Journal of Digital Contents Society Vol. 14 No. 2 Jun. 2013(pp. 179-189)
http://dx.doi.org/10.9728/dcs.2013.14.2.179

정보보안의식이 패스워드 보안행동에 미치는 영향에 관한 연구

하상원*, 김형중**

요 약

21세기가 되면서 컴퓨터 및 인터넷 등을 포함한 정보통신기술의 발전으로 다양한 기기에서 네트워크를 이용한 컴퓨팅 환경이 제공되어 지고 있다. 사이버 공간에서 사용자 인증방식은 텍스트 기반의 패스워드 인증방식을 사용하고 있다. 정보시스템의 비인가된 접근과 노출은 사용자, 공급자 모두에게 큰 피해를 입힐 수 있다. 이러한 인증방식은 기술적인 문제뿐만 아니라 사람들의 행동학적인 문제를 가지고 있다. 연구결과에 따르면 사용자들 대부분이 다양한 사이트를 이용하지만 사용하는 비밀번호개수는 그보다 훨씬 적었다. 또한 오랜 기간 한 가지 비밀번호를 사용하는 사용자가 많았으며 변경 시에도 기존의 비밀번호를 이용하여 최소한의 변경을 원하였다. 이에 정보보안의 차원에서 사람들의 전반적인 비밀번호 선택과 사용에 있어서 영향을 미치는 요인을 통계분석을 통해 알아보고자 한다.

키워드 : 사용자 인증방식, 통계적 분석, 정보시스템 사용자 행동 연구

The Effects of User's Security Awareness on Password Security Behavior

Sang-won Ha*, Hyoung-Joong Kim**

Abstract

With the rapid development of information technology in 21st century, networks are being used with various devices. Most human actions are processed through cyber space, and it is no longer separate from daily life; it has changed into one of the most important aspects of human life. Unfortunately, in cyber space, certification method has not only technical problems, but also ethological problems. Many users seemed to use the same password throughout several sites. And for a long period they refused to change it or made a small change from the earlier password. This research aims to discuss general factors of choosing and using passwords within information security through statistical analysis.

Keywords : User Authentication, Statistical analysis, User behavior

1. 서론

오늘날 정보통신기술의 급속한 발전에 따라 pc, 스마트폰 등 다양한 기기에서 네트워크를 이용한 컴퓨팅 환경이 보편화되고 있다. 이러한 환경을 기반으로 예전과 비교할 수 없을 정도로 정보양은 폭발적으로 증가하였을 뿐만 아니라, 기존의 오프라인 영역에서 행해지던 일상생활에서의 대부분의 활동이나 정보 교류는 물론이고 뱅킹, 증권거래, 등과 같은 업무도 사이버공간에

※ 교신저자(Corresponding Author):Hyoung Joong Kim
접수일:2013년 05월 13일, 수정일:2013년 06월 08일
완료일:2013년 06월 16일
* 고려대학교 정보보호대학원
** 고려대학교 정보보호대학원
Tel: +82-2-3290-4251 , Fax: +82-2-928-9109
email: hrecht@naver.com
▣ "이 논문은 2012년도 대한민국 정부(교육과학기술부)의 재원으로 시행하는 한국연구재단 국제협력사업의 지원으로 수행 된 연구결과임(과제번호: 2009-00678)."

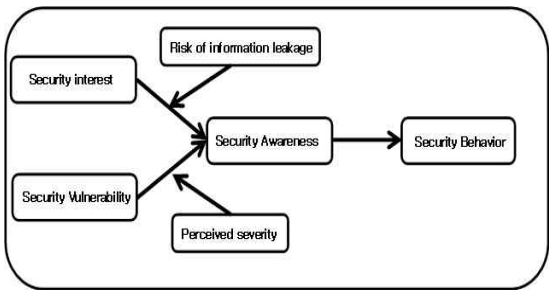
서 이루어지고 있다는 점에서 사이버 공간은 더 이상 별개의 영역이 아닌 중요한 생활 공간으로 자리 잡게 되었다[1]. 이러한 상황에서 2008년 옥션의 1800만명의 개인정보유출사고에 이어 2011년 사상 최대인 3500만명의 개인정보가 유출된 SK커뮤니케이션즈의 사건 등 최근 몇 년 새 국내외에서 크고 작은 개인정보유출사고가 일어나고 있다. 이러한 개인정보 유출은 당사자의 사생활 침해 및 그에 따른 정신적 피해뿐 아니라 금융 사기나 범죄 같은 2, 3차 피해를 일으킬 가능성이 다분하다[2]. 이러한 내·외부의 정보유출 위험에 대비하기 위해서는 적절한 기술과 보안시스템의 개발이 무엇보다 중요하다. 이러한 정보보안에 관련된 기술이 개발되고 있지만 사용자 인증방식은 아직까지도 알파벳이나 숫자 등을 이용한 패스워드 입력 방식에 의존하고 있다[3]. 이에 기존의 패스워드 입력 방식을 탈피한 새로운 그래픽 기반의 패스워드, 생체인식 기반의 패스워드들이 개발되어지고 있지만 아직은 그 한계점과 실현가능성이 낮은 상황이기 때문에 기존 패스워드 인증방식은 계속 사용되어질 것이다. 이러한 텍스트 기반의 패스워드 인증방식은 기술적인 문제뿐만 아니라 사람들의 행동학적인 문제를 가지고 있다. 2010년 동일한 IP에서 네이버 이용자들의 로그인 시도가 발생되었다. 이는 NHN 서버 해킹이 아닌 다른 곳에서 유출된 개인정보를 네이버에 대입해보는 방식으로 이루어졌다. 2012년 IT 보안업체인 ESET가 야후 서버에서 해킹당한 45만명의 계정을 분석한 결과 대다수의 사용자가 '123456', 'password', 'qwerty'와 같은 흔한 비밀번호를 사용하고 있었다. 대부분의 사용자가 흔한 비밀번호를 사용하고 이러한 비밀번호를 여러 사이트에서 동일하게 사용하고 있다[4]. 이러한 사실은 정보유출사고 등의 방지를 위해서는 정보보안기술시스템이나 제도의 개선과 함께 개인의 정보보안의식이 매우 중요하다는 점을 확인시켜주고 있다. 보안의식과 보안행동에 관련하여서는 기존 강다연(2008)의 연구에 따르면 보안정책의 수용과 권장은 사용자의 개인적 특성과 보안의식에 영향을 미치고 이것이 보안효과로 이어진다는 점을 검증해 주고 있다[5]. 또한 Post와 Kagan(2007)의 연구에 의하면 보안의식을 측정하기 위해서는 개인적 특성을 고려하였다[6]. 이러한 기존 연구에서 도출된 사용자의 보안의식과 행동에 관한 일반적 내용을 토대로 본 연구에서는 구체적으로 비밀번호의 설정 및 변경과 관련하여 정보보안행동으로 정의하고 정보보안의식에 영향을 주는 요인과의 상관관계를 고찰하고자 한다. 이를 위해 보안의식에 영향을 미치는 개인적 특성을 보안관심도와 보안취약성에 따른 인식으로 세분화하고 이 요인들에 조절효과를 하는 변인인 정보유출위험과 인지된 심각성을 중심으로 연구모형을 설계하고 이에 따라 설정한 보안의식과 이러한 보안의식이 정보보안행동에 주는 영향을 실증분석하였다. 본 논문은 2장 연구내용에서는 연구모형에 대한 설명과 각각의 변인들에 대한 조작적 정의와 설문문항의 타당성에 대하여 서술을 한 후 연구문제와 가설을 설정하였다. 3장에서는 실증분석의 방법과 그 분석결과에 대해 서술하였다. 4장에서는 본 논문의 결과에 대한 결론을 내렸다.

