은행 IT 인력의 정보보호 정책 준수에 영향을 미치는 정보보호 대책에 관한 연구

심준보* · 황경태**

A Study on the Information Security Measures Influencing Information Security Policy Compliance Intentions of IT Personnel of Banks

Joonbo Shim* · K.T. Hwang**

Abstract

This study proposes the practical information security measures that help IT personnel of banks comply the information security policy. The research model of the study is composed of independent variables (clarity and comprehensiveness of policy, penalty, dedicated security organization, audit, training and education program, and top management support), a dependent variable (information security policy compliance intention), and moderating variables (age and gender).

Analyses results show that the information security measures except 'clarity of policy' and 'training and education program' are proven to affect the 'information security policy compliance intention.' In case of moderating variables, age moderated the relationship between top management support and compliance intention, but gender does not show any moderating effect at all.

This study analyzes information security measures based solely on the perception of the respondents. Future study may introduce more objective measurement methods such as systematically analyzing the contents of the information security measures instead of asking the respondents' perception. In addition, this study analyzes intention of employees rather than the actual behavior. Future research may analyze the relationship between intention and actual behavior and the factors affecting the relationship.

Keywords : Information Security Policy, Information Security Measures, Compliance Intention

논문접수일 : 2015년 05월 13일 논문게재확정일 : 2015년 06월 25일

* 동국대학교 서울캠퍼스 경영대학 경영정보학과 박사과정, e-mail : jbshim33@naver.com
** 교신저자, 동국대학교 서울캠퍼스 경영대학 경영정보학과 교수, e-mail : kthwang@dongguk.edu

1. 서 론

1.1 연구의 배경 및 필요성

정보사회에 접어들면서 민간과 공공 부문을 불문하고 거의 모든 조직들은 조직의 운영에 있어서 정보시스템과 정보에 대한 의존도가 매우 높아지고 있다. 특히, 금융기관의 경우에는 이러한 정보와 정보시스템에 대한 의존도가 더욱 높고, 금융기관의 운영에 필수적인 요소이다[Bauer et al., 2013].

그런데 최근 들어 시스템들 간의 네트워킹이 확대되면서 승인받지 않은 접근 기회가 많아지고, 분산 컴퓨팅 환경의 확산으로 중앙 집중적이고 전문화된 IT 설비의 통제 범위가 줄어들면서, 정보보호에 대한 위협은 보다 광범위해지고 고도화되고 있다[Solms, 1988]. 국내 금융 산업의 경우, 비대면 방식의 전자금융 거래가 급격히 증가하여, 전자금융 이용 비중이 2013년 3월 기준으로 88%에 이르고, 이로 인해 소비자들의 이용 편의성은 높아졌으나, 이와 함께 보안 위협 또한 크게 증가하고 있다[금융위원회 전자금융과・금융감독원 IT감독국, 2013]. 최근 들어, 금융 전산시스템 해킹을 비롯하여 개인정보 유출 등과 같은 금융 사고가 연이어 발생하고 있다.

조직에 중요한 자산인 정보시스템과 정보의 가용성, 무결성, 기밀성 등을 확보하여 보안 위협에 관련된 위험을 관리하는 것은 기업의 경쟁우위, 수익성, 법규 준수, 회사의 명성을 유지하는데 필수적일 수 있다[Cavusoglu et al., 2004; Bauer et al., 2013]. 금융기관들의 경우에는 국제규약인 바젤 Ⅱ의 도입 이후, 운영 위험, 그 중에서도 특히 정보보호를 포함한 IT 운영 위험에 대비한 최소한의 대책을 갖추고 있어야 한다[Bauer et al., 2013]. 이에 따라 오늘날 정보보호는 거의 모든 조직에서 우선순위가 매우 높고, 해결해야 할 중요한 과제로서, 최고 경영진의 우선순위 중의 하나가 되어가고 있다[Brancheau et al., 1996; Lohmeyer et al., 2002; Ransbotham and Mitra, 2009].

정보보호에 대한 위협을 경감하기 위해 조직들은 여러 가지 대책을 구현하고 있는데, 전통적으로는 기술적인 접근방법으로 문제를 해결하기 위해 노력하였다[Hagen et al., 2008; Spears and Barki, 2010]. 그러나 여러 연구에서 증명된 바와 같이, 기술적인 솔루션만으로는 조직을 보호할 수 없다. 왜냐하면, 조직의 구성원들이 잠재적인 보안 위험을 인식하고 여기에 대응하지 못한다면 기술적인 대책만으로는 충분하지 않기 때문이다[Lebek et al., 2013]. 언론 매체에서는 정보보호에 관련하여 컴퓨터 핵커와 범죄자들이 크게 부각되고 있지만, 보다 많은 수의 정보보호 관련 사고는 내부 직원의 행위로 발생하고 있고, 직원들의 단순한 실수에서부터 고의적인 행동을 포함하여 그 비중은 50~70%에 이른다고 한다[Richardson, 2008; Haeussinger and Kranz, 2013]. 조직에서 정보보호를 확보하는 것은 어려운 과제로서, 특히 조직 내의 내부인으로부터의 위협을 피하는 것은 매우 어려운 일이다[Pricewaterhousecoopers, 2012].

이에 따라 정보보호 전문가들은 기술적인 대책뿐만 아니라 보안 정책, 보안 교육 및 훈련 프로그램 등을 포함하여 정보시스템의 오용에 대한 절차적인 대책을 같이 사용할 것을 권고하고 있다[Hovav and D'Arcy, 2012]. 최근 들어 정보보호에 대한 초점이 개인 및 조직적인 관점으로 이동하면서, 직원들이 정보보호 정책을 준수하도록 하는 것이 핵심 사항으로 등장하고 있다[Boss et al., 2009; Siponen et al., 2012].

정책은 조직에서 정보보호를 확보하는데 중요한 도구 중의 하나이다[Cheng et al., 2013], 그러나 모범적인 보안 정책 자체가 보안을 보장해 주지 못하며, 보안정책이 수립되었다고 해서, 직원

들이 반드시 준수할 것이라는 것을 의미하지도 않는다[Hagen et al., 2008; Gundu and Flowerday, 2013]. 따라서 직원들이 조직의 정보보호 정책을 준수하도록 유도하는 요인이 무엇인지를 이해하고, 직원들이 조직이 수립해 놓은 보안정책을 잘 준수하도록 하는 것은 정보보호 관리에서 필수적인 일이 되었다[Bulgurcu et al., 2010]. 이러한 배경에서 최근 이 분야의 연구의 초점은 정보보호에서 가장 취약한 고리로 간주되고 있는 직원들의 행동, 그 중에서도 특히 정보보호 정책의 준수 행위에 영향을 미치는 요인들을 식별하는데 맞춰지고 있다[Siponen, 2000; Bulgurcu et al., 2010; Boss et al., 2012].

이 분야에서 비교적 많은 연구가 수행되었지만, 공통적인 제약점 중의 하나는 직원들의 보안 행위에 영향을 미칠 수 있는 조직적인 대책을 개발하고 검정하는 연구는 거의 이루어지지 않았다는 것이다[Lebek et al., 2013]. 즉, 학술적인 연구에서 직원들의 보안 행위에 영향을 미친다고 이론적으로 설명하는 내용과 실무에서 어떤 관리기법이나 대책을 적용할 필요가 있는지 간에 괴리가 존재한다는 것이다. 따라서 이론과 실무 간의 간극을 줄이고, 이 분야의 학술적인 발전에 기여할 수 있도록, 기존의 이론적 기반 위에 직원들의 보안 행위에 영향을 미칠 수 있는 구체적인 대책을 개발하고 검증하는 연구가 절실히 필요하다[Bulgurcu et al., 2010].

이에 따라 본 연구에서는 여러 산업 중에서 정보와 정보시스템에 대한 의존도, 그리고 정보보호에 대한 위협이 가장 높은 산업 중의 하나인 금융 산업, 그 중에서도 은행을 대상으로 직원들의 정보보호 정책 준수를 확보할 수 있는 실질적인 정보보호 대책에 대해 연구하고자 한다. 즉, 기존의 이론적 지식의 기반 위에 은행 직원들의 정보보호 정책 준수 행위에 영향을 미칠 수 있는 구체적인 대책을 식별하고, 이를 검정하고자 한다.

1.2 연구의 범위 및 내용

본 연구는 금융기관들 중에서 은행을 대상으로 한다. 그리고 보안정책 준수 행위를 분석하는 구체적인 대상으로 은행의 최종 사용자가 아니라, 정보시스템 부서의 인력을 대상으로 한다. 정보보호는 모든 사람들에게 적용되는 것이지만, 본 연구에서는 정보보호 정책을 가장 잘 알고 있는 사람들인 IT 인력의 행위에 초점을 맞추고자 한다. 이러한 접근방법은 Workman et al.[2008] 등과 같은 이 분야의 다른 연구에서도 채택된 방법이다. 이러한 접근방법을 채택하는 이유는 정보보호에 대한 경험이나 지식이 적은 사람들을 대상으로 분석한 내용에 비해 보다 실제적인 내용을 제공할 수 있기 때문이다.

그리고 본 연구의 주제인 정보보호(information security)는 정보보안이라고도 번역되는데, 최근 들어 정보보호라는 용어가 보다 공통적으로 활용되고 있기 때문에, 본 연구에서도 정보보호라는 용어를 채택하도록 한다. 본 연구의 주제는 정보보호 정책인데, 일반적으로 정책이란 “조직의 경영 철학, 최고 경영진 및 현업 책임자들이 가지고 있는 전반적인 사고를 정리한 상위수준의 문서”를 말한다[황경태, 2011]. 따라서 정보보호 정책이란 “정보보호에 대한 근본적인 목표를 제시하고, 그 중요성을 해당 조직의 장이 선언하는 내용을 포함한 문서”라고 볼 수 있다[교육과학기술부, 2011].

또한 이러한 정책의 내용은 보다 상세화되고 구체화되어, 실무에서 적용이 용이하도록 지침과 절차로 작성된다. 본 연구에서 분석하고자 하는 정보보호 정책의 범위에는 가장 상위의 정책뿐만 아니라 이를 구체화한 지침과 절차가 모두 포함된다.

또한 본 연구에서는 이 분야의 기존 이론에서 제시하고 있는 핵심 변수들을 분석하기 보다는

은행에서 실무적으로 적용 가능한 보안 대책에 초점을 맞춘다. MIS 분야의 연구에서는 실무에 관련성이 높은 연구를 수행하라는 요구가 높다[Zmud, 1998; Rosemann and Vessey, 2008]. 기존 이론에서 제시하고 있는 변수들은 이미 많은 연구에 의해서 입증되었고, 따라서 이러한 기존의 이론적인 변수들보다는 실무적인 보안 대책에 초점을 맞춤으로써, 이 분야에 존재하고 있는 이론과 실무 간의 괴리를 줄이는데 기여하고자 한다.

마지막으로 본 연구에서는 직원들의 보안정책 준수에 대한 실제적인 행위가 아니라 의도를 연구의 대상으로 한다. 이 분야의 연구뿐만 아니라, 사회과학 분야의 다른 영역에서도 의도를 실제적인 행동의 예측 변수로 사용하고 있다. 보안정책 준수에 관련된 문헌에서도 준수 의도를 실제 준수 행위의 예측 변수로 사용하는 것을 지원하고 있다[Ajzen, 1991; Pogarsky, 2004]. 물론 실제적인 준수 행동을 분석하는 것이 궁극적으로 효과적일 수 있겠지만, 대부분의 연구에서 의도를 평가하는 것은 보안에 대한 실제 행동을 관찰하는 것이 현실적으로 어렵기 때문이다[Lebek et al., 2013]. 이러한 이유에서 본 연구에서도 직원들의 보안정책 준수 의도를 연구의 대상으로 한다.

2. 이론적 배경

본 장에서는 먼저, 정보보호 정책의 준수 행위에 관련된 연구의 기반이 되는 이론과 해당 이론을 바탕으로 수행된 연구의 결과를 분석하고, 문헌 분석의 시사점을 정리한다.

2.1 관련 이론

지난 10여 년 동안 조직 내 인력들의 정보보호에 대한 인식과 행동에 관련된 연구는 몇 가지 이론을 바탕으로 수행되었다. 이 분야에서 가장 많이 사용된 이론으로는 합리적 행동 이론/계획된 행동 이론, 일반 억제 이론, 보호 동기 이론, 기술 수용 모델 등을 들 수 있다[Hu et al., 2012; Lebek et al., 2013].

먼저, 합리적 행동이론(Theory of Reasoned Action : TRA)과 계획된 행동이론(Theory of Planned Behavior : TPB)은 연관된 이론으로서, TPB는 TRA를 확장한 이론이다. TPB는 가장 예측력이 높은 이론 중의 하나로서, 다양한 영역에서 광범위하게 사용되고 있다[Ifinedo, 2012]. 이 이론에서 행동하려는 의도는 실제적인 행위의 선행 요인으로 간주된다. 이 이론에 의하면, 행위 의도는 행위에 대한 태도(attitude toward behavior), 주관적 기준(subjective norm), 인지된 행동통제(perceived behavioral control) 등의 세 가지 요인에 의해 결정된다고 한다[Ajzen, 1991]. TPB는 정보시스템에 대한 윤리적인 행위와 사람들이 수용 가능한 컴퓨터 보안 조치를 채택하고, 정보보호 정책을 준수하기로 결정하는 것을 분석하는데 널리 사용되고 있다[Ifinedo, 2012].

