경영정보학연구
제5권 1호
1995 년 6 월

정보시스템통제 및 감사가 컴퓨터범죄의 인지된 위험에 미치는 영향: 금융기관을 중심으로

한 인 구[1], 윤 종 호[2]

The Impact of Information System Control and Audit on the Perceived Risk of the Computer Crime in Case of Financial Institutions

The information system control includes organizational structure, control mechanism, and management tools which contribute to accomplish the goals of information system: asset safeguarding, data integrity, effectiveness, and efficiency. Information system audit is the process to evaluate whether the information system accomplishs the goals. Information system auditors examine the reliability of information system control and suggest recommendations to improve the information system control. Both information system control and information system audit activities contribute to prevent and detect the computer crime for the organization.

This paper proposes a causal model of information system control/audit and the perceived risk of computer crime, and tests the model using a survey on 38 financial institutions in Korea. Statistical results show that information system control and audit significantly reduce the computer crime risk perceived by the user group. The general control has a stronger impact than the application control. In addition, it turns out that the greater the deviation between the importance and the actual level of information system control is, the higher the perceived risk of computer crime is.

1) 한국과학기술원 서울분원 경영정보공학과

2) 제일투자신탁 운용부

Ⅰ. 서 론

현대 기업경영에 있어서 컴퓨터활용의 중요성은 날로 증대되고 있다. 초기의 컴퓨터활용은 자료처리에 중점이 있었으며 자료처리를 주로 수행하는 시스템을 전산자료처리시스템(EDPS:Electronic data processing system)이라고 부른다. 컴퓨터의 활용이 자료처리의 수준을 넘어서 경영관리에 필요한 정보를 생산, 전달하여 준다는 관점에서 경영정보시스템의 개념으로 발전하였다. 경영정보시스템을 광의로 보면 기업의 모든 정보를 다루는 종합정보시스템 또는 단순히 정보시스템이라고 할 수 있다. 경영정보시스템의 이론과 기법이 발전하면서 의사결정의 지원에 중점을 두는 의사결정지원시스템, 정보기술을 경쟁력제고의 차원에서 활용하는 전략정보시스템 등 새로운 개념이 출현하면서 정보시스템분야는 빠른 속도로 발전하고 있다.

정보시스템이 지향하는 목표로는 자산의 보호, 자료완전성(data integrity)의 유지, 조직목표의 효과적 달성, 전산자원의 효율적 사용 등을 들 수 있다. 정보시스템이 이러한 목표를 달성하는 것을 촉진하기 위한 기업내의 모든 조직계획과 조정방법 및 수단을 정보시스템통제라고 한다. 정보시스템의 수준이 고도화되면서 정보시스템이 소기의 목표를 달성할 수 있도록 기업환경에 적합한 정보시스템통제를 설계하고 개선해 나가는 것이 주요한 과제라고 할 수 있다.

금융기관의 전산화는 신속, 정확한 업무처리와 광범위한 정보의 효율적 관리를 가능하게 함으로써 고객에 대한 서비스 향상은 물론 금융기관의 경영합리화에 기여하게 된다. 최근에 광주은행이 다운사이징을 통하여 은행의 전산업무를 획기적으로 개선한 것이 그 예라고 할 수 있다. 금융기관들은 정보시스템의 발전을 경쟁력강화의 관건으로 보고 정보시스템에 대한 투자를 늘려가고 있는 추세이다. 금융기관의 전산화가 고도화됨에 따라 정보시스템의 효과적인 운영을 위해서는 새로운 방식의 내부통제제도가 요구되고 있으나 전문인력의 부족, 전산시스템 및 상황변화에 관한 인식부족 등으로 금융기관의 변화하는 전산환경에 대한 대응이 미흡한 실정이다. 이러한 대응력의 결핍은 컴퓨터를 이용한 범죄 및 사고발생의 요인이 될 수 있다.

우리나라 금융기관에서 발생하는 전산관련 사고가 공식적으로 보고된 사례는 미국 등 선진국에 비하여는 상대적으로 많지 않으며 단순하고 초보적인 사고가 대부분이지만 앞으로 기업-은행간 및 가정-은행간 전산망 구축 등 금융기관의 전산시스템이 확산됨에 따라 미국, 일본 등 선진국에서 보는 바와 같이 고도의 기술을 이용하는 대형사고의 발생가능성도 늘어날 것으로 보인다. 컴퓨터범죄를 방지하기 위하여는 건전한 정보시스템통제를 구축하고 체계적인 정보시스템감사를 실시하여야 할 것이다. 본 논문은 금융기관 전산시스템의 역기능을 제어하기 위한 취지에서 정보시스템통제 및 감사와 컴퓨터범죄와의 관계를 분석하고자 한다. 연구결과는 컴퓨터 범죄예방을 위한 정보

시스템통제의 개선방향을 설정하는데 도움을 줄 수 있을 것이다.

금융기관을 연구대상으로 한 이유는 첫째, 최근 대검찰청의 통계(노연후, 1992)에 따르면 지난 70년부터 92년까지 20여년동안 발생한 컴퓨터 범죄중 은행이 전체의 75.5%를 차지했으며 증권회사 등을 포함한 금융권에서의 범죄발생율이 전체의 80%를 차지하고 있기 때문이다. 둘째, 금융기관의 특성상 컴퓨터의 활용도 및 의존도가 높으므로 금융기관의 정보시스템통제의 중요성이 매우 크기 때문이다.

연구방법으로는 금융기관을 대상으로 설문조사를 통한 실증분석을 실시하였다. 설문지는 세가지를 사용하였다. 설문지(1)은 금융기관의 정보시스템통제를 평가하기 위한 것으로서 전산실에서 작성하도록 하였으며 설문지(2)와 설문지(3)은 컴퓨터 범죄위험을 측정하기 위한 것으로서 감사실과 영업부에서 작성하도록 하였다.

본 논문의 전개는 다음과 같다. 2장에서는 컴퓨터범죄의 현황 및 정보시스템통제 및 감사의 개념을 살펴보고 3장에서는 연구모형을 도출하고 가설을 설정하였다. 4장에서는 설문조사결과를 분석하고 5장에서는 결론을 제시하였다.

