패스워드 선택을 위한 사용자의 보안행위의도에 영향을 미치는 요인

김종기[a] 강다연[b]

[a] 부산대학교 경영학부 부교수
부산 금정구 장전동 산30번지, 609-735
Tel: +82-51-510-2582, E-mail: jkkim1@pusan.ac.kr

[b] 부산대학교 일반대학원 경영학과
부산 금정구 장전동 산30 번지, 609-735
Tel: +82-51-510-2582, E-mail:kdy@pusan.ac.kr

Abstract

최근 정보시스템의 개방성과 접근성의 확대는 조직 내·외부로부터 보안위협을 증가시키고 있다. 일반적으로 정보시스템은 패스워드를 이용하여 사용자 인증과 자료의 접근을 제한하고 있으므로 패스워드의 선택은 정보보안에 있어서 매우 중요하다. 적절한 패스워드의 선택은 정보시스템의 오·남용 방지 및 불법적인 사용자의 제한 등의 보안효과를 가져올 것이다.

본 연구의 목적은 정보를 보호하기 위한 적절한 패스워드선택을 위한 사용자의 보안행위의도에 미치는 요인을 분석하는 것이다. 이를 위하여 정보시스템 사용자의 적절한 패스워드의 선택에 영향을 미치는 핵심적인 요인으로 위험분석 방법론을 토대로 한 위험을 활용한다. 또한 위험을 사용자의 보안의식과 패스워드 관리지침을 패스워드 선택의 태도에 영향을 미치는 요인으로 보고, 사용자의 적절한 패스워드의 보안행위의도를 TRA(Theory of Reasoned Action)를 기반으로 모형을 설계하였다.

본 연구를 분석한 결과 정보자산이 위험에 관련성이 없는 반면, 정보자산을 제외한 위협, 취약성, 위험, 사용자의 보안의식, 패스워드 보안태도, 보안행위의도는 요인간에 유의한 영향을 미치는 것으로 분석되었다.

Keywords:
패스워드 보안태도, 보안행위의도, 보안인식

I. 서론

정보시스템의 급속한 발전에 따라 정보보안의 관점에서 패스워드의 사용은 정보시스템 보안에 있어서 일부에 지나치지 않지만 패스워드의 선택은 정보보안의 활동 중 매우 중요하다(한국전산원, 1997). 오늘날 정보화 사회는 컴퓨터 사용자들은 패스워드를 만들고 사용하는데 있어서 보안의식이 매우 낮은 것으로 판단되며, 또한 쉽게 추측할 수 있는 패스워드를 만드는 경향이 있다. 해킹의 첫 관문이라 할 수 있는 패스워드에 대한 보안교육이 철저하게 이루어져야 할 것이며, 조직은 패스워드의 선택과 사용에 관한 규범을 제정할 필요가 있다(정경수 외, 2001). 정보화 사회에서 정보의 수집, 분석 및 활용능력은 국내. 외의 경쟁력을 좌우하는 중요한 자산이라 할 수 있다. 그러나 정보를 취급하는 과정에서 오는 취약성으로 인하여 정보에 대한 무단 유출 및 파괴, 변조 등과 같은 공격이 자행되고 있으며, 또한 인가 받지 않은 불법적인 사용자에 의한 정보시스템의 파괴, 개인신상 비밀의 누설 및 유출, 불건전 정보의 유통등과 같은 피해도 증가하고 있다. 이에 따른 피해를 줄이고자 정보보안의 방법 중 하나가 패스워드의 선택이라고 할 수 있겠다.

위험의 선행요인인 자산, 위협취약성, 그리고 위험, 사용자 보안인식, 패스워드보안태도를 보안행위의도에 미치는 요인으로 보고 실증적으로 분석하고자 한다..

II. 선행연구

1. 패스워드 선택과 정보보안

정보기술 시스템의 다양화로 인해 사용자들이 필요로 하는 아이디와 패스워드가 범람하는 사회에 이르렀고, 다양한 애플리케이션과 운영체제를 관리하여야 하는 시스템 운영자의 관점에서도 아이디와 패스워드의 관리에서도 많은 문제점이 노출되었다. 이러한 패스워드의 노출을 방지하기 위한 최적의 방법 중 하나가 적절한 패스워드의 선택이라 하겠다. 패스워드는 시스템에 들어가고자 하는 사용자를 인증하거나 시스템을 이용하고 있는 사용자에게 자료의 접근을 제한하는 용도로 이용된다(이필중, 문희철, 1991).