둘째로 일반 억제 이론(General Deterrence Theory : GDT)은 형사법 분야에서 기원하였는데, 이 이론의 기본적인 가정은 사람들은 이성적인 의사결정을 한다는 것이다[Lebek et al., 2013]. GDT에서는 제재/처벌의 엄정성(perceived severity of sanctions)과 확실성(perceived certainty of sanctions)이 이러한 행위에 가담하기로 결정하는데 영향을 미친다는 것이다. 정보보호 분야의 연구에서는 이 이론을 이용하여, 직원들이 정보시스템을 오용하려는 의도를 방지하기 위한 보안 대책과 기타 예방 전략을 분석하고 식별하는데 초점을 맞춘다[Lebek et al., 2013].

셋째로 보호 동기 이론(Protection Motivation Theory : PMT)은 치료 심리학 분야에서 비롯되었는데, 이 이론은 다양한 종류의 예방 행위들을 예측함으로써 잠재적인 위협에 대응하는 과정을 설명한다. 이 이론에 의하면, 특정한 행위는 위협에

대한 평가(threat appraisal)와 대응에 대한 평가(coping appraisal)라는 두 가지 인지적 평가결과에 의해 결정된다고 한다. PMT는 사람들이 보호 행위를 하려는 의도를 예측할 수 있는 강력한 이론 중의 하나로 주목받고 있다[Ifinedo, 2012; Gundu and Flowerday, 2013]. 정보보호 정책의 준수에 관련된 많은 이전 연구에서 PMT를 활용하였고, 대응 평가와 위협 평가는 정보보호 정책의 준수 의도에 유의한 영향을 미친다는 것이 많은 연구에 의해 입증되었다[Cheng et al., 2013].

넷째, 기술수용 모델(Technology Acceptance Model : TAM)은 기술 수용에 영향을 미치는 요인을 설명하는 이론으로서, 여러 기술에 대해 반복적으로 입증된 모형이다. TAM에서는 기술 수용에 영향을 미치는 요인으로 기술의 유용성(perceived usefulness)과 사용 용이성(perceived ease-of-use)을 들고 있다. 기술의 유용성은 해당 기술을 사용함으로써 자신의 직무 성과를 향상시킬 수 있는지에 대한 주관적인 확률로 정의된다. 이에 반해서, 사용 용이성은 해당 기술을 사용하는데 필요한 노력의 정도를 나타낸다. 정보보호의 측면에서 보면, TAM은 직원들이 정보보호 정책을 준수하려는 의도를 결정하는데 있어서 정보보호 정책의 사용을 통해 얻을 수 있는 유용성과 정책사용의 용이성의 영향을 받는다는 것이다. 이 분야의 연구에서는 정책의 유용성과 정책사용의 용이성 이외에도 정책의 명확성, 간결성, 포괄성, 깊이 등이 사용되고 있다[Herath and Rao, 2009; 박종원, 김현규, 2012; 박철주, 임명성, 2012; Siponen et al., 2012; 임명성, 2013; 임명성, 한군희, 2013; Haeussinger and Kranz, 2013].

마지막으로 이 분야의 일부 연구에서는 인력들의 정보보호에 관련된 행위를 설명하기 위해, 위에서 정리한 표준적인 이론을 확장하여 추가적인 요인들을 도입하였다. 대표적인 예로 정보보호에 관련된 직원들의 행위에 영향을 미칠 수 있는 정보보호에 관련된 대책을 제시한 Hagen et al. [2008]을 들 수 있다. 이 연구에서는 보안 대책을 다음과 같은 네 가지 그룹으로 분류하고 있다 : (1) 정보보호 정책, (2) 절차 및 통제, (3) 비기술적인(행정적인) 도구 및 방법, (4) 조직 및 개인의 인식도 개발 및 제고에 관련된 대책. 각 대책은 다시 몇 가지의 세부 항목으로 구분되고 있다.

터키 중소기업들의 정보보호 관리에 영향을 미치는 요인을 분석한 연구[Yildirima et al., 2011]에서는 보안 대책으로 보안 정책, 보안 조직, 자산 분류 및 통제, 인력 보안, 물리적 및 환경적 보안, 의사소통 및 운영 관리, 접근 통제, 시스템 개발 및 유지보수 등을 제시하였다. 조직의 구성원들이 정보보호 정책의 내용을 알고서도 이를 지키지 않는 행동의 원인을 분석한 한 연구[Workman et al., 2008]에서는 문헌 분석을 통해 이를 개선하기 위한 대책으로 처벌, 보안 인식의 제고, 보안 절차의 확대, 보안 전문가들이 권고한 절차를 구현할 수 있는 시간을 가질 수 있도록 작업 부하를 줄이는 것과 같은 상황적 요인의 해결, 정책의 품질 개선, 조직의 보안 목표와 프랙티스 간의 연계 향상, 소프트웨어 개발 주기 동안에 보안 구현의 개선 등을 제시하고 있다.

우리나라의 한 공공기관에서 발표한 지침[교육과학기술부, 2011]에서는 공공기관들이 갖추고 있어야 할 모범적인 보안 대책으로 크게 기술적, 물리적, 관리적 보안의 세 가지를 제시하고 있는데, 이 중 본 연구의 초점인 관리적 보안 대책의 세부 사항에는 문서화 및 자산관리, 조직 및 예산, 인적 보안, 정보보안 교육, 준거성, 보안사고 관리, 운영 보안 등이 포함된다.

기타 국내에서 수행된 이 분야의 연구에서 제시되고 분석된 정보보호 대책에는 보안 정책[박종원, 김현규, 2012; 박철주, 임명성, 2012; 임명성, 2013; 임명성, 한군희, 2013], 최고 경영진의 지원[임명성,

2013; 임명성, 한군희, 2013], 교육[안중호 등, 2010; 장명희, 강다연, 2012; 임명성, 2012; 박철주, 임명성, 2012; 임명성, 2013; 강다연, 장명희, 2014], 보상[박종원, 김현규, 2012], 처벌[안중호 등, 2010; 김상현, 송영미, 2011; 박종원, 김현규, 2012; 강다연, 장명희, 2014] 등이 포함된다.

2.2 문헌 분석의 시사점

이 분야의 지배적인 연구 경향은 위에서 정리한 관련 이론(TPB, GDT, PMT, TAM 등) 중의 한 가지 관점을 적용하여 사람들의 행위를 분석하는 것이다[Lebek et al., 2013]. 즉, 이 분야 연구의 공통적인 제약으로 개인의 행위에 관련된 요인들에만 초점을 맞춘 연구가 가장 많이 수행된 점을 들 수 있다. 이렇게 되면, 사람들의 행위를 설명하고 예측하려는 이론들이 이러한 현상을 효과적으로 설명하지 못할 수 있다.

또한 기존 이론에서 제시하고 있는 핵심 변수들 간의 관계는 이미 많이 연구에서 입증되었다. 따라서 이 분야의 연구를 종합적으로 분석한 한 연구[Lebek et al., 2013]에서는 이 분야의 향후 연구는 이미 확인된 핵심 변수들 간의 관계를 분석하기 보다는 직원들의 정보보호 정책 준수 행위에 영향을 미칠 수 있는 추가적인 변수에 초점을 맞추라고 제안하고 있다

또 다른 고려사항 중의 하나는 학술적인 연구결과의 실무적인 관련성이다. MIS 분야의 연구에서는 실무와의 관련성(relevance)과 연구의 엄정성(rigor) 간의 균형이 오랫동안 논란이 되어왔다[Zmud, 1998; Rosemann and Vessey, 2008]. 학술 연구의 결과가 실무와 관련성이 없으면, 해당 분야는 해당 학문 공동체를 넘어서 미칠 수 있는 영향이 거의 없기 때문에, 학분 분야 그 자체의 존립 여부가 문제가 될 수 있다.

기존 이론에서 제시하고 있는 영향 요인들은 이미 많은 연구에 의해서 입증되었다. 그런데 문제는 학술적인 연구에서 직원들의 보안 행위, 즉, 정보보호 정책의 준수 행위에 영향을 미친다고 이론적으로 설명하는 요인들과 실무에서 어떤 관리기법이나 대책을 적용할 필요가 있는지 간에는 괴리가 존재한다는 것이다. 즉, 실무자들은 직원들의 행위를 결정한다고 입증된 이론적인 변수들에 어떻게 영향을 미칠 수 있는지의 문제에 봉착하고 있다.

기존의 이론을 확장하고, 실무적인 관점을 추가하여 여러 가지 다른 요인들을 분석한 연구들도 일부 있었지만, 제시된 정보보호 대책들이 종합적이지 못하고 단편적인 대책에 국한된 연구가 많았다. 비교적 체계적인 대책을 제안한 일부 연구[예 : Hagen et al., 2008; Yildirima et al., 2011]들도 대책들을 개념적으로만 제시하거나, 해당 대책의 효과성을 주관적으로 평가하고, 직원들의 행위와의 관계를 실증적으로 분석하지 못한 한계를 가지고 있다.

따라서 이론과 실무 간의 간극을 줄이고, 이 분야의 학술적인 발전에 기여할 수 있도록, 기존의 이론적 기반 위에 직원들의 보안 행위에 영향을 미칠 수 있는 구체적인 대책을 개발하고 검증하는 연구가 필요하다[Bulgurcu et al., 2010; Lebek et al., 2013].

3. 연구 설계

3.1 연구 모형 및 가설

본 연구에서는 은행을 대상으로 정보보호의 확보를 위해 매우 중요한 요소인 내부 구성원의 정보보호 정책 준수에 긍정적 또는 부정적인 영향을 미칠 수 있는 정보보호 대책들을 식별하여 이를 실증적으로 검정하고자 한다.

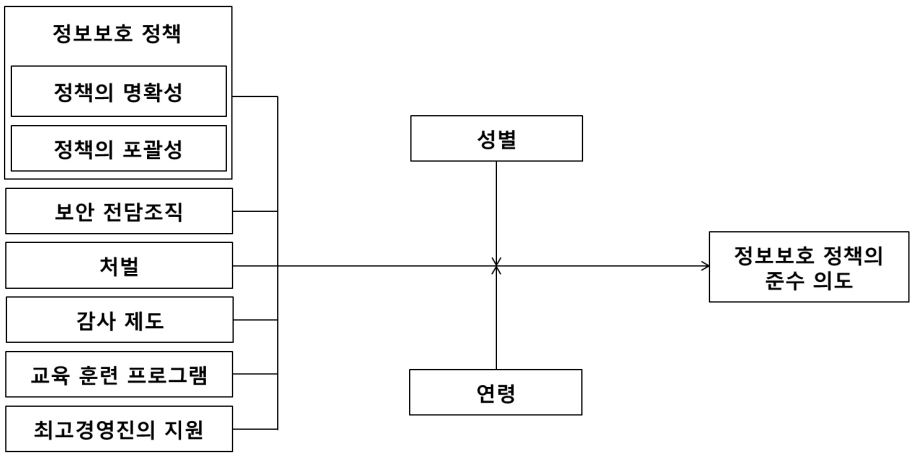
이를 위해 먼저, 본 연구에서는 문헌 분석에서 살펴본 정보보호 대책에 관한 기존 연구들 중에

서 정보보호 대책을 비교적 체계적으로 분류하여 제시하고 있는 Hagen et al.[2008]의 분류를 바탕으로 은행에 중요하다고 판단되는 보안 대책을 식별하였다.

본 연구에서는 먼저 정보보호 정책 측면에서는 정책의 특성을 구체화하여 '정책의 명확성'과 '정책의 포괄성'을 독립변수로 채택하였다. 둘째, 절차 및 통제 측면에서는 Hagen et al.[2008]에서 제시하고 있는 '처벌'을 채택하고, 여기에 조직의 일반적인 통제 중의 하나인 '보안 전담조직'을 추가하였다. 셋째, 행정적인 도구 및 방법 측면에서는 '감사(audit) 제도'를 선택하였다. 마지막으로 조직 및 개인의 인식도 개발 및 제고 측면에서는 '교육 훈련 프로그램'과 '최고 경영진의 지원'을 독립변수로 채택하였다.

또한 이러한 조직적인 정보보호 대책과 조직 내부 구성원들의 정보보호 정책의 준수 의도 간의 관계에 조절 효과를 미칠 수 있는 변수로 성별과 나이를 채택하여, 다음의 <그림 1>과 같이 연구 모형을 설정하였다.

다음의 <표 1>에는 본 연구의 모형에 포함되어 있는 변수들의 의미가 정리되어 있다.