Ⅱ. 컴퓨터범죄 및 정보시스템통제의 개념 및 체계

2.1 컴퓨터범죄의 개념 및 현황

컴퓨터 범죄의 개념은 아직 정확히 설정되어 있지 못하다. 컴퓨터범죄의 정의에 대해서는 광의설과 협의설, 최협의설 등 세 가지로 나누어 볼 수 있다(노연후, 1992). 광의설은 컴퓨터를 행위의 수단으로 하거나 목적으로 하여 부정행위를 저질러 처벌대상이 된 모든 행위, 즉 컴퓨터와 관련된 모든 범죄(Computer Related Crime)를 컴퓨터 범죄라고 보는 주로 미국학자들의 견해이다(Parker, 1976).

협의설을 주장하는 학자들은 컴퓨터범죄를 전자적으로 자료를 처리하는 장치와 관련이 있는 고의적인 재산적인 침해 행위로 정의한다. 이 학설은 주로 일본학자들이 주장하고 있다. 최근 일본에서는 협의의 컴퓨터 범죄내에서의 현금지급기에 사용하는 현금인출카드와 각종 신용카드를 이용한 범죄는 따로 분리시키고, 나머지 부분을 컴퓨터 범죄로 보는 최협의의 해석을 내리고 있는 경향이 나타나고 있다. 본 논문에서 다루는 금융기관의 컴퓨터 범죄는 주로 현금과 관계된 고의적, 재산적 침해에 해당하기 때문에 협의설의 입장에서 접근하고자 한다.

컴퓨터 범죄는 1960년대 초반에 미국에서 최초로 발생하여 1970년에 접어들면서부터 미국을 중심으로 각국에서 컴퓨터 범죄 발생이 급격히 증가하여 점차 사회문제화되기 시작했다. 컴퓨터 선진국인 미국이나 일본등에서 발생한 주요사례를 보면 은행의 프로그램개발부장과 컴퓨터 업무부장이 공모하여 자기들이 개설한 구좌에 타인의 구좌에서 거액의 돈을 이체시킨 경우가 있었는가 하면 예금자가 알아차

리지 못할 정도의 소액의 예금을 오랜 기간에 걸쳐 자기 구좌에 불입하게 하는 사건도 일어났고, 대량의 정보가 기록되어 있는 자기테이프의 데이터나 프로그램을 삭제하여 이를 복구하는데 1천만 달러이상이 소요되는 경우도 있었다. 또한 주요 정치인을 태운 항공기가 공항에 착륙하려고 할 때 관재관이 컴퓨터에 부정데이타를 입력하여 항공기의 공중충돌을 일으킬 뻔한 경우가 있었으며, 병원의 진단기록이 입력된 데이타를 함부로 개조하여 치료업무를 마비하게 하는 사건이 발생하였고, 회사직원이 통신회선으로부터 온라인 시스템의 데이타를 도청하여 그것을 해독, 현금카드를 위조행사함으로써 현금자동지급기로부터 수회에 걸쳐 타인의 구좌에서 거액의 현금을 인출해 갔었다. 회사가 10년동안 20억원이라는 막대한 비용을 투자하여 개발한 소프트웨어를 그 회사의 프로그래머가 순식간에 복사하여 시판하는 바람에 회사를 궁지에 몰아넣는 등 예상하기 어려운 새로운 컴퓨터범죄가 발생하여 사회적으로 큰 충격을 주고 있다(은행감독원, 1992).

최근에는 컴퓨터범죄의 발생건수 및 규모가 급격히 증가함과 동시에 각종의 컴퓨터 범죄가 전세계적으로 확산되는 추세를 보이고 있다. 이에 따라 컴퓨터 범죄 방지를 위한 대책수립이 각국의 주요한 과제가 되고 있다. 선진국에서는 이러한 컴퓨터 범죄를 예방하고 사전에 통제하려는 노력을 지난 1970년대부터 진행시켜 왔다. 우리나라에서는 1960년대에 컴퓨터가 도입된 후 급속히 확대보급되어 왔다. 우리나라 최초의 컴퓨터범죄는 1973년 10월 KIST 중앙전산소 프로그래머가 반포AID차관아파트 입주 추첨과 관련하여 프로그램을 조작, 청탁받았던 9가구분을 당첨시킨것이었다. 1993년에는 한 유학지망생이 청와대를 사칭하여 금융기관의 전산망에 침투하여 거액의 돈을 휴면계좌로 부터 인출하려는 시도가 있었다. 금년도에는 재벌기업의 국제금융팀에 근무하는 엘리트 직원이 전산시스템을 조작하여 수입물품 결제대금 15억원을 횡령한 사건이 발생했다.

대검찰청통계에 의하면 지난 72년부터 92년 10월 23일까지 20여년동안 발생한 컴퓨터 범죄는 총 51건으로, 그 가운데 은행이 38건으로 전체의 74.5%를 차지했으며, 일반기업체 4건, 정부기관 4건, 그리고 증권, 보험, 기타가 각 1건으로 나타나 금융권에서의 범죄 발생율이 전체의 80% 가까이 차지하고 있는 것으로 집계된다(노연후, 1992). 실제 발생은 이보다 몇십배 또는 몇백배에 달할 것으로 추정된다. 93년이후에는 국내에서 컴퓨터범죄의 건수 및 금액이 급증하는 추세는 보이고 있다. 보안수준이 높은 미국에서도 공식적으로 집계된 컴퓨터범죄가 90년에는 1백30건, 92년에는 8백건, 93년에는 1천3백건, 94년에는 2천3백건으로 급격한 증가추세를 보이고 있다(전자신문, 1995). 컴퓨터 범죄의 발생율 및 사고규모는 컴퓨터의 발전과 더불어 증가추세를 보이고 있으나 우리나라에서는 아직까지 컴퓨터조직, 운영 및 보안에 관한 제반지침이 완비되지 못하였으며 컴퓨터 범죄를 처벌할 수 있는 법률의 정비도 이루어지지 않고 있는 실정이어서

이에 대한 연구가 시급하다고 하겠다.

2.2 컴퓨터범죄의 유형, 동기 및 특성

컴퓨터범죄는 컴퓨터의 운영과 관련하여 입력상의 범죄, 프로그램상의 범죄, 출력상의 범죄의 세가지로 나누어 볼 수 있다. 장소별로 구분하여 보면 내부 및 외부로 나누어 볼 수 있다. 내부로는 조직내의 전산부서와 사용자부서 등이 있다. 금융기관의 업무특성과 연계하여 보면 컴퓨터범죄를 전산부서, 영업점, 외부인 사고의 세가지로 나누기도 한다. 컴퓨터운영운영상의 범죄이외에도 현금카드 및 신용카드를 이용한 범죄도 있다.

