情報保護學會論文誌
第16卷 第5號, 2006. 10

대기업과 중소기업 간의 정보보안 요소에 대한 사용자의 인지 비교: 컴퓨터 바이러스를 중심으로

김 종 기[1†], 전 진 환[2‡]

[1]부산대학교, [2]부산대학교 금융·증권·선물 교육연구사업단

Comparison of Users' Perception of Information Security Elements on Computer Virus Between Large and Small-and-Medium Companies

Jongki Kim[1†], Jinhwan Jeon[2‡]

[1]Pusan National University, [2]Research and Education Institute of Banking, Securities and Derivatives of Pusan National University

요 약

컴퓨터 바이러스는 정보화 시대에 사용자들이 가장 흔하게 경험하는 정보보안 문제 중 하나이다. 본 연구에서는 컴퓨터 바이러스를 대상으로 대기업과 중소기업간 보안요소에 대한 사용자의 인지도 차이를 분석하였다. 설문지를 이용하여 수집된 자료에 대하여 t-test를 이용하여 기업규모별 인지차이를 분석한 결과 보안위협과 위험을 인지하는데 별다른 차이가 없는 것으로 나타났으며, 컴퓨터 바이러스에 대한 위협과 피해를 심각하게 고려하는 것으로 확인되었다. 또한, 사용자들은 전반적으로 소속된 조직의 보안정책 수준에 대해 만족하고 있으나 보안정책을 인지하는데 차이가 있으며 기업규모별 보안정책 집행의 효과에 차이가 있음을 확인하였다. 또한 바이러스에 대한 정보자산, 보안취약성, 보안효과를 인지하는데 차이가 있는 것으로 나타나 기업규모별 자산의 중요도와 위협의 노출정도, 바이러스 감염방지 노력의 결과가 상이한 것으로 분석되었다.

ABSTRACT

Computer virus is one of the most common information security problems in the information age. This study investigates the difference of users' perception of security elements between large companies and small-and-medium companies on the subject of computer virus. Based on t-test, no significant difference is found in users' perception on security threat and security risk. While users satisfy with the level of security policy, there is a significant difference on the level of security policy recognition between the two sizes of companies. Moreover, there are significant differences on information assets, security vulnerability and security effectiveness, which implies difference in the users' perception on importance of assets, exposure to threats and computer virus prevention efforts between large and small-and-medium companies.

Keywords : *computer virus, security policy, security risk, security effectiveness, security perception*

Ⅰ. 서 론

오늘날 기업은 생산성 향상뿐만 아니라 경영전략적

접수일: 2006년 6월 28일; 채택일: 2006년 8월 22일
† 주저자, jkkim1@pusan.ac.kr
‡ 교신저자, jeonjinhwan@pusan.ac.kr

차원에서 정보시스템을 적극적으로 활용하고 있다. 이에 따라 정보시스템과 관련된 하드웨어 및 소프트웨어, 내·외부 네트워크 등의 정보통신 인프라의 안전성이 확보되지 못할 경우 정보자산에 치명적인 위협이 가해질 수 있으므로, 정보자산의 효과적인 관리를 위한 위험관리는 정보보안에 있어 핵심적인 요소 중의 하나로 여겨지고 있다.

정보보안(information security)은 다양한 내·외적인 위협들로부터 조직의 손실을 최소화하고 이익을 최대화하기 위해 정보자산을 보호하는 것을 의미한다[1][2]. 이때 위협은 그 원천에 따라 다양한 형태로 나타날 수 있으며, 컴퓨터 바이러스에 의한 위협은 사용자들이 가장 흔하게 경험하는 정보보안 문제이며, 정보보안에 미치는 파급효과가 매우 큰 위협 중의 하나이다[3][4][5]. 더욱이 정보기술 발전에 따른 다양한 공격기법과 함께 새로운 침입패턴의 등장은 바이러스에 의한 피해를 한층 더 증가시키는 계기가 되고 있다[6][7].

바이러스의 발생 이후에 백신이 제작되는 바이러스 대응 소프트웨어(Anti-Virus(AV) S/W)의 태생적인 한계는 사용자로 하여금 감염발생 이전에 예방활동에 대한 관심을 가져야 할 필요성을 제기하고 있다[8]. 이를 위해 바이러스 탐지 기술뿐만 아니라 관리적 측면에서 사용자의 정보보안에 대한 이해가 뒷받침되어야 할 필요가 있다. 특히, 최근 등장한 스파이웨어의 경우 컴퓨터에 설치되어 사용자의 통제권한을 제한하거나 주요정보를 빼내기 때문에 사용자의 역할이 무엇보다 중요하다. 일례로 2005년 3월 발생한 영국 스미토모 은행의 절도사건은 키로거에 의한 패스워드와 계정정보가 유출된 사건으로, 사용자 부주의에서 발생한 여러 사건 중 하나에 지나지 않는다[9].

중소기업은 대기업에 비해 정보시스템의 보안 취약점에 대한 파악 수준이 낮고 보안에 대한 투자도 낮기 때문에 효과적인 바이러스 예방을 위해서는 사용자 및 운영자의 정보보안에 대한 인식 제고가 더욱 더 필요하다. 따라서 본 연구에서는 정보시스템 사용자를 대기업과 중소기업의 두 집단으로 나누어 위험분석방법론에서 적용되는 자산, 취약성, 위협, 위험의 보안요소와 함께 보안정책과 사용자특성에 대해 평가하도록 함으로써 컴퓨터 바이러스 관련 보안인지도의 차이를 실증적으로 검증하고자 한다.

II. 정보보안 요소

2.1 보안정책

보안정책은 정보시스템을 보호하기 위해서 수립된 조직의 제반 규정과 절차를 의미[10][11]하는 것으로, 잘 수립된 보안정책은 성공적인 정보보안의 핵심이라 할 수 있다. 정보보안정책은 크게 예방적 정책과 억제적 정책의 두 가지로 구분할 수 있다. 예방적 정책은 사용자의 정보시스템 오·남용을 통제함으로써 허용되지 않는 행위를 사전에 방지하고자 수립된 보안정책으로 암호시스템이나 접근통제의 활용을 예로 들 수 있다[12]. 컴퓨터 바이러스와 관련한 예방적 정책으로는 사용자의 바이러스 관련 교육, 보안사고 사례공지, 송·수신전 데이터의 검사 등이 있다[13].

억제적 정책은 사용자에게 정보보안의 준수 의무를 위반한 경우 처벌의 확실성과 심각성을 강조함으로써 악의적 의도를 가진 사용자에게 처벌의 두려움을 심어주어 유사행위를 방지할 수 있도록 수립된 보안정책이다[12]. Hoffer & Straub[14]는 정보보안 위반 사례가 발생한 경우 해당 사용자의 지위나 권한에 따라 처벌수준을 차별화한다면 좀 더 효과적인 제재가 가능함을 강조하였다.

최근 웜, 스파이웨어, 피싱 등 악성 프로그램들은 빠른 확산력을 기반으로 감염사고를 발생시키고, 감염 목적 또한 기존 파일감염 등의 단순한 증상을 벗어나 사용자 인증정보 혹은 금융정보를 유출하고자 하는 의도를 가지고 있다[5][7]. 이에 반해 바이러스 예방을 위해 사용되는 AV S/W는 이미 알려진 컴퓨터 바이러스에 대한 차단효과를 가질 뿐 새로 출현한 바이러스에 대한 백신이 개발되기 전까지는 감염에 대한 원활한 대응이 매우 어렵다[15].

