

# 금융회사의 정보보호활동이 정보보호의식 및 정보보호자신감에 미치는 영향 : 정보보호의식의 매개효과를 중심으로

(Influence of Information Security Activities of Financial Companies on Information Security Awareness and Information Security Self Confidence : Focusing on the Mediating Effect of Information Security Awareness)

소현철<sup>1)</sup>, 김종근<sup>2)\*</sup>

(Soh Hyeon-Chul and Kim Jong Keun)

**요약** 본 연구의 목적은 금융회사의 정보보호활동이 정보보호담당자들의 보안업무에 대한 자신감에 미치는 영향을 파악하고 미흡한 점을 보완하기 위한 학문적, 실무적 시사점을 찾기 위한 연구이다. 연구결과, 금융회사가 정보보호교육, 침해사고 대응 및 입/출입 보안에 중점을 두고 정보보호활동을 하면 정보보호담당자의 회사에 대한 정보보호자신감 및 직원들의 정보보호의식 수준이 높아진다는 것을 확인할 수 있었다.

**핵심주제어** : 정보보호, 정보보호활동, 정보보호의식, 정보보호자신감

**Abstract** The Purpose of this Study is to find out the Implications of the Information Security Activities of Financial Companies on the Confidence of the Information Security Officers and to find Academic and Practical Implications to Supplement the Insufficiencies. As a Result, it was Confirmed that the Information Security Officer's Confidence in Information Security for Companies and the Level of Information Security Awareness of the Employees are Increased when Financial Companies Conduct Information Protection Activities Focusing on Information Security Education, Security Incident Responses and In/Out Security.

**Key Words** : Information Security, Information Security Activity Information Security Awareness, Information Security Confidence

---

\* Corresponding Author : 107068@hoseo.edu

† 본 논문은 소현철이 작성중인 박사학위 논문을 기반으로 작성하였음.

Manuscript received July 31, 2017 / revised Aug 29, 2017 / accepted Aug 30, 2017

1) 호서대학교 벤처경영학과, 제1저자

2) 호서대학교 벤처경영학과, 교신저자

## 1. 서론

금융회사는 급속한 정보통신기술(ICT : Information and Communication Technology)의 발전에 힘입어 고객이 금융회사의 영업점을 방문하지 않고 PC 및 스마트폰 등을 활용해 장소와 시간에 상관없이 온라인으로 결제, 송금, 대출 및 보험 가입 등을 할 수 있는 금융서비스를 제공하여 국민들로부터 많은 호응을 받아 왔다. 한국은행(2017)[1]이 발표한 ‘2016년도 금융정보화 추진 현황’에 의하면 금융회사의 전자금융서비스 규모는 지속적인 성장세를 보여, 2016년중 인터넷뱅킹 이용건수 및 금액(모바일뱅킹 이용 실적 포함)은 일평균 8,750만건, 42조 4,247억원으로 전년대비 각각 12.2%, 5.3% 증가하였고, 모바일트레이딩 서비스 이용건수는 전년대비 27.6% 증가한 일평균 3,779만건이며, 보험 인터넷마케팅 일평균 이용건수는 329만건으로 전년대비 25.3% 증가하였다. 그러나 PC, 스마트폰을 이용한 인터넷 뱅킹, 모바일트레이딩 및 보험 인터넷마케팅 등과 같은 전자금융거래의 증가는 우리가 과거에 경험하지 못한 많은 부작용을 일으키고 있다. 대표적인 사례는 해커들이 이용자 PC 및 스마트폰을 대상으로 정보를 유출하여 불법으로 이용자의 예금을 인출하거나, 또는 금융회사의 정보시스템을 타깃으로 디도스(DDOS : Distributed Denial of Service) 공격을 실시하여 금융시스템을 마비시키는 등 사회적 혼란을 초래하는 경우이다.

정부는 이와 같은 정보보호 사고를 사전에 예방하기 위해 금융회사가 준수하여야 할 내용을 금융관련 법규에 명시한 후, 정기적으로 금융회사의 법 준수 여부를 점검하고 있다. 정부는 전자금융거래 안전성 확보 및 이용자 보호를 위해 금융회사가 IT부문에서 지켜야 할 인력, 조직, 시설 및 정보시스템 등에 대한 운영기준을 정보보호 관련 법규에서 규정하고 있으며, 금융회사는 법규 준수를 통한 정보보호활동을 통해 회사의 정보보호수준을 향상시켜 정보보호 사고를 사전에 예방하는 등 정보보호성과를 거두고 있으나, 여전히 정보보호 사고는 끊임없이 발생하고 있다.

기존의 대부분의 연구는 정보보호사고의 예방

을 위한 기업의 정보보호활동이 정보보호성과 등에 미치는 영향을 기업의 임직원을 대상으로 설문 등을 이용하여 분석하였는데, 정보보호성과를 측정하는 주요 요소는 전년대비 정보보호사고의 감소 또는 향후 발생할 정보보호사고의 예방 등이었다[2-3]. 그러나 정보보호 사고는 외부에 공개되지 않거나 또는 축소하여 공개되는 자료로 특정인이외에는 정확한 내용을 파악하기 어려우며, 정보보호활동을 통해 향후 발생할 사고를 사전에 예방하여 수치화한 후 정보보호성과를 측정하는 방법에는 많은 어려움이 있었다.

이에, 본 연구는 정보보호활동이 정보보호의식 및 정보보호성과에 미치는 선행연구 등을 바탕으로 금융회사 정보보호활동의 대표적인 하위요인 중에서 정보보호정책, 정보보호인력, 정보보호예산, 정보보호교육, 침해사고대응, 외주업체 보안, 입/출입 보안 등 7개 요인을 변수로 추출하여 각각의 요인이 금융회사 직원의 정보보호 의식에 미치는 영향과 정보보호담당자의 정보보호자신감에 미치는 영향을 실증분석 하여 학문적 실무적 시사점을 찾고자 한다. 본 연구결과가 금융회사의 정보보호수준 향상을 위한 방향 및 정보보호 관련 의사결정에 중요한 역할을 할 수 있기를 기대한다.

## 2. 이론적 배경

### 2.1 정보보호 및 정보보호 관리체계

‘정보보호’란 일반적으로 ‘정보보안’이라고 하는데 IT보안 초창기에는 정보통신망 등 기술적 부문이 강조된 정보보안이라는 용어를 많이 사용하였으나, 최근에는 기술적 부문뿐만 아니라 관리적, 제도적 차원을 포괄하는 광의의 용어로 ‘정보보호’를 사용하고 있다[4]. 반면 해외에서는 국내와 달리 정보보호를 Information Protection(보호) 대신 Information Security(보안)라는 용어를 사용하여 Security(보안)를 정보보호의 의미로 사용하고 있다[5]. 기존 정보보호의 정의에 대한 연구에서 Pipkin(2000)[6]은 정보보안을 조직의 지적자산을 보호하기 위한 절차라고 정의하였

고, Kim(2017)[7]은 정보보호는 정보에 대한 관리적, 기술적, 물리적 통합적인 관리체계를 말하며 회사의 정보보호정책을 계획하고 실행하기 위한 조직을 만들고 회사의 모든 중요 정보자산을 보호하고 위험을 사전에 예방하는 활동이라고 했다. Park et al.(2014)[8]는 정보보호관리는 정보자산의 안전한 환경 확보를 위해 기업 거버넌스, 조직, 정책, 모범사례, 윤리적 컴플라이언스, 인식, 그리고 기술, 측정, 감사 등 다차원적이고 복합적인 요인을 고려하여야 한다고 했다. 국가정보화기본법에서는 ‘정보보호’를 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적 수단과 기술적 수단을 강구하는 것이라 규정하고 있다[9].

한국인터넷진흥원(KISA, Korea Internet Security Agency)은 조직 또는 기업이 체계적으로 정보보호활동을 할 수 있도록 KISA ISMS(정보보호관리체계; Information Security Management System) 모델을 개발하여 기업에게 제공하고 있다. 동 모델은 기업이 스스로 정보보호 관리체계를 구축/운영하는데 활용할 수 있는 관리체계모델로서, 기업의 정보보호수준을 제고하고자 도입되었다. 또한 한국인터넷진흥원은 조직 또는 기업의 정보보호활동이 정보보호 관리체계 인증기준에 적합한지 심사하는 KISA ISMS 인증제도를 도입하여 일정규모 이상의 주요정보통신서비스 제공자는 의무적으로 인증을 획득하도록 하였다[10]. 한국인터넷진흥원은 조직 및 기업의 주요 정보자산을 보호하는 정보보호활동을 KISA ISMS에서 관리적, 기술적, 물리적 통제활동으로 구분하여 체계화 하였는데, 현재 대부분의 금융회사는 KISA ISMS를 토대로 정보보호활동을 수행하고 있다.

