「정보시스템연구」 제15권 제1호
한국정보시스템학회
2006년 3월, pp. 145~168

정보보안정책, 보안통제 및 사용자특성이 정보보안효과에 미치는 영향: 컴퓨터 바이러스를 중심으로*

김종기** · 전진환*** · 임호섭****

<목 차>

Ⅰ. 서 론

컴퓨터 바이러스(computer virus)는 정보화 시대에 사용자들이 가장 흔하게 경험하는 정보보안 문제이다. 개인용 컴퓨터의 급격한 보급과 네트워크 확산, 그리고 바이러스 제작기술의 발전은 컴퓨터 바이러스 문제의 복잡성을 한층 더 증가시켜 사용자가 조기에 발견하여 이에 대처하기 어려운 상황이 되었다(Nachenberg, 1997). 2002년도 미국의 소비자 보고서(Consumer Reports, 2002)에 따르면 Consumer Reports 웹 사이트의 가입회원 8,000여 명 중 58%에 해당하는 사용자들이 2년 동안 적어도 한 번의 컴퓨터 바이러스의 공격을 받았고, 그 중 10%는 컴퓨터 바이러스에 의한 직접적인 피해를 경험하였다고 한다.

* 이 논문은 2004년도 한국학술진흥재단의 지원에 의하여 연구되었음 (KRF-2004-002-B00055).
** 부산대학교 상과대학 경영학부 부교수, jkkim1@pusan.ac.kr
*** 부산대학교 일반대학원 경영학과 경영정보 및 생산관리 전공, jeonjinhwan@pusan.ac.kr
**** 동아대학교 미디어디바이스연구센터, hslim@dau.ac.kr

2000년 5월에 발생한 아이러브유(I Love You) 바이러스는 인터넷을 통해 유포된지 5시간 만에 생산성 손실을 포함한 피해규모가 100억불에 이르렀으며(Bagchi & Udo, 2003), 2003년 1월 25일 슬래머(Slammer) 웜은 MS-SQL 서버를 공격하여 10분 만에 전세계에 걸쳐 인터넷 장애를 유발하였다(Panko, 2003). 특히, 이 사건은 국내의 사용자들에게 컴퓨터 바이러스에 대한 경각심뿐만 아니라 정보보안 전반의 취약성과 중요성을 일깨우는 일대 전환점이 되었다(한국전산원, 2003). 또한 2004년 3월부터 확산되기 시작한 넷스카이(Netsky)와 베이글(Bagle) 웜의 경우 정보시스템에 대한 파괴력도 문제였지만, 바이러스 제작자들 사이에 경쟁적으로 변종을 개발함으로써 백신업체들을 곤란하게 만들기도 하였다. 최근에는 PDA와 같은 모바일 기기를 대상으로 한 바이러스도 등장하였다(Hancock, 2000; Viveros, 2003).

이처럼 컴퓨터 바이러스에 의한 피해는 해마다 증가하고 있는 추세이며, 대체로 프로그램을 삭제한다든지 운영체제의 공격에 의한 시스템 운영 중단과 같은 손실을 발생시키고 있다(Chordas, 2004). 이와 같은 컴퓨터 바이러스에 의한 정보화의 역기능을 줄이기 위해서는 정보보안 목표 및 이에 상응한 보안대책을 포함하고 있는 보안정책의 수립이 필수적이다.

특히, 보안정책의 수립에 있어 조직 전체적인 관점에서 조화를 이룰 수 있어야 하며, 컴퓨터 바이러스와 관련하여 예외적인 상황에 대비하기 위한 사용자의 노력도 포함되어야 한다. 예를 들어, 2003년에 미국에서 실시된 CSI(Computer Security Institute)의 조사에 따르면 525개의 설문응답 기업 중에서 99%가 바이러스 대응 소프트웨어(anti-virus soft ware; AV S/W)를 운영하고 있음에도 불구하고, 그 중 82%가 컴퓨터 바이러스 관련 감염사고를 경험하였다(CSI, 2003). 2003년에 국내에서 실시된 한 조사에 따르면 중 85.9%의 기업이 바이러스 백신을 사용하고 있지만, 그중에서 74.2%의 대기업과 58.8%의 중소기업이 바이러스 피해를 경험하였다고 한다(한국전산원, 2003). 이처럼 컴퓨터 바이러스의 예방을 위해 기술적 측면에서 AV S/W의 설치와 같은 단순한 대응 수단만으로는 보안효과를 가져오기 힘들다는 것은 새로운 사실이 아니다(Nachenberg, 1997).

지금까지 MIS 분야에서 컴퓨터 바이러스를 포함한 정보보안과 관련된 실증연구는 상대적으로 미흡한 실정이었으며, 컴퓨터 바이러스의 통제와 관련된 실증연구로는 AV S/W 투자와 효과의 관계를 분석한 Post & Kagan(2000) 이외에는 거의 찾아볼 수 없을 정도로 대단히 희소한 분야에 속한다. 따라서 본 연구에서는 컴퓨터 바이러스의 통제에 영향을 미치는 요인들을 선행연구를 통해 도출하고 실증적으로 분석함으로써 이들 요인들이 컴퓨터 바이러스에 대한 정보보안의 효과성을 가지는지에 대한 타당성을 평가하고자 한다.

Ⅱ. 이론적 배경

2.1 컴퓨터 바이러스와 정보보안

컴퓨터 바이러스는 데이터의 가용성(availability)과 비밀성(confidentiality) 및 무결성(integrity)에 영향을 미치는 주요 위협요소이다(Skoudis & Zeltser, 2003). 특히, 프로그램과 프로그램, 파일과 파일, 정보시스템에서 다른 정보시스템으로 감염이 확산되는데 있어서 사용자가 인지하지 못하거나 경우에 따라서는 사용자의 관여가 없이도 전파가 가능하다(Wen, 1998). 최근 인터넷을 통해 빠른 속도로 확산되어 큰 피해를 입혔던 베이글(Bagle), 소빅(Sobig), 블라스터(W.32 Blaster) 등과 같은 웜(worm)의 경우에는 숙주 프로그램 없이 스스로 복제할 수 있는 독립성을 가지고 있으며, 짧은 시간 내에 정보시스템과 네트워크 자원을 소진시켜 정보시스템의 운영을 중지시킴으로써 결과적으로 데이터의 가용성을 저해하는 것이 특징이다(Chordas, 2004).

컴퓨터 바이러스는 스스로 다른 프로그램에 첨부되기 위해 자아복제(self-replication)를 하고, 이메일에 첨부되어 전송되기도 하며, 때로는 사용자가 감염된 플로피 디스크나 파일을 다운로드하여 사용하고자할 때 원치 않는 기능을 실행시키는 작은 프로그램으로 정의된다(Cohen, 1987; Skoudis & Zeltser, 2003; Chordas, 2004; Szor, 2005). 컴퓨터 바이러스를 넓게 보면 독립적인 자기복제력을 가진 웜이나 사용자를 기만하여 피해를 유발하는 프로그램을 작동케 하는 트로이 목마(Trojan horse)를 포함할 수도 있다. 최근에는 협의의 컴퓨터 바이러스와 웜을 엄격하게 구분하지 않고 혼용하여 지칭하는 경우가 빈번하며, 사용자가 의도하지 않는 결과를 유발하는 모든 형태의 프로그램을 통칭하여 악성 소프트웨어(malicious software; malware)로 부르고 있다(Skoudis & Zeltser, 2003; Szor, 2005).

컴퓨터 바이러스와 관련한 기존 연구들은 대부분 AV S/W 개발과 관련된 기술적 측면의 연구이거나 AV S/W 선정을 위한 고려사항을 다루고 있다(Polk & Bassham, 1992; Sherif & Gilliam, 2003). 그 외에 일반적인 정보보안 연구들(Hoffer & Straub, 1989; Loch et al., 1992)에서는 컴퓨터 바이러스를 주요한 위협요소 중의 하나로 규정하고, 위험감소의 일반적인 차원에서 여러 보안대책 중에서 감염피해를 축소하기 위한 예방적 보안대책을 언급하였다.

Wack & Carnahan(1989)의 연구는 최근 피해를 입히고 있는 인터넷 웜과 관련된 것이라기보다 협의적 관점에서 컴퓨터 바이러스에 대한 내용을 주로 다루고 있어 오늘날의 시대적인 상황이 잘 맞지 않지만, 컴퓨터 바이러스의 파괴력과 피해범위를 추정할 수 없고, 감염사고가 주로 사용자의 부주의 및 권한을 가진 악의적 사용자에 의해 고의적으로 전파되고 확산될 가능성이 있음을 지적하고 있다. 또한, Hoffer & Straub(1989)의 연구에서도 비슷한 내용이 논의되는데, 정보보안의 정책적 차원에서 사용자 교육을 통한 감독과 주기적인 데이터 백업(backup)을 포함한 비상계획이 중요함을 지적하였다.