바이러스의 감염으로부터 정보시스템을 보호하기 위한 가장 좋은 보안정책으로 철저한 사용자 보안교육을 들 수 있다[16]. 컴퓨터 바이러스는 다른 보안위협과 달리 제작자의 의도에 따라 감염증상과 침입양상이 달라질 수 있으므로 사용자들의 보안 프로그램의 참여를 통한 바이러스 관련 보안지식과 정보시스템 오·남용에 따른 손실에 대한 인지는 바이러스 차단효과를 높일 수 있다[10]. 또한 AV S/W의 꾸준한 업데이트 노력은 바이러스 출현에 대한 지속적인 경계를 유지하게 하며, 침해사고 발생 이후 신속한 대응이 가능하게 하므로 사용자 보안교육은 보안대책에 있어 핵심적인 요소라 할 수 있다[17].

2.2 사용자특성

정보시스템 및 네트워크의 보안필요성과 강화를 위해 사용자의 보안관련 이해는 필수적이다. 이러한 사용자의 인지적 특성은 이미 Frank 등[18]의 PC 보안 연구에서 지적된 바 있으며, 사용자의 지식, 비공식적 행동규범 및 공식적 보안정책의 요인들 사이에 높은 상관관계가 나타났다. 또한 보안정책과 규범은 사용자의 지식수준이 낮을 때 상당한 수준의 영향을 미치는 것으로 나타났다.

Wen[19]은 컴퓨터 바이러스 차단의 필요성을 인지하고 있는 사용자, 바이러스 탐지 및 확산방지를 위한 보안제품, 구형 및 신형 바이러스에 대한 포괄적인 보안절차가 적절히 융합될 경우 효과적인 바이러스의 대응 및 차단이 가능함을 논하였다. 이처럼 사용자의 인지적 특성과 관련하여 개인적 특성, 환경, 인구통계학적 변수를 포함한 개인적 차별성이 정보기술 사용 관련 믿음에 영향을 미칠 수 있게 되며[20], 조직의 정책수립의 측면에서도 사용자의 태도에 따라 억제적 혹은 예방적 보안정책의 적용이 달라질 수 있으므로 사용자 개인의 인지적 특성은 정보보안의 핵심적 요소 중의 하나라 할 수 있다[13].

2.3 정보자산

정보보안은 보호되어야 할 자산이 무엇인지 식별하고 각 자산의 가치를 평가하는데서 시작된다[21]. 자산은 정보시스템을 구성하는 하드웨어, 소프트웨어, 데이터, 인적자원, 각종 문서 등이 포함되는데 그중에서 정보보안의 가장 중요한 대상은 각종 데이터, 내부문서, 비즈니스 관련 문서 등을 포함하는 정보자산이다[22][23].

자산의 식별과 평가는 보안위험의 결정에 필수적인 부분이며[22], 정보자산의 보호수준은 해당 자산의 중요도와 잠재적 가치의 평가를 통해 결정된다[22][23][24]. 최근 컴퓨터 바이러스의 위협이 증가함에 따라 기존 저장매체 및 소프트웨어의 감염을 벗어나 사용자의 인증정보[25][26]라든지 거래내역, 신용카드번호 등의 금융정보[26][27]도 공격의 대상이 되고 있으며, 이들 정보들이 외부로 유출될 경우 범죄에 악용될 가능성이 높기 때문에 관리적 측면에서 상당한 주의가 요구된다.

2.4 보안위협

정보자산은 여러 위협의 공격대상이 된다. 위협은 정보시스템 혹은 정보기술과 관련되어 있는 자산에 대해 의도하지 않은 결과를 초래하는 의도된 혹은 비의도적인 요인이며[22][23], 원천에 따라 자연 발생적인 위협(화재, 수재, 정전 등), 인간에 의한 의도적인 위협(정보자원에 대한 파괴, 절취, 컴퓨터 바이러스, 해킹 등), 그리고 비의도적인 위협(시스템의 조작 미숙, 소프트웨어, 하드웨어, 통신장비 등 시스템 결함)으로 구분된다[2][28].

컴퓨터 바이러스는 응용 프로그램이나 운영체제 자체의 보안 결함을 이용해 비정상적인 방식으로 시스템에 접근을 시도하거나 공격하는 양상을 취한다[29]. 특히, 스파이웨어, 에드웨어 등과 같은 최근의 컴퓨터 바이러스는 인터넷을 통해 사용자의 개인정보를 복사하여 전송하거나, 팝업 광고창을 지속적으로 띄움으로써 업무를 방해한다든지 혹은 사용자의 컴퓨터 사용습관을 모니터링 함으로써 피해를 유발하는 것이 문제가 된다[16][30].

2.5 취약성

취약성은 정보시스템을 보호하기 위한 충분한 통제가 부족하든지 정보시스템의 치명적인 결함, 보안대책의 부적절한 집행 등에 의해 발생할 수 있으며, 보안위협에 의한 정보시스템의 공격목표가 되는 곳을 의미한다. 위험분석에 있어 취약성은 정보시스템의 손실을 유발하는 조직, 보안절차, 인력, 하드웨어, 소프트웨어 등의 약점 또는 결함을 의미하는 것으로 자산의 특성에 따라 많은 원천들을 포함하고 있다[31][22]. 해당 자산의 특성이 변경되지 않는 한 취약성은 그대로 남아 있으며[23], 위협에 의해 취약성이 현실화되기 전까지는 잘 드러나지 않는 특징이 있다[25].

특히, 컴퓨터 바이러스는 사용자가 검증되지 않은 소프트웨어를 설치한다든지 바이러스가 포함된 스팸메일을 활성화 시키는 부주의에 의해서 감염되는 경우가 많으므로 주의할 필요가 있다[32][33]. 덧붙여, 인터넷과 조직내 공유 네트워크의 취약성을 이용한 시스템 버퍼의 오버플로우, 사용자의 URL 입력 오류 또는 시스템 인증 암호의 노출 등의 취약성은 보안위험을 초래할 수 있으므로 주의해야 한다[11].

2.6 위험인지

위험분석방법론에서 위험은 자산이 가진 취약성이 위협에 의해 현실화됨으로써 조직의 피해나 손실을

발생시키는 것을 의미하는 것으로[23], 위험에 노출된다는 것은 불법적인 데이터의 유출, 파괴, 제거, 수정 등의 피해를 초래할 수 있다[31]. CSI 보고서[34]에 의하면 컴퓨터 관련 범죄 중 컴퓨터 바이러스에 의한 금전적 손실이 가장 큰 것으로 나타났으며, 그 뒤를 이어 서비스 거부(DoS)와 정보시스템에 대한 불법적 접근으로 나타나 바이러스에 의한 보안침해가 매우 심각함을 지적하였다.

컴퓨터 바이러스에 의한 감염은 정보시스템에 여러 유형의 피해를 입히게 된다. 먼저, 감염이 발생했을 경우 빠른 확산을 위한 시스템 리소스의 활용은 정보시스템을 이용한 업무처리에 차질이 불가피하고, 차단이후 사용자로 하여금 응용 프로그램과 데이터에 불신을 초래한다[12][35]. 한편으로 고객의 입장에서 감염사고로 인한 비정상적인 서비스가 제공될 경우 불만족의 원인이 될 수 있으며, 감염사고로 인하여 기업 이미지의 훼손은 물론 재무적 영향까지 야기할 수 있어 심각성을 더하게 된다[36].

2.7 보안효과

정보보안에 대한 투자가 보안관련 사고의 감소에 효과적인지에 대한 평가는 매우 중요하다[14]. 이러한 평가를 통해서 관리자들에게 보안투자에 대한 가치를 알리고, 침해사고와 보안대책과의 관계를 밝힘으로써 추후 사용자의 정보시스템 오·남용과 관련된 보안사고를 감소하는데 기여할 수 있기 때문이다.

