情報保護學會論文誌
第18卷 第4號, 2008. 8

보안정책, 보안의식, 개인적 특성이 패스워드 보안효과에 미치는 영향

김 종 기†, 강 다 연‡
부산대학교

The Effects of Security Policies, Security Awareness and Individual Characteristics on Password Security Effectiveness

Jongki Kim†, Dayeon Kang‡
Pusan National University

요 약

정보시스템의 확대 및 인터넷 사용의 급격한 증가에 따라 정보보안의 중요성이 대두되고 있다. 그럼에도 불구하고, 우리는 정보보안의 중요성을 심각하지 않게 받아들이고 있다. 본 연구는 조직에서의 보안정책이 정보시스템 사용자의 보안의식과 개인적 특성에 변화가 있는지 살펴보고, 보안의식과 개인적 특성이 패스워드 사용에 있어서의 보안효과를 가져다주는지 실증분석 하는 것이 궁극적인 목적이다. 구조방정식 모형 기법을 적용한 본 연구모형의 분석결과에 의하면, 보안정책은 개인적 특성과 사용자의 보안의식 향상에 통계적으로 유의한 영향을 미친다. 또한 개인적 특성과 보안의식은 보안효과에 긍정적인 영향을 미치는 것으로 나타났다. 따라서 기업 내의 정보보안은 보안정책을 잘 준수하고 이에 따른 개인적 특성과 보안의식 수준이 향상되었을 때 보다 안전한 패스워드의 보안효과를 거둘 수 있다.

ABSTRACT

Information securiry is considered important due to the side effect generated from the expansion of information system and rapid increase of the use of internet. Nevertheless, we are getting unconscious of the importance of information security. The purpose of this research is to empirically analyze that the effects of security policies, security awareness and individual characteristics on password security effectiveness. Based on the analysis of research model using structural equation modeling technique, security policies were influencing individual characteristics and improving user's security awareness. Also individual characteristics and security awareness had positive impact on security effectiveness.

Keywords : Security Policy, Individual Characteristics, Security Awareness, Security Effectiveness.

Ⅰ. 서 론

정보시스템 사용이 대중화되면서 단순 자료검색에서 전문화된 서비스 및 애플리케이션의 제공으로 정보보안 분야가 점점 넓혀지고 있다. 이와 함께 개인정보유출의 피해와 심각성은 정보시스템 분야의 발전과 더불어 나

접수일 : 2008년 3월 12일; 수정일 : 2008년 4월 28일;
채택일 : 2008년 5월 23일
† 주저자, jkkim1@pusan.ac.kr
‡ 교신저자, kdy@pusan.ac.kr

날이 증가하고 있는 추세이다. 한국 기업의 20.5%가 기밀정보유출로 인한 피해를 경험하였으며, 이로 인해 외부 공격으로부터 방어하기 위한 네트워크 보안에서 기밀정보유출을 방지하기 위한 콘텐츠 보안으로 보안의 패러다임이 변화하고 있다[1]. 즉, 정보유출방지를 위한 정보시스템보안의 중요성이 그 어느 때보다 강조되어야 함을 보여준다. 정보시스템 보안이 완벽하다는 것은 있을 수 없다. 미래의 보안위험에 대해 아무도 정확하게 예측할 수 없으며, 이는 정보시스템 보안의 특성상 대부분의 정보 및 정보시스템은 공격에 취약하며 완전한 정보시스템은 존재하지 않기 때문이다[2]. 하지만 정보시스템 보안을 통하여 개인 프라이버시를 보장하고 정보범죄를 차단함으로써 정보의 안전성, 신뢰성을 가져다 줄 수 있기 때문에 정보시스템 보안을 위한 노력은 중요하다.

컴퓨터 정보보안에 가장 일반적으로 사용하는 방법이면서 그에 따른 위험이 많이 존재하는 것이 패스워드이며, 내·외부로부터의 정보유출 위험을 대비하기 위하여 적절한 패스워드를 선택할 수 있도록 보안정책을 설정하는 것이 중요하다[3,4]. 정보보안을 위한 패스워드의 중요성에 관한 연구는 다수 있지만[3,5], 패스워드 사용에 있어서의 보안효과에 영향을 미치는 요인들을 분석하는 연구는 없었다.

본 연구에서는 패스워드 사용에 있어서의 보안효과에 영향을 미치는 요인으로 보안정책, 개인적 특성, 보안의식으로 구성하여 실증분석 하고자 한다. 이는 조직에서의 보안정책이 정보시스템 사용자의 보안의식과 개인적 특성에 변화가 있는지 살펴보고, 보안의식과 개인적 특성이 패스워드 사용에 있어서의 보안효과를 가져다주는지 확인함으로써 패스워드 노출로 인한 정보유출 위험을 최소화하고자 한다.

Ⅱ. 이론적 배경

2.1 정보보안과 패스워드

정보보안은 시스템 및 정보를 고의 혹은 실수에 의한 공개, 변조, 파괴 및 지체로부터 보호하는 것이다[6]. 정보화 사회에서의 정보보안은 정보시스템 보안에서부터 시작되어야하며, 정보시스템 사용자는 보안의 중요성을 인식해야 한다. Goodue & Straub[7]은 정보보안의 관심은 산업의 특성에 기인하는 보안취약성, 보안향상을 위하여 조직이 취한 행동, 그리고 사용자의 시스템에 대한 인지도 및 지식에 의존한다고 하였다. 이때 사용자가 잠재적인 보안위험에 대해 더 많이 인식하고 있을 경우 정보시스템 관련 보안에 대해 더 높은 관심이 나타날 것이며, 현재의 시스템 보안대책에 대하여 덜 만족할 것이라고 하였다. 김종기의 연구[8]에서는 정보시스템에 대한 적정수준의 관심과 인지도는 합리적인 보안대책 선정의 전제조건이라고 가정하고, 정보시스템 보안을 위한 투자의 효과와 투자 결정에 영향을 미치는 정보시스템 내·외적인 요인들을 나타내었다. 정보통신부[9]에서 제안한 정보보안지침서에 따르면 정보시스템 사용자의 PC에 패스워드를 설정하는 것이 정보시스템 사용자측면에서 가장 손쉽게 개인정보유출을 방지하기 위한 방안이라고 하였다. 이를 위해 정보시스템 사용자는 정보보안을 위한 패스워드를 선택할 때의 권고사항이 제시된 연구[10,11]를 기반으로 안전한 패스워드를 선택해야 한다. 안전한 패스워드란 제3자가 쉽게 추측할 수 없고 시스템에 저장되어 있는 정보 또는 인터넷을 통해 전송되는 정보를 해킹해서 사용자의 패스워드를 알아낼 수 없거나 알아낸다 하더라도 많은 시간이 요구되는 패스워드를 말한다. 이러한 패스워드는 정보시스템 사용자의 정보유출 피해를 감소시킬 수 있으며, 정보의 손실을 최소화 시킬 수 있을 것이다.

