마이크로컴퓨터의 네트워크화 여부가 보안 위협 인식에 미치는 영향 : 군조직을 대상으로

이 찬 희* · 김 준 석** · 서 길 수**

The Effects of Microcomputer Networking on the Perception of Threats to Security : the Military Users' Case

Chan-Hee Lee* · Jun-Seok Kim** · Gil-Su Seo**

Abstract

The purpose of this study was to identify the effect of microcomputer networking on user perception of potential threats to security employing user attitudes as a moderating variable. A research model consisting of microcomputer networking as the independent variable, user perception of potential threats to security as the dependent variable, and user attitude toward security control as the moderating variable was developed through literature review.

The results of this study provide an empirical evidence of the importance of environmental change(information systems networking) on user perception of potential threats to security. Furthermore the results imply that in order to improve security performance through the reinforcement of user perception of threats to security in the organization, user attitudes should be made favorable.

* 국방부
** 연세대학교 경영학과

1. 서 론

최근 정보통신기술 및 클라이언트/서버 기술의 급속한 발전에 따라 많은 조직들이 데이터의 분산처리체제를 채택하고 있다. 이에 따라 근거리통신망 등의 네트워크를 통하여 과거의 독립형(Stand-alone) 시스템에서는 불가능했던 정보자원의 공유가 가능하게 되었다. 이러한 일련의 추세는 정보시스템의 효율성을 크게 높임으로써 생산성 향상에 많은 기여를 해 왔다. 그러나 네트워크환경의 급속한 확대는 보안유지의 측면에서 위험도를 증가시키며, 여러 가지 부수적인 문제점을 야기시킨다[Donovan 1993]. 이에 따라 정보시스템의 안정적인 이용을 저해하는 위협으로부터 정보시스템을 보호하기 위한 여러 가지 수단을 강구하는 것이 정보시스템 관리분야의 중요한 과제가 되고 있다[Dickson et al. 1984, Niderman et al. 1991].

정보시스템 보안 문제에 있어 근래에 가장 심각한 문제중의 하나가 바로 네트워크 보안이다. 전형적인 예로서 최근에 급속히 증가하고 있는 해킹의 문제를 들 수 있다. 기업에서는 최첨단의 설계도면이 빠져나가고, 군조직에서는 기밀사항이 빠져나갈 위험성이 과거 어느 때 보다 높아지고 있다. 선행연구에 의하면 네트워크에 연결된 정보시스템은 업무의 효율성을 증가시킬 수 있는 장점이 있으나 접근의 용이성 등으로 인하여 오히려 보안에 대한 위협이 증가된다고 강조하고 있다[Belden 1991, Kelly, 1988, Rivera 1991]. 또한 Loch 등이 정보시스템 부문의 중역들을 대상으로 실시한 연구에 의하면, 정보시스템의 사용은 급속히 네트워크 환경으로 변화하면서 보안상에 매우 큰 위협으로 대두되고 있는 것으로 나타났다[Loch 1992].

이러한 잠재적 위협의 증가에도 불구하고 실무에서의 대책은 종래의 독립적 시스템을 사용하던 환경과 크게 다르지 않은 실정이다. 최근에 국내 기업의 전산 책임자들을 대상으로 한 실태조사에 의하면 자사의 '정보 보안 환경'에 대해 만족하는 기업은 27%에 불과하며, 네트워크 부문의 보안 위협을 인식하고 이에 대비책을 강구하고 있는 기업도 40% 정도에 불과한 것으로 나타났다[전자신문사 1996]. 이 조사결과는 정보시스템 부문의 책임자나 중역들을 대상으로 밝혀진 내용인데, 이들보다 상대적으로 책임의식이 적은 일반 사용자들이 인식하는 보안 위협에는 더 큰 문제가 있을 것으로 보인다. 이러한 점에서 네트워크로 구성된 컴퓨팅 환경하에서 보안 문제는 매우 중요한 의미를 가진다. 네트워크 환경으로의 변화에 따른 보안 문제의 중요성에도 불구하고 그간 이에 관한 실증적 연구들은 거의 없었던 실정이다. 또한 소수의 기존 연구들도 주로 정보시스템 부문의 책임자들을 대상으로 하였으며, 상대적으로 보안에 대한 인식이 더욱 취약할 것으로 생각되는 일반 사용자들을 대상으로한 실증적인 연구는 없었다.

한편, 정보시스템 분야에서 사용자 태도는 대표적인 개인특성으로서 시스템 사용과 정보시스템의 성공적 실행에 영향을 미치는 것으로 알려지고 있다[Schewe 1976]. 그러나 보안관련 연구에 있어서는 사용자의 태도와 같은 심리적 요인이 간과되어 왔는데, 최근에 권영규의 연구에서 사용자의 태도가 보안성과를 향상시키는데 매우 중요한 요인이라는 것이 실증적으로 밝혀진 바 있다[권영규, 1994]. 즉, 사용자가 어떠한 태도를 갖고 있는지에 따라 보안 위협에 대한 인식이 달라질 수 있으며, 이에 따라 사용자의 태도를 호의적으로 유도함으로써 보안 성과를 높일 수 있다는 것이다. 권영규의 연구는 사용자의 태도요인을 보안 분야의 연구에 처음으로 도입하여 연구한 결과였으므로 추가적인 검증이 요구된다.

이 연구에서는 네트워크 환경으로의 변화에 따라 마이크로컴퓨터를 사용하는 일반 실무자들이 인식하는 잠재적 보안 위협의 정도를 보안 성과와 연결시켜 연구하고자 한다. 즉, 마이크로컴퓨터의 네트워크화 여부가 사용자의 보안 위협에 미치는 효과를 검증하고, 보안 성과에 영향을 미치는 중요한 요인으로 밝혀진 사용자의 태도가 이러한 두 요인들과 결합하여 어떻게 작용하는가를 분석함으로써 효과적인 보안 통제 방안을 도출하고자 한다.

2. 이론적 배경

지금까지의 연구에서 정보시스템 보안에 영향을 미치는 주요 변수들은 조직 특성 요인, 개인 특성 요인, 그리고 과업 특성 요인들이었다. 조직 특성 요인으로는 보안 통제 수준, 보안에 대한 투자, 조직 규모 등이었으며, 개인 특성 요인으로는 정보시스템 사용 능력, 경험 그리고 과업 특성으로는 산업부문별 보안 취약성 정도를 들 수 있다.

보안 위협 인식에 관한 연구로서 Goodhue와 Straub [Goodhue & Straub 1991]는 직무만족이론에 기초하여, 보안에 대한 관심이 높으면 보안 만족도가 높아지고 이에 따라 보안 성과가 향상될 것이라는 개념하에 이론적 모델을 개발하고 실증적 검증을 실시하였다. 즉, 업무특성(산업별 보안 취약성), 정보시스템 자체의 환경특성(조직의 투자활동), 그리고 개인특성(사용자의 경험, 인식) 등의 세 가지 요소가 사용자의 보안 만족도에 영향을 미치며, 보안 성과를 나타내는 대리변수로서 '사용자의 보안 관심도'를 측정하였다. 각각의 요인들을 구체적으로 설명하면 다음과 같다.

첫째, 업무특성은 특정 산업에 내재된 보안 취약성으로서 일반적으로 금융기관과 같은 특정 산업은 그 특성상 정보시스템의 보안 사고의 위협이 여타 산업보다 높은 것으로 인식된다. 따라서 보안 위협이 높은 산업의 사용자는 시스템 보안에 더 많은 관심을 가지며, 또한 그들의 정보시스템 보안 환경에 덜 만족할 것이다.

둘째, 정보시스템 환경 특성은 보안성 향상을 위하여 조직이 취한 활동으로 보았는데, 이는 조직이 정보시스템 보안을 위하여 더 많은 자원을 투자한다면 사용자는 정보시스템 보안에 대하여 더 높은 만족도를 나타낼 것이다. 그러므로 조직의 정보시스템 보안 노력이 정보 보안에 대한 관심과 인식 정도에 영향을 미치는 중요한 요인으로 작용할 것이다.

셋째, 개인적 특성으로는 시스템에 대한 인식(Awareness) 및 지식(Knowledge)으로 보았는데, 사용자가 보안 위협에 대하여 더 많이 인지하고 있으며, 시스템에 대한 지식이 높을 경우, 보안에 대하여 더 높은 관심을 나타낼 것이며, 따라서 현재의 보안대책에 대하여 덜 만족할 것이다.