2.2 보안정책

보안정책(security policy)은 조직의 중요정보를 어떻게 관리하고 보호하며, 배포하는가에 관한 일련의 규칙과 실무지침을 규정해 놓은 것으로 정보시스템 활용에 있어 사용자와 조직구성원들에게 보안관련 기준을 제시해 놓은 것이다(Russsell & Gangemi, 1991). 적절하게 설정된 보안정책은 사용자 스스로 정보기술에 대한 부적절한 활용을 통제하여 정보시스템 보안을 강화하도록

하며, 감염확산의 차단 및 재발 가능성을 억제할 수 있게 한다(Wen, 1998).

Wack & Carnahan(1989)은 컴퓨터 바이러스와 관련된 위협들이 어제 오늘 일이 아니지만 과거 컴퓨터 바이러스에 의한 피해정도가 경미하였거나 발생빈도가 낮았기 때문에 잠재적인 위협이 클 것이라고 예상만 할 뿐 정보시스템의 설계나 관리적 측면에서 컴퓨터 바이러스의 위협을 경시하였음을 지적하였다. 이러한 현상은 오늘날까지 지속되고 있으며, 따라서 컴퓨터 바이러스에 대한 효과적인 대응이 이루어지지 못하고 있다. Wen(1998)은 컴퓨터 바이러스 차단의 필요성을 인지하고 있는 사용자와 AV S/W 제품이 바이러스 탐지와 차단을 위한 절차와 통합됨으로써 효과적인 컴퓨터 바이러스 대응이 가능함을 지적하였지만, Frank et al.(1991)은 사용자의 보안인지와 AV S/W의 컴퓨터 바이러스의 차단 효과에도 불구하고 이의 활용을 효과적으로 관리하지 못하는 조직내 대응책의 부재를 가장 큰 문제점으로 지적하기도 하였다.

대부분의 정보보안 관련 연구에서 컴퓨터 바이러스와 관련하여 언급되고 있는 보안정책으로는 컴퓨터 바이러스 인지 프로그램 활용(Post & Kagan, 2000; Lee & Lee, 2002), 사용자 정보보안 교육(Post & Kagan, 2000; Hoffer & Straub, 1989; Wen, 1998), 대내·외 보안사고 공지(Post & Kagan, 2000; Wen, 1998), 데이터 송·수신전 검사(Post & Kagan, 2000), 데이터 백업(Hoffer & Straub, 1990; David, 1996; Highland, 1997; Post & Kagan, 2000), 정보시스템 접근통제(Straub & Nance, 1990; Kankanhalli et al., 2003), 보안 시스템 활용(Wen, 1998; Hubbard & Forcht, 1998; Gordineer, 2003; Kankanhalli et al, 2003; Straub, 1990) 등이 있으며, 이를 통해 조직에서 컴퓨터 바이러스를 포함한 정보보안 침해사고의 예방효과를 높이고자 노력하는 것으로 나타났다.

2.3 보안통제

컴퓨터 바이러스로부터 잠재적인 위협과 감염사고의 발생을 축소하기 위해서는 효과적인 보안통제가 이루어져야 한다. 보안통제(security controls)는 보안사고를 미연에 방지하거나 발생된 보안사고의 영향을 최소화하기 위한 기술적, 관리적 활동을 의미하는 것으로(Wack & Carnahan, 1989), 적절한 보안통제가 이루어지지 않을 경우 보안운영절차, 기술적 통제 및 물리적 통제 등의 미비나 결여로 인하여 정보시스템이 취약성(vulnerability)을 가지게 되며, 생성된 취약성은 특정 위협에 정보시스템을 노출시켜 위험을 초래하게끔 한다(김세헌, 2002; CSE, 1996; NIST, 1998).

특히, 컴퓨터 바이러스의 감염사고를 통제하기 위해 AV S/W 등의 기술적인 측면에서 접근하는 것만으로는 위험을 줄이지 못한다. 이는 Bagchi & Udo(2003)의 연구에서도 지적된 바 있는 것으로 컴퓨터 바이러스 관련 사고의 발생과 AV S/W의 사용 사이에는 상관관계가 없다는 점에서 기인한다. 컴퓨터 바이러스의 사고를 방지하기 위해 기본적으로 시행되어야 할 보안대책은 업무종료 후 컴퓨터를 전원을 차단하고, 인증받지 않은 사용자가 정보시스템의 사용을 할 수 없도록 해야 한다. 또한, 디스켓의 경우 가급적 쓰기방지를 선택하고, 컴퓨터 바이러스 관련 감염사

고에 대해 조직구성원에게 숙지시킬 필요가 있다(Peltier, 2001). 이를 위해 사용자의 보안 인지를 높일 수 있는 보안교육을 실시하고, 백업 및 접근 통제 등의 기술적 통제가 적절히 활용되어야 한다.

컴퓨터 바이러스 관련 보안통제는 다른 보안대책들과 더불어 조직의 정보보안 목적에 부합되는지와 효과성에 대한 평가가 통합적으로 이루어져야 한다(Wack & Carnahan, 1989; Peltier, 2001; Gordineer, 2003). 또한 소프트웨어의 결함(Wack & Carnahan, 1989; Barsanti, 1999; Gordineer, 2003), 네트워크에 다수의 익명 접근 권한을 부여함으로써 네트워크의 오·남용의 용이성(Wack & Carnahan, 1989; Barsanti, 1999)에 대한 평가도 이루어져야 한다. 이에 대한 평가 결과에 따라 보안통제들이 불충분하거나 모순적일 경우 수정이 불가피하다(DeMaio, 1989).

2.4 사용자특성

Frank et al.(1991)은 조직내 PC 사용자의 백업, 문서 및 데이터 저장과 파일 접근 등 일련의 보안활동을 통제하는데 영향을 미치는 요인들을 분석한 결과 조직내 PC 보안에 대한 사용자 지식, 비공식적 행동규범(informal norms) 및 공식적 정책(formal policy)간에 상관관계가 있는 것으로 나타났다. 공식적인 보안정책은 사용자의 보안관련 행동에 그다지 많은 영향을 미치지 않지만, 사용자의 보안관련 지식수준이 낮을 경우 정책과 규범이 상당한 영향력을 행사하며, 역으로 사용자의 지식수준이 높을 경우 정책과 규범의 영향력은 다소 떨어지는 것으로 평가되었다.

Leach(2003)는 조직내 PC사용자의 보안관련 행동을 향상시킬 수 있는 핵심 요인들을 조직구성원에게 요구되는 행동에 대하여 사용자가 이해해야할 부분과 규범 내에서 행동하고자 하는 사용자의 의지라는 두 부분으로 나누어 설명한다. 먼저, 보안목표, 보안정책, 표준 및 절차 등의 보안지식, 최고경영자와 동료로부터 학습된 행동수칙, 사용자의 보안관련 일반상식과 의사결정 능력의 세 가지는 사용자가 이해해야 하는 사항에 해당하며, 사용자의 개인적 가치와 행동표준, 사용자의 고용주에 대한 의무감, 행동표준과 절차를 지키기 위한 순응노력 등의 세 가지는 사용자가 조직에서 수용하려고 하는 규범으로 규정하고 있다. 이들 요소들은 여러 기술적인 통합을 통해 사용자의 보안능력을 향상시키게 되며, 보안위협으로부터 조직의 정보시스템을 보호할 수 있게 된다는 것이다. 더불어 이를 위한 조직내 강력한 정보보안 관련 문화는 필수적임을 강조하였다.

그 외에도 Goodhue & Straub(1991)는 정보보안에서의 사용자의 개인적인 특성을 잠재적인 문제 발생의 지각정도로 평가하여 보안문제의 발생정도의 수용에 따라 보안관련 만족도에 영향을 미친다고 설명하였으며, Wack & Carnahan(1989)은 PC 사용자를 대상으로 한 AV S/W는 사용자의 기술적 통제 능력의 부족과 바이러스 차단 결과를 중시하기 때문에 사용자 참여에 많이 의존함을 지적하기도 하였다.

2.5 보안효과

조직에서 정보시스템의 기능은 단위부서와 관련 업무의 생산성과 효율성을 제공하며, 조직내 핵심 보안자원에 대한 적극적인 투자는 보안효과의 극대화로 직결되고 이는 곧 조직의 성과 향상으로 이어진다(Hoffer & Straub, 1989). Goodhue & Straub(1991)는 정보시스템 사용자의 보안관심(security concern)과 관련한 연구에서 정보시스템에 대한 보안대책의 만족도는 과업특성, 정보시스템 환경, 사용자의 개인적 특성에 의해 영향을 받는 것으로 설명하였다. 특히, 정보시스템에 대한 사용자의 보안인지와 지식이 조직의 적절한 보안대책을 선정하는데 중요한 영향을 미치는 것으로 평가되었다.