2.2 보안정책

보안정책은 조직체 내에서 정보보안 임무를 수행하기위한 최상위 보안 요구사항이다[9,12]. 보안정책은 하나의 정형화된 정책이 존재하는 것만 말하는 것이 아니며, 조직의 임무, 정보시스템의 종류, 규모, 역할, 운영방식 등 조직의 목표와 특성에 맞는 정책을 말한다[13]. 보안성 강화를 위해서 잘 정의되고 검증된 보안정책은 조직구성원들로부터 안전성과 신뢰성을 확보할 수 있다. 이러한 보안정책을 수립하기 위해서 고려해야 할 요소를 살펴보면 다음과 같다. 먼저, 조직원의 이해와 시행에 혼선을 초래하지 않는 보안정책이 수립되어야 하며, 조직의 목표변화, 기술능력의 변화, 보안요구의 변화 등에 따라 융통성을 가질 수 있어야 하기 때문에 경직된 보안정책이 되어서는 안된다. 이러한 보안정책은 조직의 정보보안에 보다 효과적인 방안을 제시할 것이다.

2.3 보안의식

인터넷과 정보통신 기술의 사용이 대두되면서 개인정보는 단순한 신분정보에서 현재는 자산적 가치로 높게 평가되고 있으며, 이러한 개인정보는 사회적 경쟁력을 높이는데 기여한다. 만약 중요한 개인정보가 유출 될 경우 개인정보가 오용되어 개인·조직의 안전과 재산에 중대한 손실을 초래할 수 있기에 우선적으로 정보시스템 사용자는 스스로의 보안의식을 가져야 할 필요성이 있다. 2006년 정보보호 실태조사 결과 중 '정보보호 인식 부문'에서 정보시스템 사용자인 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 것으로 나타났다[14]. 정보시스템 사용자가 정보보안에 대한 인식을 가지고 있을 때 정보보안과 관련된 의식수준이 향상되며, 정보유출피해를 최소화할 수 있는 것이다.

2.4 개인적 특성

개인적 특성은 정보시스템 이용과 성과에 영향을 주는 개인정보 보호와 관련한 사전지식의 정도이다[15]. 정보시스템 사용에 관한 보안인지 여부와 패스워드 관련 지침의 인지정도는 개인적 특성을 반영할 수 있으며, 정보시스템 사용기간과 보안의 관심도로 보안관련 개인적 행위 특성을 측정할 수 있다. Ronald et al.[16]과 Lee et al.[17]은 개인적 특성 또는 사용자 능력이 정보시스템 이용과 성과에 영향을 주는 중요한 요인이라고 지적하였으며, 최종사용자 능력인 개인적 특성이 성과변수인 정보시스템 만족도에 직접적인 영향을 준다고 하였다. 또한 Baldwin & Rice[18]와 King & Xia[19]의 연구에서는 최종사용자 능력을 향후 사용자 특성, 또는 개인적 특성이라는 구성개념으로 사용되고 있었다. Albrechtsen[20]은 사용자를 위해 개인적인 보안의식과 행동에 영향을 주는 요소들을 가지고 정보보안의 취약점을 해결하기 위한 가이드라인을 제시하였다. 따라서 정보시스템의 보안효과에 영향을 주는 요소로 개인적 특성을 설명한다.

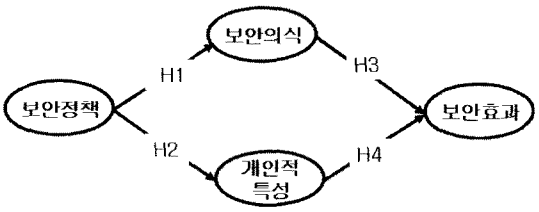
2.5 보안효과

정보시스템 보안의 위험을 식별하고, 위험의 정도를 결정하여 보안대책 또는 보안통제가 필요한 곳을 식별함으로써 위험관리 측면의 보안효과를 기대할 수 있다[8]. 정보시스템에서 처리, 운용되는 주요정보의 가용성과 유용성, 무결성과 인증성, 비밀성과 정보의 소유성 확보도 주요 정보보안의 효과를 극대화 할 수 있다. 정보시스템 보안효과를 위한 방안으로 공인되지 않은 소프트웨어의 설치·실행의 방지를 제시하였으며 보안을 위한 관리부분에서는 이메일과 패스워드의 보호, 보안 자동화의 설정이 있다[21]. 정보시스템 보안효과를 극대화하기 위해서는 정보유출을 통제하기 위한 보안교육과 보안대책을 강구해야하며, 정보시스템 사용자는 이러한 보안대책을 수행하였을 때 보안효과를 기대할 수 있다.

Ⅲ. 연구모형 및 연구가설

3.1 연구모형 및 설계

본 연구에서 조직 내의 보안정책이 보안효과에 영향을 미치는 요인들에 대해 실증적으로 규명하고자 다음 [그림 1]과 같이 연구모형을 설정하였다. 우선 조직 내의 보안정책이 사용자의 보안의식과 개인적 특성에 영향을 미치며, 이러한 보안의식과 개인적 특성은 보안효과에 정(+)의 영향을 미칠 것이라는 연구모형을 설정하였다.