공식적으로 집계된 컴퓨터범죄의 유형별 분포를 보면 컴퓨터운영상의 부정이 44건인데 이중 입력부정이 38건, 프로그램 및 콘솔상의 부정이 65건이었으며 현금지급기 부정 4건 및 신용카드 부정 3건등으로 나타났다.

컴퓨터 범죄는 범행동기, 범죄행위자, 범죄행위 등이 일반범죄와 다른 특징을 지니고 있다. 컴퓨터를 다룰 수 있는 정도의 사람이면 대부분 고학력자들이고 두뇌도 명석한 편에 속하며 빈곤을 해결하기 위한 것보다는 향락을 추구하는 데 필요한 재원을 얻기 위한 범행이 많다. 또한 개인 또는 회사에 대한 불만 또는 원한관계에 의한 범행이 많은 편이다. 직장에서 업무적으로 또는 인간관계나 인사문제로 불평과 원한을 갖게 되는 경우에 컴퓨터를 파괴하거나 시스템 프로그램 또는 데이터화일을 지워버리는 범죄를 저지르게 되는 경우가 흔히 발생하고 있다.

정치적인 동기도 주요한 부분을 차지하는데 정치적 자료가 수록된 컴퓨터를 고장나게 하거나, 경쟁자의 정치적 자료를 지워버려 혼란을 가져오게 하거나, 경쟁자의 정치적 자료를 부정입수하기도 한다. 또한 국제적 관계에서도 범행이 많은데 적대관계에 있는 국가에 대하여 국가기밀을 빼가거나 주요 국가기밀과 자료가 들어 있는 컴퓨터를 파괴하는 경우도 발생하고 있다. 최근에는 냉전체제가 종식되고 국가간의 경제적 경쟁이 격심해지자 각종 산업정보와 기술정보를 부정으로 빼내거나 주요 자료를 지워버리는 행위가 발생할 가능성이 높아졌다고 할 수 있다.

앞에서 살펴본 범행동기와는 달리, 자기 자신이나 제 3자의 재산적 이익이 없이 오직 자신의 지적 모험심을 충족시키는 동기로 범행하는 경우가 많다. 소위 핵커(Hacker)들은 남의 접근을 못하게 장치한 보안장치, 즉 비밀번호나 패스워드 등을 파괴하거나 교묘히 피해서 들어가는 것을 취미로 하는 경우이다.

컴퓨터 범죄는 컴퓨터에 대한 특수 기술이나 컴퓨터와 근접이 가능해야 하는 특징때문에 범죄자의 대부분은 컴퓨터기술이 있는 전문가나 컴퓨터기기와 접근이 가능한 내부인이 대부분이라는 것이다. 일반 범죄가 외부인이 많은데 비해 내부인이 많은 것은 컴퓨터에 접근할 수 있는 기회가 외부인보다 많다는 데 있으며 컴퓨터시스템을 모르고는 범행할 수 없기 때문이다.

컴퓨터 범죄를 저지르는 사람은 대부분 젊은

연령층이 많은 것으로 나타나고 있다. 그 이유는 첫째 사회에 대한 두려움이 적고 둘째 모험심이 많으며, 세째 향락을 추구하는 경향이 높고, 네째 컴퓨터 프로그램의 개발자는 연령층이 젊은 사람이 많기 때문으로 분석되고 있다. 우리나라에서 공식 집계된 컴퓨터범죄의 57%가 20대에 의하여 발생하고 있으며 30대를 포함하면 전체범죄의 약 90%를 점하고 있다.

컴퓨터 범죄자는 대부분이 범행에 대한 죄의식이 거의 없다. 이는 일반 범죄가 사람을 상대하여 범행하거나 또는 직접 재물을 상대하여 범행하는데 비해 컴퓨터 범죄는 기계를 상대로 범행하기 때문에 죄의식을 느끼지 못하는 것으로 분석되고 있다.

컴퓨터 범죄는 범죄의 발각이 어려운 것이 대부분이다. 이는 모든 자료의 처리과정이나 처리된 자료의 기억이 전자적으로 되어 사ㅂ람의 눈으로 볼 수 없기 때문이다. 또한 컴퓨터 범죄는 범죄의 발각이 되더라도 증거를 잡기가 매우 어려운 경우가 많다. 모든 자료가 전자적으로 처리되고 기억되기 때문에 범행자가 부정 프로그램으로 범행한 후 그 프로그램을 지워버릴 경우 그 내용을 찾아 입증하기는 어렵다. 특히 단순한 오류와 고의성을 구분하기가 더욱 어렵다.

2.3 정보시스템통제 및 감사의 의의

정보시스템통제는 일반통제(general control)와 응용통제(application control)로 나누어 볼 수 있다. 일반통제는 전산시스템에 대한 전반적인 통제로서 조직과 경영통제, 정보시스템 개발 및 유지통제, 컴퓨터시스템의 운영통제, 안전통제, 통신통제 등으로 구분할 수 있다. 응용통제는 거래처리의 완전성(integrity)을 확인하기 위하여 각 응용시스템(application system)별로 적용되는 통제로서 입력통제, 처리통제, 출력통제 등으로 분류할 수 있다(Weber, 1988; EDPAA, 1992). 조직 및 경영통제는 조직을 경영하는 데에 있어서 권한의 위임, 업무의 분담 및 승인절차가 적절하게 이루어 지도록 하는 것이다. 승인은 권한의 위임과 밀접한 관계를 가지고 있다. 권한의 위임은 일반적으로 거래가 시작하기 전에 발생하고 승인은 거래중이거나 거래가 완성된 후에 하게 된다. 컴퓨터 시스템에 있어서는 수작업 때문에 적은수의 인원에게 자료처리 활동영역이 집중되어 있기 때문에 적당한 조직계획과 업무분담이 필수적이다.

정보시스템 개발, 획득, 유지통제는 SDLC(system development life cycle)에 입각하여 프로젝트 개시, 실행가능성조사, 설계단계, 개발과 실행, 운영과 유지, 사후이행의 검토 등으로 나누어 볼 수 있다(EDPAA, 1992). 운영통제는 컴퓨터 기계나 자료, 프로그램의 사용 전반에 걸친 통제이다.

