韓國IT서비스學會誌
第19卷 第5號
2020年 10月, pp.15-31

Journal of Information Technology Services
https://doi.org/10.9716/KITS.2020.19.5.015

정보보호 정책의 전유과정이 정보보호 준수의도에 미치는 영향에 대한 탐색적 연구 : 콜센터와 병원 종사자들을 중심으로*

오진욱** · 백승익***

Exploring Effects of Appropriation on the Compliance Intention to Information Security Policy*

Jinwouk Oh** · Seung Ik Baek***

■ Abstract ■

This study explores the process in which employees adopt the information security policy. The results of this study, which surveyed 234 employees in three call centers and four hospitals, show that the employees adapt the information security policy through the social structuring process suggested by the AST model. In particular, this study identifies roles of two appropriation activities (FOA : Faithfulness of Appropriation & COA : Consensus on Appropriation) observed in the social structuring process. Regarding to the interactions between the two appropriation activities, FOA, which indicates a better understanding of the information security policy, is examined as a more critical factor than COA, which indicates the degree of agreement among employees about how to use it. FOA not only has a direct effect on compliance intention toward the information security policy, but also indirectly through COA, whereas COA has only a indirect effect through FOA. This result shows that, in order for a company to successfully implement a new information security policy, it is important for employees to understand its purpose and intention. The adaption of information security policy through two appropriation activities is observed in both hospitals and call centers, but due to the different working environments, there were differences in the preceding variables affecting the appropriation activities. The results of this study are expected to provide guidelines for companies who want to successfully adopt information security policy.

Keyword : Information Security Policy, Adaptive Structuration Theory, Appropriation, Concern for Information Privacy, Security Knowledge, Job Characteristics

Submitted : March 3, 2020 1st Revision : July 28, 2020 Accepted : August 31, 2020

* 본 논문은 2018년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2018S1A5A2A01028435)

** 한양사이버대학교 해킹보안학과 겸임교수

*** 한양대학교 경영대학 교수, 교신저자

1. 서 론

인간 생활 전반에 정보시스템과 컴퓨터를 매개로 하는 미디어 사용 증가로 개인의 정보를 타인과 공유하는 빈도가 증가하고 있다. 기업 또한 가능한 많은 고객정보를 수집 · 저장 · 가공하여 고객만족을 극대화하기 위한 새로운 서비스를 지속적으로 출시하고 있다. 이에 따라 개인정보를 오남용하는 사례가 지속적으로 보고되고 있으며, 개인정보를 제공하는 정보주체 또한 불안감이 증가되고 있는 실정이다. 정보주체는 자신의 정보를 보유하고 있는 기업에게 본인 정보의 안전한 관리와 정보 제공 목적에 합당하게 사용할 것을 강하게 요구하고 있다. 사회단체 및 국가에서는 개인정보의 오남용으로 인한 사회적 갈등과 개인의 피해를 줄이기 위하여 다양한 법률과 규제를 시행하고 있으며 기업 또한 정보보호를 체계적으로 관리하고 사회적으로 요구하고 있는 정보보호 수준 제고를 위하여 자체적인 정보보호 활동을 강화하고 있다.

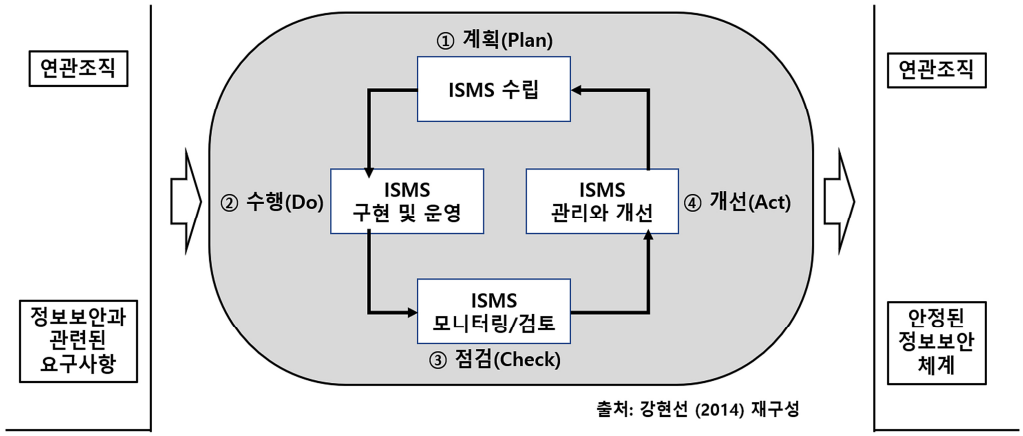
우리나라는 1999년도에 처음 정보통신망의 이용을 촉진하고 정보통신 서비스 이용자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하고자 “정보통신망 이용촉진 및 정보보호 등에 관한 법률”(이하 정통망법)을 제정하였고, 2011년에는 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 “개인정보보호법”을 제정하였다. 한국인터넷진흥원(KISA)은 정통망법을 근거로 정보보호 관리체계(ISMS : Information Security Management System)라는 인증 제도를 운영하고 있다. 기업들은 정기적으로 ISMS 심사 기준을 근거로 그들이 보유한 고객정보를 적절하게 수집 · 관리 · 운영하는지를 객관적으로 평가를 받고 있다(박민정 외, 2019).

기업은 ISMS가 가지고 있는 정보보호 사상을 수용하고 이를 자사에 접목하기 위하여 정책과 지침을 제정하고 고객정보를 대량으로 다운로드 시 목적, 사용범위, 다운로드 건 수 등의 타당성을 사전에 검토하여 승인 후 처리하도록 정보시스템의 이용절차를 구체적으로 수립 · 운영하고 있다. 그럼에도 불구하고 고객정보 유출사고는 지속적으로 발생하고 있는 실정이다. 최근에 일어난 일련의 정보 유출사고를 살펴보면, 기술적 취약점으로 인한 보안 사고보다는 고객정보를 취급하고 있는 내부 직원의 의도적 혹은 비의도적 실수로 인한 정보 유출사례가 빈번히 발생하고 있다(Karimi and Peikar, 2019).

따라서 정보보호 관리체계가 효율적으로 운영되어 정보 유출을 비롯한 보안 사고를 최소화하기 위해서는 제도의 정립과 수용도 필요하지만 무엇보다도 조직 구성원들이 고객정보 취급 시 준수하여야 하는 지침과 절차를 구성원 나름대로 자신의 업무 환경에 적절하게 적용하는 과정이 필요할 것이다(Yayla and Sarkar, 2018). 기존 연구에서는 조직 구성원들의 정보보호 정책 준수의도에 영향을 미치는 환경요인들을 탐색하는데 초점이 맞추어져 있어, 정보보호 정책 준수 과정에 관한 연구는 상대적으로 관심이 적었다. 새로운 정보보호 정책을 수용하는 과정은 구성원들이 환경요인들과 밀접하게 상호작용을 하면서 지속적으로 의사결정을 내리는 과정일 것이다(Ko et al., 2008). 이 과정에 대한 이해는 새로운 정보보호 정책을 효율적으로 구성원들에게 소개하는데 있어 매우 중요할 것이다. 적응 구조화 이론은 이런 역동적인 수용과정을 탐색하기 위한 프레임워크를 제시하고 있다(Schwieger et al., 2006). 이에 본 연구에서는 적응 구조화 이론(AST : Adaptive Structuration Theory)에서 정의한 전유 활동을 이용하여 구성원들이 정보보호 정책을 수용하는 과정에서 전유 활동의 역할을 탐색하여 보았다.