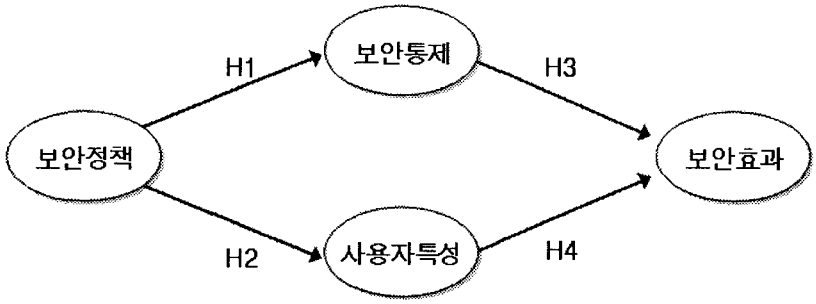
Straub(1990)의 연구에서는 관리자가 사용자에게 정보시스템의 사용과 관련하여 허용되는 행위와 허용되지 않는 부적절한 행위에 대해 사용자들에게 공지하고, 허용되지 않는 정보시스템 오·남용에 대해서는 벌칙을 부여할 경우 사고발생의 횟수, 기회비용 손실 등이 축소되는 것으로 확인하였다. 또한, 예방적 보안대책과 같은 정보보안에 대한 투자는 컴퓨터 오·남용에 따른 막대한 손실을 현저하게 감소시킬 수 있음을 지적하였다.

보안효과와 관련된 다른 선행연구 중에서 Post & Kagan(2000)은 발생건수, 심각성, 백업빈도, AV S/W의 만족도를 통해 컴퓨터 바이러스 예방과 관련된 투자에 대한 효과성을 평가하였다. 컴퓨터 바이러스의 경우 보안정책과 노력을 통해 바이러스 위협을 축소하고 효과적으로 대응할 수 있는지에 대한 평가가 필요하고, 이는 침해사고 발생건수(Straub, 1990), 기회비용 및 생산성 손실(Straub, 1990; Post & Kagan, 2000) 등의 측면에서 평가될 수 있다.

Ⅲ. 연구모형 및 가설

3.1 연구모형의 설계

본 연구에서 컴퓨터 바이러스 보안통제의 효과에 영향을 미치는 요인들을 실증적으로 규명하고자 다음의 <그림 1>과 같이 연구모형을 설정하였다. 먼저, 조직의 보안정책이 정보시스템과 관련된 보안통제의 수준을 결정지을 수 있으며, 사용자의 정보시스템 관련 책임 및 인지 등의 개인적 특성에 영향을 미치는 것으로 보안정책과의 관계를 설정하였다. 또한, 조직의 정보시스템 보안관리 활동의 측면에서 논의되는 보안통제 요인은 실질적인 보안효과를 가져오게 되며, 정보시스템 활용과 관련된 사용자의 개인적 특성 또한 컴퓨터 바이러스로부터 정보보안 효과에 영향을 미치는 선행요인으로 보았다.



<그림 1> 컴퓨터 바이러스 통제의 영향요인에 관한 연구모형

3.2 연구가설

연구모형을 토대로 컴퓨터 바이러스 통제에 영향을 미치는 요인들에 대한 실증분석을 위해 다음과 같이 연구가설을 수립하였다.

3.2.1 보안정책과 보안통제의 관계

연구가설 1은 조직의 보안정책과 보안통제 사이의 관계를 설명하는 것이다. 정보보안에서 보안정책은 정보시스템 보안 프로그램의 목적을 설정하고, 책임을 부여하며, 특정한 정보시스템에 적용되는 구체적인 보안규칙을 의미한다(Gasser, 1988). 또한, 조직구성원의 정보보안 관련 행동지침을 제공하고, 이메일 보안, 프라이버시 보호, 컴퓨터 바이러스 등 구체적인 사안에 대한 관리적 지침을 제시한다(NIST, 1998).

다수의 연구자들은 조직의 정보보안과 관련된 타당한 보안정책이 사전에 확보되어 있어야만 효과적인 정보보안이 가능하다고 지적하였다(Bergeron & Berube, 1990; Whitman, 2004). 이를 통해 조직내 정보시스템의 내재적인 취약성을 축소함과 동시에 사용자들이 보안사고를 사전에 방지할 수 있도록 도움을 주게 된다.

보안통제는 조직의 정보자원에 대한 비밀성, 무결성, 가용성을 보존하기 위한 제반관리 활동들로 구성된다(Wack & Carnahan, 1989; Blatchford, 1995). 컴퓨터 바이러스는 감염 발생을 예측할 수 없는 외적 위협요소로 규정하고 있으며(Loch et al, 1992), 이로부터 발생하는 보안 침해사고는 사용자의 통제가 거의 이루어지지 못한 상황에서 빠르게 전파되기 때문에 예방적 차원에서 보안통제의 역할은 매우 중요하게 된다. 이러한 이유로 인해 조직의 보안정책이 적절하게 수립되어 있을 경우 조직의 보안통제 수준 또한 자연적으로 높아지는 현상이 발생한다. 그러므로 연구가설 1이 다음과 같이 수립되었다.

H1: 조직내 컴퓨터 바이러스 관련 보안정책 수준이 높을수록 보안통제의 수준도 높아진다.

3.2.2 보안정책과 사용자특성

연구가설 2는 조직의 컴퓨터 바이러스 관련 보안정책과 사용자특성 사이의 관계를 설명하는 것이다. 대부분의 조직이 정보자산을 보호하기 위해 보안정책을 수립하고 정보시스템을 사용하는데 있어 민감한 정보의 취급상 주의점, 아이디 및 패스워드의 활용, 잠재적인 보안사고의 대응법, 인터넷 접속 등의 허용되지 않은 행위를 규정하고, 사용자에게 일련의 허용가능한 행위의 기준을 제시하고 있다(Straub & Welke, 1998; Lee & Lee, 2002). 잘 설정된 보안정책은 조직구성원에게 실무적인 지침을 제공하고, 여러 보안대책들이 미비하거나 부적절함으로 인해 결정적인 통제가 불가능할 경우 사용자 스스로 조직차원의 손실을 축소하기 위해 노력을 가할 수 있는 환경을 형성하게끔 한다(Frank et al, 1991). 특히, 정보보안에서 컴퓨터 바이러스 관련 피해 사고의 재발방지와 총체적인 관점에서 피해를 최소화할 수 있도록 사용자의 적극적인 예방노력은 매우 중요한 것이라 할 수 있다. 이에 따라 보안정책의 적절성은 사용자가 컴퓨터 바이러스의 감염으로 인한 피해 및 관련 지식을 습득하고, 정보시스템 보안과 관련된 개인적인 책임을 이해하는데 도움을 주게 된다. 그러므로 연구가설 2는 다음과 같이 수립되었다.

H2: 조직내 컴퓨터 바이러스 관련 보안정책 수준이 높을수록 사용자특성은 높아진다.

3.2.3 보안통제와 보안효과의 관계

연구가설 3은 컴퓨터 바이러스에 대한 보안통제와 보안효과 사이의 관계를 설명한다. 정보시스템 보안통제는 일련의 실천적 보안 활동으로 볼 수 있으며, 보안통제가 불충분하거나 통제방식이 부적절하게 활용될 경우 정보시스템을 보안위협에 노출시키게 되어 의도하지 않은 일련의 보안사고를 발생시키게 된다(Wack & Carnahan, 1989; Pipkin, 2000; Gordineer, 2003). 특히, 컴퓨터 바이러스는 개발자들에 의해 정보시스템의 특정한 취약성만을 고려해 제작된다는 기술적 특징을 가지고 있으며, 변칙성을 포함하고 있으므로 보안통제가 적절치 못할 경우 이에 따른 보안효과는 자연적으로 떨어지게 된다. 이에 따라 보안통제와 보안효과 사이의 관계는 다음과 같은 연구가설 3으로 수립하였다.

H3: 조직내 컴퓨터 바이러스 관련 보안통제의 수준이 높을수록 보안효과의 수준도 높아진다.

3.2.4 사용자특성과 보안효과의 관계

연구가설 4는 정보시스템 사용자의 보안관련 지식 및 인지 등의 개인적인 특성과 보안효과 사이의 관계를 설명하는 것이다. 사용자의 컴퓨팅 특성을 규정짓는 여러 요인 중 대표적으로 사용자의 정보시스템 책임인지 및 보안 지식이 여기에 해당하며(Goodhue & Straub, 1991), 더불어 조직문화, 개성, 정보시스템에 관한 관심과 같은 요인도 포함되기도 한다(Harris, 1999). 부지불

식간 발생하는 컴퓨터 바이러스의 특성상 감염피해를 방지하는데 조직의 보안정책 뿐만 아니라 사용자의 보안관련 인지가 컴퓨터 바이러스를 포함한 정보보안의 문제를 대처하는 중요한 역할을 하게된다. 이처럼 사용자의 정보시스템 활용에 관한 경험과 관련 지식수준은 조직내 합리적인 정보보안을 위한 전제조건이며, 보안효과를 형성하는데 중요한 역할을 하게 되므로 다음과 같이 연구가설 4를 수립할 수 있다.