## 2.2 정보보호활동

기업의 정보보호활동에 대한 개념은 명확하게 정의되어 있지 않지만, 국가정보대학원(2006)[11]은 기업보안을 첨단기술 뿐만 아니라 기업활동에 유용한 기술상, 경영상의 정보나 인원, 문서, 시설, 통신 등을 산업스파이나 경쟁관계에 있는 기업은 물론이고 특정한 관계가 없는 자에게 누설 또는

침해당하지 않도록 보호, 관리하기 위한 대응방안이나 활동을 의미한다고 정의하였다. 본 연구는 기존연구를 바탕으로 미래창조과학부와 한국인터넷진흥원이 정보통신망법에 근거하여 기업의 정보자산 보호를 위해 시행하는 ‘정보보호 관리체계(KISA ISMS)’, 전자금융거래법에 의거하여 금융감독원이 금융회사의 IT수준을 평가하는 제도의 일환으로 실시하는 ‘IT경영실태평가’ 및 국가정보원이 정부 및 공공기관을 대상으로 매년 실시하는 ‘정보보호 관리실태 평가’의 평가항목들을 토대로 금융회사 정보보호활동을 7개(정보보호정책, 정보보호인력, 정보보호예산, 정보보호교육, 침해사고대응, 외주업체보안, 입/출입보안)로 구분하였다.

### 2.2.1 정보보호정책

Sun(2004)[12]은 정보보호정책은 조직의 정보보호 관리의 방향을 명시하는 상위수준의 문서로써 조직의 구성원들이 정보보호의 목적과 필요성, 책임과 역할을 인지할 수 있도록 해야 하며, 정보보호 정책을 통해 조직의 정보보호의 방향이 명시될 때 정보보호의 기술, 물리, 관리적 통제가 모두 효과적이고, 효율적으로 운영될 수 있는 기반이 형성될 수 있다고 하였다. Lee(2010)[13]은 기업의 보안정책이란 기업이 보유하고 있는 자산 정보를 다양한 위협으로부터 보호하고 불법적인 자산 또는 정보유출을 사전에 예방하여 회사의 가치 및 기업자산의 손실을 최소화하기 위한 기업의 정책을 규정하는 것으로 기업의 보안정책은 최고경영자에 의한 승인을 받드시 필요로 하며 경영자는 조직전반에 걸쳐 보안정책이 효과적으로 작용될 수 있도록 명확하게 정책방향과 원칙을 제시하고 그 의지를 전 직원에게 천명하여야 한다고 하였다.

### 2.2.2 정보보호인력 및 정보보호예산

정보보호 인력은 “금융회사의 총임직원 중 내부 규정에 따라 정보보호 업무를 처리하는 사람” 그리고 “정보보호 업무를 담당하는 상시 종업원 중 해당 금융회사의 정보보호 업무를 적법한 절

차에 의해 수행하는 사람으로 전자금융감독규정 제60조제1항제13호에 의한 업무수행 인력관리방안에 따라 관리되고 있는 사람으로 정의하고 있다. 금융위원회의 「전자금융감독규정」은 금융회사의 인력, 조직, 예산과 관련하여 정보기술부문 인력은 총 임직원수의 100분의 5 이상, 정보보호 인력은 정보기술부문 인력의 100분의 5 이상, 정보보호예산은 정보기술부 예산의 100분의 7 이상이 되도록 권고하고 있다[14]. 방해경(2011)[15]은 공기업의 정보보안 인력은 IT인력의 6% 이상, 정보보호 예산은 IT예산의 8% 이상 유지하는 것이 바람직하다고 주장하였고, 송기정(2014)[16]은 금융당국이 2011년 발표한 IT보안강화 종합대책으로 금융회사의 정보보호예산은 많이 증가했으나 투자집행에 소극적인 경향으로 예산 집행률은 오히려 낮아지는 등 실질적으로 금융회사의 정보보호수준 향상에 반영되지 못하는 비효율이 있다고 하였다. 전정훈(2011)[17]은 정보보호예산 및 정보보호 전문인력의 부족은 정보보안시스템의 효율적인 운영에 많은 영향을 미칠 수 있다고 분석하였다. 정철용(2015)[18]은 금융회사의 정보보호인력 및 정보보호예산을 조사한 결과 대부분이 금융감독당국이 제시한 기준을 충족하고 있다고 하였다.

### 2.2.3 정보보호교육

Gyeon(2015)[19]은 기업이 정보보안교육에 더 많이 투자 할수록 침해사고는 감소할 것이며, 이는 정보보안교육으로 인해 피교육자의 보안에 대한 인식이 제고되고 정보보안과 관련된 정책을 준수하려는 의지가 강해지기 때문이라고 했다. D'Arcy, Hovay & Galletta(2009)[20]은 정보보안교육은 직원들의 정보보안 인식 수준을 높여 정보시스템(Information System)의 오용을 줄여 준다고 하였다.

Kim et al.(2010)[21]는 정보화 교육을 자체적으로 실시하는 지자체와 아웃소싱을 실시하고 있는 지자체로 분류하여 두 집단의 사용자 만족과 성과에 대한 차이를 연구하였는데, 그 결과 정보화교육 아웃소싱을 실시할 경우 서비스 품질, 교육내용의 특성이 사용자의 만족도에 긍정적인 영

향을 준다고 하였다.

### 2.2.4 침해사고 대응

정보통신기반보호법(제2조)에서는 침해사고와 전자적 침해행위에 대해 정의하고 있다. 침해사고란 전자적 침해행위로 발생한 사태이며, 전자적 침해행위라 함은 정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스 거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위를 말한다. 전자금융거래법(제2조)에서는 전자적 침해행위를 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스거부 또는 고출력 전자기파 등의 방법으로 전자금융기반시설을 공격하는 행위라고 정의하고 있다.

정보통신기술의 급격한 발달로 인한 인터넷 및 스마트폰 등의 보급과 확산은 한 국가에서 발생한 침해사고가 전 세계로 빠르게 전파되어 국가의 중요한 정보들이 해커들의 위협에 쉽게 노출되게 하였다. 금융산업의 경우 사회적 중요성 및 정보통신시스템에 대한 의존도가 심화되면서 침해사고에 대한 위험이 높아지자, 정부는 인터넷 뱅킹, 사이버트레이딩 등을 운영하는 금융회사의 정보통신시스템을 국가적으로 중요한 정보통신기반시설로 지정하고 중점관리하고 있는데 중점관리대상으로 지정된 금융회사들은 정보통신기반보호법에 의거 침해사고를 예방하고 유사시 적절한 대응 및 복구를 하기 위해 정기적으로 정보통신시스템에 대해 취약점 분석 및 평가를 실시하고 보호대책을 마련하여야 한다[22].

### 2.2.5 외주업체(outsourcing company) 보안 관리

Ha et al.(2011)[23]은 기업의 내부 프로젝트나 제품의 생산, 유통, 용역 등을 외부의 제3자에게 위탁처리 하는 것을 아웃소싱(outsourcing)이라 하였다. Kim(2014)[24]은 IT아웃소싱이란 공공 혹은 민간기업내의 정보시스템을 외부전문기업에 위탁하여 서비스를 대신 수행하는 계약형태를 말한다 고 하였다. 이를 종합해 보면 금융회사의 외주업체(아웃소싱업체)는 금융회사를 대신하여 금

금융회사의 정보시스템 운영 및 개발과 관련된 업무를 수행하는 업체다. 과거 금융회사들은 외주업체 직원들에 대한 관리부실로 고객의 금융정보 및 주요 정보들이 외부로 유출되어 회사에 막대한 손해를 입힌 바 있다. 2014년 발생한 카드사 정보유출사고는 외주업체 직원이 카드사의 정보시스템에 접근하여 자신의 USB(Universal Serial Bus)에 고객정보를 복사한 후 약 1억 400만 건의 고객정보를 유출하였다[25]. 이러한 IT 외주용역업체를 통한 정보보호 사고가 빈번하게 발생함에 따라 금융회사는 외주용역업체에 대한 보안을 한층 강화하고 있다. Anat(2013)[26]은 정보보안사고의 부정적 영향은 선진국과 비교해서 우리나라에서 더 장기화 된다고 주장하였다.

### 2.2.6 입/출입 보안관리

금융감독원이 금융회사 IT부분의 안전성을 평가할 때 이용하는 IT경영실태평가 매뉴얼에서는 물리적 통제부문에서 전산실, 통신실 등에 대한 인적 및 물적 자산에 대한 입/출입 보안 관리의 적정성을 점검하고 있다[27]. Chung(2014)[28]은 중요시설에 대해서는 출입구역 및 출입자에 대한 보안등급을 구분하고 구역별 개인별 세분화 된 출입기준을 출입통제시스템과 연계하는 것이 정보자산을 보호하는데 중요하다고 했다. 금융관련 법규 등에 의거 금융회사는 인가받은 사람만이 회사의 전산센터 및 사무실 출입을 할 수 있도록 사람에 대한 입·출입 보안통제를 하고 있는데, 최근 금융회사는 전산센터 및 사무실 주변에 CCTV 설치를 강화하여 선제적으로 정보보호 사고에 대비하거나 사고 발생 시 추적이 가능하도록 하고 있다. 금융회사는 2011년 카드사 정부유출사고를 계기로 디지털장비를 통한 정보유출을 막기 위해 개인용PC, 노트북, 휴대폰, 외장형하드, USB 및 디지털 카메라에 대한 반·출입 통제를 전산센터 한층 강화하고 있다. 금융회사의 전산센터 및 사무실 등에 대한 입/출입 통제는 정보보호 관리체계(ISMS), IT경영실태평가 및 정보보호 관리실태 평가에서 중요한 통제항목이다.