〔그림 1〕 연구모형

3.2 연구가설

3.2.1 보안정책과 보안의식

연구가설1(H1)은 정보시스템 보안침해 사고를 최소화하기 위한 조직의 규정, 절차인 보안정책이 정보시스템 사용자의 보안의식에 영향을 미치는 인과관계에 대한 가설이다. 보안정책의 훈련과 교육이 사용자의 보안

의식에 중요한 역할을 하며[13,22], 전략적 정보시스템 계획에 따른 조직의 목표를 이루기 위해서는 조직의 발전을 위한 보안정책이 제공된다[23]. 특히, 정보시스템 사용자의 정보보안을 위한 보안정책의 인지정도는 조직 내의 정보유출 방지를 위한 보안정책의 권고사항에 따라 보안정책이 평가되고 있는지 확인해야 할 필요성이 있다. 이러한 보안정책의 권장은 정보시스템 사용자의 보안의식 향상에 긍정적인 영향을 미칠 것이라는 연구가설을 도출하였다.

H1 : 보안정책은 정보시스템 사용자의 보안의식에 정(+)의 영향을 미칠 것이다.

3.2.2 보안정책과 개인적 특성

연구가설2(H2)는 조직 내의 정보보안 임무를 수행하기 위한 최상위 보안요구사항인 보안정책이 정보시스템 보안관련 지식과 인지정도인 개인적 특성 간의 관계에 대한 가설이다. 조직의 임무, 정보시스템의 종류, 규모, 역할, 운영방식 등 조직의 목표와 특성에 맞는 정책이 수립되면 개인적 특성인 보안지식과 보안인지도가 높아진다는 것이다[13,16]. 즉, 보안정책의 목적은 보안침해 사고 또는 직원들의 고의 또는 실수에 의한 위험을 최소화시키고 직원들의 실질적인 정보보안 수준 향상을 위하여 인식제고, 보안교육, 성과측정, 훈련, 감사체계를 정의하는 것이다. 이를 위해 정보시스템 사용자는 보안유지를 위해 필수적으로 포함되어야 하는 보안정책 적용과 동시에 정보보안의 중요성을 인식하고 컴퓨터 관련 배경지식의 습득을 통한 개인적 특성을 지니는 것이다. 따라서 정보보안을 위한 보안정책은 정보시스템 사용자의 개인적 특성에 긍정적인 영향을 미칠 것이라는 가설을 도출하였다.

H2 : 보안정책은 개인적 특성에 정(+)의 영향을 미친다.

3.2.3 보안의식과 보안효과

연구가설3(H3)은 정보보안을 위한 사용자의 보안의식이 보안효과를 가져다준다는 가설이다. 정보시스템 사용자의 보안의식은 지속적으로 변화하는 보안환경에 따라 효율적인 위험관리 문제를 사전 방어적인 보안체계를 가지도록 해준다. 정보시스템 사용자 보안의식은 보안에 대한 위험과 보안의 중요성을 인지한 상태에서 행해지기 때문에 효율적인 보안효과는 개인정보유출 피해를 최소화하기 위한 보안위험을 감소시키는 결과를 가져다준다. 정보시스템 내의 보안관심도가 높으면 보안관련 지식이 많고 그에 따른 보안의식의 수준도 높게 평가될 수 있으며, 이와 반대로 보안관심도가 낮으면 보안관련 지식이 적고 보안의식 수준이 낮다고 평가할 수 있다. 따라서 사용자의 보안의식은 보안효과에 긍정적인 영향을 미친다는 가설을 도출하였다.

H3 : 보안의식은 보안효과에 정(+)의 영향을 미친다.

3.2.4 개인적 특성과 보안효과

연구가설4(H4)는 정보시스템 이용과 성과에 영향을 주는 개인정보 보호와 관련한 사전지식인 개인적 특성이 보안효과를 가져다준다는 가설이다. 개인적 특성에 따라 최종사용자 행동을 분석한 Stanton et al.[24]의 연구에서 컴퓨터 관리문제 해결방안의 개인적 특성이 보안효과를 가져다준다고 하였으며, Lee et al.[17]은 정보시스템 보안효과를 보안훈련과 수용을 통한 보안지식의 습득이 개인적 특성이자 보안효과를 기대할 수 있다고 하였다. 또한 Baldwin & Rice[18]와 King & Xia[19]의 연구에서도 정보시스템의 보안효과를 개인적 특성과 연관되어 있다는 점을 다시 한 번 강조한다. 컴퓨터와 관련된 문제 발생을 해결하는 능력이 곧 컴퓨터 보안관리를 할 수 있는 개인적 특성이며, 이는 정보시스템 사용자의 보안관련 지식의 관심과 인지도라고 할 수 있으며, 보안효과는 보안의 만족도로 측정한다. 따라서 개인적 특성은 보안효과에 긍정적인 영향을 미친다는 가설이 도출되었다.

H4 : 개인적 특성은 보안효과에 정(+)의 영향을 미친다.

3.3 연구변수의 조작적 정의 및 설문항목

본 연구에서 패스워드에 관한 보안효과를 보안정책, 보안의식, 개인적 특성 요인들로 검정하기 위해 수립된 연구 개념들은 아래의 [표 1]과 같이 조작적으로 정의되었다. 먼저 보안정책은 정보시스템 보안침해 사고를 최소화하기 위한 조직의 규정, 절차라고 조작적 정의를 내렸다[12]. 본 연구에서의 보안정책은 패스워드 보안정책 측면에서 살펴보았다. 정보유출 방지를 위한 패스워드 정책의 권고사항에 따라 보안정책이 평가되고 있는지 확인할 필요성이 있다. 패스워드 보안정책을 측정하고자 하는 변수로는 ISO/IEC[25]와 정보통신부[9]에