H4: 조직내 컴퓨터 바이러스 관련 사용자특성이 높을수록 보안효과의 수준도 높아진다.

3.3 연구변수의 조작적 정의 및 설문항목 구성

연구변수에 대한 조작적 정의는 구성개념을 실증적으로 분석할 수 있도록 측정의 관점에서 구체화하였다. 본 연구에서 컴퓨터 바이러스의 통제효과를 검정하기 위해 수립된 연구 개념들은 아래의 <표 1>과 같이 조작적으로 정의되었으며, 모든 측정항목은 리커트(Likert) 7점 척도로 설문항목을 구성하였다. 본 연구에서 보안정책은 정보시스템 사용에 있어 수용되거나 수용되지 못하는 행위에 대해 명확하게 정의를 내리고, 정보시스템을 보호하기 위한 조직의 제반 규정 또는 절차를 의미하는 것(Lee & Lee, 2002; Peltier, 2001; Gordineer, 2003)으로 정의하였다. <표 1>에 제시되어 있는 선행연구를 토대로 컴퓨터 바이러스 관련 사용자의 정보보안 교육, 조직의 컴퓨터 바이러스 공지 정도, 컴퓨터 바이러스 검사 정도, 데이터 백업 및 복구 계획 정도 등을 통해 연구변수를 측정할 수 있도록 구성하였다.

보안통제는 보안효과에 영향을 미치는 선행요인으로 조직의 정보보안을 지원하는 기술적, 관리적 보안활동을 의미하는 것으로 조작적인 정의가 내려졌으며, Wack & Carnahan(1989), NIST(1998), Barsanti(1999), Peltier (2001), Gordineer(2003) 등의 연구에서 제시하고 있는 항목들을 참고하여 보안통제의 수준, 운영체제 보안 정도, 소프트웨어 결함 정도 등을 평가함으로써 구성개념을 측정하였다.

사용자특성 또한 조직의 보안효과에 영향을 미치는 요인으로 개인의 정보시스템 보안 관련 지식과 인지의 차별화 정도를 평가하기 위해 조작적으로 정의되었으며, Wack & Carnahan(1989) Frank et al.(1991), Goodhue & Straub(1991), Harris(1999), Thatcher & Perrewé(2002) 등의 선행연구에서 제시된 개념들을 수정하여 사용자 책임 및 권한의 인지정도, 보안정책의 인지 정도, 컴퓨터 바이러스 관련 인지도 등의 측정항목으로 평가하였다.

보안효과는 컴퓨터 바이러스의 위협으로부터 정보시스템을 효과적으로 보호하고 있는지에 대한 평가로 정보보안 관련 여러 연구들(Hoffer & Straub, 1989; Straub, 1990; Goodhue & Straub, 1991; Post & Kagan, 2000)로부터 보안효과를 평가할 수 있도록 사용된 업무손실, 기회비용의 발생, 정보시스템 손실, 정보자산 손실의 개념 등을 통해 측정하였다.

<표 1> 변수의 조작적 정의

연구변수	조작적 정의	측정항목	관련연구
보안 정책	정보시스템의 보안을 위한 일련의 규칙 또는 보안절차의 정도	◦ 사용자 정보보안 교육 정도 ◦ 컴퓨터 바이러스 공지 정도 ◦ 컴퓨터 바이러스 검사 정도 ◦ 송·수신전 데이터 검사 정도 ◦ 데이터 백업 및 복구계획 시행 정도	Hoffer & Straub(1989), Straub(1990), Straub & Nance(1990), David(1996), Highland(1997), Hubbard & Forcht(1998), Wen(1998), Lee & Lee(2002), Gordineer(2003), Kankanhalli et al.(2003)
보안 통제	정보보안을 지원하는 기술적, 관리적 활동 정도	◦ 보안통제 수준 정도 ◦ 보안통제 활용 정도 ◦ 운영체제 보안 정도 ◦ 네트워크의 감염 용이성 정도 ◦ 소프트웨어 결함 정도	Wack & Carnahan(1989), NIST(1998), Barsanti(1999), Peltier(2001), Gordineer(2003)
사용자 특성	사용자 개인의 정보보안관련 지식과 인지의 차별화 정도	◦ 책임 및 권한인지 정도 ◦ 정보보안 정책 인지 정도 ◦ 컴퓨터 바이러스 관련 인지 정도 ◦ 백신 활용정도 ◦ 컴퓨터 관련지식 정도	Wack & Carnahan(1989), Frank et al.(1991), Goodhue & Straub(1991), Harris(1999), Thatcher & Perrewé(2002)
보안 효과	컴퓨터 바이러스의 위협에 효과적으로 대응하고 있는지에 대한 평가	◦ 업무 손실 정도 ◦ 기회비용 손실 정도 ◦ 정보시스템 손실 정도 ◦ 정보자산 손실 정도	Hoffer & Straub(1989), Straub(1990), Goodhue & Straub(1991), Post & Kagan(2000)

Ⅳ. 실증분석

4.1 자료수집

본 연구에서는 부산·경남 지역 4개 대학교의 경영대학원(MBA) 학생들을 표본집단으로 선정하여 조사항목에 대해 응답자의 주관적 인식을 설문함으로써 자료를 수집하였다. 경영대학원 학생들을 표본집단으로 선정한 이유는 대부분이 직장에 소속된 조직의 구성원들임으로 소속된 조직의 정보보안정책에 대한 설문이 가능하기 때문이다. 연구조사를 위해 전체 330부의 설문지를 배포하여 281부를 회수하였으며, 이중 응답이 비논리적이거나 지나치게 불성실한 27부를 제외한 254부가 분석에 사용되었다.

4.2 표본특성

연구를 위해 수집된 응답자의 인구통계학적 특성을 살펴보면 다음의 <표 2>와 같다. 먼저, 응답자 중 남성이 211명(83.1%), 여성은 43명(16.9%)으로 상대적으로 남성 응답자의 비율이 높은

편이었다. 응답자의 연령대에 있어 40대 111명(44%), 30대 106명(42%)으로 전체의 86%를 차지하였으며, 그 외에 20대 7.5%, 50대 7.1% 순으로 응답 비율을 나타내었다. 소속된 조직의 산업별 특성으로는 제조업이 77명으로 30.3%를 차지하였으며, 다음으로 기타 60명(23.6%), 금융 및 보험업이 36명으로 14.2%를 차지하였다.

<표 2> 응답자의 인구통계 특성

구 분		빈도	비율(%)	구 분		빈도	비율(%)
성별	남자	211	83.1	산업 유형	운수업	6	2.4
	여자	43	16.9		제조업	77	30.3
	합계	254	100.0		통신업	7	2.8
연령대	20대	19	7.5		정보기술	12	4.7
	30대	106	41.7		교육 서비스업	28	11.0
	40대	111	43.7		보건 및 복지사업	9	3.5
	50대	18	7.1		도·소매업	19	7.5
	합계	254	100.0		금융 및 보험업	36	14.2
					기타	60	23.6

현재 조직내 정보보안정책의 수준을 묻는 질문에 보통이상으로 응답한 비율이 90.6%로 나타나 대부분의 응답자들이 자신이 소속된 조직의 정보보안정책에 대체로 만족하고 있는 것으로 나타났다.

<표 3> 조직내 정보보안 정책의 만족도

구 분		빈도	비율(%)
보안 정책	매우 잘되어 있다	39	15.4
	잘되어 있다	78	30.7
	보통이다	113	44.5
	잘못되어 있다	17	6.7
	매우 잘못되어 있다	7	2.8

최근 1년 동안 컴퓨터 바이러스 감염사고와 관련한 질문에 응답자의 81.9%인 208명이 지난 한 해 동안 감염사고를 한번이라도 경험한 것으로 나타났으며, 감염사고 경험자의 68.7%가 2회 이상 감염사고를 경험해 본 것으로 나타나 컴퓨터 바이러스의 심각성을 간접적으로 확인할 수 있었다. 추가적으로 감염 당시의 바이러스의 감염경로를 묻는 질문에 인터넷 또는 인터넷이 86명(33.9%), 전자우편을 통한 감염이 61명(24%), 공유폴더 및 내부 네트워크가 41명(19.7%)으로 나타났다. 추가적으로 감염증상을 묻는 질문에 시스템 및 네트워크의 속도 저하가 101명(48.6%), 소프트웨어의 손상은 53명(25.5%), 저장된 데이터의 손실이 31명(14.9%)으로 주로 개방형 네트

워크를 통한 컴퓨터 바이러스의 유입과 유입경로가 된 네트워크가 피해를 입은 것으로 나타났다.

4.3 측정모형의 평가

본 연구에서 연구모형과 연구가설의 검정을 위해 구조방정식(structural equation modeling; SEM)을 사용하였다. 구조방정식은 확인적 요인분석과 다중회귀분석 또는 경로분석 등이 결합된 방법론으로 측정변수의 공분산행렬(covariance matrix)을 토대로 연구자가 설정한 연구모형을 전체적인 관점에서 검증할 수 있도록 만들어진 연구방법론이다(Garver & Mentzer, 1999).