### 2.3 정보보호의식

정보보호의식 수준이란 개인이 정보보호에 대한 관심과 중요성을 인지하여 스스로 정보를 보호하는 행동을 하는 정도라 정의할 수 있다. Bulgurcu et al.(2009)[29]은 정보보안인식은 조직 구성원의 정보보안에 대한 일반적 지식(General Knowledge)과 그들의 조직의 정보보안정책에 대한 인식 정도라 정의하였고, Siponen(2000)[30]은 정보보안인식의 증가는 사용자와 관련된 실수를 최소화 할 것이고 사용자 관점의 보안기술 및 절차의 효율성을 최대화 할 것 이라고 주장하였다. Bulgurcu et al.(2010)[31]의 연구결과에 따르면, 정보보안 인식이 높은 직원 일수록 정보보안의 필요성에 대한 태도가 긍정적이며 정보보안 필요성을 긍정적으로 인식하는 직원 일수록 정보보안 정책을 준수하려는 의지가 강한 것으로 나타났다. Von Solms(2001)[32]은 조직의 정보자원을 보호하기 위해 정보보안 기술구현에 많은 투자를 하더라도 조직구성원이 정보보안에 대한 충분한 인지를 하고 있지 않다면 무용지물이 될 것이라고 했다.

### 2.4 정보보호 자신감

일반적으로 사용되는 자신감(Confidency)이란 용어는 수행을 성공적으로 해낼 수 있는 능력에 대한 개인적 확실성의 정도 또는 믿음이라고 정의된다[33]. 어떠한 일을 해낼 수 있다는 자신감이 높다는 것은 그 일을 성공적으로 수행할 수 있다는 기대가 높다는 것으로, 자신감은 어떠한 성취상황에서 인간의 수행을 높여 좋은 결과를 나올 수 있도록 하는 것이라 말할 수 있다. 이상을 종합해 볼 때 금융회사의 정보보호 자신감이란, 금융회사가 자신들이 운영하고 있는 정보보호체계를 통해 이룩한 정보보호수준에 대해 갖고 있는 믿음 또는 신뢰라 하겠다.

## 3. 연구모형 및 연구가설

### 3.1 연구모형

본 연구는 금융회사의 정보보호활동이 정보보

호의식 및 정보보호자신감에 미치는 영향을 분석하고자 하며, 실증분석 모형은 Fig. 1과 같다.

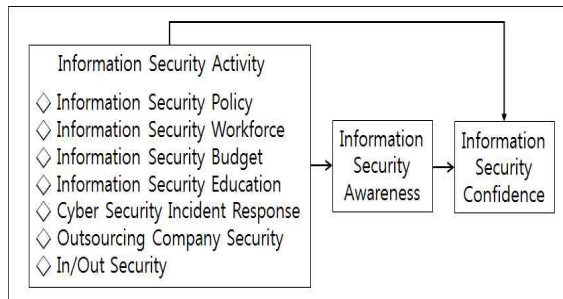


Fig. 1 Research Model

### 3.2 자료수집 및 측정도구

본 연구는 금융회사 정보보호담당자를 대상으로 2017년 5월10일에서 6월30일까지 응답받은 총 280부의 설문지를 SPSS 통계 프로그램(Ver. 21.0)을 이용하여 다음과 같이 분석하였다. 첫째, 연구 대상의 인구통계학적 특성은 빈도분석(frequency analysis)으로 빈도와 백분율을 살펴보았다. 둘째, 측정도구의 타당성과 신뢰성을 검증하기 위해 요인분석과 신뢰성 분석을 실시하였다. 요인 분석은 Kaiser 규칙이 있는 직각회전방식인 Varimax 회전을 이용한 주성분 분석(principal component analysis)을 실시하였고, 신뢰성 분석(reliability analysis)에서는 내적일관성법에 의한 Cronbach's  $\alpha$  계수를 산출하였다. 셋째, 금융회사의 정보보호활동과 정보보호의식, 정보보호자신감의 영향관계는 위계적 회귀분석(hierarchical regression analysis)으로 분석하였고, 정보보호의식의 매개효과는 다중회귀분석(multiple regression analysis)을 실시하여 분석하였다.

### 3.3 연구가설

#### 3.3.1 금융회사의 정보보호활동과 정보보호의식

연구가설 1은 금융회사의 정보보호활동이 직원의 정보보호의식에 영향을 미친다는 가설이다. Im(2006)[34]는 정보보안인식을 사람들이 직무를

수행하는데 있어서 정보보안의 함축된 상태를 잘 알 수 있도록 하는 프로세스로, 정보보안 인식은 정보보안의 중요성 인식뿐만 아니라 보안사고가 발생 시 대응방안과 보고체계 등이 포함된다고 하였다. Choi et al.(2008)[35]은 정보보안실천(보안정책과 절차, 보안 훈련 및 교육, 접근제어, 시스템과 프로그램 업데이트, 보안담당조직)이 정보보안인식의 수준을 높인다는 것을 증명하였다. 이상의 연구들을 살펴보면 조직의 정보보호활동이 조직구성원의 정보보호의식에 영향을 준다는 것을 알 수 있기 때문에 다음과 같은 가설 1을 도출하였다.

가설 1. 금융회사의 정보보호활동은 직원의 정보보호의식에 유의한 영향을 미칠 것이다.

가설 1-1: 금융회사의 정보보호정책은 직원의 정보보호의식에 유의한 영향을 미칠 것이다.

가설 1-2: 금융회사의 정보보호인력은 직원의 정보보호의식에 유의한 영향을 미칠 것이다.

가설 1-3: 금융회사의 정보보호예산은 직원의 정보보호의식에 유의한 영향을 미칠 것이다.

가설 1-4: 금융회사의 정보보호교육은 직원의 정보보호의식에 유의한 영향을 미칠 것이다.

가설 1-5: 금융회사의 침해사고대응은 직원의 정보보호의식에 유의한 영향을 미칠 것이다.

가설 1-6: 금융회사의 외주업체보안은 직원의 정보보호의식에 유의한 영향을 미칠 것이다.

가설 1-7: 금융회사의 입/출입 보안은 직원의 정보보호의식에 유의한 영향을 미칠 것이다.

#### 3.3.2 금융회사의 정보보호의식과 정보보호자신감

연구가설 2는 금융회사 직원의 정보보호의식이 정보보호담당자의 정보보호자신감에 영향을 미친다는 가설이다. Na(2015)[36]는 조직구성원의 보

안의식수준은 조직의 보안수준에 영향을 미치며, 조직의 보안수준을 향상시키기 위해서는 조직에 대한 보안관리 인식, 개인에 대한 보안교육 및 훈련 등이 우선적으로 요구된다고 하였다. 금융회사 직원의 정보보호의식이 높다는 것은 정보보호에 대한 중요성을 알고 개인이 수행해야 할 정보보호행동을 준수하기 때문에 정보보호 사고를 감소시킬 수 있다. 즉 직원이 정보보호에 대한 관심이 높고, 정보보호관련 지식을 많이 습득하고 있으면 정보보호의식 수준이 높아 금융회사 정보보호담당자의 정보보호자신감에 긍정적인 영향을 미치기 때문에 다음과 같은 가설 2를 도출하였다.

가설 2. 금융회사의 정보보호의식은 직원의 정보보호자신감에 유의한 영향을 미칠 것이다.

### 3.3.3 금융회사의 정보보호활동과 정보보호자신감

연구가설 3은 금융회사의 정보보호활동이 금융회사의 정보보호를 담당하고 있는 정보보호 담당자의 자신감에 영향을 준다는 가설이다. Lee et al.(2008)[37]은 정보보안은 조직구성원의 행동에 의하여 많은 부분 영향을 받게 된다고 하였으며 Chen et al.(2008)[38]은 보안위협은 사용자의 지식과 행동의 부주의와 결핍에 그 직접적인 원인이 있다고 주장하며, 오늘날의 정보보안의 성공에 있어 구성원의 보안인지와 행동이 기술적 요소보다 더 중요할 수도 있다고 하였다. Kim et al.(2008)[39]은 기업 내의 정보보안은 보안정책을 잘 준수하고 이에 따른 개인적 특성과 보안의식 수준이 향상되었을 때 안전한 보안효과를 거둘 수 있다고 하였으며, 정보노출 대응조치, 보안지침의 실천, 정기적인 패스워드 변경 등의 보안행동이 보안효과에 영향을 주는 것을 실증적으로 증명하였다. 기업의 정보보호활동이 정보보안효과에 영향을 준다는 기존연구를 바탕으로 금융회사의 정보보호활동이 정보보호담당자의 정보보호 자신감에 영향을 미친다는 연구가설 3을 수립하였다.

가설 3. 금융회사의 정보보호활동은 정보보호 자신감에 유의한 영향을 미칠 것이다.

### 3.3.4 정보보호의식의 매개효과

연구가설 4는 정보보호의식이 정보보호활동과 정보보호자신감 간에 매개효과가 있을 것이라는 가설이다. Kang(2008)[40]은 직원의 보안의식수준이 높아지는 것은 조직 내의 보안정책 권장도 영향을 미친다고 하였으며, 정보시스템 사용자의 보안의식이 정보보안효과에 유의한 영향을 미친다고 실증적으로 분석하였다. 정보보호활동이 보안의식수준을 높이고 보안의식이 정보보안 효과에 영향을 준다는 기존연구를 바탕으로 금융회사의 정보보호활동이 금융회사 정보보호담당자의 보안자신감에 영향을 미치는 영향에 대해 분석하는 과정에서 직원의 정보보호의식의 매개효과를 검증하기 위해 다음과 같이 가설4를 설정하였다.

가설 4. 금융회사의 정보보호활동과 정보보호 자신감 간에 직원의 정보보호의식의 매개효과가 있을 것이다.