보안통제란 현재 자료의 처리에 영향을 미쳐 자료의 완전성을 저해하거 데이타시스템의 가용성에 영향을 끼치는 파괴나 손실에 대하여 컴퓨터 시설, 프로그램, 데이타 등을 보호하고 처리장비의 복구를 꾀하기 위한 통제로서 컴퓨터시설의 보호, 프로그램이나 자료의 보호, 재

해나 손상시 계속적 운영확보 등 세가지로 나누어 볼 수 있다. 통신시스템에 대한 위협에는 통신시스템에 잠입하여 통신내용을 도청하는 것과 같은 수동적 공격과 통신시스템에 침투하여 내용을 변조하는 적극적 위협의 두가지로 나누어 볼 수 있다. 통신시스템의 보호를 위하여 암호화 기법, 응답회신기법 등이 사용된다 (Weber,1988).

입력통제는 원시자료의 작성과정에서 입력자료의 타당성을 확인하고 입력시 부정 및 오류를 방지하기 위한 것이다. 프로그램통제는 프로그램에 대한 권한없는 변경을 예방, 통제하기 위한 수단이다. 출력통제에서는 출력의 분배전에 관련자료의 상호검증등을 통하여 출력내용을 검토하여 출력의 완전성을 확보하는 것이다.

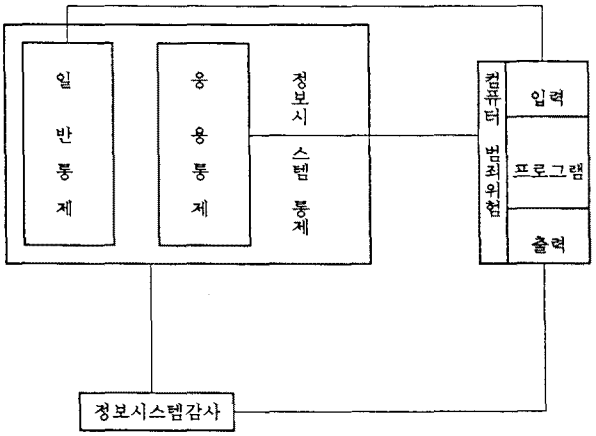
정보시스템감사는 정보시스템이 자산보호, 자료의 완전성, 효과성 및 효율성과 같은 소기의 목표를 달성하고 있는가를 평가하기 위하여 증거를 수집하고 평가하는 과정으로 정의할 수 있다. 정보시스템감사의 영역은 응용시스템개발감사, 응용시스템통제감사, 보안감사, 유지보수감사, 시스템취득감사 등 다양한 분야에 다양한 목적으로 활용될 수 있다. 정보시스템감사의 절차에서는 정보시스템의 일반통제 및 응용통제를의 신뢰성를 평가하고 이를 토대로 준거검사 및 실증검사를 실시하는 과정을 거치게 되며 감사결과 발견된 정보시스템통제의 취약점에 대한 개선안을 제시하여 정보시스템통제를 개선시켜나가게 된다. 정보시스템감사활동은 정보시스템통제기능과 보완적으로 작용하여 컴퓨터범죄를 예방하고 적발하는 기능을 수행하게 된다.

Ⅲ. 연구모형 및 설계

3.1 연구모형 및 가설설정

컴퓨터범죄와 관련된 기존의 연구로는 컴퓨터범죄에 따른 손실에 대한 설문조사(Ernst and Winney, 1988; ABA, 1984; AICPA, 1984; Kusserow, 1983; Wong 1985), 범죄에 대한 경찰보고나 매체로부터 기록자료의 분석(Parker, 1976; 1981) 등 현황분석적인 연구가 대부분이었으며 인과관계에 관한 연구는 드문 편이다. 인관관계를 분석한 연구로는 Straub(1990)가 있는데 법률이론을 바탕으로 정보시스템보안에 대한 투자하고자 하는 의사결정이 컴퓨터범죄를 더 효과적으로 통제할 수 있는지에 관한 인과관계를 연구하였다.

본 논문은 정보시스템감사론의 토대에서 정보시스템통제의 강도와 인지된 컴퓨터 범죄위험과의 인과관계를 분석하는 최초의 시도이다. 정보시스템통제는 정보시스템이 자산보호, 자료완전성, 효과성 및 효율성을 달성하는 것을 지원하는 조직계획, 조정방법 및 수단이라고 할 수 있다. 컴퓨터범죄는 컴퓨터와 관련하여 자산적 피해를 가지고 오는 행위이며 이러한 과정에서 자료의 조작이 수반되는 경우가 많다. 이러한 관점에서 정보시스템통제가 강하면 컴퓨터범죄위험은 감소된다는 인과성이 존재한다. 예를 들면 정보시스템통제는 전산시스템



〈그림 2〉 정보시스템통제와 컴퓨터범죄의 인과관계 연구모형

의 목표중의 하나인 재산보호를 위해 비인가자 또는 권한을 받지 않은 자의 정보자산에 대한 접근을 제한함으로써 컴퓨터 범죄 예방에 기여할 수 있다.

정보시스템감사는 정보시스템이 자산보호, 자료완전성, 효과성 및 효율성을 달성하고 있는지를 평가하기 위하여 증거를 수집하고 평가하는 과정이라고 할 수 있다. 정보시스템감사는 정보시스템통제를 개선해 나가는 역할을 수행하므로 정보시스템감사활동이 잘 수행된다면 정보시스템통제도 강할 것이다. 또한 컴퓨터범죄를 예방하고 발생된 범죄를 발견하는 것이 정보시스템감사의 한 기능이라고 할 수 있다. 정보시스템통제와 컴퓨터범죄위험과의 인과성을 검증하는 것이 본 논문의 주목적이며 부차적으로 정보시스템감사와 컴퓨터범죄와의 인과성도 분석할 것이다.

본 논문의 연구모형에서는 일반적인 분류대로 정보시스템통제를 일반통제와 응용통제로 나누었다. 일반통제는 경영통제, 정보시스템개발, 획득 및 유지통제, 정보시스템운영통제, 보안통제 등 4가지로 나누었으며 응용통제는 입력통제, 처리통제, 출력통제로 분류하였다. 정보시스템감사의 실시정도를 파악하기 위하여 감사체제, 조직구성, 감사횟수를 변수로 사용하였다 . 컴퓨터범죄의 행태는 입력부정, 처리부정, 출력부정으로 나누었다.

정보시스템통제 및 정보시스템감사가 컴퓨터범죄에 미치는 영향을 분석하기 위하여 다음과 같은 대립가설을 설정하였다.