〔표 1〕 변수의 조작적 정의 및 측정항목

연구변수	조작적 정의	측정항목	관련문헌
보안정책 (POL)	정보시스템 보안침해 사고를 최소화하기 위한 조직의 보안규정, 절차의 권장	POL1 정보보안교육 실시 POL2 패스워드 설정 권장 POL3 조합된 패스워드 권장 POL4 패스워드 변경 권장	Doherty & Fulford(2006) Karyda et al(2005) 정보통신부(2008) 정보통신부(2006) 김종기 & 전진환(2006) ISO/IEC(2005)
보안의식 (AWN)	정보시스템 사용자 스스로의 정보보안에 대한 관심과 중요성을 인지하는 정도	AWN1 정보보안 제반규정 AWN2 정보노출 대응조치 AWN3 정보노출 관심도 AWN4 보안지침의 실천 AWN5 정기적 패스워드 변경	Drevin et al.(2007) Leach(2003) Frank(1991) 임채호(2006)
개인적 특성 (IND)	정보시스템 이용과 성과에 영향을 주는 개인정보 보호와 관련한 사전지식의 정도	IND1 보안지식 정도 IND2 패스워드 권고사항 인지 IND3 컴퓨터 해결방안 지식 IND4 정보보안 대응방안 지식	Stanton et al.(2005) Baldwin & Rice(1997) King & Xia(1997) Lee et al.(1995)
보안효과 (EF)	정보시스템 사용자의 적정수준의 관심과 인지도를 통한 보안의 만족도의 정도	EF1 데이터 노출 EF2 중요 파일 노출 EF3 개인정보 노출 EF4 업무문서 노출	Roger A(2006) Zviran(1999) Menkus(1998) Goodue & Straub(1991) 김종기(1998)

서 제시하고 있는 패스워드 노출 예방을 위해 정보보안 교육을 실시하면서 노출 방지를 하고 있는지를 확인하는 것이다. 또한 정보시스템 사용자에게 임시로 부여 받은 패스워드는 반드시 새로운 패스워드로 권장하는 것을 권장하고 있는지 여부를 확인한다. 또한 패스워드 생성 시 문자·숫자의 조합된 패스워드 사용을 제시하고, 정보유출 피해를 예방하기 위한 컴퓨터 사용제한을 위한 패스워드 설정을 권장하는 것도 보안정책을 측정하기 위한 변수로 구성하였다. 보안의식은 정보시스템 사용자 스스로의 정보보안에 대한 관심과 중요성을 인지하는 정도라고 조작적 정의를 내렸다[26]. 개인정보 보안의식의 변수로는 Frank et al.[27]의 연구에서 조직 내의 PC 사용자행위를 정보보안을 위한 보안관련 제반 규정의 중요성 부분에서 측정하도록 한다.

또한 Leach[28]의 연구에서 제시한 보안절차를 준수하는 것, 보안지침의 실천이 사용자 보안의식의 향상을 위한 행동으로 바라보고 측정변수를 설정한다.

Drevin et al.[29]의 연구에서는 정보통신 기술발달로 인한 보안의식은 정보보안을 행함으로써 보안의식 수준이 높아진다고 하였기에 개인정보 노출 대응조치의 중요성을 강조하였다. 이러한 대응조치는 임채호[26]의 연구에서 정보시스템 사용자의 정보보안을 위한 인식제고가 우선적으로 이루어질 때 가능하다고 강조하였다. 인식제고를 위해서는 개인정보 노출에 대한 관심의 정도가 높아야 하며, 패스워드 노출 가능성을 줄이기 위해 사용자는 정기적인 패스워드 변경이 이뤄질 때 정보보안의 중요성을 인지하는 것이라고 보며, 보안의식을 측정하기 위한 변수를 구성하였다.

개인적 특성은 정보시스템 이용과 성과에 영향을 주는 개인정보 보호와 관련한 사전지식이라고 조작적 정의를 내렸다[24]. Lee et al.[17]은 정보시스템 보안효과를 보안훈련과 수용이라는 결과를 통해 나타나는 컴퓨터 보안지식 정도라고 설명했다. 패스워드 보안과 관련된 개인적 특성은 패스워드 권고사항을 얼마나 잘 인지하고 있는지, 정보시스템의 사용에 대한 보안에 대해 알고 있는지의 보안관련 지식, 패스워드 책임에 대해 알고 있는지 정보보안 대응방안 변수를 말한다. 또한 컴퓨터와 관련된 문제 발생을 해결하는 능력이 곧 컴퓨터 관리를 할 수 있는 개인적 특성이라고 보았기에 컴퓨터 해결방안 변수를 개인적 특성을 측정하기 위한 변수로 구성하였다.

보안효과는 정보시스템 사용자의 적정 수준의 관심

과 인지도를 통한 보안의 만족도라고 조작적 정의를 내렸다[7]. 이를 위해 정보보안과 관련된 연구들에서는 보안효과를 위한 정보시스템 보안의 중요성에 대해 설명하고 있다. 정보시스템 보안의 기본적인 요건은 처리 대상인 정보나 정보시스템에 따라 기밀성, 무결성, 가용성 측면에서 보안을 설명할 수 있다. 기본적으로 정보보호의 목표에 도달했는지 내부 또는 외부 침입자에 의해 행해지는 각종 정보의 파괴, 변조 및 노출 등과 같은 행위로부터 정보를 보호하여, 보안에 대한 만족도를 측정하기 위한 변수로 구성하였다. 따라서 정보시스템 사용자가 선택한 패스워드로 인해 데이터 노출은 없었는지, 중요한 파일 노출의 피해, 개인정보 노출의 피해, 업무문서 노출의 피해의 변수를 구성하여 실증분석 하고자 한다.

Ⅳ. 실증분석

4.1 자료수집

본 연구에서는 보안정책에 따른 개인적 특성과, 보안의식이 보안효과에 영향을 미치는지 실증적으로 검정하기 위해 표본집단으로 직장을 가지면서 학업을 하는 경영대학원생들을 선택하였다. 경영대학원생들을 선정한 이유는 직장인들로 구성되어 있기에 조직에서의 업무를 위한 정보시스템을 사용하고 있으며, 본 연구에서 설문하고자 하는 보안정책과 관련하여 소속된 조직의 정보보안 정책을 이해할 수준이라고 생각했기 때문이다.