2. 연구내용

2.1 연구모형 및 설계

본 연구에서는 사용자의 정보보안 의식에 영향을 미치는 요인들에 대해 실증적으로 규명하고 정보보안 의식이 정보보안 행동에 미치는 영향을 연구하기 위해 아래그림과 같이 연구모형을 설정하였다. 우선 보안 관심도, 보안 취약성이 정보보안 의식에 영향을 미치며 정보유출위험, 인지된 심각성이 조절작용을 한다. 이러한 정보보안의식이 정보보안 행동에 영향을 미칠 것이라는 연구 모형을 설정하였으며, (그림 1)은 다음과 같다.

(그림 1) 연구모형



(Figure 1) Research Model

2.2 조사도구

2.2.1 보안관심도

본 연구에서 보안 관심도는 정보시스템 사용자가 시스템 이용에 영향을 받는 개인정보보호와 관련된 개인적 특성에 따른 관심도로 정의하였다. McCoy와 Fowler(2004)는 사용자가 보안의 핵심 요소라는 전제하에 Security awareness 프로그램을 사용하여 사용자의 보안 관심도를 높이고 이것이 보안행동인식에 긍정적인 영향을 미치는 요인으로 보았다[7]. 보안에 대한 경각심을 고취시키기 위해서는 보안에 대한 관심도를 높여야 한다고 주장하였다. 장명희(2012)의 연구에 따르면 항만기업 종사자들의 정보보안관심도가 정보보안 인식에 긍정적인 영향을 미친다는 가설을 도출하였다[8]. 본 연구에서는 보안관심도를 개인의 보안 관심도를 측정할 수 있는 4가지 문항으로 구성하였다. 4가지 문항은 개인의 컴퓨터 보안에 대한 지식, 보안 관련 이슈에 대한 관심도, 보안 권고사항의 인식정도, 아이디-패스워드의 관리로 이루어 졌다. 이 문항들의 신뢰성을 평가하기 위해 Cronbach's Alpha Coefficient를 사용하였다. 문항의 일관성을 타나내는 계수로 신뢰성을 평가하는 척도인 알파계수는 0~1의 값을 갖고, 값이 높을 수록 신뢰도가 높다. 0.7이상이면 설문문항이 신뢰성을 갖는다고 볼 수 있다. 수식은 다음과 같다.

$$\text{Cronbach's Alpah } \alpha = \frac{1}{k-1}\left(1 - \frac{\sum_{i=1}^{k}\sigma_i^2}{\sigma_y^2}\right)$$

(k:항목수, σ_y^2: 총분산, σ_i^2:각항목의 분산)

Likert 5점측도를 사용한 4문항에 대한 신뢰도 계수(Cronbach' alpha)는 .823로 높은 신뢰도를 보였다.

2.2.2 보안 취약성

취약성이란 정보시스템에 손해를 끼치는 원인이 될 수 있는 조직, 절차, 인력관리, 행정, 하드웨어와 소프트웨어의 약점을 뜻한다. 이러한 약점을 확인하고 분류하여 위협을 감소시키는 것이 취약성을 분석하는 목적이다[5]. 본 연구에서는 정보시스템 사용자에 손해를 줄 수 있는 패스워드의 노출위험으로 정의하였다. 2007년 KISA의 패스워드 선택 및 이용가이드를 참고하여 사용자들이 인지하는 패스워드로 인한 취약성을 측정하였다. 보안의 취약성은 패스워드 변경유무에 따른 취약성 인식, 여러 사이트에 중복된 패스워드의 사용에 대한 인식, 패스워드의 길이에 따른 취약성에 대한 인식, 민감한 정보를 사용해 만든 패스워드의 취약성에 대한 인식을 측정하는 4문항으로 구성되었다. 4문항에 대한 신뢰도 계수(Cronbach' alpha)는 .814로 높은 신뢰도를 보였다.

