「정보시스템연구」 제25권 제3호
한국정보시스템학회
2016년 9월, pp. 117～146

http://dx.doi.org/10.5859/KAIS.2016.25.3.117

조직내 최종사용자의 합목적적인 정보보호 시스템 사용 내재화와 학습, 피드백 추구 행동 연구

김 민 웅* · 정 기 주**

〈목 차〉

Ⅰ. 서 론

정보보호가 금융회사를 비롯한 기업 및 공공기관에서 이미 주요한 관심사가 되었음에도 불구하고, 국내 금융회사들에서 빈번하게 발생하는 고객정보, 개인정보 유출사고는 끊이지 않고 있다. 2011년 7월이후 하나SK카드, 삼성카드, IBK 캐피탈, 한국 스탠다드챠타드 은행, 한국씨티 은행에서 정보유출 사고가 발생하였으며, 2014년 1월에는 KB카드, NH카드, 롯데카드사의 1억 건이 넘는 정보유출사고가 발생하였다. 해당 카드사의 FDS(Fraud Detection System) 구축 프로젝트에 참여한 협력업체 직원이 카드사의 고객 신용정보를 암호화가 해제된 상태로 USB를 통해 외장 하드디스크에 저장하여 유출했다는 것이다(보안뉴스, 2014). 아무리 암호화 정책을 세워 고객DB를 암호화하여도, 매체제어 기술을 도입하여 통제를 하여도 이런 유출사고가 발생한 것은 기술적인 대책으로는 정보유출을 차단하기에 충분하지 않다는 것을 말해

* 전남대학교 대학원 전자상거래 협동과정 박사과정, alexkimbox@gmail.com
** 전남대학교 경영대학 교수, kcheong3@chonnam.ac.kr, 교신저자

주고 있으며, 또한 일련의 정보유출은 정보접근권한을 가진 내부 직원들에 의해 발생했다는 특징을 가지고 있다(임명성, 2012).

금융회사를 비롯한 조직에서는 내부자의 정보유출 사고를 포함하여 정보보호에 대한 위험수준을 낮추기 위해 해커 혹은 바이러스와 같은 외부로부터의 침입을 막기 위한 기술적인(technology -focused) 접근방법으로 문제를 해결하기 위해 노력하였다(Spears & Barki, 2010). 하지만 이미 여러 연구에서나 현실에서 증명된 바로는 기술적인 접근법의 경우 항상 존재하는 약점을 악용할 가능성이 상존하는데다가, 조직의 구성원들이 잠재적인 정보보호 위험을 인식하고 여기에 대응하지 못한다면 기술적인 대책만으로는 조직의 정보자산을 보호하는 데에 충분치 않다(Lebek et al., 2013).

정보유출을 비롯한 정보보호 관련 사고는 주로 내부직원의 악의 없는 단순실수에서부터 고의적인 유출행동을 포함하여 그 비중은 50~70%를 차지한다고 알려져 있다(Haeussinger & Kranz, 2013). 그와 같은 상황에서 내부조직원은 가장 약한 고리로 취급되고 있다(Lebek et al., 2013).

하지만 약한 고리이면서 결국에는 문제해결의 원천이 바로 조직구성원이기에(Spears & Barki, 2010), 정보보호행위가 조직원들에 의해 지속적으로 수행되고 마치 제2의 본성과 마찬가지로 행해질 때 기업의 정보보호는 확보될 수 있다(Thomson et al., 2006).

이런 맥락에서 조직구성원들의 낮은 수준의 정보보호 정책 준수에 주목하면서, 이를 준수하도록 하는 것이 조직내 정보보호 문제의 핵심(Siponen & Vance, 2010)이라는 주장과 연구가 진행되었다. 또한 개인의 정보보호 행동수준을 높임으로써 보안문제를 해결하고자 연구가 진행되었는데, 조직의 정책 및 규정을 준수하는 조직원의 의식, 심리적 태도에 초점을 맞추는 논의(D'Arcy et al., 2009; Herath & Rao, 2009)가 그것이다.

하지만, 기술적인 접근에서 정책 및 규정준수, 조직원의 의식과 태도, 자발성에 이르기까지 진행된 연구에서도 조직원들을 문제(problem)에서 해결방안(solution)화하는 방법에 대한 구체적인 연구는 미비하였다.

현재 금융회사를 비롯한 대다수의 회사조직에서는 정보시스템에 대한 외부로부터의 침입(해킹, DDos공격 등)에 대비하여 탐지 및 방어를 위해 인프라차원의 전문가용 정보보호시스템을 갖추고 있다. 뿐만 아니라 업무담당자들이 정보 조회, 처리를 함에 있어 접근권한통제, 암호화 및 해제, 문서암호화, 단말기내 개인정보 검색 및 삭제 솔루션, 바이러스백신, USB등의 매체제어 솔루션 등 사용자용 정보보호 시스템을 도입한 상태이다. 본 연구에서 정보보호 시스템이라고 할 때, 후자인 사용자용 정보보호 시스템을 의미한다.

이러한 시스템에는 정보보호 정책과 지침이 반영되어 있으므로, 결국 정보보호 정책과 지침을 준수하도록 하려면, 사용자로 하여금 정보보호 시스템을 설계한 취지에 맞게 쓰도록 하는 것이 최선의 방법이라 할 수 있다. 이를 조직내 최종사용자의 합목적적인 정보보호 시스템 사용 내재화(Faithfulness of Appropriation)로 개념화할 수 있다(Chin et al., 1997).

이는 정보기술 수용에 관한 조직차원의 연구인 적응구조화 이론(Adaptive Structuration Theory; AST)에서 강조한 개인의 GDSS (Group Decision Support System)사용과 이에

따른 성과는 그룹 구성원들 개개인의 GDSS 내재화(Appropriation)방식에 따라서 영향을 받는다고 한 것에 이론적 배경을 두고 있다(DeSanctis & Poole, 1994).

정보보호 학문을 크게 분류하면, 정보보호 기술 분야와 정보보호 경영분야로 나눌 수 있으며, 이런 분류체계에 따른 연구동향을 검토해 본 결과 국내외 모두 정보보호 경영분야의 연구보다 기술분야의 연구가 대단히 활발하게 이루어졌으며, 상대적으로 정보보호 경영분야는 미비하다고 볼 수 있다(김혜리 등, 2014).

정보보호 기술이 발전함에도 불구하고 정보유출 사고가 발생하는 이유는 정보보호를 하는 주체와 경영흐름에 필요한 조치를 충분히 고려하지 못하고 있기 때문이며, 이런 점을 개선하고 정보보호 분야의 균형적인 발전을 위해서는 암호화 연구, 시스템, 네트워크 보안 등에 관한 기술 분야뿐만 아니라 정보보호 경영분야 특히, 정보보호 인적분야 및 정보보호 개인행위를 분석하는 연구가 반드시 필요하다(김혜리 등, 2014).

구체적으로 본 연구의 목적은 다음과 같다. 첫째, 조직원들의 정보보호 행위의 구체적인 형태로서 정보보호 시스템을 올바르게 사용하게 하는 데에 최종사용자의 학습활동과 피드백 추구행동의 영향 관계를 규명하려 한다.

둘째, 조직원들의 능동적인 학습활동과 피드백 추구 행동에 대해 선행연구를 통해 밝혀진 정보보호 영향요인들이 어떠한 영향을 미치는지를 알아본다.

셋째, 변수들의 구조적 관계를 검정하여 정보보호 시스템 사용 내재화를 위한 즉, 내부의 정보자산 보호와 유출사고 위험수준을 낮추기 위한 효과적인 방안에 대한 시사점을 제시한다.

본 연구에서는 연구목적을 달성하기 위하여 문헌연구와 실증연구를 병행하였다. 문헌연구를 통해서 정보보호에 관한 조직차원의 요인과 개인차원의 요인이 최종사용자의 조직내 학습활동과 피드백 추구 행동에 그리고 최종사용자의 합목적적인 정보보호 시스템 사용 내재화에 어떤 영향을 미치는 지 변수간의 가설 설정과 검정을 위한 이론적 배경을 구축하였다.

본 연구의 구성은 다음 장에서 이론적 배경을 그리고 연구모형과 가설을 제시하고, 그 다음으로 실증분석을 토대로 가설을 검정한다. 마지막에는 결론과 시사점을 제시한다.

Ⅱ. 이론적 배경

2.1 정보보호 관련 행위이론

지난 10 여년간 조직 구성들원들의 정보보호 의식과 행동에 관한 연구는 몇가지 이론에 근거하여 수행되었는 바, 이 분야에서 가장 많이 사용된 이론으로는 합리적 행동이론/계획된 행동이론, 일반 억제 이론, 보호 동기 이론, 기술수용 모델 등을 들 수 있다(Lebek, et al., 2013). 위의 이론 중에서 빈도수가 가장 높은 합리적 행동이론/계획된 행동이론과 전통적인 기술수용모델을 살펴보고,이에 더하여 정보기술 수용에 관한 조직적 차원의 연구인 적응구조화 이론을 이론적 배경으로 살펴보려고 한다.

2.1.1 합리적 행동이론/계획된 행동이론

합리적 행동이론(Theory of Reasoned Action: TRA)과 그 확장인 계획된 행동이론(Theory of Planned Behavior: TPB)은 연관된 이론으로서,

정보보호에 관한 조직구성원의 행동과 의식뿐만 아니라 조직원의 자기계발 참여 결정에 관한 주요한 요인을 연구하는데 유용한 프레임웍을 제공한다(Hurtz & Williams, 2009).

이 이론에서는 행위 의도(intention to behave, behavior intention)는 실제 행위(actual behavior)의 선행요인으로 파악된다. 이 이론에 의하면, 행위의도는 행위에 대한 태도(attitude toward behavior), 주관적 기준(subjective norms), 지각된 행동 통제(perceived behavioral control) 등의 세 가지 요소에 의해 결정된다고 한다(Ajzen, 1991).

먼저, 태도는 인간의 행동을 설명함에 있어서 중요한 요인 중 하나로서, 어떤 사람 또는 사물에 대한 태도를 의미하는 것이 아니라, 사람의 행위에 대한 태도를 말하는데, 사람이 특정한 행위를 수행하는 데 있어서 개인이 가지는 호의적 감정을 의미하며, 이 분야의 연구에서 태도란 정보보호 정책의 준수에 대한 태도를 나타낸다(Pahnila et al., 2007).

다음으로 주관적 기준은 행동을 실행함에 있어서 자신의 판단의 기준이 될 수 있는 준거집단의 사람들이 해당 행위의 수행 여부에 대해 어떻게 생각하고 있는지를 말한다. 즉, 자신들에게 중요한 사람들이 자신이 수행하는 특정한 행위를 어떻게 생각하는지를 나타낸다. 이것은 규범적 신념(normative beliefs), 사회적 요인 등으로도 불린다(Lebek et al., 2013).

마지막으로 지각된 행동통제는 TRA에서 도입되었는데, TPB에서는 자기 효능감(self-efficacy)으로 불린다(Lebek et al., 2013). 지각된 행동통제는 특정한 행위를 하는데 이용 가능한 자원과 기회에 대한 사람들의 생각을 나타내는데 반해, 자기효능감은 특정한 행위를 할 수 있는 자신들의 능력에 대한 생각을 나타낸다(Lebek et al., 2013).

TPB는 가장 예측성이 높은 설득 이론으로서, 다양한 분야에서 광범위하게 활용되고 있으며, 위에서 본 태도, 주관적 기준, 지각된 행동 통제에 의해서 큰 영향을 받는 개인의 정보보호 정책을 준수의도를 설명하고 분석하는데 널리 사용되고 있다(Ifinedo, 2012).

2.1.2 기술 수용 모델

기술 수용 모델(Technology Acceptance Model: TAM)은 1980년대 후반부터 진행되어 온 정보기술의 수용에 관한 연구이론으로서, 많은 연구자들에 의하여 계속적으로 검증, 확장되어왔고 이론과 실증을 통하여 지지되고 있는 모델이다(강소라 등, 2008).

TAM은 개별사용자의 정보기술 수용에 영향을 미치는 영향을 설명하기 위해 신념(belief)-태도(attitude)-의도(intention)-행동(behavior)으로 이어지는 합리적 행동이론(TRA)을 근간으로 사용하였다. TAM에서는 지각된 유용성(perceived usefulness)과 지각된 사용용이성(perceived ease-of-use)이라는 개념을 도입하였는데, 지각된 유용성은 해당기술을 사용함으로써 자신의 직무성과를 향상시킬 수 있는지에 대한 주관적인 확률로 정의된다. 이에 반해서 지각된 사용용이성은 해당 기술을 사용하는데 필요한 노력의 정도를 나타낸다.

정보보호 측면에서 TAM 의하면, 조직원들이 정보보호 정책을 준수하려는 의도를 결정하는데 있어서 정보보호 시스템의 사용을 통해 얻을 수 있는 유용성과 사용 용이성의 영향을 받는다는 것이다. 또한 정책의 유용성과 정책사용의 용이성 이외에도 정책의 명확성, 간결성, 포괄성

등이 사용되고 있다(Haeussinger & Kranz, 2013).