정보통신 기술의 발달로 인한 컴퓨터범죄가 급속히 증가하는 가운데 한 국가의 기간 정보통신망에

막대한 해를 입히는 경우도 있는데, 이는 정보보안 기술적 측면에서의 컴퓨터범죄를 사전에 막기 위한 목적으로 개발된 기술 또는 보안 시스템을 중요시 할 필요가 있다고 하겠다(김세헌, 2002). 이에 따른 보안방법으로 패스워드의 선택에 있어서 안전한 패스워드를 선택하여 정보보안을 하도록 몇 가지 권고사항이 있다. 우선, 패스워드는 보통 10자리 미만의 짧은 길이를 가지기 때문에 이를 안전하게 만들기가 어렵다. 따라서 패스워드의 길이를 충분히 길게 하고, 패스워드 선택 시 사전에 나올만한 실제 단어는 피하며, 자신의 신상정보와 관련된 단어, 숫자는 되도록 피해야 한다. 그리고 패스워드를 정기적으로 교체 해야 한다. 또한 패스워드를 머릿속에 기억하고, 적어서 보관하지 말고, 키보드에서 연속된 문자열을 사용하지 않도록 권고한다. 이에 정보의 위협에 대한 취약성을 보안할 수 있다(BSI, 1999).

2. 위험분석 방법론

정보를 보호하기 위한 관점에서 위험분석방법론은 정보보호 서비스의 취약점을 인식하고 이를 보호하기 위해 자산, 위협, 취약성의 문제점을 해결하고 보호하는 방법이 최선의 방법이라 할 수 있겠다. 위험 분석이란 정보자산이 갖고 있는 취약성에 따라 사고가 발생할 수 있는 가능성과 피해 수준을 예측하는 것이다. 이를 통해 혹시나 발생할 수 있는 위험의 정도를 평가하고 이를 감소시킬 수 있는 통제 방법을 도출하는 것이다. 특히 취약성과 위협의 증가는 시간에 따라 계속 증가하며 이에 대응하는 보호대책은 일정시간이 흐른 뒤에 진행된다(김인중 외 , 2005).

위험 분석은 위험관리 과정 중 가장 중요한 단계로써 자산 위협, 취약성, 보안대책, 그리고 손실을 계산하는 여러 요소들 간의 관계를 분석하는 과정이다(김기윤 외, 1994). 위험분석은 보안관련 항목들에 대한 위험파악과 위험평가로 구성된다(최상수 외, 2003). 위험분석의 모형은 자산, 위협, 취약성에 대한 위험의 분석단계와 위험에 대한 보안대책의 관리단계로 나타낸다(Tregear, 2001). 위험관리는 위험에 의한 피해를 최소화하기 위해 보안정책을 수립하고 이에 기반한 보안통제를 통해 기업 보안수준을 일정 수준이상으로 유지할 수 있도록 하는 것이 목표라고 하겠다. 이와 같이 위험분석은 요구되는 정보보호서비스의 취약점을 해결하고 그에 따른 위험관리에 대한 정보보안의 대책이 필수적이라고 하겠다.

III. 연구모형 및 가설 설정

1. 연구모형의 설계

본 연구에서는 정보시스템 사용자의 적절한 패스워드의 선택을 위한 요인들을 위험분석 방법론(Tregear, 2001)을 토대로, 자산, 위협, 취약성을 분석하여 발생 가능한 위험을 측정한 후, 이에 따른 위험을 사용자의 보안의식에 영향을 미치는 요인으로 보고, 또한 사용자의 보안의식이 패스워드 보안의 태도에 영향을 미치는 요인으로 보고, 패스워드 보안태도에 따른 패스워드의 보안행위의도를 TRA(Theory of Reasoned Action)를 참조하여 <그림 1> 연구모형을 구성하였다.