2.2.3 정보유출위험

위협이란 개인정보의 기밀성, 무결성, 가용성을 위태롭게 할 수 있는 상황으로[12], 본 연구에서는 개인정보 노출로 인해 예상되는 위험에 대한 측정치로 정의하였다. 정보유출위험을 측정하기 위하여 측정하기 위해서 ISO/IEC(2005)와 정보통신부(2006)가 제시한 패스워드 노출 예방을 위한 정기적 패스워드 변경에 관한 사항을 기반으로, 이윤선(2009)의 연구에서 쓰인 도구를 참고하여 사용하였다[9][10][11]. 사용자의 정보유출위험을 측정하는 문항들은 정보유출로 인해 개인정보 침해를 가져올 가능성, 신상정보가 공개되어 악용될 수 있는 위험, 정보유출위험으로 인한 금전적인 손해의 가능성, 정보유출로 인한 스팸메일 발송으로 인한 위험을 측정하는 4가지 문항으로 구성되었다. 4문항에 대한 신뢰도 계수(Cronbach' alpha)가 .877으로 나타나 높은 신뢰도가 확보되었음을 알 수 있다.

2.2.4 인지된 심각성

인지된 심각성은 사용자가 인지한 위험의 심각성이라고 정의를 하였다. 이기혁(2008)의 연구에 따르면 위험의 심각도는 서비스 환경이 잠재적으로 가지고 있는 취약성이 위협에 의해 현실화 되었을 때, 나타날 수 있는 잠재 위험의 정도를 말한다[12]. 인지된 심각성을 측정하기 위해 사용자가 생각하는 개인정보유출로 인한 피해와 피해의 확산의 심각성에 대한 2문항이 사용되었다.

2.2.5 정보보안 의식 측정

정보보안 의식 측정을 위해 Drevin 등(2007)의 개인정보 보안의식에 대한 연구를 바탕으로 김종기와 강다연(2008)의 연구에서 쓰인 개인정보 보안 의식 측정 도구를 수정 및 보완하여 사용하였다[13][14]. 본 척도는 정보보안을 위한 지침과 규정, 개인정보 노출의 대응조치, 정보보안 기본소양, 보안지침의 실천, 정기적 패스워드 변

경, 패스워드의 관리와 관련된 총 6개의 문항으로 구성 되었다. 정보보안 의식 측정을 위한 6문항에 대한 신뢰도 계수(Cronbach' alpha)가 .780로 나타나 신뢰도가 확보되었음을 알 수 있다.

2.2.6 정보보안 행동

본 연구에서 주요하게 알아보고자 하는 종속변인으로 개인정보를 보호하기 위해서 개인이 실제 실시하는 패스워드 행동으로 정의하였다. 또한 정보보안 행동은 비밀번호 변경 주기, 비밀번호 유추 가능성, 비밀번호 안전성, 중복 비밀번호 개수의 4가지 하위 항목으로 구성하였다. 우선, 비밀 번호 변경 주기 하위 항목은 비밀번호 변경 주기와 비밀번호 변경 공지 무시 정도의 2문항으로 구성되었으며, 비밀번호 유추 가능성은, ID와의 유사성, 신상정보 이용정도, 유추가능성의 3문항으로 구성되었다. 또한 안전성의 경우, 비밀번호의 길이, 연속된 문자열 사용 정도, 반복된 패턴 사용 정도, 영문과 숫자 혼합 정도의 4문항으로 구성되었으며, 중복 비밀번호 개수는 ID와 비밀번호 쌍 개수, 새로운 비밀번호 생성 시 기존 비밀번호의 이용의 2문항으로 구성되었다. 모든 문항은 Likert 5점 척도로 응답하도록 하였다. 신뢰도 계수(Cronbach' alpha)는 .515으로 낮은 수준인 것으로 나타났지만 이는 보안행동이 비교적 독립된 차원들로 구성되어 있기 때문이다.

2.3 연구 문제와 가설

2.3.1 보안관심도와 정보보안 의식

연구가설1(H1)은 개인의 보안관심도에 따라 정보보안 의식에 어떠한 영향을 미치는 인과관계에 대한 가설이다.

정보시스템 사용자의 사회적 영향과의 관계는 규범적 영향 보다는 정보적 양향에 국한되어 있는 경우가 많다[15]. 정보적 영향이란 다른 사람으로부터 얻은 정보가 자신이 가지고 있는 믿음구조에 영향을 미치는 것이다. 따라서 주위 사람, 신문, 잡지, TV, 인터넷으로부터 얻은 정보로 형성된 보안관심도는 개인별로 다르게 나타날 것이고 이러한 관심도가 정보보안 의식에 긍정적인 영향을 미칠 것이라는 연구 가설을 도출하였다.

H1: 보안관심도가 정보보안 의식에 정(+)적인 영향을 미칠 것이다.

2.3.2 보안취약성과 정보보안 의식

연구가설2(H2)는 사용자가 인지한 보안취약성이 사용자의 정보보안 의식에 어떠한 영향을 미치는 인과관계에 대한 가설이다. 장익진(2010)의 연구에 따르면 취약성은 "개인정보 유출 위협이 나에게 얼마나 심각한 해를 입힐 것인가"에 대한 지각이며 제시된 위험이 자신과 무관하거나 사소하다고 판단될 경우에는 정보보안 의식에 아무런 영향을 주지 않을 것이다[16]. 하지만 취약성을 인지하고 그로인해 심각한 해를 입을 수 있다고 믿는다면 이를 막기 위해 정보보안 의식을 높이는 동기부여가 될 것이다. 따라서 이러한 보안취약성이 정보보안 의식에 긍정적인 영향을 미칠 것이라는 가설을 도출하였다.