4.3.1 단일차원성 분석

연구모형의 검증에 앞서 연구도구의 타당성을 확인하여야 하며, 단일차원성(unidimensionality)에 대한 분석이 먼저 수행되어야 한다(Garver & Mentzer, 1999). 단일차원성은 각 구성개념들의 측정지표(indicator)들이 하나의 구성개념(construct)에 의해 수용될 수 있는 적합도를 의미하며, 탐색적 요인분석에서 신뢰도(reliability)와는 별개의 개념으로 크론바흐 알파(cronbach- α)가 높다고 해서 단일차원성이 있다고 볼 수는 없다(Anderson & Gerbing, 1990). 이는 연구개념에 대한 단일차원성의 검정은 측정항목간 공유분산의 표준화된 잔차(standardized residuals)가 지나치게 크거나 모형의 수정지수(modification index)가 5를 초과하는 측정항목을 하나씩 제거하는 방식을 사용함으로써 분석되어 진다(Segars, 1997; Anderson & Gerbing, 1988; Gefen, 2003).

본 연구의 확인적 요인분석에서 제안된 측정항목들이 하나의 구성개념에 수용되는지에 대한 단일차원성을 검정한 결과 잔차와 수정지수가 큰 POL4(송·수신전 데이터 검사 정도), CTL5(소프트웨어 결함 정도), USR4(백신 활용정도)의 3개 측정항목이 제외되었으며, 나머지 16개의 항목이 최종 측정 하부모형을 분석하는데 사용되었다.

4.3.2 측정모형의 신뢰성 평가

구조방정식 모형에서 측정 하부모형의 신뢰성을 평가하는데 주로 사용되는 측정치로 각 구성개념의 합성신뢰도(composite construct reliability)와 평균분산추출(average variance extracted; AVE)을 들 수 있다. 먼저, 합성신뢰도는 관측변수의 내적 일관성을 측정하는 측정치로 다르게 개념 신뢰도(construct reliability)라 부르기도 한다. 일반적으로 합성신뢰도의 측정치가 0.7 이상일 경우 수용가능한 수준이라 할 수 있다. 신뢰성 검정을 위한 또 다른 측정치인 AVE는 구성개념에 대해 지표가 설명할 수 있는 분산의 크기를 의미하는 것으로 측정치가 0.5 이상일 경우 수용 가능한 수준으로 볼 수 있다(Fornell & Larcker, 1981). 다음의 <표 4>와 같이 본 연구를 위

한 측정 하부모형의 합성신뢰도와 평균분산추출(AVE)의 측정치는 대체적으로 양호한 수준으로 나타나 연구모형의 내적 일관성이 충분히 확보되었음을 확인할 수 있다.

<표 4> 연구모형의 합성신뢰도 및 AVE

구성개념	합성신뢰도 (≥ 0.7)	AVE (≥ 0.5)
보안정책	0.88	0.66
보안통제	0.87	0.64
사용자특성	0.85	0.58
보안효과	0.91	0.73

4.3.3 수렴 타당성 검증

수렴 타당성(convergent validity)이란 하나의 연구개념을 측정하기 위해 다중지표가 사용된 경우 이 항목들 사이에는 높은 상관관계가 있어야 한다는 개념이다(Garver & Mentzer, 1999). 즉 동일 개념을 측정하는 다중의 척도가 어느 정도 일치하는가와 관련되는 것으로 측정항목의 추정치가 0.5 이상이고, t-값이 2.0 이상일 경우 수렴 타당성이 있는 것으로 판단한다(Bagozzi & Yi, 1988). 다음에 제시된 <표 5>에서 나타난 바와 같이 측정모형을 분석한 결과 모든 항목의 추정치(factor loading; λ)가 권고수준을 상회하는 것으로 나타나 연구개념의 수렴 타당성을 충족함을 확인할 수 있다.

<표 5> 수렴타당성 분석 결과

구성개념	항목	부하량	t-값	구성개념	항목	부하량	t-값
보안정책	사용자 정보보안 교육 정도	0.86	16.51	사용자 특성	책임 / 권한인지 정도	0.69	11.82
	바이러스 공지 정도	0.90	17.77		정보보호 정책 인지 정도	0.86	16.23
	바이러스 검사 정도	0.76	13.76		바이러스 관련 인지 정도	0.83	15.41
	데이터 백업/복구 계획 시행 정도	0.72	12.70		컴퓨터 관련지식 정도	0.64	10.74
보안통제	보안통제 수준 정도	0.90	17.73	보안효과	업무 손실 정도	0.70	12.70
	보안통제 활용 정도	0.92	18.48		기회비용 손실 정도	0.82	15.73
	운영체제 보안 정도	0.70	12.41		정보시스템 손실 정도	0.93	19.22
	네트워크의 감염 용이성 정도	0.64	11.45		정보자산 손실 정도	0.94	19.75

4.3.4 판별 타당성 검증

판별 타당성(discriminant validity)이란 서로 다른 개념들의 측정치 사이에는 확실한 차이가 존재해야 한다는 개념이다(Gefen, 2003). 구성개념간 판별 타당성을 측정하는 방법에는 여러 가지가 있으나 본 연구에서는 2개의 구성개념의 항목들을 통합하여 제약모형(constrained model)으로 만든 뒤 이를 비제약 모형(unconstrained model)과의 쌍 비교(pairwise discriminant analysis)를 통해 개념적 차이를 분석하는 방법(Anderson, 1987)을 활용하였다. 즉, 실증연구를 위한 본래의 측정모형과 구성개념들의 조합모형간 카이자승(χ^2) 추정치의 차이를 비교하여 차별성을 판단하는 방식이다. 다음의 <표 6>에서 나타난 바와 같이 4개 구성개념을 각각 쌍으로 묶어 총 6개의 모형에 대한 판별 타당성을 분석한 결과 측정모형과 조합모형 사이의 χ^2에 대한 차이가 모두 유의한 것으로 나타나 각각의 연구개념들이 고유성(uniqueness)을 가지는 것으로 분석되어 판별 타당성을 가지는 것으로 확인하였다.

<표 6> 측정모형의 쌍비교 판별 타당성 분석 결과

모형	df	χ^2	p-값	모형	df	χ^2	p-값
측정모형	98	197.20	0.00	측정모형	98	197.20	0.00
보안정책-보안통제 개념의 조합모형	101	882.80	0.00	보안통제-사용자특성 개념의 조합모형	101	879.58	0.00
보안정책-사용자특성 개념의 조합모형	101	540.90	0.00	보안통제-보안효과 개념의 조합모형	101	958.71	0.00
보안정책-보안효과 개념의 조합모형	101	1097.26	0.00	사용자특성-보안효과 개념의 조합모형	101	1104.72	0.00

4.3.5 측정모형의 적합도 평가

연구를 위한 전체 측정모형에 대한 단일차원성, 신뢰성, 타당성이 충분히 확보되었을 경우 측정모형의 전반적인 적합도 지수에 대한 분석이 이루어진다. 다음의 <표 7>에서 제시한 바와 같이 본 연구의 측정모형에 대한 적합도 지수는 일반적으로 권고하는 수용기준에 전반적으로 양호한 수준에서 부합하는 것으로 확인되었다.

먼저, 연구모형의 자유도가 98이고, χ^2가 197.20로 나타나 χ^2를 자유도로 나눈 값이 2.01이므로 χ^2가 자유도의 3배를 넘지 않아 연구모형은 적절하다고 볼 수 있다. 또한, 전반적인 모형의 적합도를 평가하는 절대 적합도 지수 중 GFI가 0.91, AGFI가 0.88, NFI는 0.93으로 적합도 부합 수준을 만족하는 것으로 나타났다. 특히, 표준부합지수(normed fit index; NFI)의 지수가 0.9보다 클 경우 '잘 부합되는 모형(good fitting model)'으로 해석할 수 있다(강병서, 2002). 그 외 SRMR이 0.45, RMSEA는 0.063로 낮았다. 증분부합지수 중 IFI와 CFI는 0.96로 상당히 높게 나타났으며, 간명부합지수 중 PGFI는 0.66, PNFI는 0.76으로 전체적으로 권고하는 수용기준을 모

<표 7> 측정 하부모형의 적합도 지수

구분	적합도 지수	수용기준	분석결과
절대 부합 지수	χ^2/자유도	≦ 3.00	2.01
	χ^2 자유도(df) p-value	≧ 0.05	197.20 98 0.00
	기초부합지수(GFI)	≧ 0.90	0.91
	표준원소평균잔차(SRMR)	≦ 0.10	0.045
	근사원소평균자승잔차(RMSEA)	≦ 0.08	0.063
증분 부합 지수	수정부합지수(AGFI)	≧ 0.80	0.88
	표준부합지수(NFI)	≧ 0.90	0.93
	관계부합지수(RFI)	1.0 근사시 양호	0.91
	증분부합지수(IFI)	1.0 근사시 양호	0.96
	비교부합지수(CFI)	≧ 0.90	0.96
간명 부합 지수	간명기초부합지수(PGFI)	≧ 0.60	0.66
	간명표준부합지수(PNFI)	≧ 0.60	0.76

두 충족시키는 것으로 나타나 연구의 측정모형이 우수한 적합도를 가진 것으로 평가할 수 있다.