정보보안에 대한 지속적인 통제노력은 추후 컴퓨터 바이러스에 의한 손실발생 가능성을 감소할 수 있기 때문에 보안효과로 직결된다고 볼 수 있다[13][37][38]. 그리고 감염발생 이후 사용자의 컴퓨터 바이러스에 대한 인지는 기존 시스템에 잔존해 있는 보안위험을 축소할 수 있기 때문에 보안효과에 기여할 수 있게 된다. 그러나 보안효과는 오·남용 사건에 대한 정확한 평가가 어렵고, 보안사고에 의해서 발생한 실제 손실을 정확히 알 수 없기 때문에 정량적인 측정이 매우 어렵다[14].

Ⅲ. 실증분석

3.1 연구가설

컴퓨터 바이러스 통제를 위한 대기업과 중소기업의 사용자간 보안요소에 대한 인지 차이를 분석하기 위해 다음과 같이 연구가설을 수립하였다. 먼저, 가설 1은 기업규모별 보안정책의 차이가 있음을 살펴본다. Hubbard & Forcht[17]의 연구에서 대부분의 조직들이 바이러스의 차단을 위해 AV S/W를 설치하여 사용하고 있으나 신종 바이러스의 빈번한 출현에 따라서 AV S/W의 주기적인 업데이트와 더불어 새로운 바이러스의 출현에 대해서 항상 주의 깊은 관심을 가져야 한다고 지적하였다. 바이러스 대응을 위한 사용자의 행동 지침은 보안정책에 기반을 두게 되는데, 일반적으로 중소기업에 비해 투자 여력이 더 많은 대기업은 보다 체계적인 보안정책의 수립이 가능하며, 이는 곧 사용자가 인지하는 보안정책의 수준에 차이로 귀결된다.

〔가설 1〕 기업규모별로 사용자가 인지하는 보안정책의 수준에 차이가 있다.

다음 가설 2는 사용자의 인지적 차별성을 설명하기 위해 수립된 가설로, 기업규모에 따라 정보시스템 관련 지식 및 바이러스 감염 피해에 대한 사용자의 인지에 차이가 발생한다는 것이다. 사용자들의 보안관련 이해의 차이는 정보시스템 환경이나 시스템의 변화에 대한 빠른 감지가 가능하며, 보안지식의 습득 등 바이러스의 감염으로부터 위험을 감소시킬 수 있도록 적절한 행동기회를 증가시키게 된다. 이는 사용자의 정보보안 이해가 바이러스 감염예방과 차단 등의 사고발생에 따른 적절한 대응방식을 선택할 수 있도록 하기 때문이다. 특히, 기업규모에 따라 정보보안에 대한 투자의 차이로 인해 보안교육의 수준에 차이가 있을 수 있으며, 따라서 대기업과 비교하여 중소기업의 사용자의 보안관련 이해에 차이가 발생할 것이다.

〔가설 2〕 기업규모별로 사용자의 정보보안 인지 특성에 차이가 있다.

가설 3은 사용자가 인지하는 정보자산의 중요도가 기업규모에 따라 달라질 수 있음을 설명하기 위해 수립되었다. 조직의 정보자산에는 하드웨어, 소프트웨어, 데이터, 정보서비스 등이 포함되며[12], 이들 정보자산들은 기업의 산업내 경쟁우위를 지키기 위한 핵심가치를 포함하고 있기 때문에 해당 정보자산의 노출을 방지하기 위한 지속적인 노력이 요구되고 있는 실정이다. 특히, 자산의 중요도에 따라 이를 분류하고 보호하기 위한 정보보안 투자규모가 달라질 수 있으며, 이로 인한 기업규모별 적절한 보안수준의 차이가

발생하게 된다[26]. 따라서 사용자가 인지하는 정보자산의 중요성은 기업의 규모와 환경적 특성에 따라 달라질 수 있으며, 이를 다음의 가설 3과 같이 수립할 수 있다.

〔가설 3〕 기업규모별로 정보자산을 인지하는데 차이가 있다.

가설 4는 컴퓨터 바이러스에 대한 보안위협을 기업규모에 따라 사용자들이 다르게 인지함을 설명하기 위해 수립되었다. 보안위협은 정보시스템 또는 서비스에 의해 다루어지는 정보에 대해 직접 또는 간접적인 공격요인을 의미하는 것으로 컴퓨터 바이러스의 범주에 포함되는 웜, 스팸, 스파이웨어 등의 악성 프로그램 등은 정보시스템에 피해를 입히고자 인위적으로 만들어진 보안위협 중의 하나이다[23]. 이와 같은 컴퓨터 바이러스 침입에 대한 보안위협의 발생가능성과 심각성을 사용자가 인지하는데 기업규모에 따라 달라질 수 있음을 다음의 가설 4에서 설명하고자 한다.

〔가설 4〕 기업규모별로 보안위협을 인지하는데 차이가 있다.

가설 5는 사용자가 바이러스에 대한 정보시스템의 보안취약성을 인지하는데 차이가 있음을 설명하기 위해 수립되었다. 컴퓨터 바이러스에 의한 위협은 다양한 공격패턴과 기법을 이용하여 서버나 인터넷 등의 특정 취약점을 주요 침입경로로 설정하며, 공격에 성공한 경우 감염이 빠르게 확산된다. 정보시스템의 결함의 존재는 정보자산에 치명적인 손실로 이어지기 때문에 이와 같은 약점을 확인하고 분류하여 위협에 대비하는 것은 매우 중요하다. 조직규모에 따라 정보보안에 대한 투자 수준이 달라지며, 이에 따라 보안대책의 수준에도 영향을 미쳐 정보시스템에 잔존하는 취약성에 대한 사용자의 인지에 차이를 유발할 수 있음을 다음 가설로 수립하였다.

〔가설 5〕 기업규모별로 보안취약성을 인지하는데 차이가 있다.

가설 6은 바이러스 감염에 의한 정보시스템의 피해를 기업별 사용자에 따라 다르게 인지함을 설명하기 위해 수립하였다. Mtembu & Cairns[39]은 컴퓨터 범죄와 관련된 위험으로 금전적 손실뿐만 아니라 시장점유율의 감소, 혹은 서비스 부인으로 인한 대외 이미지 추락, 시장내 평판에 부정적인 영향을 미칠 수 있으며, 이러한 위험은 사용자의 잘못된 실수나 범죄의 악용기회가 높아질수록 증가하게 된다. 특히, 바이러스에 의한 감염사고는 사용자의 부주의에 의한 발생과 확산이 대부분이며, 이는 감염피해에 대한 사용자의 인지적 차이에서 발생하는 것으로 볼 수 있다.

〔가설 6〕 기업규모별로 보안위험을 인지하는데 차이가 있다.

다음의 가설 7은 컴퓨터 바이러스로부터 피해를 축소 및 차단하기 위해 집행되는 여러 방지대책과 보안투자가 기업규모별 정보보안 효과의 차이로 나타날 수 있음을 설명하기 위해 수립된 가설이다. 즉, 컴퓨터 바이러스의 예방을 위해 조직의 보안시스템의 개발과 유지에 충분한 금액을 투자했을 경우 성공과 실패에 따라 사용자의 만족도가 달라질 수 있다. 이러한 효과의 차이는 기업의 규모에 따라 차이가 발생할 수 있다.

〔가설 7〕 기업규모별로 보안효과를 인지하는데 차이가 있다.

3.2 측정항목의 조작적 정의

3.2.1. 보안정책

본 연구에서 보안정책은 조직에서 컴퓨터 바이러스를 포함한 정보보안 침해사고의 예방효과를 높이기 위해 수립한 일련의 보안규칙과 보안절차로 정의한다. 특히, 컴퓨터 바이러스와 관련된 보안정책의 평가를 위해 정보보안 관련 연구에서 제시하고 있는 컴퓨터 바이러스 인식 프로그램 활용[10][13], 정보보안 교육[13][14][19], 대내·외 보안사고 사례공지[13][19], 송·수신전 데이터 검사[13], 업무 연속성 계획[4][14][40], 정보시스템 접근통제[12][41], 보안 시스템 활용[11][12][17][42] 등의 항목을 통해 측정하였다.

