「정보시스템연구」 제17권 제1호
한국정보시스템학회
2008년 3월, pp. 23~43

패스워드 선택을 위한 사용자의 보안행위의도에 영향을 미치는 요인

김종기* · 강다연** · 전진환***

〈목 차〉

Ⅰ. 서 론

최근의 컴퓨팅 환경은 사용자가 언제 어디서든지 네트워크에 접근이 가능하도록 하여 인터넷을 통해 전송되는 정보량이 과거에 비해 큰 폭으로 증가하였다. 이러한 정보량의 증가세는 앞으로도 지속될 것으로 전망되나 정보를 생성, 처리, 저장, 출력하는 과정에서 정보주체가 의도하지 않은 정보의 훼손, 손실 및 파괴는 정보보안의 차원에서 주요 문제점으로 부각되고 있다. 대한상공회의소(2006)는 국내기업들에서 고객의 개인정보나 기업의 비밀정보 등이 이메일, 인스턴트 메시징 서비스 등을 통해 무분별하게 유출되고 있으며, 정보 유출에 따른 기업의 손실이 증가하고 있음을 지적하였다.

정보보안에서 데이터에 대한 비밀성은 무엇보다 중요한 요소이다. 이를 위해 조직내 보호받아야 할 정보자산을 식별하여 해당 가치를 평가하고, 의도하지 않은 잠재적인 위협과 정보시스템의 치명적인 결함의 노출로부터 적정수

* 부산대학교 경영학부 부교수, jkkim1@pusan.ac.kr
** 부산대학교 경영학과 박사과정, kdy@pusan.ac.kr
*** 부산대학교 경영학박사(교신저자), jeonjinhwan@pusan.ac.kr

준의 보안을 유지하기 위한 지속적인 관리는 필수적이다. 정보시스템에서 비밀성은 사용자를 인증하는 메커니즘인 패스워드(password)에 상당부분 의존하게 된다(Adams & Sasse, 1999). 패스워드는 악의적인 사용자에 의한 내·외부 침투로부터 민감한 정보를 보호할 수 있는 첫 번째 관문으로써 정보보안을 위한 적절한 패스워드의 선택은 필수적인 요소이다(Gehringer, 2002).

하지만, 대부분의 사용자들은 쉽게 추측할 수 있는 패스워드를 생성하는 경향을 가지고 있고, 사용에 있어 매우 낮은 보안인식을 보임에 따라 전반적인 보안효과가 낮다(한국정보보호진흥원, 2007). 사용자의 허술한 패스워드의 선택 및 사용은 다수의 계정을 보호하기 위해 하나의 패스워드를 설정함으로써 동시다발적으로 개인정보가 노출될 수 있는 도미노 현상(domino effect)을 발생시킨다(Ives et al., 2004). 이로인해 조직의 핵심자산인 정보자산에 대한 노출 및 파괴, 변조 등의 공격을 가능케 하며, 인가받지 않은 불법적인 사용자에 의한 정보시스템의 파괴, 개인정보 노출, 불건전 정보의 유통 등과 같은 피해를 증가시키는 근본적인 원인을 제공한다(Gehringer, 2002; Ives et al, 2004). 이에 따라 정보자산에 상대적으로 높은 가치를 두고 있는 조직에서는 사용자의 적절한 패스워드 선택과 사용에 관한 보안정책의 강조 및 보안교육 강화 등 다방면에서 많은 노력을 기하고 있다(Martinson, 2005).

최근 정보시스템 패스워드 노출방지와 원활한 데이터 관리를 위한 대다수의 연구들은 기술적 측면에서 패스워드의 구성에 대한 가이드라인 형태의 연구(CERT/CC, 2002; Juang, 2004; O'Gorman et al., 2005)가 주를 이루고 있는 반면 정보보안을 위한 적절한 패스워드 관리에 대한 사용자의 인지적 차원에서 보안의도를 실증분석하여 설명한 연구는 극히 희소한 편이다. 이에 따라 본 연구에서는 사용자가 패스워드 관련 위험인지가 패스워드 관리를 위한 정보보안 행위의도에 직접적인 영향을 미치는 요인인지에 대해 행태적 차원에서 규명하고자 하였다.

이를 위해 본 연구에서는 선행연구를 바탕으로 패스워드와 정보보안 관련 전반적인 개념을 설명하고, 사용자의 위험인지 요인을 설명하기 위해 위험분석방법론을 통한 위험에 선행하는 정보자산, 위협, 취약성의 요인들의 관계에 대해 설명하였다. 또한, 합리적 행동이론(Theory of Reasoned Action; TRA)으로부터 도출된 태도와 의도 사이의 관계를 정보보안 측면에서 규정함으로써 패스워드 보안의도가 정보보안활동을 위한 패스워드 선택에 결정적인 영향을 미치는 요인인지를 실증적으로 평가하고자 하였다.

Ⅱ. 선행연구

2.1 패스워드와 정보보안

정보시스템에서 적법한 사용자를 인증하는 절차는 사용자에 대한 식별(identification; ID)과 ID를 합법적으로 소유한 사용자가 올바른 사용자가 맞는지 확인하는 인증(authentication)의 두 부분으로 구성된다(Adam & Sasse, 1999). 이때 패스워드는 정보시스템과 네트워크의 사용에 있어 인가된 사용자를 확인하는데 사용되는 하나의 보안수단에 해당한다. 다시말해, 정보시스

템에서 사용자를 인증하거나 해당 시스템을 이용하는 사용자에게 데이터의 접근을 제한하는 기능을 가진 개체가 바로 패스워드이다(Zviran & Haga, 1999; 정경수 외, 2001).

사용자의 적절한 패스워드 선택과 사용은 데이터 조작미숙, 정보시스템의 무단사용 및 파괴 등의 오·남용으로부터 정보시스템을 보호하며, 고의적 노출, 변조, 파괴 등으로부터 정보자산을 보호할 수 있도록 한다. 최근 다양한 정보시스템 어플리케이션의 출현으로 인해 사용자의 정보시스템 접속횟수가 증가하고, 동일한 패스워드를 복수의 정보시스템과 어플리케이션에 접속을 위해 사용함으로써 정보보안 측면에서 위험을 증가시키고 있다(Ives et al., 2004). 이로 인해 이들 어플리케이션과 운영체제를 관리하는 시스템 운영자와 사용자에게 아이디와 패스워드의 노출방지를 위한 관리적 차원의 많은 노력들이 요구되고 있다.

대부분의 패스워드 관련 주요 연구들(Zviran & Haga, 1999; 정경수 외, 2001; CERT/CC, 2002; Gehringer, 2002; Wakefield, 2004; Martinson, 2005)의 동향을 살펴보면 패스워드 노출방지와 효과적인 관리를 위한 다음과 같은 공통의 가이드라인을 제안하고 있다. 우선, 패스워드를 구성할 때 최소 8자리 정도가 적당하며, 문자와 숫자를 혼용해서 사용해야 한다. 또한, 입력이 편해야 하고, 사전을 통한 검색 및 유추가 불가능해야 한다. 그리고 타인과 공유해서는 안되며, 메모지 등에 쓰지 않고 자신이 기억할 수 있어야 한다는 기준이다. 하지만 언급된 선택기준들만으로 패스워드의 적절한 선택 및 효과적 사용, 사용자의 오·남용으로 부터 직접적인 정보보안 효과를 발생시키기에 여러 어려움과 제약이 따른다.

이러한 어려움과 제약을 가져오는 근본적인 요인으로 패스워드 가이드라인에 의해 발생되는 문제가 가장 크다. 대부분의 가이드라인에서 제안된 기준들은 기술적 차원에서 사용자에게 적절한 패스워드의 선택만을 강조할 뿐 까다로운 패스워드 선택이 정보보안을 위해 왜 필요한지에 대한 인지적 차원의 설명이 부족한 특징을 가지고 있다. 이로 인해 패스워드가 자신만 알고 있는 보안장치로 생각하고 있는 보안지식이 상대적으로 약한 사용자는 정보보안의 중요성을 쉽게 간과하거나 특별히 의식하지 않게 된다(전정훈, 2007).