H2: 보안취약성은 정보보안 의식에 정(+)의 영향을 미칠 것이다.

2.3.3 정보유출위험의 조절 효과

연구가설3(H3)은 보안관심도와 정보보안의식의 관계에서 정보유출위험의 조절효과에 대한 가설이다. 정보유출위험으로 인해 정보시스템 이용자가 입을 수 있는 해는 다양한 형태가 될 수 있기 때문에 이런 위험으로 인한 파급 효과의 종류를 규명하는 일이 매우 중요하다[15][17]. 본 연구에서는 정보유출위험이 있을 경우 보안관심도와 정보보안의식사이의 인과관계에 조절효과가 있을 것이라는 가설을 도출하였다.

H3: 정보유출위험이 보안관심도와 정보보안의식사이에서 조절효과가 있을 것이다.

2.3.4 인지된 심각성의 조절효과

연구가설4(H4)는 보안취약성과 정보보안의식의 관계에서 인지된 심각성의 조절효과에 대한 가설이다. 취약성이 위협에 의하여 현실화되어 심각성의 정도가 늘어났을 경우 정보시스템 사용자의 보안취약성과 정보보안의식사이의 인과관계에서 인지된 심각성이 조절효과가 있을 것이라는 가설을 도출하였다.

H4: 인지된 심각성이 보안취약성과 정보보안의식사이에서 조절효과가 있을 것이다.

2.3.5 정보보안의식과 정보보안행동

연구가설5(H5)는 정보보안의식이 정보보안 행동에 미치는 인과관계에 대한 가설이다. 정보시스템 사용자가 보안관심도, 인지한 보안취약성등 여러 가지 요인으로 인해 생성된 정보보안의식

이 패스워드 보안행동으로 이어지는지에 대한 가설이다. 정보보안행동은 패스워드 관련보안행동으로 비밀번호 변경 주기, 비밀번호 유추 가능성, 비밀번호 안전성, 중복 비밀번호 개수로 4가지로 이루어져있다. 정보보안의식이 높은 사용자일수록 정보보안행동에 적극적일 것이라고 보고 이러한 가설을 도출하였다.

H5: 정보보안의식이 정보보안 행동에 정(+)적인 영향을 미칠 것이다.

2.3.6 정보보안의식의 매개효과 분석

연구가설6(H6)과 연구가설7(H7)은 보안관심도와 보안 취약성이 정보보안의식을 통하여 보안행동에 영향을 줄 것이라는 가설이다.

H6: 보안관심도가 정보보안의식을 통하여 보안행동에 영향을 줄 것이다.

H7: 보안취약성이 정보보안의식을 통하여 보안행동에 영향을 줄 것이다.

2.4 요인분석

변인들은 주축요인분해법으로 분해하고 사각회전을 하였다. 그 결과 보안행동을 제외한 모든 변인은 하나의 요인만이 존재하였다. 보안행동은 Eigenvalue 값이 1 이상이 4개이므로 4개의 요인이 도출되었다. 이는 본 연구에서 보안행동을 개념화할 때 네 개의 차원으로 나눈 것과 일치하는 것이다. 그러므로 모든 변인의 문항들은 조작적 정의에 맞게 잘 작성되었다. 각 변인의 문항들이 다른 변인들의 문항들과 구별되는지 확인해보기 위하여 즉, 변별타당도를 검토하기 위하여 다른 변인의 문항들과 함께 요인분석을 하였다. 그 결과 동일 변인에 속한 문항들끼리 명확히 묶인 것을 알 수 있었다. 그러므로 각 변인을 측정하는 문항들간에는 명확한 변별타당도가 있음을 알 수 있었다.

3. 실증분석

3.1 자료수집

본 연구에서는 정보보안의식에 영향을 미치는 요인들과 이러한 정보보안의식이 패스워드 관련한 개인의 행동으로 정의된 정보보안행동에 영향을 미치는지 실증적으로 검정하기 위하여 표본집단으로 대학교내에서 학업을 진행 중인 학생들을 선택하였다. 그 이유로는 학교 내의 모든 행정, 과제 업무를 위한 정보시스템을 사용하고 있으며, 사이버공간상에서의 활동이 어느 집단보다도 활발하다고 생각했기 때문이다.

본 연구는 H1, H2, H5의 가설을 검증하기 위하여 회귀분석을 실시하였으며, H3, H4 조절효과(moderating effect)의 가설을 검증하기 위하여 위계적 회귀분석(hierarchical regression analysis)을 실시하였다. 또한 Cohen(1988)의 공식을 사용하여 그 유의미성 정도를 알아보았다[18]. H6, H7의 매개효과(mediating effect)의 가설을 검증하기 위하여 Baron과 Kenny(1986)이 제시한 방식에 따라 3단계로 검증을 하였다[19]. 분석도구로는 SPSS 12.0을 사용하여 수집된 데이터를 실증적으로 분석하였다.