이상과 같은 개념으로 실증적 연구를 실시한 결과 업무특성상 높은 보안 위험에 처해 있는 사용자일수록 보안에 대한 관심이 높으며, 개인적 특성인 사용자의 보안문제에 대한 인식과 지식도 보안관심과 정의 상관관계에 있는 것으로 규명되었으나, 정보시스템 보안에 대한 조직의 지원정도와 사용자의 보안 관심간에는 負의 상관관계에 있는 것으로 밝혀졌다.

이 연구에서는 Goodhue와 Straub이 직무만족이론을 토대로 개발한 이론적 모델에 기반하여 다음과 같이 연구를 진행하고자 한다. 즉, 사용자의 보안관심에 영향을 미치는 세 요소 중에서 이 연구의 대상을 동일 조직으로 한정함에 따라 산업의 보안 취약성을 나타내는 업무특성 요소는 통제가 가능하다. 따라서 나머지 두 요소들을 중심으로 사용자의 보안관심 즉, 보안 위협 인식에 미치는 영향을 살펴 보고자 한다.

한편, 정보시스템 분야에서 태도는 사용자 특성 중의 대표적인 예로서 시스템 사용과 정보시스템의 성공적 실행에 영향을 미치는 것으로 인식되고 있다. Schewe[1976]는 태도를 어떤 사물이나 객체에 대한 호의적, 또는 비호의적 감정으로 정의하고, 이러한 사용자 태도가 시스템 성공에 미치는 영향을 연구한 바 있다. 또한 Lucas[1978]는 시스템 성공에 관련된 요인들에 관한 연구를 통하여 사용자의 태도와 지각은 성공적인 시스템 실행에 영향을 미치는 것으로 밝혀낸 바 있다.

Robey[1979]에 의하면 사용자의 특성, 시스템의 특성, 환경적 특성요인이 사용자의 업무성과와 시스템 사용에 영향을 미치며 사용자의 가장 대표적인 속성을 시스템 사용에 대한 태도로 보고 있다. 이 같은 Robey의 연구는 앞에서 고찰하였던 Goodhue 등의 정보시스템 사용자의 보안 관심에 미치는 영향에 관한 연구와 같이 생각해 볼 수 있다. Goodhue 등의 연구에서도 직무만족 이론에 기반하여 과업 특성, 개인 특성, 환경 특성 등이 정보

시스템 사용자들의 보안 관심에 유의적인 영향을 미치는 것으로 밝혀진 바 있다. 정보시스템에 관한 위의 두 연구는 사용자 특성을 중요한 요소로 다루고 있다. 특히 Robey의 연구에서 사용자의 가장 대표적인 속성을 태도로 보았듯이 이 연구에서도 Goodhue 등의 연구 모형에서의 개인 특성을 사용자의 태도라는 구성개념으로 사용한다. 따라서 사용자의 태도는 보안 위협 인식에 영향을 미칠 수 있음을 기대할 수 있다. 또한 권영규[1994]는 이와 같은 사용자 태도를 처음으로 보안관련 연구에 도입하였는데, 조직의 보안통제가 사용자 자신에게 긍정적이거나 부정적으로 미치리라는 영향의 방향을 의미한다고 주장하였다. 즉, 호의적인 태도를 갖는 사용자는 보안이 자기 자신에게 긍정적으로 영향을 주리라고 기대하는 사용자이며, 비호의적인 사용자는 자신에게 부정적으로 영향을 미칠 것이라고 생각하는 사용자로 볼 수 있다고 하였다.

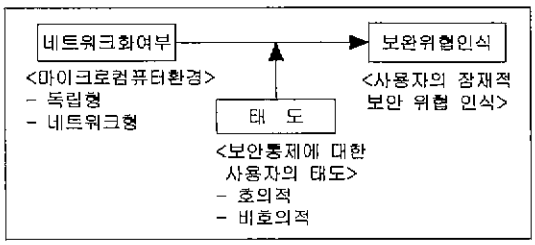
이상의 연구들을 통하여 사용자의 태도라는 요소가 본 연구에서 조절변수의 역할을 할 수 있음을 살펴보고자 한다. 조절변수(Moderator Variables)는 일반적으로 그 변수를 체계적으로 변화시킬 때 다른 두개의 변수간의 관계에 변화를 야기시키는 변수이다. 즉, 두개의 변수간의 관계가 제3의 변수인 조절변수의 수준에 의해 좌우되는 것이다[Stone 1981]. 정보시스템 보안에 관한 연구 중에서 권영규가 처음으로 사용자의 태도 변수를 도입하여 연구하였으므로 이 연구에서는 권영규의 연구결과를 토대로 태도 변수가 보안 위협 인식 수준을 조절할 수 있음을 살펴보고자 한다. 권영규의 연구에서 사용자의 태도가 보안 성과를 향상시키는데 매우 중요한 요인이라는 것이 실증적으로 검증되었다. 그리고 조직 구성원들은 보안규정의 준수가 그들의 업무 수행에 지장을 초래한다고 인식하기 때문에 보안 자체에 대해 부정적인 반응을 보일 수도 있으며, 따라서 조직에서 사용자의 보안에 대한 태도를 호의적으로 함으로써 보안의 성과를 극대화시킬 수 있을 것이라고 주장하였다.

이상에서 살펴본 사용자의 태도와 인식에 관한 연구들을 정리하면, 태도는 인식에 영향을 미칠 수 있으며, 특히 보안 분야에 있어서 태도는 네트워크화 여부와 사용자의 보안 위협 인식이라는 두 변수간의 관계를 조절하는 역할을 할 수 있음을 알 수 있다.

3. 연구모형 및 변수의 정의

3.1 연구모형

선행연구를 토대로 정보시스템 보안에 영향을 미치는 주요 변수를 도출하였다. 보안에 영향을 미치는 여러 가지 변수들 중에서 정보시스템의 환경 특성을 마이크로컴퓨터의 네트워크화 여부로 한정하고, 이 변수와 사용자의 보안 위협 인식간의 관계에 있어 사용자의 태도 요인이 어떠한 영향을 미치는가에 초점을 맞추었다. 따라서 연구의 모형은 (그림 1)과 같이 설정된다.



(그림 1) 연구 모형

이론적 배경에서 이미 살펴 본 바와 같이 정보시스템의 사용 환경 즉 네트워크화로의 변화는 사용자의 보안 위협 인식에 영향을 미칠 수 있다. 또한 사용자의 보안 통제에 대한 태도는 보안에 관한 성과를 향상시키는데 매우 중요한 요인이라는 것이 실증적으로 밝혀진 바 있는데, 이는 태도에 따라 보안 위협 인식 수준에 차이를 보일 수 있음을 의미한다. 선행연구 결과를 토대로 이들 변수들간의 관계는 다음과 같이 예상된다. Boockholt, Goodhue 등의 연구결과로부터 네트워크화 여부는 정보시스템 환경 특성 중의 하나로 사용자의 보안 위협 인식에 영향을 미칠 수 있음을 예측할 수 있다. 또한 Robey, 권영규의 연구결과를 통하여 사용자의 보

안 통제에 대한 태도는 네트워크화 여부가 보안 위협 인식에 영향을 미침에 있어 보안 위협 인식의 수준을 체계적으로 변화시킬 수 있음을 기대할 수 있다. 따라서 이 연구에서는 마이크로컴퓨터의 네트워크화 여부가 사용자의 잠재적 보안 위협 인식에 미치는 영향과 사용자의 태도 요인이 이들 두 변수간의 관계에 미치는 영향을 밝히고자 한다.

3.2 연구변수의 정의

이 연구에서는 마이크로컴퓨터의 네트워크화 여부를 독립변수, 정보시스템에 대한 사용자의 보안 위협 인식을 종속변수로 하며, 사용자의 보안 통제에 대한 태도를 조절변수로하는 연구모형을 설정하고 이에 대한 가설을 도출하였다. 각 변수들에 대한 조작적 정의는 다음과 같으며, 구체적인 설문은 부록에 첨부하였다.

3.2.1 독립변수 : 마이크로컴퓨터의 네트워크화 여부

마이크로컴퓨터의 네트워크화 여부는 컴퓨터의 사용환경에 대한 Boockholdt의 정의에 따라 크게 독립형과 네트워크형으로 분류된다[Boockholdt 1987]. 여기서 독립형이란 다른 컴퓨터와 전혀 연결되어 있지 않고 순수하게 워드프로세싱과 같은 사무 자동화 기능을 수행하는 마이크로컴퓨터를 의미한다. 또한 네트워크형이란 메인프레임을 보충하기 위하여 사용되는 것으로 통신망에 의해 다른 컴퓨터와 연결되어 데이터의 공유 등을 할 수 있는 마이크로컴퓨터를 말한다. 단, 사용 환경 구분에 있어 네트워크의 유형은 본 연구에서 고려하지 않기로 한다. 지금까지 이에 관한 측정도구는 개발되어 있지 않다. 이 연구에서는 조직내에서 마이크로컴퓨터 사용자들이 업무를 수행하면서 주로 사용하는 마이크로컴퓨터의 환경이 네트워크화 되었는지의 여부를 묻는 명목척도로서 측정하였다.