다른 제약요인으로 Martinson(2005)의 패스워드 사용과 정책에 관한 연구결과에서 나타난 바와 같이 패스워드 가이드라인은 정보시스템 사용에 있어 사용자에게 상당히 성가신 조건이며, 패스워드 관리를 소홀하게 하는 요인이라는 점이다. 특히, 응답자의 70% 이상이 5개 정도의 패스워드를 가지고 있었으나 대부분 다수의 어플리케이션에서 하나의 패스워드를 반복적으로 사용하고 있어 패스워드 오·남용의 심각성을 인지하지 못하고 있었으며, 많은 사용자들이 패스워드 정책의 일방적 강요를 선호하지 않는다는 사실을 지적하였다.

추가적으로 앞서 가이드라인에서 언급된 사용자의 기억에 의존해야하는 문제가 있다. Yan et al.(2000)의 연구에서는 패스워드 가이드라인이 사용자에게 어려운 패스워드의 사용을 강요할 경우 패스워드의 난이도가 높아져 기억하는데 어려움을 느끼게 되고, 그만큼 사용성이 떨어지게 됨을 지적하였다. 이에 반해 기억하기 쉬운 패스워드를 선택해서 사용할 경우 악의적

인 사용자에 의해 쉽게 노출될 수 있는 특성을 가지고 있기 때문에 패스워드 선택에서 난이도와 사용용이성 사이에 상충관계에 대한 주의를 가질 필요가 있음을 지적하였다. 이와 같이 패스워드의 선택과 사용상의 여러 어려움과 제약에도 불구하고, 효과적인 정보보안을 위한 적절한 패스워드의 선택과 활용은 매우 중요하다.

2.2 위험분석방법론

정보보안은 정보자산을 내·외부 위협 또는 오·남용으로부터 보호하는 것을 의미한다(Finne, 1998; ISO/IEC, 2005a). 이는 정보시스템에서 정보자산이 조직업무와 전략적 목표달성을 위해 필수적인 요소이고, 이에 대한 고의적인 노출, 변조 및 파괴의 악의적 활동은 사용자에게 금전적인 측면의 손실과 피해를 발생시키기 때문이다. 이로 인해 조직에서 정보자산을 효과적으로 보호하기 위한 위험분석(risk analysis) 프로세스가 요구되며, 이를 통해 위험을 식별하고 관리할 수 있어야한다(Eloff & Solm, 2000). 위험분석방법론은 정보자산이 갖고 있는 취약성에 따라 사고가 발생할 수 있는 가능성과 피해수준에 대한 적절한 예측을 통해 발생할 수 있는 위험의 정도를 평가하고, 해당 위험을 감소시킬 수 있도록 최적의 대응책을 수립하고자 하는 방법론이다(Baskerville, 1991; Rainer et al., 1991).

현재 위험분석방법론은 국제표준인 ISO/IEC (2005b)를 비롯하여 영국(CCTA, 2001), 미국(NIST, 2001), 캐나다(CSE, 1996) 등 세계 각국의 정부기관 뿐만 아니라 여러 기관에서 다양한 방법론들을 제시하고 있다. 다음의 <그림 1>에 나타난 바와 같이 위험분석방법론은 자산, 위협, 취약성에 대한 평가를 통한 위험을 평가하는 분석단계와 위험평가에 따른 보안대책을 수립하여 정보시스템을 관리하는 위험관리의 크게 두 부분으로 나누어 설명이 가능하다(Tregear, 2001).

위험분석은 조직이 보유하고 있는 자산(asset)의 가치에 대한 식별과 평가로부터 시작된다. 자산에는 정보자산, 소프트웨어 자산, 물리적 자산, 인적자원, 서비스 등을 포함하며, 이들 자산에 대한 평가는 자산이 조직에서 가지는 중요도에 따른 잠재적인 피해로 평가하게 된다(CSE, 1996; CMU/SEI, 1999; ISO/IEC, 2005b). 다음 단계에서 정보자산에 가해질 수 있는 위협에 대한 식별과 평가가 이루어진다. 위협(threat)은 정보자산에 의도하지 않은 결과를 파생시킬 수 있는 일련의 사건들로 해당 위협의 발생빈도와 발생가능성으로 평가되어진다(NIST, 2001; ISO/IEC, 2005b).

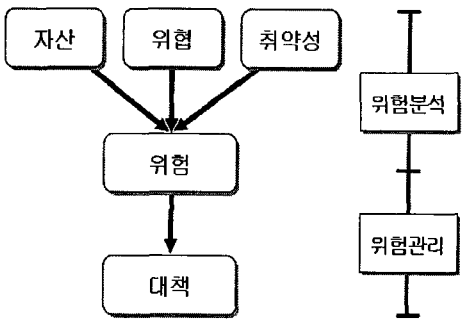
위협은 천재지변에 의한 자연발생적 위협, 시스템 조작미숙, 하드웨어 및 소프트웨어 결함, 입·출력 오류 등에 의한 비의도적인 위협, 고의적인 파괴, 절취 등의 의도적인 위협으로 분류할 수 있다. 의도적인 위협의 경우 내부 사용자에 의해 고의적인 시스템 침입, 데이터 변조 및 파괴 등을 발생시킬 수 있으며, 외부로부터 물리적인 침입뿐만 아니라 데이터 절도 등도 포함된다(Loch et al., 1992: ISO/IEC, 2005b).

그 다음 단계에서 취약성(vulnerability)에 대한 식별과 평가가 이루어지며, 취약성은 정보시스템의 기술·절차적 보안에 내재된 약점으로 내·외부의 위협요인에 의해 현실화될 수 있는 문제들을 의미한다(CSE, 1996; ISO/IEC, 2005b). 취약성은 보안통제의 부재나 취약성 노출의 수

준으로 평가하게 된다.

끝으로 위험(risk)의 평가는 조직에 악영향을 미치는 사건들의 발생으로 인해 조직이 받을 것으로 예상되는 충격에 대한 수준을 측정하는 것이다(CSE, 1996; NIST, 2001). 위험분석방법론에서 위험은 f(자산, 위협, 취약성)의 함수로 설명이 가능하며, 이에 따라 자산, 위협, 취약성 요소 중 하나라도 증가할 경우 위험도 증가하게 되며, 하나라도 감소할 경우 자연스럽게 감소하게 된다. 대부분의 조직들은 위험으로부터 발생하는 손실의 예방과 이를 위한 적절한 비용수준을 고려한 최적의 조합을 찾으려 노력하고 있으며, 이러한 조합을 찾아내는 것이 위험분석의 목적이다(Rainer et al., 1991; ISO/IEC, 2005b).

위험분석 프레임워크에서 두 번째 단계인 위험관리에서는 발생가능한 손실을 최소화하기 위해 관리차원에서 위험분석을 통해 식별 및 평가된 위험에 대한 보안대책을 수립하고, 이를 일정수준까지 유지 및 관리하는 단계이다. 이와 같이 위험분석방법론은 정보시스템에서 발생할 수 있는 위험을 최소화하기 위한 여러 보안대책을 수립하는데 필요한 정보를 제공하기 위한 핵심 프로세스라 할 수 있다.