3.2 표본의 특징

표본은 컴퓨터 사용시간과 익숙도가 높은 대학생, 대학원생을 대상으로 조사하였다. 표본의 일반적 특성을 분석하기 위하여 응답자의 성별, 연령, 직업, 컴퓨터 사용시간, 하루 컴퓨터 사용시간, 주로 사용하는 포털 사이트 개수, 주로 사용하는 패스워드 개수에 관한 빈도 분석을 실시하였다. 성별은 남성이 55명(51.9%), 여성이 51명(48.1%)으로 남성의 비율이 더 높았다. 연령에서는 10~19세가 6명(5.7%), 20~29세가 85명(80.2%), 30~39세가 15명(14.2%)로 20~29세 응답자가 가장 많은 것으로 나타났다. 응답자의 직업은 학생이 77명(72.6%), 사무직이 12명(11.3%), 생산직 0명(0%), IT관련 직종이 8명(7.5%), 기타 7명(6.6%)으로 나타나 학생이 가장 많았으며, 응답자의 컴퓨터 사용 기간에서는 1년 이하 1명(0.9%), 1~5년 3명(2.8%), 6년~10년이 22명(20.8%), 11년~15년 48명(45.3%), 16년~20년 26명(24.5%), 21년 이상 6명(5.7%)으로 11년~15년의 응답자가 가장 많은 것으로 나타났다. 하루 컴퓨터 사용시간에서는 1시간 미만이 15명(14.2%), 1~3시간이 46명(43.4%), 4~6시간이 18명(17.0%), 7~9시간이 10명(9.4%), 10시간 이상이 17명(16%)으로 1~3시간의 응답자가 가장 많은 것으로 나타났다. 응답자가 주로 사용하는 포털 사이트 개수는 1개가 4명(3.8%), 2개가 33명(31.1%), 3~4개가 53명(50.0%), 5~6개가 11명(10.4%), 7개 이상이 5명(4.7%)으로 3~4개 응답

자가 가장 많았다. 주로 사용하는 패스워드 개수는 3~4개 응답자가 51명(48.1%)으로 가장 많은 것으로 나타났고, 그 다음으로 2개가 36명(34.0%), 7개 이상이 9명(8.5%), 5~6개가 6명(5.7%), 1개가 4명(3.8%) 순으로 나타났다.

3.3 가설검증

H1) 보안관심도와 정보보안의식

보안관심도가 정보보안의식에 미치는 영향을 알아보기 위해 보안관심도를 독립변수로 설정하고, 정보보안의식을 종속변수로 설정한 회귀분석을 실시하였다. 분석 결과, 회귀모형의 설명력을 나타내는 R2의 값이 .177로 보안관심도가 정보보안의식에 미치는 영향에 대한 설명력(R2)이 17.7%라는 것을 알 수 있었다. 또한 자유도를 반영한 수정된 R2은 .169로 나타났다. 보안관심도가 정보보안의식을 설명하는 이 회귀모형은 통계적으로 유의하였으며 보안관심도가 정보보안의식에 미치는 영향력(β)은 .421으로 이 영향력은 통계적으로 유의하였다(t=4.732, p<.001). 이 결과는 정보보안의식에 미치는 보안관심도의 영향이 정(+)의 영향임을 시사하며, 따라서 가설 H1은 검증되었다. 이상의 결과는 <표 1>에 요약제시 되었다.

<표 1> 보안관심도와 정보보안의식의 회귀분석표

Model	Unstandardized Coefficients		Beta	t	sig
	B	Std.Error			
Constant	18.921	.943		20.059	.000
Interest	.406	.086	.421	4.732	.000
a. Dependent Variable: Awareness					

<Table 1> Coefficients table of Security interest & Security Awareness

H2) 보안취약성과 정보보안의식

보안취약성이 정보보안의식에 미치는 영향을 알아보기 위해 보안취약성을 독립변수로 설정하고, 정보보안의식을 종속변수로 설정한 회귀분석을 실시하였다. 분석 결과, 회귀모형의 설명력을 나타내는 R2의 값이 .224로 보안취약성이 정보보안의식에 미치는 영향에 대한 설명력(R2)이 22.4%라는 것을 알 수 있었다. 또한 자유도를 반영한 수정된 R2은 .216로 나타났다. 보안취약성이 정보보안의식을 설명하는 이 회귀모형은 통계적으로 유의하였으며 보안취약성이 정보보안의식에 미치는 영향력(β)은 .474으로 이 영향력은 통계적으로 유의하였다(t=5.476, p<.001). 이 결과는 정보보안의식에 미치는 보안취약성의 영향이 정(+)의 영향임을 시사하며, 따라서 가설 H2은 검증되었다. 이상의 결과는 <표 2>에 요약제시 되었다.

<표2> 보안 취약성과 정보보안의식의 회귀분석표

Model	Unstandardized Coefficients		Beta	t	sig
	B	Std.Error			
Constant	13.942	1.708		8.162	.000
Vulnerability	.574	.105	.474	5.476	.000
a. Dependent Variable: Awareness					

<Table 2> Coefficients table of Security Vulnerability & Security Awareness

H3) 정보유출위험의 조절 효과

정보보안의식 수준에 영향을 미치는 보안관심도의 효과를 정보유출위험이 조절할 것(moderating effect)이라는 가설을 검증하기 위하여 위계적 회귀분석(hierarchical regression analysis)을 실시하였다. 1단계에서 독립변인인 보안관심도와 조절변인인 정보유출위험, 2단계에서는 다중공선성문제를 해결하기 위해 독립변인과 조절변인의 센터링 값을 곱한 상호작용항을 투입하여 단계별로 설명량이 유의하게 증가하는지 살펴보았다. <표 3>에서 제시된 바와 같이 정보보안의식과 보안관심도의 관계에서 정보유출위험의 조절효과가 확인되었다. 2단계의 정보유출위험과 보안관심도의 상호작용(Beta=.173, p<.05)과 증분설명량($\Delta R^2 = .030, p < .05$) 이 모두 유의하였다. Cohen(1988)의 공식을 사용하여 계산한 조절효과의 유의미성 정도인 f^2은 .038으로서 Cohen의 임계치(.02)보다 커서 조절효과가 있는 것으로 결론지었다[18]. 따라서 가설 H3는 검증되었다. 이상의 결과는 <표 3>에 요약제시 되었다.