4.4 구조모형 평가 및 연구가설 검증

4.4.1 구조모형의 적합도 평가

본 연구에서 제시된 구조모형에 대한 적합도 지수는 다음의 <표 8>에 나타난 바와 같다. χ^2를 자유도로 나눈 값은 2.03이며, 절대부합지수 중 GFI는 0.91, AGFI는 0.88로 적합한 것으로 나타났다. RMSEA는 0.064, SRMR은 0.054로 낮은 것으로 분석되었다. 또한 증분부합지수에서 NFI는 0.92로 연구모형이 적합하며, AGFI가 0.88, RFI는 0.91, CFI와 IFI가 각각 0.96으로 적절한

<표 8> 구조 하부모형의 적합도 지수

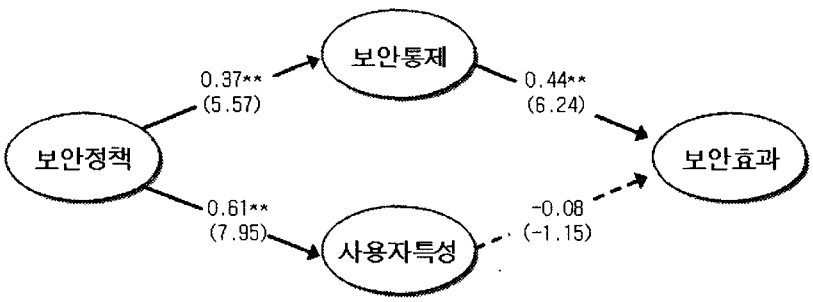
구분	적합도 지수	수용기준	분석결과
절대 부합 지수	χ^2/자유도	≦ 3.00	2.03
	χ^2 자유도(df) p-value	≧ 0.05	203.08 100 0.00
	기초부합지수(GFI)	≧ 0.90	0.91
	표준원소평균잔차(SRMR)	≦ 0.10	0.054
	근사원소평균자승잔차(RMSEA)	≦ 0.08	0.064

증분 부합 지수	수정부합지수(AGFI)	≧ 0.80	0.88
	표준부합지수(NFI)	≧ 0.90	0.92
	관계부합지수(RFI)	1.0 근사시 양호	0.91
	증분부합지수(IFI)	1.0 근사시 양호	0.96
	비교부합지수(CFI)	≧ 0.90	0.96
간명 부합 지수	간명기초부합지수(PGFI)	≧ 0.60	0.67
	간명표준부합지수(PNFI)	≧ 0.60	0.77

것으로 분석되었다. 간명부합지수에서 PGFI가 0.67, PNFI가 0.77로 구조모형 적합도 지수가 전반적으로 우수한 것으로 평가되었다.

4.4.2 연구가설 검정

본 연구에서 연구가설은 연구모형에서 구성개념 사이의 경로로 설정되었다. 구조모형 분석결과는 각 경로의 계수와 t-값으로 확인할 수 있으며, 아래의 <그림 2>에 나타난 바와 같이 사용자특성과 보안효과에 이르는 경로를 제외한 다른 모든 경로는 통계적으로 유의한 영향을 미치는 것으로 나타났다.



<그림 2> 연구의 구조모형의 분석결과

주) 괄호 안은 t-값, **: 유의수준 α=0.01에서 유의함.

각 연구가설에 대한 분석결과를 살펴보면, 먼저 조직의 보안정책과 보안통제 사이의 관계를 규정한 가설 1의 경우 경로계수가 0.37이며, t-값이 5.57로 보안정책이 보안통제에 유의한 영향을 미치는 것으로 확인할 수 있었다. 이로써 조직내 컴퓨터 바이러스 관련 보안정책 수준이 높을수록 보안통제의 수준도 높아지게 된다는 연구가설 1은 채택되었다.

두 번째, 보안정책과 사용자특성 사이의 관계는 경로계수가 0.61이고, t-값이 7.95로 보안정책이 사용자의 특성에 유의한 영향을 미치는 것으로 나타났다. 특히, 다른 경로에 비해 높은 수준에서 경로계수가 나타나 관련성은 상당히 높은 수준으로 볼 수 있으며, 조직내 컴퓨터 바이러스에 대한 보안정책 수준이 높을수록 사용자특성이 높아진다는 가설 2는 채택되었다.

세 번째, 컴퓨터 바이러스의 보안통제 수준과 보안효과사이의 관계는 경로계수가 0.44, t-값이 6.24로 유의한 영향을 미치는 것으로 나타났다. 이를 통해 컴퓨터 바이러스에 대한 보안통제의 수준이 높을수록 보안효과의 수준도 높아진다는 연구가설 3은 채택되었다.

마지막으로 연구가설 4에서 설명하고자 하였던 정보시스템 사용자의 보안관련 지식 및 인지 등의 개인적인 특성과 보안효과 사이의 관계는 경로계수가 -0.08, t-값이 -1.15로 유의한 영향을 미치지 못하는 것으로 나타났으며, 따라서 가설 4는 기각되었다.

4.5 분석결과 논의 및 시사점

본 연구에서는 컴퓨터 바이러스 통제의 효과성에 영향을 미치는 요인을 보안통제 및 사용자특성으로 보고, 또 이 두 요인의 선행요인으로 조직의 보안정책을 설정하여 모형화하고 실증분석을 수행하였다. 분석 결과, 먼저 조직의 정보시스템 사용기준을 제시한 보안정책이 보안통제에 미치는 영향은 유의한 것으로 나타났다. 이는 조직의 보안정책이 명확하게 수립되어 있을 경우 컴퓨터 바이러스의 대응을 위한 적절한 관리활동이 가능해질 수 있음을 의미하는 것으로 보안정책은 조직의 체계적이고 종합적인 정보보안 활동 수행의 전제조건이라는 점을 시사한다.

두 번째로 보안정책이 사용자특성에 미치는 영향도 통계적으로 유의한 것으로 나타났다. 이 또한 조직이 정보시스템을 보호할 수 있도록 명확한 정보보안 규정과 허용기준을 제시해 두었을 경우 사용자는 조직에서 제시한 정보시스템 활용과 관련된 지침 및 절차 등을 수용하고, 컴퓨터 바이러스로 인해 발생되는 사고와 피해 등의 책임 및 권한을 인지함으로써 감염확산의 축소와 피해예방에 노력을 하게 된다는 것이다.

세 번째로 연구가설 3에서 제시한 조직의 보안통제와 보안효과 사이의 관계 또한 통계적으로 유의하게 나타났다. 이는 정보보안을 위한 보안절차, 기술 및 관리적 활동이 원활할 경우 컴퓨터 바이러스에 의해 발생하는 감염의 확산을 방지하거나 감염피해를 축소할 수 있으므로 보안효과를 기대할 수 있다는 것으로 해석할 수 있다. 역으로 조직의 보안관리 활동이 부적절할 경우 정보시스템이 취약성을 가지게 되므로 컴퓨터 바이러스에 의한 공격의 목표가 되고, 이에 따라 보안효과는 낮아지게 된다는 것이다.

네 번째로 연구가설 4에서 제시한 사용자특성과 보안효과 사이의 관계는 통계적으로 유의하지 않은 것으로 나타났다. 이는 사용자 스스로 정보시스템 사용과 관련된 개인적인 책임 및 권한의 인지, 정보시스템과 관련하여 습득한 지식 등은 컴퓨터 바이러스에 의한 공격으로부터 보안효과에 기여하지 못하는 것을 의미한다.

연구모형에서 보안정책과 보안효과 사이에 경로를 추가하여 독립변수가 매개변수를 통해 종속변수에 유의한 영향을 미치는지에 대한 매개효과를 분석해 보았다. 그 결과 경로계수가 -0.05, t-값이 -0.57로 유의하지 않은 것으로 나타났다. 이에 따라 보안통제는 보안정책과 보안효과 사이에 완전매개(full mediation)의 특성을 나타내는 것을 확인할 수 있었다. 즉, 보안정책은 보안효과에 직접적인 영향은 미치지 못하지만 보안통제를 통해 구체화됨으로써 적절한 보안통제를 수립하게 되고, 이는 곧 정보보안에 긍정적인 효과를 미치는 것으로 볼 수 있다.