<그림 1> 위험분석 프레임워크
출처: Tregear, 2001

2.3 사용자의 신념, 태도 및 행위의도

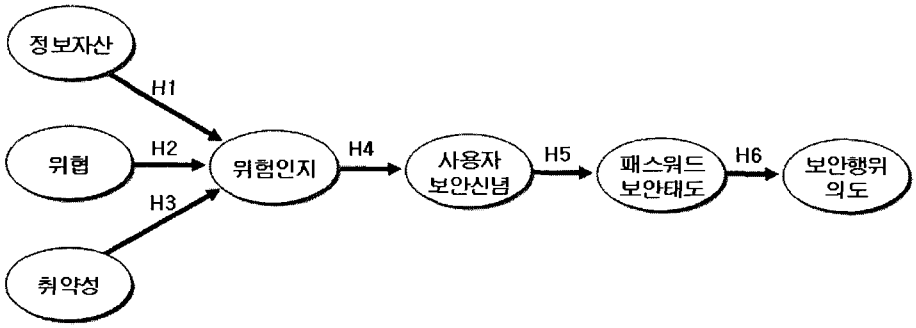
Ajzen & Fishbein(1980)이 주장한 합리적 행동이론은 사람들의 특정행위가 자신에게 주어진 상황이나 시간의 제약에 따른 여러 정보를 합리적으로 선택하고 목표에 도달하기 위해 수행된다는 이론이다(Davis et al. 1989). TRA 모형에서 개인의 행동은 행위의도(behavioral intention)에 의해서 결정되며, 이러한 행위의도는 개인의 행동에 대한 태도(attitudes toward behavior)와 주관적 규범(subjective norm)에 의해서 결정된다. 이때 태도는 특정 행위에 대한 개인의 긍정 혹은 부정적인 감정으로서 특정 행위에 대한 개인의 태도가 긍정적일수록 그 행위를 수행할 의도 역시 높아지게 된다(Davis et al., 1989; 차윤숙 & 정문상, 2007; 장명희, 2005).

어떤 행위에 대한 개인의 태도는 결과에 대한 평가와 행동 결과에 대한 개인의 신념(belief)으로부터 결정되고, 이러한 신념은 자신의 직접적인 경험과 내·외부의 정보 등에 의해 형성된다. 즉, 이러한 일련의 과정은 정보자산의 보호과정에 위험을 인지한 사용자는 정보보안에 대한 긍정적인 태도를 형성하게 되며 이를 통해 강력한 보안행위를 수행하게 됨을 예측가능하게 한다.

Ⅲ. 연구모형 및 연구가설

3.1 연구모형

본 연구모형은 다음과 같이 크게 두 부분으로 구성하였다. 먼저, 정보보안에 대한 사용자



<그림 2> 연구모형

의 위험인지는 위험분석방법론을 토대로 한 정보자산, 위협, 취약성의 세 가지 요인에 의해 형성되는 것으로 설정하였다. 이렇게 형성된 위험인지는 사용자의 보안신념과 패스워드 보안태도를 통해 보안행위의도를 설명할 수 있도록 하였다.

3.2 연구가설

3.2.1 위험인지와 선행요인간의 관계

연구가설1(H1)은 정보자산과 위험인지 사이의 관계를 설명하기 위해 설정되었다. 위험분석 방법론에서 자산은 보호되어야 할 대상으로 정보, 하드웨어, 소프트웨어, 데이터 등의 유형자산과 인적, 조직 이미지 등 무형자산을 포함한다(CMU/SEI, 1999). 본 연구에서는 자산의 범위를 패스워드 노출로부터 보호되어야 할 데이터, 개인 신상정보, 업무관련 정보 등의 정보자산(information asset)으로 규정하고, 이들 정보자산의 변조, 노출 및 삭제될 경우 발생할 금전적 피해 및 손실을 고려하였다. 이에 따라 사용자가 인지하는 정보자산의 상대적 가치가 높아질수록 패스워드의 노출에 따른 위험인지에 긍정적인 영향을 미치게 된다.

연구가설2(H2)는 위협과 위험인지 사이의 관계를 설명한 것으로 위협은 정보자산에 해로운 영향 또는 피해를 발생시키는 위험의 원천이다. 정보시스템에서 발생 가능한 위협들은 자연발생적 위협, 비의도적 위협 및 의도적 위협으로 구분되며, 이들 위협이 증가할수록 위험수준도 동시에 증가하게 된다(ISO/IEC, 2005b). 본 연구에서는 패스워드 노출로 인한 정보자산에 대한 직·간접적인 침해를 고려하였으며, 이러한 위협이 증가할수록 사용자의 위험인지는 높아지게 된다.

연구가설3(H3)에서 취약성과 위험인지 사이를 설명한 관계는 정보시스템에서 정보자산 보호에 실패할 수 있는 조직, 절차, 인력, 하드웨어, 소프트웨어 등의 내재적인 약점(ISO/IEC, 2005b)이 사용자의 위험인지에 영향을 미치는 것을 분석하기 위해 설정하였다. 패스워드 관리에 있어 장기간 사용에 따른 노출가능성의 증가와 패스워드 기억의 한계, 동일한 패스워드 중복사용은 정보시스템의 취약성을 증가시키는 요인이다. 이로 인해 사용자가 설정한 패스워드 취약성에 대한 인지가 증가할수록 위험인지의 수준도 따라서 증가하게 된다.

H1: 정보자산의 중요성은 사용자의 위험인지에 정(+)의 영향을 미친다.

H2: 패스워드 노출 위협은 사용자의 위험인지에 정(+)의 영향을 미친다.

H3: 패스워드 취약성은 사용자의 위험인지에 정(+)의 영향을 미친다.

3.2.2 위험인지, 보안신념 및 보안태도의 관계

연구가설4(H4)에서는 사용자의 위험인지와 보안신념 사이의 관계를 설명하였다. 정보시스템 내 정보자산, 위협, 취약성 요인들의 수준이 증가할수록 사용자가 인지하는 위험은 자연스

<표 1> 연구변수의 조작적 정의 및 측정항목

연구개념	조작적 정의	측정항목	관련문헌
정보자산 (AS)	패스워드의 노출로부터 보호해야 할 대상으로 데이터, 인적정보, 핵심 업무자료 등의 가치 있는 정보의 중요성 정도	· 데이터파일의 중요성 · 인증정보의 중요성 · 업무관련 정보의 중요성 · 개인정보의 중요성	Rainer et al.(1991), CMU/SEI(1999), NIST(2001), ISO/IEC(2005b)
위협 (TH)	정보자산에 해를 줄 수 있는 해킹, 테러, 고의적 노출 등과 같은 위협으로부터 사용자의 패스워드가 불법적으로 노출될 가능성의 정도	· 타인노출 가능성 · 해커의 도청가능성 · 악용 될 가능성 · 패스워드 노출 가능성 · 해커의 노출가능성	이필중, 문희철(1991), Loch et al.(1992), ISO/IEC(2005b)
취약성 (VL)	정보시스템에 손해를 끼칠 수 있는 패스워드 노출의 원인이 될 수 있는 약점의 정도	· 패스워드 사용기간 · 패스워드 기억의 한계 · 패스워드 중복사용 · 패스워드 공유	Gilbert(1991), CSE(1996), NIST(2001), ISO/IEC(2005b)
위험인지 (RSK)	패스워드 노출로 인해 개인 및 조직이 받을 것으로 예상되는 영향, 손실, 피해의 정도	· 업무방해 위험 · 프로그램 삭제 위험 · 중요파일 삭제 위험 · 중요정보 공개 위험	Rainer et al.(1991), NIST(2001), ISO/IEC(2005b)
사용자 보안신념 (USR)	정보시스템 사용자 스스로의 정보보안에 대한 보안인식과 정보보호의 중요성을 인지하는 정도	· 패스워드 기억정도 · 어려운 패스워드 설정정도 · 주기적 변경의 보안효과 · 패스워드 노출에 대한 보안	이필중, 문희철(1991), Zviran & Haga(1999) 정경수 외 (2001)
패스워드 보안태도 (AT)	정보시스템 사용자의 패스워드 보안관리에 보이는 긍정적인 태도의 정도	· 보안 교육 참여의 태도 · 불법적 시스템 변경방지 · 화면 보호기능의 태도 · 패스워드의 변경	Ajzen & Fishbein (1980), Davis et al.(1989)
보안 행위의도 (INT)	패스워드 노출위험의 방지를 위한 적극적인 보안행위의지에 대한 정도	· 상이한 패스워드 사용의도 · 신상관련 비사용의도 · 기록하지 않을 의도 · 패스워드 갱신 의도 · 패스워드 비공유 의도	Ajzen & Fishbein (1980), Davis et al.(1989)

럽게 증가하게 된다. 다시 말해 패스워드 노출에 따른 업무방해, 프로그램 및 주요 파일삭제, 신상정보 유출 등의 위험을 사용자가 인지할 경우 이로부터 발생할 손실과 피해를 방지하기 위해 위한 패스워드 관리의 필요성을 인지하게 된다. 이에 따라 사용자가 인지하는 위험의 수준이 높아질수록 패스워드 관리를 위한 보안 신념 또한 강해지게 된다.