2. 정보보호 관리체계(ISMS : Information Security Management Systems)

정보보호 관리체계(ISMS)는 정보보호의 주요 목적인 기밀성, 무결성, 가용성을 확보하기 위하여 기업



[그림 1] 정보보호 관리체계 라이프 사이클

내에 정보관리 절차와 과정을 체계적으로 수립하고, 지속적으로 운영하는 관리 시스템을 총칭한다. 기업은 ISMS 도입을 통하여 단순 일회성, 단편적 정보보호 대책에서 벗어나 조직적이고 종합적인 정보보호 대책을 구현하여 전반적인 기업의 정보보호 관리 수준을 향상시키고자 노력하고 있다(강현선, 2014). ISMS는 PDCA(Plan-Do-Check-Act) 사이클을 기반으로 정보자원을 보호하기 위한 체계적인 절차를 정의하고 있다([그림 1] 참조).

국내에서 ISMS 인증은 정보시스템을 중심으로 안정성과 신뢰성 확보를 위한 인증제도이며, 과거 정통부가 2002년부터 운영하여 왔다. ISMS 인증은 연매출액 100억원 이상 또는 일평균 이용자 100만명 이상 사업자는 의무대상이며, 그 외의 기업들은 자율적으로 신청할 수 있다. ISMS 인증 기준은 정보보호 관리과정(5단계, 12개 통제항목)과 정보보호 대책(13개 분야, 92 통제항목)에 대한 심사 항목들로 구성되어 있다.

ISMS가 도입되면 정보보호와 연관된 사고 빈도는 감소되어질 수 있으나, 정보를 직접 관리하는 내부 구성원들의 활동은 크게 통제되어 업무에 소극적인 자세를 취할 가능성이 높아졌다(Zeng and Koutny, 2019). 장기적으로 업무 생산성과 만족도를 크게 저하시킬 가능성도 배제할 수 없을 것으로 생각된다. ISMS 인증이 기업에 미치는 영향을 조사한 기존 연구에서는 기업의 가치, 보안사고 빈도 등 결과물 중심으로 수행되어졌다(최동권, 윤현식. 2019). 그러나 실질적으로 ISMS가 어떤 과정을 거쳐서 구성원들의 정보보호 활동과 실적에 영향을 미치는 지에 대한 연구는 찾아보기가 힘든 상태이다(Ormond et al., 2019)

이에 본 연구에서는 ISMS 통제항목을 기반으로 수립한 조직의 정보보호 정책, 지침 및 절차가 조직 구성원들의 자발적이고 적극적인 정보보호 활동을 유도하는 과정을 적응 구조화 이론을 기반으로 탐색하여 보았다.

3. 적응 구조화 이론(AST : Adaptive Structuration Theory)

적응 구조화 이론(Adaptive Structuration Theory; AST)은 사회구조의 변화를 설명하기 위하여 Gidden (1984)에 의해 처음 소개되었다. Gidden(1984)은 사회구조를 사회규범, 규칙, 그리고 업무 프로세스라고 정의하고, 이것에 의해 구성원들의 행동이 제한을 받는다고 주장하였다. Gidden(1984)이 AST 이론에서 주장한 핵심적인 내용은 이런 사회구조가 일방적으로 주어진 것이 아니라 구성원들이 나름대로 그들의 목적과 상황에 맞도록 주어진 사회구조를 재생산하고, 선별적으로 이용함으로써 역동적으로 형성되어진다는

점이다(Schmitz et al., 2016). 즉 구성원들이 외부환경과 상호작용을 하면서 사회구조가 형성되고, 그 사회구조는 지속적으로 변화하게 된다. Gidden(1984)는 이 과정을 구조화(Structuration) 과정이라고 정의하였다. 이런 구조화 과정을 거쳐서 구성원들은 새로운 변화를 수용하게 된다. AST모델은 일반적인 조직구조 변화 뿐만 아니라, 정보시스템에 의해 변화하는 조직구조의 수용과정을 설명하기 위해서도 널리 사용되고 있다. DeSantis and Poole(1994)는 AST모델을 이용하여, 구성원들이 그룹의사결정 시스템(Group Decision Support System : GDSS) 도입으로 발생한 조직구조 변화 수용 과정을 설명하였다. 정보시스템 수용과정을 설명하는데 AST모델을 적용함으로써 수용에 있어서 기술적 요인 뿐만 아니라 사회적 요인이 중요한 역할을 함을 보여 줄 수 있었다.

AST모델을 적용한 연구는 새로운 정보시스템의 도입으로 인한 변화 이외에도 새로운 절차나 규칙의 수용과정을 설명한 연구도 적지 않게 찾아 볼 수 있다. Cao et al.(2009)는 새로운 정보시스템 개발 방법론의 적용으로 인한 팀의 수용과정을, Figueiredo and Morley(2013)는 새로운 프로젝트 관리 방법의 적용으로 인한 팀의 수용과정을 탐색하기 위하여 AST모델을 이용하였다.

정보보호에 대한 중요성이 강조되면서 기업에서는 방화벽, 서버접근제어, DB접근제어, 매체제어시스템, DRM 등과 같은 보안시스템 도입을 서두를 뿐만 아니라 정책, 지침 및 절차를 조직에 적용하여 개인정보를 이용하는 구성원 개개인의 업무활동을 엄격하게 규제 하고 있다. 고객정보의 과다 조회 등과 같이 과거에는 일반적인 관행(Norm)으로 여겨졌던 행동이 정보보호와 관련된 정책이나 절차가 조직에 도입되면서 더 이상은 조직 내에서 용납되지 않는 행동이 되었다.

본 연구의 목적은 정보보호 정책으로부터 발생한 추가적인 업무절차와 조직구조의 변화를 조직 구성원들이 자신의 업무환경에 적절하게 재구조화하는 과정을 AST모델을 기반으로 탐색하는 것이다.

4. 전유(Appropriation) : FOA & COA

AST모델에 의하면 새로운 정보시스템은 구성원에게 새로운 업무환경을 제공하고, 구성원들은 선택적인 환경 수용 과정을 통하여 정보시스템이 조직에 수용된다고 주장하고 있다(이준기 외, 2009). 이 과정을 사회적 구조화 과정이라고 칭하고 있다. 동일한 정보시스템이라고 할지라도 팀/조직의 환경적 요인에 따라 사회적 구조화 과정은 상이하게 나타날 것이다. DeSantis and Poole(1990)은 이런 구조화 과정에서 가장 기본적으로 관측되는 구성원들의 행동을 전유(Appropriation)라고 정의하고, 다음과 같이 2가지 행동유형을 제시하였다.

- FOA(Faithfulness of Appropriation, 전유의 충실성) : 정보시스템 설계자의 고유한 의도와 일치하는 방식으로 이용자들이 사용하는 행동
- COA(Consensus on Appropriation, 전유의 일치도) : 정보시스템을 설계자의 고유한 의도와는 다르게 팀/조직 내에서 합의된 방식으로 이용자들이 사용하는 행동

FOA는 정보시스템 설계자가 의도한 대로 사용자가 정보시스템을 사용하고 있는 정도를 의미한다. 설계자의 의도는 설계도나 매뉴얼 형태로 사용자에게 동일한 형태로 전달되지만 모든 사용자들이 이를 충실히 따르는 것은 아닐 것이다. 개인/팀/조직의 환경에 따라서 설계자가 의도한 사용 방법을 준수하는 정도는 차이가 있을 것이다. 설계자의 의도대로 정보시스템을 사용하게 되면 충실한 전유가 일어나게 되고, 이것은 직접적으로 긍정적인 결과와 연관될 가능성이 높을 것이다(Chin et al., 1997).