〈그림 1〉 연구 모형

〈표 1〉 변수의 정의

구 분	변수		정의
독립변수	정보보호 정책	정책의 포괄성	정보보호 정책이 조직의 정보보호에 필요한 요소들을 포함하고 있는 정도
		정책의 명확성	정보보호 정책이 명확하고, 이해하기 용이한 정도
	보안 전담조직		정보보호를 위한 적절한 전담조직을 갖추고, 정보보호에 관한 역할과 책임을 명확하게 정의하여 할당하고 있는 정도
	처벌		정보보호 정책을 준수하지 않았을 때 조직이 직원들에게 가하는 처벌의 강도
	감사 제도		정보보호 정책/지침에 규정된 사항들을 준수하고 있는지를 확인하기 위한 감사 제도가 적정하게 시행되고 있는 정도
	교육 훈련 프로그램		회사에서 정보보호에 관련된 교육 훈련 프로그램을 적절하게 실시하고 있는 정도
	최고 경영진의 지원		정보보호에 대해 최고 경영진이 지원하고 참여하는 정도
조절변수	성별		남성 혹은 여성
	연령		나이
종속변수	정보보호 정책의 준수 의도		조직의 정보보호 정책을 준수하려는 의지의 정도

독립변수와 조절변수의 구체적인 내용과 연구 모형에 포함시킨 이유는 다음과 같다.

⑴ 정책

정보보호 정책은 보안에 대한 기대사항들을 명확하고, 구체적이고, 측정 가능한 목표와 의무사항으로 기술한 조직의 문서로서, 직원들이 조직의 정보보호에 대한 요구사항에 맞게 행동하도록 하는 도구이다[Goel and Smith, 2010]. 일반적으로 정보보안 정책을 토대로 지침과 절차의 계층 구조로 이루어진다[D'Arcy et al., 2009; 교육과학기술부, 2011]. 정보보호 정책을 수립하는 것은 정보보호 관리를 위해 필수적인 작업이다[Chan et al., 2005; D'Arcy et al., 2009; Haeussinger and Kranz, 2013].

정보보호 정책이 정보보호에 미치는 영향에 대해서는 상충하는 결과가 나타나고 있다. 예를 들면, D'Arcy et al.[2009]에서는 전사적인 정보보호 정책의 존재는 정보시스템의 오용 행위를 방지하는데 효과적이라고 주장하는 반면, Lee et al.[2004]에 의하면, 정보보호 정책은 정보시스템의 오용 행위에 전혀 영향을 미치지 못하는 것으로 나타났다. 이러한 결과는 정보보호 정책이 단순히 존재하는 것만으로는 충분하지 않고, 정책은 포괄적이고, 모호하지 않고, 읽기 쉽고, 이해하기 용이해야 한다는 사실을 나타내고 있다[Haeussinger and Kranz, 2013].

유용성, 사용 용이성, 명확성, 간결성, 포괄성, 깊이 등 여러 가지 정보보호 정책의 특성들이 제시되고 검정되었다[Siponen et al., 2009; Herath and Rao, 2009; Goel and Chengalur-Smith, 2010; 박종원, 김현규, 2012; 박철주, 임명성, 2012; 임명성, 2013; 임명성, 한군희, 2013; Haeussinger and Kranz, 2013]. 이러한 연구들 중에서 정책과 정보 품질 분야의 문헌 분석을 바탕으로 정보보호 정책이 얼마나 잘 작성되었는지를 결정하는데 사용될 수 있는 요소를 제시한 Goel and Chengalur- Smith [2010]에서는 정보보호 정책의 품질을 나타내는 요소로 포괄성(breadth), 명확성(clarity), 간결성(brevity)의 세 가지를 제시하고 있다.

첫 번째 요인인 정책의 명확성은 정책이 명확하고, 이해하기 용이한지의 여부를 말하고, 두 번째 요인인 포괄성은 정책의 범위를 나타낸다. 세 번째 요인인 간결성은 정책이 장황하지 않고 간결하게 표현되어 있는 정도를 나타낸다. 이 세 가지 요인들 중에서 간결성은 여러 연구에서 정책 준수 의도와의 관계가 기각되었고[박철주, 임명성, 2012; 임명성, 2013; 임명성, 한군희, 2013], 또한 간결성은 명확성과 유의한 상관관계를 가지고 있는 것으로 나타났다[Goel and Chengalur-Smith, 2010].

이에 따라 본 연구에서는 정보보호 정책의 준수 의도에 영향을 미칠 수 있는 정보보호 정책의 특성으로 정책의 간결성은 제외하고, 정책의 명확성과 포괄성을 채택한다.

⑵ 보안 전담조직

조직이 정보보호를 제대로 관리하기 위해서는 적절한 조직을 갖추고, 적정한 업무 프로세스를 수립하고, 책임과 역할을 적절히 할당해야 한다[Tsohou et al., 2012]. 정보보호 부문에서 가장 중요한 역할은 정보보호 최고책임자(Chief Information Security Officer : CISO)이다. CISO는 전사적인 차원에서 조직의 정보시스템은 물론 기술적, 물리적, 인적 보안 체계에 관련된 전반적인 업무를 조정, 검토, 감독하는 등 정보보호에 대한 총괄적인 기능을 수행하는 책임자로서, 상위 관리자로 지정하고, 조직의 장이 공식적으로 임명하는 것이 일반적이다[교육과학기술부, 2011; 김지수 등, 2012]. 국내의 경우, 전자금융거래법 개정안의 시행으로 금융기관은 의무적으로 CISO를 지정해야 하는데, 점차 조직 내 정보보안을 총괄하는

CISO의 역할과 기능이 중요해지고 있다.

CISO의 지휘 하에, 정보보호 업무를 기획하고 추진하는 담당조직을 구성하여, 정보보호에 관련된 문서(정책, 지침, 절차 등)를 개발하고, 정보보호 계획을 수립하고, 정보보호 교육/훈련 및 인식 제고 프로그램을 실시하고, 각종 보안대책을 구현하고 이행하는 등 정보보호 프로그램을 수행하도록 하는 것이 필요하다. 조직이 구성되면, 정보보호 활동을 수행하는데 적합한 역량과 스킬을 갖춘 인력을 지정하고, 이들의 책임과 역할을 명시하여 문서화하고, 또한 내부 보고 체계와 외부 연락 체계 등을 수립해야 한다[교육과학기술부, 2011].

정보보호에 적합한 조직 체계와 업무 프로세스를 갖추고, 정보보호에 대한 역할과 책임이 적절히 정의되고 할당된 정보보호 전담조직을 갖추고 있는 조직에서는 직원들이 정보보호 정책을 준수할 가능성이 높아질 것으로 기대된다. 따라서 본 연구에서는 보안 전담조직을 정보보호 정책의 준수 의도에 영향을 미치는 하나의 정보보호 대책으로 채택한다.

⑶ 처벌

범죄 행위에 가담 여부를 예측하는 이론인 일반 억제 이론(GDT)에서는 처벌을 가장 주요한 변수로 제시하고 있다. GDT에 의하면, 처벌의 확실성과 처벌의 엄정성을 통해서 처벌될 수 있다는 사실을 사람들에게 인지시키면, 사람들의 행동이 영향을 받는다는 것이다. 이러한 억제 이론은 IT 분야를 포함하여 많은 상황에 적용되어 검증된 이론이다.

처벌의 엄정성의 경우, 많은 연구에서 처벌의 강도가 높아지면, 사람들이 비정상적인 행위를 하려는 경향이 낮아진다는 결론을 얻었다[Herath and Rao, 2009]. 이와 유사한 논리가 정보보호의 경우에도 적용될 수 있다. 직원이 회사의 정보보호 정책을 위반하다 적발되는 경우, 해고와 같은 중징계를 한다면, 직원들이 이러한 부정적인 행위를 하려는 의도가 크게 낮아질 것이다.

GDT에서 제시하고 있는 또 다른 요인인 처벌의 확실성은 여러 연구에서 유의하지 않은 결과를 얻었다[D'Arcy et al., 2009; Cheng et al., 2013]. 처벌을 확실하게 하기 위해서는 조직이 직원들의 잘못된 행위를 탐지할 수 있어야 하므로, 사용자들의 행위를 검사하는 감사(audit)와 같은 수단의 중요성을 강조하고 있다[Vroom and Solms, 2004; Herath and Rao, 2009]. 이에 따라, 본 연구에서는 처벌의 확실성 대신 직원들의 잘못된 행위를 탐지할 수 있는 주요한 수단인 감사 제도를 연구 모형에 포함시키고, 처벌은 처벌의 엄정성을 의미하는 것으로 정의하였다.

⑷ 감사 제도

앞서 본 바와 같이, 처벌의 확실성도 비정상적인 행위를 억제하는데 중요한 요소이다. 규칙을 제대로 집행하지 않으면, 규칙을 만들었다고 해서 변화를 발생시킬 수 없다[Herath and Rao, 2009]. 그러나 처벌의 집행은 먼저 직원들의 잘못된 행위를 조직이 탐지할 수 있을 때만이 가능하다. 따라서 직원들의 보안에 관련된 행위를 조사하고 평가하는 일종의 모니터링 및 탐지 메커니즘이 필요하다[Vroom and Solms, 2004]. 이러한 사항들을 보다 종합적이고 체계적으로 조사하는 활동이 감사(audit)로서, 감사란 정보보호에 관련된 경영 목적을 달성하기 위하여 수립해 놓은 통제들이 제대로 작동하고 있는지를 검증하고, 여기에 대한 조언을 제공하는 기능을 말한다[황경태, 2011].

조직이 감사 활동을 통해서 정보보호 정책의 준수에 대한 모니터링과 탐지를 위해 노력한다는 사실을 직원들이 인지하게 되면, 적발되어 처벌될 수 있다는 생각에 정책을 준수할 가능성이 높아질 것이다. 따라서 정보보호 정책/지침에 규정

된 사항들을 준수하고 있는지를 확인하기 위한 감사 제도가 적정하게 시행된다면, 직원들은 정보보호 정책을 준수할 가능성이 높아질 것으로 기대할 수 있다. 따라서 본 연구에서는 감사 제도를 정보보호 정책의 준수 의도에 영향을 미치는 하나의 요인으로 채택한다.

⑸ 보안 교육 훈련 프로그램

조직의 정보보호 정책을 조직 전반에 걸쳐서 전파하고, 정보보호 활동에 적합한 역량을 강화하기 위해서는 적절한 수준의 교육 및 훈련이 필요하다[교육과학기술부, 2011; Gundu and Flowerday, 2013]. 보안 교육 훈련 프로그램의 목표는 잠재적인 보안 위험, 정책, 책임 등에 대한 직원들의 지식과 인식을 향상시킴으로써 조직의 정보보호를 향상시키고[Haeussinger and Kranz, 2013], 조직의 구성원들에게 조직의 정보보호 정책과 절차를 준수하는데 필요한 스킬을 제공하는 것이다[Lee and Lee, 2002; D'Arcy et al., 2009].

이러한 교육 훈련 프로그램은 보안 관리의 초석이고, 모든 직원들이 조직이 수립해 놓은 정보보호 정책과 절차를 준수하도록 한다[Sari and Trianasari, 2014]. 잘 훈련받은 직원들은 정보보호 측면에서 가장 강력한 고리가 될 수도 있다. 정책에서 서술하고 있는 보안 행동을 준수하는 의식 있는 사용자들은 다른 사람들의 행동에 긍정적인 영향을 미칠 것이다. 그 뿐만 아니라, 이들은 사고가 발생하거나, 발생하기 이전에 보안 사고를 탐지할 수 있는 역량을 갖추게 된다[Hagen et al., 2008].

정보보호 이슈에 대한 직원들의 이해도가 높아질수록, 직원들은 보안의 중요성과 보안이 자신들을 보호하고, 안전하고 보다 효과적인 환경에서 자신들의 업무를 수행하도록 해 주는 방법을 더욱 잘 이해하게 된다[Gundu and Flowerday, 2013]. 따라서 본 연구에서도 정보보호에 관한 교육 훈련 프로그램을 정보보호 정책의 준수 의도에 영향을 미치는 주요한 요인으로 채택한다.

⑹ 최고 경영진의 관심 및 지원

정보보호에 최고 경영진이 관심을 가지고, 참여하고, 지원하는 것은 손실 예방 문화의 가장 중요한 차원 중의 하나이다. 정보보호 업무는 기본적으로 하향식(top-down) 구조이므로, 최고 경영진의 정보보호에 대한 관심과 의지의 정도는 해당 조직의 정보보호 수준과 일치할 수 있다[교육과학기술부, 2011]. 정보보호에 대한 경영진의 관심과 지원이 높으면 높을수록, 조직의 정보보호에 관련된 문제에 더 많은 자원들이 가용해진다[Herath and Rao, 2009]. 정보보호의 관리에 합리적인 수준의 자원을 투여하는 것은 직원들이 충분한 수준의 보안 인식을 가지도록 하는데 필수적이다[Tsohou et al., 2010].