본 연구는 기존의 다른 분석법과 구별되는 중요한 특성인 다중 및 상호종속관계를 동시에 추정할 수 있고 이들 관계에서 잠재변수를 포함할 수 있으며,또한 측정오차를 추정할 수 있는 분석방법인 구조방정식모형(Structural Equation Modeling; SEM)을 사용하였으며, 분석도구로 AMOS 7.0을 사용하여 수집된 데이터를 실증적으로 분석하였다. 경영대학원에 재학 중인 학생들에게 총 200개의 설문지를 배부하여 181부를 회수하였으며, 결측치가 있거나 불성실하게 응답한 설문지 13부를 제외한 168부가 최종분석에 사용되었다.

4.2 표본의 특성

본본 연구를 위한 표본집단의 인구통계특성은 다음과 같이 나타났다. 아래에 제시된 [표 2]는 응답자가 소속되어 있는 조직의 특성 및 개인의 컴퓨터 사용 특성이다.

〔표 2〕 응답자의 특성

구분		빈도(명)	비율(%)
IT부서	있다	123	73.2
	없다	45	26.8
보안전담 조직	있다	114	67.9
	없다	54	32.1
컴퓨터 사용기간	5년 이하	12	7.1
	6~10년	23	13.7
	11~15년	58	34.5
	16~20년	65	38.7
	21년 이상	10	6
1일 컴퓨터 사용시간	1시간 미만	7	4.2
	1~3시간	32	19
	4~6시간	61	36.3
	7~9시간	45	26.8
	10시간 이상	23	13.7
패스워드 수	1개	6	3.6
	2개	45	26.8
	3~4개	86	51.2
	5~6개	23	13.7
	7개 이상	8	4.8
패스워드 변경	한 달 이내	2	1.2
	1~3개월	38	22.6
	4~6개월	21	12.5
	6개월~1년	38	22.6
	변경하지 않음	69	41.1
패스워드 노출경험	있다	15	8.9
	없다	153	91.9
합계		168	100

응답자의 성별 비율은 여자가 23명(13.7%) 남자가 145명(86.3%)으로 남자의 비율이 상대적으로 높게 나타났으며, 연령에서는 20~30세가 3명(1.8%), 30~40세가 57명(33.9%) 40~50세 이상이 108명(64.3%)으로 나타났다. 업종별로는 제조업 53명(31.5%), 금융 및 보험업 32명(19%), 기타 23명(13.7%), 통신업 16명(9.5%)순이었다. 종업원 수는 100명 이하가 43명(25.6%), 100명 이상에서 300명 이하가 37명(22%), 300명 이상에서 1000명 이하가 36명(21.4%), 1000명 이상이 52명(31%)으로 기업의 규모가 고루 분포된 비율로 나타났다. 연간매출액은 500억 이상이 60명(35.7%), 50억 미만이 42명(25%), 200억 이상에서 500억 미만 40명(23.8%), 50억 이상에서 200억 미만이 26명(15.5%)으로 종업원 수와 연간 매출액은 비례하는 것으로 나타났다.

4.3 측정모형의 추정과 분석

본 연구에서는 기존의 타당성이 인정된 연구 모형을 재검증하는 확인적 성향의 연구로, 측정모형의 추정과 분석을 위하여 확인적 요인분석(Confirmatory Factor Analysis)으로 측정모형을 추정한 뒤, 구조모형을 추정하는 구조방정식 모형의 2단계 접근법을 실시하였다[30]. 먼저 구조방정식 모형의 1단계 분석에서 확인적 요인분석을 통해 측정모형을 추정하였으며, 분석도구는 구조방정식 모형을 분석하기 위한 AMOS 7.0을 사용하였다. 확인적 요인분석을 이용하여 척도의 타당성을 분석하고, 측정모형의 신뢰도와 평균분산추출값(AVE; Average Variance Extracted)을 산출하였다.

4.3.1 측정모형의 신뢰성과 집중타당성

확인적 요인분석은 구성개념 타당성에 대해 전반적이고 확증적인 평가를 가능하게 해주며, 집중타당성과 판별타당성에 대해서 확인평가를 가능하게 한다[31]. 측정하부모형의 신뢰성을 평가하기 위해 합성개념신뢰도와 AVE값, Cronbach-값을 검정한 결과는 다음의 [표 3]과 같다. 먼저 합성개념신뢰도의 경우 모든 구성개념이 권장수준인 0.7이상을 상회하는 것으로 나타나 전반적으로 양호한 수준으로 평가되었다. 다음으로 AVE값의 경우 구성개념에 의해서 설명되는 분산의 양을 나타내며 0.5보다 작은 경우에는 측정오차가 구성개념에 의해서 설명되는 분산보다 크기 때문에 신뢰성이 없다고 할 수 있다. 본 연구에서는 AVE값에 대한 모든 항목이 0.5이상으로 나타났으므로 신뢰성이 있는 것으로 판단하며 측정항목의 집중타당성이 충분히 있다고 판단한다.

〔표 3〕 측정모형의 신뢰성과 집중타당성

연구개념	항목	표준화 추정치	측정오차	평균(표준편차)	합성개념신뢰도	Cronbach-α	AVE
보안정책	POL1	0.883	0.221	5.60(1.229)	0.937	0.933	0.787
	POL2	0.903	0.184	5.77(1.093)			
	POL3	0.946	0.105	5.82(1.051)			
	POL4	0.812	0.341	5.79(1.184)			
보안의식	AW1	0.8	0.36	5.00(0.994)	0.898	0.892	0.638
	AW2	0.772	0.405	6.03(0.918)			
	AW3	0.89	0.208	6.11(0.746)			
	AW4	0.784	0.385	6.00(0.941)			
	AW5	0.742	0.45	6.13(0.919)			
개인적특성	IND1	0.928	0.138	5.27(1.462)	0.935	0.934	0.782
	IND2	0.919	0.155	5.32(1.441)			
	IND3	0.869	0.245	4.82(1.626)			
	IND4	0.817	0.333	4.71(1.745)			
보안효과	EF1	0.912	0.168	6.01(1.362)	0.964	0.964	0.871
	EF2	0.945	0.107	6.00(1.414)			
	EF3	0.942	0.113	6.02(1.338)			
	EF4	0.934	0.127	5.99(1.358)			