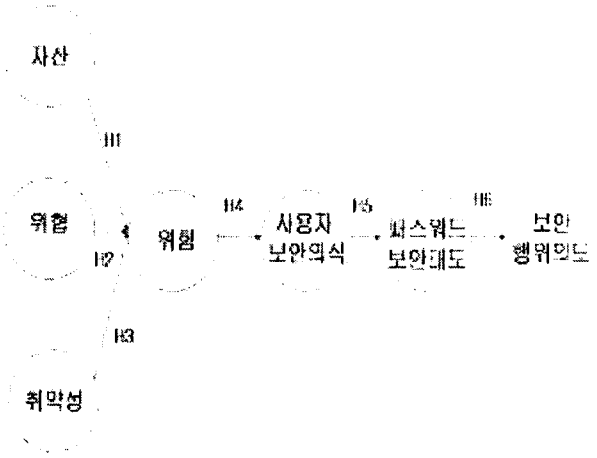

그림1-패스워드 선택이 사용자의 행위의도에 미치는 요인에 관한 모형

2. 연구모형의 가설

1) 위협과 선행요인간의 관계

자산은 하드웨어, 소프트웨어, 데이터, 등 물리적인 유형자산뿐만 아니라 인적, 조직의 이미지 등 무형자산도 포함한다(CMU/SEI, 1999). 자산을 식별하기 위해서는 많은 비용과 시간 등의 제약조건을 통해서 구체적으로 분석하여야 한다(Rainer et al., 1991). 본 연구에서의 정보자산이란 패스워드의 노출에 대해 보호되어야 할 요소로 데이터파일, 인증과정의 개인신상 정보, 업무관련의 정보를 포함한다.

가설1: 정보시스템 사용자의 정보자산은 위험에 긍정적인 영향을 미칠 것이다.

위협은 자산에 해를 줄 수 있는 위험의 원천이며 특히 해킹, 테러, 시스템 결함 등과 같은 의도적인 위험으로부터 사용자의 패스워드가 불법적으로 노출되는 것을 말한다(이필중 & 문희철, 1991; BSI, 1999). 위협은 위협원천의 위치에 따라서 내부 및 외부위협으로, 가해자가 누구인가에 따라서 인간 및 비인간위협으로, 또한 의도의 유무에 따라서 우연적 및 의도적 위협으로 구분했다. (Loch et al., 1992).

위협은 위협의 특성이나 위협의 원천에 따라서

정보에 대한 접근을 제어한다. 이에 따른 접근을 제어하는 것은 정보의 소유자가 원하는 대로 비밀이 유지 되어야 하는 비밀성과, 정해진 절차와 주어진 권한에 의해서 정보가 변경되어야 하는 무결성과, 정보자산이 허가된 자에게는 필요 시에 편리하게 사용할 수 있는 가용성의 위험이 존재한다(Jackson et al., 1992).즉 위협은 위험에 영향을 미친다고 하겠다.

가설 2: 정보시스템 사용자의 위협은 위험에 긍정적인 영향을 미칠 것이다

취약성은 정보시스템에 손해를 끼치는 원인이 될 수 있는 조직, 절차, 인력관리, 행정, 하드웨어, 소프트웨어의 약점을 말한다(BSI, 1999). 정보시스템에 해를 끼치는 원인 등의 공격을 위협에 대해서 공격을 방지할 수 있는 보안대책이 미비하다는 것이 특징이다(Gilbert, 1991). 취약성 분석은 환경과 기존의 보안대책을 고려하여 현존하는 위협의 공격대상이 될 수 있는 자산의 약점을 검사하는 것이다(한국전산원, 1997; NIST, 2001). 자산에 손실이 발생될 수 있는 약점을 식별하고 분류하여 위협을 감소시키도록 하는 것이 취약성의 목적이라 보며(김법진, 1996; CSE, 1996), 이는 취약성이 위험에 영향을 미치는 것을 알 수 있다.

가설 3: 정보시스템 사용자의 취약성은 위험에 긍정적인 영향을 미칠 것이다.

2) 보안 태도와 선행요인간의 관계

위험은 특정 위협이 취약성을 이용하여 자산을 공격해서 손상을 초래할 수 있는 잠재력이다(한국전산원, 1997). 정보 자산마다 취약성을 파악하고 위험발생 가능성을 측정, 위험 보장 수준에 따른 손실을 분석하는 과정이다(ISO/IEC, 2000). 위험은 자산, 취약성, 위협 분석과정을 통해 최종적으로 도출되는 수치로써, 위험분석을 통해 닥치게 될지 모르는 위험을 파악하고 나면 조직은 존재 위험에 대한 수용 여부를 결정한다고 하였다. 위험이란 조직에 악영향을 미치는 불확실한 사건들의 발생으로 인해 조직이 평균적으로 받을 것으로 예상되는 충격의 양의 대한 측정치를 말한다(NIST, 2001) 즉, 정보시스템의 위험은 보안태도에 영향을 미칠 것이다.

가설4: 정보시스템 위험은 보안태도에 긍정적인 영향을 미칠 것이다.

정보시스템 사용자는 스스로 정보보안에 대한 보안인식을 가지고 있어야 한다. 2006년 정보보호 실태조사 결과 중 가장 먼저 눈길이 가는' 정보보호 인식 부문' 에서 응답자의 대부분인 약 98.2%(매우 중요 60.5%, 중요한 편 37.7%)가 정보보호의 중요성을 인식하고 있었다. 정보보호의 중요성에 대한 인식이 높게 나타난 것은 단순히 당위적인 측면만이 아닌 정보화 역기능에 대한 두려움과 결부된 실질적인 관심인 것이다. (KISA, 2007).

