Information Systems Review
Vol. 19, No. 3 September 2017 http://dx.doi.org/10.14329/isr.2017.19.3.069

사용자의 PC와 스마트폰에 대한 정보보안 인식 차이에 관한 연구

The Study on the Difference of Information Security Awareness between PC and Smartphone

박 정 현 (Piao Zhengxian) 중앙대학교 일반대학원 경영학과
강 성 민 (Sungmin Kang) 중앙대학교 경영경제대학 경영학부, 교신저자

요 약

정보화 시대에서 사람들은 정보기술이 빠른 속도로 발전하여 편리하고 체계적인 생활을 체험하고 있지만 정보보안 이슈들로 인하여 다양한 피해도 많이 경험하고 있다. 특히 스마트폰은 새로운 단말기로서 PC와 같이 정보보안 이슈에 있어 최근에 크게 화두가 되고 있으며, 이러한 환경에서 사용자의 PC 및 스마트폰 정보보안에 대한 인식을 분석할 필요가 있다. 즉, 어떠한 요인이 정보보안 인식에 영향을 미치고 또한 어떠한 요인에서 PC 및 스마트폰 간의 차이가 있는지를 분석하고자 한다. 하지만 스마트폰 정보보안 인식에 대한 연구 및 PC와 스마트폰 정보보안 인식의 차이에 대한 기존의 연구는 찾아보기가 어렵다. 본 연구는 이러한 부분에 중점을 두고 선행연구에 기반한 연구 모델을 제시하였고 실증적 검증을 수행하였다.

본 연구의 결과를 요약하면 다음과 같다. 첫째, 보안 기술의 이해도, 정보보안 위협의 이해도, 정보보안 교육이 사용자의 PC 및 스마트폰 정보보안 인식에 긍정적인 영향을 미친다는 것을 검증하였다. 정보보안 의도는 사용자의 PC 정보보안 인식에 영향을 끼치고 스마트폰 정보보안 인식에는 영향을 끼치지 않는 것으로 나타났다. 또한, 정보보안 정책은 사용자의 PC 및 스마트폰 정보보안 인식에 영향을 미치지 않았다. 둘째, 사용자의 PC 및 스마트폰 정보보안 인식이 차이가 있음을 검증하지 못했다. 하지만 각 요인별 차이를 살펴보게 되면 보안 기술의 이해도, 정보보안 정책 및 정보보안 교육 3가지 측면에서 PC와 스마트폰 간의 차이가 있음을 검증할 수 있었고 정보보안 위협의 이해도와 정보보안 의도 측면에서 보면 PC와 스마트폰의 차이가 있음을 검증할 수 없었다.

키워드 : 스마트 시대, 정보보안 위협, 정보보안 교육, 정보보안 의도, 정보보안 정책, 정보보안 인식

Ⅰ. 서 론

현대사회는 정보화 사회라고 불린다. 급속히 성장한 IT기술을 바탕으로 사회의 각 분야가 정보화되면서 사람들의 삶도 이 트렌드에 따라 변화하여 스마트화 되었다. 여기서 스마트화란 하드웨어나 소프트웨어에 의해 지금까지 상상도 못했던 정도의 처리 능력으로 정보를 처리하는 것을 의미하며(이기주, 2013), 요즘에 화두가 되고 있는 새로운 용어인 '지능형'과 같은 의미로 생각할 수도 있다.

이러한 스마트 시대에서는 스마트 생활, 스마트 작업, 스마트 경영 등이 우리 삶에 있어서 중요한 역할을 하고 있다. 최근 스마트 시대에서 주장하는 키워드는 모바일로, 현대 사회에서는 모바일 퍼스트(Mobile First)에서 모바일 온리(Mobile Only)까지 변화하고 있다(박호현, 2014). 즉, 인터넷 이용 환경이 PC환경에서 모바일 환경으로 전환되고 있다는 것이다. 모바일 퍼스트 및 모바일 온리라는 용어는 구글 회장 에릭 슈미츠(Eric Schmidt)가 제시하였으며, 그는 2010년에 모바일 퍼스트 시대를 주장하였고 2014년에는 모바일 온리 시대를 강조하였다. 2010년에는 IT 발전에 따라 생활, 작업 등 각 사회적인 분야에서 모바일 기기나 기술을 선호했고, 2014년부터는 이러한 트렌드가 더욱 심화되어 지금까지 사람들이 주로 모바일만 사용하는 추세이다. 세계적인 IT 기업들도 대부분 모바일 분야에 적극적으로 투자하고 있다. 2011년 마이크로소프트(Microsoft)는 스카이프(Skype)를 인수하여 기업의 모바일 사업 분야를 더욱 강화시켰으며, 2013년에 핸드폰 기업인 노키아(Nokia)를 인수하여 윈도우 폰(Windows phone)사업을 강화하고 경쟁우위를 증가시켰다. 또한 페이스북(Facebook)은 2004년에 설립되어 Social Network Service(SNS) 사업을 시작했고 2014년까지 사용자 수가 10억 명으로 증가하였다(Facebook, 재무보고서, 2014). 이렇듯 IT 및 모바일 산업의 발전에 따라 사람들의 생활방식 및 사고방식이 전환되었기 때문에 IT기업들은 초고속으로 성장할 수 있었다.