가설 4-1: 금융회사의 정보보호정책과 정보보호자신감 간에 직원의 정보보호의식의 매개효과가 있을 것이다.

가설 4-2: 금융회사의 정보보호인력과 정보보호자신감 간에 직원의 정보보호의식의 매개효과가 있을 것이다.

가설 4-3: 금융회사의 정보보호예산과 정보보호자신감 간에 직원의 정보보호의식의 매개효과가 있을 것이다.

가설 4-4: 금융회사의 정보보호교육과 정보보호자신감 간에 직원의 정보보호의식의 매개효과가 있을 것이다.

가설 4-5: 금융회사의 침해사고 대응과 정보보호자신감 간에 직원의 정보보호의식의 매개효과가 있을 것이다.

가설 4-6: 금융회사의 외주업체관리와 정보보호자신감 간에 직원의 정보보호의식의 매개효과가 있을 것이다.

가설 4-7: 금융회사의 입/출입보안과 정보보호자신감 간에 직원의 정보보호의식의 매개효과가 있을 것이다.

### 3.4 연구변수의 조작적 정의 및 설문항목

본 연구의 주요 변수에 대한 조작적 정의는 선행연구를 중심으로 정의하였으며 측정항목은 금융회사의 정보보호활동과 정보보호의식을 본 연구에 적합하게 수정/보완하였다. 모든 변수는 Likert 5점으로 측정하였으며 변수의 조작적 정의는 Table 1과 같다.

## 4. 실증분석 및 결과

### 4.1 표본의 인구통계학적 특성

본 연구의 표본의 특성인 성별, 연령, 회사업종, 근무기간, 전문분야를 빈도 분석한 결과, 성별에서는 남성 250명(89.3%), 여성 30명(10.7%)로 나타났고, 연령은 20대 18명(6.4%), 30대 103명(36.8%), 40대 114명(40.7%), 50대 이상 45명(16.1%)으로서 30대와 40대의 비중이 높았다.

회사업종은 은행 169명(24.6%), 금융투자 63명(22.5%), 보험 46명(16.4%), 비은행 62명(22.2%), 금융관련기관 40명(14.3%)으로 나타났고, 근무기간은 5년 미만 89명(31.8%), 5년~10년 미만 61명(21.8%), 10년~15년 미만 35명(12.5%), 15년~20년 미만 35명(12.5%), 20년 이상 60명(21.4%)으로 분석되었다. 전문분야는 정보보호기획(정보

Table 1 Operational Definition of Variable and Measurement Question

Variable	Operational Definition	Previous Research	Number of Question
Information Security Policy	Compliance with Information Security Polices and Regular Checks and Problem Improvements	- K-ISMS(2016) - IT based Managerial Performance Evaluation(2016) - SUN, H. G(2004)	5
Information Security Workforce	The Existence of Information Security Personnel, Information Security Organization and Officer	- IT based Managerial Performance Evaluation(2016) - Information Security Management Performance(2016)	4
Information Security Budget	The Introduction of Budget and Equipment to Secure the Protection of Organization's Information	- IT based Managerial Performance Evaluation(2016) - Information Security Management Performance(2016)	5
Information Security Education	Regular Conduct of Information Security Training for Employees and Management	- IT based Managerial Performance Evaluation(2016) - Information Security Management Performance(2016) - Gyeon, E. K(2015)	10
Cyber Security Incident Response	Information Security Accident Detection, Response and Recovery and Security Measures Prepared by Analysis of the Cause of the Accident	- IT based Managerial Performance Evaluation(2016) - Information Security Management Performance(2016)	6
Outsourcing Company Security	Preventing the Outflow of Company's Information Assets through Security Management of Outsourcing Companies	- IT based Managerial Performance Evaluation(2016) - Information Security Management Performance(2016)	6
In/Out Security	Control and Management of Computer Center and Office Access for People, PC, Notebook and Mobile Phone	- IT based Managerial Performance Evaluation(2016) - Information Security Management Performance(2016) - K-ISMS(2016)	7
Information Security Awareness	The Grade of Employees and Management being Aware of the Importance of Information Security and their Concerns about Information Security Activities	- Bulgurcu and Cavusogle(2009) - Kim, J. K. and Kang, D. Y(2008)	14
Information Security Confidence	The Confidence of Information Security Professionals who can Protect a Financial Company's Information Assets from Hackers or Internal Information Leaks	- Kim, J. Y(2010) - K-ISMS(2016)	7



보호정책, 예산, 사업) 92명(32.9%), 정보보호시스템운영(방화벽, 서버, 네트워크 보안, 보안장비) 88명(31.4%), 권한관리(내부사용자계정 및 권한관리) 21명(7.5%), 프로그램(개발) 보안 28명(10.0%), 정보보호 점검(정보보호 관제, 사고대응) 24명(8.6%), 개인정보보호 27명(9.6%)으로서 정보보호기획과 정보보호시스템운영의 비중이 비교적 높았다.

따라서 본 연구의 표본은 30대와 40대의 연령대가 가장 많으며 은행과 금융투자, 비은행 등의 금융회사에 근무하면서 정보보호기획과 정보보호시스템운영 등의 전문분야 경력을 지닌 남성이 대부분이라 할 수 있다.

## 4.2 타당성 및 신뢰성 분석

본 연구는 금융회사의 정보보호활동과 정보보호의식, 정보보호자신감의 타당성을 검증하기 위해 요인분석을 실시하였고, 고유치 1.0이상, 요인적재량 0.5이상을 기준으로 하여 요인을 추출하였다. 신뢰성 분석에서는 내적일관성법에 의한 Cronbach's  $\alpha$ 계수를 산출하였는데, 이 값이 0.6 이상일 경우 신뢰할 수 있다고 판단하였다[41].

### 4.2.1 독립변수의 타당성 및 신뢰성 분석

본 연구의 독립변수인 정보보호활동의 타당성

Table 2 Characteristics of Research Subjects

	Factor	Frequency(person)	Percentage(%)
Sex	male	250	89.3
	female	30	10.7
Age	twenties	18	6.4
	thirties	103	36.8
	forties	114	40.7
	fifties	45	16.1
Company Industry	bank	69	24.6
	financial investment	63	22.5
	insurance	46	16.4
	non banking	62	22.2
	financial related institution	40	14.3
Working Period	under 5 years	89	31.8
	from 5 years under 10 years	61	21.8
	from 10 years under 15 years	35	12.5
	from 15 years under 20 years	35	12.5
	over 20 years	60	21.4
Specialty	security planing	92	32.9
	security system operation	88	31.4
	authority management	21	7.5
	program security	28	10.0
	security check	24	8.6
	personal information security	27	9.6
SUM		280	100.0

과 신뢰성 검증을 위해 요인분석과 신뢰성분석을 실시한 결과는 Table 3과 같다. 정보보호활동은 총 43개 문항으로 구성하였는데, 요인분석 과정에서 요인적재량이 0.5이하인 정보보호인력 1개 문항을 제거하였으며, 최종 요인분석에서 고유치는 1.0이상인 7개의 요인이 도출되었다. 각 요인을 구성하는 문항의 유사성을 근거로 하여 요인 1은 ‘정보보호교육’, 요인 2는 ‘입/출입보안’, 요인 3은 ‘외주업체보안’, 요인 4는 ‘침해사고대응’, 요인 5는 ‘정보보호예산’, 요인 6은 ‘정보보호정책’, 요

Table 3 The Analysis Results of Validity and Reliability on Information Security Activity

Factor	Items	Communi-ty	Factor loading						
			1	2	3	4	5	6	7
Information Security Education	information security education 1	.731	.800	.023	.161	.158	.124	.122	.094
	information security education 2	.695	.784	.165	.115	.116	.148	.068	-.009
	information security education 3	.750	.779	.025	.159	.128	.168	.071	.260
	information security education 4	.665	.721	.196	.136	.187	.151	.169	.049
	information security education 6	.713	.707	.029	.220	.158	.180	.212	.248
	information security education 8	.711	.691	.036	.246	.153	.203	.157	.287
	information security education 5	.673	.658	.201	.074	.359	.247	.063	.027
	information security education 7	.583	.642	.202	.037	.152	.134	.187	.229
	information security education 10	.572	.560	.110	.215	.058	.294	.328	.054
	information security education 9	.481	.503	.268	.062	.072	.283	.255	.048
In/Out Security	in/out security 7	.797	.110	.834	.187	.200	.033	.123	.048
	in/out security 5	.802	.183	.828	-.003	.099	.118	-.049	.226
	in/out security 6	.717	.110	.824	.154	.147	.078	.238	-.018
	in/out security 4	.799	.128	.784	.017	.125	.129	-.074	.217
	in/out security 3	.729	.134	.656	.209	.126	.105	.438	-.135
	in/out security 2	.740	.123	.644	.244	.125	.141	.450	-.108
Outsourcing Security Company	in/out security 1	.550	.069	.570	.081	.101	.235	.383	-.030
	outsourcing company security 1	.701	.117	.163	.770	.214	.088	.069	-.098
	outsourcing company security 2	.650	.109	-.043	.760	.073	.153	.122	.122
	outsourcing company security 3	.726	.184	.094	.747	.198	.194	.074	.208
	outsourcing company security 5	.781	.217	.155	.721	.239	.023	.178	.317
	outsourcing company security 4	.694	.182	.236	.710	.177	.117	.219	.091
Cyber Security Incident Response	outsourcing company security 6	.719	.251	.259	.638	.201	.060	.140	.344
	cyber security incident response 2	.853	.212	.222	.228	.764	.264	.214	.085
	cyber security incident response 3	.818	.272	.212	.217	.751	.135	.257	.062
	cyber security incident response 4	.731	.218	.119	.239	.743	.137	.031	.200
	cyber security incident response 1	.799	.253	.329	.199	.701	.209	.197	.113
	cyber security incident response 5	.776	.225	.113	.334	.611	.284	.336	.184
Information Security Budget	cyber security incident response 6	.674	.212	.156	.223	.591	.280	.327	.143
	information security budget 2	.807	.211	.208	.186	.149	.793	.126	.135
	information security budget 3	.816	.317	.151	.168	.146	.779	.154	.116
	information security budget 4	.728	.293	.087	.005	.215	.755	.107	.083
	information security budget 1	.755	.223	.061	.206	.158	.750	.196	.181
Information Security Policy	information security budget 5	.751	.260	.198	.120	.268	.712	.201	.107
	information security policy 3	.713	.224	.303	.198	.208	.179	.668	.101
	information security policy 1	.731	.323	.269	.105	.206	.224	.654	.149
	information security policy 5	.625	.289	.270	.054	.256	.227	.616	.144
Information Security Workforce	information security policy 2	.672	.262	.102	.295	.256	.151	.599	.241
	information security policy 4	.677	.239	.023	.262	.211	.149	.588	.294
	information security workforce 3	.754	.252	.050	.266	.069	.137	.157	.755
	information security workforce 2	.764	.251	.178	.102	.196	.196	.204	.735
	information security workforce 1	.643	.223	.024	.292	.228	.208	.099	.634
Eigenvalue			6.298	4.917	4.429	4.107	4.081	3.616	2.617
Variance %			14.995	11.708	10.545	9.779	9.717	8.609	6.231
Cronbach's α			.928	.909	.891	.934	.921	.886	.843