특정행위와 관련된 개인의 태도는 해당 행위를 수행하기 위한 긍정적 또는 부정적으로 평가한다(Davis, 1989; Ajzen &Fishbein, 1980).

이는 정보시스템을 사용하는 사용자가 직접적으로 정보보안에 대한 인식을 가지고 있고 정보보안에 대한 보안태도에 영향을 미친다고 하겠다.

가설 5: 정보시스템 위험은 특히 사용자의 보안의식이 보안태도에 긍정적인 영향을 미칠 것이다.

3) 패스워드보안태도와 보안행위의도간의 관계

정보시스템 사용자가 패스워드의 보안관리로부터의 긍정적인 태도를 형성하고 있을 경우 패스워드 노출위험의 방지를 위한 적극적인 보안행위의도를 가지게 된다. 적극적인 태도와 행위에 대한 믿음이 강할수록 행위를 수행하고자 하는 개인의 의도가 더욱 강해진다(Davis, 1989; Ajzen &Fishbein, 1990). 이는 패스워드의 보안을 위한 태도로부터 패스워드의 노출에 보호하기 위한 충분한 보안행위의도를 측정할 수 있다.

가설 6: 패스워드 보안태도는 보안행위의도에 긍정적인 영향을 미칠 것이다.

3. 연구 변수의 설문항목

본 연구모형과 가설을 검증하기 위해 실증연구와 분석을 하기 전 조작적 정의가 필수적이다. 조작적 정의는 측정에 앞서 정의된 변수의 개념적 정의를 보다 구체적인 형태로 표현한 것으로 실증검증에 전제되는 관찰가능성, 즉 측정가능성과 직결된 정의이다(채서일, 2005). 패스워드 선택이 보안행위의도에 미치는 영향을 검정하기 위해 연구변수를 설정하였다. 모든 측정항목은 리커트(Likert) 7점 척도로 구성하였다<표1>.

표1-연구변수의 설문항목

변수	설문항목	관련문헌
자산 (AS)	데이터파일의 중요성 인증정보의 중요성 업무관련정보의 중요성 개인정보의 중요성	CMU/SEI(1999) NIST(2001) Rainer(1991)
위협 (TH)	타인노출 가능성 해커의 도청가능성 공개 악용 될 가능성 허락무의 접근 가능성 해커의 노출가능성	BSI(1999) Loch et al.(1992) Jackson et al.(1992) 이필중&문희철(1991)
취약성 (VL)	사용기간의 노출 기억의 한계 중복사용의 노출	CSE(1996) NIST(2001) Gilbert(1991)

	공유의 정보유출 추측의 용이성	김법진(1996) 한국전산원(1997)
위험 (RSK)	업무방해 위험 프로그램 삭제 위험 중요파일 삭제 위험 중요정보공개 위험 개인 신상 노출 위험	ISO/IEC(2000) NIST(2001) Milier et al.(1996) Rainer(1991) 이문구(2004)
사용자 보안 의식 (USR)	패스워드 기억정도 어려운패스워드설정정도 패스워드 변경 정도 타인노출 방지 정도 새로운 패스워드 생성	정경수&김기영(1999) 이필중&문희철(1991)
보안 태도 (AT)	보안 교육 참여의 태도 기억에 의존한 호의성 시스템 변경방지 태도 화면보호기능의 태도 관리자제공패스워드변경	Ajzen& Fishbein(1980) Davis et al. (1989) Roger A(2006)
보안 행위 의도 (INT)	상이한패스워드사용의도 개인신상피한 사용의도 기록하지 않을 의도 패스워드갱신 의도 공유금지 의도	Davis et al., (1989) Ajzen& Fishbein(1980) BSI(1999)

Ⅳ. 실증분석 및 결과

4.1 연구절차

본 연구에서는 수집된 자료를 분석하기 위해서 SPSS Windows 12.0과 LISREL 5.1를 이용하였다. 먼저 SPSS Windows 12.0을 이용하여 대상자의 인구통계학적 특성을 분석하였다.

다음으로 패스워드 선택이 보안행위의도에 미치는 영향에 대한 선행 변수인 자산, 위협, 취약성, 위험, 사용자의 보안의식, 보안태도, 보안행위의도에 관한 가설을 검증하기 위하여 먼저 SPSS Windows 12.0으로 총 32개 변수로 탐색적 요인분석을 한 결과 7개의 변수가 제거된 25개의 변수를 통한 LISEL5.1를 이용한 구조방정식 모형분석을 실시하였다.