모바일 환경에서 사용되는 기기는 다양하며 대표적인 기기는 스마트폰이라고 볼 수 있다. 전 세계에서 스마트폰의 보유율은 2012년 5.2%에서 2014년 24.5%까지 상승하였으며 2018년에 36.5%까지 증가될 것으로 예상되며, 반면에 PC의 보유율은 2012년 20%에서 2014년까지 정체된 상태이고 2018년까지 여전히 변화가 없을 것으로 예상하고 있다(KT경제경영연구소, 2015). 또한 아시아경제에 따르면 스마트폰, 태블릿 등 모바일 환경에 대한 모바일 홈페이지 보유율은 전년도 보다 10.4%p 증가하여 2014년에는 18.1%로 증가하였다(이초희, 2014). 그리고 미래부가 발표한 '2016년 인터넷 이용 실태조사'에 따르면, 국내에서 스마트폰은 만 6세 이상 국민의 85%가 보유하고 있으며 65세 이상도 10명 중 3명이 보유하고 있는 것으로 나타났으며, 이러한 스마트폰 등 모바일기기의 급속한 대중화의 직접적인 영향으로 가구당 컴퓨터 보유율은 2011년에 81.9%로 최고점을 찍은 이후 지속적으로 하락세를 보여 2016년에는 75.3%를 차지하고 있다(왕혜민, 2017).

나아가 모바일화에 따른 정보보안 이슈도 부각되고 있다. 모바일 기술 때문에 PC에서 작업하던 일을 스마트폰을 통해 언제 어디서든 할 수 있게 된 반면, 이러한 편리성은 또 다른 위험의 이면을 가지고 있다. PC환경에서 일어나고 있었던 보안 위협들이 그대로 스마트폰에서 발생되고 있는 것이다. 2014년 중국 스마트폰 보안 침해사고 보고서에 따르면 스마트폰 악성코드 감염사고 수가 2013년에 비해 2014년에 326만 건으로 늘어났고, 이것은 2013년의 3.86배 증가한 수치이다. 반면 PC 악성코드 감염사고 수를 살펴보면 2013년에는 2012년보다 5.4억 건이 추가로 증가하였고, 2014년에는 2013년에 비해 3.24억 건이 추가로 증가하였다. 즉, PC환경에서의 악성코드 감염사고 증가 비율은 감소하는 추세지만 스마트폰 환경에서의 악성코드 감염사고 증가 비율은 늘어나는 추세다(360 Internet Security Center, 2015). 그리고

국내에서도 스마트폰 정보보안 이슈가 심각해지고 있다. 안드로이드 운영체계 기반 스마트폰의 사용자를 대상으로 분석한 결과는 악성코드 감염수가 2014년에 143만 247건으로 나타났으며, 2013년의 125만 1586건보다 14.2%까지 증가하였고 2012년의 26만 2699건에 비해 5.4배까지 증가하였다(안랩, 2015). 이스트소프트(www.estsoft.co.kr)가 발표한 '2016 정보보호보안인식실태조사' 설문 결과에 의하면 보안 사고로 인한 피해 경험에 있어 응답자의 절반 이상인 51.2%가 본인 또는 주변 지인이 PC · 스마트폰 보안 피해를 경험했다고 하였으며, 일반 사용자들이 겪는 보안 피해가 심각한 수준인 것으로 나타났다(최민지, 2016). 또한, 개인정보 유출 피해 사례가 늘면서 사이버 보안의 중요성이 부각되고 있지만 스마트폰 사용자들은 아직까지 이 문제의 심각성에 관심을 기울이지 않는 것으로 밝혀졌다. 이는 스마트폰 사용자들의 보안 불감증이 상대적으로 심각하다는 것을 보여주고 있다(진성철, 2017). 사용자들은 다양한 사용자 친화적 서비스를 이용하고 있으나 현재의 인터넷 환경에서 스마트폰과 개인 컴퓨터는 많은 보안 위협들로 안전하지 않다. 매일 새로운 보안 위협이 생겨나고 있으며 이에 대한 대응 차원의 보안기능과 성정, 보안 프로그램 증 다양한 보안 기술도 등장하고 있다. 따라서 사용자들은 보안 위협을 인식하고 보안 기술에 대한 지속적인 관심을 유지해야 하며, 정보보안 의식의 결여로 인해 발생하는 피해를 정확히 인지하고 있어야 한다(김종기, 김재현, 2014).