하지만, TAM에서는 정보기술을 수용하는데 고려하는 기술적인 요인들에 대해서만 다루고 있고, 연구대상도 개인이 자의적으로 사용하는 기술을 중심으로 검증됨에 따라, 조직에 도입된 그룹웨어, 인트라넷, 정보보호 시스템 등의 조직 정보시스템 수용에 관한 연구는 미흡하다.

2.1.3 적응 구조화 이론과 합목적적인 정보보호 시스템 사용 내재화

정보기술에 대한 조직차원의 수용성 등에 대한 연구인 적응구조화 이론(AST)에 의하면, 그룹과업의 결과는 그룹이 어떠한 구조(Structures)를 이루며, 정보기술들을 어떻게 내재화(Appropriation)하는가에 의해 영향을 받는다는 것이다(DeSantis & Poole, 1994).

조직내에서 구조(Structures)라는 것은, 조직의 업무, 프로세스, 문화, 규칙, 정보기술의 사용패턴, 조직 구성원들의 지식 등 조직이 구체적으로 작동되는 특징들(Mechanism)을 일컬으며, 어떠한 구조적 특성들을 만들어 가는 과정을 구조화(Structuration)라고 한다. 그런데, 구조화 과정은 일방적인 수동적 적응과정만은 아니라서, 조직 구성원들의 기존의 구조에 자신들을 맞추기도 하고, 역으로 구성원들 간의 상호작용과정이 진행됨에 따라 새로운 구조를 지속적으로 재생산하기도 한다. 따라서 개인의 정보기술 사용과 그에 따른 성과는 조직구성원들의 정보기술 내재화방식과 내재화정도에 따라서 영향을 받는다고 볼 수 있다(Poole, 2008).

내재화는 사용자들이 주어진 사회적 구조를 자신에 맞도록 적절하게 사용하고 있는 정도로 보기 때문에 정보시스템 사용의 유효성을 결정할 수 있는 개념 가운데 하나로 간주된다(노희옥, 2008). 따라서 정보보호 시스템의 사용자인 주요 정보접근 권한과 처리권한을 가진 조직구성원들에게는 기술적 적합도나 인구통계적 요인들보다는 설계된 의도대로 충실히 사용하는가 즉 충실한 내재화가 성과에 큰 영향을 미칠 것으로 판단할 수 있다.

정보보호 시스템에서 충실한 내재화에 대한 논의를 위해 AST의 주요개념을 적용시켜 내재화를 구체화하면 다음과 같다. 합목적적인 정보보호 시스템 사용이란 “최종사용자가 정보보호 시스템의 목적대로 해당 시스템을 올바르게 이용하는 것(Chin et al., 1997)”을 의미하며, 합목적적인 정보보호 시스템 사용 내재화란 “최종사용자가 정보보호 시스템의 합목적적인 사용에 익숙해지고 숙달되는 것”으로 정의할 수 있다(Wheeler et al., 1996).

올바른 정보보호 시스템의 사용은 개발 목적대로 사용하는 것으로 본래 의도(Original intent), 객관적 정신(Objective spirit), 기술정신(the sprit of technology)에 입각하여 사용하는 것이며, 이를 통해 충실한 내재화(Faithfulness of Appropriation)가 달성될 수 있다고 본다(Chin et al., 1997).

내재화(Appropriation)의 개념은 적응구조화 이론(AST)에서 출발한다(Poole, 2008). 적응구조화 이론은 기술중심적인 시각에서 벗어나 기술 외적 측면을 강조하는 것이 특징인데, 이와 관련하여 동일한 기술의 정신(the spirit of technology)이 구현되어 있더라도 기술사용에 대한 평가(Evaluation of Technology Usage)가 다르고 이는 내재화 정도(Assessment of Faithfulness)에 영향을 준다는 것이다(Chin et al., 1997).

일반 업무용 시스템의 경우와 마찬가지로 정

보보호 시스템의 경우도, 동일한 시스템을 사용하더라도 사용하는 조직의 조직구조, 문화, 과업, 상호작용과 같은 조직의 프로세스적 차이가 서로 다른 활용을 가져오고, 해당 시스템에 대한 상반된 평가가 가능하다는 것이다. 이런 맥락에서 적응구조화 이론은 같은 정보보호 시스템을 도입하고 사용하더라도 조직에 따라서 다른 사용 형태와 성과를 가져오게 되는 현상을 설명하는 데 매우 유용하다고 할 수 있다. 요약하면, 동일한 시스템을 도입한 두 조직은 비록 같은 기술을 사용하고 있지만 자신들의 과업에 있어서 이를 어떻게 적용시킬 것인가에 대해 인지하고, 활용하는 과정에서 많은 차이가 있고, 이는 다시 성과의 차이로 나타나는 것이다 (Sambamurthy & Chin, 1994).

내재화의 특징을 세 가지로 분류하여 고찰할 수 있는데, 내재화는 충실성(faithfulness, 개발된 의도에 맞게 사용하는 정도), 합의성(consensus, 어떻게 사용되어야 할 것인가에 대한 구성원간의 합의정도), 태도(attitude, 사용에 대한 구성원들의 시각) 등으로 특징지워질 수 있다는 것이다(Chin et al., 1997).

일반적인 정보시스템의 경우에는 세 가지 특징 중에서 충실성이 내재화의 성과를 측정하는데 가장 적합하다고 하였다(Chin et al., 1997). 이는 곧 정보보호 시스템 최종 사용자들이 그 시스템의 개발의도대로 사용한다면 이는 충실한 내재화가 일어났다고 간주할 수 있으며, 이러한 충실한 내재화는 곧 합목적적인 사용의 내재화를 의미한다.

2.2 정보보호 영향요인 선행연구

앞에서 사용자의 정보보호 의식과 행위 연구의 기반이 되는 이론들과 더불어 조직 및 개인 차원에서 정보보호에 영향을 미치는 요인들에 관한 선행연구를 간략히 살펴보려한다.

정보보호 관련 연구자들이 자주 언급한 것과 같이 사용자의 정보보호 의식의 결여는 정보보호 실패의 주요원인으로 꼽을 수 있다 (Thomson & von Solms 1998; Siponen 2000). 하지만 정보보호 정책을 인지하고 있는 사용자들도 다양한 상황에서 정보보호 정책을 준수하지 않을 수 있기 때문에(Pahnila et al., 2007; Workman et al. 2008), 성공적인 보호프로그램을 만들기 위해서는 사용자로 하여금 정보보호 정책을 준수하도록 하는 즉, 사용자행위에 대한 이해가 관건이라 할 수 있다(Proctor & Byrnes 2002).

최근에, 최종사용자의 정보보호 행위의 중요성에 대한 인식이 높아지고, 정보시스템 연구자들과 실무자들은 다양한 이론적 관점에서 현상들을 이해하기 위해 시도하였다. 하지만, 정보보호라는 주제는 기본적으로 복합적, 동적, 다면적 속성을 가지고 있어(박정국, 2014), 이러한 정보보호 연구의 특성으로 인해 정보보호에 대한 통합적인 관점을 제시하지는 못하고 있다 (Abraham, 2011). 또한, 정보보호에 대한 선행연구들은 연구성격상 다양한 연구주제들을 다루고 있을 뿐만 아니라 일반적인 정보보호 연구흐름을 제공하는 수준에 머물러 있어 (Siponen & Oinas-Kukkonen, 2007; Zafar & Clark, 2009), 사용자 행동관점에서 최종 사용자의 정보보호 행위에 영향을 주는 요인, 준수행위에서의 장애요인 등에 대한 분석이 미흡하였다(Abraham, 2011).

사용자의 정보보호행위에 영향을 주는 요인을 찾아 사용자 행위를 개선하기 위한 방안을

모색하는 시도를 진행한 Leach(2003)의 연구에 의하면, 영향요인들을 두 개의 그룹으로 구분할 수 있다. 첫 번째 그룹은 조직에서 사용자들에게 원하는 행동이 무엇인가를 중심으로, 그리고 두 번째 그룹은 기준에 맞춰 행동을 하게 만드는 사용자의 개인적인 의지에 영향을 주는 요인들로 구분하였으며, 그 구분에 기초하여 연구를 정리하면 <표 1>과 같다.

정리하면, 주로 외국에서 이루어진 상당수의 연구들은 조직내에서 부정적인 시스템 사용을 어떻게 예방할 수 있는가를, 그리고 사용자들의 정보보호 행위를 하도록 동기부여할 수 있을지에 대한 연구가 주를 이루는 것으로 보여진다. 몇몇 연구들은 정보보호 정책을 사용자들이 어떤 사유로 지키지 못하는지를 서술하면서, 조직내 준수행위의 장애물에 대해 설명하고 있다.

비록 이런 연구들이 사용자의 행위를 광범위하게 설명하는 노력은 하고 있으나, 결국은 사

<표 1> 정보보호 영향요인에 대한 주요논의

정보보호 행위에 영향을 미치는 요인	해당 논문	요약
조직차원의 필수적인 정보보호요소들 1. 정보보호 정책 2. 의사소통 행위 3. 의식제고 컨텐츠	Anderson and Agarwal, 2010 Frank et al., 1991 Helin and Sandstrom, 2007 Johnston and Warkentin, 2010	- 조직은 공식적인 정책에만 의존하고 있지 않음 - 정보보호 관련연구에서 정보보호 정책이 조직원들에게 어떻게 의사소통되는 지에 대한 연구는 부족한 편임
조직원차원에서 정보보호 행동에 영향을 미치는 요인 1. Management Influences 2. Peer Influences 3. Detterrence Efforts 4. Rewards 5. Employee Participation	Albrechtsen and Hovden, 2010 Aytes and connolly, 2003 Herath and Rao, 2009 Kankanhalli, 2003 Spears and Barki, 2010 Stanton et al., 2004 Straub and Welke, 1998	- 관리자는 정보보호 준수행위에서 모범을 보여야 함 - 조직원들은 정보보호 행위를 함에 있어 동료들의 행동을 관찰함 - 정보보호행위에 사용자 참여는 긍정적인 결과로 이어짐 - 보상은 직접적으로 정보보호 행위에 영향을 미치지 않음
사용자 개인차원의 요소 1. 사용자의 지식 2. 자기 효능감	Aytes and connolly, 2003 Dinev and Hu, 2007 Loch and Conger, 1996 Ng et al., 2009 Rhee et al., 2009 Workman et al., 2008	- 자기 효능감은 정보보호행위의 중요한 요소 - 자기 효능감이 높은 사람들에 대한 이해와 어떻게 개발한 것인가에 대한 논의가 필요함
사용자의 개인적인 가치와 행위기준 1. 태도 2. 신념	Bulgurcu et al., 2010 Gattiker and Kelly, 1999 Leonard et al., 2004 Loch and Cogner, 1996	- 태도는 정보보호 행위에 있어서 강한 영향을 미침
사용자의 심리적 계약관계 1. 심리적 책임감 2. 조직의 약속 3. 신뢰 4. 절차공정성	Anderson and Agarwal, 2010 Luker, 1990 Stanton et al., 2003 Workman et al., 2008	- 조직공정성에 대한 조직원들의 인식은 정보보호 행위에 영향을 미침 - 모니터링에 대한 선행공지를 통해 신뢰형성에 부정적인 효과를 예방할수있음 - 조직의 약속과 정보보호행위에는 상관성이 높음
정보보호 기술의 수용에서 요구되는 요소 1. 사용용이성 2. 정보보호 기술의 효과성	Cannoy and Salam, 2010 Dinev and Hu, 2007 Herath and Rao, 2009	- 인지된 사용용이성은 안티스파이웨어기술의 채택을 비롯한 정보보호 기술수용에 영향을 줌

용자의 의식에 의존하고 있으며, 그 의식은 실제 행동에 반영되고 있지 못한 경우가 많다(Kruger & Kearney, 2006). 사용자들의 정보보호 행위를 다룬 대부분의 연구들은 정보보호 행위에 대한 사용자 의식에 초점을 맞추고 있어 실제 행동을 관찰하지 못하는 데에 따른 연구의 한계를 노정하고 있다(Abraham, 2011).

이에 본 연구에서는 그 실제행동으로 보여주는 정보보호 시스템 사용에 대한 내재화로 연결되는 사용자의 능동적인 활동을 밝혀 사용자의 정보보호 행위를 촉진하도록 하는 조직의 활동에 의미 있는 시사점을 제공하고자 한다.