다양한 분야의 많은 연구에서 최고 경영자의 적극적인 지원은 새로운 기술과 제도의 도입이나 좋은 정책 개발의 성공 여부를 예측할 수 있는 척도라고 언급하고 있다. 직원들의 정보보호 정책 준수에 최고 경영진이 미치는 영향을 분석한 한 연구[Hu et al., 2012]에 의하면, 정보보호에 최고 경영진이 관심을 가지고 참여하는 것은 조직 문화에 큰 영향을 미치고, 이것은 다시 정보보호 정책의 준수에 대한 직원들의 태도에 직간접적으로 큰 영향을 미친다고 한다. 이러한 연구 결과는 직원들이 정보보호 정책을 준수하도록 만드는데 최고 경영진이 사전예방적인 역할을 수행할 수 있다는 것을 나타낸다. 이에 따라 본 연구에서도 최고 경영자의 지원이 직원들의 정보보호 정책 준수 의도에 영향을 미치는 주요한 요인으로 채택한다.

⑺ 조절변수(연령 및 성별)

성별과 연령과 같은 개인적인 특성은 사람들의 여러 가지 행위 의도를 예측하는데 활용되었다.

정보보호 분야에서도 정보보호 정책의 준수에 영향을 미칠 수 있는 추가적인 변수로 성별과 연령을 제안하는 연구가 다수 있다[Leonard et al., 2004; D'Arch et al., 2009; Hova and D'Arcy, 2012; Cheng et al., 2013; Haeussinger and Kranz, 2013].

이에 따라 본 연구에서도 성별과 연령을 정보보호 대책과 정보보호 정책의 준수 의도 간의 관계를 조절하는 변수로 채택한다.

설정된 연구 모형에 따라 본 연구에서 수립한 연구 가설들을 종합적으로 정리하면 다음과 같다.

가설 1a: 정책의 명확성은 직원들의 정보보호 정책 준수 의도에 정(+)의 영향을 미친다.

가설 1b: 정책의 포괄성은 직원들의 정보보호 정책 준수 의도에 정(+)의 영향을 미친다.

가설 2 : 보안 전담조직은 직원들의 정보보호 정책 준수 의도에 정(+)의 영향을 미친다.

가설 3 : 처벌은 직원들의 정보보호 정책 준수 의도에 정(+)의 영향을 미친다.

가설 4 : 감사 제도는 직원들의 정보보호 정책 준수 의도에 정(+)의 영향을 미친다.

가설 5 : 교육 훈련 프로그램은 직원들의 정보보호 정책 준수 의도에 정(+)의 영향을 미친다.

가설 6 : 최고 경영진의 지원은 직원들의 정보보호 정책 준수 의도에 정(+)의 영향을 미친다.

가설 7a: 정보보호 대책이 정보보호 정책의 준수 의도에 미치는 영향은 성별에 따라 차이가 있다.

가설 7b: 정보보호 대책이 정보보호 정책의 준수 의도에 미치는 영향은 연령에 따라 차이가 있다.

3.2 연구 변수의 측정항목 및 설문 구성

본 연구의 변수들에 대한 측정항목은 선행 연구에서 타당성과 신뢰성이 검증된 문항들을 중심으로 구성하였다(<표 2> 참조). 문항들은 리커트(Likert) 5점 척도로 측정되었다.

〈표 2〉 변수들의 측정문항

변수	측정 문항	출처
정책의 명확성	① 우리 회사의 정보보호에 관한 정책/지침/절차서는 이해하기 쉬운 편이다. ② 우리 회사의 정보보호에 관한 정책/지침/절차서는 읽기 쉬운 편이다. ③ 우리 회사의 정보보호에 관한 정책/지침/절차서는 내용을 명확하게 제시하고 있다. ④ 우리 회사의 정보보호에 관한 정책/지침/절차서는 일반적인 한글 용어와 표현을 사용하여 작성되어 있다. ⑤ 우리 회사의 정보보호에 관한 정책/지침/절차서는 다른 자료를 참고하지 않고도 이해할 수 있다.	Goel and Chengalur-Smith [2010]
정책의 포괄성	① 우리 회사의 정보보호에 관한 정책/지침/절차는 조직이 법규를 위반하는 것을 방지해 준다. ② 우리 회사의 정보보호에 관한 정책/지침/절차서에는 법규를 위반했을 때 어떤 일이 발생할 수 있는지가 나타나 있다. ③ 우리 회사의 정보보호에 관한 정책/지침/절차서에는 우리 회사의 외부 용역직원에 대한 정보보호 정책에 대해 명확하게 기술되어 있다. ④ 우리 회사의 정보보호에 관한 정책/지침/절차는 우리 회사의 정보보호에 필요한 거의 모든 요소들을 담고 있다.	Goel and Chengalur-Smith [2010]

보안 전담 조직	① 우리 회사는 정보보호 활동에 대한 독립성과 전문성을 확보할 수 있도록 조직의 규모와 특성을 고려하여 정보보호 전담조직(예 : 정보보호팀)를 구성하고 있다. ② 우리 회사는 충분한 경력과 자격을 갖춘 정보보호 전문가를 확보하여 정보보호 관리자나 정보보호 담당자의 역할을 수행하도록 하고 있다. ③ 우리 회사는 정보보호 인력(최고 정보보호 책임자, 정보보호 관리자, 정보보호 담당자 등)별로 수행해야 할 업무와 책임을 직무기술서와 같은 문서에 명확하게 기술하고 있다. ④ 우리 회사에는 정보보호 전문가가 회사 내부에도 있지만, 없는 경우에는 외부에서 자문을 얻고 있다.	Yildirima et al.[2011]; 교육과학기술부[2011]
처벌	① 내가 정보보호 정책/지침/절차를 위반하다가 적발되면, 나는 매우 심한 처벌을 받을 것이다. ② 회사로부터 심한 처벌을 받는다면, 이것은 나에게 큰 문제이다. ③ 회사로부터 처벌을 받는 것은 내 경력 관리에 나쁜 영향을 미칠 것이다.	Peace et al.[2003]; Herath and Rao[2009]; Siponen et al.[2012]; Cheng et al.[2013]
감사 제도	① 우리 회사는 정보보호 정책/지침에 규정된 사항들을 준수하고 있는지를 확인하기 위한 감사(audit)를 시행하고 있다. ② 감사의 대상자에는 정보보안 담당자들뿐만 아니라 우리 회사의 모든 IT 인력이 포함된다. ③ 감사는 계획에 따라 연 1회 이상 정기적으로 수행되고 있다. ④ 정기 감사 이외에도 보안 침해의 징후가 있거나 보안사고 발생 시 등 필요에 따라 특별 감사가 시행되고 있다.	Goel and Chengalur-Smith [2010]; 교육과학기술부[2011]
교육 훈련 프로그램	① 우리 회사는 정보보호 관련 이슈에 대한 IT 인력들의 인식과 지식을 높이기 위한 훈련을 실시하고 있다. ② 우리 회사는 IT 인력들에게 정보보호 관련 법규에 대한 교육을 하고 있다. ③ 우리 회사는 정보보호 관련 규정이나 법규를 어겼을 때 발생할 수 있는 일에 대해 알려주고 있다. ④ 우리 회사는 IT 인력들에게 정보보호에 대한 자신들이 맡고 있는 책임을 교육하고 있다.	D'Arcy et al.[2009]
최고 경영진의 지원	① 우리 회사의 최고 경영진은 정보보호에 관심을 가지고 있다. ② 우리 회사의 최고 경영진은 정보보호의 중요성을 이해하고 있다. ③ 우리 회사의 최고 경영진은 정보보호가 전략적으로 중요하다고 생각한다. ④ 우리 회사의 최고 경영진은 정보보호에 관련된 활동을 적극적으로 지원하고 후원하는 편이다. ⑤ 우리 회사의 최고 경영진은 정보보호에 대한 자원/예산의 추가 요청을 대부분 들어주는 편이다.	Khalid et al.[2004]; Štemberger et al.[2011]; Khan et al.[2013]; Feng and Zhao[2014]
정보보호 정책의 준수 의도	① 나는 우리 회사의 정보보호 정책/지침/절차를 지속적으로 준수할 것이다. ② 나는 업무를 수행할 때마다 정보보호 절차를 준수할 것이다. ③ 나는 우리 회사의 정보시스템과 정보를 보호하기 위해 회사의 정보보호 정책/지침/절차를 준수할 것이다. ④ 나는 우리 회사의 정보보호 정책/지침/절차를 준수하겠다는 나의 태도를 확신한다.	Herath and Rao[2009]; Hu et al.[2012]

4. 분석 결과

본 연구에서는 구조방정식 모형(Structure Equation Model)을 적용하여 측정 모형(Measurement Model)과 구조 모형(Structure Model)의 분석을 통해 잠재변수들 간의 인과관계를 식별하였다. 통계 분석에는 LISREL 8.8과 SPSS 20이 사용되었다.

4.1 데이터 수집 방법 및 표본의 인구통계학적 특성

본격적인 데이터 수집에 앞서, 설문지에 담긴 용어와 문항의 정확성과 명확성 등을 확인하기 위한 사전 테스트(pre-test)를 실시하였다. 먼저, 설문지 초안을 경영정보학 전공 교수 1인, 경영정

〈표 3〉 인구통계학적 특성(N : 371)

구 분	항목	빈도(%)	구 분	항목	빈도(%)
성별	남성	313(84.4)	직급	팀원	318(85.7)
	여성	52(14.0)		팀장(관리자)	50(13.5)
	무응답	6(1.6)		무응답	3(0.8)
혼인여부	기혼	56(15.1)	담당업무	정보보호	87(23.5)
	미혼	272(73.3)		보안 시스템 개발	10(2.7)
	무응답	43(11.6)		S/W 개발유지 보수	213(57.4)
				기타	55(14.8)
				무응답	6(1.6)
연령	20대	31(8.3)	재직기간	1년 미만	7(1.9)
	30대	113(30.5)		1년~3년 미만	31(8.4)
	40대	206(55.5)		3년~5년 미만	33(8.9)
	50세 이상	20(5.4)		5년~10년 미만	64(17.3)
	무응답	1(0.3)		10년 이상	233(62.8)
				무응답	3(0.8)

보학 전공 박사과정생 4인을 대상으로 확인하고, 필요한 수정을 하였다. 그 후에 설문 응답 조직에서 3명을 선정하여 다시 확인하고 필요한 수정을 거친 후 설문지를 최종 확정하였다.

본 연구에서는 시중은행 총 자산의 약 70%를 차지하고 있는 3대 시중은행을 대상으로 데이터를 수집하였다. 3개 시중은행의 CISO 또는 CIO의 협조 하에 해당 은행의 IT 인력들을 대상으로 2015년 3월 30일부터 약 2주에 걸쳐서 설문지를 직접 배포하여 데이터를 수집하였다. 3개 은행으로부터 411부의 설문지가 회수되었는데, 이 중에서 주요 설문 항목에 응답을 하지 않았거나, 여러 개의 항목에 대해 동일한 응답을 한 경우(예 : 모두 1로 응답) 등 불성실한 설문지 40부를 제외하고, 최종적으로 총 371부의 설문지가 분석에 포함되었다.

설문 응답자들의 인구통계학적 특성은 다음의 <표 3>에 정리되어 있다. 종합해 보면, 표본에 포함되어 있는 IT 인력들의 일반적인 특성은 40대의 인력들로서, 여성보다는 남성이, 관리자급보다는 팀원들이 주를 이루고 있고, 재직 기간은 10년 이상인 것으로 나타났다. 일반 산업보다는 연령과 재직 기간이 높은 것으로 나타났는데, 이것은 금융산업의 특성 때문인 것으로 판단된다.

4.2 측정 모형의 분석 결과

측정 모형을 분석하는 목적은 측정 항목의 신뢰성과 타당성을 검증하는 것이다. 본 연구는 사전 연구를 기반으로 연구 모형을 설계하였고, 요인들과 측정 변수들 간의 관련성에 초점을 두고 있기 때문에 확인적 요인분석을 실시하여, 집중타당성(Convergent Validity), 내적일관성(Internal Consistency), 판별타당성(Discriminant Validity) 등을 검증한다.

첫째, 집중타당성은 잠재 변수가 관측 변수에 의해 설명되는 정도를 나타낸다. 요인분석을 통해서 다중상관자승(Squared Multiple Correlation R^2)과 표준요인적재량(Standardized Factor Loadings)을 기준으로 설명 정도를 결정하는데, 기준치는 각각 0.49와 0.7 이상이다[Carmines and Zeller, 1979]. 4차에 걸쳐 확인적 요인분석을 진행하여 포괄성(di1, di2), 처벌(pu3, pu4), 보안 전담조직(de1, de4), 최고경영진의 지원(su5) 총 7개의 관측 변수를 제외시켰다. 7개의 관측 변수를 제외하고는 모든 문항이 기준을 충족시키는 것으로 나타났다(<표 4>).