연구가설5(H5)는 사용자의 보안신념이 보안태도에 미치는 영향관계를 설명하기 위해 설정된 것으로 정보시스템 사용자가 인지하는 위험의 수준이 증가할수록 보안교육의 참여 및 패스워드 변경 가능성의 중요성을 고려하게 되며, 정보보안의 신념이 강해질수록 패스워드 관리를 위한 보안활동들에 긍정적인 태도를 형성하게 된다.

H4: 사용자의 위험인지는 보안신념에 정(+)의 영향을 미친다.

H5: 사용자의 보안신념은 패스워드 보안태도에 정(+)의 영향을 미친다.

3.2.3 패스워드 보안태도와 보안행위의도 간의 관계

TRA 모형(Ajzen & Fishbein, 1980)에서 사람의 행위는 행위의도로부터 출발한다고 주장함으로써 태도와 행위 사이의 관계에 대한 논의를 확장하였다. 특히, 사용자가 행위에 대한 호감이 높을수록 해당 행위를 수행하기 위한 의지가 강해지게 된다. 따라서 연구가설6(H6)에서는 정보시스템 사용자가 패스워드를 통한 정보보안에 긍정적인 태도를 형성하고 있을 경우 패스워드 노출방지를 위한 적극적인 보안행위의도를 가지게 될 것으로 설정하였다(Davis et al., 1989; 김종기, 전진환, 2006).

H6: 패스워드 보안태도는 보안행위의도에 정(+)의 영향을 미친다.

3.3 연구변수의 조작적 정의

본 연구에서 연구모형의 실증분석을 위해 다음과 같이 연구개념에 대한 조작적 정의를 내리고 설문도구를 구성하였다. 여기서 모든 측정항목은 리커트(Likert) 7점 척도로 구성하였다.

Ⅳ. 실증분석

4.1 표본선정 및 분석기법

본 연구에서는 사용자의 정보시스템 위험인지에 따른 패스워드 선택의도에 미치는 영향을 평가하기 위해 학부생과 대학원생을 표본집단으로 선정하여 설문을 수행하였다. 연구모형의 분석을 위해 전체 250부의 설문을 배포하여 246부를 회수하였으며, 결측치가 있거나 불성실하게 응답한 3부의 설문지를 제외한 총 243부를 최종분석에 활용하였다. 수집된 데이터는 응답자의 인구통계적 특성과 탐색적 요인분석을 위해 SPSS Windows 12.0이 사용되었으며, 연구모형의 적합성을 검증하기 위해 적용된 구조방정식 모델의 평가를 위해 LISREL 8.54로 분석하였다.

4.2 표본특성

응답자의 표본특성을 살펴보면 남자가 110명(45.3%), 여자가 133명(54.7%)으로 성별비율이 비교적 균등하게 나타났으며, 연령대는 학부생과 대학원생을 대상으로 설문하였기 때문에 20~30대가 대부분을 차지하였다. 또한, 응답자의 대부분은 컴퓨터 사용기간이 7~9년이 141명으로 58%를 차지하였으며, 10년 이상이 81명으로 33.3%를 차지하고 있어서 정보시스템에서 패스워드 활용과 관련한 표본집단으로 적절하다고 판단하였다.

<표 2> 응답자의 패스워드 사용특성

구분	항목	빈도수	비율(%)
패스워드 수	1~3개	121	49.8
	4~6개	105	43.2
	7~9개	10	4.1
	10개 이상	7	2.9
패스워드 유형	전부 같은 패스워드	23	9.5
	일부는 같고 일부는 다름	212	87.2
	전부 다른 패스워드	8	3.3
변경빈도	한 달 이내	0	0.0
	1~3개월	6	2.5
	4~6개월	23	9.5
	6개월~1년	39	16.0
	변경하지 않음	175	72.0
패스워드 노출경험	1번	28	11.5
	2~3번	64	26.3
	4~5번	3	1.2
	5번 이상	2	8.0
	노출된 적 없음	146	60.1

<표 2>에서 응답자의 패스워드 사용특성에서 나타난 바와 같이 응답자들이 자주 사용하고 있는 패스워드의 개수를 묻는 질문에 1~3개가 121명(49.8%)으로 절반에 가까웠으며, 4~6개가 105명(43.2%)으로 대부분의 사용자들의 6개 이하의 패스워드를 가지고 있는 것으로 나타났다. 또한, 소유한 패스워드의 유형을 묻는 질문에 '일부는 같고 일부는 다른 패스워드를 사용한다'가 212명(87.2%)으로 전체 응답자의 대부분을 차지하는 것으로 나타나 어플리케이션에 따라 패스워드를 가급적 달리 쓰고자 함을 간접적으로 확인할 수 있었다. 패스워드 변경빈도에 대해서는 '전혀 변경하지 않는다'가 175명(72%), '6개월에서 1년'이 39명(16%)으로 패스워드 변경이 잘 이루어지지 않고 있음을 확인할 수 있었다. 또한, 패스워드 노출경험에 대해서는 응답자의 절반이 넘는 146명(60.1%)이 노출된 적이 없다고 응답하였으며, 1~2번이 28명

<표 3> 연구개념의 신뢰도

연구개념	기존항목	수정항목	평균	표준편차	Cronbach-α
정보자산	4	4	6.34	0.92	0.74
위협	5	4	5.18	0.05	0.84
취약성	4	3	5.31	0.18	0.72
위험인지	4	4	5.42	0.14	0.88
사용자신념	4	3	5.75	0.06	0.73
패스워드 보안태도	4	3	5.11	0.08	0.70
보안행위의도	5	3	4.18	0.03	0.70

(11.5%), 2~3번이 64명(26.3%)으로 분석되었다.

4.3 연구개념의 신뢰도

<표 3>과 같이 본 연구의 연구개념(construct)에 대한 신뢰도를 검증한 결과 Cronbach-α 계수가 사회과학연구에서 제안하는 0.7을 넘는 것으로 나타나 본 연구에서 사용된 변수들의 신뢰도가 높은 것으로 검증되었다.

4.4 측정모형의 검증

본 연구에서 연구모형을 검증하기 위해 Anderson & Gerbing(1988)이 제안한 2단계 접근법(two-step approach)을 적용하였다. 이 방법은 연구모형에서 잠재변수를 측정하기 위한 측정모형과 연구모형의 구조를 설명하는 구조모형으로 분리하여 분석함으로써 해석상의 교락효과((interpretational confounding)을 줄일 수 있다는 장점을 가지고 있다(Anderson & Gerbing, 1988). 이는 측정모형과 경로의 추정을 동시에 수행할 경우 측정에 있어 심각한 오차가 감추어짐으로써 잘못된 결론이 유도될 수 있으므로(Segar, 1997) 구조방정식을 활용한 연구에서 이 단계 접근법은 널리 적용되고 있다(Garver & Mentzer, 1999).