<표 3> 정보유출위험의 조절효과분석표

Model	Unstandardized Coefficients		Beta	t	sig
	B	Std.Error			
Constant	23.117	.285		81.147	.000
cInterest	.368	.085	.382	4.314	.000
cRisk	.287	.121	.210	2.373	.020
Constant	.23.019	.285		80.761	.000
cInterest	.354	.084	.367	4.194	.000
cRisk	.313	.120	.229	2.608	.010
cInterest xcRisk	.061	.031	.173	2.003	.048

a. Dependent Variable: Awareness

<Table 3> Coefficients table to verify moderating effect (Risk of information leakage)

H4) 인지된 심각성의 조절효과

정보보안의식 수준에 영향을 미치는 보안취약성의 효과를 인지된 심각성이 조절할 것(moderating effect)이라는 가설을 검증하기 위하여 위계적 회귀분석(hierarchical regression analysis)을 실시하였다. 1단계에서 독립변인인 보안취약성와 조절변인인 인지된 심각성, 2단계에서는 다중공선성문제를 해결하기 위해 독립변인과 조절변인의 센터링 값을 곱한 상호작용항을 투입하여 단계별로 설명량이 유의하게 증가하는지 살펴보았다. <표 4>에서 제시된 바와 같이 정보보안의식과 보안취약성의 관계에서 정보유출위험의 조절효과가 확인되지 못하였다. 2단계의 인지된심각성과 보안취약성의 상호작용(Beta=.156, p>.05)과 증분설명량($\Delta R^2 = .023, p > .05$)이 모두 유의하지 않았다. 하지만 Cohen(1988)의 공식을 사용하여 계산한 조절효과의 유의미성 정도인 f^2은 .030으로서 Cohen의 임계치(.02)보다 커서 조절효과가 있는 것으로 결론지었다[18]. 그러므로 유의확률이 .078로 유의수준 .05보다 약간 크고 Cohen의 f^2은 최소 유의미성을 상회함으로 조절효과의 가능성이 있음을 보여주었다. 따라서 가설 H4는 검증되었다. 이상의 결과는 <표 4>에 요약제시 되었다.

<표 4> 인지된 심각성의 조절효과분석표

Model	Unstandardized Coefficients		Beta	t	sig
	B	Std.Error			
Constant	22.954	.283		81.007	.000
cVulnerability	.534	.108	.440	4.922	.000
cSeverity	.311	.226	.123	1.378	.171
Constant	22.835	.288		79.210	.000
cVulnerabilty	.491	.110	.404	4.464	.000
cSeverity	.298	.223	.118	1.335	.185
cVulnerability xcSeverity	.136	.076	.156	1.783	.078

a. Dependent Variable: Awareness

<Table 4> Coefficients table to verify moderating effect(Perceived severity)

H5) 정보보안의식과 정보보안행동

정보보안의식이 정보보안행동에 미치는 영향을 알아보기 위해 정보보안의식을 독립변수로 설정하고, 정보보안행동을 종속변수로 설정한 회귀분석을 실시하였다. 분석 결과, 회귀모형의 설명력을 나타내는 R2의 값이 .051로 정보보안 의식이 정보보안행동에 미치는 영향에 대한 설명력(R2)이 5.1%라는 것을 알 수 있었다. 또한 자유도를 반영한 수정된 R2은 .041로 나타났다. 보안취약성이 정보보안의식을 설명하는 이 회귀모형은 통계적으로 유의하였으며 보안취약성이 정보보안의식에 미치는 영향력(β)은 .225으로 이 영향력은 통계적으로 유의하였다(t=2.355, p<.05). 이 결과는 정보보안행동에 미치는 정보보안의식의 영향이 정(+)의 영향임을 시사하며, 따라서 가설 H5은 검증되었다. 이상의 결과는 <표 5>에 요약제시 되었다.

<표 5> 정보보안의식과 정보보안행동 회귀분석표

Model	Unstandardized Coefficients		Beta	t	sig
	B	Std.Error			
Constant	22.076	2.569		8.593	.000
Awareness	.259	.110	.225	2.355	.020

a. Dependent Variable: Behavior

<Table 5> Coefficients table of Security Awareness & Security Behavior

H6) 보안행동과 보안관심도간 정보보안의식의 매개효과분석

보안행동 수준에 영향을 미치는 보안관심도와 보안관심도의 효과를 정보보안의식의 정도가 매개할 것(mediating effect)이라는 가설은 Baron과 Kenny(1986)가 제안한 방식에 따라 3단계로 검증하였다[19]. 1단계에서는 보안행동수준에 대한 보안관심도의 총효과를 알아본 것으로 보안행동수준과 보안관심도간의 정적 관계는 유의하였다.($\beta = .259, p < .01$). 2단계에서는 보안관심도와 정보보안의식간의 관계가 유의하였다.($\beta = .421, p < .001$). 3단계에서는 보안행동을 예측하기 위하여 정보보안의식과 보안관심도를 동시에 투입하였다. 정보보안의식은 정보보안행동과 유의한 관계를 나타내지 않았고 ($\beta = .141, p > .05$) 보안관심도와도 유의한 관계를 보이지 않았다.($\beta = .199, p > .05$) 그러므로 정보보안의식이 보안관심도와 보안행동사이를 매개하지 않는 것으로 나타났다. 이상의 결과는 <표 6>에 요약제시 되었다.