Ⅲ. 가설설정 및 연구모형

3.1 가설설정

3.1.1 최고경영진의 지원

조직의 정보보호수준 향상에 필요한 많은 요인 중에서 최고경영진의 지원은 새로운 기술과 제도의 도입을 비롯하여 정보보호 정책의 실질적인 성공여부를 예측할 수 있는 척도(Beatty et al., 2001)이며, 최고경영진의 정보보호에 대한 관심과 강조는 조직내에서 정보보호 전담부서와 타 부서간의 협조를 증진시켜 줄 것이므로(Kankanhalli et al., 2003), 보안업무 담당자는 보안활동이나 정책집행시 효과적인 달성을 위해 반드시 최고경영층의 지원과 그 영향도를 고려해야한다(Knapp et al., 2006).

또한 최고경영진의 지원정도가 높을수록 정보보호에 필수적인 조직내 자원(resource)을 동원하는 데에 훨씬 용이하며, 조직구성원들의 정보보호의식수준을 충분한 수준으로 구축하고 유지하는 데에도 결정적 요인이 된다(Tsohou et al., 2008).

조직원들의 정보보호 정책준수(Compliance)에 최고경영진이 미치는 영향을 분석한 한 연구(Hu et al., 2012)에 의하면, 정보보호에 최고경영진이 관심을 가지고 참여하는 것은 조직문화에 큰 영향을 미치고, 이것은 다시 정보보호 정책의 준수에 대한 직원들의 태도에 직간접적으로 큰 영향을 미친다고 하였다.

이에 본 연구에서는 위의 연구를 응용하여, 최고경영진의 영향에 대한 다음과 같은 가설을 설정하였다.

H1a. 최고경영진의 지원은 최종사용자의 합목적적인 정보보호 시스템 사용내재화에 정(+)의 영향을 미칠 것이다.

H1b. 최고경영진의 지원은 최종사용자의 조직내 학습활동에 정(+)의 영향을 미칠 것이다.

H1c. 최고경영진의 지원은 최종사용자의 피드백 추구 행동에 정(+)의 영향을 미칠 것이다.

3.1.2 정보보호 지침 제공

조직이 조직구성원에게 정보보호 정책과 지침을 수립하여 제공하는 것은 비즈니스를 영위하는데 있어서 지켜야할 규제 혹은 가이드라인에 대한 준수(Compliance)의 의미뿐만 아니라 정보시스템보호 및 관리에서 조직으로서 확보해야할 주요한 자원으로 평가되고 있다(Chan et al., 2005). 또한 정보보호 정책과 지침 제공은 일반적인 의미에서 조직이 정보보호를 위해 각 단위의 책임, 역할, 행동지침을 정의하여 배포한 문서로 이를 통해 조직의 정보자산을 보호하기 위한 적합한 방법을 구체적으로 제시하

는 것이다(D'Arcy et al., 2009).

기존연구에서는 정보보호 정책의 효과성에 대한 상반된 관점의 논의들이 이루어지고 있다. 한편에서는 정보보호 정책의 존재야말로 위반 행위 억제 메카니즘을 가동시켜 조직구성원들의 정보보호 위반 혹은 미준수 행위를 사전에 예방하는 효과를 가져온다고 하고(D'Arcy et al., 2009), 다른 한편에서는 정보보호 정책은 정보보호 미준수 행위에 별로 영향이 없다고 주장하였다(Lee et al., 2004).

이러한 상반된 주장들은 조직원들의 정보보호 의식의 결여로 인해 결과가 달라진다고 하는 논의로 볼 수 있으며, 이런 점에서 '단순한' 정보보호 정책의 존재 자체로는 불충분하다는 점을 강조하고 있다. 또한 정보보호 정책은 이해하기 쉽고, 이용용이성 또한 충분하도록 구체적으로 제공되어야만 한다는 점을 강조하고 있다. 이를 정보보호 정책을 구체화하여 실행지침으로 제공한다는 의미에서 '정보보호 지침제공'으로 의미정리를 할 수 있겠다(Haeussinger & Kranz, 2013).

조직에 정보보호 정책이 존재한다는 것 자체만으로는 충분하지 않고, 정책이 모호하지 않고, 쉽게 이해할 수 있어야 하며, 이러한 정책을 작성함에 있어서 정책품질 요소를 갖추어야 하는데, 포괄성(breadth), 명확성(clarity), 간결성(brevity)의 세 가지를 제시하고 있다(Goel & Chengalur-Smith, 2010).

따라서 정책이 지침으로 명확하고 간결하게 작성되어 최종사용자 제시되어야 하는 것을 조직차원의 정보보호 영향요인으로 간주하고, 그 요인이 최종사용자의 정보보호 시스템 활용에 영향을 주는 변수로서 정보보호 지침제공으로 명명하였다.

H2a. 정보보호 지침제공은 최종사용자의 합목적적인 정보시스템 사용 내재화에 정(+)의 영향을 미칠 것이다.

H2b. 정보보호 지침제공은 최종사용자의 조직내 학습활동에 정(+)의 영향을 미칠 것이다.

H2c. 정보보호 지침제공은 최종사용자의 피드백 추구행동에 정(+)의 영향을 미칠 것이다.

3.1.3 정보보호 교육훈련

정보보호 관련교육은 조직이 사용하는 정보보호 대책(information security countermeasures)중의 하나로 조직원들에게 정보보호 정책의 준수를 강화시키며, 시스템 오용으로 인한 잠재적 결과를 주지시키는 역할을 한다(D'Arcy et al., 2009). 또한 해당 기업조직이 제시하는 정보보호 정책을 정확히 이해하고 이를 받아들이도록 하는 요인으로도 작용한다. 하지만 단지 정책의 존재만으로 자동적으로 조직에서 요구하는 행동이 유도되는 것은 아니며, 조직구성원들은 해당 정책의 존재 자체로 조직의 정보자원을 보호하기 위한 요구된 행동을 형성하고자하는 동기를 부여받지 않는다(Bulgurcu et al., 2010).

따라서, 정보보호 교육과 훈련의 중요한 내용인 인식제고 프로그램은 조직의 실행활동(practice)중 하나로 정보보호 행위를 유도하는 핵심요인중 하나임에는 틀림없다(Chan et al., 2005).

정보보호 인식교육으로 인해 조직원들은 정보보호에 대한 중요성을 인식하고 관련 지침에 대한 준수가 제대로 이루어지지 않을 경우 자신이 속한 조직에 어떠한 부정적 영향을 미치게 되는지 이해하게 된다. 또한 이러한 인식의 전환으로 인해 정보보호 정책과 지침을 준수하는 것이 개인의 생산성 저하를 유발하는 원인

이 아니라 자신의 조직을 위해 필요한 절차라는 것을 인식하게 된다(임명성, 2013).

정보보호 교육 훈련 프로그램은 잠재적인 불확실성, 조직의 정책과 책임 등에 대한 조직구성원들의 지식과 인식을 개선시킴으로써 조직의 정보보호를 달성하고자 시행하며(Haeussinger & Kranz, 2013), 조직의 구성원들에게 조직의 정보보호 정책과 절차를 준수하는데 필요한 스킬을 제공하는 것이다(Lee & Lee, 2002; D'Arcy et al., 2009). 정보보호 관리의 가장 중요한 측면은 보안 교육 훈련 프로그램으로서, 이 프로그램의 긍정적인 효과에는 신뢰성 향상, 정보 보호, 정확성 및 신뢰성 향상, 원하지 않는 내부 사건의 감소, 윤리성 및 탐지 역량 증가, 법규의 준수 향상 등이 포함된다(Hagen, et al, 2008).

조직에서 제공하는 정보보호 교육훈련에 지속적으로 노출되어 훈련수준이 높은 조직원들은 정보보호 정책에서 서술하고 있는 행동을 준수하는 사용자들이고, 이들은 사고가 발생하거나, 발생하기 전에 사고를 찾아낼 수 있는 역량을 갖추게 된다(Hagen et al., 2008).

정보보호 교육훈련 프로그램이 정보보호 행동에 영향을 미친다는 것은 여러 연구에 의해 입증된 바 있으며(Haeussinger & Kranz, 2013), 따라서 본 연구에서도 이를 영향요인 변수로 채택하였다.

H3a. 정보보호 교육훈련은 최종사용자의 합목적적인 정보보호 시스템 사용 내재화에 정(+)의 영향을 미칠 것이다.

H3b. 정보보호 교육훈련은 최종사용자의 조직 내 학습활동에 정(+)의 영향을 미칠 것이다.

H3c. 정보보호 교육훈련은 최종사용자의 피드백 추구행동에 정(+)의 영향을 미칠 것이다.

3.1.4 IT지식과 활용능력

선행연구를 보면, 조직구성원 개인의 컴퓨터와 인터넷 관련된 지식과 활용능력이 정보보호 시스템을 사용하는 데에 영향요인이 될 수 있으며, 회사조직에서 주로 사용하는 업무용 단말기인 PC와 인터넷에 대한 지식과 활용능력은 정보보호에서의 자기 효능감(Self-Efficacy)에 긍정적인 영향을 주고 있으며, 자기효능감은 다시 정보보호 노력을 강화시키고 정보보호 행위에 긍정적인 영향을 주고 있음을 실증하였다(Rhee et al., 2009).

또한 사용자들은 개인용 업무 단말기에 설치된 문서암호화 솔루션(DRM Solution), 네트웍 접근 통제(NAC), 개인정보 검색 솔루션, PC 매체제어솔루션, 바이러스 백신 등 정보보호를 위한 사용자 시스템에 대한 지식과 활용능력뿐만 아니라, 실제로 담당업무에 필요한 영업관리시스템, FDS(Fraud Detection System), 자산운용시스템, 교육시스템 등에 대한 지식과 활용능력 역시 정보보호 사용자 시스템과 무관하지 않다고 볼 수 있다(Dinev & Hu, 2007).

개인차원의 정보보호 및 정보시스템 활용능력에 대한 인식과 신념은 개인의 정보보호 행위를 설명하는 데 유용하며, 구체적으로는 개인차원에서 컴퓨터와 인터넷에 대한 수준 높은 역량과 정보보호가 이루어지지 않음으로써 피해를 당했거나 이를 어겨서 문제가 되었던 경험은 분명히 정보보호 인식과 행위에 영향을 주고 있다(Rhee et al., 2009).

IT 지식과 활용능력은 안티 바이러스 소프트웨어, 안티 스파이웨어, 그리고 팝업 창 제어 기능 사용 등의 보안 소프트웨어를 활용할 수 있는 역량과 연관되어 있으며, 시스템에 접근할

때 인증 패스워드를 어렵게 한다든가 일상적으로 업무와 관련된 문서에 대해 암호화를 진행하거나 백업하는 등 보안 컴플라이언스를 준수하는 데도 연관되어있다.

또한 이는 업무에 사용하는 시스템에 대한 숙련 정도와 경험에도 반영되어있는데, 선행연구에서도 최종사용자의 컴퓨터 사용능력은 업무용 정보시스템 활용에 강한 긍정적인 작용을 한다고 하였다(Torkzadeh et al., 1999).

따라서, 컴퓨터와 인터넷 활용에 대한 자신감과 역량은 결국 정보보호를 위해 필요한 개개인의 능력을 향상시키는 데 기여하는 것으로 가정할 수 있다(Rhee et al., 2009).

H4a. IT 지식과 활용능력은 최종사용자의 조직내 학습 활동에 정(+)의 영향을 미칠 것이다.

H4b. IT 지식과 활용능력은 최종사용자의 피드백 추구 행동에 정(+)의 영향을 미칠 것이다.

3.1.5 부정적 경험

조직원들은 직접적으로 혹은 간접적으로 정보보호와 관련된 각종 스파이웨어, 바이러스, 악성코드, 피싱메일 등으로 인한 사고를 개인적인 영역 혹은 업무영역에서 경험했거나 타인의 경험을 들어보았을 것이다. 이러한 부정적인 경험들로 인해 향후 벌어질 가능성이 있는 유사 상황들을 회피하는데 관심을 가질 것이다. 실제로 개인정보 침해신고 및 상담의 증가는 이에 대한 인식이 점점 높아지고 있음을 보여주고 있다(김영렬, 2010).

이는 정보보호 인식에 대한 긍정적인 작용으로 해석 할 수 있으며, 보안규칙과 지침을 지키지 않아 바이러스 혹은 악성코드로 피해를 입은 경험은 개인의 정보보호 인식을 높이는 것으로 알려졌다(Bulgurcu et al., 2010).

또한 개인적 차원의 부정적인 경험, 예를 들면, 바이러스나 악성코드에 감염되어 본 경험 혹은 개인정보가 유출된 경험, 정보보호 컴플라이언스를 위배해서 조직으로부터 불이익 처분을 받은 경험은 자신의 정보보호에 대한 효능감을 떨어뜨리는 부정적인 인식을 갖게 하지만(Wood & Bandura, 1989), 조직구성원의 보안 위반 경험으로부터 현재 상태를 진단하고 언제, 어디서, 어떤 모습으로 발생할지 알 수 없는 상황에 대해 시행착오적 접근으로 간주한다면 예방이 가능하다고 볼 수 있다(Potosky, 2002), 즉 과거의 부정적 경험은 조직구성원의 고의성이 없는 실수 혹은 무지에 의한 행동에 대해 자율적 예방과 경감활동을 촉진하고 조율하기 위한 방편이 될 수 있다(Compeau & Higgins, 1995).