인 7은 ‘정보보호인력’이라 하였다. 이들 요인의 총 분산은 71.584%였으며, 신뢰성 분석에 따른 Cronbach’s α계수가 정보보호교육 .928, 입/출입 보안 .909, 외주업체보안 .891, 침해사고대응 .934, 정보보호예산 .921, 정보보호정책 .886, 정보보호 인력 .843으로서 신뢰성이 높게 나타났다.

**4.2.2 매개변수와 종속변수의 타당성 및 신뢰성 분석**

본 연구의 매개변수와 종속변수에 대한 요인분석과 신뢰성분석을 실시한 결과는 Table 4와 같다. 요인분석 과정에서 모든 문항의 요인적재량이 0.5이상으로 나타났으며, 요인 1은 ‘정보보호 자신감’에 관한 7문항, 요인 2는 ‘정보보호의식’에 관한 8문항으로 구성되었다. 이들 요인의 총 분산은 70.397%였으며, 신뢰성 분석에 따른 Cronbach’s α계수는 정보보호자신감 .941, 정보 보호의식 .927 로서 문항의 신뢰성이 높게 나타났다.

고, 그 결과는 Table 5와 같다. 측정변수 간에는 어느 정도 이상의 상관성이 있었고, 그 방향성은 양(+)의 상관관계가 있는 것으로 나타났다.

**4.4 가설검증**

본 연구는 금융회사의 정보보호활동과 정보보호의식 및 정보보호자신감 간의 영향관계를 분석하기 위해 인구통계학적 특성을 통제변인으로 하는 위계적 회귀분석을 실시하였고, 정보보호의식의 매개효과는 다중회귀분석을 실시하였다. 인구통계학적 특성과 같은 통제변수는 회귀분석 결과의 타당성을 높이기 위해 투입하며, 다수의 독립변수의 투입으로 인한 다중공선성(multicollinearity)의 문제는 분산 팽창 계수(VIF, variance inflation factor)를 통해 파악하였다. 이 VIF 값이 10 이상으로 나타나면 높은 다중공선성으로 인한 문제가 발생하기 때문에 주의할 필요가 있다.

Table 4 The Analysis Results of Validity and Reliability on Information Security Awareness

Factor	Items	Community	Factor loading	
			1	2
Information Security Confidence	information security confidence 6	.821	.825	.375
	information security confidence 3	.818	.819	.385
	information security confidence 2	.810	.810	.391
	information security confidence 7	.737	.770	.380
	information security confidence 1	.739	.765	.393
	information security confidence 5	.708	.757	.367
	information security confidence 4	.582	.710	.277
Information Security Awareness	Information security awareness 4	.727	.284	.804
	Information security awareness 2	.737	.338	.789
	Information security awareness 1	.742	.362	.782
	Information security awareness 5	.738	.376	.773
	Information security awareness 8	.708	.443	.716
	Information security awareness 6	.572	.309	.690
	Information security awareness 3	.656	.456	.669
	Information security awareness 7	.466	.305	.610
Eigenvalue			5.323	5.137
Variance %			35.485	34.912
Cronbach’s α			.941	.927

**4.3 상관관계분석**

본 연구는 측정변수 간 상관관계를 분석하였

**4.4.1 정보보호활동이 정보보호의식에 미치는 영향**

Table 5 Correlation Analysis

Factor	1	2	3	4	5	6	7	8	9
1. Information Security Education	1								
2. In/Out Security	.307***	1							
3. Outsourcing Company Security	.505***	.404***	1						
4. Cyber Security Incident Response	.621***	.362***	.615***	1					
5. Information Security Budget	.628***	.191**	.440***	.611***	1				
6. Information Security Policy	.651***	.363***	.556***	.689***	.591***	1			
7. Information Security Workforce	.560***	.243***	.525***	.537***	.497***	.540***	1		
8. Information Security Awareness	.636***	.319***	.501***	.657***	.583***	.711***	.424***	1	
9. Information Security Confidence	.653***	.312***	.484***	.741***	.646***	.660***	.491***	.779***	1

\*\* $p < .01$ , \*\*\* $p < .001$

금융회사의 정보보호활동이 정보보호의식에 미치는 영향을 분석하기 위해 인구통계학적 특성을 통제변수로 하고 정보보호활동을 독립변수로 하는 위계적 회귀분석을 실시하였다. VIF 값의 경우 1 단계에서는 1.209-3.167, 2단계에서는 1.300-3.331로서 10이하로 나타나 다중공선성의 문제는 발생하지 않았다. 금융회사의 정보보호활동이 정보보호의식에 미치는 영향을 분석한 결과는 Table 6과 같이 나타났다.

통제변수인 인구통계학적 특성을 투입한 1단계 회귀모형은  $F=2.047$ ,  $p < .05$ 에서 유의하였고, 전체 설명력이 8.4%의 결과를 보였다. 인구통계학적 특성에서는 성별( $\beta = -.170$ ,  $t = -2.635$ ,  $p < .01$ )이 정보보호의식에 부(-)의 영향을 미치고 있었고, 회사업종 3( $\beta = .185$ ,  $t = 2.320$ ,  $p < .05$ )이 정보보호의식에 정(+)의 영향을 미치고 있어 남성이면서 보험업종의 경우 직원들의 정보보호의식이 높다고 할 수 있다.

정보보호활동을 추가로 투입한 2단계 회귀모형은  $F=30.659$ ,  $p < .001$ 에서 유의하였고, 전체 설명력이 69.1%로서 1단계보다 60.7% 상승하였다. 인구통계학적 특성에서는 회사업종 1( $\beta = -.107$ ,  $t = -2.023$ ,  $p < .05$ )이 정보보호의식에 부(-)의 영향을 미치고 있어 은행일 경우 다른 업종에 비해 직원들의 정보보호의식이 낮다고 할 수 있다. 정보보호의식에 대해서는 정보보호정책( $\beta = .263$ ,  $t = 4.522$ ,  $p < .001$ )과 정보보호교육( $\beta = .218$ ,  $t = 4.017$ ,  $p < .001$ ), 침해사고대응( $\beta = .134$ ,  $t = 2.335$ ,  $p < .05$ ), 입/출입 보안( $\beta = .342$ ,  $t = 6.684$ ,  $p < .001$ )이 정보보

호의식에 정(+)의 영향을 미치고 있었고, 입/출입 보안의 상대적 영향력이 가장 높게 나타났으며, 정보보호인력과 정보보호예산, 외주업체보안은 영향을 미치지 않았다. 이는 정보보호정책, 정보보호교육, 침해사고대응, 입/출입보안이 정보보호인력, 정보보호예산 및 외주업체보안 보다 직원의 정보보호의식에 더 중요하게 영향을 미치기 때문이다.

따라서 금융회사의 입/출입 보안, 정보보호정책 및 교육, 침해사고대응력이 높을수록 정보보호의식이 높아진다고 할 수 있다. 이와 같이 금융회사 정보보호정책과 정보보호교육, 침해사고대응, 입/출입보안이 정보보호의식에 정(+)의 영향을 미침으로써 금융회사의 정보보호활동이 정보보호의식에 유의한 영향을 미칠 것으로 설정한 연구가설 1은 일부 채택되었다.