3.2.2 조절변수 : 사용자의 태도

이 연구에서는 바키 등의 정의를 도입하여 사용자의 태도를 조직의 네트워크화 여부에 따른 보안 통제에 대한 사용자들의 감정적, 평가적 반응으로 정의한다. 여기서 사용자의 감정적 반응이란 조직의 보안규정과 같은 공식적 보안정책 등의 보안 통제 요인에 대한 사용자의 유쾌감(愉快感)이나 연계감(連繫感)을 의미한다. 유쾌감이나 연계감을 가지는 사용자는 이러한 보안 통제 요인에 대해 긍정적으로 생각할 것이며, 반대로 불유쾌감을 가지는 사용자는 부정적으로 생각한다. 평가적 반응이란 보안 통제에 대한 사용자의 의견이며, 보안 통제가 사용자 자신에게 미치는 효과에 대해 긍정적 또는 부정적으로 평가하느냐의 태도이다.

이 연구에서는 Barki[1994] 등이 개발한 정보시스템 도입에 대한 사용자의 태도를 측정한 항목으로 보안 통제에 대한 사용자 태도의 측정문항을 변형하여 보안통제에 대한 사용자의 태도를 측정하였다(부록 참조).

3.2.3 종속변수 : 보안 위협 인식

정보시스템 보안이란 컴퓨터시스템 자체뿐만 아니라 모든 프로그램과 데이터의 무결성을 보호함으로써 시스템의 안전과 지속적인 운용을 보장하는 것을 의미한다. 따라서 보안의 궁극적인 실행목표는 조직의 내 외부에서 작용하는 각종 위협으로부터 정상적이고 신뢰성 있는 시스템의 운용을 보장하는 것이라고 볼 수 있다. 그러나 시스템의 사용에 있어 보안에 관한 성과가 일정기준에 따라 측정될 수 있는 명확한 도구를 가지고 있지 못하다.

Goodhue와 Straub[1991]는 사용자의 보안관심을 보안대책에 대한 만족도로 측정하였으며, 이를 보안의 성과와 연관시켜 설명하였다. 또한 권영규[1994]는 보안 성과를 Goodhue 등의 연구에서 신뢰성과 타당성이 검증된 사용자의 보안 만족도라는 대리변수로 측정하였다. 그러나 마이크로컴퓨터의 보안에 관한 성과를 설명함에 있어 Goodhue 등이 보안 성과와 연결하여 설명하였던 '보안에 대한 일반적인 관심' 보다 좀 더 구체적인 개념이 필요하다.

이 연구에서는 '사용자의 잠재적 보안 위협 인

식'을 측정하여 이를 보안 성과로 나타내고자 한다. 여기서 잠재적 보안 위협 인식은 현재의 조직에서 보안 유지를 위해 반드시 이행해야 할 공식적 정책이나 비공식적 규범 등(각종 규정이나 지침 등)을 준수하지 않을 경우, 예상되는 보안의 위협에 대하여 사용자들이 인식하는 정도로 정의된다. 왜냐하면 잠재적 보안 위협에 대한 사용자의 인식이 높을수록 보안이 잘 이행되며, 따라서 성과도 높아질 것으로 예측할 수 있기 때문이다. 측정은 시스템 보안문제를 감소시키는 방법으로서 일반적으로 인용되고 있는 Frank의 여덟 가지 통제 리스트를 수정하여 활용하며[Frank 1988], 추가적으로 연구대상 조직의 보안 업무에 관한 규칙을 참고하여 연구목적에 맞게 설문지를 수정 보완하여 리커트 5점척도로 측정한다(부록 참조).

4. 가설의 설정

연구의 목적을 달성하기 위해 실증적으로 검증해야 할 가설들은 마이크로컴퓨터의 네트워크화 여부에 따른 사용자의 잠재적 보안 위협 인식의 효과와 이들 두 변수들간에 사용자의 태도 요소의 조절작용 효과이다. 마이크로컴퓨터의 네트워크화 여부는 사용자의 잠재적 보안 위협 인식에 영향을 미치며, 사용자의 태도와 같은 심리적 요인은 사용자의 보안 위협 인식의 수준에 영향을 미칠 수 있는 조절작용을 하는 것으로 보고 가설을 설정한다.

각각의 가설들을 구체적으로 설명하면 다음과 같다.

[가설 1] 마이크로컴퓨터의 네트워크화 여부는 사용자의 잠재적 보안 위협 인식에 유의적인 영향을 미칠 것이다.

가설 1은 조직의 마이크로컴퓨터의 네트워크화 여부가 사용자의 잠재적 보안 위협 인식에 미치는 효과를 보고자 하는 것이다. Goodhue 등이 직무만족 이론에 기반하여 사용자의 보안 관심에 영향을 미치는 요인들에 관하여 연구한 결과를 토대로 정보시스템의 사용 환경은 사용자의 보안 위협 인식에 유의적인 영향을 미칠 수 있음을 기대할 수 있다. 따라서 본 연구에서는 네트워크화 여부에 따라 사용자의 보안 위협 인식에 차이가 있을 것이라는 대립가설을 설정하였다. 만일 이 가설이 채택된다면 마이크로컴퓨터의 네트워크화 여부에 따라 사용자의 보안에 관한 잠재적인 위협 수준이 다름을 알 수 있다.

가설 2, 3은 네트워크화 여부에 따라 보안 위협 인식수준의 변화에 사용자의 태도가 미치는 조절작용 효과를 보고자 하는 것이다. 권영규[1994]의 연구에 의하면 보안 통제에 대한 사용자의 태도는 보안성과를 향상시키는데 매우 중요한 요인이라는 것이 밝혀진 바 있다. 또한 이 연구에서 조직 구성원들은 보안규정의 준수가 그들의 업무 수행에 지장을 초래한다고 인식하기 때문에 보안 자체에 대해 부정적인 반응을 보일 수도 있으며, 따라서 조직에서 사용자의 보안에 대한 태도를 호의적으로 함으로써 보안의 성과를 극대화시킬 수 있을 것이라고 주장하였다. 그러므로 태도는 인식에 영향을 미칠 수 있으며, 특히 보안 분야에 있어서 태도는 사용자의 보안 위협 인식의 수준을 조절할 수 있음을 예측할 수 있다. 따라서 다음과 같이 대립가설을 설정한다.

[가설 2] 마이크로컴퓨터 사용자의 보안통제에 대한 태도가 호의적일 경우 네트워크화 여부에 따라 보안 위협 인식에 차이가 있다.

가설 2는 사용자의 태도가 호의적일 경우, 네트워크화 여부에 따라 보안 위협 인식수준의 변화에 사용자의 태도가 미치는 조절작용 효과를 보고자 하는 것이다. 만일 이 가설이 채택된다면 보안 통제에 대한 사용자의 태도가 호의적일 경우 네트워크화 여부는 사용자의 보안 위협 인식을 높이는데 유의적인 영향을 미칠 것임을 알 수 있다. 즉 사용자의 태도가 호의적일 경우 네트워크화 여부는 보안 위협 인식에 긍정적인 영향을 미치게 됨을 알 수 있다.

[가설 3] 마이크로컴퓨터 사용자의 보안통제에 대

한 태도가 비호의적일 경우 네트워크화 여부에 따라 보안 위협 인식에 차이가 있다.

가설 3은 사용자의 태도가 비호의적일 경우, 네트워크화 여부에 따라 보안 위협 인식수준의 변화에 사용자의 태도가 미치는 조절작용 효과를 보고자 하는 것이다. 만일 이 가설이 채택된다면 보안통제에 대한 사용자의 태도가 비호의적일 경우에도 네트워크화 여부가 사용자의 보안 위협 인식에 유의적인 영향을 미칠 것임을 알 수 있다.

가설 2, 3이 모두 채택될 경우 각각 사용자의 태도가 호의적인 경우와 비호의적인 경우에 있어 네트워크화 여부에 따른 보안위협 인식의 차이를 알 수 있다. 따라서 각각의 경우에 있어서의 보안 위협 인식의 정도를 비교해 봄으로써 태도변수가 보안 위협 인식의 정도를 조절하는지의 여부를 검증할 수 있다.