<표 6> 정보보안행동과 보안관심도간 정보보안의식의 매개효과분석표

Model	Unstandardized Coefficients		Beta	t	sig
	B	Std.Error			
Constant	21.998	2.537		8.671	.000
Interest	.221	.115	.199	1.916	.058
Awareness	.259	.120	.141	1.356	.178
a. Dependent Variable: Behavior					

<Table 6> Coefficients table to verify mediating effect(Security Awareness: Security Interest & Security Behavior)

H7) 보안행동과 보안취약성간 정보보안의식의 매개효과분석

정보보안의식이 보안취약성과 정보보안행동과의 관계에서 매개효과를 갖는지에 대해서도 3단계검증을 하였다[19]. 1 단계에서는 보안행동수준에 대한 보안취약성의 총효과를 알아본 것으로서 정보보안행동수준과 보안취약성간의 정적 관계는 유의하였다.($\beta = .173, p < .05$). 2 단계에서는 보안취약성과 정보보안의식간의 관계가 유의하였다.($\beta = .173, p < .05$). 3 단계에서는 정보보안행동을 예측하기 위하여 정보보안의식과 보안취약성을 동시에 투입하였다. 정보보안의식은 보안행동과 유의한 관계를 나타내지 않았고($\beta = .152, p > .05$) 보안취약성도 유의한 관계를 보이지 않았다.($\beta = .155, p > .05$) 따라서 정보보안의식이 보안취약성과 정보보안행동사이를 매개하지 않는 것으로 나타났다. 이상의 결과는 <표 7>에 요약제시 되었다.

<표 7> 보안행동과 보안취약성간 정보보안의식의 매개효과분석표

Model	Unstandardized Coefficients		Beta	t	sig
	B	Std.Error			
Constant	20.555	2.767		7.429	.000
Vulnerabilty	.216	.151	.155	1.436	.154
Awareness	.174	.124	.152	1.406	.163
a. Dependent Variable: Behavior					

<Table 7> Coefficients table to verify mediating effect(Security Awareness: Security Vulnerability & Security Behavior)

3.4 분석결과 논의

본 연구에서는 정보시스템 사용자의 정보보안의식에 영향을 미치는 요인으로 보안에 '얼마나 관심을 가지고 있는 가' 하는 보안관심도와 보안의 취약성에 대해 '얼마나 인지하고 있는 가'를 보안취약성으로 설정하였다. 보안관심도와 보안취약성은 정보보안의식에 유의한 설명력을 가지는 것으로 나타났다. 강다연(2008)의 연구에서는 정보보안의식이 정보유출위험에 영향을 미치는 것으로 나타났다[5]. 하지만 본 연구에서는 정보유출위험을 보안관심도와 정보보안의식에서 조절효과를 나타내는 변인으로 보았고 유의한 결과가 나왔다. 이는 보안의 관심도에 따라 정보보안의식이 높아지고 정보유출위험의 인지정도에 따라 정보보안의식에 영향을 미치는 정도가 다른 것으로 판단하였다. 또한 사람들이 보안의 취약성 인지에 따라 정보보안의식에 영향을 미치고 인지하는 심각성정도에 의하여 정보보안의식에 영향 주는 정도가 다르다는 결과를 도출해냈다. 또한 이러한 정보보안의식이 패스워드설정과

관련된 정보보안행동에 정적인 영향을 미친다는 가설도 채택되었다. 정보시스템 사용자의 보안관심도와 보안의 취약성에 대해 인지할 경우, 개인의 정보보안의식은 높아질 것이며 이러한 정보보안의식은 정보보안효과를 증진시키는 효과를 기대할 수 있을 것이다.

4. 결론

사이버 공간이 제2의 생활공간이 되어감에 따라 예전과 비교할 수 없을 정도로 정보양은 폭발적으로 증가되고 있다. 이러한 상황에서 민감한 개인정보들이 해킹, 바이러스로 인해 유출되고 제2,3의 범죄로 이어지면서 정보보안의 필요성이 점차 커지고 있다. 디지털의 특성은 아날로그 콘텐츠에서 경험했던 것 이상의 상호작용을 사용자에게 제공한다[24]. 이러한 디지털 콘텐츠의 특성에 의하여 취약한 패스워드는 도둑에게 제대로 닫히지 않은 현관문을 공개하는 것과 같다[22]. 디지털환경에서 텍스트 기반의 패스워드는 사용자인증이나 기업 내부 컴퓨팅 시스템에서도 필수적이다. 이러한 텍스트 기반의 패스워드를 변화시키기 위해 지문, 동체인식과 같은 사람의 생물학적 특성을 이용하는 방법도 개발 중이지만 아직 실효성이 낮은 상황이다[20]. 정보시스템의 사용자 인증을 위한 패스워드 관리는 자신의 중요한 개인정보를 보호할 수 있는 가장 쉬운 방법이면서도 기초적인 방법이다[22]. 하지만 사용자 대다수가 여러 사이트에 가입을 하지만 비밀번호는 자신의 기본적으로 사용하는 패스워드나 손쉽게 기억이 가능한 패스워드를 여러 곳에 사용한다. 이와 같은 이유로 사이트 한곳만 개인정보가 유출되게 되더라도 domino처럼 다른 사이트나 시스템의 개인정보 역시 유출되게 된다[23]. 기업이나 정보시스템관리자의 패스워드관리도 중요하지만 사용자들의 정보보안행동도 필수적이다. 이러한 보안행동을 증진시킬 수 있는 방법에 대해 알아보고 사용자의 정보보안의식을 높여 이러한 Human vulnerability를 줄여야 할 것이다[21]. 본 연구에서는 통계적 방법론을 기반으로 사용자의 패스워드 선택이 어떠한지 이러한 보안행동을 강화시키려면 정보보안의식이 필요하고 이러한 정보보안의식수준을 높이기위해서는 보안관심도, 보안의 취약성에 대해 아는 것이 중요하다는 것을 확인할 수 있었다. 즉, 정보시스템 사용자의 정보보안의식이 패스워드 관리에 통계적으로 유의한 영향을 미치며 이러한 사용자의 정보보안의식을 높여 정보보안효과를 높여야 할 것이다.