연구의 분석결과에 따른 시사점은 다음과 같이 도출될 수 있다. 먼저, 컴퓨터 바이러스와 관련하여 조직의 정보보안정책은 상당히 중요한 요인이라는 것이다. 통계적 측면에서 볼 경우 다음의 <표 9>에서 나타난 바와 같이 보안정책이 보안통제와 사용자의 인지적 특성에 직접적으로 상당한 영향을 미치고 있으며, 보안효과에 대해서도 간접효과를 나타내는 경로계수가 0.12, t-값은 2.40으로 앞서 언급된 매개효과를 통해 간접적인 영향을 미치는 것으로 나타났다. 특히, 이러한 결과는 Wen(1998)의 개념적 연구, 즉 조직의 명확한 보안정책은 AV S/W와 더불어 컴퓨터 바이러스를 효과적으로 차단할 수 있다는 것을 실증적으로 분석한 것으로 중요성이 크다고 볼 수 있다. 또한 부적절한 보안정책으로 인해 보안통제 수준이 낮아지게 될 경우 컴퓨터 바이러스에 의한 보안사고를 발생시킬 수 있으므로 관리적 차원에서 보안정책을 정보보안에서 출발점으로 인식하고, 체계적이고 종합적인 보안정책을 수립하고, 조직구성원들에 의해서 지켜야할 의무로써 수용될 수 있어야 할 것이다.

<표 9> 구성개념간 직·간접 효과 분석

구분	보안통제			사용자특성			보안효과		
	직접	간접	전체	직접	간접	전체	직접	간접	전체
보안정책	0.37**	-	0.37**	0.61**	-	0.61**	-	0.12*	0.12*
t-값	5.57	-	5.57	7.95	-	7.95	-	2.40	2.40
보안통제	-	-	-	-	-	-	0.44**	-	0.44**
t-값	-	-	-	-	-	-	6.24	-	6.24
사용자특성	-	-	-	-	-	-	-0.08	-	-0.08
t-값	-	-	-	-	-	-	-1.15	-	-1.15

주) *: 유의수준 α=0.05, **: 유의수준 α=0.01에서 유의함

두 번째 시사점은 컴퓨터 바이러스에 대한 보안통제의 중요성이다. 보안통제와 관련된 제반 보안활동이 적절치 못할 경우 정보시스템은 취약성을 가지게 된다(NIST 1998; Peltier, 2001). 대표적인 사례로 MS-SQL의 취약성을 대상으로 감염피해를 발생시켰던 슬레머 웜의 경우 Microsoft에서 이를 차단할 수 있는 패치(patch) 프로그램을 사건발생 6개월 전에 배포하였음에도 불구하고, 업데이트되지 않은 많은 MS서버들이 공격의 대상이 되었다. 이처럼 검증된 이메일 첨부파일의 열기, AV S/W의 업데이트, 운영체제의 패치 등의 컴퓨터 바이러스 통제와 관련된 기본적인 활동들이 보안효과에 많은 의미를 가지는 것을 알면서도 실행하지 않고 있다면 매우 심각한 것이다. 따라서 조직의 지속적인 보안통제의 시행여부와 효과성에 대한 평가가 이루어져야 할 필요가 있으며, 컴퓨터 바이러스 대응 소프트웨어의 결함 및 결점의 보완, 보안통제의 부적절성과 모순의 수정에 적극성을 가져야 할 필요가 있다(DeMaio, 1989; Barsanti, 1999; Gordineer, 2003).

세 번째 시사점은 컴퓨터 바이러스로 인해 발생하는 보안사고는 더 이상 한 개인의 정보시스

템 사용상의 부주의에 대처하는 문제로 국한되는 것이 아니라 조직적 차원에서 정보시스템과 정보자산의 보안에 대한 인식의 측면에서 제고될 필요성이 있다는 것이다(Loch et al., 1992). 이것은 사용자의 개인적 특성은 조직의 보안정책에 의해 상당한 영향을 받고 있지만 실질적인 보안효과에 기여하지 못하는 것으로 나타난 분석결과에 기초하고 있다.

최근 컴퓨터 바이러스는 사용자를 기만함으로써 감염을 유도하는 방식이 다양해지고, 코드의 변칙성 및 네트워크상에서 빠른 확산 능력 등의 특성을 가지고 있다. 이러한 상황적 특성들로 인해 사용자의 개인적 책임과 권한의 인지 및 정보시스템 관련 지식만으로는 보안효과를 기대하기 힘들며, 조직의 전체적인 관점에서 컴퓨터 바이러스에 대한 대응이 이루어져야 할 필요성을 시사하는 것이다.

마지막으로 최근에 국내외에서 실시된 조사결과와 동일하게 본 연구에서도 컴퓨터 바이러스는 매우 보편적인 정보화 역기능 중의 하나임을 알 수 있다. 흥미로운 점은 대다수의 응답자들이 컴퓨터 바이러스에 의한 침해사고를 한 번쯤 경험해보았지만, <표 3>에서 나타난 바와 같이 많은 응답자들이 조직내 보안정책이 양호하다고 느끼는 것이다. 이는 여러 가지로 해석이 가능한데, 컴퓨터 바이러스가 PC에 침입했지만 실제로 피해를 유발하기 전에 설치된 AV S/W가 검색하여 무력화하였거나, 바이러스가 작동하였더라도 그로 인한 피해의 정도가 미미하기 때문일 수 있다. 그런데, 사용자 개인이 느끼는 직접적인 피해는 다소 사소하더라도 조직 전체의 차원에서 유발되는 기회비용을 포함한 간접적인 피해를 고려하면 보다 더 심각한 문제로 인식되어야 할 것이다.

V. 결 론

컴퓨터 바이러스로 인해 발생하는 피해는 단순히 정보시스템을 정상화하는데 드는 비용만으로 그치지 않는다. 컴퓨터 바이러스에 의한 정보시스템의 서비스 중단은 생산성 손실 및 기회비용의 발생과 주요 정보자산에 대한 노출로 인한 비밀성과 무결성에 손상을 가져온다(Coursen, 1997). 나아가 기업 이미지의 치명적인 훼손도 가능하다. 이처럼 컴퓨터 바이러스는 오늘날 가장 접하기 쉬운 정보보안 문제 중 하나로 본 연구에서는 이로 인해 발생하는 감염사고의 축소와 방지를 위해 조직의 보안정책과 보안통제, 사용자특성이 컴퓨터 바이러스 통제에 영향을 미치는 요인으로 보고 연구모형을 설정하였다.

본 연구를 위해 수집된 데이터를 실증분석한 결과 조직의 보안정책은 보안절차 및 기술과 관리적 측면의 보안통제와 사용자의 인지적 특성을 형성하는데 통계적으로 유의한 영향을 미치는 것으로 나타났다. 또한, 조직의 보안통제는 컴퓨터 바이러스를 통제하는데 상당히 많은 영향을 미치는 것으로 나타났으나, 사용자의 개인적인 특성은 보안효과에 통계적으로 유의한 영향을 미치지 못하는 것으로 나타났다.

마지막으로 본 연구의 한계와 향후 연구과제는 다음과 같다. 먼저, 실증분석을 통해 사용자의

인지적 특성이 보안정책과 밀접한 관련성이 있다는 것을 밝혀내었지만, 사용자의 특성과 컴퓨터 바이러스 통제효과 사이의 관련성은 명확하게 규명해내지 못했다. 향후 연구에서는 사용자의 인지적 측면에서 접근 이외에 사용자의 조직내 역할과 보안효과 측면에서 고려해 봄으로써 정보보안 사고에 있어 사용자의 영향을 분석할 필요가 있을 것이다.

두 번째는 실증분석을 위해 사용된 분석단위의 문제로 본 연구에서는 개별 사용자를 대상으로 설문하고 이에 대한 분석이 이루어졌다. 이는 컴퓨터 바이러스 문제의 특성상 개별 사용자가 가장 흔히 경험하는 정보보안 문제이기 때문에 이에 대한 보안효과를 측정하는데 있어 조직적 차원과 개인적 차원 모두 적용이 가능하다고 보았기 때문이다. 추후 연구에서 조직의 관점에서 보안효과에 대한 분석이 이루어진다면 본 연구 결과와 결합하여 다각적인 분석이 가능할 것이다.

세 번째는 횡단적 연구를 통한 실증분석의 문제점으로 컴퓨터 바이러스에 대한 보안정책 및 보안통제가 구현되어 운영될 때 그 효과가 현실화되기 위해서는 상당한 시간이 필요한 것이 일반적이다. 따라서 보안효과의 시간적인 변화를 고려한 측정을 위해 종단적인 연구를 수행할 필요가 있다고 본다.

참고문헌

강병서, 인과분석을 위한 연구방법론, 무역경영사, 2002.

김세헌, 정보보호 관리 및 정책, 생능, 2002.

채서일, 사회과학조사방법론, 학현사, 2003.

한국전산원, 2003 한국인터넷백서, 한국전산원, 2003

Anderson, J., "An Approach for Confirmatory Measurement and Structural Equation Modeling of Organizational Properties," *Management Science*, Vol. 33, No. 4, 1987, pp. 525-541.