5. 연구결과의 분석

이 연구의 모집단은 조직에서 마이크로컴퓨터를 사용하는 일반 실무자들이다. 연구의 목적을 달성하기 위해 표본은 군조직에서 마이크로컴퓨터의 네트워크 환경이 비교적 잘 구비된 사단사령부급 이상 부대의 실무부서 최종 사용자로 다양하게 선정하였다. 다양한 부서의 사용자를 선택한 이유는 연구대상이 특정조직이나 부서에 속하여 연구결과가 그 조직과 부서의 특성에 영향을 받을 가능성을 제거하기 위해서이다. 그리고 사단사령부급 이상의 부대로 한정한 이유는 조직의 규모가 보안에 있어 주요한 상황요인이 되므로 이를 통제하기 위한 것이다.

실증분석을 위한 자료는 설문지를 이용한 현장 연구를 통하여 수집되었다. 연구의 목적을 달성하기 위해서는 네트워크화 여부(독립형, 네트워크형) 및 사용자의 태도(호의적, 비호의적)에 따른 네 개의 집단에 표본이 고르게 분포되어야 한다. 이를 위하여 연구자가 대상조직을 직접 방문하여 연구목적을 설명한 후 연구대상이 되는 사용자에게 설문지를 배포하고 이를 회수하는 방법을 사용하였다.

5.1 표본특성과 신뢰성 분석

이 연구를 위해 총 8개 사단사령부급 이상의 군부대를 대상으로 280명의 마이크로컴퓨터 사용자에게 설문지를 배포하였다. 배포된 설문지 중에서 261부가 회수되어 93.2%의 회수율을 보였다. 이 중에서 일관성이 없거나 무책임하게 응답한 12부의 설문지를 제외하여 최종적으로 249부의 설문지를 분석자료로 사용하였다. 표본의 조직 규모 및 계급별 분포는 <표 1>과 같으며, 비교적 고루 분포되어 있음을 알 수 있다. 또한 측정도구에 대한 신뢰성 분석을 위하여 각 항목간의 내적 일관성을 나타내는 크론바하 알파 계수를 조사하였는데, 보안 통제에 대한 태도와 보안 위협 인식이 각각 .86과 .85로 나타나 신뢰성이 있는 도구로 판단되어 후속 분석을 진행하였다.

5.2 가설의 검증

5.2.1 집단의 구분

분산분석을 이용하기 위해서는 독립변수와 조절변수를 바탕으로 집단을 분류하는 작업이 필요하다. 네트워크화 여부 및 사용자의 보안 통제에 대한 태도에 따라 집단을 네 개로 구분하기 위하여 각 집단에 해당되는 응답자들을 분류하였다. 분석대상 전체 태도의 평균(2.965)을 기준으로 전체의

〈표 1〉 조직 규모 및 계급별 현황

조직 규모(빈도/비율)			계 급(빈도/비율)			
사단급	군단급	군 본부급	사병	하사관	군무원	장교
117(47%)	49(19.7%)	83(33.3%)	78(31.3%)	63(25.3%)	31(12.4%)	77(30.9%)

평균보다 큰 경우 호의적인 태도로, 전체평균 이하인 경우에는 비호의적 태도로 구분하였다. 각 집단의 보안 위협 인식의 평균값은 <표 2>와 같으며, 괄호 안의 숫자는 각 집단의 표본 수를 나타낸다.

〈표 2〉 집단별 보안 위협 인식의 평균값

네트워크화 여부 / 태 도	독립형	네트워크형	합 계
호 의 적	3.73(65)	3.95(67)	3.84(132)
비호의적	3.26(62)	3.60(55)	3.43(117)
합 계	3.50(127)	3.80(122)	3.65(249)

(괄호안은 표본수)

5.2.2 분산분석에 의한 가설의 검증

(1) 가설 1의 검증

가설 1은 마이크로컴퓨터의 네트워크화 여부는 사용자의 잠재적 보안 위협 인식에 유의적인 영향을 미친다는 것이다. 이 가설은 마이크로컴퓨터의 네트워크화 여부가 사용자의 잠재적인 보안 위협 인식에 영향을 미치는 변수임을 검증하는 것이다. 가설 1의 검증을 위하여 이 연구에서는 마이크로컴퓨터의 사용환경이 독립형인 집단과 네트워크형인 집단에 있어서 보안 위협 인식이 유의적인 차이를 보이는가를 일원분산분석을 통해 검증하였다. 그 결과 <표 3>에서 보는 바와 같이 P값이 0.0005이므로 가설 1은 유의수준 1%에서 채택된다. 따라서 마이크로컴퓨터의 네트워크화 여부는 사용자의 잠재적 보안 위협 인식에 유의적인 영향을 미치는 것을 알 수 있다.

〈표 3〉 네트워크화 여부에 따른 보안 위협 인식에 대한 분산분석표

변수	자유도(df)	F	P
네트워크화 여부	1	12.519	0.0005*

* 유의수준 0.01에서 유의적임

(2) 가설 2, 3의 검증

가설 2, 3은 네트워크화 여부에 따라 보안 위협 인식 수준의 변화에 사용자의 태도가 미치는 조절작용 효과를 보고자 하는 것이다. 이 가설이 검증되기 위해서는 우선적으로 사용자의 태도가 조절변수로서의 자격을 갖추고 있음이 밝혀져야 한다. 조절변수란 일반적으로 독립변수(또는 원인변수)와 종속변수(또는 결과변수)간의 관계성이나 강도에 영향을 미치는 질적변수나 양적변수를 의미한다. 이러한 조절변수는 독립변수와 유의한 상호작용을 통하여 독립변수와 종속변수 간의 관계에 영향을 미쳐야 하고, 하나의 독립변수로서 종속변수에 주 영향을 미쳐야 한다[Baron & Kenny 1986]. Shama[Shama et al. 1981] 등은 조절변수가 독립변수와 상호작용을 하는 동시에 종속변수와 유의적인 관계에 있는 경우 이를 유사조절변수라 하고, 독립변수와의 상호작용이 있는 경우에는 이를 순수조절변수라고 하였다.

조절변수의 영향력 즉, 조절효과를 검증하기 위한 절차로서 세 개의 회귀식을 통하여 회귀계수의 동일성 여부를 확인할 필요가 있다. 즉, XYZ를 각각 독립변수, 종속변수, 조절효과를 검증하기 위한 제3의 변수라 하고 a를 상수항, b를 회귀계수라고 할 때 다음과 같이 세 개의 회귀식으로 나타낼 수 있다.

$$Y = a + b1X \quad (1)$$

$$Y = a + b1X + b2Z \quad (2)$$

$$Y = a + b1X + b2Z + b3XZ \quad (3)$$

세 회귀식 간의 회귀계수를 비교하여 관계를 규명함으로써 변수 Z의 조절효과를 검증해야 하는 것이다. 회귀식 2)와 3)이 유의하게 다르지 않은 경우(즉, b2≠0 ; b3=0일 경우), Z는 조절변수가 아니라 단순히 종속변수를 설명하는 독립변수이다. 회귀식 1)과 2)가 서로 다르지 않고, 회귀식 3)과는 다른 경우(즉, b2=0 ; b3≠0), Z는 순수조절변수가 된다. 회귀식 1), 2), 3) 모두가 서로 다를 경우(즉 b2≠b3 ; b2,b3≠0), Z는 유사조절변수로 분류될 수 있다[Zedeck, 1971].

이 연구에서 독립변수인 네트워크화 여부(X), 종속변수인 보안 위협 인식(Y)에 대하여 사용자 태도(Z)가 조절작용을 할 수 있는 변수인가를 밝히기 위하여 회귀식을 구해보면 다음과 같다.

$$Y = 3.21 + 0.29X \quad (4)$$
$$Y = 2.20 + 0.26X + 0.35Z \quad (5)$$
$$Y = 1.75 + 0.58X + 0.51Z - 0.10XZ \quad (6)$$

회귀식 4), 5), 6)간의 회귀계수를 비교해 보면, 각각 0.29, 0.26, 0.58로 세 개의 회귀식들이 모두 다르게 나타나므로 유사조절변수에 해당됨을 알 수 있다. 즉, 보안통제에 대한 사용자의 태도는 네트워크화 여부와 보안 위협 인식간의 관계를 조절할 수 있는 변수이다.