전유를 측정하는 또 다른 변수는 전유의 일치도(COA : Consensus on Appropriation)이다. 이는 사용자 그룹 내에서 정보시스템을 사용하는 방식의 합의 정도를 의미한다. 새로운 정보시스템 사용 방식에 대해 여러 의견을 가진 사용자들이 합의를

도출하기 위해서는 많은 의사소통을 통한 정보공유가 선행되어야 할 것이다. 정보시스템 사용에 대해 합의 수준이 높다는 것은 사용자들이 공동의 목표를 위하여 새로운 정보시스템을 사용하고 있다는 것과 동일한 의미이며, 이는 사용자 간의 긴밀한 협조가 전제되었음을 의미한다. 조직 내부에서 새로운 정보시스템의 합의 정도가 높다는 것은 새로운 시스템을 조직이 수용하는데 긍정적인 영향을 미칠 것이다(Salisbury et al., 2002).

우리는 Chin et al.(1997)이 개발한 FOA 척도와 Salisbury et al.(2002)이 개발한 COA 척도를 본 연구의 주요 주제인 정보보호 정책의 전유 활동에 적합하게 수정하여 설문문항을 작성하였다(<부록> 참조).

5. 연구모델

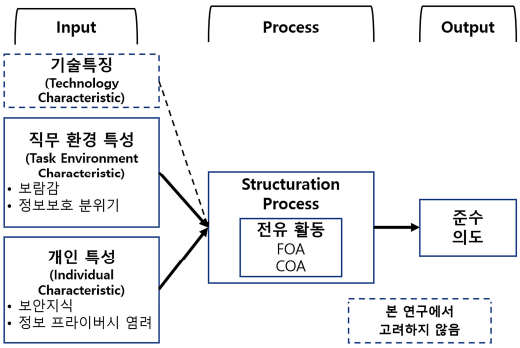
DeSantis and Poole(1994)는 정보시스템의 전유에 영향을 미치는 선행요인으로 정보시스템의 특징, 조직 및 직무의 특징, 그리고 조직의 내부 시스템을 제시하였다.

첫 번째 요인은 새롭게 도입된 정보시스템의 특징이다. 이는 사회구조의 변화를 유발하는 정보시스템 자체의 특징을 의미하며, 정보시스템의 구조적 특징(Structural Features)과 정신(Sprit)으로 구성된다. 정보시스템의 구조적 특징은 사용자에게 제공하는 다양한 기능과 규칙을 의미한다. 사용자들은 정보시스템이 제공하는 기능을 이용하여 업무를 수행할 것이고, 이 과정에서 사용법과 규칙을 준수할 것이다. 사용자들의 전유 활동은 준수하여야 할 규칙의 유연성과 복잡도에 따라서 크게 영향을 받게 될 것이다. 정보시스템 정신은 정보시스템을 이용하여 의도적으로 추구하고자 하는 가치나 목표를 의미한다. 예를 들어, DeSantis and Poole(1994)는 그룹의사결정 시스템(GDSS)의 정신을 의사결정 프로세스, 리더쉽, 효율성, 갈등관리, 팀 분위기로 정의하였고, Ruel(2002)은 사무용 기술(Office Technology)의 정신을 “Open Organizational Communication”이라고 정의하였다.

두 번째 요인은 정보시스템을 제외한 직무 환경을 의미한다. 직무 환경을 구성하고 있는 조직과 직무의 특징은 새로운 정보시스템의 성공적인 수용에 적지 않은 영향을 미칠 것이다. 비록 동일한 정보시스템을 이용하더라도, 사용자의 전유 활동은 직무의 복잡도나 자율성에 따라 크게 차이가 있을 것이다. 예를 들어 복잡한 직무에는 다양한 기능과 적은 수의 규칙을 제공하는 정보시스템이 수용되어질 가능성이 높을 것이다(Sun, 2012). 직무뿐만 아니라 조직의 문화나 분위기 또한 영향을 미칠 것이다. 새로운 정보시스템에 대하여 호의적인 조직 분위기라면, 수용 가능성은 높을 것이다(Ahmadi et al., 2015).

세 번째 요인은 조직 내부 시스템의 변화를 수용하는 주체인 조직 구성원들의 특징을 의미한다. 이 요인에는 사용자 간의 사회적 상호작용의 형태, 정보시스템에 대한 사전 지식이나 경험의 유무, 그리고 정보시스템 사용에 대한 동의 정도 등이 포함된다 (Chang et al., 2008).

본 연구는 정보보호 정책 운영으로 인하여 파생된 사회구조의 변화 수용 과정을 ASP모델을 이용하여 탐색하는데 초점을 두고 있다. 우리는 기존의 ASP 모델에서 전유 활동에 영향을 미치는 3개의 선행요인 중에서 “정보시스템의 특징”을 제외한 2개의 선행요인이 전유 활동에 미치는 영향을 살펴보았다. 본 연구에서 ASP모델의 “정보시스템의 특징”은 “정보보호 정책의 특징”으로 대체될 수 있을 것이다. “정보보호 정책”은 “정보시스템”과는 달리 기업 별로 준수 수준에는 차이가 있으나 정보보호라는 전체적인 목적과 적용분야에 있어서는 큰 차이가 존재하지 않는다고 판단되어 본 연구에서는 기술특징과 관련된 선행요인을 제외한 정보보호 정책 운영과 관련된 환경적 요인이 전유 활동에 미치는지 영향만을 탐색하였다. 여기서 환경적 요인이란 조직 문화(Information Security Climate), 직무 특징(Job Characteristics), 구성원의 개인적 특징(Information Security Knowledge and Concern for Information Privacy)을 의미한다([그림 2] 참조).



[그림 2] 연구모델

5.1 직무 특징(Job Characteristics)

Hackman and Oldham(1976)은 직무특성 모형(Job Characteristic Model)을 이용하여 5개의 핵심 직무특성이 종업원의 심리상태에 긍정적인 영향을 미치고, 나아가 종업원들의 직무만족과 성과에도 긍정적 영향을 미친다는 것을 발견하였다. 직무특성 모형에 의하면, 직무가 가지고 있는 5가지의 핵심 직무차원은 종업원들의 내적 심리적 상태에 영향을 미치고, 이는 다시 개인과 조직의 성과에 영향을 준다고 가정하고 있다. 이들이 제시한 핵심 직무 차원은 다음과 같다.

- 기술다양성(Skill Variety)
- 직무정체성(Task Identity)
- 직무중요성(Task Significance)
- 직무자율성(Job Autonomy)
- 직무피드백(Feedback)

기술다양성은 직무를 수행하는데 있어 다양한 활동이나 기술을 필요로 하는 정도를, 직무정체성은 개인이 독립적으로 혼자 책임지고 직무 전체를 수행할 수 있는 정도를, 직무중요성은 자신의 직무수행 결과가 다른 사람들의 육체적 혹은 심리적 안정에 중요한 영향을 미친다는 것을 개인이 인지하고 있는 정도를, 직무자율성은 자신의 창의적인 발상이나 아이디어 등을 활용하여 자기 주도적인 직무 수행을 할 수 있는 정도를, 마지막으로 직무피드백은 직무수행결과에 대해 직접적이고 명확한 정보를 얻을 수 있고, 다른 직무수행자에게도 알려지는 정도를 의미한다. Hackman and Oldham(1976)는 5개의 직무특성 중에서 기술다양성, 직무정체성, 그리고 직무중요성은 직무에 대한 구성원들의 보람감을 측정할 수 있는 변수라고 정의하였다.