이렇게 심각해진 스마트폰 정보보안 환경의 원인은 모바일 기기의 보안에 대한 취약점도 있지만, 스마트폰 관련 기업들이 스마트폰의 일반적인 기능 및 성능에만 주로 몰두하여 보안문제의 해결에 있어 소홀하기 때문이며, 아울러 사용자의 부족한 스마트폰 정보보안 인식도 중요한 원인이 되고 있다. 또한 학교 및 기업 등의 특정한 조직에서의 부족한 정보보안에 대한 정책 및 교육도 중요한 원인으로 나타나고 있다.

이상의 배경으로 본 연구에서는 기존의 IT 환경에서 수행된 정보보안에 대한 분석 및 방법론 등에 대한 다양한 사전 연구 혹은 선행 연구를 기반으로 조직 구성원의 PC 및 스마트폰 정보보안에 대한 인식수준을 측정하기 위한 모델을 제시하고 이를 실증적으로 검증하고자 한다. 즉, 정보보안의 기술적, 인적, 제도적 요인에 기반하여 구성원의 PC 및 스마트폰 정보보안에 대한 인식 및 인식의 차이를 살펴보고자 한다. 또한 선행연구를 통하여 기술적, 인적, 제도적 요인에 대하여 구체적인 변수를 파악하여 각 변수가 PC 및 스마트폰 정보보안에 대한 인식 차이에 미치는 영향을 분석하고, 연구의 결과를 통하여 조직 구성원의 정보보안에 대한 인식의 중요성을 강조하고자 한다. 특히 스마트폰 환경에서 정보보안 이슈가 심각해지는 추세로서 스마트폰이 사람들에게 편리성, 가용성 등 많은 이점을 주는 반면에 스마트폰 정보보안 문제 때문에 사람들이 사회적, 경제적 등의 피해를 많이 받고 있다. 이렇듯 정보보안의 중요성이 커지고 있지만 스마트폰 정보보안과 관련된 연구는 아직도 부족한 실정이다. 따라서 본 연구는 특히 정보보안에 취약한 스마트폰 사용 피해를 막기 위하여 스마트폰 사용자들의 정보보안 인식을 자세히 살펴보고 사용자들의 정보보안 인식을 제고하여 기업들이 스마트폰 정보보안을 강조하는 효과적인 대응방안을 마련하는데 기여하고자 한다.

Ⅱ. 이론적 배경

2.1 정보보안 인식의 중요성

인식의 개념은 사회과학(사회인지), 심리학, 의학 및 정보시스템 분야의 연구수행 관점에서 다양하게 사용되어 왔으며, 인식은 각 개인의 자각으로 정의될 수 있고 정해진 이슈에 대한 관심이 증가하는 것으로 이해할 수 있다(Choi *et al*., 2008; 백민정, 손승희, 2010). 정보보안 인식이란 정보보

안에 의한 다차원적인 특성을 반영하여 사람을 중심으로 정보보안을 강조한 것으로, 그 동안 정보보안 인식을 측정하기 위하여 기술적, 인적, 제도적 측면에서 연구가 진행되어 왔다(신현민, 2009; 이선중, 이미정, 2008). 이러한 연구의 측정 대상은 주로 개인, 조직 내부, 조직 외부로 구분되며, 개인 중심으로 각각의 영역을 살펴보면 기술적 측면에서는 IT인프라의 취약점을 분석하고 이를 통하여 위협 방지 요소를 관리 및 처리하는 것까지 포함하고 있다. 이는 유선 및 무선 네트워크, 정보시스템, 데이터베이스(Database) 등에 대한 분석으로, 관리적 사용자가 정보보안 정책, 정보보안 절차 등에 대한 운영관리를 수행하는 것을 의미하고 있다. 그리고 정보보안에 대한 운영관리는 정보보안 교육, 정보보안 규정, 정보보안 추진체계 등을 포함한다.