다음은 각각의 가설 2, 3에 대한 검증을 통하여 태도변수가 실질적으로 조절작용을 하는지 여부를 알아보고, 조절작용을 한다면 어느 정도의 조절작용을 하는지를 검증하였다.

가설 2는 보안 통제에 대한 사용자의 태도가 호의적인 경우 네트워크화 여부에 따라 보안 위협 인식에 유의적인 차이가 있는지를 검증하는 것이다. 이를 검증하기 위하여 태도가 호의적인 집단 내에서 네트워크화 여부와 보안 위협 인식간에 일원분산분석을 실시하였다. 그 결과 <표 4>의 분산분석표에서 보는 바와 같이 P값이 0.0487이므로 가설 2는 5% 유의수준에서 채택된다. 즉, 태도가 호의적일 경우 네트워크화 여부는 사용자의 보안 위협 인식에 유의적인 영향을 미치는 것을 알 수 있다.

〈표 4〉 보안 위협 인식에 대한 분산분석표
(태도가 호의적일 경우)

변 수	자유도	F	P
네트워크화 여부	1	3.9595	0.0487

가설 3은 보안 통제에 대한 사용자의 태도가 비호의적인 경우 네트워크화 여부에 따라 보안 위협 인식에 유의적인 차이가 있는지를 검증하는 것이다. 이를 검증하기 위하여 태도가 비호의적인 집단 내에서의 네트워크화 여부와 보안 위협 인식간에 일원분산분석을 실시하였다. 그 결과 <표 5>의 분산분석표에서 보는 바와 같이 P값이 0.0051이므로 가설 3은 1% 유의수준에서 채택된다. 즉 태도가 비호의적일 경우에도 네트워크화 여부는 사용자의 보안 위협 인식에 유의적인 영향을 미치는 것을 알 수 있다.

〈표 5〉 보안 위협 인식에 대한 분산분석표
(태도가 비호의적일 경우)

변 수	자유도	F	P
네트워크화 여부	1	8.141	0.0051

지금까지 살펴 보았듯이 태도변수가 조절변수로서의 자격을 갖추고 있으며, 가설 2, 3이 채택되었으므로 이제 실질적인 조절효과를 검증하고자 한다. 이를 위하여 태도에 따른 인식의 평균값을 비교하여 태도변수의 조절효과 정도를 살펴보고자 한다. 태도에 따른 보안 위협 인식의 조절효과를 비교하기 위해 하나의 표로 나타내면 다음의 <표 6>과 같다.

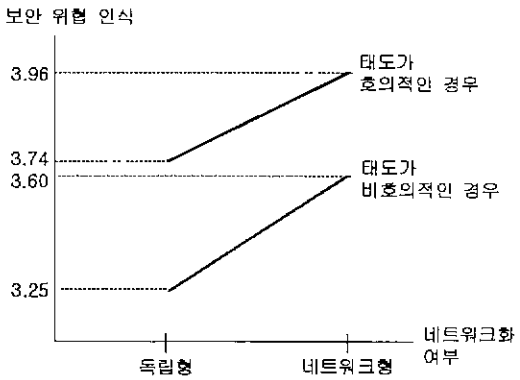
〈표 6〉 태도에 따른 인식의 조절효과 비교

집단구분		표본수	인식의 평균	비교(차이)
호의적	독립형	64	3.74	0.22
	네트워크형	67	3.96	
비호의적	독립형	63	3.25	0.35
	네트워크형	55	3.60	

<표 6>에서 보면 비호의적인 집단의 인식평균의 차이가 0.35로 호의적인 집단의 0.22에 비하여 네트워크화 여부에 따른 보안 위협 인식의 차이가 크게 나타남을 알 수 있다. 즉, 태도변수는 보안 위협 인식을 조절한다고 볼 수 있다. 이러한 조절효과를 보다 구체적으로 살펴보면 다음의 (그림 2)와 같이 나타낼 수 있다. 이러한 꺾은선 그림을 프로파일이라고 하며, 프로파일을 통하여 자료를 분석하는 것을 프로파일 분석이라고 한다.

이러한 결과를 통하여 사용자의 태도가 호의적인 경우 마이크로컴퓨터의 사용환경에 따른 보안 위협 인식의 차이는 적은 반면, 태도가 비호의적인 경우에는 큰 차이를 보이고 있음을 알 수 있다. 이는 조직에서 마이크로컴퓨터 사용자의 보안 통제에 대한 태도를 호의적으로 유도해 나갈 경우

환경의 변화에 따른 보안 위협 인식의 차이를 줄일 수 있으며, 이를 통하여 잠재적 보안 위협에 대한 예방이 가능함을 시사해 준다고 볼 수 있다.



(그림 2) 집단별 보안 위협 인식의 프로파일 분석

또한 정보시스템 보안분야의 연구에 있어서 사용자의 태도에 관한 선행연구는 매우 미흡한 실정인데, 권영규[1994]의 연구에서 처음으로 사용자의 보안 통제에 대한 태도가 보안성과에 영향을 미치는 것으로 밝혀진 바 있다. 따라서 가설 2, 3이 채택되었고, 보안 위협 인식에 대한 태도의 조절효과도 검증됨에 따라 사용자의 태도변수는 정보시스템의 보안에 있어 중요한 요인임을 알 수 있다.

(3) 네트워크 이용도에 따른 보안 위협 인식 검증

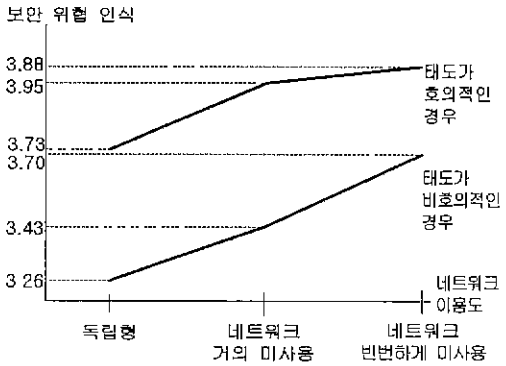
지금까지 네트워크화 여부를 독립형과 네트워크형으로 구분하였는데, 본 절에서는 네트워크환경하에서 마이크로컴퓨터를 사용하는 집단 중에서도 네트워크를 매우 자주 사용하는 집단과 거의 사용하지 않는 집단으로 더 세분화하여 분석하여 보았다. 네트워크형으로 구분된 122개의 표본 중에서 네트워크로 연결되어 있으나 네트워크로 연결하여 수행하는 작업을 전혀하지 않거나 중간 정도로 이용하는 사용자의 표본을 제외한 63개의 표본을 '거의 미사용'과 '빈번 사용' 집단으로 나누었다. 그리고 이 두 집단과 독립형의 세 집단을 비교하여 네트워크 이용도가 보안 위협 인식에 어떠한 영향을 미치는지를 분석하였다. 그 이유는 네트워크 이용도에 따라 관련 보안교육의 빈도 및 수준 등을 달리해야 할 필요성 여부를 살펴보기 위해서이다. 이를 위하여 각각 세 집단의 보안 위협 인식의 평균값을 비교하면 다음의 <표 7>과 같이 나타낼 수 있다.

<표 7>에서 알 수 있는 바와 같이 네트워크를 빈번하게 사용할수록 보안 위협은 높게 인식하고 있는 것으로 나타났다. 네트워크 이용도에 따른 인식 및 태도의 프로파일분석은 각각 (그림 3) 및 (그림 4)와 같이 나타낼 수 있다.

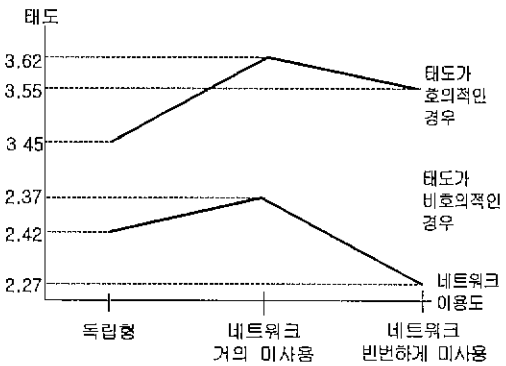
〈표 7〉 집단별 보안 위협 인식의 평균값 비교

태도 \ 네트워크화 여부	독립형	네트워크 거의 미사용	네트워크 빈번 사용
호의적	3.73(65)	3.88(16)	3.95(17)
비호의적	3.26(62)	3.43(13)	3.70(17)

(괄호안은 표본수)



(그림 3) 네트워크 이용도에 따른 프로파일 분석



(그림 4) 태도변수의 프로파일 분석

(그림 3)에서 보면 먼저 비호의적인 경우의 인식에 대한 증가폭이 호의적인 경우의 증가폭 보다 큰 것으로 나타남을 볼 수 있는데 이는 가설검증에서도 살펴보았듯이 태도가 보안 위협 인식의 정도를 조절하는 작용을 하고 있음을 알 수 있다.