〈표 4〉 집중타당성 분석

구 분	잠재변수	관측변수	1차		2차		3차		4차		
			R^2	로딩	R^2	로딩	R^2	로딩	R^2	로딩	
정보보호 정책	정책의 명확성	cl1	0.74	0.86	0.74	0.86	0.74	0.86	0.74	0.86	-
		cl2	0.75	0.87	0.75	0.87	0.76	0.87	0.76	0.87	-
		cl3	0.62	0.79	0.62	0.79	0.62	0.78	0.61	0.78	-
		cl4	0.52	0.72	0.52	0.72	0.51	0.72	0.51	0.72	-
		cl5	0.59	0.77	0.59	0.77	0.58	0.76	0.58	0.76	-
	정책의 포괄성	di1	0.49	0.70	0.48	0.69					2차 삭제
		di2	0.49	0.70	0.49	0.70	0.48	0.70			3차 삭제
		di3	0.58	0.76	0.57	0.76	0.58	0.76	0.58	0.76	-
		di4	0.72	0.85	0.72	0.85	0.74	0.86	0.79	0.89	-
처벌		pu1	0.56	0.75	0.77	0.88	0.78	0.88	0.77	0.88	-
		pu2	0.64	0.80	0.61	0.78	0.61	0.78	0.62	0.79	-
		pu3	0.40	0.64							1차 삭제
		pu4	0.42	0.65							1차 삭제
보안 전담조직		de1	0.41	0.64							1차 삭제
		de2	0.66	0.81	0.70	0.84	0.70	0.83	0.70	0.84	-
		de3	0.62	0.78	0.66	0.81	0.66	0.81	0.65	0.81	-
		de4	0.43	0.65							1차 삭제
감사 제도		au1	0.70	0.84	0.70	0.84	0.70	0.84	0.70	0.84	-
		au2	0.69	0.83	0.69	0.83	0.69	0.83	0.69	0.83	-
		au3	0.74	0.86	0.74	0.86	0.74	0.86	0.74	0.86	-
		au4	0.74	0.86	0.74	0.86	0.74	0.86	0.74	0.86	-
교육 훈련 프로그램		tr1	0.69	0.88	0.69	0.83	0.69	0.83	0.69	0.83	-
		tr2	0.72	0.85	0.71	0.84	0.71	0.84	0.71	0.84	-
		tr3	0.63	0.79	0.63	0.79	0.63	0.79	0.63	0.79	-
		tr4	0.63	0.79	0.63	0.79	0.63	0.79	0.63	0.79	-
최고경영진의 지원		su1	0.77	0.88	0.79	0.89	0.79	0.89	0.79	0.89	-
		su2	0.81	0.90	0.82	0.91	0.82	0.91	0.82	0.91	-
		su3	0.76	0.87	0.76	0.87	0.76	0.87	0.76	0.87	-
		su4	0.65	0.81	0.61	0.78	0.61	0.78	0.61	0.78	-
		su5	0.46	0.68							1차 삭제
정보보호 정책의 준수 의도		in1	0.95	0.97	0.95	0.97	0.95	0.97	0.95	0.97	-
		in2	0.75	0.87	0.75	0.87	0.75	0.87	0.75	0.87	-
		in3	0.82	0.91	0.82	0.91	0.82	0.91	0.82	0.91	-
		in4	0.82	0.91	0.82	0.91	0.82	0.91	0.82	0.91	-

둘째, 내적일관성은 Cronbach's Alpha를 이용한 잠재 변수의 신뢰도, 개념신뢰도(Construct Reliability : CR), 평균분산추출값(Average Variance Extracted : AVE)을 통해 검증한다. 일반적으로 Cronbach's Alpha 값이 0.6~0.7정도면 허용 가능한(acceptable) 수준이고, 0.7~0.9정도면 좋은(good)편이고, 0.9 이상이면 우수한(excellent) 것으로 받아들인다[George and Mallery, 2003]. 8개의 잠재 변수에 대한 신뢰성을 검증한 결과, 모든 요인들의 Cronbach's Alpha 값이 0.8 이상으로 신뢰성이 높게 나타났다(<표 5>). 개념신뢰도(CR)는 측정 모델을 평가하는데 사용되는

〈표 5〉 내적일관성 분석

변수		Cronbach's α	CR	AVE
정책의 명확성	cl1, cl2, cl3, cl4, cl5	0.898	0.898	0.578
정책의 포괄성	di3, di4	0.808	0.812	0.685
처벌	pu1, pu2	0.814	0.823	0.699
보안 전담조직	de2, de3	0.808	0.810	0.681
감사제도	au1, au2, au3, au4	0.910	0.911	0.655
교육 훈련 프로그램	tr1, tr2, tr3, tr4	0.888	0.886	0.661
최고 경영진의 지원	su1, su2, su3, su4	0.917	0.921	0.746
정책의 준수 의도	in1, in2, in3, in4	0.951	0.954	0.839

〈표 6〉 상관계수와 AVE 제곱근(SPSS 20)

잠재변수		관측변수	명확성	포괄성	조직	처벌	감사	지원	훈련	의도
정보보호 정책	정책의 명확성	cl1, cl2, cl3 cl4, cl5	0.73							
	정책의 포괄성	di3, di4	0.670	0.77						
보안 전담조직		de2 de3	0.548	0.568	0.77					
처벌		pu1 pu2	0.141	0.240	0.265	0.78				
감사 제도		au1, au2 au3, au4	0.275	0.377	0.494	0.496	0.76			
최고 경영진의 지원		su1, su2 su3, su4	0.252	0.330	0.476	0..440	0.631	0.80		
교육 훈련 프로그램		tr1, tr2, tr3, tr4	0.444	0.532	0.603	0.419	0.503	0.549	0.76	
정보보호 정책의 준수 의도		in1, in2 in3 in4	0.242	0.343	0.448	0.306	0.604	0.498	0.357	0.86

주) 대각선 음영 부분은 AVE의 제곱근.

주요한 측정치로서, 일반적으로 0.7 이상이면 잠재변 수의 측정이 내적으로 일관성을 확보하고 있는 것으로 판단한다[Fornell and Larcker, 1981]. 검증 결과는 CR 값이 모두 0.8 이상으로 관측변수에 대한 응답의 내적일관성을 확보하고 있는 것으로 나타났다(<표 5>). 평균분산추출값(AVE)은 신뢰도의 또 다른 측정치로서, 잠재 변수에 대해 관측 변수가 설명할 수 있는 분산의 크기를 나타낸다. 기준은 값이 0.5 이상이면 신뢰도가 있는 것으로 판단하는데[Fornell and Larcker, 1981], 검증 결과, AVE값이 모두 0.5 이상으로 내적일관성을 확보하고 있는 것으로 나타났다(<표 5>).

마지막으로 판별타당성은 구성개념간의 상관관계를 보여주는 것으로서, 잠재 변수에 대한 상관행렬(Correlation Matrix)을 분석한다. 일반적으로 피어슨 상관계수(Pearson's correlation coefficient)가 기준으로 사용되는데, 그 값이 0.8 이상이면 잠재 변수간에 다중공선성이 존재하는 것으로 판단한다. 분석 결과, 상관계수(r)의 값이 0.8 이하로 나타나, 잠재 변수 간에 다중공선성의 문제는 없는 것으로 확인되었다(<표 6>).

또한 <표 6>에서 볼 수 있는 바와 같이, 평균분산추출의 제곱근($\sqrt{AVE}$)의 값이 최소 0.7 이상이고, 각 대각선에 있는 제곱근의 값이 잠재 변수들 간의 상관계수 값보다 높게 나타나 구성개념들 간의 판별타당성을 확인하였다.

4.3 구조 모형의 분석 결과

구조 모형의 분석에서는 모형의 적합성과 모형에서 제시한 가설을 검정한다. 본 절에서는 통계적인 분석 결과와 그 의미를 정리하도록 한다.

4.3.1 구조 모형의 적합성

구조 모형의 적합도는 이론 모형과 실제 공분산 간의 일치성 정도를 나타내는 것으로서, 절대적합지수, 증분적합지수, 간명부합지수 등으로 구분하여 판단한다. 분석 결과를 종합해 보면, 구조모형의 적합성은 전반적으로 타당한 것으로 나타났는데(<표 7> 참조), 세부적인 분석 결과를 정리하면 다음과 같다.

첫째, 절대적합지수(Absolute Fit Measures)는 연구 모형의 전반적인 부합 정도를 나타내는 지수로서, 여기에는 GFI, RMR, RMSEA 등이 있다. 적합도지수(Goodness-of-Fit Index : GFI)는 모형의 표본공분산행렬을 설명하는 비율로서 0~1 사이의 값을 가지며, 값이 클수록 양호한 것으로 판단한다. 전통적으로 0.9를 기준으로 적용하는데, 본 모형의 GFI 값은 0.90으로 양호한 것으로 나타났다. 잔차평균자승이중근(Root Mean Square Residual : RMR)은 관찰된 공변량행렬(S)과 예측된 공변량행렬(Z) 간의 차이로서, S와 Z의 차이가 작을수록 적합한 모형이 되기 때문에, RMR 값이 0에 가까울수록 좋은 모형으로 평가하는데, 일반적으로 0.05 이하이면 대체로 양호한 모형으로 평가한다[배병렬, 2005; Tomarken and Waller, 2005]. 본 모형의 RMR 값은 0.030으로 양호한 것으로 나타났다. 근사오차평균자승의 이중근(Root Mean Square Error of Approximation : RMSEA) 값은 대체로 0.05 이하이면 양호한 모형으로 평가하는데[Browne and Cudeck, 1993], 본 모형의 RMSEA 값은 0.050으로 양호한 것으로 나타났다.

〈표 7〉 구조모형의 적합성

구 분	내용	결과값	기준
절대적합지수 (Absolute Fit Measures)	X^2/자유도(df)	1.97	$\leq 2^{**}$, $\leq 3^{*}$
	GFI	0.90	$\geq 0.90^{**}$, $\geq 0.80^{*}$
	RMR	0.030	$\leq 0.05^{**}$, $\leq 0.08^{*}$
	RMSEA	0.050	$\leq 0.05^{*}$
증분적합지수 (Incremental Fit Measures)	NFI	0.97	$\geq 0.90^{**}$
	NNFI	0.98	$\geq 0.90^{**}$
	CFI	0.99	$\geq 0.90^{**}$
간명부합지수 (Parsimonious Fit Measures)	AGFI	0.87	$\geq 0.90^{**}$, $\geq 0.80^{*}$
	PGFI	0.70	클수록 우수
	PNFI	0.82	클수록 우수

주) Acceptability : **acceptable, *marginal.

둘째, 증분적합지수(Incremental Fit Measures)는 기초 모형에 대해 제안 모형이 얼마나 적합한지를 나타내는 지수로서, 여기에는 NFI, NNFI, CFI 등이 포함된다. 표준적합지수(Normed Fit Index : NFI)는 기초 모형에 대해 제안 모형이 어느 정도 적합한지를 나타내는 지수로서, 값이 0.90 이상이면 적합한 모형이라고 평가한다[Bentler, 1990]. 본 모형의 NFI 값은 0.97로서 모형의 적합도가 높은 것으로 나타났다. 비표준적합지수(Non-Normed Fit Index : NNFI)는 표본의 크기가 작은 경우에 모형의 적합성을 설명하는데, 0.90 이상이면 양호하고 적합한 모형이라고 평가한다[Marsh et al., 1998]. 본 모형의 경우 NFI와 NNFI 모두 0.90 이상으로 기초 모형에 대한 제안 모형의 적합도가 높은 것으로 나타났다. 비교적합지수(Comparative Fit Index : CFI)는 기초 모형과 제안 모형을 비교하여 데이터가 부합하는 정도를 나타내는 값으로서, 보통 0.90 이상이면 양호한 수준을 나타낸다. 본 연구 모형의 경우, CFI 값이 0.99로

양호한 것으로 나타났다.