본 연구에서는 구성원이 수행하는 직무에 대해서 인지하는 보람감(Meaningfulness)이 그들의 전유활동에 미치는 영향을 탐색하여 보았다. 직무에 대한 보람감을 측정하기 위하여 Hackman and Oldham (1976)이 제시한 대로 5가지의 핵심 직무 차원 중에서 기술다양성, 직무정체성, 그리고 직무중요성을 이용하였다(<부록> 참조).

5.2 정보보호 분위기(Information Security Climate)

정보보호 정책이 조직에 도입되면 정보자원 관리에 조직 전체가 노력하는 분위기가 형성될 것이다. 다수의 기존 연구에서 조직 분위기는 구성원의 행동의도를 변경시키는 주요한 선행요인으로 제시하고 있다(Shadur et al., 1999). 특히 산업재해 등 안전관리 분야에 있어서는 조직 분위기가 안전성과에 절대적인 영향을 미치는 것을 여러 연구를 통하여 검증하였다. “안전 분위기(Security Climate)”라는 개념을 정보보호 분야에 적용하여 조직 구성원들의 정보보호 활동을 촉진시키기 위한 전략을 수립하는데 초점을 맞춘 연구들이 소개되었다(Chan et al., 2005; Goo et al, 2014). Zohar and Luria(2005)는 안전 분위기를 “안전과 관련된 조직 내의 정책, 절차, 그리고 관행에 대한 조직 구성원들의 지각”으로 정의하고 있다.

본 연구에서는 조직 구성원에게 정보보호를 강조하는 조직의 분위기 정도를 측정하여, 전유 활동에 미치는 영향을 살펴보았다(<부록> 참조).

5.3 보안지식(Information Security Knowledge)

Safa et al.(2016)과 Wang(2010)은 정보보안 관점에서 종업원들이 정보보호에 대한 지식이 풍부할 때,

정보보호의 중요성을 더욱 심각하게 인지하여 정보보호 정책 준수의도에도 긍정적인 영향을 미치는 것을 실증적으로 검증하였다. 이러한 관점에서 기업은 다양한 방법을 이용하여 정보보호에 대한 지식을 종업원들에게 적극적으로 전달하고자 많은 노력을 기울이고 있다.

본 연구에서는 종업원 개인이 가지고 있는 보안지식의 수준이 그들이 정보보호 정책 준수의도에 영향을 미치는 과정에서 전유 활동이 어떤 영향을 미치는지를 실증적으로 조사하였다(<부록> 참조).

5.4 정보 프라이버시 염려(CFIP : Concern for Information Privacy)

본 연구에서는 조직 구성원의 보안에 대한 인식 정도를 측정하기 위하여, 경영정보학 분야에서 널리 사용되어지고 있는 정보프라이버시 염려(CFIP)라는 개념을 사용하였다. Culnan(1993)는 CFIP를 '본인 정보에 대한 외부의 감시, 저장, 검색 등으로 인하여 소비자가 느끼는 위협의 정도'라고 정의하였으며, Smith et al.(1996)는 CFIP를 '개인정보가 다양한 위협으로부터 누출되어지는 우려의 정도'라고 정의하였다. Smith et al.(1996)는 CFIP를 측정할 수 있는 모델을 개발하였다. 그 모델에서는 CFIP를 다음과 같이 4개의 세부차원으로 분류하여 측정하였다.

- 정보수집(Collection)과 연관된 염려
- 비 인가된 2차사용(Unauthorized secondary use)과 연관된 염려
- 부적절한 접근(Improper access)과 연관된 염려
- 잘못된 정보(Errors)와 연관된 염려

CFIP에 대해서 아직까지 정보보호 준수의도의 선행요인으로써 어떠한 영향을 미치는지를 직접적으로 탐색한 연구는 없었다. CFIP와 연관된 대부분의 연구는 CFIP가 신뢰에 긍정적인 영향을 미치고, 신뢰는 다시 사용자의 긍정적인 행동의도에 영향을 미치는 과정을 설명하고 있다. 여러 학자들 중에서 Liu et al.(2004)는 **CFIP-신뢰-행위의도** 모형을 제시하고, 소비자 관점에서 개인정보 제공에 대한 염려수준이 기업에 대한 신뢰수준에 영향을 미치고, 신뢰 수준을 기반으로 기업과 거래를 지속적으로 이어갈지, 아니면 거래를 중단 할지에 대한 행동의도를 결정하는 과정을 설명하였다. 이처럼 CFIP 관련 선행연구들의 일반적인 주장은 평소 개인정보 유출에 대해 개인이 가지는 지각수준이 높을수록 행동의도에도 영향을 미친다는 것이다.

본 연구에서는 개인의 CFIP가 개인의 전유 활동에 어떤 영향을 미치는지를 실제적으로 검증하여 보았다. 본 연구에서는 Smith et al.(1996)가 제시한 CFIP의 4가지 차원을 기반으로 설문 문항을 재구성하였다(<부록> 참조).

5.5 정보보호 준수의도

본 연구에서는 Hearath and Rao(2009)가 정보보호 준수의도를 측정하기 위하여 제시한 설문문항을 재구성하여 사용하였다.

6. 분석 결과

본 연구를 위하여 ISMS 인증을 받은 3개의 콜센터와 4개의 병원 종사자들을 대상으로 설문을 실시하였다. 콜센터 상담사들은 고객의 정보를 직접적으로 관리·이용하고 있기 때문에 ISMS 도입으로 그들의 업무는 많은 영향을 받을 것으로 생각되어 설문 대상으로 선택하였고, 병원 종사자들 또한 환자정보에 쉽게 접근하여 열람할 수 있기 때문에 콜센터의 상담사들 만큼 정보보호가 매우 중요하게 여겨지는 직무 중 하나라고 판단되어 설문대상으로 선택하였다. 설문지는 해당 조직의 정보보호 책임자를 통해 종업원들에게 배포되었고, 불성실한 설문지를 제외하고 총 360부의 설문지를 대상으로 분석을 실시하였다(<표 1> 참조).

〈표 1〉 응답자 특징

성별	남자	46명	13%
	여자	314명	87%
연령	20대	102명	28.30%
	30대	119명	33.10%
	40대	95명	26.30%
	50대	44명	12.30%
교육수준	고등학교 졸업	96명	26.70%
	대학교 졸업	254명	70.50%
	대학원 졸업 이상	10명	2.80%
조직	콜센터 (3개의 콜센터)	126명	35%
	병원 (4개의 병원)	234명	65%

본 연구의 목적은 개인정보를 취급하는 조직 구성원의 특징(정보보호에 대한 지식 정도와 프라이버시에 대한 염려 정도)과 직무 환경의 특징(업무에 대해 의미를 부여하는 정도와 정보보호에 대해 소속된 조직/팀의 강조 정도)이 개인의 정보보호 준수의도에 영향을 미치는 과정에서 두 가지 전유 활동(FOA와 COA)의 역할을 탐색하는데 있다([그림 2] 연구모델 참조).

본 연구에서 사용된 설문 문항들의 타당도와 신뢰도를 측정하기 위하여 주성분 분석을 실시하였으며, 각 측정 항목의 요인 부하량이 0.5 이상인 측정항목들이 의미가 있는 변수로 판단하여 분석에 사용하였다. 또한 추출된 요인을 구성하고 있는 측정항목들의 내적 일치도를 알아보기 위하여 신뢰도 검증을 실시하였다. 일반적으로 Cronbach's α 계수가 0.6 이상이면 신뢰성이 확보되었다고 판단하며, 본 연구의 분석에 사용된 모든 요인들의 Cronbach's α 계수가 0.6 이상으로 신뢰도에도 문제가 없는 것으로 판단되었다(<표 2> 참조).