#### 4.4.2 정보보호의식이 정보보호자신감에 미치는 영향

금융회사의 정보보호의식이 정보보호자신감에 미치는 영향을 분석하기 위해 인구통계학적 특성을 통제변수로 하고 정보보호의식을 독립변수로 하는 위계적 회귀분석을 실시하였다. 그 결과는 Table 7과 같으며, VIF 값의 경우 1단계에서는 1.209-3.167, 2단계에서는 1.241-3.175로서 10 이하로 나타나 다중공선성의 문제는 발생하지 않았다. 인구통계학적 특성을 투입한 1단계 회귀모형은  $F=2.097$ ,  $p < .05$ 에서 유의하였고, 전체 설명력

Table 6 Effects of Information Security Activity on Employee's Information Security Awareness

Dependent variable Independent variable		Phase 1			Phase 2		
		$\beta$	t	P	$\beta$	t	P
Population Statistical Characteristics	sex <sup>a)</sup>	-.170	-2.635**	.009	-.058	-1.483	.139
	age	-.034	-.380	.705	.082	1.518	.130
	company industry <sup>b)</sup>						
	company industry1	.044	.511	.610	-.107	-2.023*	.044
	company industry2	-.038	-.454	.650	-.074	-1.377	.170
	company industry3	.185	2.320*	.021	-.082	-1.596	.112
	company industry4	.080	.952	.342	-.074	-1.423	.156
	employment period	.079	.906	.366	-.026	-.496	.620
	specialty <sup>c)</sup>						
	specialty1	.119	1.148	.252	.048	.789	.431
	specialty2	.086	.829	.408	.075	1.187	.236
	specialty3	.024	.318	.751	-.022	-.479	.632
	specialty4	.031	.386	.700	.053	1.092	.276
	specialty5	.038	.484	.629	.066	1.392	.165
Information Security Activity	information security policy				.263	4.522***	.000
	information security workforce				-.027	-.562	.575
	information security budget				.092	1.790	.075
	information security education				.218	4.017***	.000
	cyber security incident response				.134	2.335*	.020
	outsourcing company security				-.009	-.192	.848
	in/out security				.342	6.684***	.000
F		2.047*			30.659***		
R <sup>2</sup>		.084			.691		
$\Delta R^2$					.607		

\*  $p < .05$ , \*\*  $p < .01$ , \*\*\*  $p < .001$

<sup>a)</sup>sex(M=0, F=1), <sup>b)</sup>company industry(financial related institution=0), company industry1(bank=1), company industry2(financial investment=1), company industry3(insurance=1), company industry4(nonbanking=1), <sup>c)</sup>specialty(personal information security=0), specialty1(security planning=1), specialty2(security system operation=1), specialty3(authority management=1), specialty4(program security=1), specialty5(security check=1)

은 8.6%였다. 인구통계학적 특성에서는 회사업종 3( $\beta=.256$ ,  $t=3.214$ ,  $p<.01$ )과 근무기간( $\beta=.174$ ,  $t=2.002$ ,  $p<.05$ )이 정보보호자신감에 정(+)의 영향을 미치고 있어 보험업종이면서 근무기간이 오래될수록 정보보호에 대한 자신감이 높아진다고 할 수 있다. 정보보호의식을 추가로 투입한 2단계 회귀모형은  $F=35.824$ ,  $p<.001$ 에서 유의하였고, 전체 설명력이 63.6%로서 1단계보다 55.0% 상승하였다. 인구통계학적 특성에서는 회사업종 3( $\beta=.113$ ,  $t=2.053$ ,  $p<.05$ )과 근무기간( $\beta=.113$ ,  $t=2.053$ ,  $p<.05$ )이 정보보호자신감에 정(+)의 영향을 미치고 있었고, 정보보호의식( $\beta=.775$ ,  $t=20.067$ ,  $p<.001$ )

이 정보보호자신감에 정(+)의 영향을 미치고 있었다. 따라서 금융회사의 정보보호의식이 정보보호자신감에 유의한 영향을 미칠 것으로 설정한 연구가설 2는 채택되었다.

#### 4.4.3 정보보호활동이 정보보호자신감에 미치는 영향

금융회사의 정보보호활동이 정보보호자신감에 미치는 영향을 분석하기 위해 인구통계학적 특성을 통제변수로 하고 정보보호활동을 독립변수로 하는 위계적 회귀분석을 실시하였다. 그 결과는

Table 7 Effects of Information Security Awareness on Information Security Confidence

Dependent variable / Independent variable		Phase 1			Phase 2		
		$\beta$	t	P	$\beta$	t	P
Population Statistical Characteristics	sex <sup>a)</sup>	-.095	-1.474	.142	.037	.892	.373
	age	-.114	-1.269	.205	-.088	-1.542	.124
	company industry <sup>b)</sup>						
	company industry1	.096	1.114	.266	.062	1.135	.258
	company industry2	.042	.503	.615	.072	1.354	.177
	company industry3	.256	3.214**	.001	.113	2.214*	.028
	company industry4	.067	.801	.424	.005	.098	.922
	employment period	.174	2.002*	.046	.113	2.053*	.041
	specialty <sup>c)</sup>						
	specialty1	.090	.870	.385	-.002	-.033	.974
	specialty2	.039	.374	.709	-.028	-.426	.670
	specialty3	.082	1.063	.289	.063	1.292	.197
	specialty4	-.051	-.631	.529	-.076	-1.472	.142
	specialty5	.014	.180	.857	-.015	-.310	.757
	Information Security Awareness					.775	20.067***
F		2.097*			35.824***		
R <sup>2</sup>		.086			.636		
$\Delta R^2$					.550		

\*  $p < .05$ , \*\*  $p < .01$ , \*\*\*  $p < .001$

<sup>a)</sup>sex(M=0, F=1), <sup>b)</sup>company industry(financial related institution=0), company industry1(bank=1), company industry2(financial investment=1), company industry3(insurance=1), company industry4(nonbanking=1), <sup>c)</sup>specialty(personal information security=0), specialty1(security planning=1), specialty2(security system operation=1), specialty3(authority management=1), specialty4(program security=1), specialty5(security check=1)

Table 8 과 같으며, VIF 값의 경우 1단계에서는 1.209-3.167, 2단계에서는 1.300-3.331로서 10이하로 나타나 다중공선성의 문제는 발생하지 않았다. 인구통계학적 특성을 투입한 1단계 회귀모형은  $F=2.097$ ,  $p < .05$ 에서 유의하였고, 전체 설명력은 8.6%였다. 인구통계학적 특성에서는 회사업종3( $\beta=.256$ ,  $t=3.214$ ,  $p < .01$ )과 근무기간( $\beta=.174$ ,  $t=2.002$ ,  $p < .05$ )이 정보보호자신감에 정(+)의 영향을 미치고 있어 보험업종이면서 근무기간이 오래될수록 정보보호에 대한 자신감이 높아진다고 할 수 있다.

정보보호활동을 추가로 투입한 2단계 회귀모형은  $F=31.253$ ,  $p < .001$ 에서 유의하였고, 전체 설명력이 69.5%로서 1단계보다 60.9% 상승하였다. 정보보호자신감에 대해서는 정보보호정책과 정보보호인력, 외주업체보안은 영향을 미치지 않았으나, 정보보호예산( $\beta=.184$ ,  $t=3.604$ ,  $p < .01$ )과 정보

보호교육( $\beta=.201$ ,  $t=3.734$ ,  $p < .001$ ), 침해사고대응( $\beta=.360$ ,  $t=6.313$ ,  $p < .001$ ), 입/출입보안( $\beta=.258$ ,  $t=5.087$ ,  $p < .001$ )은 정보보호자신감에 정(+)의 영향을 미치고 있었다. 정보보호자신감에 대한 금융회사의 정보보호예산과 정보보호교육이 높을수록 정보보호에 대한 자신감이 높아진다고 할 수 있다.

요약하면, 금융회사의 정보보호예산과 정보보호교육, 침해사고대응, 입/출입보안이 정보보호자신감에 유의한 영향을 미치는 반면 정보보호정책 및 인력, 외주업체보안은 정보보호자신감에 유의한 영향을 미치지 않는 것으로 나타났다. 이는 정보보호예산과 정보보호교육, 침해사고대응, 입/출입보안이 정보보호정책, 정보보호인력 및 외주업체보안 보다 직원의 정보보호자신감에 더 중요하게 영향을 미치기 때문이다. 따라서 금융회사의 정보보호활동이 정보보호자신감에 유의한 영

Table 8 Effects of Information Security Activity on Information Security Confidence

Dependent variable		Phase 1			Phase 2		
		$\beta$	t	P	$\beta$	t	P
Population Statistical Characteristics	sex <sup>a)</sup>	-.095	-1.474	.142	.025	.642	.521
	age	-.114	-1.269	.205	.006	.108	.914
	company industry <sup>b)</sup>						
	company industry1	.096	1.114	.266	-.054	-1.027	.306
	company industry2	.042	.503	.615	-.024	-.452	.652
	company industry3	.256	3.214**	.001	-.008	-.150	.881
	company industry4	.067	.801	.424	-.050	-.972	.332
	employment period	.174	2.002*	.046	.044	.845	.399
	specialty <sup>c)</sup>						
	specialty1	.090	.870	.385	.026	.432	.666
	specialty2	.039	.374	.709	.071	1.132	.259
	specialty3	.082	1.063	.289	.046	.989	.323
	specialty4	-.051	-.631	.529	.007	.143	.886
	specialty5	.014	.180	.857	.073	1.547	.123
	Information Security Activity	information security policy				.053	.915
information security workforce					.025	.507	.612
information security budget					.184	3.604***	.000
information security education					.201	3.734***	.000
cyber security incident response					.360	6.313***	.000
outsourcing company security					-.063	-1.308	.192
in/out security					.258	5.087***	.000
F			2.097*		31.253***		
R <sup>2</sup>			.086		.695		
$\Delta R^2$					.609		

\*  $p < .05$ , \*\*  $p < .01$ , \*\*\*  $p < .001$

<sup>a)</sup>sex(M=0, F=1), <sup>b)</sup>company industry(financial related institution=0), company industry1(bank=1), company industry2(financial investment=1), company industry3(insurance=1), company industry4(nonbanking=1), <sup>c)</sup>specialty(personal information security=0), specialty1(security planning=1), specialty2(security system operation=1), specialty3(authority management=1), specialty4(program security=1), specialty5(security check=1)

향을 미칠 것으로 설정한 연구가설 3은 일부 채택되었다.