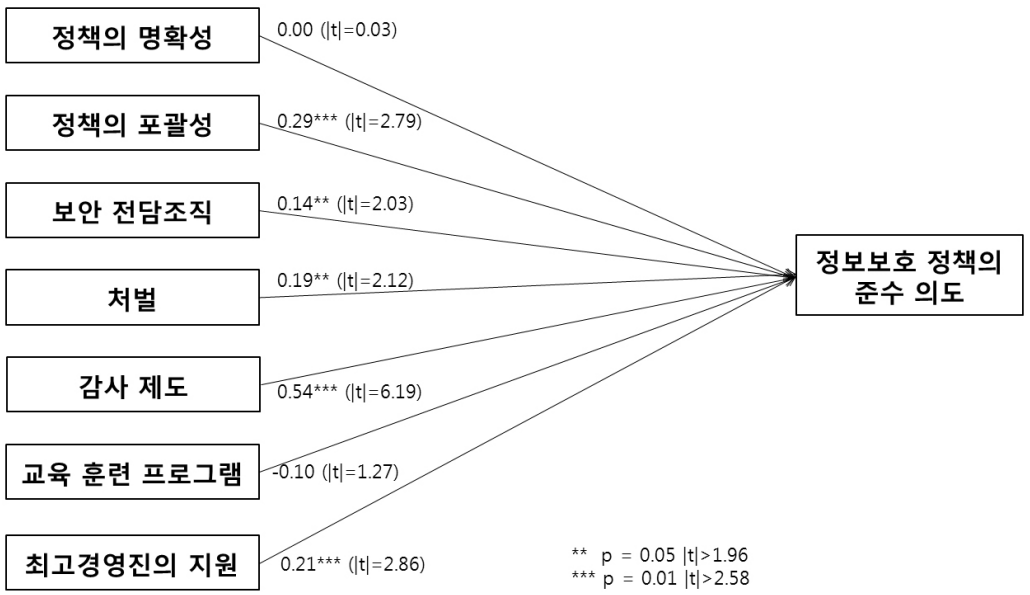
마지막으로 간명부합지수(Parsimonious Fit Measures)는 모형의 복잡성과 객성성의 차이를 평가하는 추정치로서, 여기에는 AGFI, PNFI, PGFI 등이 있다. 조정적합지수(Adjusted Goodness-of-Fit-Index : AGFI)는 GFI를 확장시킨 개념으로서, 일반적으로 0~1사이의 값을 가지는데, 0.8 이상이면 수용 가능한 수준, 0.9 이상이면 양호한 수준으로 판단한다. 본 모형의 AGFI 값은 0.87로서 수용 가능한 수준으로 나타났다. 간명적합지수(Parsimonious Goodness-of-Fit-Index : PGFI)는 GFI를 수정하여 구한 값으로 0~1 사이의 값을 가지며, 높을수록 모형의 간명도가 높다고 판단한다. 본 연구 모형의 경우 PGFI 값은 0.70으로 양호한 것으로 나타났다. 간명표준적합지수(Parsimonious Normed Fit Index : PNFI)는 NFI를 수정하여 구한 값으로 값의 범위가 0.6~0.9사이에 있으면 유의한 것으로 본다. 본 연구 모형의 PNFI 값이 0.82로 유의한 결과 값이 나타났다.

4.3.2 가설 검정 결과

먼저, 독립 변수와 종속 변수 간의 관계에 관해 수립된 가설을 검정하기 위한 경로분석 결과는 다음의 <그림 2>에 정리되어 있다. 변수들 중에서 '정보보호 정책의 명확성'과 '교육 훈련 프로그램'을 제외한 모든 변수들이 통계적으로 유의한 결과를 나타냈다.

다음으로 조절 효과의 분석은 자유 모형(기본모형)과 등가제약 모형(두 집단간 경로계수가 동일하다는 제약을 가한 모형)의 X^2(chi-square) 값의 차이가 3.84 이상 이면 조절 효과가 있는 것으로 판단하였다[Brockman and Morgan, 2006]. 다음의 <표 8>에는 조절변수들의 조절 효과를 분석한 결과가 정리되어 있다.

연령의 경우, 최고 경영진의 지원과 정보정책 준수 의도 사이의 ΔX^2가 4.96으로 나타나 연령(40세 미만 그룹, 40세 이상 그룹)에 따른 조절 효과가 있는 것으로 나타났다. 성별의 경우에는 모든 변수의 ΔX^2가 3.84 미만으로 통계적으로 유의한 조절 효과가 나타나지 않았다.



〈그림 2〉 경로 분석 결과(주모형)

〈표 8〉 조절효과 분석결과

조절 변수	그룹 A	그룹 B	검증결과(ΔX^2 > = 3.84 채택)				
			독립 변수	자유모형 (df = 612)	등가제약 모형 (df = 613)	ΔX^2	채택 여부
연령	40대 미만 (N = 144)	40대 이상 (N = 227)	정책의 명확성	948.52	949.62	1.1	-
			정책의 포괄성		94836	0.16	기각
			처벌		951.71	3.19	기각
			보안 전담조직		948.95	0.43	기각
			감사제도		948.68	016	기각
			최고경영진 지원		953.48	4.96	채택
			교육 훈련		948.97	0.45	-
성별	남자 (N = 313)	여자 (N = 58)	정책의 명확성	900.3	900.2	0.1	-
			정책의 포괄성		900.74	0.44	기각
			처벌		903.57	3.27	기각
			보안 전담조직		898.79	1.51	기각
			감사제도		901.86	1.56	기각
			최고경영진 지원		901.48	1.18	기각
			교육 훈련		901.5	1.2	-

그리고 조절 효과가 있는 것으로 확인된 조절 변수인 연령이 최고 경영진의 지원과 정책 준수 의도 간에 미치는 조절 효과의 강도를 판단하기 위하여 두 집단(40대 미만과 40대 이상 그룹)의 경로계수의 통계적 유의성을 비교 분석하였다 [Brockman and Morgan, 2006]. 다음의 <표 9>에서 볼 수 있는 바와 같이, 최고 경영진의 지원이 준수 의도에 미치는 영향이 40대 이상의 그룹에서는 유의하였으나, 40대 미만의 그룹에서는 유의하지 않았다. 이것은 최고 경영진의 지원이 준수 의도에 미치는 영향은 나이가 많은 집단에서 더 크다는 것을 의미한다.

〈표 9〉 연령 집단별 경로계수 및 t값

최고경영진의 지원 (연령)	40대 이상 그룹	40대 미만 그룹
	0.41***(|t| = 3.21)	0.06(|t| = 0.60)

4.3.3 분석 결과에 대한 토의

데이터 분석 결과, 정보보호 대책이 정보보호 정책의 준수에 미치는 영향에 관해 수립한 7개 가설 중에서 2개를 제외하고는 모두 채택되었다. 그리고 조절 변수에 관한 가설의 경우, 연령의 경우 최고 경영자의 지원과 정책의 준수 의지간의 관계에 조절 효과가 있는 것으로 나타났으나, 성별은 조절 효과가 없는 것으로 나타나 가설이 채택되지 않았다.

다음에서는 연구 모형의 각 변수에 대해 가설이 채택되었거나 채택되지 못한 배경과 이유에 대해 탐색해 보도록 한다.

(1) 정보보호 정책의 명확성 및 포괄성

정보보호 정책의 포괄성은 직원들의 정보보호 정책 준수 의도에 정의 영향을 미치는 것으로 나타나, 정책의 범위, 즉, 정책이 조직의 정보보호에 필요한 요소들을 포함하고 있는 정도가 높을수록 직원들이 정보보호 정책을 준수하겠다는 의도가 높아진다는 예상된 결과를 얻었다.

그러나 기대했던 정책의 명확성은 정책의 준수 의도에 영향을 미치지 않는 것으로 나타났다.

즉, 정보보호 정책이 명확하고 이해하기 용이한 정도가 높아질수록 해당 정책을 준수하려는 의도가 높아질 것이라는 가설이 채택되지 못했다. 이것은 직원들이 정책을 준수하겠다는 의도는 정책의 형식이 아니라 정책의 내용에 의해 영향을 받는다는 것을 의미한다.

이러한 결과가 나타난 가능한 이유로 정책의 품질요소 중의 하나인 정책의 간결성에 관련된 연구의 결과를 생각해볼 수 있다. 정책의 간결성은 정책의 명확성과 높은 상관관계를 가지고 있는데[Goel and Chengalur-Smith, 2010], 이러한 간결성은 여러 연구에서 정책 준수 의도와의 관계가 기각되었다[박철주, 임명성, 2012; 임명성, 2013; 임명성, 한군희, 2013]. 따라서 정책의 명확성은 정책의 간결성과 관련성이 높기 때문에, 정책의 간결성과 동일한 결과를 얻은 것으로 추측해 볼 수 있다.

그러나 정책의 명확성이 정책의 준수 의도에 직접적인 영향을 미치지는 않는다고 하더라도, 정책의 품질을 결정하는 요소 중의 하나이므로 정책 수립 및 작성시 주의를 기울일 필요가 있다. 그런데 다음의 <표 10>에서 볼 수 있는 바와 같이, 응답 기업에서의 정책의 명확성은 본 연구에서 조사한 정보보호 대책들 중에서 가장 수준이 낮은 것으로 나타났다(5점 만점에 3.4점). 따라서 은행에서는 향후 정보보호 정책을 수립할 때, 정책의 내용뿐만 아니라 형식에도 보다 세심한 주의를 기울일 필요가 있는 것으로 보인다.

⑵ 보안 전담조직

보안 전담조직은 직원들의 정보보호 정책 준수 의도에 정의 영향을 미치는 것으로 나타나, 정보보호를 위한 적절한 전담조직을 갖추고, 정보보호에 관한 역할과 책임을 명확하게 정의하여 할당하고 있는 정도가 높을수록 직원들이 정보보호 정책을 준수하겠다는 의도가 높아진다는 기대했던 결과가 나타났다.

이것은 정보보호에 적합한 조직 체계와 업무 프로세스를 갖추고, 정보보호에 대한 역할과 책임이 적절히 정의되고 할당된 정보보호 전담조직을 갖추고 있는 조직에서는 직원들이 정보보호 정책을 준수할 가능성이 높다는 것을 의미한다.

국내 은행들의 경우, CISO의 선임이 의무화되어 있다. 보안 전담조직의 적절한 역할과 기능이 정보보호 정책의 준수에 영향을 미치는 것이 입증되었으므로, CISO 제도를 단순히 의무적으로만 운영하지 말고, CISO의 지휘 하에, 정보보호 업무를 기획하고 추진하는 전담조직을 구성하여, 정보보호에 관련된 업무를 보다 체계적이고 효과적으로 수행하도록 하는 것이 중요하다고 판단된다. 또한 조직이 구성되면, 정보보호 활동을 수행하는데 적합한 역량과 스킬을 갖춘 인력을 지정하고, 이들의 책임과 역할을 명시하여 문서화하고, 또한 내부 보고 체계와 외부 연락 체계 등을 수립해야 할 것이다.

⑶ 처벌

처벌은 직원들의 정보보호 정책준수 의도에 정의 영향을 미치는 것으로 나타났다. 이것은 정보보호 정책을 준수하지 않았을 때, 조직이 직원들에게 가하는 처벌의 강도가 높을수록 직원들이

〈표 10〉 본 연구에서 조사한 정보보호 대책들의 통계량

통계량							
	정책의 명확성	정책의 포괄성	보안 전담조직	처벌	감사 제도	교육 훈련	최고경영자 지원
평균	3.4097	3.6321	3.8706	3.9542	4.3349	3.8437	4.2810
표준편차	.7727	.8519	.9106	.7273	.6782	.7896	.7382

정보보호 정책을 준수하겠다는 의도가 높아진다는 예상된 결과이다.

처벌의 엄정성은 이미 많은 분야에서 사람들의 비정상적인 행위를 하려는 경향에 영향을 미친다는 사실이 입증되었고, 본 연구에서도 이와 동일한 결과를 얻었다.

처벌은 부정적인 대책이기는 하지만, 모든 직원들에게 조직의 정보보호 정책을 준수할 의무가 있으며, 이를 위반할 때에는 징계나 해고의 사유가 될 수 있음을 알리고, 그러한 사건이 발생했을 때 처벌을 집행하는 것은 직원들이 정보보호 정책을 지속적으로 준수하도록 하는데 매우 주요한 요인으로 판단된다.

⑷ 감사 제도

감사 제도는 직원들의 정보보호 정책 준수 의도에 정의 영향을 미치는 것으로 나타나, 정보보호 정책/지침에 규정된 사항들을 준수하고 있는지를 확인하기 위한 감사 제도가 적정하게 시행되고 있는 정도가 높을수록 직원들이 정보보호 정책을 준수하겠다는 의도가 높아진다는 예상된 결과를 얻었다.

조직이 감사 활동을 통해서 정보보호 정책의 준수 여부를 모니터링한다는 사실을 직원들이 인지하게 되면, 직원들의 정책을 준수하지 않으면 적발되어 처벌될 수 있다는 생각에 정책을 준수할 가능성이 높아질 것이라는 자연스러운 현상으로 판단된다. 특히, 은행의 경우에는 정보시스템 감사의 역사가 길고, 법규에 의해 의무적으로 정보시스템 감사를 시행해 오고 있기 때문에 이러한 결과가 나타난 것으로 판단된다.

⑸ 교육 훈련 프로그램

예상과 달리, 교육 훈련 프로그램은 직원들의 정보보호 정책 준수 의도에 영향을 미치지 않는 것으로 나타났다. 이것은 회사에서 정보보호에 관련된 교육 훈련 프로그램을 적절하게 실시하고 있는 정도는 직원들이 정보보호 정책을 준수하겠다는 의도가 영향을 미치지 않는다는 것을 의미한다.