4.3.2 측정모형의 판별타당성

판별타당성은 한 잠재요인이 실제로 다른 잠재요인과 얼마나 다른가에 관한 것으로, 판별타당성을 평가하는 방법에는 두 가지가 많이 이용된다. 첫째, Fornell & Larker[32]의 이론을 따라 하나의 구성개념 내의 평균분산추출 값이 다른 구성개념과 공유하는 분산보다 커야 한다는 것이다. 따라서 [표 4]에서 보듯이 각 구성개념들의 평균분산추출 값의 제곱근이 다른 구성개념들 간의 상관계수를 상회하여야 한다. 둘째, 요인과 교차 요인의 적재 값을 검증하는 것으로 이는 주성분요인분석과 유사한 방식으로 측정항목 수준에서 판별타당성을 검증하기 위한 방법이다. 즉 한 구성개념 내에서의 측정항목들은 자체 로딩한 값이 다른 구성개념과 크로스 로딩한 값보다 큰가를 측정하여 판별타당성을 다시 한 번 확인하였다.

〔표 4〕 변수간의 상관계수와 AVE의 제곱근 값

변수	추출된 평균분산 제곱근 값			
	1	2	3	4
1. 보안정책	(0.887)			
2. 보안의식	0.421	(0.799)		
3. 개인적 특성	0.346	0.215	(0.884)	
4. 보안효과	0.176	0.254	0.218	(0.933)

4.3.3 측정모형의 적합도 평가

아래의 [표 5]에서와 같이 측정모형의 적합도를 살펴보면 χ^2(p-값)은 269.426(0.00)이고, χ^2을 자유도로 나눈 비율이 2.384로 나타나 권장수준(≤3.00)을 만족시키는 것으로 나타났다. 그리고 GFI는 0.846, AGFI는 0.791으로 GFI가 권장수준보다 약간 낮게 나타났지만,

〔표 5〕 모형의 적합도 지수

구분	적합도지수	수용 기준	측정모형 분석결과	구조모형 분석결과
절대부합지수	χ^2/자유도	≤3.00	2.384	2.352
	χ^2 자유도 (df) p-value	≥0.05	269.426 113 0.000	270.446 115 0.000
	기초부합지수 (GFI)	≥0.90	0.846	0.845
	잔차평균자승이중근 (RMSR)	≤0.1	0.073	0.076
	근사원소평균자승잔차 (RMSEA)	≤0.08	0.091	0.090
증분부합지수	수정부합지수 (AGFI)	≥0.80	0.791	0.794
	표준부합지수 (NFI)	≥0.90	0.904	0.904
	관계부합지수 (RFI)	1.0근사	0.884	0.886
	증분부합지수 (IFI)	1.0근사	0.942	0.942
	비교부합지수 (CFI)	≥0.90	0.941	0.942
간명부합지수	간명기초부합지수 (PGFI)	≥0.60	0.625	0.635
	간명표준부합지수 (PNFI)	≥0.60	0.751	0.764

1.0에 근사할 경우 적합하다고 볼 수 있는 IFI는 0.942, CFI는 0.941등으로 수용기준에 부합하는 것으로 나타났다. 그 외에 PGFI는 0.625, PNFI는 0.751로 일반적으로 권고하는 수용기준인 0.6이상을 상회하는 것으로 나타나 대체적으로 측정모형의 적합도가 수용기준을 충족하는 것으로 평가하였다.

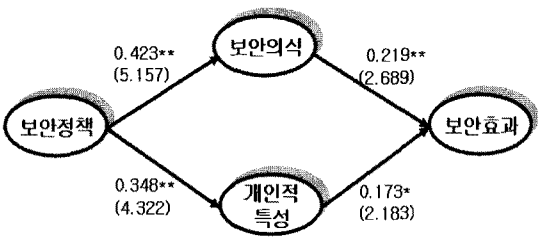
4.4 구조모형의 평가 및 가설검증

4.4.1 구조모형의 적합도 평가

본 연구모형에서 구성개념의 구조적 관계를 설명하고 있는 구조모형에 대한 적합도 지수는 아래의 [표 5]와 같다. 먼저 χ^2(p-값)은 270.446(0.00)이며, χ^2을 자유도로 나눈 비율이 2.352로 권장수준(≤3.00)에 부합하였다. 그러나 GFI는 0.845로 권장수준인 0.90보다 약간 낮은 것으로 나타났지만, AGFI는 0.794로 권장수준인 0.80에 근접하고 있으며 IFI는 0.942, CFI는 0.942, PGFI는 0.635, PNFI는 0.764 등 수용기준에 상회하는 것으로 나타나 구조모형이 연구개념들 사이의 관계를 설명하는데 적절한 것으로 판단하였다.

4.4.2 구조모형의 가설검증

본 연구에서 연구가설은 연구모형에서 구성개념 사이의 경로로 구성되어 있다. 구조모형의 분석결과에 따르면 각 경로의 추정치와 t-값은 아래의 [그림 2]와 같이 나타났으며, 모든 경로는 통계적으로 유의한 것으로 확인되었다.



〔그림 2〕 연구모형 검증결과

보안정책이 보안의식에 미치는 영향을 평가하기 위해 설정한 연구가설1(H1)은 경로계수가 0.423으로 나타났으며, t-값이 5.157로 유의수준 0.01에서 통계적으로 유의한 것으로 나타나 가설을 채택한다. 보안정책이 개인적 특성에 영향을 미친다는 연구가설2(H2)의 경우 경로계수가 0.348이며, t-값이 4.322이며, 유의수준 0.01에서 통계적으로 유의하게 나타나 가설이 채택되었다. 또한 보안의식이 보안효과에 영향을 미친다는 연구가설3(H3)은 경로계수가 0.219이며, t-값이 2.689로 유의수준 0.01에서 통계적으로 유의한 것으로 나타나 가설이 채택되었으며 개인적 특성은 보안효과에 영향을 미친다는 것으로 설정된 연구가설4(H4)도 경로계수가 0.173, t-값이 2.183으로 유의수준 0.05에서 가설이 채택되었다. 본 연구가설 검증결과의 요약은 아래의 [표 6]과 같다. 연구모형 검증결과 모든 경로는 통계적으로 유의한 것으로 확인되었다.