#### 4.4.4 정보보호활동과 정보보호자신감 간 정보보호의식의 매개효과

금융회사의 정보보호활동과 정보보호자신감 간 정보보호의식의 매개효과를 분석하기 위해 다중회귀분석을 실시하였고, 그 결과는 Table 9 과 같다. 첫째, 독립변수인 정보보호활동이 매개변수인 정보보호의식에 미치는 영향을 분석하였고 (Model I), 둘째, 독립변수인 정보보호활동이 종속변수인 정보보호자신감에 미치는 영향을 분석

하였으며(Model II), 셋째, 독립변수인 정보보호활동과 매개변수인 정보보호의식이 정보보호자신감에 미치는 영향을 분석하였다(Model III). 또한 매개변수를 포함한 회귀모형에서 종속변수에 대한 독립변수의 영향력이 감소하면 부분매개효과, 유의하지 않으면 완전매개효과라 판단하였으며, VIF 값의 경우 Model I 과 Model II 에서는 1.300-3.331, Model III 에서는 1.311-3.349로서 10 이하로 나타나 다중공선성의 문제는 발생하지 않았다.

금융회사의 정보보호활동과 정보보호자신감 간 정보보호의식의 매개효과를 분석한 결과에서는 정보보호정책, 정보보호인력, 외주업체보안은 매

개효과가 없었는데 이는 동 정보보호활동이 정보 보호의식을 통해 정보보호자신감에 영향을 주지 않기 때문이다. 정보보호예산과 정보보호교육, 침해사고대응, 입/출입보안에서 정보보호의식의 매개효과가 분석되었다. 정보보호예산이 정보보호자신감에 미치는 영향이  $\beta=.184$ 에서  $\beta=.148$ 로 감소하였고, 정보보호교육이 정보보호자신감에 미치는 영향이  $\beta=.201$ 에서  $\beta=.116$ 으로 감소하였으며, 침해사고대응이 정보보호자신감에 미치는 영향이  $\beta=.360$ 에서  $\beta=.308$ 로 감소하였다. 입/출입보안이 정보보호자신감에 미치는 영향은  $\beta=.258$ 에서  $\beta=.125$ 로 감소하였으며, 정보보호의식은  $\beta$

$=.389$ 에서 정보보호자신감에 영향을 미치는 것으로 나타났다. 다시 말하면, 정보보호예산, 정보보호교육, 침해사고대응 및 입/출입보안과 정보보호자신감 간에는 정보보호의식의 부분매개효과가 있다고 할 수 있다. 따라서 정보보호활동과 정보보호자신감 간 정보보호의식의 매개효과를 분석하고자 하는 연구가설 4는 일부 채택되었다.

### 5. 결론 및 시사점

본 연구에서는 금융회사의 정보보호활동이 정

Table 9 Mediation Effects thru Information Security Awareness between Information Security Activity and Information Security Confidence

Independent variable		Model I			Model II			Model III		
		$\beta$	t	P	$\beta$	t	P	$\beta$	t	P
Population Statistical Characteristics	sex <sup>a)</sup>	-.058	-1.483	.139	.025	.642	.521	.048	1.321	.188
	age	.082	1.518	.130	.006	.108	.914	-.026	-.525	.600
	company industry <sup>b)</sup>									
	company industry1	-.107	-2.023*	.044	-.054	-1.027	.306	-.012	-.253	.801
	company industry2	-.074	-1.377	.170	-.024	-.452	.652	.005	.094	.925
	company industry3	-.082	-1.596	.112	-.008	-.150	.881	.024	.512	.609
	company industry4	-.074	-1.423	.156	-.050	-.972	.332	-.021	-.448	.655
	employment period	-.026	-.496	.620	.044	.845	.399	.054	1.126	.261
	specialty <sup>c)</sup>									
	specialty1	.048	.789	.431	.026	.432	.666	.007	.134	.894
	specialty2	.075	1.187	.236	.071	1.132	.259	.042	.721	.471
specialty3	-.022	-.479	.632	.046	.989	.323	.054	1.276	.203	
specialty4	.053	1.092	.276	.007	.143	.886	-.014	-.308	.759	
specialty5	.066	1.392	.165	.073	1.547	.123	.047	1.083	.280	
Information Security Activity	information security policy	.263	4.522***	.000	.053	.915	.361	-.049	-.893	.373
	information security workforce	-.027	-.562	.575	.025	.507	.612	.035	.789	.431
	information security budget	.092	1.790	.075	.184	3.604***	.000	.148	3.129**	.002
	information security education	.218	4.017***	.000	.201	3.734***	.000	.116	2.274*	.024
	cyber security incident response	.134	2.335*	.020	.360	6.313***	.000	.308	5.796***	.000
	outsourcing company security	-.009	-.192	.848	-.063	-1.308	.192	-.059	-1.337	.182
	in/out security	.342	6.684***	.000	.258	5.087***	.000	.125	2.476*	.014
Information Security Awareness							.389	6.847***	.000	
F		30.659***			31.253***			32.274***		
R <sup>2</sup>		.691			.695			.742		
Adj.R <sup>2</sup>		.669			.673			.722		

\* $p<.05$ , \*\* $p<.01$ , \*\*\* $p<.001$

a)sex(M=0, F=1), b)company industry(financial related institution=0), company industry1(bank=1), company industry2(financial investment=1), company industry3(insurance=1), company industry4(nonbanking=1), c)specialty(personal information security=0), specialty1(security planning=1), specialty2(security system operation=1), specialty3(authority management=1), specialty4(program security=1), specialty5(security check=1)



보보호의식 및 정보보호자신감에 미치는 영향에 대해 분석하였으며, 그 결과를 요약하면 다음과 같다. 첫째, 금융회사의 정보보호활동이 정보보호의식에 미치는 영향을 검증한 결과, 정보보호정책, 정보보호교육, 침해사고대응, 입/출입 보안이 정보보호의식에 정(+의 영향을 미치고 있었다. 둘째, 정보보호의식은 정보보호자신감에 정(+의 영향을 미치고 있었으며, 셋째, 정보보호활동이 정보보호자신감에 미치는 영향을 검증한 결과, 정보보호예산, 정보보호교육, 침해사고대응, 입/출입보안이 정보보호자신감에 정(+의 영향을 미치는 것으로 나타났다. 넷째, 금융회사의 정보보호활동과 정보보호자신감 간 정보보호의식의 매개효과를 분석한 결과, 정보보호예산, 정보보호교육, 침해사고대응, 입/출입보안과 정보보호자신감 간 정보보호의식의 매개효과가 나타났다.

본 연구의 결과를 바탕으로 다음과 같은 이론적 시사점을 제시할 수 있다. 금융회사가 정보보호교육, 침해사고 대응 및 입/출입보안에 중점을 두고 정보보호활동을 하면 정보보호담당자의 회사에 대한 정보보호자신감 및 직원들의 정보보호의식수준이 높아진다는 것을 확인할 수 있었다. 또한 직원의 정보보호 의식수준이 높아지면 정보보호에 대한 자신감도 함께 높아진다는 것을 확인할 수 있었다. 다만, 정보보호정책 및 정보보호인력이 보안성과에 영향을 미친다는 기존 연구와 달리, 본 연구에서는 정보보호정책, 정보보호인력 및 외주업체보안은 정보보호담당자의 자신감에 영향을 미치지 않았으며, 정보보호예산, 정보보호인력 및 외주업체보안의 경우 직원의 정보보호의식에 영향을 미치지 않는다는 것을 확인할 수 있었다. 정보보호교육, 침해사고대응 및 입/출입보안과 같은 정보보호활동이 금융회사 정보보호담당자의 자신감에 큰 영향을 미치는 이유는 동 활동을 평상시 꾸준히 하고 있어, 직접적으로 활동의 결과를 확인할 수 있기 때문이라 추정된다.

또한 다음과 같은 실무적 시사점을 제시할 수 있다. 금융회사는 정보보호담당자의 자신감을 향상시키기 위해 정보보호예산을 확보하는 것이 중요하다. 금융회사가 충분한 정보보호예산을 확보하기 위해서는 금융회사 내부로부터 정보보호의 중요성과 필요성에 대한 인식이 지속적으로 확산

되어야 하는데, 이는 직원 및 경영진을 대상으로 꾸준한 정보보호교육을 통해 정보보호의식 수준을 제고함으로써 가능하다. 즉, 정보보호예산 확보를 통해 정보보호관련 하드웨어 및 소프트웨어를 도입하고, 임직원을 대상으로 정보보호교육을 강화하여, 정보보호 의식수준을 제고시킴으로써 회사의 정보보호수준과 더불어 정보보호담당자의 정보보호자신감을 높일 수 있다. 현실적으로 가장 중요한 것은 정보보호예산이다. 현재 국내 금융회사의 정보보호예산은 전체 정보화예산의 5%에 불과하나, 선진국인 미국은 정보화예산대비 정보보호예산을 1/5로 확대하여 정보보호분야에 공격적으로 투자하고 있다[42]. 이러한 점 등을 고려해 볼 때 국내 금융회사의 정보보호예산 확대가 불가피하다고 판단된다.