〈가설 1〉: 일반통제의 실시정도가 클수록 컴퓨터범죄의 인지된 위험도는 낮아진다.

〈가설 2〉: 응용통제의 실시정도가 클수록 컴퓨터범죄의 인지된 위험도는 낮아진다.

〈가설 3〉: 정보시스템감사의 실시정도가 클수록 컴퓨터범죄의 인지된 위험도는 낮아진다.

정보시스템통제를 효율적으로 운영하기 위

하여는 중요성의 원칙에 입각하여 중요한 통제 요소에 비중을 두어야 할 것이다. 통제의 중요성과 실시정도가 일치할수록 정보시스템통제가 효율적으로 운영된다고 볼 수 있으며 괴리가 클수록 정보시스템에 대한 위험이 커질 것이다. 통제의 중요성과 실시정도의 괴리와 컴퓨터범죄위험과의 관계를 검증하기 위하여 다음과 같은 가설을 설정하였다.

〈가설 4〉: 정보시스템통제의 중요도와 실시정도가 일치할 수록 컴퓨터범죄의 인지된 위험도는 낮아진다.

3.2 변수의 조작화 및 설문설계

독립변수는 일반통제(GC: general control)로서 경영통제(MC: management control), 정보시스템 개발, 획득 및 유지통제(DAMC: development, acquisition, and maintenance control of information system), 운영통제(OC: operational control), 보안통제(SC: security control)와 응용통제(AC: application control), 정보시스템감사(ISA: information system audit) 등 6개이다.

금융기관 정보시스템통제의 실시정도를 조사하기 위해 EDPAA(1992)가 제시한 통제목표중 일반통제와 응용통제의 146개 항목중에서 은행감독원의 전산센터 내부통제설문항목을 참조하여 금융기관에 적합한 45개의 항목을 선정하여 통제유형별로 분류하였다. 이 45개 설문 문항을 5개 금융기관 전산센터의 책임자에게 먼저 예비조사한 결과 용어가 너무 학술적이어서 어려우며 문항수가 많다는 반응을 받았다. 따라서 문구를 이해하기 쉽도록 수정하고 각 통제 유형별로 대표적인 것만 골라 24개의 설문 항목으로 줄였서 전산실용 설문지(1)을 구성하였다. 컴퓨터범죄위험을 측정하기 위한 감사실용 설문지(2)와 영업부용 설문지(3)은 은행감독원이 분석한 유형별 대표적인 컴퓨터 범죄사례를 참조하여 항목을 작성하였다.

정보시스템통제 및 감사를 요소별로 변수화하기 위하여 다음과 같은 항목을 이용하여 설문서(1)을 구성하였다.

(1) MC: 1) 직무의 분리
2) 권한과 책임의 명확화 및 성과평가의 적절성

(2) DAMC: 3) 프로그램의 변경 및 검사의 분리
4) 프로그램의 문서화
5) 데이타파일의 사용통제
6) 프로그램변경의 주기적 보고

(3) OC: 7) 콘솔로그의 비정상적인 작업검토
8) 일별 시스템가동시간 파악 및 예외적인 가동사유 검토
9) 시스템 가동시 2인이상의 오퍼레이터 근무
10) 데이타화일과 프로그램 라이브러리의 암호등에 의한 보호
11) 암호의 주기적 변경
12) 현용 및 back-up 테이프와 디스크에 대한 정기적 재고조사

(4) SC: 13) back-up장소의 입출입 기록관리
14) 자료처리요원이 아닌 자의 전산실 입장통제
15) 재해복구계획
(5) AC: 16) 입력자료의 승인절차
17) 잘못된 입력자료의 수정을 위한 절차확립
18) 출력자료의 사용자부서의 확인절차
(6) ISA: 19) 감사부서의 권고안의 수용성
20) 정보시스템감사기준의 규정화
21) 정보시스템감사 전담기구의 설치
22) 정보시스템감사 전담요원의 수
23) 정보시스템 정기감사의 빈도
24) 정보시스템의 부정기감사의 빈도

설문지에서의 측정은 1점에서 5점까지의 리커트척도에 의하였다. 정보시스템통제에 관한 설문지(1)은 전산실용으로서 각 금융기관의 전산담당자가 작성하였다. 먼저 각 회사의 정보시스템통제의 현황을 표시하도록 하였으며 다음으로 컴퓨터범죄의 방지를 위하여 각 통제항목의 중요성을 기입하도록 하였다.

컴퓨터범죄의 위험도를 측정하기 위하여 감사실용 설문지(2)에서는 최근 1년간 실제로 발생한 컴퓨터범죄를 조사하였으며 영업부용 설문지(3)에서는 정보시스템 이용자가 인지하고 있는 컴퓨터범죄위험을 조사하였다. 감사실용 설문서(2)의 항목은 다음과 같다.

(1) 입력부정:
1) 영업점에서의 무자원입금 및 출금 횟수
2) 고객의 승인없이 영업점단말기를 통한 인출 횟수
3) 고객의 저축금 입금을 직원의 계좌로 입금시킨 횟수
(2) 프로그램부정:
4) 전산요원이 프로그램을 조작하여 자기구좌에 허위입금한 횟수
5) 전산요원이 프로그램을 조작하여 고객구좌에서 허위이체한 횟수
(3) 콘솔부정:
6) 전산요원이 콘솔을 조작하여 결제가 지연되거나 중단된 횟수
7) 전산요원이 콘솔을 조작하여 자기구좌에 이자를 발생시킨 회수
(4) 출력부정:
8) 고객의 구좌에 관한 허위적 출력 횟수
(5) 기타:
9) 직책별 사고건수
10) 부서별 발생건수 및 금액
11) 사고발생시 공모인 관계

영업부용 설문서(3)의 항목은 다음과 같다.