4.2 표본특성

패스워드 사용자의 인구통계적 특성을 분석하면 다음과 같다<표2>.

표2- 인구통계학적 특성

응답자 특성	구분	빈도	비율
성별	남 여	68명 82명	45.3% 54.7%
연령	20세 이하 20~30세 30~40세 40~50 이상	0명 143명 7명 0명	0% 95.3% 4.7% 0%
학력	고졸 대학재학 대졸 대학원재학 대학원졸업이상	0명 99명 2명 44명 5명	0% 66% 1.4% 29.3% 3.3%
직업	전문직 공무원 자영업 학생 주부 기타	3명 0명 0명 143명 4명 0명	2% 0% 0% 95.3% 2.7% 0%
컴퓨터사용기간	3년 이하 4~6년 7~9년 10년 이상	2명 11명 55명 82명	1.3% 7.3% 36.7% 54.7%
패스워드 수	1~3개 4~6개 7~9개 10개 이상	83명 55명 7명 5명	55.3% 36.7% 4.7% 3.3%
변경여부	한달 이내 1~3개월 4~6개월 6개월~1년 변경하지 않음	0명 4명 14명 25명 107명	0% 2.7% 9.3% 16.7% 71.3%
패스워드유형	전부 같은 패스워드 일부는 같고 일부는 다름 전부 다른 패스워드	15명 131명 4명	10% 87.3% 2.7%
패스워드 노출	1번 2~3번 4~5번 5번 이상 노출된 적 없음	16명 40명 2명 1명 91명	10.7% 26.7% 1.3% 7% 60.9%
총계		150명	100%

4.3 측정모형의 평가

4.3.1신뢰성 평가

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

있다(Fornell&Larcker, 1981). 다음의 <표3>와 같이 본 연구를 위한 측정 하부모형의 합성신뢰도와 평균분산추출(AVE)의 측정치는 대체적으로 적합한 수준으로 나타나 연구모형의 내적 일관성이 확보되었음을 알 수 있다.

표3 -연구모형의 합성신뢰도 및 AVE

구성개념	합성신뢰도(≥0.7)	AVE(≥0.5)
자산	0.77	0.46
위협	0.85	0.59
취약성	0.73	0.42
위험	0.92	0.74
사용자보안의식	0.54	0.29
패스워드보안태도	0.59	0.33
보안행위의도	0.70	0.51

4.3.2 수렴타당성

수렴타당성(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 0.5이상이고, t-값이 2.0이상일 경우 수렴 타당성이 있는 것으로 판단한다(Bagozzi&Yi, 1988). <표4>에서 나타난 바와 같이 모든 항목의 추정치(factor loading; λ)가 권고수준을 상회하는 것으로 나타나 연구개념의 수렴 타당성을 충족함을 확인할 수 있다.

표4 -수렴타당성 분석 결과

구성개념	항목	부하량	t-값
자산	데이터파일의 중요성	0.81	10.32
	인증정보의 중요성	0.61	7.33
	업무관련정보의중요성	0.65	7.90
	개인정보의 중요성	0.63	7.60
위협	타인노출 가능성	0.54	6.76
	해커의도청 가능성	0.85	12.27
	공개 악용 될 가능성	0.84	12.11
	해커의 노출가능성	0.80	11.25
취약성	사용기간의 노출	0.84	11.09
	기억의 한계	0.47	5.54
	중복사용의 노출	0.75	9.96
	공유의 정보유출	0.46	5.42
위험	업무방해 위험	0.86	13.06
	프로그램 삭제 위험	0.94	15.12
	중요파일 삭제 위험	0.94	15.21
	중요정보공개 위험	0.66	8.98
사용자 보안의식	패스워드 기억정도	0.44	4.57
	어려운패스워드설정정도	0.57	5.91
	타인노출방지정도	0.59	6.13
	보안 교육 참여의 태도	0.65	7.08
패스워드 보안태도	기억에 의존한 호의성	0.50	5.44
	시스템 변경방지 태도	0.56	6.07
보안 행위의도	상이한패스워드사용의도	0.79	9.07
	기록하지 않을 의도	0.45	5.07
	패스워드갱신 의도	0.73	8.38

4.3.3 측정모형의 적합도 평가

다음의 <표5>에서 제시한 바와 같이 본 연구의 측정모형에 대한 적합도 지수는 일반적으로 권고하는 수용기준에 일부 지표가 기준에 약간 부족하지만 전체적으로 볼 때 부합하고 있다.