본 연구의 한계점과 향후 연구과제에 대해서 살펴보면 다음과 같다. 본 연구는 첫째, 금융회사의 정보보호활동 중 침해사고예방, 접근통제, 암호화 등과 같은 기술적 정보보호활동을 포함하지 않았으며, 둘째, 경영진에 대한 정보보호 의식수준을 측정하지 않았다. 향후 연구에서는 금융회사의 정보활동중 기술적인 분야와 경영진에 대한 정보보호 의식수준을 포함하여 연구함으로써, 금융회사의 정보보호활동이 회사의 정보보호자신감에 미치는 영향을 더욱 세분화하여 연구를 진행할 필요가 있다.

## References

- [1] Bank of Korea, "2016 Finance Information Enforcement Situation," 2017.
- [2] Hong, K. H., "A Study on the Effect of Information Security Controls and Processes on the Performance Security", Doctor's Dissertation, Dept of Management Information Systems Graduate School, Kookmin University, pp. 64-75, 2003.
- [3] Park, S. S., "A Study on the Effort and Status of the Enterprise Information Asset Protection Activity", Master's Dissertation, IT Management Strategy Graduate School,

- Yonsei University, pp. 50-57, 2008.
- [4] Baek, M. J., "A Study on the Effect of Information Ethics on the Performance of Information Security in Organization", Doctor's Dissertation, Department of Business Administration, Graduate School Dankook University, pp. 37-128, 2010.
- [5] Son, T. H., "The Effect of Corporate Information Security Activities on the Performance of Information Security and Information Management", Doctor's dissertation, Department of Industrial and Management Engineering Graduate School, Myongji University, pp. 6-7, 2015.
- [6] Pipkin, D. L., "Information Security", Prentice Hall PTR, 2000.
- [7] Kim, S. C., "The Effect of Broadcasting Company's Information Security Activity on the Compliance Attitude and Intention of Employees - Focusing on the Information Security Management System -", Doctor's Dissertation, The Graduate School of Public Policy and Information Technology, Seoul National University of Science and Technology Companies, 2017.
- [8] Park, J. K. and Kim, I. J., "A Study for Influencing Factors of Organizational Performance : The Perspective of the Mediating Effect of Information Security Maturity Level", The Journal of Information Systems, Vol. 23, No. 3, pp. 99-125, 2014.
- [9] National Intelligence Service, "Framework Act on National Information Article 3", 2017.
- [10] Korea Internet Security Agency, "Information Security Management System Certification Guideline", 2013.
- [11] National Information Graduate School, Industrial Security Practical Affairs, 2006.
- [12] Sun, H. G., "Impacts of Information Security Policies and Organizations on the Information Security Performance in Korean Enterprises", Doctor's dissertation, Dept. of Management Systems Graduate School, Kookmin University, 2004.
- [13] Lee, C. H., "A Study on the Influential Factors for the Security Policy - Focusing on the Recognition of Corporate Security Manager", Doctor's Dissertation, Department of Public Administration Graduate School, Kyungwon University, 2010.
- [14] The Financial Supervisory Service, "Regulation on Supervision of Electronic Financial Transactions", Article 8.
- [15] Bang, H. G., "A Study of Security Personal Managements and Adequacy by State-Owned Company", June. 2011.
- [16] Song, K. J., "Rish Management of Customer Information Asset in Financial Institute", Deloitte Anjin Review 2014, Vol. 18, No. 1, pp. 39-48, 2014.
- [17] Jeon, J. H., "A Study on the Costs Factors of an Being Additional Budget by the Security System", Korean Institute of Communications and Information Sciences Vol. 36, No. 12, pp. 1481-1490, 2011.
- [18] Jeong, C. Y., "Recent Financial Supervisory Authorities' Policy and Financial Company Response to Financial Information Security Accidents", Credit Union Research, Vol. 63, No. 2, pp. 45-82, 2015.
- [19] Gyeon, E. K., Lee, H. S. and Chae, S. M., "An Empirical Study of Relationship Between Information Security Education and Information Security Incidents", Korea Academic Society of Business Administration, 2016 Spring Congress, The Graduate School Ewha University, 2016.
- [20] 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, pp.79-98, 2009.

- [21] Kim, J. W. and Kim, Y. G., "A Research on Information Education Outsourcing at Public Organizations", *E-Business Research*, Vol. 11, No. 1, pp. 265-282, 2010.
- [22] National Intelligence Service, "2016 a White Paper on National Information Security", 2017.
- [23] Ha, G. R., Yoon, S. H., and Choi, S. B., "Critical Factors for Outsourcing Partner Selection of Manufacturing Firms: An AHP Based Analysis", *The Journal of Management Education*, Vol. 26, No. 2, pp. 489-515, 2011.
- [24] Kim, G. M., "The Impact of IT Governance and IT Service Management Process Maturity on IT Outsourcing Success", Master's Dissertation, Graduate School of Information and Telecommunication, KonKuk University, 2014.
- [25] Jang, Y. S., Jeon, S. and Jeon, D. H., "Cases Analysis and Implications of Personal Information Leaking in E-Business", *E-Trade Review*, Vol. 12, No. 1, pp. 1-27, 2014.
- [26] Anat Hovav. and Han, J. Y., "The Impact of Security Breach Announcements on the Stock Value of Companies in South Korea", *The Journal of Internet Electronic Commerce Research*, Vol. 13, No. 3, pp. 43-67, 2013.
- [27] Financial Supervisory Service, "IT Business Practice Evaluation Manual", 2016.
- [28] Chung, T. H., "Improvement of Physical Security System Operation", *Journal of the Korea Society of Disaster Information*, Vol. 10, No. 2, pp. 282-286, 2014.
- [29] Bulgurcu, B. H. and Cavusogle, H., "Roles of Information Security Awareness and Perceived Fairness in Information Security Policy Compliance", *AMCIS 2009 Proceedings*, 2009.
- [30] Siponen, M, A., "Conceptual Foundation for Organizational Information Security Awareness", *Information Management and Computer Security*, Vol. 8, No. 1, pp. 31-41, 2000.
- [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, pp. 523-548, 2010.
- [32] Von Solms, B., "Information Security - A Multidimensional Discipline", *Computers and Security*, Vol. 20, No. 6, pp. 504-508, 2001.
- [33] Kim, J. Y., "Effect of Sport Confidence and Competitive State Anxiety on Performance of Bowling Player", Master's Dissertation, Graduate School of Education Kookmin University, pp. 13, 2010.
- [34] Im, C. H., " Effective Information Security Awareness Improvement Policy", *Korea Institute of Information Security & Cryptology*, Vol. 16, No. 2, pp. 30-36, 2006.
- [35] Choi, N., Kim, D. and Whitmore, A., "Knowing is doing", *Information Management & Computer Security* Vol. 16, No 5, pp. 484-501, 2008.
- [36] Na, Y. S., "A Study of the Organization associated with Security Awareness and Security Level in Smart Business Environment", Master's Whitmore, Department of Business Information Graduate School, Sangmyong University, pp. 53-54, 2015.
- [37] Lee, S. J. and Lee, M. J., "An Exploratory Study on the Information Security Culture Indicator", *Information Policy*, Vol. 15, No.3, pp. 100-119, 2008.
- [38] Chen, C., Medlin, B., and Shaw, R., "A Cross-Cultural Investigation of Situational Information Security Awareness Programs",

Information Management & Computer Security, Vol. 16, No. 4, pp. 360-376, 2008.

- [39] Kim, J. K. and Kang, D, Y., "The Effects of Security Policies, Security Awareness and Individual Characteristics on Password Security Effectiveness", Korea Institute of Information Security & Cryptology, pp. 123-133, 2008.
- [40] Kang, D, Y., "The Influence of Password Selection on the Security Effectiveness", Master's Dissertation, Department of Business Administration Graduate School, Pusan National University, pp. 72-73, 2010.
- [41] Kang, J. H. and Ha, K. S., "A Study of Effect of Self-Leadership by College Student on Recognition of Opportunity on Establishment of Company and of Establishing Company: Created on Mediated Effect of Entrepreneurship", The Korea Society of Business Venturing, Vol. 10, No. 4, pp. 1-12, 2015.
- [42] The SEOUL ECONOMIC DAILY, "'Hacker Frequenter Target', Domestic Financial Institutions' Security Investment is Only 10 % of their IT Budget", 2017.



**소 현 철** (Soh Hyeon-Chul)

- 정회원
- 서강대학교 전자계산학과 이공학사
- 일리노이주립대학교 경영대학원 경영학과 석사
- 호서대학교 벤처경영학과 박사과정
- 현재 금융감독원 대전지원 과건실장
- 관심분야 : 금융보안, 경영정보, 금융보안정책, 개인정보보호



**김 종 근** (Kim Jong Keun)

- 정회원
- 서강대학교 경제학과 학사
- 서강대학교 경제학과 석사
- 서강대학교 경제학과 박사
- 호서대학교 벤처대학원 벤처경영학과 교수
- 대외경제정책연구원 연구위원
- 공정거래위원회 평가위원