6.1 구조방정식 모델 검증

본 연구에서는 조직 구성원들이 정보보호 정책을 수용하는 과정에서 전유의 역할을 탐색하기 위하여 두 개의 구조방정식 모델을 검증하였다(모델 1 : FOA → COA, 모델 2 : COA → FOA).

구조방정식 모델 검증을 위해 본 연구에서는 구조

〈표 2〉 신뢰도와 타당성 검증결과

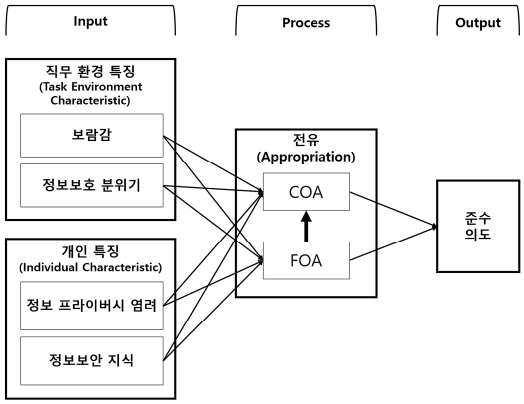
Variable		Items	Factor	Cronbach α
전유의 충실성 (FOA)		FOA_3	0.62	0.94
		FOA_4	0.61	
		FOA_2	0.6	
		FOA_1	0.6	
전유의 일치도 (COA)		COA_3	0.82	0.91
		COA_2	0.81	
		COA_4	0.79	
		COA_1	0.67	
기술다양성 (Skill Variety)		VA_2	0.89	0.76
		VA_1	0.85	
		VA_4	0.61	
		VA_3	0.59	
보람감	직무정체성 (Task Identity)	ID_2	0.83	0.8
		ID_3	0.82	
		ID_4	0.79	
	직무중요성 (Task Significance)	SIG_2	0.87	0.88
		SIG_3	0.85	
		SIG_1	0.84	
		SIG_4	0.77	
	정보보호 분위기 (Security Climate)	SC_3	0.8	0.87
		SC_1	0.76	
		SC_2	0.75	
보안지식 (Security Knowledge)		SK_3	0.85	0.88
		SK_4	0.79	
		SK_2	0.73	
		SK_5	0.7	
		SK_6	0.66	
정보 프라이버시 염려 (CFIP)		CFIP_1	0.85	0.71
		CFIP_2	0.85	
		CFIP_5	0.63	
정보보호 준수의도 (Compliance Intention)		CI_3	0.81	0.87
		CI_2	0.76	
		CI_5	0.71	
		CI_4	0.7	
		CI_1	0.65	

방정식 모델링을 지원하는 R 패키지 가운데서 안정적이고 다수의 연구에서 사용하고 있는 lavaan 패키지를 이용하였다(곽기영, 2019). 모델 검증 결과, 본 연구에서 검증하고자 한 2개 모델의 적합도 지표들이 모두 권고 수준을 만족하는 것으로 조사되었다(<표 3> 참조).

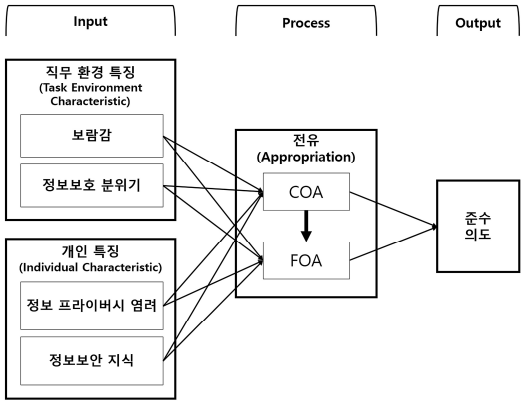
〈표 3〉 모델적합도

	Best Range	모델 1	모델 2
RMSEA	RMSEA < .08	0.04	0.04
GFI	GFI > .9	0.91	0.91
CFI	CFI > .9	0.97	0.97
NFI	NFI > .9	0.92	0.92

RMSEA(Root Mean Square of Error Approximation) : 근사 오차 제곱 평균의 제곱근
GFI(Goodness of Fit Index) : 적합도 지수
CFI(Comparative Fit Index) : 비교 적합도 지수
NFI(Normed Fit Index) : 표준 적합도 지수



[그림 3] 모델 1 : FOA → COA



[그림 4] 모델 2 : COA → FOA

6.2 경로분석 결과

위에서 검증된 모델을 기반으로 경로분석을 실시하였다. 병원과 콜센터 종사자 모두를 대상으로 분석한 결과는 다음과 같다(<표 4> 참조).

〈표 4〉 콜센터+병원 분석결과

Dep	Indep	Z	p	Sig.
FOA	CFIP	0.12	0.9	X
FOA	보안지식	6.33	0	***
FOA	보람감	1.97	0.05	*
FOA	정보보호 분위기	9.65	0	***
COA	CFIP	2.33	0.02	*
COA	보안지식	4.87	0	***
COA	보람감	1.64	0.1	X
COA	정보보호 분위기	4.56	0	***

COA ← FOA(모델 1)				
COA	FOA	10.66	0	***
Intention	FOA	11.86	0	***
Intention	COA	12.67	0	***

FOA ← COA(모델 2)				
FOA	COA	11.83	0	***
Intention	FOA	23.93	0	***
Intention	COA	0.75	0.45	X

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$.

정보프라이버시 염려정도(CFIP)가 FOA에 미치는 영향과 직무에 대한 보람감(Meaningfulness)이 COA에 미치는 영향을 제외한 대부분의 개인특징, 직무환경 특징 변수들은 전유 활동인 FOA와 COA에 통계적으로 유의한 영향을 미치는 것으로 조사되었다. 특히 FOA가 COA에 영향을 준다는 가정(모델 1)에서는 FOA가 정보보호 준수의도에 직접적인 영향뿐만 아니라 COA를 통한 간접적인 영향을 미치는 경로를 추가로 발견하였다. COA가 FOA에 영향을 준다는 가정(모델 2)에서 COA는 FOA를 통해서만 준수의도에 영향을 미치고, COA가 직접적으로 준수의도에는 영향을 미치지 못하는 것으로 조사되었다. 즉 정보보호 정책의 의도와 취지에 대한 충분한 이해(FOA)를 기반으로 구성원들 간의 합의된 이해(COA)에 영향을 미친다는 가정(FOA → COA)에 있어서는 두 가지 전유 활동이 모두 준수 의도에 통계적으로 유의한 영향을 미치는 것으로 조사되었다. 반면에

정보보호 정책에 대한 구성원들 간의 합의된 이해(COA)를 이용하여 구성원들이 정보보호 정책 도입 취지대로(FOA) 정보시스템 이용을 촉진시키려는 전략(COA → FOA)에 있어서는 정보보호 정책에 대한 구성원들 간의 합의된 이해(COA)는 준수의도에 직접적인 영향을 미치지 못하고, 정보보호 정책에 대한 의도와 취지에 대한 충분한 이해(FOA)를 통해서 간접적으로 준수의도에 영향을 미치는 것으로 조사되었다. 이러한 결과는 콜센터와 병원 종사자 모두 동일하게 관찰되었다(<표 5>, <표 6> 참조).