표5 -측정 하부모형의 적합도 지수

구분	적합도지수	수용기준	분석결과
절대 부합 지수	x^2/자유도	≤3.00	1.69
	x^2 자유도(df) p-value	≥0.05	429.97 254 0.00
	기초부합지수(GFI)	≥0.90	0.81
	표준원소평균잔차(SRMR)	≤0.10	0.072
	근사원소평균자승잔차(RMSEA)	≤0.08	0.068
증분 부합 지수	수정부합지수(AGFI)	≥0.80	0.76
	표준부합지수(NFI)	≥0.90	0.86
	관계부합지수(RFI)	1.0근사	0.84
	증분부합지수(IFI)	1.0근사	0.94
	비교부합지수(CFI)	≥0.90	0.94
간명 부합 지수	간명기초부합지수(PGFI)	≥0.60	0.64
	간명표준부합지수(PNFI)	≥0.60	0.73

4.4 구조모형 평가 및 연구가설 검증

4.4.1 구조모형의 적합도 평가

다음의 <표6>에서 제시한 바와 같이 본 연구의 구조모형에 대한 적합도 지수는 일반적으로 권고하는 수용기준에 일부 지표가 기준에 약간 부족하지만 전체적으로 볼 때 부합하고 있다.

표6-구조 하부모형의 적합도 지수

구분	적합도지수	수용기준	분석결과
절대 부합 지수	x^2/자유도	≤3.00	1.60
	x^2 자유도(df) p-value	≥0.05	425.19 266 0.00
	기초부합지수(GFI)	≥0.90	0.82
	표준원소평균잔차(SRMR)	≤0.10	0.084
	근사원소평균자승잔차(RMSEA)	≤0.08	0.063
증분 부합 지수	수정부합지수(AGFI)	≥0.80	0.77
	표준부합지수(NFI)	≥0.90	0.86
	관계부합지수(RFI)	1.0근사	0.84
	증분부합지수(IFI)	1.0근사	0.94
	비교부합지수(CFI)	≥0.90	0.94

간명 부합 지수	간명기초부합지수(PGFI)	≥0.60	0.67
	간명표준부합지수(PNFI)	≥0.60	0.76

4.4.2 연구가설 검정

본 연구에서 연구가설은 연구모형에서 구성개념 사이의 경로로 설정되었다. 구조모형 분석결과는 각 경로의 계수와 t-값으로 확인할 수 있으며, 아래의<그림2>에 나타난 바와 같이 자산과 위험에 이르는 경로를 제외한 다른 모든 경로는 통계적으로 유의한 영향을 미치는 것으로 나타났다.

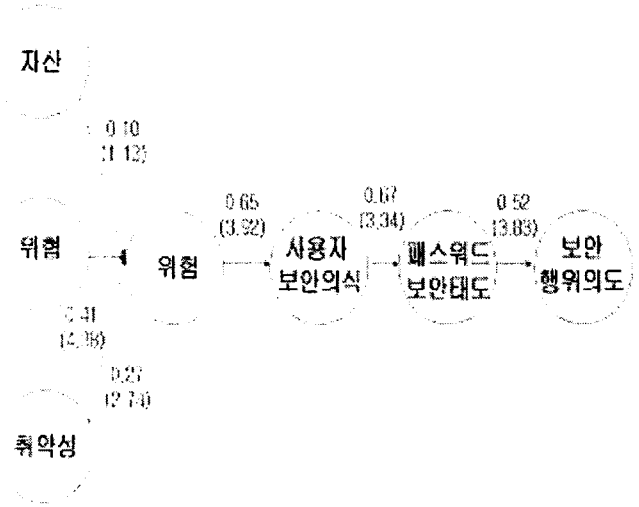

그림2-연구의 구조모형의 분석결과
주) 괄호 안은 t-값, **:유의수준 α =0.01에서 유의함.

각 연구 가설에 대한 분석결과를 살펴보면, 자산과 위험 사이의 관계를 규정한 가설1의 경우 경로계수가 0.10이며, t값이 1.13으로 유의한 영향을 미치지 못하는 것으로 나타났으며, 가설1은 기각되었다.

두 번째, 위협과 위험 사이의 관계를 규정한 가설2의 경우 경로계수가 0.41이며, t값이 4.38로 위협이 위험에 유의한 영향을 미치는 것을 확인할 수 있었다. 연구가설 2는 채택되었다.

세 번째, 취약성과 위험의 관계를 규정한 가설 3의 경우 경로계수가 0.27, t값이 2.74로 유의한 영향을 미치는 것으로 나타났으며 가설 3은 채택되었다.