더욱이 정보유출 사고가 빈번하게 발생하고, 특히 금융회사에서 정보유출 사고는 CEO문책, 영업정지 등의 치명적인 영향을 주는 분위기에서 이런 경험은 오히려 정보보호와 관련된 조직내 학습활동이나 피드백 추구 행동을 활성화 할 것으로 가정하고 이와 관련된 가설을 세워 검증하려 하였다.

H5a. 과거의 부정적인 경험은 최종사용자의 조직내 학습활동에 정(+)의 영향을 미칠 것이다.

H5b. 과거의 부정적인 경험은 최종사용자의 피드백 추구행동에 정(+)의 영향을 미칠 것이다.

3.1.6 조직내 학습활동

일반적인 업무용 정보시스템과 유사하게 정보보호 시스템 역시 도입보다는 도입후의 상황

즉 제대로 된 사용으로 도입의 목적을 달성하여야 함이 무엇보다 중요하다 할 수 있다. 최근의 정보보호 시스템의 도입은 관계법령과 감독기관의 컴플라이언스를 준수하는 차원에서 도입이 급속도로 이루어지게 되어, 맞춤형 정보보호 시스템이 되기보다 기존에 개발된 패키지형을 주로 선택하게 되는데, 중복 혹은 일부 기능의 미비에도 불구하고 불가피한 도입이 진행된 경우도 적지 않다고 할 수 있다.

따라서 정보보호 시스템의 도입이후의 사용환경에 대해 검토할 때, 과업-기술 적합성 모델(TTF, Task-Technology Fit)과 같은 '기술위주의 관점'보다는 '사용자와 그를 둘러싼 사용 환경의 관점'으로의 전환이 필요하다고 하겠다. '사용자 환경, 사용 환경으로의 관점의 전환'의 의미는 정보보호 시스템에 대한 최종사용자의 학습과 훈련 관점을 위주로 하여 운영모델을 채택하는 것이다.

과업-기술 적합성에 초점을 맞춘 모델들은 시스템을 도입하기 전이나 도입당시 행위를 설명하는 데는 적합하지만, 도입이후의 환경에서는 사용자가 주어진 시스템을 어떻게 하면 잘 사용할 수 있을까가 성과를 결정짓는데 더 중요한 요소일 것이기 때문이다. 최종사용자의 학습과 훈련은 성공적인 정보시스템의 도입과 활용을 연구한 선행연구에서도 중요한 요인으로 인식되어 왔지만(Davis et al., 1993), 정보보호 시스템의 유용성과 사용용이성으로 볼 때, 최종사용자의 자발적 학습이 훨씬 더 중요한 역할을 한다고 하겠다. 더욱이 조직내부의 정보보호 수준을 높이기 위해서는 조직원의 자발적인 보안준수를 위한 접근이 필요하다(황인호· 김대진, 2016).

학습은 개인이 행동과 실천의 변화를 위해 새로운 지식과 통찰력을 습득하는 과정(양우섭, 2013)이나, 개인의 자발성에 기초한 정보보호 시스템에 대한 구성원들의 학습은 단순히 새로운 사용법의 숙지 차원이 아니라 정보보호 인식과 행위가 내재화되는 훈련(appropriation training)으로 볼 수 있으며, 훈련과 학습의 양이 증가할수록 최종사용자는 정보보호 시스템이 디자인된 의도대로 충실하게 내재화하게 될 것이다(Wheeler & Valacich, 1996).

H6. 최종사용자의 조직내 학습활동은 합목적적인 정보보호 시스템 사용 내재화에 정(+)의 영향을 미칠 것이다.

3.1.7 피드백 추구행동

피드백 추구행동에 대한 연구는 자기조절(Self-regulation)연구에서 광범위하게 다루어지고 있으며(Ashford & Tsui, 1991), 개념적으로는 '조직에서 개인이 가치 있고 유용한 정보나 자원을 얻기 위해 피드백을 주는 다른 대상에게서 피드백을 추구하는 행위'로 정의할 수 있으며, 피드백은 조직에서 개인의 성공을 위한 필수적이라는 관점을 제공한다(Ashford & Tsui, 1991).

조직 안에서 개인들은 특정 환경의 요구에 적합하도록 그들의 행위를 수정함으로써 적응하게 되는데, 이 과정에서 개인은 적극적으로 자신의 상사나 부하, 동료들로부터 피드백을 추구하며, 이를 통해 지속적으로 발전하고 업무성과를 높일 수 있다. 이러한 추구행위, 도식화(mapping), 해석, 정리 등은 모두 일반적인 형태의 적응(Adaptation)행위에 속한다고 할 수 있다(Ashford, 1986).

피드백 추구 행동은 개인의 능동적인 환경적응행위이며, 직무수행상의 역할 및 성과달성에 유용한 정보 확보 측면에서, 그리고 성과향상에 기여할 수 있다는 측면에서 피드백은 조직구성

원의 성공에 유용한 소중한 자원임을 알 수 있다(Ashford & Tsui, 1991).

피드백 추구 행위를 할 때 피드백을 구하고자 하는 자는 심리적으로 자신과 가까운 원천(자기자신, 동료)을 그렇지 않은 원천(상사)보다 더 많이 선호한다는 연구(Van Dyne & LePine, 1998)에서 보듯이, 심리적인 거리가 가까운 원천에서 제공되는 피드백이 보다 신빙성이 있다고 믿으며, 피드백을 얻는 과정도 수월할 뿐만 아니라, 피드백 획득과정에서의 상호작용도 손쉽기 때문이라 볼 수 있다.

본 연구에서는 피드백 추구 행동은 '정보보호 시스템 최종 사용자가 자신이 정보보호 시스템을 올바르게 사용하고 있는지를 주변사람을 통해 관찰(monitoring)하거나 질문(inquiry)함으로써 확인, 검토하는 행위'로 정의하였다.

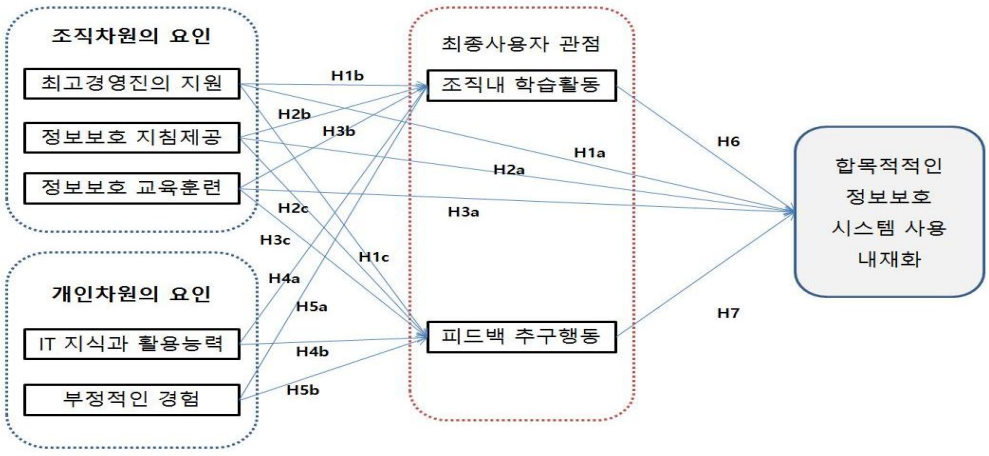
조직구성원의 관점에서 볼 때, 다양한 정보보호 영향요인들에 대해 수동적인 반응이 아닌, 사용자 스스로 정보보호 시스템을 올바르게 사용할 수 있도록 적응하기 위해서 학습활동과 피드백 추구 행동은 필수적 요인이라는 가설을 설정할 수 있다.

H7. 최종사용자의 피드백 추구행동은 합목적적인 정보보호 시스템 사용 내재화에 정(+)의 영향을 미칠 것이다.

3.2 연구모형

앞에서 살펴본 이론적 배경을 바탕으로 본 연구의 모형을 다음과 같이 설정하였다. 본 연구모형은 최종사용자가 정보보호 시스템을 올바르게 사용하도록 영향을 미치는 최종사용자 주변의 촉진 요인들을 최종사용자의 능동적 적응행위(학습과 피드백 추구 행동)를 중심으로 살펴보도록 설계되었다.

최종사용자가 도입된 정보보호 시스템을 의도된 목적대로 사용하도록 하는 요인들과 사용하는 조직의 프로세스적 차이로 서로 다른 사용형태와 성과를 가져오게 되는 현상을 설명하고자 적응구조화 이론(AST)을 바탕으로 '합목적적인 정보보호 시스템 사용의 내재화'를 변수로 채택하였고, 최종사용자의 능동적 행위인 학습활동과 피드백 추구 행동을 매개변수로 채택하였다. <그림 1>에서 연구모형을 정리하여 제시하였다.



<그림 1> 연구 모형

Ⅳ 연구방법

4.1 변수의 측정

본 연구에서는 총 8개의 잠재변수를 사용하고 있는데, 외생잠재변수는 최고경영진의 지원(Top Management Support; TMS), 정보보호 지침제공(Provision of Guideline; POG), 정보보호 교육훈련(Security Education & Training Activities; SETA), IT지식과 활용능력(IT Ability; ITA), 부정적인 경험(Negative Experience; NEX)이며, 매개변수로는 조직내 학습활동(Learning Activities in Organization; LAO), 피드백 추구행동(Feedback Seeking Behavior; FSB), 내생잠재변수로는 합목적적인 정보보호 시스템 사용 내재화(Faithfulness of Appropriation; FOA)를 설정하였다. 모든 변수에 대한 설문은 리커트 5점 척도를 사용하였으며, 본 연구에서 사용된 변수들의 조작적 정의는 다음과 같다.

TMS는 '조직 최고경영진의 정보보호에 대한 관심과 강조수준에 따른 지원정도(Knapp et al., 2006; 임명성, 2013)'로서 Knapp et al.(2006)의 측정항목을 활용하여 측정하였다.

POG는 '조직의 정보보호를 위해 조직구성원에게 제시된 정책과 행동지침(Haeussinger & Kranz, 2013)'으로서, 이를 측정하기 위해 Goel and Chengalur-Smith(2010)의 연구에서 개발한 설문항목을 활용하였다.

SETA는 '정보보호를 위해 조직구성원에게 제공되는 정기・비정기 온라인 및 오프라인 교육과 모의훈련(D'Arcy et al., 2009)'으로서, 이를 측정하기 위해 D'Arcy et al.(2009)에서 제시된 항목을 사용하였다.

ITA는 '개인이 정보보호 시스템을 사용하는데에 필요한 컴퓨터와 인터넷의 활용능력(Rhee et al., 2009)'으로서, 측정을 위해 Bassellier et al.(2003)와 Rhee et al.(2009)의 항목을 활용하였다.

NEX는 '과거에 개인 혹은 조직차원에서 사이버 공격, 피싱 등에 노출되어 정보유출이 되거나 이로 인한 피해, 시스템 사용에 지장을 초래했던 경험(Rhee et al., 2009)'으로서, Liang and Xue(2010)의 항목과 Rhee et al.(2009)의 항목을 보완하여 활용하였다.

LAO는 '조직구성원이 정보보호 관련 교육이나 훈련이라는 자극에 대해 적응하고자 지식과 기술의 습득을 해나가면서, 이를 향상시키기 위하여 다양한 활동에 참여하며, 적응하는 개인의 계발과정(Hurtz & Williams, 2009)'으로 정의되며, 이를 측정하기 위해 Hurtz and Williams(2009)의 항목을 활용하였다.

FSB는 '정보보호 시스템 사용을 제대로 하는 있는지에 대해 동료를 관찰, 직접 질문 등의 방법으로 확인, 검토하는 행위(Ashford, 1986)'로 정의하였으며, 이를 측정하기 위해 Callister et al.(1999)의 측정 도구를 사용하였다.

FOA는 '최종사용자인 조직원이 정보보호 시스템을 본래 개발된 의도도 맞게 합목적적인 형태로 사용되는 것(Chin et al., 1997)'이라고 정의하고 있으며, 이를 측정하기 위한 도구를 개발하여 제시하였는바, 본 연구에서도 Chin et al.(1997)에서 측정 도구로 제시한 항목들을 선택하여 합목적적인 정보시스템 사용의 내재화를 측정하였다.

위와 같이 변수의 측정내용과 출처를 <표 2>에서 제시하였다.