콜센터 종사자와 병원 종사자들 간에 차이가 나타나는 부분은 두 가지 전유 활동인 COA와 FOA에 영향을 미치는 선행요인들에서 발견할 수 있었다. 콜센터 종사자의 경우에는 개인의 특징 중에 개인의 보안지식만이 COA와 FOA에 통계적으로 유의한 영향을 미치는 것으로 조사되었고, 업무 특징 중에는 보안을 강조하는 조직 분위기만이 FOA에 영향을 미치는 것으로 조사되었다(<표 5> 참조). 반면 병원 종사자의 경우에는 개인의 정보 프라이버시 염려 정도(CFIP)가 FOA에 영향을 미치는 경로 이외의 모든 선행변수들이 COA와 FOA에 통계적으로 유의한 영향을 미치는 것으로 조사되었다(<표 6> 참조). 이러한 결과는 다음과 같은 두 기관의 상이한 업무환경에서 찾을 수 있을 것이다. 먼저 병원 종사자들은 콜센터 종사자들에 비해 환자정보에 접근하여 조회·등록 등의 취급에 능동적이며, 환자정보를 교환·참조 등이 빈번한 환경에서 근무한다고 할 수 있다. 따라서 병원 종사자 개인의 특징과 개인이 인지하는 환경요인들이 그들의 전유 활동에 영향을 미친다는 해석이 가능하다. 한편 콜센터 종사자는 고객의 상담요청이 발생했을때에만 수동적으로 고객의 정보에 접근이 가능하며, 고객정보를 다른 상담원과 교환·공유하는 빈도가 병원 종사자보다 상대적으로 낮은 특성을 가지고 있다. 또한 콜센터 상담원은 정해진 상담 매뉴얼(Script)을 기반으로 고객정보를 처리하는 환경적 특징을 가지고 있기 때문으로 해석 가능하다.

〈표 5〉 콜센터 분석결과

Dep	Indep	Z	p	Sig.
FOA	CFIP	0.06	0.95	X
FOA	보안지식	5.13	0	***
FOA	보람감	0,45	0.65	X
FOA	정보보호 분위기	8.3	0	***
COA	CFIP	1.8	0.07	X
COA	보안지식	3.07	0	***
COA	보람감	0.3	0.76	X
COA	정보보호 분위기	1.36	0.17	X

COA ← FOA(모델 1)				
COA	FOA	10.44	0	***
Intention	FOA	10.69	0	***
Intention	COA	14.6	0	***

FOA ← COA(모델 2)				
FOA	COA	10.27	0	***
Intention	FOA	27.51	0	***
Intention	COA	0.66	0.45	X

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$.

〈표 6〉 병원 분석결과

Dep	Indep	Z	p	Sig.
FOA	CFIP	-1.89	0.06	X
FOA	보안지식	4.02	0	***
FOA	보람감	3.92	0	***
FOA	정보보호 분위기	6.39	0	***
COA	CFIP	3.82	0	***
COA	보안지식	3.54	0	***
COA	보람감	2.39	0.02	*
COA	정보보호 분위기	2.91	0	***

COA ← FOA(모델 1)				
COA	FOA	9.08	0	***
Intention	FOA	9.35	0	***
Intention	COA	6.96	0	***

FOA ← COA(모델 2)				
FOA	COA	10.78	0	***
Intention	FOA	14.19	0	***
Intention	COA	1.31	0.19	X

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$.

7. 결론 및 시사점

정보보안이 기업의 중요한 이슈로 대두되면서 정보보호 준수의도에 영향을 미치는 요인들에 대한 연구는 많이 수행되어져 왔다(Cram et al., 2019; Ifinedo, 2014; Kim and Park, 2011; Safa et al., 2016). 그 중 대부분의 연구는 개인과 조직의 특성이 정보보호 준수의도에 영향을 미치는지를 탐색하는데 초점이 맞추어져 있었다. 그러나 개인과 조직의 특성이 어떤 과정을 거쳐서 개인의 정보보호 준수의도에 영향을 미치지를 탐색한 논문은 찾아보기가 힘든 상황이다(Ormond et al., 2019; Yayla and Sarkar, 2018). 이에 본 연구에서는 AST모델에서 제안한 구조화 과정의 개념을 기반으로 구성원들이 조직의 정보보호 정책을 수용하여 그들의 준수의도에 영향을 미치는 과정을 살펴보았다. 특히 구조화 과정에서 관측되는 전유의 충실성(FOA : Faithfulness of Appropriation)과 전유의 일치도(COA : Consensus on Appropriation)가 정보보호 준수의도에 영향을 미치는 과정에서 어떤 역할을 하는지를 콜센터 상담원과 병원의 간호사들을 대상으로 살펴보았다.

연구 결과, 개인과 직무의 특징이 정보보호 활동 준수 의도에 두 개의 전유 활동(FOA와 COA)을 통해서 긍정적인 영향을 미치는 것으로 조사되었다. 그리고 FOA와 COA의 상호작용에 대해서는 콜센터와 병원 모두, FOA는 정보보호 준수의도에 직접적인 영향을 줄 뿐만 아니라 COA를 통한 간접적인 영향을 미치는 것으로 조사되었으나, COA는 정보보호 준수의도에 직접적인 영향을 제공하지 못하고 FOA를 통해서만 준수의도에 긍정적인 영향을 미치는 것으로 조사되었다. 이런 연구 결과는 기업이 새로운 정보보호 정책을 도입할 때, 정보보호 정책에 대한 의도나 취지를 종업원들에게 충분히 설명하고 이해시키는(FOA) 것이 얼마나 중요한지를 설명하여 주고 있다. 종업원들의 합의된 이용 (COA)은 정책의 취지나 의도의 이해 (FOA)를 촉진시켜 정보보호 준수의도에 간접적인 영향을 제공하기는 하나, 직접적으로 준수 의도에는 영향을 미치지 못하는 것으로 본 연구에서는 조사되었다.

조직구성원이 정보보호 정책을 수용하는 과정에서의 전유 활동의 역할은 콜센터와 병원에서 동일한 결과가 조사되었다. 그러나 그들의 상이한 업무 환경으로 전유 활동에 영향을 주는 개인과 환경의 특징들이 차이를 보여 주었다. 콜센터 상담원에 비하여 상대적으로 정보접근에 능동적이고 타 조직과 정보교환이 빈번한 분위기에서 업무를 수행하는 병원 종사자의 경우에는 CFIP를 제외한 모든 선행요인들이 전유 활동에 영향을 주는 것으로 조사되었다. 반면에 콜센터 상담사의 경우에는 개인의 보안지식의 정도와 조직의 분위기만이 전유 활동에 영향을 주는 것으로 조사되었다. 그것도 조직의 분위기는 COA에는 유의한 영향을 미치지 못하고, FOA에만 유의한 영향을 미치는 것으로 조사되었다. 정보접근에 능동적이고 정보교환이 빈번한 환경에 근무하는 구성원의 경우, 그렇지 못한 구성원에 비해 개인의 인식 개선에 초점을 맞춘 전략이 필요함을 알 수 있었다.

본 연구는 ISMS를 도입・운영하고 있는 콜센터와 병원 종사자를 대상으로 설문연구를 진행하였으나 몇 가지 한계점을 가지고 있다. 설문 대상 조직의 ISMS 도입 시기가 상이하여 구성원들이 정보보호에 대한 인지와 수용정도가 조사항목에 포함되지 않았다. 해당 조직에서 수행하는 정보보호교육 횟수, 평가/반영의 정도를 측정하지 못하였다. 따라서 향후 연구에서는 ISMS 도입 시기, 정보보호교육에 대한 평가와 반영을 지표화하여 조직 구성원의 전유활동이 어떻게 다른지 탐색할 필요가 있을 것이며, 본 연구와 같이 설문을 이용한 양적연구에서 더 나아가 구성원을 대상으로 심층인터뷰를 통하여 좀 더 구체적인 구조화과정에서 관측되는 전유활동을 탐색할 필요가 있을 것이다.