본 연구의 한계점과 향후 연구과제에 대해 살펴보자면, 첫째, 본 연구에서 측정한 보안관심도와 보안 취약성은 연령, 직종, 교육에 따라 상이한 성격을 가지고 있을 수 있다. 향후 연구에서는 정보보안교육 유, 무 등을 비교 분석하는 연구가 이루어 져야 할 것이다. 둘째, 이러한 정보보안행동이 어떠한 보안효과를 나타내는지를 규명하지 않은 점을 들 수 있다. 향후 연구에서는 정보보안행동이 정보보안효과에 어떠한 영향을 미치는 지, 패스워드관련 보안행동을 잘 실천하는 집단과 그렇지 않은 집단의 정보보안효과에 대한 비교 연구가 수행될 필요가 있다.

References

[1] T. Jung, "Cyber Attack & Security Technology, HONGRUNG PUBLISHING COMPANY, 2009

[2] S. Kim, M. S, "The Effects of the Perception of an Online Risk and Prior Knowledge on Public's Communication Behavior", KOREAN ASSOCIATION FOR ADVERTISING AND PUBLIC RELATIONS, Vol. 13, pp. 528-568, 2011

[3] G. Moon, J. Kim, M. Hong, "A Graphical Passowrd Scheme Resistant to Shoulder Surfing Attack in Mobile Environments", Journal of computing science and engineering, Vol. 18, pp. 90-94, 2012

[4] Y. Bang, et al, "Improving information security management: An analysis of ID-password usage and a new login vulnerability measure", International Journal of Information Management, Vol. 32, pp. 409-418, 2012

[5] D. Kang, "The Influence of Password Selection on the Security Effectiveness", Pusan National University, 2008

[6] G. Post, A. Kagan, “Evaluating information security tradeoffs: Restricting access can interfere with user tasks”, Computers&Security, Vol. 26, pp. 229-237, 2007

[7] C. McCoy, R. Fowler, “You are the key to security: establishing a successful security awareness program”, SIGUCCS'04 Proceedings of the 32nd annual ACM SIGUCCS fall conference, pp. 346-349, 2004

[8] M. Chang, D. Kang, "Factors Affecting the Information Security Awareness and Perceived Information Security Risk of Employees of Port Companies", Journal of Navigation and Port Research, Vol. 36, pp. 261-271, 2012

[9] Ministry of Information and Communication, "A white paper of Protect the National information Security ",2006

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

[11] Y. Lee, "A Study on Factors Influencing the Preventive Efforts toward Personal Information Privacy", Sungkyunkwan University, 2009

[12] G. Lee, Y. Dong, "Measure for the risk of leakage of personal information about the methods and practices of private companies", Korea Institute of Information Security & Cryptology. Vol. 18, pp. 92-100, 2008

[13] L. Drevin, H.A. Kruger, T. Steyn, "Value-focused assessment of ICT security awareness in an academic environment", Computers & Security, Vol. 26, pp. 445-451, 2007

[14] J. Kim, D. Kang, "The Effects of Security Policies, Security Awareness and Individual Characteristics on Password Security Effectiveness", Korea Institute of Information Security & Cryptology, Vol. 18, pp. 123-133, 2008

[15] V. Mitchell, “Consumer perceived risk: conceptualisations and models”, European Journal of Marketing, Vol. 33, pp. 163-195, 1999

[16] I. Jang, "Exploring the Relationship between Prevention Behavior of Privacy Leakage and Perceived Risk, Efficacy Beliefs of Internet User: Use RPA(Risk Perception Attitude) Framework, Kookmin University, 2010

[17] W. Lee, "The Influence of Security and Risk Perception on the Reuse of Internet Banking", Asia Pacific Journal of Information Systems, Vol. 17, pp. 77-93, 2007

[18] Cohen. J, “Statistical power analysis for the behavioral sciences(2nd ed.)”, Hillsdale, NJ:Erlbaum, 1988

[19] R. Baron, D. Kenny, “The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations”, Journal of Personality and Social Psychology, Vol. 51, pp1173-1182, 1986

[20] M. Kumar, et. al, “Reducing shoulder-surfing by using gaze-based password entry”, SOUPS' 07, pp. 13-19, 2007

[21] D. Carstens, P. McCauley-Bell, “Evaluation of the Human Impact of Password Authentication practices on Information Security”, Informing Science Journal, Vol. 7, pp. 67-85, 2004

[22] J. Choi, “Using weak passwords is same as open the front door to the thief", http://www.coconut.co.kr/04news/secu/0712/htm/seculetter02.html

[23] B. Ives, K. Walsh, H. Schneider, “The domino effect of password reuse”. Communications of the ACM - Human-computer etiquette, Vol. 47, pp. 75-78, 2004

[24] C. Kim, S. Lee, E. O, "The Impact of Interaction Factors of Digital Contents on Flow and Use Intention“, Digital Contents Society, Vol. 11, pp.212-224, 2011

하 상 원

2010년 : University of Newcastle, Bachelor of Information Tech 졸업
2011년~현재 : 고려대학교 정보보호대학 석사

관심분야 : 정보보호(Personal Information),사용자 인증(User Authentication), 통계적 분석(Statistical Analysis)

김 형 중

1978년 서울대학교 전기공학과(공학사)
1986년 서울대학교 제어계측공학과(공학석사)
1989년 서울대학교 제어계측공학과(공학박사)
1990년～2006년: 강원대학교 교수
1992년～1993년: USC 방문교수
2007년～현 재: 고려대학교 정보경영공학부 교수
관심분야 : Watermarking, Image Hashing, Data Compression, Steganography