3.2.2 사용자특성

사용자특성은 보안관련 행동에 영향을 미치는 사용자의 개인적 차별성으로 정의를 하고, 개인적 책임(의무) 인지정도, 정보보호 정책의 인지정도[43][44], 사용자의 PC 활용 정도[18][44][45], 정보시스템 관련 인지도 및 PC 관련 지식[18][42], 보안 관련 지식 정도[20][46] 등으로 평가하였다.

3.2.3 정보자산

정보자산은 조직에서 보호할 가치가 충분히 있는 것으로 정의하고, 측정을 위한 항목으로 컴퓨터 바이

러스에 의해 피해가 발생할 수 있는 정보시스템 사용자의 신분, 급여내역 등과 관련된 개인정보[25][26], 거래내역, 신용카드 번호 등과 같은 민감한 고객정보[26][27] 등을 포함하였다. 또한, 정보시스템에서 개인의 ID와 패스워드와 같은 사용자 인증정보[47] 및 조직의 업무와 관련된 사업정보 또는 기업의 수익, 비용, 이익 등에 관한 재무정보, 시장 정보, 마케팅 전략 등[26]의 대외적으로 유출될 경우 심각한 피해를 유발할 수 있는 정보자산들로 평가하였다.

3.2.4 보안위협

보안위협은 컴퓨터 바이러스에 의한 정보시스템의 위협 정도와 심각성으로 정의하였다. 바이러스의 감염은 어플리케이션 또는 시스템 자체의 보안 결함이 있을 경우 불법적인 시스템 접근을 시도하거나 공격하는 방식을 취할 수 있으며[29], 주로 시스템 내부로 침입하여 자기복제를 통해 프로그램을 감염시키게 되며, 메모리나 디스크의 정보를 읽고 쓰기가 불가능하게 만들거나 내용을 삭제하기도 한다[36][48]. 또한, 프로그램의 강제종료, 파일크기 변경 등의 원치 않는 기능들을 실행시키고[4][29][49], 사용자 인증을 위한 ID와 패스워드를 절취할 수 있으므로[36][47] 이러한 위협에 대한 심각성을 사용자들이 평가토록 하였다.

3.2.5 취약성

취약성은 정보자산이 가지는 내재적인 약점으로 본 연구에서는 바이러스의 위협에 의해 정보자산에 해로운 영향을 미치는 것이 가능하도록 하는 보안통제의 결여 또는 결함으로 정의하였다. 이러한 취약성은 최신 바이러스에 대응하기 위한 조직내 충분한 보안통제가 부족하거나 기존 통제방식 등이 부적절하게 활용될 경우 증가하게 되며[11][26], 바이러스와 관련한 기존 보안통제의 비효과성[26][29], 소프트웨어의 결함[11][29][50], 네트워크를 통하여 다수의 익명접근권한을 부여함으로써 오·남용의 용이성[29][50] 등이 포함된다.

3.2.6 위험인지

위험인지는 컴퓨터 바이러스에 의한 침해사고가 발생했을 경우 정보시스템에 발생하는 여러 손실과 피해의 사용자 인지 정도로 조작화하여 평가하였다. 먼저 바이러스 감염이 발생한 경우 통상적인 업무처리가 원활하게 이루어지지 못하는 경우가 흔하며, 이로 인한 생산성 손실은 불가피하게 된다. 또한 사용자들은 정보시스템의 응용 프로그램과 데이터, 파일에 대해 불신[12][35]과 사용자의 인증정보가 유출될 경우 정보자산에 대한 불법적인 접근을 허용함으로써 프라이버시가 침해당할 수 있게 된다[4][36][47]. 또한 전반적인 시장 이미지 훼손, 명성의 상실 등 조직적 차원에서 치명적인 피해가 발생하게 된다[25][51][52].

3.2.7 보안효과

보안효과는 컴퓨터 바이러스 방지를 위한 조직의 지속적인 통제노력에 대한 사용자의 만족도로 정의하였다. 이를 위해 기존연구에서 제시하고 있는 적절한 패스워드의 분배, 보안수준에 따른 데이터와 프로그램의 분류, 의심스러운 활동에 대한 관리감독을 통해 피해발생 건수와 손실금액의 축소[42], 사용자의 정보시스템에 대한 적정수준의 관심 및 인지도의 증가를 통한 기존 보안대책의 만족도[44]를 측정함으로써 보안효과를 평가하고자 하였다. 또한, 컴퓨터 바이러스와 관련하여 침해사고 발생시 정보시스템과 손상된 데이터의 손실액에 대한 사용자의 평가[13]도 포함하였다.

3.3 연구도구의 개발

본 연구를 위해 사용된 설문지는 측정항목의 조작적 정의를 기반으로 설문문항으로 개발되었고, 설문항목의 내용이 적절한지 평가하기 위하여 전문가 의견조사와 선행조사(pilot test)의 두 단계로 구성된 사전조사를 실시하였다. 먼저, 해당 전공교수와 정보보안 관련 전문가에게 설문항목이 응답자가 쉽게 이해할 수 있는지에 대한 의견을 구하여 설문항목을 수정하였다.

1차 사전조사(pretest)에서는 일반대학원생 40명을 대상으로 실시되었다. 이를 통해 연구개념이 제대로 전달되는지에 대해 중점적으로 파악하였으며, 응답자들이 이해하기 힘든 항목에 대해 직접 표시하도록 하여 이를 토대로 설문문항의 수정에 참고하였다. 수정된 설문문항을 이용하여 본설문조사의 표본과 동일한 부산·경남지역의 2개 대학의 경영대학원생 64명을 대상으로 2차 예비조사(pilot test)를 수행하였으며, 연구개념의 적절성을 포함한 연구도구의 타당성을 확인할 수 있었다.

3.4 표본집단의 인구통계

본 연구에서는 부산·경남지역 4개 대학교의 경영대학원생을 대상으로 설문조사가 실시되었다. 설문지

배포에 앞서 설문의 목적과 취지를 설명하여 설문의 도를 명확히 전달하고자 하였으며, 연구자가 직접 설문지를 배포하고 회수하였다. 경영대학원생들을 연구 표본으로 선정한 이유는 야간에 수업이 진행되는 특수대학원의 특성상 거의 모든 학생이 직장을 가지고 있기 때문에 조직내 바이러스 감염에 대비하여 수립된 바이러스 관련 보안정책의 인지 및 정책집행의 효과성을 측정하는데 적절하다고 판단하였기 때문이다.

설문조사에서 총 260부의 설문지가 배포되었으며, 회수된 221부 중 성실하게 응답하지 않았다고 판단되는 11부를 제외한 210부(95.5%)가 최종분석에 사용되었다. 대기업과 중소기업의 구분은 관련 법규에 따라 분류기준이 매우 복잡한데, 본 연구에서는 종업원 300명 이상인 경우 대기업으로 분류하고 그 미만은 중소기업으로 구분하였다. 전체 응답자 중의 90명(42.9%)이 대기업에서 근무하고 120명(57.1%)은 중소기업에서 근무 중인 것으로 나타나 조직규모별 응답자의 인지 차이를 설명하는데 적절한 구성비를 가진 것으로 판단된다.

표본집단을 성별에 따라 분류하면 남성이 177명(84.3%), 여성은 33명(15.7%)이며, 여성 중 대기업에 근무 중인 응답자는 7명(7.8%)으로 상대적으로 낮은 구성비를 보인다. 표본집단의 연령대를 보면 평균나이는 39.9세이다. 아래의 표 1과 같이 20대에서 50대 중반까지 분포하고 있으며, 연령별로 보면 40대가 49%, 30대가 38.6%로 응답자의 대부분을 차지하고 있다.