참고문헌

곽기영, “R을 이용한 구조방정식모델링 : 매개효과 분석/조절효과분석 및 다중집단분석”, *지식경영연구*, 제20권, 제2호, 2019, 1-24.

강현선, “정보보안을 위한 정보보호 관리체계 및 인증체계 분석”, *보안공학연구논문지*, 제11권, 제6호, 2014, 455-468.

박민정, 유지은, 채상미, “ISMS-P와 GDPR의 개인정보보호 부문 연계 분석”, *한국IT서비스학회지*, 제18권, 제2호, 2019, 55-73.

이준기, 신호경, 최희재, “시스템의 도입과 전유 과정에 영향을 미치는 제도적 압력에 관한 연구 : 병원조직의 모바일 전자의무기록 시스템을 대상으로”, *Asia Pacific Journal of Information Systems*, 제19권, 제2호, 2009, 95-116.

최동권, 윤현식, “기업의 정보보호 관리가 영업성과와 기업가치에 미치는 영향 : 정보보호 관리체계(ISMS)를 중심으로”, *한국디지털콘텐츠학회 논문지*, 제20권, 제8호, 2019, 1567-1576.

Ahmadi, H., O. Ibrahim, and M. Nilashi, “Investigating a new framework for hospital information system adoption : a case on Malaysia”, *Journal of Soft Computing and Decision Support Systems*, Vol.2, No.2, 2015, 26-33.

Cao, L., K. Mohan, P. Xu, and B. Ramesh, “A framework for adapting agile development methodologies”, *European Journal of Information Systems*, Vol.18, No.4, 2009, 332-343.

Chan, M., I. Woon, and A. Kankanhalli, “Perceptions of information security in the workplace : linking information security climate to compliant behavior”, *Journal of Information Privacy and Security*, Vol.1, No.3, 2005, 18-41.

Chang, M.K., W. Cheung, C.H. Cheng, and J.H. Yeung, “Understanding ERP system adoption from the user's perspective”, *International Journal of Production Economics*, Vol.113, No.2, 2008, 928-942.

Chin, W.W., A. Gopal, and W.D. Salisbury, “Advancing the theory of adaptive structuration : The development of a scale to measure faithfulness of appropriation”, *Information Systems Research*, Vol.8, No.4, 1997, 342-367.

Cram, W.A., J. D'arcy, and J.G. Proudfoot, “Seeing the forest and the trees : a meta-analysis of the antecedents to information security policy compliance”, *MIS Quarterly*, Vol. 43, No.2, 2019, 525-554.

Culnan, M.J., “How did they get my name? : an exploratory investigation of consumer attitudes toward secondary information use”, *MIS Quarterly*, Vol.17, No.3, 1993, 341-363.

DeSanctis, G. and M.S. Poole, “Capturing the complexity in advanced technology use : Adaptive structuration theory”, *Organization Science*, Vol.5, No.2, 1994, 121-147.

Figueiredo, M.A.B. and C. Morley, Understanding the appropriation of project management norms : an empirical study in IT projects, In *ECIS 2013 : 21st European Conference on Information Systems*, 2013.

Giddens, A., The constitution of society : Outline of the theory of structuration, Univ of California Press, 1984.

Goo, J., M.S. Yim, and D.J. Kim, “A path to successful management of employee security compliance : an empirical study of information security climate”, *IEEE Transactions on Professional Communication*, Vol.57, No.4, 2014, 286-308.

Hackman, J.R. and G.R. Oldham, “Motivation through the design of work : Test of a theory”, *Organizational Behavior and Human Performance*, Vol.16, No.2, 1976, 250-279.

Herath, T. and H.R. Rao, “Protection motivation and deterrence : a framework for security policy compliance in organizations”, *European Journal of Information Systems*, Vol. 18, No.2, 2009, 106-125.

Ifinedo, P., "Information systems security policy compliance : An empirical study of the effects of socialisation, influence, and cognition", *Information and Management*, Vol.51, No.1, 2014, 69-79.

Karimi, Z. and H.R. Peikar, "Information Security Management : The Impacts of Organizational Commitment and Perceived Consequences of Security Breach on the Intention of Patients' Information Security Violation", *Medical Ethics Journal*, Vol.13, No.44, 2019, 1-10.

Kim, S.H. and S.Y. Park, "Influencing factors for compliance intention of information security policy", *The Journal of Society for e-Business Studies*, Vol.16, No.4, 2011, 33-51.

Ko, E., S.H. Kim, M. Kim, and J.Y. Woo, "Organizational characteristics and the CRM adoption process", *Journal of Business Research*, Vol.61, No.1, 2008, 65-74.

Liu, C., J.T. Marchewka, J. Lu, and C.S. Yu, "Beyond concern : a privacy-trust-behavioral intention model of electronic commerce", *Information and Management*, Vol. 42, No.1, 2004, 127-142.

Ormond, D., M. Warkentin, and R.E. Crossler, "Integrating Cognition with an Affective Lens to Better Understand Information Security Policy Compliance", *Journal of the Association for Information Systems*, Vol.20, No. 12, 2019, 1794-1843.

Ruël, H.J., "The non-technical side of office technology : managing the clarity of the spirit and the appropriation of office technology", *In Managing the human side of information technology : Challenges and solutions*, IGI Global, 2002, 78-104.

Safa, N.S., R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations", *Computers and Security*, Vol. 56, 2016, 70-82.

Salisbury, W.D., W.W. Chin, A. Gopal, and P.R. Newsted, "Better theory through measurement-Developing a scale to capture consensus on appropriation", *Information Systems Research*, Vol.13, No.1, 2002, 91-103.

Schmitz, K.W., J.T. Teng, and K.J. Webb, "Capturing the complexity of malleable IT use : Adaptive structuration theory for individuals", *MIS Quarterly*, Vol.40, No.3, 2016, 663-686.

Schwieger, D., A. Melcher, C. Ranganathan, and H.J. Wen, "Applying adaptive structuration theory to health information systems adoption : A case study", *International Journal of Healthcare Information Systems and Informatics(IJHISI)*, Vol.1, No.1, 2006, 78-92.

Shadur, M.A., R. Kienzle, and J.J. Rodwell, "The relationship between organizational climate and employee perceptions of involvement : The importance of support", *Group and Organization Management*, Vol.24, No.4, 1999, 479-503.

Smith, H.J., S.J. Milberg, and S.J. Burke, "Information privacy : measuring individuals' concerns about organizational practices", *MIS Quarterly*, Vol.20, No.2, 1996, 167-196.

Sun, J., "Why different people prefer different systems for different tasks : An activity perspective on technology adoption in a dynamic user environment", *Journal of the American Society for Information Science and Technology*, Vol.63, No.1, 2012, 48-63.

Wang, P.A., "Information security knowledge and behavior : An adapted model of technology acceptance", *In 2010 2nd International Con-*

ference on Education Technology and Computer (IEEE), June, 2010, V2-364.

Yayla, A. and S. Sarkar, "THE DYNAMICS OF INFORMATION SECURITY POLICY ADOPTION", *In Proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy*, 2018.

Zeng, W. and M. Koutny, "Modelling and analysis of corporate efficiency and productivity loss associated with enterprise information security technologies", *Journal of Information Security and Applications*, Vol.49, 2019, 1-11.