또한 네트워크 이용도에 따른 태도의 차이를 알아보기 위해 네트워크화 여부 및 태도에 대한 집단별 태도의 평균값을 비교해 보면 다음의 <표 8>과 같고, 이를 프로파일 분석으로 나타내면 (그림 4)와 같다. 앞의 (그림 3)과 <표 8> 및 (그림 4)를 비교해 보면, 네트워크를 빈번하게 사용할수록 보안 위협은 높게 인식하고 있는 것으로 나타났으나 보안 통제에 대한 태도는 오히려 비호의적인 것으로 밝혀졌다. 이러한 결과를 통하여 네트워크를 빈번하게 사용할수록 보안규정 및 지침 등 현재의 보안대책에 대하여 만족도가 낮은 것으로 생각해 볼 수 있다. 따라서 네트워크를 빈번하게 사용하는 실무자들의 보안 통제에 대한 태도를 보다 호의적으로 유도하기 위해서는 네트워크 보안에 대한 규정의 보완이나 이들에 대한 별도의 보안교육 수준의 강화 등 네트워크 관련 보안대책을 보완해야 할 필요성이 제기되고 있는 것으로 볼 수 있다.

〈표 8〉 집단별 태도의 평균값 비교

네트워크화 여부 / 태도	독립형	네트워크 거의 미사용	네트워크 빈번 사용
호의적	3.45(65)	3.62(16)	3.55(17)
비호의적	2.37(62)	2.42(13)	2.27(17)

(괄호안은 표본수)

5.3 공분산 분석에 의한 통제변수의 통제

독립변수 외에 종속변수인 사용자의 보안 위협 인식에 영향을 줄 수 있는 요소를 알아보기 위하여 공분산 분석을 실시하였다. 그 결과 유의수준 0.01에서 조직의 규모가, 유의수준 0.05에서 컴퓨터 보안교육 정도, 그리고 유의수준 0.1에서 계급 등이 유의적인 것으로 나타났다. 즉, 조직의 규모, 계급 그리고 사용자의 컴퓨터 보안교육 정도에 따라 보안 위협 인식이 다르게 나타남을 알 수 있다. 이는 조직의 규모가 크고 구성원의 계급이 높을수록 중요하고 민감한 정보나 데이터를 취급하기 때문에 잠재적인 보안 위협에 대하여 높게 인식하고 있는 것으로 추측된다. 또한 사용자의 컴퓨터 보안교육의 정도에 따라 보안 위협 인식이 다르게 나타났는데, 이는 보안교육을 많이 받은 사용자일수록 잠재적인 보안 위협을 높게 인식하고 있는 것으로 판단된다.

또한 공분산 분석 결과 종속변수에 유의적인 영향을 줄 수 있는 요소들로 밝혀진 조직의 규모, 계급, 컴퓨터 보안교육 정도 등 세 요소들에 대하여 추가적인 분석을 실시하였다. 즉, 각각의 요소들이 조절변수인 태도변수를 대신하여 보안 위협 인식을 조절하는 작용을 할 수 있는지를 검증하였다. 이 세 요소 중에서 조직의 규모는 연구대상을 일정규모 이상으로 제한하여 이미 통제하였고, 사용자의 계급은 조직에서 임의로 변화시킬 수 있는 요소가 아니므로 조절작용을 한다고 보기 어렵기 때문에 추가분석이 불필요하다. 따라서 태도변수를 대신하여 네트워크화 여부에 따른 보안 위협 인식을 조절할 수 있는 요소인 컴퓨터 보안교육 정도에 대하여 추가적인 검증을 실시하였다. 이를 위하여 교육의 정도에 따라 컴퓨터 보안교육을 전혀 받은 경험이 없는 집단과 교육을 받은 사용자들을 낮은 수준 및 높은 수준의 집단 등 세 집단으로 분류하였다. 여기에서 교육수준의 구분은 교육 경험자들의 교육횟수 및 시간의 전체 평균을 기준으로 평균치 보다 높은 경우에는 높은 수준으로, 평균치 보다 낮은 경우에는 낮은 수준의 집단으로 분류하였다.

그 결과 컴퓨터 보안교육 수준을 강화함에 따라 사용자의 태도를 호의적으로 변화시킬 수 있는 것으로 나타났다. 또한 교육수준은 보안 위협 인식에 유의적인 영향을 미치며, 인식을 어느 정도 조절할 수 있음을 알 수 있다. 그러나 이 연구에서는 독립변수인 네트워크화 여부와 교육수준 간의 상호작용효과는 명확하게 밝히지 못하였는데, 이는 보안교육 수준에 따른 표본의 특성으로 설명이 가능하다. 즉, 전체의 81.5%에 해당되는 응답자(203명)

가 전혀 교육을 받지 못하였거나 교육수준이 낮은 것으로 나타났다. 이는 컴퓨터 보안에 대한 교육이 아직 충분히 확산되지 않았기 때문으로 추측된다. 따라서 이 연구에서는 네트워크화 여부에 따른 보안 위협 인식에 영향을 미침에 있어 교육수준이라는 요소의 조절작용 효과는 명확하게 검증하지 못하였으며, 차후에 컴퓨터에 관한 보안 교육이 충분히 실시된 다음 이에 대한 추가적인 검증이 요구된다.

6. 결론 및 시사점

연구의 목적을 달성하기 위해 마이크로컴퓨터를 실제로 사용하는 실무자들을 대상으로 현장연구를 실시하고, 가설검증을 통하여 다음과 같은 결론을 얻었다.

첫째, 정보시스템의 네트워크화 여부는 정보시스템 사용자의 잠재적인 보안 위협 인식에 유의적인 영향을 미치는 요소이다. 즉, 시스템이 네트워크화 됨에 따라 사용자들은 잠재적인 보안 위협에 대하여 높게 인식하고 있는 것으로 나타났다.

둘째, 정보시스템 보안 통제에 대한 사용자의 태도는 보안 위협 인식을 조절하는 작용을 한다. 즉 사용자의 태도가 호의적인 경우 보다 비호의적인 경우에 보안 위협에 대한 인식에 더 큰 차이를 보이는 것으로 나타났다.

이 연구는 정보시스템 보안에 관한 연구에 있어서 점차 그 중요성은 강조되고 있으나 연구가 미흡한 분야인 네트워크화가 사용자들의 보안 위협 인식에 미치는 효과를 밝히고, 역시 그 동안 간과되었던 분야이며, 추가적인 검증이 요구되는 사용자의 태도와 같은 심리적인 요인의 보안 위협 인식에 대한 조절작용 효과를 밝히고자 하는데 그 의의가 있다. 이 연구의 결과는 다음과 같은 중요한 점을 시사하고 있다.

먼저 정보시스템의 네트워크화 여부는 정보시스템 사용자의 보안 위협 인식에 영향을 미치는 중요한 요소로 밝혀졌다. 이러한 결과는 조직의 책임자들을 대상으로 실시되었던 기존의 연구결과와는 달리 네트워크 환경하에서의 보안 위협에 대한 사용자들의 인식이 과거에 비하여 향상되었음을 사사하고 있다. 따라서 조직에서 보안 위협 인식 제고를 통하여 보안성과를 향상시키기 위해서는 보안 계획 수립시 이러한 요소를 고려해야 할 것임을 시사하고 있다.

그리고 정보시스템의 보안 통제에 대한 사용자의 태도는 보안 위협 인식을 조절하는 작용을 하는 것으로 밝혀졌다. 즉, 사용자의 태도가 비호의적일 경우, 호의적인 경우에 비하여 보안 위협 인식에 대한 차이가 크게 나타났다. 이는 조직에서 마이크로컴퓨터 사용자의 태도를 호의적으로 유도해 나갈 경우 환경의 변화에 따른 보안 위협 인식의 차이를 줄일 수 있으며, 이를 통하여 잠재적 보안 위협에 대한 예방이 가능함을 시사해 준다고 볼 수 있다.

한편, 이 연구에서는 가설의 검증과는 별도로 수집된 자료들에 대한 추가적인 분석을 통하여 몇 가지의 결과를 도출하였는데, 그 내용 및 시사점은 다음과 같다.