<표 2> 변수의 측정

변 수	문 항	출 처
최고 경영진 지원 (TMS)	1. 최고경영진의 정보보호에 대한 관심 2. 최고경영진의 정보보호에 대한 중요성 이해 3. 최고경영진의 정보보호 시스템 투자 지원 4. 최고경영진의 정보보호에 전략적 의미 부여 5. 최고경영진의 정보보호 정책 위반사항에 대한 조치 6. 최고경영진의 정보보호 정책준수의 가치	Knapp et al., 2006
정책지침제공 (POG)	1. 정보보호 정책과 지침 사내 온라인 제공여부 2. 정보보호 정책과 지침 이해 용이성 3. 정보보호 정책과 지침 명확성 4. 정보보호 정책과 지침 내용 포괄성 5. 정보보호 정책과 지침은 회사의 법규위반 방지에 기여 정도 6. 정보보호 정책과 지침은 직원에게 유용한 정도	Goel and Chengalur-Smith, 2010
교육훈련 (SETA)	1. 조직에서 정보보호 교육훈련 제공여부 2. 조직에서 정보보호 시스템 활용법 교육 3. 정기·비정기 모의훈련 실시 여부 4. 정보보호 프로그램 적용과 책임 교육 5. 정보보호 교육훈련의 직원에게 유용한 정도 6. 정보보호 교육훈련이 회사의 정보보호를 위해 적합한 정도	D'Arcy et al., 2009
IT활용 능력 (ITA)	1. 개인의 IT 활용능력 일반 2. 정보보호 소프트웨어 활용법 숙지 정도 3. 업무용 소프트웨어 활용 숙련도 4. 업무용 소프트웨어 숙련 기회 추구 5. 조직내 그룹웨어 활용한 업무정도	Bassellier et al., 2003 Rhee et al., 2009
부정적 경험 (NEX)	1. 사이버 공격 피해로 컴퓨터 사용 어려움 경험 정도 2. 파일 다운로드시 바이러스 악성코드 감염 경험 정도 3. 정보보호 지침 위반으로 주의나 경고 경험 정도 4. 고객정보, 개인정보 수칙 위반 경험 정도 5. 개인정보 유출 피해 경험 정도	Liang and Xue, 2010 Rhee et al., 2009
학습활동 (LAO)	1. 정보보호 교육 훈편 참여 정도 2. 온라인 통한 정보보호 내용 습득 3. 회의, 워크샵에서 정보보호 관련 정보 공유 정도 4. 비공식 모임에서 정보보호 관련 정보 공유 정도 5. 습득한 정보보호 관련 내용 업무 활용도 6. 습득한 정보보호 관련 내용 체계정 정리 정도	Hurtz and Williams, 2009
피드백 추구행동 (FSB)	1. 정보보호 행위에 대한 상사로 부터의 피드백 관신도 2. 정보보호 시스템 사용에 대한 동료 행위 비교정도 3. 숙련된 동료에 대한 정보보호 행위 관찰 4. 우수하게 평가받는 동료직원에 대한 관찰 5. 정보보호 시스템 사용을 포함하여 동료에게 피드백 추구 정도 6. 정보보호 전담조직에게 문의정도 7. 피드백 받는 것의 유용성	Callister et al., 1999
충실한 내재와 (FOA)	1. 정보보호 시스템 사용방식에 대한 전담(개발)자의 동의 2. 사용자들의 시스템 사용 적절성 여부 3. 회사로 부터의 사용자의 행태에 대한 동의 4. 가장 적절한 방식으로 사용하고 있는 정도 5. 정보보호 시스템 본래 의도대로 사용하고 있는 정도	Chin et al., 1997

4.2 자료수집

본 연구는 제안모형 검증을 위한 자료수집을 위해 변수측정도구를 선정한 후, 설문조사기법을 사용하였다. 자료수집대상을 선정할 때 첫째, 연구목적상 정보보호 전담부서나 내부통제부서를 제외한 실제 최종사용자로부터의 자료수집을 고려하였고, 둘째, 금융회사 정보보호 정책, 지침, 사용자 시스템의 특성이 회사마다 상이함을 고려하여 조직에서 동일한 정책과 지

침이 적용된 사용자 정보보호 시스템을 사용하는 현업 조직원을 대상으로 하였다. 설문은 2016년 5월 27일부터 6월 11일까지 총 320부를 배포하였으며, 285(응답률: 89.0%)부를 수거하여, 이중 하나의 값으로 일관된 응답이나, 무응답이 많은 경우인 17부를 제외하고, 총 268부를 최종분석에 사용하였다. 이번 설문에는 측정변수중 한 변수를 정하여, 해당변수 전체 설문항목에 역코딩(reverse coding)을 도입하여 연구모형의 모델 적합도를 높이려 시도하였다.

표본은 남성 156명(58.2%)이고, 여성 112명(41.8%)로 구성되었으며, 연령은 20대 72명(26.9%), 30대 125명(46.6%), 40대 65명(24.3%), 50대 6명(2.2%)으로 나타났으며, 학력수준은 대졸의 학력이 177명(66.6%)으로 주를 이루었고, 대학원이상 31명(11.6%)으로 구성되어있다.

직급의 경우, 저직급인 사원~대리가 183명(68.2.%), 고직급에 해당하는 과장~부장이상이 85명(31.8%)으로 나타났다. <표 3>에서 인구통계적 특성에 대해 정리하였다.

<표 3> 표본의 인구통계적 특성

구 분		빈도(명)	비율(%)
성별	남	156	58.2
	여	112	41.8
연령	20대	72	26.9
	30대	125	46.6
	40대	65	24.3
	50대	6	2.2
학력	고졸이하	21	7.8
	전문대졸	39	14.6
	대졸	177	66.0
	대학원이상	31	11.6
직급	사원	77	28.7
	주임	43	16.0
	대리	63	23.5
	과장	42	15.7
	차장	31	11.6
	부장이상	12	4.5
근속연수	2년미만	63	23.5
	2~5년미만	90	33.6
	5~10년미만	55	20.5
	10~15년미만	15	5.6
	15~20년미만	10	3.7
	20년이상	35	13.1
수행업무	영업채널	82	30.6
	마케팅	34	12.7
	경영기획	38	14.2
	고객지원	44	16.4
	고객서비스	20	7.5
	경영지원	10	3.7
	자산운용	25	9.3
	IT부서	15	5.6

Ⅴ. 실증분석결과

5.1 타당성 및 신뢰도 분석

5.1.1 탐색적 요인분석과 신뢰도

수집된 자료를 적절한 통계기법을 사용하여 가설 검정 및 분석을 실시하였으며, 본 연구에서는 SPSS 18을 이용하여 사전통계분석과 기초통계분석을 위한 빈도분석, 요인분석을, AMOS 22를 사용하여 구조방정식 모형분석을 실시하였다.

가설을 검증하기에 앞서 측정도구의 타당성(validity)과 신뢰도(reliability)분석을 실시하였다. 분석결과, 변수들의 신뢰도 수준은 모든 변수의 신뢰도 계수 Cronbach's Alpha가 0.7을 상회하여 적정한 수준의 신뢰도를 갖는 것으로 판단하였다.

타당성 분석을 위해 탐색적 요인분석을 실시하였는바, 전체 46개 문항중 3개 문항만 정제되었고, KMO-Bartlett 검증에서 모든 변수에서 기준치 0.6과 유의확률 0.05미만을 충족하는 결과를 보였고, 모든 변수의 요인 적재량이 0.6을 상회하는 수치를 보여 적절한 요인들로 추출되었음을 알 수 있다.

탐색적 요인분석결과와 신뢰도 분석결과를 [표 4]에서 정리하였다.

<표 4> 탐색적 요인분석과 신뢰도 분석 결과

개념	요인	변수명	요인 적재량	고유값	분산 설명력	Alpha if item deleted	Cronbach's α
정보보호 조직차원	최고경영진 지원 TMS	TMS2	.813	4.356	25.62	.912	.924
		TMS1	.801			.913	
		TMS3	.786			.909	
		TMS4	.771			.907	
		TMS5	.741			.909	
		TMS6	.706			.913	
	정보보호 지침제공 POG	POG2	.799	4.297	25.27	.906	.924
		POG3	.788			.901	
		POG4	.784			.906	
		POG1	.772			.922	
		POG5	.700			.911	
		POG6	.698			.916	
	정보보호 교육훈련 SETA	SETA5	.798	3.597	21.16	.869	.878
		SETA6	.776			.837	
		SETA4	.770			.842	
		SETA3	.735			.884	
		SETA1	.654			.869	
정보보호 개인차원	IT지식과 활용능력 ITA	ITA1	.819	2.916	32.395	.756	.813
		ITA2	.819			.753	
		ITA4	.727			.787	
		ITA5	.724			.792	
		IITA3	.693			.797	
	부정적 경험 NEX	NEX2	.796	2.216	24.622	.540	.705
		NEX3	.748			.467	
		NEX1	.729			.604	
		NEX4	.666			.706	
최종 사용자의 능동성	조직내 학습활동 LAO	LAO3	.829	3.746	31.22	.845	.881
		LAO2	.808			.861	
		LAO5	.756			.853	
		LAO1	.730			.881	
		LAO6	.718			.850	
		LAO4	.656			.870	
	피드백 추구행동 FSB	FSB3	.844	4.553	37.95	.911	.929
		FSB4	.842			.912	
		FSB5	.832			.916	
		FSB2	.827			.913	
		FSB1	.805			.921	
		FSB6	.788			.923	
내재화	합목적적인 정보보호 시스템 사용 내재화 FOA	FOA2	.887	3.684	73.69	.880	.908
		FOA4	.882			.880	
		FOA3	.877			.882	
		FOA5	.844			.893	
		FOA1	.799			.904	

5.1.2 확인적 요인분석과 측정모형 분석

탐색적 요인분석과 신뢰도 평가를 바탕으로 확인적 요인분석(confirmatory factor analysis)을 실시하여, 각 척도의 단일차원성(unidimensionality)을 평가하였다. [표 5]에서 나타난 모델 적합도를 통하여 알 수 있듯이, 확인적 요인분석을 통해서 각 요인별로 수용에 합당한 모델 적합도가 산출되었으며, 그 결과 채택된 측정항목으로 측정모형 분석을 실시하였다.

측정모형 분석을 통해, 측정모델의 적합도를 산출하였는 바, χ^2= 247.213, df=202, χ^2/df= 1.224, p=0.16, GFI=.928, AGFI=.901, CFI= .988, RMR=.022, RMSEA=.029를 나타내어 수용하기에 무리없는 모델적합도를 보여주었다.

확인적 요인분석과 측정모델 분석을 통하여 수용 가능한 적합도 수준에서 타당성을 확보하였지만, 타당성의 가장 엄격한 방법인 집중타당성과 판별타당성을 확보했는지를 검증하였다.

개념 신뢰도값을 산출하여 집중타당성확보를 검증하였으며, 각 잠재변수의 AVE값이 전체 변수들의 상관계수의 제곱값을 상회하는지를 확인하여 판별타당성을 검증하였다. [표 6]에서 집중타당성과 판별타당성의 분석결과를 제시하였다.

집중타당성을 확보하기 위해서는 표준화된 요인적재치의 값이 최소 0.5를 상회하고, AVE값이 0.5이상 그리고 개념신뢰도값이 0.7이상이어야 한다(Bagozzi & Yi, 1988). 본 연구의가장 엄격한 집중타당성 기준인 개념 신뢰도를 모든 변수가 0.7을 상회하여 적합한 집중타당성을 확보하였음을 알 수 있다.

또한 판별타당성은 변수별 AVE(평균분산추출값을 산출하여, 이와 상관계수중 최고값의 제곱값과 비교하는 방식과 함께, 표준오차추정구간(two standard-error interval estimate)을 해평가하는 방법인 상관계수 ± (2×standard error) ≠ 1에 대입하여 나온 각0.758, 0.646의 값이

<표 5> 확인적 요인분석 결과

변수	최종 항목수	χ^2	df	p	x2/df	RMR	GFI	AGFI	CFI	RMSEA
TMS	4	2.805	2	.246	1.402	.006	.995	.974	.999	.039
POG	4	2.692	2	.260	1.346	.007	.995	.974	.999	.036
SETA	5	7.320	5	.198	1.464	.014	.989	.967	.997	.042
ITA	5	12.011	5	.035	2.402	.024	.982	.946	.984	.072
NEX	4	5.503	2	.064	2.752	.057	.990	.949	.982	.081
LAO	4	3.675	2	.159	1.837	.013	.993	.965	.997	.056
FSB	5	13.639	5	.018	2.728	.020	.980	.939	.988	.080
FOA	4	3.450	2	.178	1.725	.005	.994	.969	.998	.052

<표 6> 집중타당성, 판별타당성 분석 결과

변 수	TMS	POG	SETA	ITA	NEX	LAO	FSB	FOA
TMS	.879							
POG	.702	.892						
SETA	.692	.658	.811					
ITA	.356	.425	.438	.735				
NEX	-.305	-.205	-.219	-.223	.882			
LAO	.426	.421	.620	.405	-.038	.812		
FSB	.371	.32	.471	.373	-.017	.689	.841	
FOA	.480	.513	.479	.521	-.231	.441	.436	.921
구성 개념 신뢰도	.910	.939	.850	.778	.874	.794	.828	.944

주) 표의 대각선 값은 AVE값의 제곱근 값이며, 나머지 값은 잠재변수간의 상관관계 계수임

1을 포함하지 않으므로, 표준오차추정구간을 통한 방법에서도 판별타당성을 확보한 것으로 판단된다(Anderson & Gerbing, 1988).