또한 제도적 측면은 사용자의 정보보안 활동에 대한 항목들을 포함하고 있으며, 이는 사용자의 정보보안 윤리적 행태, 정보보안 정책에 대한 책임, 신뢰 등을 포함한다. Cavusoglu *et al.*(2009), Choi *et al.*(2008)은 정보보안 인식은 정보보안에 대한 자각 및 정보보안 활동에 대한 관심정도라고 하였다. Huang *et al.*(2010)의 연구에 따르면 정보보안에 대한 인식은 사용자가 정보보안에 대한 위협을 평가하고 행동적 반응을 결정하는 메커니즘으로 정의되었으며, 주로 정보보안 위협을 중심으로 사용자의 위협에 대한 지식을 측정하여 이러한 지식이 정보보안 인식에 긍정적인 영향을 미친다고 주장하였다. Wolf(2010)는 정보보안 인식은 정보보안에 대한 기본적인 개념으로서 개인 및 조직 정보보안에 큰 영향을 미칠 수 있다는 정보보안 인식의 중요성을 강조하면서, 정보보안 인식은 두 가지 중요한 부분으로 구성되었다고 주장하였다. 다시 말해 사용자에게 정확한 정보보안 정책을 전달하고 사용자를 설득시켜 정보보안 행동을 유도 및 전환하는 것이며, 주로 정보보안 정책을 강조하여 정보보안 정책은 정보보안 인식에 긍정적인 영향을 끼친다고 하였다.

2.2 정보보안 인식의 영향요인

정보보안 정책은 조직 내에서 정보보안 임무를 수행하기 위한 최상의 보안 요구사항이다(Wiant, 2005; 정보통신, 2006). Bulgurcu *et al.*(2010)은 정보보안 인식의 주요 요인은 사용자의 정보보안 정책(Information security policy) 및 일반적인 정보보안 인식(General information security awareness)이라고 하면서, 이 중에 일반적인 정보보안 인식은 사용자의 정보보안 위협에 대한 지식이라고 하였다. 이 연구는 정보보안 정책 및 정보보안 위협의 이해에 대한 중요성을 강조하였으며 두 요인이 정보보안 인식에 영향을 미친다고 하였다. 그리고 Ryan (2006)은 정보보안 위협에 대한 지식이 정보보안 인식에 대한 기본적인 요인으로서 정보보안 정책과 같이 정보보안 인식에 대하여 중요한 요인으로 보았으며, 추가적으로 기술적 요인을 제시하였다. 특히 기술적 요인은 컴퓨터 활용 능력(Computer literacy)이라고 설명하여 정보보안 인식에 영향을 미친다고 하였으며, 컴퓨터 사용기간, 사용빈도, 정보보안 소프트웨어의 활용수준 등이 컴퓨터 활용 능력에 포함되어 컴퓨터 활용 능력은 정보보안 인식의 기술적인 측면에 긍정적인 영향을 미친다고 하였다. 아울러 Solms and Kerry(2005)는 정보보안 정책을 정식적인 정책 및 비 정식적인 정책으로 구분하였고, 이와 관련하여 Ryan(2006)은 정식적인 정보보안 정책은 정부, 은행 등에서 발표된 정보보안에 관한 정보이고, 비 정식적인 정보보안 정책은 친구, 동료 등에서 전달된 정보보안에 관한 정보라고 하였다. 또한, 김종기, 전진환(2006)은 정보보안 강화를 위하여 사용자가 정보보안에 관련된 기본적인 이해가 필요하다고 하면서, 이러한 기본적인 이해는 정보보안에 대한 기본적인 지식, 기술이며 소프트웨어 설치방법, 특히 백신 소프트웨어에 대한 지식을 의미한다고 하였다.