첫째, 정보시스템의 네트워크를 빈번하게 사용할수록 보안 위협은 높게 인식하고 있으나, 오히려 보안 통제에 대한 태도는 비호의적인 것으로 나타났다. 이러한 결과를 통하여 네트워크를 빈번하게 사용할수록 보안규정 및 지침 등 현재의 보안대책에 대하여 만족도가 낮은 것으로 생각해 볼 수 있다. 따라서 조직에서는 보안성과를 향상시키기 위하여 네트워크를 빈번하게 사용하는 구성원들의 태도를 보다 호의적으로 유도하기 위한 별도의 대책을 강구해야 할 필요가 있음을 알 수 있다. 예를 들면, 네트워크 관련 보안규정의 보완, 보안교육 수준의 강화 등이 여기에 해당될 수 있을 것이다.

둘째, 정보시스템 보안에 관한 교육 수준은 보안 위협 인식에 유의적인 영향을 미치며, 보안 위협에 대한 인식을 어느 정도 조절할 수 있다. 즉, 보안교육을 강화할 경우 정보시스템 사용자들의 보안 위협 인식이 높아질 것을 기대할 수 있다. 그러나 이 연구에서는 네트워크화 여부와 보안교육

수준간의 상호작용효과를 분명하게 밝히지 못함으로써 조절작용 효과를 명확하게 규명하지는 못하였다. 이는 전체 응답자 중 상당수(81.5%)가 전혀 컴퓨터 보안교육의 경험이 없거나 교육수준이 낮은 것으로 조사되었기 때문으로 보인다. 이러한 결과는 전반적인 컴퓨터관련 보안교육이 아직 미흡한 수준임을 시사해 준다.

셋째, 정보시스템 보안에 관한 교육 수준을 향상시킬 경우 사용자의 태도를 호의적인 방향으로 변화시킬 수 있다. 이 연구에서는 「네트워크화 여부 보안교육 수준 사용자의 태도 보안 위협 인식 보안성과」 등의 관계에 대하여 부분적인 검증을 하는데 불과하였다. 따라서 이러한 변수들간의 인과관계 등을 밝히기 위한 추가적인 연구가 요구된다.

결론적으로 이와 같은 연구결과는 최근 들어 정보시스템의 네트워크화가 급속히 진전되고 있는 사용환경하에서, 이에 따른 사용자들에 대한 관리를 통하여 적절한 보안대책이 강구되어야 함을 실증적으로 밝혔다는 점에서 중요한 의의를 갖는다. 따라서 향후 조직에서는 사용자의 태도와 같은 심리적 요인을 호의적으로 유도하기 위하여 네트워크와 관련한 각종 보안대책을 보완하고, 특히 네트워크를 빈번하게 사용하는 실무자들에게 별도의 보안교육을 강화하는 등 전반적으로 정보시스템에 대한 보안교육 수준의 향상을 위한 대책을 강구해야 할 것이다.

7. 연구의 한계 및 향후 연구방향

연구를 진행하는 과정에서 나타난 한계점들은 다음과 같다.

먼저 이 연구의 가장 큰 한계점은 비영리기관인 군조직을 대상으로한 현장연구를 채택함으로써 다른 조직으로 일반화시키는데 다소 문제가 있다는 점이다. 즉, 외생변수의 개입 가능성을 배제할 수 없었다는 점이다. 따라서 연구의 대상을 영리기관인 일반 기업 등으로 확대하여 현장인터뷰를 병행하는 등 연구방법의 보완을 통한 추가적인 연구가 필요하다.

그리고 이 연구의 근간이 되는 이론적 배경 부분에서 네트워크화가 진행됨에 따라 보안 위협이 증가하며, 이러한 네트워크화 여부가 사용자의 보안 위협 인식에 영향을 미칠 것이라는 내용을 설명하였다. 이러한 현상에 대한 설명은 기존의 연구를 통해 할 수 있었으나, 구체적인 이유에 대한 설명이 다소 부족하였다. 이는 네트워크 보안문제와 관련된 기존의 연구가 매우 미흡하기 때문이다. 이러한 한계점은 앞으로 이와 관련된 연구들이 진행됨에 따라 해결될 수 있는 부분이라 생각된다.

또한 이 연구에서 가설의 검증 이외에 추가적으로 분석한 부분에서 보안교육 수준이 보안 위협 인식을 조절하는 효과와 보안교육 수준이 태도에 미치는 영향에 대하여 명확하게 규명하지 못하였다. 이 연구에서는 네트워크화 여부와 보안 위협 인식간의 관계, 그리고 태도의 조절작용을 규명하는데 초점을 맞추었다. 따라서 「네트워크화 여부 보안교육 수준 사용자의 태도 보안 위협 인식 보안성과」 등의 변수들간의 인과관계를 검증할 수 있는 추가적인 연구가 필요하다.

그리고 이 연구에서는 종속변수를 사용자들의 보안 위협 인식으로 정의하고 이를 보안의 성과와 연결하여 생각하였으나, 향후 보다 객관적으로 보안성과를 측정할 수 있는 측정도구의 개발이 요구된다. 예를 들면, 조직내 사용자들의 보안 규정에 대한 위반 횟수, 보안 사고사례 및 유형 등 계량적인 자료의 수집 및 분석을 통하여 가능할 것이다. 마지막으로 인간의 인식, 태도 등의 변수가 단일 시점에서 측정됨으로써 시간적 변화에 따른 외생변수의 개입을 통제할 수 없었다는 점이다. 이 같은 한계점을 극복하기 위해서는 장기간에 걸친 종단적 연구가 필요하다고 본다.

참 고 문 헌

[1] 권영규, "마이크로컴퓨터의 보안통제에 대한 사용자의 인식과 태도가 보안성과에 미치는 영향", 연세대학교 석사학위 논문, 1994.

[2] 김세헌, "효율적인 정보시스템 보안대책", 「경영과 컴퓨터」, 1990. 7, pp.196-198.

[3] 김종기, "정보시스템 보안의 상황적 모형", 한국경영정보학회 '94 추계학술대회 논문집, pp. 299-312.

[4] 김준석, 「정보시스템 : 경영관리적 관점에서」, 법문사, 1996.

[5] 이종삼, "국내기업 정보시스템 Security 위협요소에 관한 연구", 중앙대학교 석사학위 논문, 1994.

[6] 이학종, 「조직행위론 : 이론과 사례연구」, 세경사, 1991.

[7] 이형원, 「정보 시스템 안전대책」, 영진출판사, 1993.

[8] 정인근, 유지선, "정보시스템의 주요관리대상에 관한 연구", 경영정보학연구, 제1권 제2호, 1991. 12, pp.37-56.

[9] 전자신문사, "230개 기업 대상 '정보 보안 실태' 설문조사", 「컴퓨터와 커뮤니케이션」, 1996. 6, pp.88-129.

[10] Ball, L. and R. Harris, "SMIS Member : A Membership Analysis," *MIS Quarterly*, 1982, pp.19-38.

[11] Banks, S., "Security Policy," *Computers & Security*, Vol.9, No.7, November, 1990, pp. 605-610.

[12] Barki, H. and J. Hartwick, "Measuring User Participation, User Involvement, and User Attitude," *MIS Quarterly*, Vol.18, No.1, 1994, pp.59-82.

[13] Baron, R.M. and D.A. Kenny, "The Moderator-Mediator Variable Distinction in Social Psychological Research : Conceptual, Strategic, and Statistical Considerations," *Journal of Personality and Psychology*, Vol.51, No.6, 1986, pp.1173-1182.

[14] Benson, D. H., "A Field Study of End User Computing : Findings and Issues," *MIS Quarterly*, Vol.7, No.4, December, 1983, pp.35-45.

[15] Boockholdt, J.L., "Security and Integrity Controls for Microcomputer : A summary Analysis," *Information & Management*, 1987, pp.33-41.

[16] Brancheau, J.C. and J.C. Wetherbe, "Key Issues in Information Systems Management," *MIS Quarterly*, Vol.11, No.1, 1987, pp.23-45.

[17] Canning, R.G., "Information Security and Privacy," *EDP Analyzer*, 1986.

[18] Caudle, S.L., W.L. Gorr and K.E. Newcomer, "Key Information Systems Management Issues for the Public Sector," *MIS Quarterly*, Vol.15, No.2, 1991, pp.171-188.

[19] Curt, H. and M. Herbert, "1985 Opinion Survey of MIS Managers : Key Issues," *MIS Quarterly*, Vol.10, No.4, 1986, pp.351-361.

[20] Dickson., G.W., R.L. Leitheiser, J.C. Wetherbe, and M. Nechis, "Key Information Systems Issues for the 1980's," *MIS Quarterly*, Vol.8, No.3, September, 1984, pp.135-159.