4.4.1 연구개념의 신뢰성 평가

먼저, 연구모형에 대한 측정모형의 신뢰성을 검증하였다. Bagozzi & Yi(1988)는 측정모형의 내적일관성을 평가하기 위해 각 연구개념의 Cronbach-α, 합성신뢰도(composite construct reliability)와 평균분산추출(average variance extracted; AVE)의 세 가지가 일반적으로 요구된다고 하였다. 합성신뢰도는 관측변수의 내적 일관성을 측정하는 측정치로 달리 개념 신뢰도(construct reliability; CR)라 부르기도 하며, 측정치가 0.7 이상일 경우 수용 가능한 수준으로 평가한다(Hair et al., 1998). 신뢰도 검정을 위한 또 다른 특정치인 AVE는 연구개념에 대해 지표가 설명할 수 있는 분산의 크기를 의미하는 것으로 측정치가 0.5 이상일 경우 수용 가능한 수준으로 평가한다(Fornell & Larcker, 1981).

다음의 <표 4>와 같이 본 연구를 위한 측정모형의 합성신뢰도는 권장수용 기준을 상회하는 것으로 나타나 신뢰도를 충분히 확보하였으나 AVE의 측정치는 정보자산과 보안행위의도에서 다소 낮은 것으로 나타났다. 본 연구에서 일부 연구개념들의 AVE의 추정치가 다소 떨어지지만 신뢰도와 합성신뢰도가 권장수용기준을 상회함으로 내적일관성을 가지는 것으로 평가하였다.

<표 4> 연구개념의 신뢰성 평가

연구개념	CR(≥0.7)	AVE(≥0.5)
정보자산	0.755	0.436
위협	0.878	0.706
취약성	0.754	0.517
위험인지	0.886	0.669
사용자 보안신념	0.741	0.490
패스워드 보안태도	0.742	0.506
보안행위의도	0.703	0.442

4.4.2 측정모형의 타당성

측정모형의 타당성을 검증하기 위해 집중타당성과 판별타당성을 검증하였다. 먼저, 집중타당성(convergent validity)에서 하나의 연구개념을

측정하기 위해 다중 지표가 사용된 경우 이 항목들 사이에 높은 상관관계가 있는지 평가하며(Garver & Mentzer, 1999), 요인적재량이 0.5이상이고, t-값이 2.0이상일 경우 집중타당성이 있는 것으로 판단한다(Bagozzi & Yi, 1988).

다음의 <표 5>에서 나타난 바와 같이 일부 항목을 제외하고 전반적으로 요인적재량은 적절한 것으로 나타났으며, t-값이 권고수준을 상회하는 것으로 나타나 연구개념의 집중타당성이 있는 것으로 평가하였다.

다음으로 판별타당성의 검증을 통해 서로 다른 연구개념들 사이에는 확실한 차이가 존재하는지 평가하였다(Gefen, 2003). 본 연구에서는 Anderson(1987)이 제안한 2개의 연구개념의 항

<표 5> 집중타당성 분석 결과

연구개념	변수명	측정항목	요인적재량	t-값
정보자산	AS1	데이터파일의 중요성	0.70	10.76
	AS2	인증정보의 중요성	0.68	10.38
	AS3	업무관련정보의 중요성	0.63	9.46
	AS4	개인정보의 중요성	0.63	9.53
위협	TH2	해커의 도청 가능성	0.83	14.95
	TH3	공개 악용 될 가능성	0.87	15.89
	TH5	해커의 노출 가능성	0.83	15.02
취약성	VL1	사용기간의 노출	0.83	11.83
	VL2	기억의 한계	0.49	7.21
	VL3	중복사용의 노출	0.79	11.36
위험인지	RSK1	업무방해 위험	0.81	15.16
	RSK2	프로그램 삭제 위험	0.94	18.94
	RSK3	중요파일 삭제 위험	0.90	17.80
	RSK4	중요정보 공개 위험	0.56	9.30
사용자 보안신념	USR1	패스워드 기억정도	0.69	10.69
	USR2	어려운 패스워드 설정정도	0.79	12.34
	USR4	패스워드 노출에 대한 보안	0.61	9.23
패스워드 보안태도	AT1	보안 교육 참여의 태도	0.76	12.17
	AT2	불법적 시스템 변경방지 태도	0.88	14.17
	AT3	화면보호 기능의 태도	0.44	6.55
보안행위 의도	INT1	상이한 패스워드 사용의도	0.63	9.07
	INT3	기록하지 않을 의도	0.72	10.38
	INT4	패스워드 갱신의도	0.64	9.24

<표 6> 측정모형의 쌍비교 판별 분석 결과

모형	df	χ^2	p-값	모형	df	χ^2	p-값
측정모형	209	377.51	0.00	측정모형	209	377.51	0.00
정보자산-위협 조합모형	215	859.82	0.00	취약성-위험인지 조합모형	215	589.60	0.00
정보자산-취약성 조합모형	215	597.94	0.00	취약성-보안신념 조합모형	215	661.63	0.00
정보자산-위험인지 조합모형	215	581.89	0.00	취약성-보안태도 조합모형	215	679.33	0.00
정보자산-보안신념 조합모형	215	600.22	0.00	취약성-행위의도 조합모형	215	576.06	0.00
정보자산-보안태도 조합모형	215	600.44	0.00	위험인지-보안신념 조합모형	215	515.67	0.00
정보자산-행위의도 조합모형	215	561.82	0.00	위험인지-보안태도 조합모형	215	530.98	0.00
위협-취약성 조합모형	215	576.12	0.00	위험인지-행위의도 조합모형	215	510.22	0.00
위협-위험인지 조합모형	215	726.05	0.00	보안신념-보안태도 조합모형	215	498.03	0.00
위협-보안신념 조합모형	215	658.03	0.00	보안신념-행위의도 조합모형	215	547.61	0.00
위협-보안태도 조합모형	215	661.61	0.00	보안태도-행위의도 조합모형	215	497.08	0.00
위협-행위의도 조합모형	215	552.19	0.00				

목을 합하여 제약모형(constrained model)으로 만든 뒤 비제약 모형(unconstrained model)과의 쌍비교 판별 분석(pairwise discriminant analysis)을 통해 개념적 차이를 분석하는 방식을 활용하였다. 이는 원래의 연구를 위한 측정모형과 연구개념의 조합모형 사이의 χ^2 추정치의 차이가 유의한지 평가하는 방법으로 원래의 모형과 조합모형 사이의 차이가 유의하게 나타날 경우 각각의 연구개념간 판별타당성을 확보하고 있는 것으로 판단하는 방식이다. 다음의 <표 6>에서

<표 7> 측정모형의 적합도 지수

구분	적합도지수	수용기준	분석결과
절대부합지수	χ^2/df	≤3.00	1.81
	χ^2 자유도(df) p-value	≥0.05	377.51 209 0.00
	기초부합지수(GFI)	≥0.90	0.88
	표준원소평균잔차(SRMR)	≤0.05	0.06
	근사원소평균자승잔차(RMSEA)	≤0.08	0.05
증분부합지수	수정부합지수(AGFI)	≥0.80	0.84
	표준부합지수(NFI)	≥0.90	0.90
	관계부합지수(RFI)	1.0근사	0.88
	증분부합지수(IFI)	1.0근사	0.95
	비교부합지수(CFI)	≥0.90	0.95
간명부합지수	간명기초부합지수(PGFI)	≥0.60	0.67
	간명표준부합지수(PNFI)	≥0.60	0.74

나타난 바와 같이 연구개념들의 조합모형 21개의 모형들의 χ^2 추정치가 모두 다르게 나타나 판별타당성이 있는 것으로 평가하였다.