Anderson, J. and D. Gerbing, "Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach," *Psychological Bulletin*, Vol. 103, No. 4, 1988, pp. 411-423.

Bagchi, K. and G. Udo, "An Analysis of the Growth of Computer and Internet Security Breaches," *Communications of the AIS*, Vol. 12, 2003, pp. 684-700.

Bagozzi, R. and Y. Yi, "On the Evaluation of Structural Equation Models," *Journal of the Academy of Marketing Science*, Vol. 16, 1988, pp. 74-97.

Barsanti, C., "Modern Network Complexity Needs Comprehensive Security," *Security*, Vol. 36, No. 7, 1999, pp. 65.

Bergeron, F. and C. Berube, "The management of the end-user environment: An empirical investigation," *Information & Management*, Vol. 14, No. 3, 1998, pp. 107-113.

Blatchford, C., "Information Security Controls - Are They Cost-Effective?," *Computer Audit Update*, 1995, pp. 11-19.

Chordas, L., "Unwelcome Guests," *Best's Review*, March, 2004, pp. 93-96.

Cohen, F., "Computer Viruses: Theory and Experiments," *Computers & Security*, Vol. 6, No. 1, 1987, pp. 22-35.

Consumer Reports, "Computer Security Cyberspace Invaders," *Consumer Reports*, Vol. 67, No. 6, 2002, pp. 16-20.

Coursen, S., "Financial Impact of Viruses," *Information Systems Security*, 1997, Vol. 6, No. 1, 1997, pp. 64-70.

CSE, *Guide to Security Risk Management for IT Systems,* Communications Security Establishment, Government of Canada, 1996.

CSI, *Eighth Annual CSI/FBI Computer Crime and Security Survey*, Computer Security Institute, 2003.

David, J., "The New Face of the Virus Threat," *Computers & Security*, Vol. 15, No. 1, 1996, pp. 13-16.

DeMaio, H., "Virus-A Management Issue," *Computers & Security*, Vol. 8, No. 5, 1989. pp. 381-388.

Fornell, C. and D. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research*, Vol. 18, No. 1, 1981, pp. 39-50.

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

Garver, M., and J. Mentzer, "Logistics Research Methods: Employing Structural Equation Modeling to Test for Construct Validity," *Journal of Business Logistics*, Vol. 20, No. 1, 1999, pp. 33-57.

Gasser, M., *Building a Secure Computer Systems*, Van Nostrand Rienhold Company, 1988.

Gefen, D., D. Straub, and M. Boudreau, "Structural Equation Modeling and Regression: Guidelines for Research Practice," *Communications of the AIS*, Vol. 4, No. 7, 2000, pp. 1-76.

Gefen, D., "Assessing Unidimensionality through LISREL: An Explanation and Example," *Communications of the AIS*, Vol. 12, 2003, pp. 23-47.

Goodhue, D. and D. Straub, "Security Concerns of System Users: A Study of Perception of the Adequacy of Security," *Information & Management*, Vol. 20, No. 1, 1991, pp. 13-27.

Gordineer, J., "Blended Threats: A New Era in Anti-Virus Protection," *Information Systems Security*, Vol. 12, No. 3, 2003, pp. 45-47.

Hancock, B., "First PDA Virus Hits the Airwaves," *Computer & Security*, Vol. 19, No. 7, 2000, pp. 583-584.

Harris, R., "Attitudes Towards End-User Computing," *Behaviour & Information Technology*, Vol. 18, No. 2, 1999, pp. 109-125.

Highland, H., "A History of Computer Viruses: The Famous Trio," *Computer & Security*, Vol. 16, No. 5, 1997, pp. 416-429.

Hoffer, J. and D. Straub, "The 9 to 5 Underground: Are You Policing Computer Crimes?," *Sloan Management Review*, Vol. 30, No. 4, 1989, pp. 35-43.

Hubbard, J. and K. Forcht, "Computer Viruses: How Companies Can Protect Their Systems," *Industrial Management & Data Systems*, Vol. 98, No. 1, 1998, pp. 12-16.

Kankanhalli, A., H. Teo, B. Tan, and K. Wei, "An Integrative Study of Information Systems Security Effectiveness," *International Journal of Information Management*, Vol. 23, No. 2, 2003, pp. 139-154.

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

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

Loch, K., H. Carr, and M. Warkentin, "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly*, Vol. 16, No. 2, 1992, pp. 173-186.

Nachenberg, C., "Computer Virus-Anti Virus Coevolution," *Communications of the ACM*, Vol. 40, No. 1, 1997, pp. 46-51.

NIST, *Risk Management Guide for Information Technology Systems-Recommendations of the National Institute of Standards and Technology*, NIST SP 800-30, National Institute of Standards and Technology, 1998.

Panko, R., "Slammer: The First Blitz Worm," *Communications of the AIS*, Vol. 11, 2003, pp. 207-218.

Peltier, T., *Information Security Risk Analysis*, Auerbach, 2001.

Pipkin, D., *Information Security - Protecting the Global Enterprise*, Hewlett-Packard Professional Books, 2000.

Polk, W. and L. Bassham, *A Guide to the Selection of Anti-Virus Tools and Techniques*, NIST SP 800-5, National Institute of Standards and Technology, 1992.

Post, G. and A. Kagan, "Management Tradeoffs in Anti-Virus Strategies," *Information & Management*, Vol. 37, No. 1, 2000, pp. 13-24.

Russell, D. and G. Gangemi, *Computer Security Basics*, O'Reilly & Associateds, 1991.

Schultz, E., "Virus & Worm Trends," *Computers & Security*, Vol. 23, No. 3, 2003, pp.

179-180.

Segars, A., "Assessing the Unidimensionality of Measurement: A Paradigm and Illustration Within the Context of Information Systems," *Omega*, Vol. 25, No. 1, 1997, pp. 107-121.

Sherif, J. and D. Gilliam, "Deployment of Anti-Virus Software: A Case Study," *Information Management & Computer Security*, Vol. 11, No. 1, 2003, pp. 5-10.

Skoudis, E. and Zeltser, L., *Malware: Fighting Malicious Code*, Prentice Hall, 2003.

Straub, D., "Validating Instruments in MIS Research," *MIS Quarterly*, Vol. 13, No. 2, 1989, pp. 45-60.

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

Straub, D. and W. Nance, "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS Quarterly*, Vol. 14, No. 1, 1990, pp. 45-60.

Straub, D. and R. Welke, "Coping with System Risk: Security Planning Models for Management Decision Making," *MIS Quarterly*, Vol. 22, No. 4, 1998, pp. 441-469.

Szor, P., *The Art of Computer Virus Research and Defense*, Addison-Wesley, 2005.

Thatcher, J. and P. Perrewé, "An Empirical Examination of Individual Traits as Antecedents to Computer Anxiety and Computer Self-Efficiency," *MIS Quarterly*, Vol. 26, No. 4, 2002, pp. 381-396.

Viveros, S., "The Economic Impact of Malicious Code in Wireless Mobile Networks," *4th International Conference on 3G Mobile Communication Technologies*, 2003, pp. 1-6.

Wack, J. and L. Carnahan, *Computer Viruses and Related Treats: A Management Guide*, NIST SP 500-166, National Institute of Standards and Technology, 1989.

Wen, H., "Internet Computer Virus Protection Policy," *Information Management & Computer Security*, Vol. 6, No. 2, 1998, pp. 66-71.

Whitman, M., "In Defense of the Realm: Understanding the Threats to Information Security," *International Journal of Information Management*, Vol. 24, No. 1, 2004, pp. 43-57.

<Abstract>

The Effects of Information Security Policies, Security Controls and User's Characteristics on Anti-Virus Security Effectiveness

Jong-Ki Kim · Jin-Hwan Jeon · Ho-Seob Lim

Current computer viruses are one of the most serious problems in information age due to their potential demage and impact on use of information systems. To make the problem worse, virus development technology has been advanced rapidly, and use of network systems has expanded widely. Therefore computer viruses are much more complex and use of anti-virus software(AV S/W) is not enough to prrevent virus incidents. It implies that computer viruses as well as other information security matters are not solely a technical problem but also a managerial one.

This study emphasized on computer virus controls from managerial perspective of information security and investigated factors influencing the effectiveness of computer virus controls. Organization's comprehensive security policies provide guidelines on how organization or individual can protect themselves from computer viruses. Especially, user's education has positive impact on user's security related characteristics.

Based on the analysis of research model using structural equation modeling technique, security policies were influencing security controls and improving user's computer viruses related awareness. Also security controls had positive impact on security effectiveness. However, no significant relationship was found between user's security related characteristics and security effectiveness.

Keywords: Computer Virus, Security Policy, Security Controls, User Characteristics, Security Effectiveness

* 이 논문은 2005년 12월 22일 접수하여 1차 수정을 거쳐 2006년 2월 10일 게재 확정되었습니다.