[21] Donovan, S., "Security of PCs in a Distributed Environment," *Computers & Security*, Vol.12, No.1, 1993, pp.28-31.

[22] Frank, J., B. Shamir and W. Briggs, "Security-related behavior of PC users in organization," *Information & Management*, June, 1991, pp.127-135.

[23] Frank, J., "Quality Control of Personal Computing," *Journal of System Management*, 1988, pp.32-39.

[24] Geoff N., "PC Security Issues," *Computers & Security*, Vol.11, No.5, 1992, pp.412-416.

[25] Goodhue, D.L. and D.M. Straub, "Security Concerns of System Users - A Study of Perception of the Adequacy of Security," *Information & Management*, 1991, pp.13-27.

[26] Henderson, J.C. and M.E. Treacy, "Managing End-User Computing for Competitive Ad-

vantage," *Sloan Management Review*, Winter, 1986, pp.3-13.

[27] Highland, H.J., "The Security Impact of Networks, Telecommunications, and Office Automation," *Computers & Security*, Vol. 11, No.3, 1992, pp.229.

[28] Hoffer, J.A. and D.W. Straub, "The 9 to 5 Underground : Are you Policing Computer Crimes?," *Solan Management Review*, Vol. 30, No.2, Summer, 1989, pp.35-43.

[29] Kelly, D.W., "A Guide to Cost-Effective PC Security," *Security Management*, Vol.32, No.10, October, 1988, pp.55-88.

[30] Kim, J., "An Empirical Investigation of Influencing the Effectiveness of Information System Security," *Doctoral dissertation*, Mississippi State University, Mississipi, 1992.

[31] Loch, K.D., H.C. Houston and M.E. Warkentin, "Threats to Information Systems : Today's Reality, Yesterday's Understanding," *MIS Quarterly*, June, 1992, pp.173-186.

[32] Lucas, H.C., "Empirical Evidence for a Descriptive Model of Implementation," *MIS Quarterly*, June, 1978, pp.27-42.

[33] Madnick, S.E., "Management Policies and Procedures Needed for Effective Computer Security," *Solan Management Review*, Vol. 19, No.3, Fall, 1978. pp.61-73.

[34] Menkus, B., "How to Begin Dealing with Computer Security," *Computers & Security*, Vol.10, No.3, May, 1991, pp.199-203.

[35] Niderman, F., J.C. Brancheue and J.C. Wetherbe, "Information Systems Management Issues for the 1990s," *MIS Quarterly*, Vol.15, No.4, December, 1991, pp.475-502.

[36] Ouchi, W., "A Conceptual Framework for Design of Organizational Control Mechanisms," *Management Science*, Vol.25, No.9, 1979, pp.833-848.

[37] Pfleeger, C.P., *Security in Computing*, Prentice Hall, Inc., 1989.

[38] Post, G.V. and K.Kievit, "Accessibility vs. Security," *Computers & Security*, Vol.10, No.4, June, 1991, pp.331-344.

[39] Raymond, B.C., and A. Baggaley, "The Objective Measurement of Attitude Motivation : Development Evalutation of Principles and Devices, *Journal of Personality*, 1956, pp.421.

[40] Rivera, A.L., "The Weak Link," *Security Management*, Vol.25, No.8, August, 1991, pp.91-92.

[41] Robey, D., "User Attitude and Management Information System Use," *Academy of Management Journal*, Vol.22, No.3, 1979, pp.527-538.

[42] Schewe, C.D., "The Management Information System User : An Explorator Behavioral Analysis," *Academy of Management Journal*, December, 1976, pp.577-590.

[43] Sharma, S., R.M. Durand, and O. Gur-Arie, "Identification and Analysis of Moderator Variables," *Journal of Marketing Research*, Vol.18, August, 1981, pp.80-107.

[44] Shimcha, R., "Personal Values : A Basis for Work Motivational Set and Work Attitude," *Organizational Behavior and Human Performance*, Vol.21, 1978. pp.80-107.

[45] Stone, E.F., *Research Methods in Organizational Behavior*, Scott, Foreman and Company, 1981, pp.22-29.

[46] Zedeck, S., "Problems of the use of Moderator Variables," *Phychological Bulletin*, Vol. 76, October, 1971, pp.295-310.

저자소개

이 찬 희

해군사관학교를 졸업하고, 연세대학교 경영학과에서 정보시스템을 전공하여 석사학위를 취득하였으며, 현재 해군 소령으로 재직 중이다.

김 준 석

현재 연세대학교 경영학과 교수로 재직 중이다. 그는 연세대학교 상학과를 졸업하고, 인디아나 대학교(Indiana University)에서 경영학 석사와 박사학위를 취득하였으며, 동 대학의 교환교수를 역임한 바 있다. 그의 주요 관심분야는 "정보기술과 조직성과 간의 관계"로서 모형구축에 초점을 맞추고 있다.

서 길 수

연세대학교 경영학과를 졸업하고, 인디아나대학교(Indiana University)에서 정보시스템을 전공하여 경영학 석사와 박사를 취득한 후, 현재 연세대학교 경영학과 부교수로 재직 중이다. 주요 관심분야는 매체 관련 이론, 사용자 접속, 데이터베이스 모델링, 인터넷 마케팅 등이다.

부 록 : 설문지

설 문 지

【보안 통제에 대한 태도에 관한 질문】

1. 보안규정은 유용하다고 생각한다.	전혀 그렇지 않다.	①	②	③	④	⑤	매우 그렇다
2. 보안규정은 좋은 것이다.	전혀 그렇지 않다.	①	②	③	④	⑤	매우 그렇다
3. 보안규정은 가치가 있는 것이다.	전혀 그렇지 않다.	①	②	③	④	⑤	매우 그렇다
4. 보안규정은 업무수행에 지장을 주지 않는다.	전혀 그렇지 않다.	①	②	③	④	⑤	매우 그렇다
5. 보안규정을 준수한다는 것은 흥미로운 일이다.	전혀 그렇지 않다.	①	②	③	④	⑤	매우 그렇다
6. 보안규정에 대한 거부감을 느끼지 않는다.	전혀 그렇지 않다.	①	②	③	④	⑤	매우 그렇다
7. 보안규정은 나의 적성에 맞는다.	전혀 그렇지 않다.	①	②	③	④	⑤	매우 그렇다
8. 보안규정은 좋아할만 하다.	전혀 그렇지 않다.	①	②	③	④	⑤	매우 그렇다
9. 보안규정은 매우 세밀하게 규정되어 있다.	전혀 그렇지 않다.	①	②	③	④	⑤	매우 그렇다
10. 귀하는 컴퓨터 보안규정에 대해 호감이 있습니까?	전혀 그렇지 않다.	①	②	③	④	⑤	매우 그렇다

【보안 위협 인식에 관한 질문】

1. 하드디스크 파일들에 대한 주기적인 정리와 백업(Back-up)을 해야 한다.

2. 백업된 디스켓을 규정된 적정 장소에 보관해야 한다.

3. 데이터 및 시스템(PC)에 대한 비인가된 접근을 통제하기 위하여 패스워드를 사용해야 한다.

4. 패스워드는 주기적으로 변경해야 하며, 취급자 또는 관리책임자 교체시 즉시 변경해야 한다.

5. PC 작업후 작업내용을 작업일지에 기록해야 한다.

6. 플로피 디스켓의 주기적인 백업을 실시해야 한다.

7. 사용하고 있지 않은 플로피디스켓을 규정된 적정 장소에 보관해야 한다.

8. 인가되지 않은 하드웨어를 부서내로 반입해서는 않된다.

9. 부서에서 사용하고 있는 소프트웨어를 무단복제해서는 않된다.

10. 부서에서 사용하고 있는 각 PC에 대한 관리 책임자를 임명하고, 취급자를 제한해야 한다.

11. 귀하의 조직(부대)에서 요구하고 있는 컴퓨터 보안관련 제 규정 및 절차들이 지켜지지 않을 경우 보안의 위협에 노출될 가능성이 있다고 생각하십니까?

	매우 낮다.	①	②	③	④	⑤	매우 높다
1		□	□	□	□	□	
2		□	□	□	□	□	
3		□	□	□	□	□	
4		□	□	□	□	□	
5		□	□	□	□	□	
6		□	□	□	□	□	
7		□	□	□	□	□	
8		□	□	□	□	□	
9		□	□	□	□	□	
10		□	□	□	□	□	
11		□	□	□	□	□	