표 1. 표본집단의 연령 기술통계

구분	기업규모		전체
	대기업	중소기업	
20대	6(6.7%)	7(5.8%)	13(6.2%)
30대	36(40.0%)	45(37.5%)	81(38.6%)
40대	46(51.1%)	57(47.5%)	103(49.0%)
50대	2(2.2%)	11(9.2%)	13(6.2%)
합계	90(100.0%)	120(100.0%)	210(100.0%)

응답자들에게 지난 한 해 동안 컴퓨터 바이러스에 의한 감염사고 발생 경험을 묻는 질문은 표 2와 같이 전체 83.8%(176명)의 응답자가 감염사고를 경험해 본 것으로 나타났다. 특히, 중소기업의 경우 90%의 응답자가 감염사고를 겪었던 것으로 나타나 대기업에 비해 바이러스 관련 보안문제가 더 심각한 것으로 확인되었다.

표 2. 표본집단의 감염사고 경험 기술통계

구분	기업규모		전체
	대기업	중소기업	
있음	68(75.6%)	108(90.0%)	176(83.8%)
없음	22(24.4%)	12(10.0%)	34(16.2%)
합계	90(100.0%)	120(100.0%)	210(100.0%)

또한, 다음의 표 3과 같이 감염사고를 경험해 본 176명을 대상으로 감염횟수와 관련된 질문에서 감염사고를 한 번 경험해 보았다는 응답자가 전체 34.1%인 60명이었으며, 두 번 경험한 응답자는 50명(28.4%)이었다. 그리고 3회 이상 경험한 사용자도 전체의 37.5%로 나타났으며, 더욱이 중소기업의 경우 전체의 77명(71.3%)의 응답자가 2회 이상 경험한 것으로 나타나 대기업에 비해 바이러스 감염 경험이 더 많은 것으로 조사되었다.

표 3. 표본집단의 감염사고 발생횟수 기술통계

구분	기업규모		전체
	대기업	중소기업	
1회	29(42.6%)	31(28.7%)	60(34.1%)
2회	16(23.5%)	34(31.5%)	50(28.4%)
3~4회	17(25.0%)	34(31.5%)	51(29.0%)
5~9회	5(7.4%)	8(7.4%)	13(7.4%)
10회 이상	1(1.5%)	1(0.9%)	2(1.1%)
합계	68(100.0%)	108(100.0%)	176(100.0%)

컴퓨터 바이러스에 의해 발생된 피해는 다음의 표 4와 같이 대부분의 응답자들이 시스템 및 네트워크의 속도저하(51.1%)를 선택하였으며, 그 뒤를 이어 소

표 4. 컴퓨터 바이러스 감염증상별 기술통계

구분	기업규모		전체
	대기업	중소기업	
시스템 전체 손상	3(4.4%)	10(9.3%)	13(7.4%)
소프트웨어의 손상	17(25.0%)	25(23.1%)	42(23.9%)
시스템/네트워크 속도 저하	36(52.9%)	54(50.0%)	90(51.1%)
저장 데이터 손실	8(11.8%)	17(15.7%)	25(14.2%)
저장 데이터 유출	1(1.5%)	1(0.9%)	2(1.1%)
기타	3(4.4%)	1(0.9%)	4(2.3%)
합계	68(100.0%)	108(100.0%)	176(100.0%)

프트웨어의 손상이 23.9%(42명), 저장 데이터의 손실이 14.2%(25명)로 전반적으로 조직의 업무 생산성에 영향을 미치는 감염사고의 발생이 빈번한 것으로 나타났다. 또한 바이러스에 의한 시스템 전체 손상이 7.4%(13명)로 나타나 컴퓨터 바이러스의 파괴력 또한 무시할 수 없음을 확인할 수 있다.

바이러스 감염발생 후 업무 정상화를 위해 시스템 복구에 걸리는 시간을 묻는 질문에 표 5와 같이 감염사고 경험자의 48.3%는 피해발생 6시간 안에 정보시스템을 정상화 하는 것으로 응답하였으며, 12시간 이내의 경우는 23.9%(42명)로 나타났다. 대기업의 경우 91.2%가 감염사고 발생 후 하루 안에 정보시스템을 복구하는 것에 비해 중소기업의 경우 86%가 하루 안에 복구되는 것으로 나타났다. 이러한 결과로 보면 바이러스 감염에 따른 업무처리의 불편함을 단축하기 위해 대기업과 중소기업 모두 가급적 빠른 시간 내에 정보시스템을 정상화하고자 노력하고 있음을 알 수 있다.

표 5. 기업규모별 시스템 복구시간

구분	기업규모		전체
	대기업	중소기업	
1 ~ 6시간	38(55.9%)	47(43.5%)	85(48.3%)
6 ~ 12시간	12(17.6%)	30(27.8%)	42(23.9%)
12 ~ 24시간	12(17.6%)	16(14.8%)	28(15.9%)
48시간	4(5.9%)	10(9.3%)	14(8.0%)
72시간	2(2.9%)	5(4.6%)	7(4.0%)
합계	68(100.0%)	108(100.0%)	176(100.0%)

자신이 소속된 조직의 보안정책의 만족도에 대한 질문에는 표 6과 같이 87.7%의 응답자들이 보안정책이 대체적으로 잘 구성되어 있는 편으로 평가하고 있었다. 특히, 대기업에 소속된 응답자들 중 95.6%가 보안정책이 보통이상이라고 평가한 반면 중소기업 소속 응답자들은 82.6%가 조직의 보안정책이 보통이상이라고 평가하고 있는 것으로 나타났다.

3.5 탐색적 요인분석 및 신뢰성 검정

가설검정에 앞서 분석에 사용될 변수가 측정개념을 잘 반영하고 있는지 평가하기 위해 탐색적 요인분석을 실시하였다. 탐색적 요인분석의 기준은 주성분분석을 통해 주요요인을 설정하도록 하였으며, Kaiser 정규화가 있는 베리맥스법을 적용하였다. 표 7에 제

표 6. 기업규모별 보안정책 만족도

구분	기업규모		전체
	대기업	중소기업	
매우 잘되어 있다	31(34.4%)	3(2.5%)	34(16.2%)
잘되어 있다	35(38.9%)	29(24.2%)	64(30.5%)
보통이다	20(22.2%)	66(55.0%)	86(41.0%)
잘못되어 있다	1(1.1%)	17(14.2%)	18(8.6%)
매우 잘못되어 있다	3(3.3%)	5(4.2%)	8(3.8%)
합계	90(100.0%)	120(100.0%)	210(100.0%)

시된 요인분석 결과를 살펴보면 35개의 설문항목에 대한 총 7회의 요인회전에 의한 반복계산을 통해서 일곱 개의 요인이 추출되었다. 이 가운데 사용자특성 요인에서 '개인의 책임 인지 정도' 항목의 적재값이 0.660으로 가장 낮게 나타났지만, 모든 측정항목들이 전체적으로 높은 수준의 요인적재량을 보인다. 또한, 연구표본의 데이터가 모집단을 추정하기 위한 각 변수의 동질성을 평가하는 KMO(Kaiser-Meyer-Olkin) 적합치의 경우 일반적으로 권장하는 0.8을 넘는 0.863으로 나타나 전반적인 요인 추출결과가 적절하다고 평가된다.

연구변수에 대한 신뢰성 검증은 다항목 척도의 내적 일관성을 검증하기 위한 방법 중의 하나인 크론바하 알파(cronbach-α) 계수를 이용하였으며, 모든 요인이 최소 요구수준인 0.7[53]을 상회하는 것으로 나타나 내적 일관성은 충분한 것으로 분석되었다. 이와 같은 결과를 토대로 설문에 이용된 측정항목 전체가 적절하다고 확인되었다.