Zohar, D. and G. Luria, "A multilevel model of safety climate : cross-level relationships between organization and group-level climates", *Journal of Applied Psychology*, Vol.90, No. 4, 2005, 616-628.

〈부 록〉

전유의 충실성(FOA) (Chin et al., 1997)
FOA_1. 우리 기업의 (개인)정보보호책임자(CPO, Chief Privacy Officer)나 관련 부서는 우리 팀 전체의 (개인)정보보호 활동이 적절히 이루어지고 있다고 평가할 것이다.
FOA_2. 우리 팀 전체는 기업의 (개인)정보보호 지침이나 절차의 내용을 충분히 이해하고 있다.
FOA_3. 우리 팀 전체는 기업의 (개인)정보보호 지침이나 절차가 의도하는 방향을 충분히 이해하고 있다.
FOA_4. 우리 팀 전체는 기업의 (개인)정보보호 지침이나 절차를 업무에 적절히 반영하고 있다.

전유의 일치성(COA) (Salisbury et al., 2002)
COA_1. 우리 팀 구성원들은 (개인)정보보호 절차나 지침을 업무에 언제/어떻게 반영하여야 하는지에 대해 공통의견을 가지고 있다.
COA_2. 우리 팀 구성원들은 (개인)정보보호 절차나 지침을 업무에 언제/어떻게 반영하여야 하는지에 대해 의견차이가 없다.
COA_3. 우리 팀 구성원들은 (개인)정보보호 절차나 지침을 업무에 언제/어떻게 반영하여야 하는지에 대해 상호이해가 있다.
COA_4. 우리 팀 구성원들은 (개인)정보보호 절차나 지침을 업무에 언제/어떻게 반영하여야 하는지에 대해 상호동의가 있다.

직무 다양성(VA : Skill Variety) (Hackman & Oldham, 1976)
VA_1. 나의 업무는 주 업무 외에 부가적인 일이 많이 포함되어 있다.
VA_2. 나의 업무는 다양한 일을 수행해야 한다.
VA_3. 나의 업무는 다양한 지식과 기술을 필요로 한다.
VA_4. 나의 업무는 다양한 분야의 사람들과 교류하는 것을 요구한다.

직무정체성(ID : Task Identity) (Hackman & Oldham, 1976)
ID_1. 나의 업무는 시작과 끝이 분명하게 정의되어져 있다.
ID_2. 나의 업무는 처음부터 끝까지 모든 일을 내가 수행할 수 있도록 구성되어 있다.
ID_3. 나의 업무는 내가 해야 할 일들을 명확히 정의하고 있다.
ID_4. 나의 업무는 성과를 측정하기 위한 지표가 사전에 명확히 정의되어져 있다.

직무중요성(SIG : Task Significance) (Hackman & Oldham, 1976)
SIG_1. 나의 업무 결과는 다른 사람들의 삶에 긍정적인 영향을 미칠 것이다.
SIG_2. 나의 업무는 회사의 발전에 기여할 것이다.
SIG_3. 나의 업무는 사회발전(공익)에 기여할 것이다.
SIG_4. 나의 업무 결과는 관계자들(소비자, 주주, 동료직원, 소속 팀, 소속 기업, CEO, 협력업체 등)에게 긍정적 영향을 미칠 것이다.

정보보호 분위기(SC : Information Security Climate) (Zohar & Luria, 2005)
SC_1. 나는 우리 기업의 경영진이 (개인)정보보호 절차나 지침 준수를 중요하게 여긴다고 생각한다.
SC_2. 나는 우리 기업의 경영진이 (개인)정보보호 절차나 지침 준수를 업무 효율성보다 우선시 한다고 생각한다.
SC_3. 나는 우리 기업의 경영진이 (개인)정보보호 절차나 지침 준수 여부를 정기적으로 점검한다고 생각한다.
SC_4. 나는 (개인)정보보호 절차나 지침 준수와 관련된 이슈를 나의 동료, 직장상사와 자주 논의한다고 생각한다.
SC_5. 나는 우리 기업이 (개인)정보 사고 발생 시 즉각적으로 조치를 취한다고 생각한다.
SC_6. (개인)정보보호 절차나 지침 준수와 관련하여 질문이 있을 시에 용이하게 문의할 수 있는 창구가 우리 기업 내에 존재한다고 생각한다.

보안지식(SK : Information Security Knowledge) (Wang, 2010)
SK_1. 나는 (개인)정보를 안전하게 이용하는 방법을 알고 있다.
SK_2. 나는 (개인)정보를 안전하게 수집 · 관리하는 절차를 알고 있다.
SK_3. 나는 (개인)정보와 관련된 사건이 발생 시, 대처방안을 알고 있다.
SK_4. 나는 (개인)정보와 관련된 사건이 발생 시, 누구에게 보고를 해야 하는지 알고 있다.
SK_5. 나의 업무 중에서 (개인)정보 누출 사고가 일어날 가능성이 높은 업무를 알고 있다.
SK_6. 나는 기업의 (개인)정보보호 지침이나 절차를 숙독해 본 적이 있다.
SK_7. 나는 기업에서 요구하는 (개인)정보보호와 관련된 책임과 의무를 숙지하고 있다.

CFIP(Concern for Information Privacy) (Smith et al., 1996)
CFIP_1. 나는 기업으로부터 (개인)정보를 제공할 때 두 세 번 생각하고 제공한다.
CFIP_2. 나는 기업이 (개인)정보를 과다하게 많이 수집한다고 생각한다.
CFIP_3. 기업은 권한이 없는 사람들이 (개인)정보에 접근할 수 없도록 다양한 조치를 취해야 된다고 생각한다.
CFIP_4. 기업은 (개인)정보를 허가되지 않은 어느 다른 목적으로 사용하여서는 안 된다고 생각한다.
CFIP_5. 나는 개인정보를 제공할 때 약관을 자세히 읽어봐야 한다고 생각한다.

정보보호 정책 준수의도(CI : Compliance Intention) (Hearath & Rao, 2009)
CI_1. 나는 우리 기업에서 요구하는 (개인)정보보호 지침이나 절차가 내가 수행하는 업무에 도움이 된다고 생각한다.
CI_2. 나는 우리 기업에서 요구하는 (개인)정보보호 지침이나 절차가 나의 업무수행에 필요하다고 생각한다.
CI_3. 나는 나의 업무 수행에 불편함이 있어도 (개인)정보보호 지침이나 절차를 따라야 한다고 생각한다.
CI_4. 나는 고객정보 제공이나 이용 시 궁금한 점이 있을 때 직장동료의 의견보다 개인정보보호 지침이나 절차가 최우선시 되어야 된다고 생각한다.
CI_5. 나는 (개인)정보를 사용할 때 우리 기업에서 요구하는 (개인)정보보호 지침이나 절차에 명기된 책임을 이행할 의도가 있다.

About the Authors

오 진 욱 (jwoh0915@hanyang.ac.kr)

한양대학교에서 MBA와 경영학(경영정보학 전공)박사를 받았으며 현재 한양사이버대학교 해킹보안학과 겸임교수로 재직 중이다. 주요 관심분야는 정보보호 관리체계(ISMS), 개인정보보호, 데이터베이스보안, Knowledge Management 등이다.

백 승 익 (sbaek@hanyang.ac.kr)

George Washington University에서 MBA와 경영학 박사를 받았으며 현재 한양대학교 경영대학 교수로 재직 중이다. 주요 연구분야는 Business Intelligence, Data Science, 그리고 Digital Transformation 등이다.