4.4.3 측정모형의 적합도 평가

다음의 <표 7>에서 측정모형의 적합도를 살펴보면, χ^2(p-값)은 377.51(0.00)이고, χ^2을 자유도(df = 209) 나눈 비율이 1.81로 나타나 권장수준(≤3.00)을 만족시키는 것으로 나타나 모형이 적합한 것으로 나타났다. 그리고 절대부합지수 중 GFI는 0.88로 권장수준(≥0.9)에 근접하는 것으로 나타났으며, AGFI는 0.84로 권장수준(≥0.80)에 부합하는 것으로 나타났다. 연구모형이 얼마나 잘 근사하느냐의 정도를 나타내는 RMSEA는 0.05로 권고수준을 만족하고 있으며, 또한 1.0에 근사할 경우 적합하다고 볼 수 있는 IFI는 0.95, CFI는 0.95 등으로 수용기준에 부합하는 것으로 나타났다. 그 외에 PGFI는 0.67, PNFI는 0.74로 일반적으로 권고하는 수용기준인 0.6이상을 상회하는 것으로 나타나 전반적으로 측정모형의 적합도가 수용기준을 충족하는 것으로 평가하였다.

4.5 구조모형 평가 및 연구가설 검정

4.5.1 구조모형의 적합도 평가

다음으로 구조모형에 대한 적합도를 살펴보았다. 먼저, χ^2(p-값)은 415.98(0.00)이며, 자유도(df = 221)를 χ^2로 나눈 표준 χ^2(normed χ^2)은 1.88로 권장수준(≤3.00)에 부합하였다. 적합도 지수 중 GFI는 권장수준이 0.9이상이나 0.87로 근접하는 것으로 나타났으며, AGFI는 0.84로 권장수용 기준에 부합하는 것으로 나타나 연구의 구조모형이 우수하다고는 할 수 없으나 전반적으로 적합한 모형이라고 평가하였다. 또한 RMSEA는 0.06, CFI는 0.94, PGFI는 0.70 등 수

<표 8> 구조모형의 적합도 지수

구분	적합도 지수	수용기준	분석결과
절대부합지수	χ^2/df	≤3.00	1.88
	χ^2 자유도(df) p-value	≥0.05	415.98 221 0.00
	기초부합지수(GFI)	≥0.90	0.87
	근사원소평균자승잔차(RMSEA)	≤0.08	0.06
	표준원소평균잔차(SRMR)	≤0.05	0.08
증분부합지수	수정부합지수(AGFI)	≥0.80	0.84
	표준부합지수(NFI)	≥0.90	0.89
	관계부합지수(RFI)	1.0근사	0.87
	증분부합지수(IFI)	1.0근사	0.94
	비교부합지수(CFI)	≥0.90	0.94
간명부합지수	간명기초부합지수(PGFI)	≥0.60	0.70
	간명표준부합지수(PNFI)	≥0.60	0.78

용기준에 부합하는 것으로 나타나 구조모형이 연구개념들 사이의 관계를 설명하는데 적절하다고 평가하였다.

4.5.2 연구가설 검정

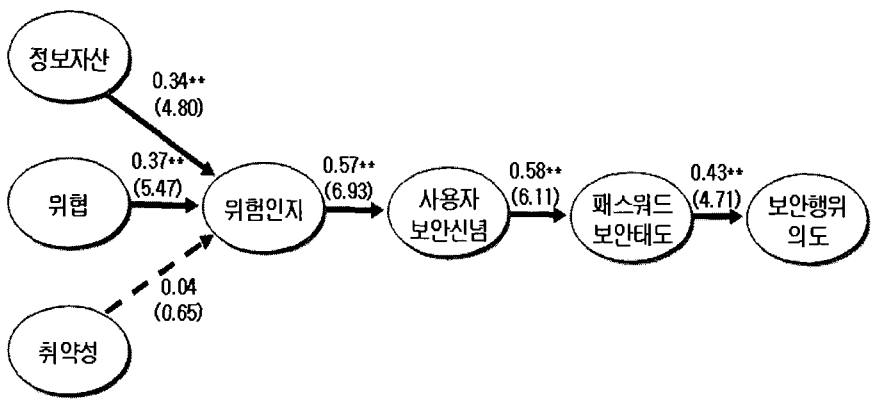
본 연구에서 연구가설의 검정결과를 요약하면 위험분석방법론을 토대로 사용자의 위험인지에 영향을 미치는 선행요인 중 취약성을 제외하고 모든 경로에서 통계적으로 유의한 것으로 평가되었다.

정보자산의 중요성이 사용자의 위험인지에 미치는 영향을 평가하기 위해 설정한 연구가설1(H1)은 경로계수가 0.34로 나타났으며, t-값이 4.80로 α=0.01에서 유의하게 설명하는 것으로 나타나 채택되었다. 또한 패스워드 노출 위협은 사용자의 위험인지에 영향을 미친다는 연구가설2(H2)의 경우 경로계수가 0.37이며, t-값이 5.47로 유의수준 α=0.01에서 통계적으로 유의하게 나타나 채택되었다. 하지만 패스워드 자체의 취약성이 사용자의 위험인지에 영향을 미친다는 연구가설3(H3)은 경로계수가 유의하지 않은 것으로 나타나 기각되었다.

사용자의 위험인지는 보안신념에 영향을 미친다고 설정된 연구가설4(H4)는 경로계수가 0.57, t-값이 6.93으로 유의수준 α=0.01에서 채택되었다. 또한 사용자의 보안신념은 패스워드 보안태도에 영향을 미친다는 연구가설5(H5)도 경로계수가 0.58, t-값이 6.11로 유의수준 α=0.01에서 채택되었으며, 전체 연구모형의 인과관계에서 가장 설명력이 높은 것으로 분석되었다. 마지막으로 패스워드 보안태도는 보안행위의도에 영향을 미친다는 연구가설6(H6)은 경로계수가 0.43, t-값이 4.71로 유의수준 α=0.01에서 통계적으로 유의하게 분석되어 채택되었다. 이로써 보안행위의도에 영향을 미치는 위험인지, 사용자 보안신념, 패스워드 보안태도 사이의 관계는 모두 통계적으로 유의한 것으로 확인되었다. 연구가설의 검정결과는 다음의 <표 9>에 요약하였다.

4.5.3 분석결과 논의

연구모형에서 사용자의 위험인지에 선행하



<그림 3> 연구모형 분석결과

주) 괄호 안은 t-값, **:유의수준 α=0.01에서 유의함.

<표 9> 연구가설의 검정결과 요약

연구가설	모형의 경로	경로계수(t-값)	검정결과
H1: 정보자산의 중요성은 사용자의 위험인지에 정(+)의 영향을 미친다.	정보자산 →위험인지	0.34(4.80)	채택
H2: 패스워드 노출 위협은 사용자의 위험인지에 정(+)의 영향을 미친다.	위협 →위험인지	0.37(5.47)	채택
H3: 패스워드의 취약성은 사용자의 위험인지에 정(+)의 영향을 미친다.	취약성 →위험인지	0.04(0.65)	기각
H4: 사용자의 위험인지는 보안신념에 정(+)의 영향을 미친다.	위험인지 →보안신념	0.57(6.93)	채택
H5: 사용자의 보안신념은 패스워드 보안태도에 정(+)의 영향을 미친다.	보안신념 →보안태도	0.58(6.11)	채택
H6: 패스워드 보안태도는 보안행위의도에 정(+)의 영향을 미친다.	보안태도 →보안의도	0.43(4.71)	채택

는 요인들 중 취약성을 제외한 정보자산 및 위협은 위험인지에 통계적으로 유의한 설명력을 가지는 것으로 나타났다. 또한, 사용자의 보안행위의도에 영향을 미치는 보안신념 및 보안태도 사이의 관계도 유의하게 나타났다.