네 번째, 위험과 사용자보안의식 사이의 관계를 규정한 가설 4의 경우, 경로계수가 0.65, t값이 3.92로 위험이 사용자 보안의식에 유의한 영향을 미치는 것으로 나타났으며, 가설 4는 채택되었다.

다섯 번째, 사용자 보안의식과 패스워드 보안태도 사이의 관계를 규정한 가설 5의 경우, 경로계수가 0.67, t값이 3.34로 사용자 보안의식이 패스워드 보안태도에 유의한 영향을 미치며, 가설 5는 채택되었다.

마지막으로 패스워드 보안태도와 보안행위의도 사이의 관계를 규정한 가설 6의 경우, 경로계수가 0.52, t값이 3.88로 패스워드 보안태도가 보안행위의도에 유의한 영향을 미치는 것으로 나타났으며, 가설 6은 채택되었다.

이상의 가설 검증 결과를 종합해 보면 위험의 선행요인 자산, 위협, 취약성에서 자산이 위험에 긍정적인 영향을 미친다는 가설은 기각되었지만, 위협과 취약성이 위험에 긍정적인 영향을 미친다는 가설은 채택되었으며, 위험은 사용자의 보안인식에 긍정적인 영향을 미치며, 사용자의 보안인식은 패스워드 보안하는 태도에 영향을 미친다고 하겠다. 이에 따른 패스워드의 보안을 위한 태도는 패스워드의 노출에 보호하기 위한 패스워드행위의도에 영향을 미치는 관계라는 것을 알 수 있다.

V. 결론

5.1 연구분석 결과

본 연구에서는 패스워드 선택이 사용자의 보안행위의도에 미치는 요인을 알아보기 위하여 연구모형을 구조방정식을 통하여 요인간의 인과관계를 검증하였다.

패스워드선택이 정보보안행위의도에 미치는 요인을 분석한 결과 정보자산이 위험에 관련성이 없는 반면,위협, 취약성은 위험에 유의한 영향을 미치는 것으로 분석된 것은 위험분석방법론에 있어서 중요한 시사점을 갖는다. 평가결과 정보자산은 객관성과 신뢰성에 의문이 제기된다. 이와 같은 결과는 김종기와 전진환(2006)의 연구에서도 동일하게 나타난 바 있다. 이는 사용자가 자산의 중요성을 위험에 영향을 미치는 다른 요인들에 비해 과대 평가함으로써 나타난 결과로 설명하였다. 이는 정보시스템에 저장되어있는 데이터 파일의 정보, 인증정보, 업무관련의 정보 개인정보 등의 정보자산은 사용자에게 매우 중요한 자산에 해당하기 때문에 사용자가 인지하고 있는 위험수준에 관계없이 높이 평가되고 있음을 설명하는 것이다. 정보자산을 제외한 위협, 취약성, 위험, 사용자의 보안의식, 패스워드 보안태도, 보안행위의도는 요인간의 유의한 영향을 미치며 보안행위의도에 영향을 미치는 요인이라고 할 수 있겠다.

5.2 연구의 한계 및 향후 연구과제

본 연구의 한계와 향후 연구과제는 다음과 같다. 먼저 실증분석을 통해서 위험의 선행요소인 자산과 위험 사이의 관련성은 명확하게 규명하지 못하였다.

향후 연구에서는 정보자산 측면에서의 사용자의 위험 정도를 고려해 봄으로써 보안행위의도에 있어서 사용자의 영향을 분석할 필요가 있을 것이다.

두 번째는 실증분석을 위해 사용된 본 연구의 대상자가 대학생과 대학원생에 국한되어 있었다. 이는 사용자 스스로 느끼는 보안행위의도에 대해 알아보고자 한 것이므로 개별 사용자를 대상으로 설문을 수행하였다. 추후 연구에서는 연구대상자를 조직의 구성원으로 바라보면, 조직의 패스워드 정책을 기반으로 조직내의 관점에서 패스워드선택을 위한 보안행위의도 분석을 할 것이다.

참고문헌

[1]채서일, (2005). *사회과학조사방법론*, 학현사.

[2]홍승필, 김영철, (2004). *최신 이론과 경향으로 배우는 정보보호의 이해*, 아이워크북.

[3]김기윤, (1994). "정보시스템 위험 분석과 관리", 경영정보시스템 추계학술대회, pp.277-297.

[4]김세헌, (2002). "정보보호 관리 및 정책", 한국정보시스템학회 1권 2호, pp.123-143.