설정된 모형에 추가하여 개인적 특성이 보안의식에 영향을 미치는지, 역으로 보안의식이 개인적 특성에 영향을 미치는지, 보안정책이 보안효과에 직접적인 영향을 미치는지에 대한 분석을 수행하였다. 그 결과 개인적 특성이 보안의식에 미치는 영향의 경로계수가 0.43, t-값이 0.942로 나타났으며, 역으로 보안의식이 개인적

〔표 6〕 연구가설 검증결과 요약

연구가설	모형의 경로	경로계수	t-값	검정결과
[H1] 보안정책은 보안의식에 정(+)의 영향을 미친다.	보안정책 → 보안의식	0.423	5.157	채택
[H2] 보안정책은 개인적 특성에 정(+)의 영향을 미친다.	보안정책 → 개인적 특성	0.348	4.322	채택
[H3] 보안의식은 보안효과에 정(+)의 영향을 미친다.	보안의식 → 보안효과	0.219	2.689	채택
[H4] 개인적 특성은 보안효과에 정(+)의 영향을 미친다.	개인적 특성 → 보안효과	0.173	2.183	채택

특성에 미치는 영향의 경로계수가 0.149, t-값이 0.942로 나타나 통계적으로 유의하지 않았다. 또한 보안정책이 보안효과에 미치는 영향의 경로계수가 0.105, t-값이 0.354로 통계적으로 유의하지 않은 것으로 나타났다. 따라서 보안정책과 보안효과 사이에 보안의식과 개인적 특성이 완전매개변수의 역할을 하는 것을 확인하였다. 즉, 보안정책은 보안의식과 개인적 특성을 통하여 보안효과에 영향을 미친다는 것을 확인할 수 있었다.

4.4.3 분석결과 논의

본 연구의 분석결과에 따르면 정보시스템 사용자의 패스워드 사용이 보안효과에 영향을 미치는 요인으로 보안정책, 보안의식, 개인적 특성이 모두 통계적으로 유의한 영향을 미치는 것으로 나타났다. 이 연구결과는 우선 기업 내의 보안정책의 수용과 권장은 정보시스템 사용자의 보안의식과 개인적 특성에 긍정적인 영향을 미친다는 것을 보여준다. 정보보안을 위한 방안으로 패스워드 설정에 관한 기업의 보안정책은 정보시스템 사용자에게 정보보안 교육을 실시하고 패스워드 설정의 권장, 조합된 패스워드의 설정과 임시로 받은 패스워드는 새로운 패스워드로 변경할 것을 권장하였다. 이러한 보안정책의 실시는 정보시스템 사용자 보안의식의 향상을 가져다준다는 것이다. 또한 보안정책은 정보시스템 사용자가 보안에 대한 관심과 보안인지의 정도인 개인적 특성에 영향을 준다는 것이다. 그리고 정보시스템 사용자의 보안의식이 형성되어 있을 때 정보보안을 위한 보안효과를 가져오며, 정보시스템 이용과 성과에 영향을 주는 정보시스템 사용자의 개인적 특성도 보안효과에 영향을 준다는 것이다. 따라서 기업 내의 정보보안은 보안정책을 준수하고 이에 따른 개인적 특성과 보안의식 수준이 향상되었을 때 보안효과를 거둘 수 있을 것이다.

V. 결 론

오늘날 인터넷 정보량의 급증과 정보시스템 사용의 증가에 따라 개인 및 기업정보 유출에 의한 피해가 급격히 증가하고 있는 추세이다. 또한 급변하는 IT 운영환경에서 네트워크와 통신 인프라의 발전에 따른 보안취약점도 강조되고 있으며 개인정보유출과 보안사고 사례로 사회적 이슈가 커지고 있는 실정이다. 본 연구에서는 패스워드 사용의 보안효과에 미치는 요인을 보안정책, 보안의식, 개인적 특성이라고 연구모형을 제시하고 구조방정식을 통하여 요인간의 인과관계를 검증하였다. 모든 경로는 통계적으로 유의하게 나타났으며, 이는 조직 내의 보안정책의 권장으로부터의 사용자의 보안의식, 개인적 특성이 정보시스템 사용자의 보안효과에 긍정적인 영향을 미친다는 것을 검증할 수 있었다.

본 연구의 결과를 바탕으로 다음과 같은 시사점을 제시할 수 있다. 먼저, 정보시스템 보안효과를 위한 방안으로 조직 내의 보안정책의 권장은 중요하다는 점이다. 조직의 목표와 특성에 맞는 보안정책을 조직구성원들이 인지하고 있을 때, 정보유출피해를 최소화할 수 있는 보안효과를 가져다 줄 수 있을 것이다. 둘째, 정보유출 위험인지와 보안의 중요성을 인지한 상태의 보안의식이 보안효과를 가져다 줄 수 있다는 점이다. 이는 정보시스템 사용자에게 보안의식 수준 향상의 중요성을 인식시켜주며, 보안효과를 거둘 수 있게 할 것이다. 셋째, 개인적 특성인 정보보안의 사전지식은 보안효과를 가져다준다는 점이다. 따라서 정보시스템 사용자의 보안에 대한 관심도가 높으면, 개인적인 보안관련 지식의 습득의 기회가 많아질 것이며, 이러한 보안지식은 효율적인 보안효과를 기대할 수 있을 것이다.

본 연구의 한계점과 향후 연구과제에 대해서 살펴보면 다음과 같다. 첫째, 본 연구에서 측정하고자 하는 보안정책이 조직의 규모에 따라 상이한 성격을 가지고 있을 수 있다. 향후 연구에서는 조직의 특성에 따른 보안정책과 조직 구성원들 간의 보안의식을 비교·분석하는 연구가 이루어져야 할 것이다. 둘째, 정보보안을 중요시 여기는 집단과 일반적으로 정보보안의 중요성을 크게

인식하지 않는 일반 정보시스템 사용자들과 구분하지 않은 점을 들 수 있다. 향후 연구에서는 정보보안을 중요시 여기는 집단과 일반 정보시스템 사용자의 패스워드 선택이 보안효과에 미치는 영향의 차이점에 대한 비교 연구가 수행될 필요가 있다.