이러한 결과에 대한 가능한 해석 중의 하나는 일반 억제 이론(GDT) 분야의 연구 결과에서 제시하고 있는 바와 같이, 처벌과 같은 부정적인 대책은 사람들의 행위에 유의한 영향을 미쳤으나, 보상과 같은 긍정적인 대책인 보상은 그 영향이 불확실하다는데서 찾아볼 수 있다[Lebek et al., 2013]. 즉, 교육 훈련 프로그램도 처벌과 같은 부정적인 대책이 아니라 인력들의 정보보호에 대한 지식을 향상시키기 위한 긍정적인 대책이므로 정책의 준수라는 사람들의 행위에 영향을 미치지 못한 것으로 추측해볼 수 있다.

또 다른 가능한 해석으로는 교육 훈련은 준수 의도에 직접적인 영향을 미치기 보다는 다른 요인을 통해 간접적으로 영향을 미칠 가능성이 있다는 것이다. 예를 들면, 교육 훈련은 직원들의 정보보호에 대한 인식(information security awareness)을 제고하는데 직접적인 영향을 미치고, 정보보호에 대한 인식은 궁극적으로 준수 의도에 영향을 미치는 것으로 추측해 볼 수 있다. 교육 훈련이 인식 제고에 영향을 미친다는 것은 여러 연구에 의해 입증되었고[Spionen, 2000; Goodhue and Peltier, 2002; Chan et al., 2005; Haeussinger and Kranz, 2013], 인식이 행동의 결정요인이 될 수 있다는 사실 또한 여러 연구에 의해 입증되었다[Dinev and Hu, 2007; D'Arcy et al., 2009; Galvez and Guzman, 2009; Haeussinger and Kranz, 2013]. 따라서 교육 훈련은 정보보호에 대한 인식을 매개로 하여 준수 의도에 영향을 미치기 때문에, 교육 훈련과 준수 의도 간의 관계를 직접 보면 그 영향이 나타나지 않을 수도 있을 것이다.

하지만, 본 연구에서는 교육 훈련 프로그램이 정책 준수 의도에 미치는 영향이 입증되지 않았

지만, 교육 훈련은 여전히 조직에서 중요한 정보보호 대책이므로, 프로그램을 잘 수립하여 직원들에게 양질의 프로그램을 지속적으로 제공해야 한다고 판단된다.

⑹ 최고 경영자의 지원

최고 경영자의 지원은 직원들의 정보보호 정책 준수 의도에 정의 영향을 미치는 것으로 나타나, 정보보호에 대해 최고 경영진이 지원하고 참여하는 정도가 높을수록 직원들이 정보보호 정책을 준수하겠다는 의도가 높아진다는 기대한 결과를 얻을 수 있었다.

정보보호 업무는 기본적으로 하향식 구조이므로, 최고 경영진이 정보보호에 관심을 가지고 참여하는 것은 조직 문화에 큰 영향을 미치고, 이것은 다시 정보보호 정책의 준수에 대한 직원들의 태도에 큰 영향을 미칠 수 있다는 사실이 입증되었다.

이러한 최고 경영자의 지원과 직원들의 정책 준수 의도 간의 관계에서 직원들의 연령이 조절 효과를 미치는 것으로 나타났다. 보다 구체적으로는 최고 경영진의 지원이 준수 의도에 미치는 영향은 나이가 많은 집단이 나이가 적은 집단에 비해 더 크게 작용하는 것으로 나타났다. 이것은 아무래도 나이가 많은 집단이 상대적으로 직급이나 직책이 높아서 최고 경영진과의 접촉이 많고, 더 많은 영향을 받을 수 있기 때문인 것으로 판단된다.

⑺ 성별의 조절 효과

조직의 보안 대책과 직원들의 정책 준수 의도 간의 관계에서 성별이 조절 효과를 나타낼 것으로 기대하였으나, 데이터 분석 결과, 어떤 보안 대책에 대해서도 조절 효과가 없는 것으로 나타났다.

이러한 결과는 최근 들어 성별 역할 구분이나 사회경제적 위치의 차이가 약화되거나 거의 없어지고 있는 현상을 반영하는 것이라고 판단된다[신윤정, 2015; Gendered Innovation, 2015]. 한 예로, 비디오 게임 분야에서는 성별에 따라 남녀의 관심사는 선천적으로 다르기 때문에 여자 아이들에게는 '핑크 계열'의 게임(예 : 패션 관련)을 남자 아이들에게는 '블루 계열' 게임(예 : 전투적 게임)을 전통적으로 개발하였다. 그러나 이러한 성별 규범은 변화하여 최근에 가장 인기가 있는 게임의 경우에는 남녀의 이용자 수가 비슷한 것으로 나타났다[Wong and Hines, 2015]. 성별 차이에 관련된 그동안의 연구들을 재분석한 한 연구[Meredith, 2015]에서는 대부분의 특성들이 성별의 차이로 인한 것이라고 볼 수 없다는 결론을 도출하였다.

5. 결 론

본 연구에서는 은행의 IT 인력들이 정보보호 정책을 준수하도록 만들기 위한 실질적인 정보보호 대책에 대해 연구하였다. 특히 본 연구에서는 이 분야의 이론적인 변수들을 분석하기 보다는 은행에서 실제적으로 적용 가능한 보안 대책에 초점을 맞춤으로써, 이 분야에 존재하고 있는 이론과 실무 간의 괴리를 줄이고, 은행에서 효과적인 정보보호 대책을 수립하는데 참조할 수 있는 실무적인 시사점을 제시하고자 하였다.

본 연구의 주요한 결과를 정리해 보면, 먼저, 정보보호 정책의 경우, 직원들이 정책을 준수하겠다는 의지는 정책의 형식이 아니라 정책의 내용에 의해 영향을 받으므로, 정책이 조직의 정보보호에 필요한 요소들을 모두 포함하도록 주의를 기울일 필요가 있다. 또한 정책의 명확성은 정책의 준수 의도에 직접적인 영향을 미치지는 않는다고 확인되었지만, 정책의 품질을 결정하는 요소 중의 하나이고, 응답 결과를 보면, 정책의 명확성이 다른 정보보호 대책에 비해 상당히 미흡하므로, 정책의 형식에도 보다 세심한 주의를 기울

일 필요가 있는 것으로 보인다. 정보보호 전담조직의 운용, 엄정한 처벌의 집행, 감사 제도 등도 효과적인 정보보호 대책으로 나타났다.

교육 훈련 프로그램은 예상과 달리 직원들의 정보보호 정책 준수 의도에 영향을 미치지 않는 것으로 나타났지만, 여전히 조직에서 중요한 정보보호 대책이므로, 프로그램을 잘 수립하여 직원들에게 양질의 프로그램을 지속적으로 제공해야 한다고 판단된다.

마지막으로 최고 경영자의 지원은 직원들의 정보보호 정책 준수를 유도하는 정보보호 대책의 하나로 입증되었다. 그런데, 직원들이 연령대에 따라 서로 다른 효과가 나타났는데, 나이가 많은 집단에 더 큰 영향을 미치는 것으로 나타났다. 따라서 경영진은 정보보호에 대한 관심과 지원을 보낼 때, 모든 직원들을 대상으로 하기보다는 그 대상에 따라 방법을 달리하는 것을 고려하는 것이 효과적인 방안의 하나로 판단된다.

본 연구의 한계점과 향후 연구 방향은 다음과 같다. 첫째, 본 연구에서는 정보보호 대책들을 응답자의 인식만을 바탕으로 측정하였다. 예를 들면, 정보보호 정책의 포괄성이나 교육훈련 프로그램을 객관적으로 측정하는 방법은 응답자들의 주관적인 생각을 묻는 대신에 수립되어 있는 정책이나 교육훈련 프로그램의 내용을 실제로 분석해서 정책의 범위나 프로그램의 적정성을 결정하는 것이다. 따라서 향후 연구에서는 응답자의 인식만을 바탕으로 정보보호 대책을 분석하지 말고, 보다 객관적인 측정방법을 도입하여 연구를 진행하는 것이다.

둘째, 이 분야에서 수행된 대부분의 연구에서와 마찬가지로 본 연구에서도 종속 변수로 직원들의 실제 행동이 아니라 의도를 측정하고 분석하였다. 실제 행동이 아니라 의도를 분석한 가장 큰 이유는 실제적인 행동을 관찰하는 것이 어렵기 때문이다. 그러나 사람들은 의도는 확실히 가지고 있었더라도 실제로 행동하지 못할 수 있다. 따라서 향후 연구에서는 의도와 실제 행동 간의 관계와 이러한 관계에 영향을 미치는 요인들을 분석할 필요가 있다.

참 고 문 헌

[1] 강다연, 장명희, “정보보안 정책 준수가 정보보안능력 및 행동에 미치는 영향 분석 : 해운항만조직 구성원을 대상으로”, *한국항만경제학회지*, 제30권 제1호, 2014, pp. 97-118.

[2] 교육과학기술부, 정보보안 모범사례 가이드, 2011.

[3] 금융위원회 전자금융과, 금융감독원 IT감독국, “금융전산 보안 강화 종합대책”, 2013.

[4] 김상현, 송영미, “조직 구성원들이 정보보안 준수 동기요인에 관한 연구”, *e-비즈니스 연구*, 제12권 제5호, 2011, pp. 327-349.

[5] 김상훈, 박선영, “정보보안 정책 준수 의도에 대한 영향요인”, *한국전자거래학회지*, 제16권 제4호, 2011, pp. 33-51.

[6] 김지수, 김종배, 신용태, “조직 내 정보보호 최고책임자(CISO)의 역할인식이 정보보호 성과에 미치는 영향에 관한 연구”, *경영컨설팅연구*, 제12권 제4호, 2012, pp. 21-34.

[7] 박종원, 김현규, “정보보안 전략과 보안준수 의도의 관계에 관한 연구모델개발을 위한 탐색적 연구”, 한국경영정보학회 추계학술대회, 2012, pp. 559-564.

[8] 박철주, 임명성, “보안 대책이 지속적 보안 정책 준수에 미치는 영향”, *디지털정책연구*, 제10권, 제4호, 2012, pp. 23-35.

[9] 배병렬, LISREL 구조방정식 모델-이해와 활용, 청람, 2005년.

[10] 보안뉴스, “개정 전자금융거래법! 꼭 체크해야 할 8개 보안조항”, 보안뉴스, 2014. 12. 9.

[11] 신윤정, “저출산 시대의 가사 노동 및 자녀 돌봄 시간 변화와 시사점”, 보건・복지 Issue and Focus, 2015.

[12] 신현구, 이주락, “조직공정성이 산업보안담당자의 보안정책 준수의지에 미치는 영향”, *한국경호경비학회*, 제39권, 2014, pp. 241-268.

[13] 안중호, 박준형, 성기문, 이재홍, “처벌과 윤리교육이 정보보안 준수에 미치는 영향 : 조직유형의 조절효과를 중심으로”, *Information Systems Review*, Vol. 12, No. 1, 2010, pp. 23-42.

[14] 위키백과, “정보보안”, http://ko.wikipedia.org/w/index.php?title=%EC%A0%95% EB%B3%B4_%EB%B3%B4%EC%95%88&oldid=13061197, 2015. 2. 1.

[15] 임명성, “조직 구성원들의 정책 준수행위 의도에 관한 연구”, *디지털정책연구*, 제10권 제10호, 2012, pp. 119-228.

[16] 임명성, “정보보안 정책의 채택이 구성원들의 보안정책 준수 행위에 미치는 영향에 관한 연구”, *디지털정책연구*, 제11권 제1호, 2013, pp. 27-38.

[17] 임명성, “조직 구성원들의 정보보안 정책 준수에 영향을 미치는 요인에 관한 연구 -금융서비스업을 중심으로”, *서비스경영학회지*, 제14권 제1호, 2013, pp. 143-171.

[18] 임명성, 한군희, “정보보안 정책준수에 영향을 미치는 요인 : 위험보상이론 관점에서”, *The Journal of Digital Policy and Management*, Vol. 11, No. 10, 2013, pp. 153-168.

[19] 장명희, 강다연, “항만지업 종사자들의 정보보안인식과 지각된 정보보안위험에 영향을 미치는 요인”, *한국항해항만학회지*, 제36권 제3호, 2012, pp. 261-271.

[20] 황경태, 정보시스템 감사- IT 거버넌스의 핵심수단, 탑북스, 2011.

[21] Gendered Innovation, “지나치게 성별 차이를 강조하면 문제가 될 수 있다”, <http://genderedinnovations.wiset.re.kr/terms/overemphasizing.jsp>, 2015. 5. 1.

[22] Nellycw, “우리나라 은행 순위 및 종류”, 2015. 2. 17.<http://nellycw.tistory. com/47>.

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

[24] Bauer, S., Bernroider, E. W. N., and Chudzikowski, K., “End User Information Security Awareness Programs for Improving Information Security in Banking Organizations : Preliminary Results from an Exploratory Study”, Proceedings of the Eighth Pre-ICIS Workshop on Information Security and Privacy(SIGSEC), 2013, pp. 33-49.

[25] Bentler, P. M., “Comparative Fit Indexes in Structural Models”, *Psychological Bulletin*, Vol. 107, No. 2, 1990, pp. 238-246.