5.2 연구모형분석

본 연구의 가설을 검증하기 위해 구성개념들 간의 영향관계를 동시에 고려하여 검증하는 구조방정식 모형을 이용하였는 바, 측정도구의 타당성과 신뢰도를 확보하였고, 최종 연구모형의 적합도를 평가하였다.

데이터와 모델간의 관계를 나타내는 절대적합도 지수와 null모델과의 비교를 통해 연구모형의 적합도를 평가하는 증분 적합도 지수들을 산출하여 분석한 결과, χ^2=291.733, df=205, χ^2/df=1.423, RMR=0.032 GFI=0.915, AGFI=0.885, CFI=0.976, RMSEA=0.040의 값이 도출되었다.

구조방정식 모형의 적합도를 평가하기 위해서는 Chi-square 통계량이 변수의 분포나 표본의 크기에 매우 민감하기 때문에, 몇 개의 적합도 지수를 동시에 고려하여 평가하여야 하는데, 절대적합도지수인 GFI가 0.9보다 크고, 모형의 간명성을 고려하여 GFI값을 조정한 AGFI (Adjusted GFI)값이 0.85이상이면 모형의 적합도가 좋은 것으로 간주할 수 있다(강현철, 2013). 또한, CFI지수 값은 0과 1.0사이인데, 대략 0.9 이상이면 적합도가 좋다고 볼 수 있으며, RMSEA값은 RMSEA<.05이면 좋은 적합도(close fit), RMSEA<.08이면 괜찮은 적합도(reasonable fit), RMSEA<.10이면 보통 적합도(mediocre fit), RMSEA>.10이면 나쁜 적합도(unacceptable fit)를 나타낸다(Browne and Cudeck, 1993). 전반적으로 모형의 적합도 지수가 모두 바람직한 수준을 충족시키므로, 본 연구모형의 적합도는 적합한 것으로 판단된다. <표 7>에서 연구모형의 적합도 지수를 제시하였다.

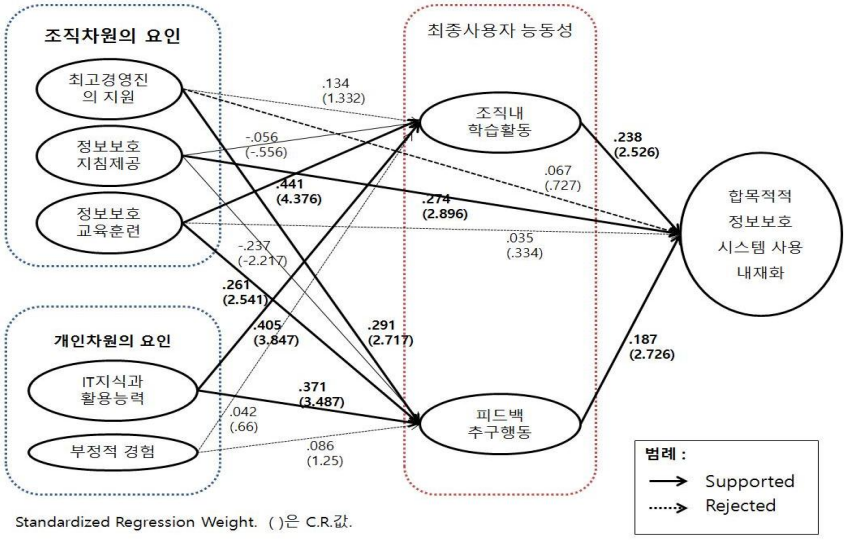
<표 7> 연구모형 적합도 분석결과

적합도 지수	연구모형	권고수준
CMIN	291.733	-
DF	205	-
CMIN/DF	1.423	< 3.00
p value	.000	< 0.05
RMR	.032	< 0.05
GFI	.915	> 0.9
AGFI	.885	> 0.85
CFI	.976	> 0.9
RMSEA	.040	< 0.08

5.3 가설검정결과

일차적으로 잠재 변수간 설정된 경로에 대한 구조모형 분석내용은 <그림 2>로, 가설을 검정한 결과는 <표 8>에 각각 제시하였다.

결과를 정리하면, 다음과 같다. 우선, 최고경영진의 지원은 조직구성원의 피드백 추구행동에 유의한 영향을 미치는 것으로 나타났으나(H1c., β=0.291, p<0.05), 충실한 내재화(H1a)와 학습활동(H1b)에는 유의한 영향을 미치지 못하고 있는 것으로 나타났다. 조직내 최고경영진의 관심과 지원(TMS)은 조직문화와 정보보호에 대한 직원들의 태도에 직간접적으로 영향을 미친다는 선행연구(Hu et al., 2012)와 부분적으로 부합하는 결과를 보여주고 있다. 하지만, 정보보호 시스템 사용의 내재화와 학습활동에 영향을 미치지 못하고 있는데, 이는 최고경영진의 지원이 조직원들의 정보보호 시스템 사용 내재화와의 관련성은 다른 요인의 작용이 있음을 암시하고 있다고 볼 수 있다.



<그림 2> 구조모형분석

<표 8> 가설검정결과

경로 (가설)	경로계수	표준화된 경로계수	표준오차	C.R.	p value	결과
H1a. FOA ⇐ TMS	0.066	.067	0.091	0.727	0.467	기각됨
H1b. LAO ⇐ TMS	0.173	.134	0.130	1.332	0.183	기각됨
H1c. FSB ⇐ TMS	0.401	.291	0.147	2.717	0.007	지지됨
H2a. FOA ⇐ POG	0.269	.274	0.093	2.896	0.004	지지됨
H2b. LAO ⇐ POG	-0.073	-.056	0.131	-0.556	0.578	기각됨
H2c. FSB ⇐ POG	-0.325	-.237	0.147	-2.217	0.027	기각됨
H3a. FOA ⇐ SETA	0.025	.035	0.074	0.334	0.738	기각됨
H3b. LAO ⇐ SETA	0.404	.441	0.092	4.376	0.001	지지됨
H3c. FSB ⇐ SETA	0.253	.261	0.100	2.541	0.011	지지됨
H4a. LAO ⇐ ITA	0.575	.405	0.149	3.847	0.001	지지됨
H4b. FSB ⇐ ITA	0.559	.371	0.160	3.487	0.001	지지됨
H5a. LAO ⇐ NEX	0.050	.042	0.075	0.660	0.509	기각됨
H5b. FSB ⇐ NEX	0.107	.086	0.086	1.250	0.211	기각됨
H6. FOA ⇐ LAO	0.181	.238	0.072	2.526	0.012	지지됨
H7. FOA ⇐ FSB	0.134	.187	0.043	2.726	0.006	지지됨

다음으로 정보보호 지침제공(POG)은 정보보호 시스템 사용의 합목적적인 내재화(H2a, β=0.274, p<0.05)에 유의한 영향을 미치는 것으로 나타났으나. 학습활동(H2b, β=-0.056)과 피드백 추구행동(H2c, β=-0.237)에는 유의한 영향을 미치지 않는 것으로 나타났다. 정보보호 정책과 지침은 해당 시스템에 모두 반영되어 있으므로, 정책과 지침을 학습하거나, 피드백을 추구하기 보다는 시스템을 직접적으로 활용하는 것으로 인식하고 있음을 알 수 있다.

정보보호 교육훈련(SETA)은 조직내 학습활동(H3b, β=0.441, p<0.001)과 피드백 추구행동

(H3c, β=0.261, p<0.05)에 유의한 영향을 미치는 것으로 나타났으나, 직접적으로 정보보호 시스템 사용의 내재화(H3a)에는 영향을 미치지 않는 것으로 나타났다. 교육훈련을 통한 조직원의 정보보호 의식제고와 실제 시스템 사용에 대한 전달은 사용자의 능동적인 적응과정을 거치는 것으로 해석할 수 있으며, 학습과 피드백 추구행동의 매개작용을 암시하고 있다.

IT지식과 활용능력(ITA)은 조직내 학습활동(H4a, β=0.405, p<0.001)과 피드백 추구행동(H4b, β=0.371, p<0.001)에 유의한 영향을 미치는 것으로 나타났다. 최종 사용자의 컴퓨터 사용능력은 업무용 정보시스템 활용에 강한 긍정적인 작용을 한다는 연구(Torkzadeh et al., 1999)와 컴퓨터와 인터넷 활용에 대한 자신감과 역량이 정보보호를 위한 개인의 능력을 향상시키는 데 기여한다(Rhee et al., 2009)는 선행연구에 부합하고 있으며, 조직원에 대한 계발 프로그램을 개발하거나 운영할 때 반드시 고려하여야 할 사항으로 해석된다.

부정적 경험(NEX)은 다른 변수에 유의한 영향을 주지 못하는 것으로 나타났다. 악성코드 감염 혹은 보안위반에 대한 개인적인 경험이 조직내에서 고의성 없는 실수 혹은 무지에 의한 행동에 대해 경감활동을 촉진하고 조율하기 위한 방편(Compeau & Higgins, 1995)으로 작용한다는 연구에 부합하지 않는 결과를 보여주고 있다. 이는 표본의 특성에 기인하는 것으로, 금융업은 금융자산을 다루는 산업이므로 위험과 그에 따른 통제수준이 높아(이장형·김종원, 2010) 금융업 종사자들은 개인의 특성 혹은 경험이 조직내에서 크게 드러나지 않도록 훈련되고 적응한 상태를 반영하고 있다고 볼 수 있다.

최종사용자의 능동성을 보여주는 조직내 학습활동(LAO)은 합목적적인 내재화에 유의한 영향을 미치고 있으며(H6, β=0.238, p<0.05), 피드백 추구 행동(FSB)도 합목적적인 내재화에 유의한 영향(H7, β=0.187, P<0.05)을 미치고 있는 것으로 나타났다. 훈련과 학습량이 증가할수록 정보보호 시스템이 디자인된 의도대로 충실하게 내재화될 것으로 본 Wheeler and Valacich(1996)의 연구에 부합하는 결과를 보여주고 있다.

5.4 매개효과 분석 결과

매개변수인 조직내 학습활동과 피드백 추구행동에 대해 Sobel's Test를 통해 매개효과를 검정하였다.

Sobel's Test 결과 피드백 추구행동은 최고경영진의 지원과 충실한 내재화를 매개(z=2.052, p<0.05)하고 있으며, 또한 정보보호 교육훈련과 충실한 내재화를 매개(z=1.964, p<0.05)하고 있는 것으로 나타났다. 부분적인 매개역할에 그치는 것이 아니라 완전매개효과를 나타낸 것은 피드백 행동 추구라는 조직원들의 능동적인 적응과정의 중요성을 입증하는 것이라 할 수 있다. 조직내 학습활동의 매개효과에 대한 결과로는, 정보보호 교육훈련과 충실한 내재화를 매개(z=2.181, p<0.05)하는 것으로 나타났다. 역시 완전매개역할을 하는 것으로 보여, 정보보호를 위한 핵심조치인 정보보호 교육훈련을 통한 조직의 작용은 학습활동과 피드백 추구 행동을 통해서 가시적인 성과로 귀결될 수 있다고 볼 수 있다.

<표 9> 매개효과 분석 결과

매개경로	Sobel's Test (z)	p value	mediation
FOA ⇐ FSB ⇐ TMS	2.052	0.040	Full Mediation
FOA ⇐ LAO ⇐ SETA	2.181	0.029	Full Mediation
FOA ⇐ FSB ⇐ SETA	1.964	0.049	Full Mediation

최고경영진의 지원과 정보보호 교육훈련은 대표적인 조직차원의 영향요인으로 볼 수 있는데, 정보보호 시스템 사용의 합목적적인 내재화도 최종사용자의 능동적인 적응과정인 학습활동과 피드백 추구 행동이 매개되어야만 제대로 효과가 발휘된다는 중요한 시사점을 제공하고 있다.

Ⅵ. 결 론

6.1 연구결과의 요약

첫째, 최고경영진의 지원은 최종사용자로 하여금 피드백 추구 행동에 나서게 하고, 이를 통해 정보보호 시스템을 더욱 합목적적으로 사용하게 하는 것으로 나타났다. 측정항목에서도 알 수 있듯이, 조직의 CEO 혹은 최고경영층에서 보여주는 정보보호에 대한 관심과 강조는 구성원들의 피드백 추구 행동을 통해 합목적적인 정보보호 시스템 사용에 대한 압력으로 작용하고 있음을 보여주고 있다.