3.6 연구가설의 검정

컴퓨터 바이러스에 대한 기업규모별 사용자의 보안요소에 대한 인지 차이를 분석하기 위해서 t-test를 실시하였다. 일곱 개 연구개념에 대한 두 집단간 평균의 차이를 분석한 결과 다음의 표 8과 같이 기업의 규모에 따라 사용자들이 인지하는 보안정책에 대한 만족도와 사용자의 보안관련 이해의 차이가 있다고 나타났다. 또한, 조직내 정보자산의 중요도에 대한 인지가 다르며, 정보시스템에 내재하고 있는 취약성에 대해서도 기업규모에 따라 사용자들의 인지적 차이가 발생함을 알 수 있었다. 더욱이 기업규모별로 보안효과에 대한 인지에도 차이가 있는 것으로 나타났다. 그러나 보안위협과 위험인지의 두 연구개념에 대해서는 별다른 차이를 보이지 않았다.

표 7. 탐색적 요인분석 및 신뢰도 분석 결과

개념	측정항목	요인 적재값							신뢰도 (α)
		보안정책	사용자특성	정보자산	보안위협	취약성	위험인지	보안효과	
보안정책	사용자 정보보안 교육	0.782	0.304	0.056	-0.027	0.140	0.080	0.086	0.909
	바이러스 사고사례 공지	0.824	0.213	0.077	0.014	0.111	0.055	0.104	
	정기적인 바이러스 검사	0.774	0.196	0.145	0.049	0.196	-0.022	0.016	
	송수신전 데이터 검사	0.867	0.133	0.088	-0.024	0.124	-0.087	-0.026	
	데이터 백업 및 복구계획 시행	0.797	0.220	0.059	0.020	0.099	0.010	-0.004	
사용자 특성	개인의 책임 인지 정도	0.224	0.660	0.031	-0.007	-0.095	0.133	0.002	0.842
	정보보호 정책 인지 정도	0.428	0.687	0.010	0.081	-0.032	-0.015	0.126	
	바이러스 감염피해 인지 정도	0.314	0.798	0.021	0.110	-0.006	0.044	0.035	
	백신 활용정도	0.148	0.691	0.114	0.164	0.120	-0.155	-0.009	
	컴퓨터 관련지식 정도	0.107	0.845	0.033	0.085	0.151	0.000	-0.042	
정보자산	개인정보의 중요성	0.131	-0.056	0.823	0.074	-0.077	0.004	0.023	0.833
	사용자 정보의 중요성	0.072	0.105	0.701	0.009	0.043	0.096	0.091	
	사용자 인증정보의 가치	-0.006	0.085	0.774	0.117	0.101	0.162	-0.103	
	거래정보의 중요성	0.031	0.032	0.804	0.094	-0.045	0.022	-0.029	
	업무정보의 가치	0.120	0.021	0.793	0.032	-0.016	0.017	-0.008	
보안위협	사용자기만 빈도	-0.009	0.122	0.064	0.821	-0.107	0.215	-0.100	0.930
	인증정보 유출 빈도	0.023	0.041	0.050	0.865	-0.126	0.223	-0.133	
	불법적 시스템 접근발생 빈도	-0.035	0.103	0.022	0.833	-0.206	0.241	-0.085	
	스팸 메일 발송빈도	0.082	0.147	0.164	0.749	-0.157	0.267	-0.087	
	OS 강제종료 발생빈도	0.011	0.061	0.127	0.792	-0.166	0.300	-0.174	
취약성	보안통제 수준	0.249	0.025	0.060	-0.180	0.767	-0.185	0.249	0.897
	보안통제 활용	0.250	0.051	-0.008	-0.132	0.742	-0.224	0.310	
	운영체제 보안	0.133	0.147	0.091	-0.058	0.741	-0.195	0.208	
	네트워크의 감염 용이성	0.112	-0.056	-0.077	-0.340	0.691	-0.256	0.089	
	소프트웨어 결함	0.120	0.011	-0.098	-0.297	0.700	-0.301	0.219	
위험인지	생산성 손실 위험	0.042	-0.054	0.046	0.283	-0.208	0.785	-0.118	0.939
	정보시스템 신뢰 위험	0.021	-0.015	0.051	0.311	-0.206	0.805	-0.065	
	응용 프로그램 신뢰 위험	0.021	-0.024	0.077	0.281	-0.237	0.799	-0.084	
	재무적 손실 위험	0.002	-0.010	0.068	0.192	-0.171	0.850	-0.156	
	프라이버시 침해 위험	-0.031	0.064	0.077	0.157	-0.112	0.821	-0.132	
	조직 신뢰도 저하 위험	-0.010	0.046	0.064	0.114	-0.093	0.844	-0.144	
보안효과	업무 손실	0.080	0.035	0.027	-0.159	0.189	-0.148	0.754	0.910
	기회비용 손실	0.054	0.031	-0.012	-0.184	0.180	-0.141	0.837	
	정보시스템 손실	-0.009	0.012	-0.014	-0.085	0.208	-0.129	0.883	
	정보자산 손실	0.033	-0.011	-0.011	-0.066	0.169	-0.159	0.895	
초기 고유값		2.834	1.281	1.516	6.056	2.105	9.421	2.389	
설명분산(%)		8.096	3.661	4.332	17.301	6.014	26.918	6.826	
누적분산(%)		8.096	11.757	16.089	33.391	39.405	66.322	73.148	

표 8. 연구가설 검정결과

요인	t-값	유의확률	연구가설	검정결과
보안정책	5.621	0.000	가설 1	채택
사용자특성	3.424	0.001	가설 2	채택
정보자산	2.285	0.023	가설 3	채택
보안위협	-0.415	0.679	가설 4	기각
취약성	-3.715	0.000	가설 5	채택
위험인지	0.697	0.487	가설 6	기각
보안효과	3.580	0.000	가설 7	채택

Ⅳ. 분석결과 논의

분석결과에 따르면 먼저, 연구가설 1에서 사용자의 조직내 보안정책에 대한 인지의 차이는 유의한 것으로 나타났다. 이는 조직내 바이러스에 의한 사고사례의 전파, 정기적인 데이터의 백업 및 데이터의 무결성 검사 등의 보안정책의 집행이 기업규모에 따라 차이를 보인다는 것이다. 표 6에 나타난 바와 같이 대기업과 중소기업간 보안대책의 만족에 대한 응답에서 중소기업 사용자들의 보안정책에 대한 만족도가 대기업에 비해 낮으며, 중소기업에서의 바이러스 침해사고 예방을 위한 보안정책이 부족함으로 적절한 보안정책의 수립이 시급함을 알 수 있다.

두 번째로 사용자의 개인적 특성의 차이도 통계적으로 유의한 것으로 나타났다. 즉, 기업규모에 따라 바이러스 예방과 차단을 위한 사용자들의 보안인지에 차이를 보인다는 것이다. 앞서 설명된 보안정책과 마찬가지로 조직내 정보보안의 투자부족은 시스템 관리자 또는 사용자들의 정보보안에 대한 이해의 차이를 형성하는 원인이 될 수 있다. 또한, 이렇게 형성된 집단간 사용자들의 보안인지의 차이는 감염사고의 발생가능성을 상대적으로 높일 수 있다. 이는 표 2와 표 3에서 감염사고의 경험유무와 사고발생 횟수에서 설명하고 있듯이 대기업의 감염사고 발생률이 75.6%인데 비해 중소기업의 경우 90%로 상대적으로 침해사고 발생률이 높다는 점과 2회 이상의 감염 사고가 중소기업에서 더 많다는 점에서 유추할 수 있다.

세 번째로 연구가설 3에서 제시한 정보자산의 중요도와 잠재적 가치에 대한 기업규모별 인지적 차이도 유의한 것으로 나타났다. 즉, 바이러스 감염발생시 동일한 정보자산에 대해서도 중요도와 가치를 서로 다르게 평가하고 있다는 것이다. 이는 정보시스템 활용을 위해 필요한 사용자 인증정보와 사용자 정보라든지, 기업운영에 핵심인 거래정보와 업무정보 등과 같은 보호되어야 할 자산의 중요도를 기업규모에 따라 서로 다르게 평가하는 것으로 해석할 수 있다.