그리고 Decker(2008)는 정보보안 인식을 측정할 때 사용자의 정보보안 교육이 중요하다고 하면서, 사용자는 정보보안 정책을 통하여 정보보

안의 예방조치를 이해할 수 있으며, 나아가 정보보안에 대한 실천도 강조하였다. Holbert(2013)의 연구에서 정보보안 인식은 정보를 접근 및 사용할 때 사용자가 얻는 정보보안 정책, 정보보안 교육, 정보보안 절차 및 행동에 대한 지식이라고 주장하였으며, 이중정 등(2014)의 연구에서는 기술적/물리적인 요인과 관리적인 요인을 강조하였다. 특히 기술적/물리적 요인은 정보보안 위협을 위주로 분석하였으며, 관리적 요인은 크게 사전관리 및 사후관리로 분류하였고, 나아가 사전관리는 정보보안 정책, 정보보안 교육 등을 의미하고 사후관리는 정보보안 침해사고 발생한 후 사용자가 정보보안 절차에 따라 실행한 정보보안 행동을 의미한다고 하였다.

또한 백민정(2010), 백민정, 손승희(2010)는 크게 조직적 요인, 기술적 요인, 인적 요인으로 정보보안 인식을 측정하였으며, 기술적 요인에서는 주로 정보유출 방지 시스템, 데이터 백업시스템 및 재해복구시스템 3가지 독립변수를 제시하였다. 신호영(2012)의 연구에서는 심각성 및 취약성에 대한 지각을 분석하여 스마트폰 사용자의 정보보안 행위의도를 측정하였으며, 심각성은 정보보안 위협 때문에 발생한 결과들의 심각성에 대한 지각이고 취약성은 위협이 발생할 가능성에 관한 지각이라고 하였다. 이기정(2012)의 연구에서는 스마트폰의 정보를 보호하기 위한 정보보안 관리체계 모형을 제시하면서 정보보안 정책, 정보보안 교육, 인적보안, 암호 통제, 접근 통제, 보안사고 관리, 모니터링 7가지 측면으로 모형을 구성하였다. 인적보안이란 조직의 보안정책에 따라 보안임무를 안전하게 수행하는데 영향을 주는 조직 구성원들에 대한 보안을 지칭한다(강다연, 장명희, 2014). 그리고 박진완(2011)은 스마트폰의 악성코드 위주로 진행하여 악성코드가 스마트폰 정보보안에 영향을 끼친다는 것을 강조하였으며, 장명희, 강다연(2012)은 정보보안 교육, 정보보안 관심도 및 정보보안 의도의 3가지 정보보안 인식에 영향을 끼치는 변수를 제시하면서, 정보보안 의도는 조직 내부의 정보보호를 위해 개인이 중요시 하는 정보보안 방안의 중요성을 의식하여 보호하려는 행동의지 정도로 정의하였다.

아울러 Spurling(1995)은 정보보안 의도를 기업의 내부 정보를 보호하기 위한 행동의지로 정의하였으며, 조직의 중요정보 유출에 대하여 정보보안 의도를 가지고 있을 때 정보보안 인식에 보다 긍정적인 영향을 미친다고 하였다. 이는 기업 구성원의 정보보안 인식의 증진을 위해서는 정보보안 교육과 정보보안 관심도, 그리고 정보보안 의도 등이 중요한 변수임을 알 수 있다. Hawkins *et al.*(2000)의 연구에서는 정보보안 의도를 네트워크 환경에서 인터넷을 통해 유출되는 위험에서 보호하려는 의지로 보았으며 네트워크 환경이 발달함에 따라 정보유출이 될 수 있는 확률이 높아지기에 이에 따른 명확한 정보보안 인식의 중요성을 언급하였고, Petrova and Sinclair(2003)는 정보보안 의도를 보안에 위협적인 요소들과 보안대응을 위한 방안 및 보안 기술을 적용하여 정보를 보호하려는 행동의지로 분석하면서, 사용자의 보안에 대한 행동의지가 정보보안 인식에 긍정적인 영향을 주는 것으로 나타났다. 그리고 Rhee *et al.*(2009)의 연구에서는 정보보안 행위의도를 사용자가 정보보안을 강화하기 위해 지속적으로 노력하려는 의지라고 하였고, Dinev and Hart(2006)는 기술 인식도를 사용자가 기술적 이슈와 그것을 다루는 전략에 대하여 아는 것에 흥미를 느끼고 의식을 높이게 되는 것이라고 하면서, 이는 사용자가 정보보안 기술에 대하여 얼마나 이해하고 있는지를 나타낸다고 하였다.