[26] Blakley, B., McDermott, E., and Geer, D., “Information Security is Information Risk Management”, Proceedings of the 2001 workshop on New security paradigms, ACM, 2001, pp. 97-104.

[27] Boss, S., Kirsch, L., Angermeier, I., Shingler, R., and Boss, R., “If Someone Is Watching, I'll Do What I'm Asked : Mandatoriness, Control, and Information Security”, *European Journal of Information Systems*, Vol. 18, No. 2, 2009, pp. 151-164.

[28] Brancheau, J. C., Janz, B. D., and Wetherbe, J. C., Key Issues in Information Sstems Mnagement : 1994~1995 SIM Delphi Results”, *MIS Quarterly*, Vol. 20, No. 2, 1996,

pp. 225-242.

[29] Brockman, B. K. and Morgan, R. M., "The Moderating Effect of Organizational Cohesiveness in Knowledge Use and New Product Development", *Journal of the Academy of Marketing Science*, Vol. 34, No. 3, 2006, pp. 295-307.

[30] Browne, M. W. and Cudeck, R., "Alternative Ways of Assessing Model Fit", *Sage Focus Editions*, Vol. 154, 1993, pp. 136-136.

[31] 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.

[32] Cavusoglu, H., Mishra, B., and Raghunathan, S., "A Model for Evaluating IT Security Investments", *Communications of the ACM*, Vol. 47, No. 7, 2004, pp. 87-92.

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

[34] Chang, A. J.-T. and Yeh, Q.-J., "On Security Preparations Against Possible IS Threats Across Industries", *Information Management and Computer Security*, Vol. 14, No. 4, 2006, pp. 343-360.

[35] Cheng, L., Li, Y., Li, W., Holm, E., and Zhai, Q., "Understanding the Violation of IS Security Policy in Organizations : An Integrated Model Based on Social Control and Deterrence Theory", *Computers and Security*, Vol. 39, 2013, pp. 447-459.

[36] CNSS, CNSSI-4014 Information Assurance Training Standard for Information Systems Security Officers, 2010.

[37] Crossler, R. E., Johnston, A. C., Lowry, P. B., Hud, Q., Warkentin, M., and Baskerville, R., "Future Directions for Behavioral Information Security Research", *Computers and Security*, Vol. 32, 2013, pp. 90-101.

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

[39] Doherty, N. F., Anastasakis, L., and Fulford, H., "The Information Security Policy Unpacked : A Critical Study of the Content of University Policies", *International Journal of Information Management*, Vol. 29, No. 6, 2009, pp. 449-457.

[40] Feng, T. and Zhao, G., "Top Management Support, Inter-organizational Relationships and External Involvement", *Industrial Management and Data Systems*, Vol. 114, No. 4, 2014, pp. 526-549.

[41] Fornell, C. and Larcker, D. F., "Structural Equation Models with Unobservable Variables and Measurement Error : Algebra and Statistics", *Journal of Marketing Research*, No. 18, No. 3, 1981, pp. 382-388.

[42] Furnell, S. and Thomson, K.-L., "From Culture to Disobedience : Recognising the Varying User Acceptance of IT Security", *Computer Fraud and Security*, No. 2, 2009, pp. 5-10.

[43] George, D. and Mallery, P., SPSS for Windows Step by Step : A Simple Guide and Reference. 11.0 update (4th ed.), 2003, Boston : Allyn and Bacon.

[44] Goel, S. and Chengalur-Smith, I. N., "Metrics for Characterizing the Form of Security Policies", *The Journal of Strategic Information Systems*, Vol. 19, No. 4, 2010, pp. 281-295.

[45] Gundu, T. and Flowerday, S. V., "Ignorance to Awareness : Towards an Information Security Awareness Process", *SAIEE Africa Research Journal*, Vol. 104, No. 2, 2013, pp. 69-79.

[46] Guo, K. H., "Security-related Behavior in Using Information Systems in the Workplace : A Review and Synthesis", *Computers and Security*, Vol. 32, 2013, pp. 242-251.

[47] 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.

[48] Hagen, J. M., Albrechtsen, E., and Hovden, J., "Implementation and Effectiveness of Organizational Information Security Measures", *Information Management and Computer Security*, Vol. 16, No. 4, 2008, pp. 377-397.

[49] H¨ansch, N. and Benenson, Z., "Specifying IT Security Awareness", 25th International Workshop on Database and Expert Systems Applications, 2014, pp. 326-330.

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

[51] Hovav, A. and D'Arcy, J., "Applying an Extended Model of Deterrence Across Cultures : An Investigation of information Systems Misuse in the U.S. and South Korea", *Information and Management*, Vol. 49, No. 2, 2012, pp. 99-110.

[52] 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 Sciences*, Vol. 43, No. 4, 2012, pp. 615-659.

[53] Ifinedo, P., "Understanding Information Systems Security Policy Compliance : An Integration of the Theory of Planned Behavior and the Protection Motivation Theory", *Computers and Security*, Vol. 31, No. 1, 2012, pp. 83-95.

[54] ISO, ISO/IEC 27000:2009 Overview and Vocabulary, 2009.

[55] Khalid, S., Solimana, K. S., and Janzb, B. D., "An Exploratory Study to Identify the Critical Factors Affecting the Decision to Establish Internet-based Interorganizational Information Systems", *Information and Management*, Vol. 41, No. 6, 2004, pp. 697-706.

[56] Khan, S. A., Lederer, A. L., and Mirchandani, D. A., "Top Management Support, Collective Mindfulness, and Information Systems Performance", *Journal of International Technology and Information Management*, Vol. 22, No. 1, 2013, p. 6.

[57] 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.

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

[59] 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. 6, 2004, pp. 707-718.

[60] Leonard, L. N. K., Cronan, T. P., and Kreie, J., "What Influences IT Ethical Behavior Intentions-Planned Behavior, Reasoned Action, Perceived Importance, Individual Characteristics?", *Information Management*, Vol. 42, No. 1, 2004, pp. 143-158.

[61] Li, M., Lou, W., and Ren, K., "Data Security and Privacy in Wireless Body Area Networks", Wireless Communications, *IEEE*, Vol. 17, No. 1, 2010, pp. 51-58.

[62] Lohmeyer, D. F., McCrory, J., and Pogreb, S., "Managing Information Security (Current Research)", The McKinsey Quarterly, 2002, p. 12.

[63] Meredith, S. L., "Comparative Perspectives on Human Gender Development and Evolution", *American Journal of Physical Anthropology*, Vol. 156, No. S59, 2015, pp. 72-97.

[64] Merete, J., Eirik, H., and Hovden, A. J., "Implementation and Effectiveness of Organizational Information Security Measures", *Information Management and Computer Security*, Vol. 16, No. 4, 2008, pp. 377-397.

[65] Mobley, W. H., Griffeth, R. W., Han, H. H., and Meglino, B. M., "Review and Conceptual Analysis of the Employee Turnover Process", *Psychological Bulletin*, Vol. 86, No. 3, 1979, pp. 493-522.

[66] Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A., "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules and Quest; An Empirical Study", *European Journal of Information Systems*, Vol. 18, No. 2, 2009, pp. 126-139.

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

[68] Peace, A. G., Galletta, D. F., and Thong, J. Y. L., "Software Piracy in the Workplace : A Model and Empirical Test", *Journal of Management Information Systems*, Vol. 20, No. 1, 2003. pp. 153-177.

[69] Pogarsky, G. and Piquero, A. R., "Studying the Reach of Deterrence : Can Deterrence Theory Help Explain Police Misconduct?", *Journal of Criminal Justice*, Vol. 32, No. 4, 2004, pp. 371-386.

[70] PricewaterhouseCoopers, "Global State of Information Security Survey 2011", http://www.pwc.com/gx/en/information-security-survey/pdf/giss-2011-survey-report.pdf, July 25, 2012.

[71] Ransbotham, S. and Mitra, S., "Choice and Chance : A Conceptual Model of Paths to

Information Security Compromise", *Information Systems Research*, Vol. 20, No. 1, 2009, pp. 121-139.

[72] Rosemann, M. and Vessey, I., "Toward Improving the Relevance of Information Systems Research to Practice : The Role of Applicability Checks", *MIS Quarterly*, Vol. 32, No. 1, 2008, pp. 1-22.

[73] Sari, P. K. and Trianasari, N., "Information Security Awareness Measurement with Confirmatory Factor Analysis", 2014 International Symposium on Technology Management and Emerging Technologies(ISTMET 2014), 2014, pp. 218-223.

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

[75] Siponen, M., Vance, A., and Willison, R., "New Insights into the Problem of Software Piracy : The Effects of Neutralization, Shame, and Moral Beliefs", *Information and Management*, Vol. 49, No. 7, 2012, pp. 334-341.

[76] Solms, R., "Information security management(3) : the Code of Practice for Information Security Management (BS 7799)", *Information Management and Computer Security*, Vol. 6, No. 5, 1998, pp. 224-225.

[77] Richardson, R., "CSI Computer Crime and Security Survey", *Computer Security Institute*, Vol. 1, 2008, pp. 1-30.

[78] Sandhu, R. S. and Samarati, P., "Access Control : Principle and Practice", Communications Magazine, *IEEE*, Vol. 32, No. 9, 1994, pp. 40-48.

[79] Son, J. Y., "Out of Fear or Desire? Toward a Better Understanding of Employees' Motivation to Follow IS Security Policies", *Information and Management*, Vol. 48, No. 7, 2011, pp. 296-302.

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

[81] Srinivasan, S., "Information Security Policies and Controls for a Trusted Environment", *Information Systems Control Journal*, No. 2, 2008.

[82] Steel, R. P., "Turnover Theory at the Empirical Interface : Problems of Fit and Functions", *Academy of Management Review*, Vol. 27, No. 3, 2002, pp. 346-360.

[83] Štemberger, M. I., Manfreda, A., and Kovačič, A., "Achieving top management support with business knowledge and role of IT/IS personnel", *International Journal of Information Management*, Vol. 31, No. 5, 2011, pp. 428-436.

[84] Straub, D., "Effective IS Security : An Empirical Study", *Information Systems Research*, Vol. 1, No. 3, 1990, pp. 255-276.

[85] Tomarken, A. J. and Waller, N. G., "Structural Equation Modeling : Strengths, Limitations, and Misconceptions", *Annu. Rev. Clin. Psychol.*, Vol. 1, 2005, pp. 31-65.

[86] Tariq, M. A., Brynielsson, J., and Artman, H., "The Security Awareness Paradox : A Case Study", 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining(ASONAM 2014), 2014, pp. 704-711.

[87] Tsohou, A., Karyda, M., Kokolakis, S., and Kiountouzis, E., "Analyzing Trajectories of Information Security Awareness", *Information Technology and People*, Vol. 25, No. 3, 2012, pp. 327-352.

[88] Vance, A. and Siponen, M. T., "IS Security Policy Violations : A Rational Choice Perspective", *Journal of Organizational and End User Computing (JOEUC)*, Vol. 24. No. 1, 2012, pp. 21-41.

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

[90] Vroom, C. and Solms, R. von, "Towards Information Security Behavioural Compliance", *Computers and Security*, Vol. 23, No. 3, 2004, pp. 191-198.

[91] Wenzel, M., "The Social Side of Sanctions : Personal and Social Norms as Moderators of Deterrence", *Law and Human Behavior*, Vol. 28, No. 5, 2004, p. 547.

[92] Wong, W. I. and Hines, M., "Preferences for Pink and Blue : The Development of Color Preferences as a Distinct Gender-Typed Behavior in Toddlers", Archives of Sexual Behavior, 2015, pp. 1-12.

[93] Workman, M., Bommer, W. H., and Straub, D., "Security Lapses and the Omission of Information Security Measures : A Threat Control Model and Empirical Test", *Computers in Human Behavior*, Vol. 24, 2008, pp. 2799-2816.

[94] Yildirima, E. Y., Akalpa, G., Aytacb, S., and Bayramb, N., "Factors Influencing Information Security Management in Small- and Medium-sized Enterprises : A Case Study from Turkey", *International Journal of Information Management*, Vol. 31, 2011, pp. 360-365.

[95] Zmud, B., "Editor's Comments", *Management Information Systems Quarterly*, Vol. 22, No. 3, 1998, p. 1.

저자소개

심 준 보

(주)시너지 센트릭스 대표이사이고, 현재 동국대학교 경영대학 경영정보학과 박사과정에 재학 중이다. 부산대학교 문리과대학을 졸업하고 서강대학교 경영대학원에서 경영학 석사(MIS 전공)를 취득하였다. 주요 관심분야는 정보전략, Cloud Security, Forensic, Cyber Security, Information Security Culture 등이다.

황 경 태

현재 동국대학교 경영대학 경영정보학과 교수로 재직 중이다. 연세대학교 상경대학을 졸업하고, Geroge Washington University에서 경영학 석사, State University of New York at Buffalo에서 경영정보학 박사학위를 취득하였다. 주요 관심분야는 정보 전략, IT 거버넌스, IT 서비스 관리 등이다.