먼저, 연구가설1에서 정보자산과 사용자 위험인지 사이의 유의한 관계는 정보시스템에 저장되어 있는 데이터, 개인정보 및 거래 정보, 인증정보 등의 상대적 가치를 사용자가 중요하게 여기고 있기 때문에 대외적으로 이들 정보자산이 노출 및 변조될 경우 파생될 여러 피해와 손실에 대해 사용자가 심각하게 수용하고 있음을 알 수 있다.

연구가설2를 통한 정보시스템 내·외부로부터 패스워드 노출 및 오·남용의 직접적인 원인 등의 시스템에 유해한 활동들에 대한 위협수준이 증가할수록 정보보안에 대한 사용자 우려를 증가시키고 이에 대한 위험을 크게 인지하는 것으로 평가할 수 있다.

그러나 연구가설3에서 패스워드 자체의 취약성과 정보보안의 위험인지 사이의 통계적으로 유의하지 않은 관계에 대해서는 현재 사용하고 있는 패스워드에 대해 사용자가 장기간의 사용, 기억력의 한계 및 여러 사이트에 중복사용으로 인한 약점을 사용자 스스로가 평가하기 어렵기 때문에 이로 인해 발생될 위험의 심각성을 인지하지 못하는 것으로 유추할 수 있다.

다음으로 보안신념, 보안태도, 보안의도 사이의 관계를 살펴보면 먼저, 연구가설4에서 사용자의 위험인지가 보안신념에 유의한 영향을 미치는 것으로 분석되었다. 이는 패스워드 노출로 인해 발생할 수 있는 프로그램 삭제, 개인정보 노출, 중요파일 삭제 등의 위험이 정보보안의 측면에서 사용자가 그 심각성을 인지하게끔 하는 선행요인이며, 패스워드 관리를 통한 보안사고 대응의 필요성과 중요성을 확신하도록 영향을 미치는 주요요인임을 확인할 수 있었다.

연구가설5를 통한 사용자 보안신념은 패스워드 보안태도에 유의한 영향을 미친다는 점을 확인할 수 있었다. 이는 사용자가 인지하는 보안

위험은 정보보안의 중요성과 필요성에 대한 강도가 커질수록 적절한 패스워드 관리에 대한 긍정적인 보안태도를 형성하는데 중요한 역할을 한다는 것을 알 수 있다.

또한, 연구가설6에서 패스워드 보안태도가 보안행위의도에 통계적으로 유의한 영향을 미치는 관계는 사용자의 적절한 패스워드 선택과 활용 등의 관리가 향후 긍정적인 정보보안 효과로 이어질 수 있다는 기대를 높이기 때문에 향후 여러 보안활동들에 대한 충분한 동기를 제공할 수 있음을 확인하였다.

V. 결 론

본 연구에서 정보보안을 위한 사용자의 패스워드 선택과 관련하여 위험인지가 정보보안 행위의도에 영향을 미치는지에 대해 구조모형을 이용한 실증분석이 이루어졌다. 분석결과에 따르면 자산과 위협이 사용자 위험인식에 통계적으로 유의한 반면, 취약성과 사용자의 위험인식 사이에는 관련성이 없는 것은 정보보안의 관점에서 중요한 시사점을 가진다. 이는 대부분의 사용자들은 자신이 설정해 놓은 패스워드에 대해 신뢰하고 의심을 하지 않기 때문으로 볼 수 있다. 이로 인해 조직에서 정보시스템의 보안을 위해 상당한 노력과 시간을 투자하고 있지만 사용자들의 무지와 어리석음으로 인해 쉽게 간과되어진다고 볼 수 있다(Yapp, 2001). 이러한 원인은 사용자들의 부족한 정보보안 지식과 전반적인 조직의 보안 매커니즘이 사용자의 행태적인 차원보다 기술적 측면에서 설명되었기 때문으로 볼 수 있으며, 이를 방지하기 위해서는 사용자에게 강력한 패스워드를 설정하기 위한 가이드라인이 강조되어야 한다.

하지만, Martinson(2005)의 연구에서 지적된 바와 같이 사용자들은 패스워드 선택과 사용에 있어 패스워드 설정 초기에 가이드라인을 귀찮은 것으로 여기는 것으로 나타나 패스워드 선택과 구성시 필수적인 요소들을 쉽게 잊어버리고, 이렇게 생성된 패스워드의 취약성에 대한 심각성을 잘 인지하지 못한다고 지적하였다. 이와 같은 패스워드 기능의 무력화를 방지하기 위해서는 정보시스템 또는 시스템 관리자가 정기적으로 패스워드 변경을 요청하거나 공지하도록 하며, 패스워드 구성과 선택방식에 대해 사용자의 보안의식 제고에 도움을 줄 수 있도록 다른 시스템과의 차별화를 가질 필요가 있다(Yan et al., 2000). 특히, 지나치게 긴 패스워드를 사용함으로써 사용자의 기억에 어려움을 가지게 할 필요가 없으며(Zivran & Haga, 1988), 악의적인 사용자에게 노출 또는 추측을 방지할 수 있도록 안전하고 좋은 패스워드의 길이와 구성, 변경주기 등(Gehringer, 2002)을 인지시킴으로써 보안활동의 동기를 부여할 수 있어야 한다.

다른 시사점은 사용자의 보안태도가 보안의도를 형성하는데 중요한 역할을 한다는 점이다. Adam & Sasse(1999)의 연구에서 사용자는 원래부터 패스워드 절차에 대한 불충분한 지식과 해당 원리를 잘 이해하지 못하기 때문에 정보보안에 대한 동기부여가 쉽지 않다고 설명하였다. 이에 따라 패스워드 선택과 사용에 관한 보안교육과 정책을 통한 사용자 보안인지의 증가가 정보보안을 위한 동기부여에 상당부분 기여함을 지적하였다. Ajzen & Fishbein(1980)이 TRA 모형에서 검증하였듯이 개인의 행위에 대해 가지

는 호감이 행위에 대한 의지를 증가시키는 주요 요인이므로 패스워드의 효율적인 관리가 보안 효과로 직결됨을 강조할 경우 사용자는 정보보안활동에 대한 호의적인 태도를 형성하게 되며, 이에 따라 보안침해를 예방할 수 있는 보안활동에 강력한 의도를 형성하게 될 수 있음을 시사하고 있다.

본 연구를 통한 연구의 의의는 다음과 같다. 먼저, 위험분석방법론의 정보자산, 위협, 취약성 요인의 개념적 프레임워크를 이용하여 정보보안의 차원에서 사용자의 위험인지를 실증 데이터를 이용하여 분석하였다. 또한, 정보보안에 대한 사용자의 행태적인 차원의 분석을 위해 TRA 모형의 신념, 태도, 행위의도를 수정 및 적용하여 구조방정식을 통해 분석함으로서 향후 정보보안 문제에 대해 연구모형의 적용 및 활용 가능성을 증가시켰다고 보았다. 그리고 사용자의 패스워드 취약성과 보안 위험인지 사이의 관계를 밝혀냄으로써 사용자의 인지적 차원에서 보안교육의 중요성과 사용자 친화적인 패스워드 설정과 사용 대해 관리적 차원의 문제를 부각시켰다.

마지막으로 본 연구의 한계와 향후 연구방향에 대해 살펴보면 먼저, 분석단위의 문제로 실증분석을 위해 사용된 표본집단이 대학생과 대학원생으로 국한되어 있어 정보시스템 사용자의 범위가 제한되어 있다. 추후 다양한 연령층을 대상으로 표본을 수집하여 측정함으로써 다양한 인구통계학적 특성을 가미한 연구결과를 검증해 볼 필요가 있다. 두 번째는 연구모형의 문제로 취약성과 위험인지 사이의 인과관계가 유의하지 않게 나타났다. 향후 연구에서 패스워드 관리상의 취약성과 위험인지 사이에 보안교육을 조절변수로 보고 해당 조절효과의 차이를 비교·분석할 필요가 있을 것이다.