이상의 정보보안 인식에 대한 선행 연구를 살펴보면 정보보안 인식은 정보보안에 대한 중요성을 강조하며 정보보안 인식을 측정하는 영역은 다양하게 존재한다는 것을 알 수 있다.

Ⅲ. 연구 방법

3.1 연구의 모형

본 연구는 조직 내 구성원을 대상으로 진행된

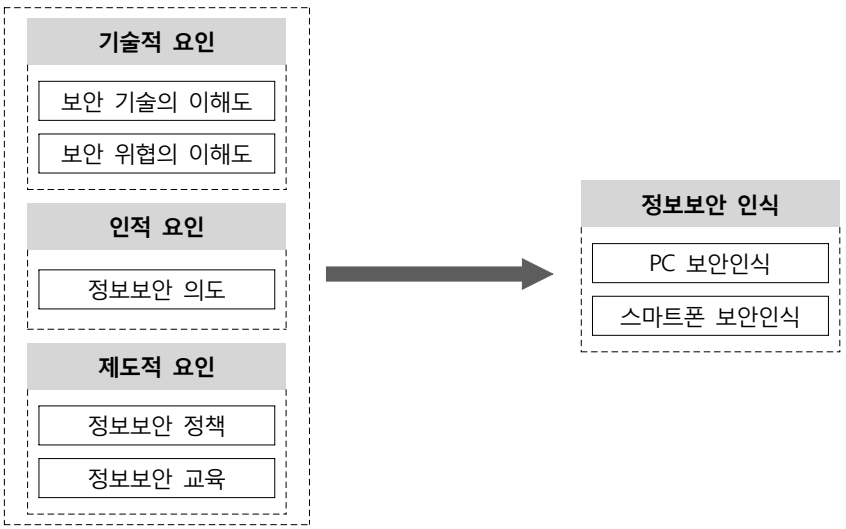
선행연구를 바탕으로 정보보안 인식의 영향요인으로 기술적, 제도적 및 인적 요인으로 분류하여 <그림 1>과 같이 연구모형을 도출하였다. 이와 관련하여 백민정(2010)은 정보활동을 기술적 요인, 인적 요인, 제도적 요인으로 구분하여 일한 조직의 정보활동이 조직 내의 구성원의 정보보안 인식에 긍정적인 영향을 끼친다고 주장하였으며, Decker(2008)는 고유요인, 외부요인, 기술요인 및 관리요인 4가지 요인으로 조직 내 구성원의 정보보안 인식을 측정하면서, 조직 내 구성원의 정보보안 인식에 영향을 끼치는 요인들은 조직 차원의 요인뿐만 아니라 구성원 자신의 요인도 중요하다고 주장하였다. 그리고 Petrova and Sinclair(2003)는 정보보안 의도를 보안 위협적인 요소들과 보안 대응을 위한 방안 및 보안 기술을 적용하여 정보를 보호하려는 행동의지로 분석하였으며, 그 결과 사용자의 보안에 대한 행동의지가 정보보안 인식에 긍정적인 영향을 준다고 하였다. Bulgurcu *et al.*(2010)의 연구에서는 일반적인 정보보안 인식(General information security awareness)을 정보보안의 위협 및 부정적 영향에 대한 지식으로 정의하여 조직 구성원의 정보보안 인식에 정의 영향을 끼친다고 제시하였으며, Ryan(2006)의 연구에서는 정보보안 위협을 강조하여 정보보안 위협의 적절한 대책에 대한 지식도 정보보안 인식에 영향을 끼친다고 주장하였다.

이러한 배경으로 본 연구에서 제시된 변수들이 구성원의 PC 및 스마트폰 정보보안 인식에 어떠한 영향을 미치는가를 검증하고자 한다.

3.2 연구의 가설 설정

3.2.1 보안 기술의 이해도에 대한 가설

보안 기술의 이해도는 기술적 요인의 한 가지 변수로서 조직 구성원의 정보보안 인식에 대한 중요한 요인이라고 볼 수 있다. 이에 Decker(2008)는 정보보안 인식을 측정할 때 사용자 특성이라는 요인을 강조하면서, 사용자 특성을 정보보안의 핵심적인 요인으로 보고 이러한 특성으로 인하여 사용자의 정보보안 인식은 차이가 난다고 하였다. 또한, Ryan(2006)은 컴퓨터 활용 능력(Computer literacy)을 정보보안 인식 연구에서 중요한 요인으로 제시하였으며, 컴퓨터 활용 능력을 정보보안에 대한 기본적인 기술이라고 정의하



〈그림 1〉 연구 모형

고 컴퓨터 활용 능력이 높은 사용자가 정보보안 인식도 높다고 검증하였다. 그리고 Dinev and Hart(2006)의 연구에 따르면 기술 인식도는 사용자가 기술적 이슈에 대하여 아는 것에 흥미를 느끼고 의식을 높이게 되는 것이라고 하면서, 사용자의 정보보안 기술에 대한 이해도가 높을수록 정보보안 인식도 높아진다고 하였다.