[5]김인중, 이영교, 정윤정, 원동호, (2005). "정보시스템에 대한 보안위험 분석을 위한 모델링 기법에 대한 연구", 정보처리학회 12권 C호, pp.989-997.

[6]김종기, 전진환,(2006). "컴퓨터 바이러스 통제를 위한 보안행위의도 모형", 정보화정책 13권 3호, pp.174-193.

[7]박승배, 박성배, 강문설, (2003). "타인의 관찰에 의한 패스워드 노출로부터 안전한 패스워드 시스템", 정보처리학회 10-C권 2호,pp.141-144.

[8]이필중, 문희철, (1991). "패스워드 시스템의 보안에 관한 고찰", 한국통신정보보호학회지 1권 1호, pp.109-118.

[9]정경수, 김기영, 박종필, (2001). "패스워드 이용과 관한 실증분석: 대학과 종합병원을 중심으로", Information Systems , 30권 1호, pp.143-157.

[10]KISA, *정보보호 뉴스* , (2007). 2월호, pp.12-14.

[11]최상수, 방영환, 최성자, 이강수, (2003). "보안관리 및 위험분석을 위한 분류체계, 평가기준 및 평가스케일의 조사연구", 정보보호학회지 13권 3호, pp.28-49.

[12]한국전산원, (1997). "정보시스템 보안을 위한 위험분석 실무 지침서", 한국정보사회진흥원 NCAIII-GER-97054.

[13]Ajzen, Icek. and Fishbein, Martin, (1980). *Understanding Attitudes and Predicting Social Behavior*. Prentice-Hall, Inc., Englewood Cliffs: New Jersey.

[14]BSI, (1999). BS7799: Code of Practices for information Security Management. London: British Standard Institution.

[15]CMU/SEI, (1999). Operationally Critical Threat, Asset, Vulnerability Evaluation(OCTAVE) Framework, Ver. 1.0, CMU/SEI-99-TR-017. Pittsburgh: Carnegie Mellon University/ Software Engineering Institute.

[16]CSE, (1996), Guide to Security Risk Management for IT System. Government of Canada: Communication Security Establishment.

[17] Davis, F.D., Bagozzi, R., and Warchaw, P.R.,(1989). "User Acceptance of computer Tech-nology: A Comparison of Two Theoretical Models", Management Science, Vol.35, No.8, pp.982-1003.

[18] Gilbert, I. A, (1991). "Risk Analysis : Concepts and Tools", Datapro Reports on Information Security, Risk Analysis, September, pp. 101-112.

[19] Shen, Jau-Ji, Lin Chih-Wei and Hwan Min-Shiang, (2003). "Security enhancement for the timestamp-based password authentication scheme using smart cards", Computers and Security, Vol. 22, No. 7, October, pp. 591-595.

[20] K. M Jackson., and J. Hruska, (1992). " Computer Security Reference Book, "British Library Cataloging in Publication Data", pp. 227-263.

[21] Lawrence O'Gorman, Baga, Amit & Bentley , Jon, (2005). "Query-directed passwords", Computer and Security, Vol. 24, NO. 7, pp. 546-560.

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

[23] Marshall A. Berger, (2003). " Password Security Is a Must for Any Organization" Computer in Libraries, Vol. 23, No. 5, pp.41.

[24] Menkus, B, (1988). "Understanding the Use of Passwords," Computer and Security, Vol. 7, No. 2, pp.132-136.

[25] Mohammad Peyravian and Nevenko Zunic,(2000). " Methods for Protecting Password Transmission" Computer and Security, Vol. 19, No. 5, pp. 466-469.

[26] NIST, (2001), "Risk Management Guide for Information Technology Systems", Special Publication 800-30.

[27] Rainer, R. K., C. A, Snyder. and H. H, Carr , (1991). "Risk Analysis for Information Technology", Journal of Management Information System, Vol. 8, No. 1, pp.129-147.

[28] Raphael C.and W. Phan, (2006). "Cryptanalysis of two password-based authentication schemes using smart cards", Computer and Security, Vol. 25, pp.52-54.

[29] Roger A. Grimes, (2006). "Top 14 Security Tactics" Infoworld.com, pp.16.

[30] Robert Lemos,, (2006). "Password Policies", Pc Magazine, September, pp.116.

[31] "Seven Top Security Tips", (2006). Communication News, August, pp.8.

[32] Tregear, J, (2001). "Risk Assessment", Information Security Technical Report, Vol. 6, No. 3, pp.19-27.

[33] Zviran, M., and Haga, (1999). "Password Security: an empirical study", Journal of Management Information System, Vol. 15, No. 4, pp. 161-185.