참고문헌

김종기, 전진환, "컴퓨터 바이러스 통제를 위한 보안행위의도 모형", *정보화정책*, 제13권, 제3호, 2006, pp. 174-196.

대한상공회의소, "국내기업의 산업기밀유출 실태조사, 대한상공회의소," 2006. 7.

이필중, 문희철, "패스워드 시스템의 보안에 관한 고찰," *한국통신정보보호학회지*, 제1권, 제1호, 1991, pp. 109-118.

장명희, "인터넷 쇼핑몰에서 신뢰와 지각된 위험이 태도 및 구매의도에 미치는 영향," *정보시스템연구*, 제14권, 제1호, 2005, pp. 227-249.

전정훈, "누가 당신의 비밀번호를 빼간다면," *한겨레경제주간지*, 2007. 7. 23.

정경수, 김기영, 박종필, "패스워드 이용과 관한 실증분석: 대학과 종합병원을 중심으로," *한국경영정보학회*, 제30권, 제1호, 2001, pp. 143-157.

차윤숙, 정문상, "유비쿼터스 특성요인이 모바일 서비스의 사용의도에 미치는 영향," *정보시스템연구*, 제16권, 제2호, 2007, pp. 69-91.

한국정보보호진흥원, *정보보호 뉴스*, 2월호, 2007, pp. 12-14.

Adams, A., & M. Sasse, "Users are not the Enemy," *Communications of the ACM*, Vol. 42, No. 12, 1999, pp. 41-46.

Ajzen, I., & M. Fishbein, *Understanding Attitudes and Predicting Social Behavior.* Prentice-Hall, Inc., Englewood Cliffs: New Jersey, 1980.

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

Baskerville, R., "Risk Analysis: An Interpretive Feasibility Tool in Justifying Information System Security," *European Journal of Information Systems*, Vol. 1, No. 2, 1991, pp.121-130.

Bagozzi, R., & Y. Yi, "On the Evaluation of Structural Equation Models," *Journal of the Academy of Marketing Science*, Vol. 16, No. 1, 1988, pp.74-97.

CCTA, *CRAMM User Guide.* Central Computer and Telecommunications Agency, 2001.

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

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

Davis, F., R. Bagozzi, & P. Warchaw, "User Acceptance of computer Technology: A Comparison of Two Theoretical Models," *Management Science*, Vol. 35, No. 8, 1989, pp. 982-1003.

Eloff, M., & S. Solms, "Information Security Management: A Hierarchical Framework for Various Approaches," *Computers & Security*, Vol. 19, No. 3, 2000, pp. 243-356.

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

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

Garver, M., & 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.

Gefen, D., "Assessing Unidimensionality through LISREL: An Explanation and Example," *Communications of the Association for Information Systems*, Vol. 12, No. 2, 2003, pp. 23-47.

Gehringer, E., "Choosing Passwords: Security and Human Factors," *Proceedings of the 2002 IEEE International Symposium on Technology and Society*, June, 2002, pp. 369-373.

Gilbert, I., "Risk Analysis: Concepts and Tools," *Datapro Reports on Information Security*, 1991, pp. 101-112.

Hair, J., R. Anderson, W. Black, & R. Tatham, *Multivariate Data Analysis(5th eds.)*, Prentice Hall, 1998.

ISO/IEC, *IT 보안관리를 위한 지침- 제3부: IT 보안관리를 위한 기술*, KS X ISO/IEC TR 13335-3, 2005a.

ISO/IEC, *Information Technology-Security Techniques-Code of Practice for Informations Security Management*, ISO/IEC 17799, 2005b.

Ives, B., K. Walsh, & H. Schneider, "The Domino Effect of Password Reuse," *Communications to the ACM*, Vol 47, No. 4, 2004, pp. 75-78.

Juang, W., "Efficient Password Authenticated Key Agreement Using Smart Cards," *Computers & Security*, Vol. 23, No. 2, 2004, pp. 167-173.

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

Martinson, W., *Passwords: A Survey on Usage and Policy*, Masters Thesis, Air Force Institute of Technology, 2005.

NIST, *Risk Management Guide for Information Technology Systems*, Special Publication 800-30, 2001.

O'Gorman, L., A. Bagga, & J. Bentley, "Query-Directed Passwords," *Computers & Security*, Vol. 24, No. 7, 2005, pp. 546-560.

Rainer, R., C. Snyder., & H. Carr, "Risk Analysis for Information Technology," *Journal of Management Information System*, Vol. 8, No. 1, 1991, pp. 129-147.

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.

Tregear, J., "Risk Assessment," *Information Security Technical Report*, Vol. 6, No. 3, 2001, pp. 19-27.

Wakefield, R., "Network Security and Password Policies," *The CPA Journal*, June, 2004, pp. 7-8.

Yan, J., Blackwell, A., Anderson, R., & A. Grant, *The Memorability and Security of Passwords - Some Empirical Results*, Cambridge University Computer Laboratory, 2000.

Yapp, P, "Passwords: Use and Abuse," *Computer Fraud & Security*, Vol. 2001, No. 9, 2001, pp. 14-16.

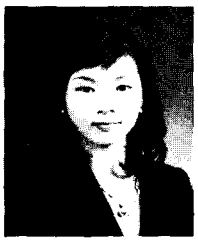
Zviran, M., & W. Haga, "Password Security: An Empirical Study," *Journal of Management Information Systems*, Vol. 15, No. 4, 1999, pp. 161-485.

CERT/CC, http://www.cert.org/tech_tips/passwd_file_protection.html, 2002.

김종기(JongKi Kim)

부산대학교 경영학과에서 경영학학사를 받고, Arkansas State University에서 경영학석사, Mississippi State University에서 경영학 박사학위를 받았다. 현재 부산대학교 경영학부 부교수로 재직하고 있으며, 주요 관심분야는 정보시스템 보안관리, 전자상거래, 프로젝트 관리 등이다.

강다연(Dayeon Kang)



한국해양대학교 경영학과에서 경영학학사를 받고, 부산대학교 일반대학원 경영학과에서 경영학 석사학위를 받았다. 현재 부산대학교 일반대학원 경영학과 박사과정에 재학중이며, 주요 관심분야는 정보시스템 보안관리, 정보기술 보안, e-비즈니스 등이다.

전진환(JinHwan Jeon)

인제대학교 경영학과에서 경영학학사, 경영학 석사학위를 받고 부산대학교 일반대학원 경영학과에서 경영학 박사학위를 받았다. 주요 관심분야는 정보시스템 보안관리, 전자상거래, 지식경영시스템 등이다.

<Abstract>

A Study on Factors Influencing User's Security Behavioral Intention for Choosing Password

JongKi Kim · Dayeon Kang · JinHwan Jeon

Nowadays, openness and accessibility of information systems increase security threats from inside and outside of organization. Appropriate password is supposed to bring out security effects such as preventing misuses and banning illegal users. This study emphasizes on choosing passwords from perspective of information security and investigated user's security awareness affecting behavioral intention.

The research model proposed in this study includes user's security belief which is influenced by risk awareness factors such as information assets, threats and vulnerability elements. The risk awareness factors are derived from risk analysis methodologies for information security. User's risk awareness is a factor influencing the security belief, attitude toward security behavior, and security behavioral intention.

According to the result of this study, while vulnerability is not related to the risk awareness, information assets and threats are related to the user's risk awareness. There is a significant relationship between risk awareness and security belief. Also, user's security behavioral intention is significantly affected by security attitude.

Keywords: Risk Awareness, Security Belief, Security Attitude, Security Behavioral Intention

* 이 논문은 2007년 10월 19일 접수하여 2차 수정을 거쳐 2008년 1월 24일 게재 확정되었습니다.