(1) 입력부정:
1) 영업점에서 무자원 입금의 위험
2) 고객의 승인없이 인출시킬 위험
(2) 프로그램상의 부정:
3) 프로그램의 조작 위험
(3) 출력부정:

4) 고객의 구좌에 관한 허위적 출력위험

Ⅳ. 설문조사 및 결과분석

4.1 표본의 선정

설문의 대상으로는 금융기관에서 가장 큰 비중을 차지하며 업무의 특성상 컴퓨터범죄에 가장 민감할 것으로 보이는 은행 및 증권회사로 하였다. 서울에 본사를 둔 은행 및 증권회사는 각각 22개와 33개인데 이중 각각 20개를 무작위로 추출하였다. 표본중에서 두개의 은행의 설문자료협조가 불충분하여 제외되어서 분석에 포함된 금융기관은 은행 18개와 증권회사 20개등 총 38개이다. 전산실용 설문지(1)은 연구자가 각 기관을 방문하여 전산실의 중견관리자와 면담하여 정보시스템통제에 관한 설문조사를 실시하였다. 감사실용 설문지(2)는 실제 금융기관의 컴퓨터범죄 발생현황을 조사하기 위하여 각 기관을 방문하여 감사실의 경력있는 담당자에게 설문지를 작성하도록 하였다. 전산실용인 설문지(1)과 감사실용인 설문지(2)는 각 기관에 관한 설문이므로 기관별로 한부씩을 작성하였다. 영업부용 설문지(3)은 사용자들이 금융기관의 컴퓨터범죄위험을 어떻게 인지하는가를 측정하기 위한 것으로 표본회사의 사용자(영업부 직원)를 상대로 1개 회사 3명씩 대리급이상 또는 경력있는 사원으로 설문조사를 실시하여 114장의 설문지를 회수하였다.

4.2 결과분석

설문지(2)는 각 금융기관의 감사실 책임자를 대상으로 컴퓨터범죄의 실제 발생현황을 파악하기 위한 것이었으나 지난 1년간 컴퓨터 범죄가 1건도 발생하지 않은 곳이 대부분이었고 이중 불성실한 답변도 있을 것으로 생각된다. 따라서 설문지(2)는 참고자료로만 활용하였으며 통계적 분석에는 사용하지 않았다. 설문지(3)은 한 금융기관 당 3매이므로 총 114매인데 답변자료가 불충분한 12매를 제외시키고 나머지 102매를 분석에 사용하였다.

전산실용 설문지(1)은 MC, DAMC, OC, SC, AC, ISA에 속하는 항목의 점수를 평균하여 각 통제요소별로 측정하였으며 MC, DAMC, OC, SC에 속하는 항목들의 평균을 구하여 일반통제(GC: general control)을 측정하였다. 정보시스템통제의 전체적인 강도를 측정하기 위하여 MC, DAMC, OC, SC, AC에 속하는 모든 항목을 평균하여 전체 정보시스템통제(TC: total contol)을 측정하였다. 실시정도와 중요도의 괴리(Dev: deviation)를 측정하기 위하여 각 항목의 실시정도에서 중요도의 차이의 절대치를 구하여 평균을 구하였다.

영업부용 설문지(3)은 입력부정에 2개 항목, 프로그램에 1개 항목, 출력부정에 1개 항목이 있는데 각각 입력범죄위험1(IF1: input fraud 1), 입력부정2(IF2: input fraud 2), 프로그램범죄위험(PR: program fraud), 출력범죄위험(OF: output fraud)으로 측정하여 각 기관별 응답자(2-3인)의 평균을 구하였

〈표 3〉 정보시스템통제와 컴퓨터범죄위험간의 Perason상관계수

통제 / 범죄위험	MC	DAMC	OC	SC	GC	AC	TC	ISA	Dev
IF1	***	*			*		+	+	+
	−.5510	−.3982	−.2401	−.1830	−.4229	−.0712	−.3519	−.3293	.3634
IF2	***	***	***	***	***	+	***	***	***
	−.3703	−.7204	−.7082	−.7133	−.8562	−.3657	−.8212	−.5938	.4420
PF		**		**	**		*	**	**
	−.3510	−.4422	−.2902	−.3987	−.4744	−.0785	−.3961	−.4708	.5298
OF	**	***	***	***	***	*	***	***	**
	−.4702	−.7516	−.6514	−.5582	−.7516	−.4069	−.8000	−.6742	.4648
TF	***	***	***	***	***	+	***	***	***
	−.5602	−.7485	−.6174	−.5960	−.8344	−.2211	−.7714	−.6646	.5675

유의수준: +0.05 *0.01 **0.005 ***0.001

〈표 4〉 회귀분석결과: 일반통제, 응용통제, 감사 및 괴리변수

	GC	AC	ISA	Dev
IF1	−.08	−.26	−.03	.02
	(−2.56)	(−2.56)*	(−0.41)	(−1.06)
IF2	−.13	−.13	−.05	.02
	(−7.00)**	(−0.93)	(−1.24)	(−1.76)−
PF	−.05	−.22	−.00	.03
	(−2.29)+	(−3.03)**	(−0.17)	(−2.29)+
OF	−.10	−.00	−.14	.02
	(−4.07)**	(−0.91)	(−2.79)*	(−1.62)
TF	−.38	−.51	−.17	.61
	(−6.77)**	(−2.92)*	(−1.34)	(−0.33)

유의수준: −0.10 +0.05 *0.01 **0.005

다. 컴퓨터범죄의 총위험(TF: total fraud)를 측정하기 위하여 IF1, IF2, PF, OF를 평균하였다.

정보시스템통제변수와 컴퓨터 범죄변수간의

관계를 분석하기 위하여 Pearson상관관계분석을 실시하였다. 또한 Sprearman순위상관관계분석을 실시하였으며 그 결과가 거의 유사하므로 Pearson상관관계분석의 결과만 제시할 것이다.

모든 상관계수는 기대한대로 -의 부호로 나타났으며 45개의 계수중에서 5개를 제외한 40개의 계수가 통계적으로 유의하였다. 일반통제는 컴퓨터범죄의 총위험과 매우 높은 상관관계(-0.8344: 0.001수준에서 유의적)을 보이고 있으며 4가지 형태의 컴퓨터범죄위험과도 모두 유의한 상관관계를 보이고 있으므로 〈가설 1〉은 받아들일 수 있다. 응용통제는 총위험과 -0.2211의 상관계수를 나타내고 있으며 0.05의 수준에서 유의하다. 범죄위험의 형태별로 보면 응용통제는 입력범죄위험1과 프로그램범죄위험과는 유의한 관계를 보이고 있지 않으며 입력범죄위험2와 출력범죄위험과는 유의한 관계를 보이고 있다. 응용통제는 일반통제보다는 컴퓨터범죄위험과의 상관관계가 약하게 나타났으며 컴퓨터범죄위험의 형태별로 유의하지 못한 경우가 있으므로 〈가설 2〉는 부분적으로만 받아들일 수 있다. 일반통제와 응용통제를 포괄하는 전체적인 정보시스템통제변수는 컴퓨터범죄위험과 모두 유의적인 상관관계를 보이고 있다.