둘째, 정보보호 지침제공은 최종사용자의 능동성을 촉발하기보다는 조직의 정보보호 정책과 지침이 반영된 시스템의 합목적적인 사용에 직접적인 영향을 주고 있다. 조직구성원에게 정책과 지침은 그 자체의 활용성보다는 시스템에 접근권한, 처리권한, 승인권 제한 등으로 반영되어 있으므로 최종사용자로서는 이를 학습과 피드백이 아닌 직접적으로 활용하는 차원에서 인식하고 있는 것으로 해석할 수 있다.

셋째, 정보보호 교육훈련은 조직에서 목적의식적으로 조직구성원에게 지속적으로 강조하는 사항을 전달하고 인지시키는 방식인데, 이를 반영하듯이, 최종사용자의 능동적인 학습과 피드백 추구행동에 모두 유의한 영향을 주고 있다. 하지만 교육훈련을 통해 정보보호 시스템의 합목적적인 사용에 유의한 영향을 미치지는 못하고 있어, 최종사용자의 능동성에 의한 강한 매개 작용을 시사하고 있다.

넷째, 개인차원의 요인으로 꼽은 IT활용능력은 학습활동과 피드백 추구행동에 강한 영향을 주고 있는데, 이는 일반 업무용 시스템에서와 마찬가지로 IT에 대한 개인능력 역시 중요하며, IT활용능력이 높을수록 정보보호 시스템에 대한 능동성이 높아져, 다른 동료직원의 피드백 추구의 대상이 될 수 있을 뿐만 아니라, 부서단위 혹은 동료그룹에서 숙련도가 가장 높을 가능성이 크다고 할 수 있다. 조직에서는 특히 금융회사에 근무하는 조직원들에게는 IT 활용능력을 키우도록 배려할 필요도 있는 것으로 보인다.

다섯째, 개인적인 부정적 경험은 유의한 영향을 미치지 못하는 변수로 검정되었는바, 인지된 위협이 이를 회피하고자 하는 동기부여를 통해 회피행위로 나아가고(Liang & Xue, 2010), 정보보호 위반 경험이 정보보호의 자기효능감에 영향을 주는(Rhee et al.,2009) 것으로 주장한 선행연구와는 일치하지 않은 것이다. 해석해보면, 이는 연구대상의 상이함 즉, 표본의 특성에 기인하는 것으로 보인다. 선행연구의 연구대상은 대학교 학생이거나 컴퓨터 유저라고만 언급된 표본이기에 금융회사의 업무담당자가 정보보호에 대해 인지하는 수준과 영향요인의 비중에 비해 개인특성이 더 드러나 있는 것으로 보인다. 본 연구의 표본 연구대상으로 삼은 금융회사의 조직구성원들은 개인의 부정적 경험보다는 조직차원의 영향요인에 의한 반응과 행동에 충실한 것으로 파악할 수 있다.

여섯째, 매개효과분석을 통해 최종사용자의

능동적 적응과정인 학습활동과 피드백 추구행동의 매개효과를 확인할 수 있었다. 이는 기존의 연구에서 정보보호에 대한 대안으로서 최고경영자의 관심과 강조, 정보보호 교육훈련을 통한 정책준수 등의 영향요인에 주안점을 두었던 것과는 다르게 사용에 대한 합목적적인 정보보호 시스템 사용 내재화를 위해서는 최종사용자의 능동성이라고 하는 중요한 변수를 이해하고 활용할 수 있어야 함을 의미한다.

6.2 연구의 시사점

정보보호를 위해 기술적 접근, 정책적 접근을 비롯한 많은 대안을 모색하는 연구들이 진행되어 왔다. 하지만 기존 연구들은 산업적인 지평선이 넓게 형성되어있어, 해당산업에 대한 특성이 충분히 반영되어있지 않아, 실천적인 의의를 갖기에는 한계가 있었다. 특히 금융 산업이 가진 정보 집약성, 고객정보/개인정보의 광범위성, 유출시 피해범위가 넓은 점 등에서 알 수 있듯이 금융산업에서 정보보호가 갖는 의미는 금융산업 자체가 국가경제에 필수이듯이 금융회사에는 필수적이고 수준 높은 우선순위와 가치가 있다고 평가할 수 있다.

연구의 결과에서 나타난 바와 같이, 정보보호 시스템을 도입하고 사용하는 상황에서, 정보보호 시스템을 합목적적으로 사용하기 위해서는 최종 사용자의 능동적인 자세가 중요하다는 것을 알 수 있다. 본 연구는 최종사용자 스스로가 정보보호 영향요인들로부터 인지 혹은 인식되어 이를 구체적인 행위로 나타내는 정보보호 시스템 사용의 합목적성을 보유하기까지의 메카니즘에 대한 고찰이었다.

사용자가 정보보호 시스템을 업무효율성을 저해하는 것으로 인식하고 이를 무시하거나 그 중요성을 간과해서는 기존 업무 자체의 비즈니스 연속성(Business Continuity)조차도 확보할 수 없으므로, 학습활동과 피드백 추구행동을 통해 정보보호 시스템을 설계된 의도대로 충실하게 활용하는 것이 결국에는 조직의 견고한 정보보호에 이를 수 있음을 실증하고자 하였다.

본 연구는 조직에서 기존에 지속적으로 해왔던 정보보호 정책과 지침제공, 교육훈련 등의 정기적으로 진행되고 있는 이벤트와 더불어 추가로 몇 가지 제도적 장치를 제안하고자 한다.

첫째로, 피싱 메시지를 가장한 정보보호 모의훈련을 지속적으로 실시해야 한다. 중장기적인 효과를 위한 가장 확실한 방법은 기술적인 해결책에 의존하기 보다는 정보보호를 위한 교육훈련을 체계적으로 운용하는 것이다. 이는 정보보호에 대한 지식을 전달할 뿐만 아니라 실질적인 모의 훈련 등을 통해 사회공학적인 방법에 의한 외부로 부터의 내부 침입 시도 예를 들면, 이메일에 악성코드를 실어 유포하는 행위 등에 대해서도 효과적으로 대비하게 되는 것이다.

향후 망 분리를 통해 업무용 시스템과 그룹웨어 등이 외부와 분리될 것이지만, 피싱 메일 혹은 악성코드를 유포할 우려가 있는 외부메시지에 대한 정보보호 모의훈련과 문서암호화(DRM) 관리수준을 높이기 위한 훈련은 정보유출에 대한 대내외적인 보호대책이기에 필수적으로 실시하여야 한다. 해킹전문가들의 고도화된 기법이기도 한 사회공학적인 방법은 주로 홍보성 혹은 정보제공을 위장한 메일을 통해 악성코드를 시스템에 침투시키는 일차공격을 하는데 이에 대한 대응으로 모의훈련을 강화하여 조직구성원들의 경각심과 피드백 추구행동을 촉진시키는 방식을 써야만 한다.

둘째, 조직의 구성원들이 정보보호와 관련된 허점(security hole)을 신고하면 이를 포상하는 시스템인 Bounty Hunter System 제도의 도입을 조심스럽게 고려해보아야 한다. 화이트해킹과 유사하게 보이지만, 내부 정보보호 전담조직이나 외부 전문가들이 살펴보기 어려운 사각지대에서의 정보보호 취약점들은 해당 업무 담당자가 아니면 알기 어려움을 감안할 때, 정보보호 시스템을 포함하여 최종사용자의 자발성을 이끌어내기 위한 제도적 장치의 필요성이 제기되며, 공개 혹은 비공개는 조직마다 다를 수 있다.

6.3 연구의 의의와 후속연구

앞에서 밝힌 바와 같이. 정보보호 학문의 분류상 본 연구는 정보보호 경영분야이며, 정보보호 주체의 개인행위에 대한 실증적 연구로서, 정보보호 시스템의 구축 및 도입과 지속적인 사용 환경에서 합목적적인 활용을 위해서는 최종사용자들의 자발적인 학습 관점에서 연구모델을 확립하고 실증하는 시도로서 학문적 의의를 가진다.

또한 그간 정보보호 연구 분야에서 다루어지지 못했던 최종사용자의 학습과 피드백 추구행동이 갖는 매개효과를 밝혀 그 중요성을 파악하고, 조직구성원의 학습과 피드백이 가능하게 하는 지속적인 학습과 상호작용의 문화를 조성하기 위해 조직이 무엇을 제공하고 동원해야 할 자원들은 어떤 것들이 있는지에 대한 의사결정 우선순위 파악의 단서를 제공한다.

후속연구로 고려해 볼 수 있는 것으로는, 추후에 모니터링을 통해 조직간 정보보호 시스템 사용의 내재화 수준과 연관된 모의훈련결과의 비교연구가 가능하리라 본다. 이는 합목적적인 사용의 내재화가 실제 다른 정량적인 성과지수에 어떠한 영향을 주는 지에 대한 연구이며, 조직 간의 비교도 가능할 뿐만 아니라 한 조직에서 일정기간 추적연구가 가능하며, 정보보호 시스템 사용의 내재화에 관해 충분히 의미 있는 연구가 될 것으로 생각된다.

참고문헌

강소라, 양희동, 박현여, “GSS 사용과 성과요인:TAM, TTF, 조직구조화이론(AST)혼합모형,” 한국 IT 서비스학회, 제7권, 제1호, 2008, pp.63-87.

강현철, “구조방정식 모형에서 적합도지수의 해석과 모형적합 전략에 대한 논의,” *Journal of the Korean Data Analysis Society,* Vol. 15, No. 2(B), 2013, pp. 653-668.

김영렬, “개인정보보호 의식 측정 척도의 개발과 개인정보 중요성에 관한 인지도 조사,” 한국산업정보학회논문지, 제15권, 제5호, 2010, pp.259-271.

김혜리, 김양훈, 장항배, “정보보호 학문 분류체계 설계와 연구동향 메타분석,” 2014년 한국경영정보학회 추계학술대회, 2014, pp.533-538.

노희옥, “지식경영시스템 사용에서의 전유에 관한 연구: 적응구조화 이론을 중심으로,” 전남대학교 박사학위 논문, 2008.

박정국, 김인재, “정보보호의 조직성과에 영향을 미치는 요인에 관한 연구,” 인터넷전자상거래연구, 제14권, 제6호, 2014, pp.275-299.

보안뉴스, 카드회사 고객정보 유출규모 1억건 넘었다, 2014. 1. 8., http://www.boannews.com/media/view.asp?idx=39247&page=110&kind=1&sk

ind=8&search=title&find=

이장형, 김종원, “보안 및 통제와 정보기술 사용자의 성격의 관계,” 정보시스템 연구, 제19권, 제3호, 2010, pp.1-12.

임명성, “조직구성원들의 정보보안 정책준수행위 의도에 관한 연구,” 디지털정책연구, 제10권, 제10호, 2012, pp.119-128.

임명성, “조직구성원들의 정보보안 정책준수에 영향을 미치는 요인에 관한 연구-금융서비스업을 중심으로,” 서비스경영학회지, 제14권, 제1호, 2013, pp.143-171.

양우섭, “학습조직과 조직유효성의 관계에서 공유가치의 조절효과,” 벤처창업연구, 제8권 제1호, 2013, pp.111-125.

황인호, 김대진, “조직의 정보보안 환경이 조직구성원의 보안준수의도에 미치는 영향,” 정보시스템 연구, 제25권, 제2호, 2016, pp.51-77.

Abraham, S., “Information Security Behavior: Factors and Research Directions,” Proceedings of the 17th Americas Conference on Information Systems, 2011, Paper 462.

Ajzen, I., “The Theory of Planned Behavior,” Organizational Behavior and Human *Decision Processes,* Vol. 50, No. 2, 1991, pp.179-211.

Albrechtsen, E. & Hovden, J., “Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study,” *Computers & Security,* Vol. 29, No. 4, 2010, pp.432-445.

Anderson, C. & Agarwal, R., “Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions,” *MIS Quarterly,* Vol. 34, No. 3, 2010, pp. 613-643.

Anderson, J. C., and Gerbing, D. W., “Structural Equation Modelinig in Practice: A Review and Recommended Two-Step Approach,” *Psychological Blletin,* Vol. 103. No. 3, 1988, pp.411-423.

Ashford, S. J., “Feedback-seeking in individual adaptation: A resource perspective,” *Academy of Management Journal,* Vol. 29, No. 3, 1986, pp.465-487.

Ashford, S. J., Blatt, R., and VandeWalle, Don., “Reflections on the Looking Glass: A Review of Research on Feedback-Seeking Behavior in Organizations,” *Journal of Management,* Vol. 29, No. 6, 2003, pp.773-799.

Ashford, S. J., and Tsui, A. S., “Self-Regulation for Managerial Effectiveness: The Role of Active Feedback Seeking,” *Academy of Management Journal,* Vol. 34, No.2, 1991, pp.251-280.

Aytes, K., and Connolly T., “A research Model for Investigating Human Behavior Related to Computer Security,” Proceedings of the Ninth Americas Conference on Information Systems, 2003, pp. 2027-2031.

Bagozzi, R.P. and Yi, Youjae, “On the Evaluation of Structural Equation Models,” *Journal of the Academy of Marketing Science,* Vol. 16, No. 1, 1988, pp.74-94.

