대학원(Ph.D.)
· 2011년 9월: 서강대학교 경영학부 대우교수
· 2012년 3월~현재: 삼육대학교 경영학과 조교수
· 관심분야: 정보보안, 서비스 시스템, 정보심리학
· E-Mail: msyim@syu.ac.kr

〈Appendix〉 설문문항

개념	항목	문항
보안정책 명확성	SPE1	우리 회사의 보안 정책은 이해하기 쉽다.
	SPE2	우리 회사의 보안 정책은 읽기 쉽다.
	SPE3	우리 회사의 보안 정책은 각각의 조항들을 명확하게 제시하고 있다.
	SPE4	우리 회사의 보안 정책은 일반적인 단어와 구문들로 쓰여져 있다.
	SPE5	우리 회사의 보안 정책은 참고자료(혹은 타인의 도움) 없이도 이해할 수 있다.
보안정책 깊이	SPE6	우리 회사의 보안 정책은 정책위반에 따른 법적 문제로부터 조직을 보호한다.
	SPE7	우리 회사의 보안 정책은 정책위반에 따른 법적 파급효과를 구체적으로 명시하고 있다.
	SPE8	우리 회사의 보안 정책은 정보보안에 필요한 모든 내용을 포함하고 있다.
보안정책 간결성	SPE9	우리 회사의 보안 정책은 내용이 길다.
	SPE10	우리 회사의 보안 정책은 각각의 조항들을 빽빽하게 제시하고 있다.
	SPE11	우리 회사의 보안 정책은 장황하다.
	SPE12	우리 회사의 보안 정책은 반복적 어구로 쓰여져 있다.
인지된 보안정책 준수비용	PB1	정보보안 정책을 따르지 않을 경우, 비용이 절감된다.
	PB2	정보보안 정책을 따르지 않을 경우, 업무 수행을 위한 시간이 절약된다.
	PB3	정보보안 정책을 따르지 않을 경우, 나의 업무 성과가 향상된다.
	PB4	정보보안 정책을 따르지 않을 경우, 나의 업무를 더욱더 빨리 끝낼 수 있다.
	PB5	정보보안 정책을 따르지 않을 경우, 정해진 시간 동안 더욱더 많은 일을 해낼 수 있다.
보안정책 지속적 준수태도	APC1	나에게 있어서, 우리 회사의 정보보안 정책을 지속적으로 따르는 것은?(중요하지 않다-중요하다)
	APC2	회사 내 나의 컴퓨터에서 정보보안 침해 사고가 발생하지 않도록 스스로 예방하는 것은?
	APC5	나에게 있어서, 우리 회사의 정보보안 정책을 지속적으로 따르는 것은?(잘못된 생각이다-좋은 생각이다)
	APC6	회사 내 나의 컴퓨터에서 정보보안 침해 사고가 발생하지 않도록 스스로 예방하는 것은?
	APC7	나에게 있어서, 우리 회사의 정보보안 정책을 지속적으로 따르는 것은?(바람직하지 않다-매우 바람직하다)
	APC8	회사 내 나의 컴퓨터에서 정보보안 침해 사고가 발생하지 않도록 스스로 예방하는 것은?
주관적 규범	SN1	우리 회사의 최고 경영자들은 내가 정보보안 정책을 따라야 한다고 생각한다.
	SN2	나의 상관은 내가 정보보안 정책을 따라야 한다고 생각한다.
	SN3	나의 동료는 내가 정보보안 정책을 따라야 한다고 생각한다.
	SN4	나에게 있어서 중요한 사람들은 내가 정보보안 정책을 따라야 한다고 생각한다.
	SN5	나의 행동에 영향을 미칠 수 있는 사람들은 내가 정보보안 정책을 따라야 한다고 생각한다.
인지된 행위통제	PBC1	나는 내 컴퓨터를 보안 사고로부터 보호할 수 있는 충분한 능력을 가지고 있다.
	PBC2	나는 내 컴퓨터를 보안 사고로부터 미연에 방지할 수 있는 충분한 능력이 있다.
	PBC3	나는 인가되지 않은 방법으로 나의 컴퓨터에 접근하는 것을 예방할 수 있다고 확신한다.
	PBC4	나는 누구의 도움 없이도 정보보안 침해를 식별할 수 있다.
	PBC5	나는 문서로 작성된 절차나 규칙이 없이도 정보 보안 침해를 식별할 수 있다.
	PBC6	나는 이전에 유사한 상황에 대한 경험 없이도 정보보안 침해를 식별할 수 있다.
	PBC7	나는 누구의 도움 없이도, 정보보안 사건발생 시 무엇을 해야 하는지 알고 있다.
	PBC8	나는 문서화된 절차나 규칙없이도 정보보안 침해 사건 발생 시 무엇을 해야 하는지 알고 있다.
지속적 보안준수 의도	PCI1	나는 우리 조직의 정보보안 정책을 지속적으로 따를 것이다.
	PCI2	나는 우리 조직의 정보시스템을 보호하기 위해 조직의 정보시스템 보안정책을 지속적으로 준수할 가능성이 높다.
	PCI3	나는 우리 회사의 정보 시스템을 접속할 때마다 정보보안 정책을 준수할 것이다.
	PCI4	나는 업무를 수행할 때마다 정보보안 절차를 준수할 것이다.