정보시스템감사는 컴퓨터범죄의 총위험과는 -0.6646의 상관관계(0.001수준에서 유의적)를 보이고 있으며 4가지 형태의 컴퓨터범죄위험과 모두 유의적인 상관관계를 보이고 있으므로 〈가설 3〉은 받아들일 수 있다. 정보시스템통제의 중요도와 실시정도의 괴리는 컴퓨터범죄의 총위험과 -0.5675의 상관관계(0.001수준에서 유의적)를 보이고 있으며 4가지 형태의 컴퓨터범죄와 모두 유의적인 관계를 보이고 있으므고 〈가설 4〉도 받아들일 수 있다.

정보시스템통제 및 감사변수들이 컴퓨터범죄에 미치는 상대적 중요성을 분석하기 위하여 컴퓨터범죄를 종속변수로 하고 일반통제, 응용통제, 정보시스템감사 및 괴리변수를 독립변수로 하여 회귀분석을 실시하였다. 회귀계수는 다음과 같으며 괄호안은 각 회귀계수의 t값을 나타낸다.

모든 계수는 음의 값으로 나와 기대한 바와 같다. 일반통제의 회귀계수는 모든 형태의 컴퓨터범죄위험의 경우에 유의하며 응용통제는 입력범죄위험1, 프로그램범죄 및 총범죄의 경우에 유의한 것으로 나타났다. 정보시스템감사 활동은 출력범죄위험의 식의 경우에 유의한 것으로 나타났으며 괴리변수는 프로그램범죄위험의 회귀식에서만 유의한 것으로 나타났다. 회귀식별로 보면 입력범죄위험1의 경우에는 일반통제와 응용통제가 비슷한 수준의 영향력을 보이고 있으며 정보시스템감사와 괴리변수는 유의하지 않다. 입력범죄위험2의 회귀식에서는 일반통제가 가장 큰 영향을 미치고 있으며 괴리변수가 0.10수준에서 한계적으로 유의하며 나머지 변수들은 유의하지 않다. 프로그램범죄위험의 회귀식에서는 응용통제의 영향력이 가장 높게 나타나고 있으며 일반통제와 괴리변수가 유의한 것으로 나타났다. 출력범죄위험에서는 일반통제의 영향이 가장 크며 정보

〈표 5〉 회귀분석결과; 일반통제의 구성요소

	MC	DAMC	OC	SC
IF1	-.31 (-2.70)*	-.02 (-0.25)	-.02 (-0.43)	-.00 (-0.88)
IF2	-.06 (-0.75)	-.21 (-4.87)**	-.08 (-2.60)*	-.20 (-3.80)**
PF	-0.7 (-0.72)	-.08 (-1.32)	.01 (0.25)	-.13 (-1.61)
OF	-.02 (-0.24)	-.23 (-4.15)**	-.09 (-2.38)+	-.10 (-1.49)
TF	-.35 (-1.53)	-.55 (-3.56)**	-.18 (-1.70)-	-.45 (-2.35)

유의수준: -0.10 +0.05 *0.01 **0.005

시스템감사도 유의하게 나타나고 있으며 나머지 변수들은 유의하지 않다. 총범죄위험의 회귀식에서는 일반통제가 가장 유의적이며 응용통제도 유의적으로 나타나고 있다. 회귀분석의 결과가 대체적으로 상관계수분석의 경우보다 유의한 경우가 적은 것은 독립변수간에 상관관계가 높은 때문인 것으로 보인다.

일반통제의 4가지 구성요소들이 컴퓨터범죄위험에 미치는 상대적 영향을 분석하기 위하여 4가지의 일반통제의 구성요소를 독립변수로 하여 회귀분석을 실시하였다.

프로그램범죄위험의 회귀식에서는 OC의 회귀계수가 +로 나왔으나 유의하지 않으며 나머지 모든 회귀계수는 -의 값을 가지고 있다. DAMC는 입력범죄위험2, 출력범죄위험2 및 총위험의 회귀식이에서 유의한 회귀계수를 가지고 있으며 OC는 입력범죄위험2와 출력범죄위험회귀식에서 유의하며 총위험의 회귀식에서는 한계적으로 유의하다. SC는 입력범죄2와 총위험의 회귀식에서 유의하다. MC는 입력범죄위험1의 회귀식에서 유의할 뿐이다.

회귀식별로 보면 입력범죄위험1의 회귀식에서는 단지 MC가 유의하며 나머지 변수들은 유의하지 않다. 입력범죄위험2의 식에서는 DAMC가 가장 영향력이 크며 SC 및 OC가 유의한 계수를 가지고 있다. 프로그램범죄위험의 경우에는 유의한 변수가 없다. 출력범죄위험의 식에서는 DAMC의 영향력이 가장 크며 OC도 유의하다. 총범죄의 회귀식에서는 DAMC가 가장 유의하며 SC가 유의한 계수를 가지고 있으며 ISOC는 한계적으로 유의하다.

+의 계수가 한개 나타나고 유의하지 않은 계수가 상관분석이 경우보다 많이 나오는 것은 앞의 회귀분석과 마찬가지로 독립변수간의 상

관관계로 인한 다중공선성때문인 것으로 보인다.

V. 결 론

정보기술은 매우 빠른 속도로 발전하고 있으며 정보기술을 이용한 경영혁신이 최근의 관심사로 부상하고 있다. 정보시스템에 대한 투자의 비중이 높아지고 정보시스템을 전략적으로 활용하여 경쟁력을 제고시키려는 노력이 가속화되고 있으며 이러한 추세는 계속될 것이다. 정보시스템의 최근 경향은 네트워킹, 개방시스템, 다운사이징 등으로 나가고 있으며 이러한 첨단시스템에서 정보시스템에 대한 위협요인은 증가하게 된다. 컴퓨터범죄는 컴퓨터를 활용하여 조직과 개인에게 재산적인 패해를 유발시키므로 정보시스템확산에 대한 주요한 장애요인이라고 할 수 있다. 정보시스템을 발전시켜나가는 과정에서 컴퓨터범죄의 위험을 인식하고 이에 대한 적절한 대비책을 수립하여 나가야 할 것이다.