네 번째로 기업규모에 따른 사용자의 보안위협의 인지는 유의하지 않은 것으로 나타났다. 이러한 결과는 바이러스에 의해 의도하지 않은 침해사고의 발생가능성을 규모에 상관없이 대부분의 사용자들이 심각하게 수용하고 있다는 것이다. 즉, 업무처리의 향상을 위해 사용하고 있는 인터넷 및 공유 네트워크의 개방성과 높은 정보 공유성은 역으로 바이러스 침입 가능성을 높일 수 있음을 사용자 스스로 인지하고 있기 때문에 감염사고의 발생을 항상 우려하고 있는 것으로 볼 수 있다. 이것은 표 4에서 나타난 바와 같이 사용자들이 이미 여러 차례 감염을 경험해 보았기 때문이라고 볼 수 있다.

가설 5에서 기업규모별 보안 취약성 정도에 대한 인지 차이도 유의한 것으로 나타났다. 이러한 결과는 상대적으로 보다 많은 투자가 가능한 대기업이 정보보안 취약성을 감소시키기 위한 노력을 더 많이 하고 있음을 의미한다. 따라서, 정보시스템을 컴퓨터 바이러스로부터 보호하기 위한 보안대책과 통제의 수준이 기업규모에 따라 차이가 나타난다. 즉, 대기업이 중소기업에 비해 바이러스 침해사고에 따른 시스템 복구시간이 짧다는 것은 그만큼 침해사고 대응을 위한 준비가 잘 되어 있으며, 감염발생에 따른 대응이 상대적으로 빠르다는 것으로 설명이 가능하다.

기업규모에 따른 사용자의 위험인지를 설명한 연구가설 6은 유의하지 않은 것으로 나타났다. 이는 바이러스에 의한 보안위협과 마찬가지로 기업규모에 상관없이 감염발생에 의한 업무 생산성의 손실, 정보시스템에 대한 신뢰 감소, 이에 따른 재무적인 손실 및 인증정보의 노출로 인한 프라이버시 침해 등에 대한 피해를 심각하게 우려하고 있는 것으로 해석이 가능하다.

마지막으로, 연구가설 7에서 제시한 기업규모에 따른 보안효과의 차이를 분석한 결과 통계적으로 유의한 것으로 나타나 기업규모에 따른 바이러스 예방 및 차단의 효과에 사용자들 사이에 인지적 차이가 발생하는 것으로 나타났다. 이러한 이유로 기업에서 수립한 보안대책의 수준, 사용자의 보안인지 정도 및 조직의 보안취약성 정도에 따라 바이러스 감염발생시 업무적 손실, 기회비용 손실, 정보시스템에 대한 피해를 다르게 인지하고 있기 때문으로 볼 수 있다.

본 연구의 결과는 다음과 같은 시사점을 제시하고

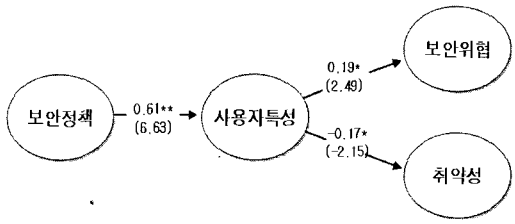
있다. 먼저, 기업규모별 컴퓨터 바이러스에 대한 사용자의 보안인지의 차이를 실증적으로 규명하고, 컴퓨터 바이러스 감염예방을 위해 정보보안의 측면에서 사용자 보안인지의 중요성을 강조하였다는데 있다. 특히, 기업에서 체계적으로 잘 수립된 보안정책을 집행하게 될 경우 사용자에게 올바른 정보시스템의 사용과 구성원으로서 지켜야할 의무와 책임, 보안정책의 인지를 효과적으로 수용하게 하며, 이는 사용자 부주의에 의해 트로이목마 혹은 스파이웨어에 감염되는 사례를 감소시킬 수 있음을 시사한다.

두 번째 시사점으로 조직내 보안정책의 중요성을 확인하였다는 점이다. 앞서 설명된 분석결과를 토대로 대기업과 중소기업간 사용자들이 가지는 정보보안의 이해차이는 보안정책의 수준 차에서 발생함을 알 수 있다. 즉, 대기업에서 보안정책의 수준이 중소기업에 비해 상대적으로 높았기 때문에 감염사고의 발생이 작았던 것으로 볼 수 있다. 이처럼 정보시스템 사용자에게 정보보안을 위한 적법한 사용과 불법사용의 개념을 명확히 전달하고, 적절한 사용에 대한 교육 및 위반의 심각성에 따른 제재조치를 천명하는 것은 정보보안에서 효과로 직결된다고 볼 수 있다. 이러한 결과는 Straub[42]의 연구에서 지적된 바와 유사한 것으로 조직내 예방적 보안대책의 집행은 컴퓨터 범죄를 효과적으로 억제할 수 있음을 실증적으로 분석한 것이라 할 수 있다.

앞서 언급한 보안정책이 사용자의 인지적 차이를 발생시키는지에 대한 인과관계를 다음의 그림 1과 같이 인과관계를 설정한 구조방정식을 통해 추가적으로 분석해 본 결과 구조모형의 적합도 지수는 절대부합지수 중 GFI(goodness-of-fit-index)가 0.79, 증분부합지수 중 NFI(normed fit index)는 0.82, 간명부합지수에서 PNFI(parsimonious normed fit index)는 0.72로 양호한 수준이며, 모든 경로가 유의하다. 이는 곧 조직의 보안정책은 사용자의 인지적 특성을 형성하는데 상당히 많은 영향을 미치고 있으며, 이를 통해 보안에 대한 이해가 높아진 사용자는 바이러스에 대한 감염 위협을 심각하게 수용함과 동시에 조직내 정보시스템 취약성을 확인하고 대책을 수립하는데 적극성을 가질 수 있음을 시사한다.

V. 결 론

본 연구는 기업규모에 따라 정보자산, 위협, 취약성, 위험, 사용자특성 등 여러 가지 정보보안 요소에



주) 괄호: t-값, *: 유의수준 $\alpha=0.05$, **: 유의수준 $\alpha=0.01$

그림 1. 보안정책과 사용자특성 중심의 인과관계 분석

대한 사용자의 인지적 차이를 컴퓨터 바이러스를 대상으로 분석하였다. 분석결과에 따르면, 먼저 보안위협과 위험인지를 제외한 다른 연구개념들은 기업규모에 따라 보안요소의 유의한 차이가 있는 것으로 확인되었다. 즉, 컴퓨터 바이러스 침입의 위협과 유출된 정보의 접근성 등 감염피해의 유형에 따라 침입방지와 감염차단 등의 대응방식은 사용자들의 정보보안에 대한 이해의 차이에 따라 달라질 수 있음을 확인하였다. 보안위협과 위험인지에 대한 별다른 차이가 나타나지 않았는데 이는 기업규모에 관계없이 사용자들이 컴퓨터 바이러스에 의해 정보시스템에 가해지는 위협의 심각성과 감염발생시 정보시스템에 발생하는 손실과 피해에 대해 우려하고 있음을 보여준다.

본 연구결과를 기초로 대기업에 비해 정보보안의 투자가 미흡한 중소기업에 있어서 보안정책의 중요성을 강조할 수 있다. 기존 연구들[39][54]에서 이미 지적된 바와 같이 정보보안의 효과는 경영층의 참여와 적극적인 지원에서 비롯된다. 효과적인 보안정책은 대기업뿐만 아니라 중소기업에 있어서도 주요한 성공요인이다. 즉, 관리자 및 사용자들에게 정보보안에 대한 투자가치를 알리고, 감염사고 발생시 손실과 보안대책간의 관계를 밝히는 것은 바이러스 침해사고 예방에 근간이 된다.