Bassellier, G., Benbasat. I., and Reich, B. H., “The influence of business managers' IT competence on championing IT,” *Information Systmes Research,* Vol. 14, No. 4, 2003, pp.317-336.

Beatty, R. C., Shun, J. P., and Jones, M., “Factors Influening Corporate Web Site Adoption: a Time-Based Assessment,” *Information & Management,* Vol. 38, No. 6, 2001, pp.337-354.

Browne, M. W. and R. Cudeck, “Alternative Ways of Assessing Model Fit,” *Sociological Methods & Research,* Vol.

21, No. 2, 1992, pp.230-258.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I., "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly,* Vol.34, No. 3, 2010, pp.523-548.

Callister, R. R., Kramer, M. W., and Turban, D. B., "Feedback seeking following career transitions," *Academy of Management Journal,* Vol. 42, No. 4, 1999, pp. 429-438.

Cannoy, S. , and Salam., A., "A framework for health care information assurance policy and compliance," *Communications of the ACM,* Vol. 53, No. 3, 2010, pp.126-131.

Chan, M., Woon, I., and Kankanhalli, A., "Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior," *Journal of Information Privacy & Security,* Vol. 1, No. 3, 2005, pp.18-41.

Chen, C. C., Shaw, R. S., and Yang, S. C., "Mitigating Information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System," *Information Technology, Learning, and Performance Journal,* Vol. 24, No.1, 2006, pp.1-14.

Chin, W. W., Gopal, A., and Salisbury, W. D., "Advancing the Theory of Adaptive Structuration: The Development of a Scale to Measure Faithfulness of Appropriation," *Information Systems Research,* Vol. 8, No. 4, 1997, pp. 342-367.

Compeau, D. R., and Higgins, C. A., "Computer self-efficacy: Development of a measure and initial test," *MIS quarterly,* Vol. 19, No. 2, 1995, pp. 189-211.

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

Davis, F. D., "User acceptance of information technology : System characteristics, user perceptions and behavioral impacts," *International Journal of Man-Machine Studies,* Vol. 38, No. 3, 1993, pp.475-487.

DeSanctis, G., and Poole, M. S., "Capturing the Complexity in Advanced Technology Use: Adaptive Structuration Theory," *Organization Science,* Vol 5. No. 2, 1994, pp.121-147.

Dinev, T., and Hu, Q., "The centrality of awareness in the formation of user behavioral intention toward protective information technologies," *Journal of the Association for Information Systems,* Vol. 8, No. 7, 2007, pp.386-408.

Frank, J., Shamir, B., and Briggs, W., "Security-related behavior of PC users' in Organizations," *Information & Management,* Vol. 21, No. 3, 1991, pp. 127-135.

Gattiker, U., & Kelley, U., "Morality and Computers: Attitudes and Differences in Judgments," *Information Systems Research,* Vol. 10, No. 3, 1999, pp. 233-254.

Goel, S., and Chengalur-Smith, I. N., "Metrics for Characterizing the Form of Security Policies," *Journal of Strategic Information Systems,* Vol. 19, 2010, pp.281-295.

Haeussinger, F. J., and Kranz, J. J., "Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior," International Conference on

Information Systems, 2013, pp.1-16.

Hagen, J. M., Albrechtsen, E., and Hovden, J., "Implementation and effectiveness of organizational information security measures," *Information Management & Computer Security,* Vol. 16, No. 4, 2008, pp.377-397.

Helin, S., and J. Sandström, "An inquiry into the study of corporate codes of ethics," *Journal of Business Ethics,* Vol. 75, No. 3, 2007, pp.253-271.

Herath, T., and Rao, H. R., "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems,* Vol. 18, 2009, pp.106-125.

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

Hu, Q., Dinev, T., Hart, P., and Cooke, D., "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture," *Decision Science,* Vol. 43, No. 4, 2012, pp. 615-659.

Hurtz, G. M., and Williams, K. J., "Attitudinal and motivational antecedents of participation in voluntary employee development activities," *Journal of Applied Psychology,* Vol. 94, No. 3, 2009, pp.635-653.

Ifinedo, P., "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Computers & Security,* Vol. 31. No. 1, 2012, pp.83-95.

Johnston, A., and Warkentin, M., "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly,* Vol. 34, No. 3, 2010, pp.549-566.

Kankanhalli, A., Teo, H., Bernard, C.Y., and Tan, K. W., "An integrative study of information systems security effectiveness," *International Journal of Information Management,* Vol. 23, No. 2, 2003, pp.139-154.

Knapp, K.J., Marshall, T. E., Rainer, R. K., and Ford, F.N., "Information security: management's effect on culture and policy," *Information Management & Computer Security,* Vol. 14, No. 1, 2006, pp.24-36.

Kruger, H., and Kearney, W., "A prototype for assessing information security awareness," *Computers & Security,* Vol. 25. No. 4, 2006, pp.289-296.

Leach, J., "Improving User Security Behavior," *Computers & Security,* Vol. 22, No. 8, 2003, pp.685-692.

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., and Hohler, B., "Employees' Information Security Awareness and Behavior: A Literature Review," 2013 46th Hawaii International Conference on System Sciences, 2013, pp. 2979-2987.

Lee, J. and Lee Y., "A Holistic Model of Computer Abuse within Organizations," *Information Management & Computer Security,* Vol. 10 No. 2, 2002, pp. 57-63.

Lee, S. M., Lee, S. G., and Yoo, S.,"An Integrative model of computer abuse based on social control and general deterrence theories," *Information Management,* Vol. 41, No. 2, 2004, pp. 114-121.

Leonard, L. N. K., Cronan, T. P., Kreie, J., "What are influences of ethical

behavior intentions - planned behavior, reasoned action, perceived importance, or individual characteristics?," *Information & Management,* Vol. 42, No. 1, 2004, pp.143-158.

Liang, H., and Xue, Y., "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems,* Vol. 11, No, 7, 2010, pp.394-413.

Loch, K. D., Conger, S., "Evaluating ethical decision making and computer use," *Communications of the ACM,* Vol. 39, No. 7, 1996, pp.74-83.

Luker, N. W., "Do You Trust Your Employees?," Security Management, Vol. 34, No. 9, 1990, pp.127-130.

Ng, B. Y., Kankanhalli, A., Xu, Y.C., "Studying users' computer security behavior: a health belief perspective," *Decision Support Systems,* Vol. 46 No. 4, 2009, pp.815-825.

Pahnila, S., Siponen, M., and Mahmood, A., "Employees' Behavior Towards IS Security Policy Compliance," Proceedings of the 40th Annual Hawaii International Conference on System Science, 2007, pp.156-166.

Poole, Marshall Scott., *"Adaptive Structuration Theory,"* A first look of Communication Theory 7th edition Ch. 18, Mcgrawhill, 2008.

Poole, S., and DeSanctis, G., *"Understanding the Use of Group Decision Support Systems: The Theory of Adaptive Structuration,"* in J.Fulkand C.Steinfield (Eds.), Organizations and Communication Technology ,Sage, Newbury Park, CA, 1990, pp.173-193.

Potosky D., "A field study of computer efficacy beliefs as an outcome of training: the role of computer playfulness, computer knowledge, and performance during training," *Computers in Human Behavior,* Vol. 18, No. 3, 2002, pp.241-55.

Proctor P. E. & Byrnes F. C., *"The Secured Enterprise: Protecting Your Information Assets,"* Prentice Hall, Upper Saddle River, 2002.

Rhee, H. S., Kim, C., and Ryu, Y.U., "Self-efficacy in information security: Its influence on end users' information security practice behavior," *Computers & Security,* Vol. 28, No. 8, 2009, pp. 1-11.

Sambamurthy, V., and Chin, W. W., "The Effects of Group Attitudes Toward GDSS Designs on the Decision-Making Performance of Computer-Supported Groups," *Decision Science,* Vol. 25, No. 2, 1994, pp.215-241.

Siponen, M., "A Conceptual Foundation for Organizational Information Security Awareness," *Information Management & Computer Security,* Vol. 8, No. 1, 2000, pp.31-41.

Siponen, M., and Vance, A., "Neutralization: New Insights into the Problem of Employee information Systems Security Policy Violations," *MIS Quarterly,* Vol. 34 No. 3, 2010, pp.487-502.

Spears, J. L., and Barki, H., "User Participation in Information Systems Security Risk Management," *MIS Quarterly,* Vol. 34, No. 3, 2010, pp.503-522.

Stanton, J. M., Stam, K. R., Guzman, I., & Caldera, C., "Examining the linkage between organizational commitment and information security," Proceedings of the IEEE Systems, Man and Cybernetics Conference, 2003.

Stanton, J. M., Stam, R. K, Mastrangelo, P and Jolton, J., "Analysis of End User

Security Behavior," *Computers & Security,* Vol. 24, No. 2, 2004, pp. 124-133.

Straub, D.W., and Welke, R.J., "Coping with systems risks: security planning models for management decision making," *MIS Quarterly,* Vol. 22, No. 4, 1998, pp. 441-469.

Thomson. M. E., and Von Solms, R., "Information security awareness: educating your users effectively," *Information Management & Computer Security,* Vol. 6, No. 4, 1998, pp.167 - 173.

Thomson, K-L., von Solms, R., and Louw, L., "Cultivating an Organizational Information Security Culture," *Computer Fraud & Security,* Vol. 2006, No. 10, 2006, pp. 7-11.

Torkzadeh, R., Pflughoeft, K., and Hall, L., "Computer self-efficacy, training effectiveness and user attitudes: an empirical study," *Behavior and Information Technology,* Vol. 18, No. 4, 1999, pp.299-309.

Tsohou, A., Kokolakis, S., Karyda, M., and Kiountouzis, E., "Investigating information security awareness: Research and practice gaps," *Information Security Journal: A Global Perspective,* Vol. 17, No. 5-6, 2008, pp.207-227.

Van Dyne, L., and LePine, J. A., "Helping and Voice Extra-Role Behaviors: Evidence of Construct and Predictive Validity," *The Academy of Management Journal,* Vol. 41, No. 1, 1998, pp.108-119.

Wheeler, B. C., and Valacich, J. S., "Facilitation, GSS, and Training as Sources of Process Restrictiveness and Guidance for Structured Decision Making: An Empirical Assessment," *Information Systems Research,* Vol. 7, No. 4, 1996, pp.429-450.

Wood, R., and Bandura, A., "Social cognitive theory of organizational management," *Academy of Management Review,* Vol. 14, No. 3, 1989, pp.361-384.

Workman, M., Bommer, W.H., Straub, D., "Security lapses and the omission of information security measures: an empirical test of the threat control model," *Journal of Computers in Human Behavior,* Vol. 24. No. 6, 2008, pp.2799-2816.

Zafar, H., and Clark, J. G., "Current State of Information Security Research In IS," *Communications of the Association for Information Systems,* Vol. 24, Article 34, 2009, pp.557-596.

김 민 웅(Kim, Min Woong)

현재 전남대학교 대학원 전자상거래협동과정 박사과정에 재학중이다. 서울대학교에서 학사, 석사학위를 취득하였다. 홍국생명 CIO, CISO를 역임하였다. 주요 관심분야는 E-business, IT, 고객센터 서비스 혁신, 정보보호 등이다.

정 기 주(Cheong, Ki Ju)

현재 전남대학교 경영학부 교수로 재직중이다. 전남대학교에서 학사, 석사를 취득하고, 미국 앨라바마 주립대에서 박사학위를 취득하고, Purdue대학 교수를 역임하였다. 주요관심분야는 고객센터 서비스품질, VoC 관리, 고객센터 운영평가 시스템, 인력관리 등이다.

<Abstract>

A Study on the Effect of Learning Activities and Feedback Seeking Behavior toward the End Users' Faithful Appropriation of Information Security System

Kim, Min Woong · Cheong, Ki Ju

Purpose

The purpose of this paper is to examine factors and mechanism inducing end users' faithful appropriation of information security behavior through the information security system. This study is also trying to find out the role of Employees' adaptive activities like learning and feedback seeking behavior for the information security in organizations.

Design/methodology/approach

An empirical study was carried out with a sample of employees working in the financial service company. Employees(n = 268) completed a written questionnaire. Structural equation modeling was used to analyze the data.

Findings

Results indicated that employees' learning activities and feedback seeking behavior fully mediated the effect of major information security factors toward end users' faithfulness of appropriation of information security systems. In order to increase the level of employees information security behavior in accordance with security guideline, organizations should facilitate interactions that support the feedback seeking process between employees on information security awareness and behavior. Additionally, organizations may reinforce these behaviors by periodical training and adopting bounty hunter systems.

Keywords: Faithfulness of Appropriation, Learning Activities, Feedback Seeking Behavior, End Users' Information Security System

* 이 논문은 2016년 8월 16일 접수, 2016년 8월 29일 1차 심사, 2016년 9월 21일 게재 확정되었습니다.