금융기관은 업무의 특성상 정보시스템에 대한 의존도가 높으며 금융자산에 대한 컴퓨터범죄의 위험도 높다고 할 수 있다. 통계적으로 컴퓨터범죄의 80%이상이 금융기관에 집중되어 있는 실정이다. 금융기관은 최근 들어서 대규모의 전산투자를 통하여 정보시스템을 빠른 속도로 발전시켜 나가고 있으나 컴퓨터범죄를 방지하기 위한 정보시스템통제 및 감사에 대한 투자 및 관심은 많지 않은 실정이다. 정보시스템통제는 자산보호, 자료의 완전성, 효과성 및 효율성을 지향하는 정보시스템과 관련된 조직계획, 조정방법 및 수단으로서 잘 설계되고 운영되는 정보시스템통제는 컴퓨터범죄를 효율적으로 예방하고 적발할 수 있을 것이다. 정보시스템감사는 정보시스템이 소기의 목표를 달성하였는가를 평가하는 과정이라고 할 수 있으며 정보시스템통제의 신뢰성을 평가하고 취약점을 개선해 나가는 역할을 한다. 정보시스템감사는 정보시스템통제와 보완적으로 컴퓨터범죄를 예방하고 적발하는 기능을 수행한다.

본 논문에서는 정보시스템통제 및 감사와 컴퓨터범죄와의 인과관계를 모형화하고 38개의 금융기관에 대한 설문조사를 통하여 이를 검증하였다. 통계적 분석결과 가설설정과정에서 기대한 바와 같이 정보시스템통제 및 감사는 이용자부서에서 인지하고 있는 컴퓨터범죄위험과 유의한 관계가 있는 것으로 나타났다.

즉 정부시스템통제 및 감사의 체계가 우수하고 잘 실시될수록 컴퓨터범죄의 위험은 감소하는 것을 의미한다. 일반통제가 응용통제보다 컴퓨터범죄위험에 더 많은 영향을 미치고 있었다. 또한 정보시스템통제의 중요도와 실시정도의 괴리가 클수록 컴퓨터범죄위험이 높아지는 것으로 나타났다. 연구의 대상이 금융기관중에서도 은행과 증권에 한정되어서 전체 금융기관의 실태와는 다소 차이가 있을 수 있으며 금융산업이외의 다른 산업에 대한 결과의 일반화에도 한계가 있다. 그러나 은행 및 증권회사가 금융산업에서 중요한 비중을 차지하고 있으며 은행과 증권회사에 대한 컴퓨터범죄가 전체의 약 80%를 차지하고 있는 실정에서 은행과 증권

회사를 중심으로 하여 금융기관을 연구대상으로 한 것은 의의가 있다고 하겠다.

금융시장 개방을 맞이하여 각 금융기관은 전산화에 대한 대규모 투자를 통하여 국제 경쟁력을 제고시키는데 노력을 경주하고 있다. 본 논문의 연구결과는 컴퓨터범죄의 방지를 위하여 정보시스템통제 및 감사를 체계화시키고 합리적으로 운영해야 할 것을 시사하고 있다. 금융기관은 물론 전산의존도가 높은 기업은 전산개발과정에서 컴퓨터범죄의 위험성을 인식하고 각 기업의 환경에 적합한 정보시스템통제 및 감사의 체계를 갖추어 나가야 할 것이다. 본 논문은 단지 방향성을 제시하였으며 앞으로의 연구는 컴퓨터범죄를 방지하기 위하여 각 기업 환경에 적합한 정보시스템통제 및 감사를 설계하고 운영하는데 도움을 줄 수 있는 구체적이고 심층적인 연구가 이루어 져야 할 것이다.

참 고 문 헌

금융전산망 추진위원회, 금융전산망 기본계획 1992-1996, 1992.

김문일, 컴퓨터 범죄론, 법영사, 1985.

노연후, 컴퓨터 범죄, 하이테크정보, 1992.

이병태, 컴퓨터 범죄, 정음문화사, 1984.

이장형, 금융기관의 내부통제가 회계정보시스템의 유용성에 미치는 영향, 회계학연구, 7월호, pp. 199-222., 1994.

전자신문, 시스템침해를 막는 데이타 안전핀 부각, 7월 29일, 1985.

한국금융연수원, 영업점 EDPS안전관리와 사고예방, 1988.

한국은행 은행감독원, 컴퓨터사고 사례 및 예방대책, 1991.

한인구, 전산감사의 의의와 현황, 월간 공인회계사, 7월호, pp. 63-68, 1993.

한인구, 정보시스템감사실무, 한국과학기술원 산학협동공개강좌, 1994.

ABA, "Report on Computer Crime" pamphlet, prepared by the Task Force on Computer crime, American Bar Association, Section on Criminal Justice, 1984.

AICPA, "Report on the Study of EDP-Related Fraud in the Banking and Insurance Industries," pamphlet, American Institute of Certified Public Accountants, 1984.

BloomBecker, J., Computer Crime, Computer Abuse, Computer Ethics, National Center for computer Crime Data., 1986.

EDPAA, Control Objectives, 4th edition, EDPAF, 1992.

Ernst and Whinney, "1989 Ernst & Whinney Conputer Security Survey Report," Phamplet, Ernst & Young, 1989.

Kusserow, R., "Computer-Related Fraud and Abuse in Government Agencies,"Phamplet, U.S. Dept of Health and Human Services.

Parker, D., Crime by computer. Scribner's., 1976.

Parker, D., Computer Security Management, Reston, 1981.

Straub, D., "Effective IS Security: An Empirical Study," Information System Research, pp. 255-276, 1990.

Weber, R., EDP Auditing, 2nd edition, McGraw-Hill, 1988.

Wong, K., "Computer Crime-Risk Management and Conputer Security," Computer & Secutrity, pp. 287-295, 1985.

◇ 저자소개 ◇

공동저자 **한인구**는 서울대 국제경제학 학사, KAIST 경영과학 석사를 취득하고 University of Illinois at Urbana-Champaign에서 회계정보시 스템을 전공하여 경영학박사학위를 취득하였으며 현재 KAIST 서울분 원 경영정보공학과에 재직하고 있다. 최근의 주요 관심분야는 정보시 벼 스템감사 및 보안, 인공신경망을 이용한 신용평가 및 주가분석 등이다.

공동저자 **윤종호**는 경북대학교 회계학과를 졸업하고 한국과학기술원 서울분원 경영정보공학과에서 석사학위를 취득하였다. 제일투자신탁 운용부에서 채권운용과장을 거쳐 현재 주식운용역으로 재직하고 있다.