참고문헌

[1] http://www.boannews.com/media/view.asp?page=1&gpage=1&idx=7386&search=&find=&kind=0

[2] 권영옥, 김병도, "정보보안 사고와 사고방지 관련 투자가 기업가치에 미치는 영향," Information Systems Review, 9(1), pp. 105-120, 2007.

[3] Juang, W., "Efficient Password Authenticated Key Agreement Using Smart Cards," Computers & Security, Vol. 23, pp. 167-173, 2004.

[4] O'Gorman, L., A. Bagga, and J. Bentley, "Query-directed passwords," Computers & Security, Vol. 24, pp. 546-560, 2005.

[5] 박승배, 박설배, 강문설, "타인의 관찰에 의한 패스워드 노출로부터 안전한 패스워드 시스템," 정보처리학회논문지, 10C(2), pp. 141-144, 2003.

[6] 정해철, 김현수, "조직구성원의 정보보안 의식과 조직의 정보보안 수준과의 관계 연구," 정보기술과 데이터베이스저널, 7(2), pp.117-134, 2000.

[7] 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.

[8] 김종기, "정보시스템 보안의 효과성 모형에 관한 실증적 연구," 정보시스템연구, 7(2), pp. 91-108, 1998.

[9] 정보통신부, 2006 국가정보보호백서, 정보통신부, 2006.

[10] Zviran, M. and W. Haga, "Password Security: An Empirical Study," Journal of Management Information Systems, Vol. 15, No. 4, pp. 161-185, 1999.

[11] 정보통신부, 패스워드 선택 및 이용가이드, 정보통신부, 2008.

[12] Wiant, T. L., "Information Security Policy's Impact on Reporting Security Incidents," Computers & Security, Vol. 24, pp. 448-459, 2005.

[13] 김종기, 전진환, "컴퓨터 바이러스 통제를 위한 보안행위의도 모형," 정보화정책, 13(3), pp. 174-186, 2006.

[14] KISA, "2006년 정보보호 실태조사 당신의 정보보호 수준은?," 정보보호뉴스, 2월호, pp. 12-17, 2007.

[15] Post, G. V. and A. Kagan, "Evaluating Information Security Tradeoffs: Restricting Access Can Interfere With User Tasks," Computers & Security, Vol. 26, pp. 229-237, 2007.

[16] Ronald, C., C. Curtis, and J. Aaron, "Phishing for User Security Awareness," Computers & Security, Vol. 26, pp. 73-80, 2007.

[17] Lee, S. M., Y. R. Kim, and J. Lee, "An Empirical Study of the Relationships among End-User Information Systems Acceptance, Training, and Effectiveness," Journal of Management Information Systems, Vol. 12, No. 2, pp. 189-202, 1995.

[18] Baldwin, N. S. and R. E. Rice, "Information-Seeking Behavior of Securities Analysis: Individual Institutional Influences, Information Sources and Channels, and Outcomes," Journal of The American Society for Information Science, Vol. 48, No. 8, pp. 674-693, 1997.

[19] King, R. C. and W. Xia, "Media Appropriateness : Effects of Experience on Communication Media Choice," Decision Sciences, Vol. 28, No. 4, pp. 877-910, 1997.

[20] Albrechtsen, E., "A Qualitative Study of Users' View on Information Security," Computers & Security, Vol. 26, pp. 276-289, 2007.

[21] Roger, A. G., "Top 14 Security Tactics" Infoworld.com, pp. 16, 2006.

[22] Karyda, M., E. Kiountouzis, and S. KoKolakis, "Information System Security Policies: A Contextual Perspective," Computers & Security, Vol. 24, pp. 246-260, 2005.

[23] Doherty, N. F. and H. Fulford, "Aligning the

Information Security Policy with the Strategic Information Systems Plan," Computers & Security, Vol. 25, pp. 55-63, 2006.

[24] Stanton, J. M., K. R. Stam, P. Mastrangelo and J. Jolton, "Analysis of End User Security Behaviors," Computers & Security, Vol. 24, pp. 124-133, 2005.

[25] ISO/IEC, Guidelines for the Management of IT Security (GMITS), International Organization for Standardization/International Electrotechnical Commission, 2005.

[26] 임채호, "효과적인 정보보호인식제고 방안," 정보보호학회지, 16(2), pp. 30-36, 2006.

[27] 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.

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

[29] Drevin, L., H. A. Kruger, and T. Steyn, "Value-Focused Assessment of IGT Security Awareness in an Academic Environment," Computers & Security, Vol. 26, pp. 36-43, 2007.

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

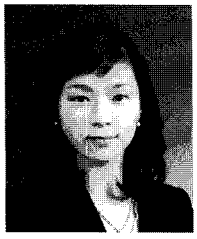
[31] 강병서, 조철호, SPSS와 AMOS 활용 연구조사 방법론, 무역경영사, 2005.

[32] Fornell, C. and F. L. Bookstein, "Two Structural Equation Models: LISREL and PLS Applied to Consumer Exit-Voice Theory," Journal of Marketing Research, Vol. 19, No. 4, pp. 440-452, 1982.

〈著者紹介〉

김 종 기 (Jongki Kim) 정회원

1987년 2월 : 부산대학교 경영학과 (경영학사)
1988년 12월 : Arkansas State University. MBA(경영학석사)
1992년 12월 : Mississippi State University. Ph.D in MIS(경영학박사)
1993년 3월~1999년 2월 : 국방정보체계연구소 선임연구원
1999년 3월~현재 : 부산대학교 경영학부 교수
<관심분야> 정보시스템 보안관리, 전자상거래 보안, 프로젝트 관리



강 다 연 (Dayeon Kang) 정회원

2006년 2월 : 한국해양대학교 경영학과(경영학사)
2008년 2월 : 부산대학교 일반대학원 경영학과(경영학석사)
2008년 3월~현재 : 부산대학교 일반대학원 경영학과 박사과정
<관심분야> 정보시스템 보안관리, 전자상거래 보안, 지식경영