본 연구결과를 기반으로 다음과 같은 향후 연구방향을 제시하고자 한다. 먼저, 본 연구에서는 컴퓨터 바이러스에 대한 기업규모별 사용자의 인지적 차이를 분석하기 위해 여러 가지 보안관련 개념들이 사용되었다. 추후에는 각 보안요소에 대한 집단간 차이만이 아니라 인과관계의 측면에서 보다 엄격한 분석기법을 적용해 보안요소의 상호관계를 비롯하여 이들이 보안효과에 미치는 영향을 살펴볼 필요가 있을 것이다.

두 번째, 분석에 사용된 표본집단에 대한 측면으로 본 연구에서는 각 기업에 소속된 사용자의 인지 수준을 기초로 분석하였으나 조직단위의 인지수준을 분석함으로써 여러 가지 보안개념을 다른 각도로 조망해

볼 수 있을 것이다. 마지막으로 사용된 표본집단의 산업유형과 관련된 것으로, 본 연구에서는 업종별 인지도의 차이를 고려하지 않았으나 향후 연구에서 산업별 비교분석을 수행한다든지 개별 업종에 따라 세분화하여 비교 분석할 수 있을 것이다. 또한, 대기업과 중소기업의 종업원 수 혹은 자본금 등 규모의 차이에 따른 세분화를 통해 보안요소 인지에 대한 비교분석도 유용하리라 판단하는 바이다.

참 고 문 헌

[1] Finne, T., "A Conceptual Framework for Information Security Management," *Computers & Security*, Vol. 17, No. 4, pp. 303-307, 1998. .

[2] 김세헌, *정보보호 관리 및 정책*, 생능, 2002.

[3] Russell, D. and G. Gangemi, *Computer Security Basics*, O'Reilly & Associates, 1991.

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

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

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

[7] Tedeschi, B., "Protect Your Identity," *PCWORLD*, pp. 107-112, Dec. 2004.

[8] 최운호, 전영태, "대규모 컴퓨터 바이러스/웜의 공격시 종합침해사고대응시스템에서의 자동화된 역추적 절차," *정보보호학회논문지*, 제15권, 제1호, pp. 50-60, 2005.

[9] 한국정보보호진흥원, *새로운 사이버 위협: 피싱 - 피싱에 따른 기술, 사회, 법제적 대응 및 시사점*, 정책기획 05-6K, 한국정보보호진흥원, 2005.

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

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

[12] 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, pp. 139-154, 2003.

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

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

[15] White, S., *Open Problems in Computer Virus Research*, IBM Thomas J. Watson Research Center, NY USA, 1998.

[16] Lee, Y. and K. Kozar, "Investigating Factors Affecting the Adoption of Anti-Spyware Systems," *Communications of the ACM*, Vol. 48, No. 8, pp. 72-77, 2005.

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

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

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

[20] 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, pp. 381-396, 2002.

[21] Stonburner, G., A. Goguen, and A. Feringa, *Risk Management Guide for Information Technology Systems*, NIST SP 800-30, National Institute of Standard and Technology, 2001.

[22] BSI, *BS7799: Code of Practices for information Security Management*, United Kingdom, 1999.

[23] ISO/IEC, *Guidelines for the management of IT security (GMITS)-Part 1: Concepts and models of IT security*, ISO/IEC JTC1 SC27 TR 13335-1, 2000.

[24] CSI, *IPAK: Information Protection Assessment Kit*, Computer Security Institute, 1997.

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

[26] Peltier, T., *Information Security Risk Analysis*, Auerbach, 2001.

[27] Bissett, A. and G. Shipton, "Some Human Dimensions of Computer Virus Creation and Infection," *International Journal of Human-Computer Studies*, Vol. 52, pp. 899-913, 2000.

[28] CMU/SEI, *Operationally Critical Threat, Asset, Vulnerability Evaluation (OCTAVE) Framework*, Ver. 1.0, CMU/SEI-99-TR-017, June 1999.

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

[30] Gordon, S., "Application Program Security Fighting Spyware and Adware in the Enterprise," *Information systems security*, Vol. 14, No. 3, pp. 14-17, 2005.

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

[32] Cannon, C., "The Real Computer Virus," *American journalism review*, pp. 28-35. Apr., 2001.

[33] Poston, R., F. Stafford, and A. Hennington, "Spyware: A View from the (Online) Street," *Communications of the ACM*, Vol.48, No. 8, pp. 96-99, 2005.

[34] CSI, *Eighth Annual CSI/FBI Computer Crime and Security Survey*, Computer Security Institute, 2005.

[35] Lee, S., S. Lee, and S. Yoo, "An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories," *Information & Management*, Vol. 41, No. 6, pp. 707-718, 2004.

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

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

[38] Jung, B., I. Han, and S. Lee, "Security Threats to Internet: A Korean Multi-Industry Investigation," *Information & Management*, Vol. 38, No. 8, pp. 487-498, 2001.

[39] Mtembu, K. and Y. Cairns, "How to Manage and Reduce Computer Crime," *IS Audit & Control Journal*, Vol. 6, pp. 27-31, 1997.

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

[41] Straub, D. and W. Nance, "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS*

Quarterly, Vol. 14, No. 1, pp. 45-60, 1990.

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

[43] Gogan, J., "Should "Personal" Computers Be Personally Allocated?", *Journal of Management Information Systems*, Vol. 7, No. 4, pp. 91-106, 1991.

[44] 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, pp. 13-27, 1991.

[45] Venkatesh, V. and M. Morris, "Why Don't Men Ever Stop to Ask For Direction? Gender, Social Influence, ad Their Role in Technology Acceptance and Usage Behavior," *MIS Quarterly*, Vol. 24, No. 1, pp. 115-139, 2000.

[46] Agarwal, R. and J. Prasad, "The Antecedents and Consequents of User Perceptions in Information Technology Adoption," *Decision Support Systems*, Vol. 22, No. 1, pp. 15-29, 1998.

[47] McGraw, G. and G. Morrisett, "Attacking Malicious Code: A Report to the Infosec Research Council," *IEEE Software*, Vol. 17, No. 5, pp. 33-41, 2000.

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

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

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

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

[52] 김종기, 이동호, 서창갑, "전자상거래환경에서 위험분석방법론의 타당성에 대한 연구," *정보보호학회논문지*, 제14권, 제4호, pp. 61-74, 2004.

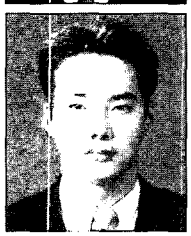
[53] 채서일, *사회과학조사방법론*, 학현사, 2003.

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

〈著者紹介〉

김 종 기 (Jongki Kim) 정회원

1987년 2월: 부산대학교 경영학과 졸업
1988년 12월: Arkansas State University, MBA
1992년 12월: Mississippi State University, Ph.D in MIS
1993년 3월~1998년 12월: 국방정보체계연구소 선임연구원
1999년 3월~현재: 부산대학교 경영학부 부교수
〈관심분야〉 정보시스템 보안관리, 전자상거래, 프로젝트 관리



전 진 환 (Jinhwan Jeon) 정회원

1999년 2월: 인제대학교 경영학과 졸업
2001년 2월: 인제대학교 경영학과 석사
2006년 2월: 부산대학교 경영학과 박사(경영정보 · 생산관리 전공)
2006년 3월~2006년 6월: 부산대학교 경영경제연구소 전임연구원
2006년 7월~현재: 부산대학교 금융 · 증권 · 선물 교육연구사업단
〈관심분야〉 정보시스템 보안관리, 전자상거래, 데이터마이닝