이러한 선행연구를 살펴보면 PC의 정보보안 인식에 영향을 끼치는 요인에 있어 정보보안 기술의 이해도가 중요하다고 볼 수 있다. 이에 본 연구에서는 선행연구에서 제시한 변수를 바탕으로 H1a를 설정하였다. 그리고 PC에서 하던 일들은 스마트폰에서도 할 수 있으며 PC 및 스마트폰 보안 기술이 동일하다고 볼 수 있다. 이에 스마트폰 보안 기술에 대한 이해도는 PC와 동일하게 정보보안 인식에 긍정적인 영향을 끼친다는 예상을 하여 H1b를 설정하였다. 또한, 본 연구에서는 보안 기술의 이해도에 있어 PC와 스마트폰 간의 비교 분석을 하고자 한다. 즉, 사용자의 PC 및 스마트폰 보안 기술의 이해도가 차이가 있는지를 연구하고자 한다. Ryan(2006)의 연구에서는 사용기간이 많을수록 보안 기술의 이해도가 높다고 주장하였다. 스마트폰 사용기간이 PC와 비교하면 많이 짧아서 보안 기술의 이해도에 있어 PC와 스마트폰 간에는 차이가 있을 것이다. 이러한 비교를 위하여 H1c을 설정하였다.

H1a: 보안 기술의 이해도는 사용자의 PC 정보보안 인식에 긍정적인(+) 영향을 끼칠 것이다.

H1b: 보안 기술의 이해도는 사용자의 스마트폰 정보보안 인식에 긍정적인(+) 영향을 끼칠 것이다.

H1c: 사용자의 PC와 스마트폰에 대한 보안 기술의 이해도는 차이가 있을 것이다.

3.2.2 보안 위협의 이해도에 대한 가설

Huang *et al.*(2010)은 정보보안 위협에 대한 지식, 영향, 기술 등의 측면으로 위협의 중요성을 강조하여 정보보안 위협이 정보보안 인식에 영향을 미친다는 것을 보여주었다. 즉, 정보보안 위협에 대한 지식이 많아 피해 영향을 잘 이해하고 정보보안 위협에 대한 대책을 잘 활용한 사용자가 정보보안 인식이 높다고 강조하였다. 또한, Bulgurcu *et al.*(2010)은 위협 측면에서 정보보안 인식을 측정하였으며 사용자가 정보보안 위협이 시스템에 어떠한 영향을 끼치는가를 알고 있으면 높은 정보보안 수준이 나타난다고 주장하였다. 이러한 정보보안 위협을 잘 이해하는 사용자들은 PC를 사용할 때 보안 위협을 잘 식별할 수 있다. 따라서 정보보안 위협의 이해도가 높기 때문에 적절한 대책방법에 대한 지식도 많아 정보보안 인식이 더욱 높을 것이다. 이에 H2a에서와 같이 정보보안 위협의 이해도는 사용자의 PC 정보보안 인식에 긍정적인 영향을 미칠 것이라고 설정하였다.

최근에 스마트 작업 및 스마트 뱅킹 등이 확산되어 사용자들은 스마트폰으로 많은 일을 하고 있다. 이에 따라 정보보안 위협이 스마트폰 환경에서도 PC와 동일하게 있을 것이다. 사용자의 스마트폰 위협에 대한 이해도가 높으면 더욱 쉽게 정보보안 위협을 식별할 수 있고 위협의 대책방법에 대한 지식도 많을 것이다. 이러한 측면에서 H2b와 같이 사용자의 정보보안 인식도 높을 것이다. 그리고 이현동(2012)의 연구에서는 스마트폰의 특징으로 인하여 어떠한 보안 위협이 생길 수 있는지를 설명하였다. 스마트폰의 특징을 살펴보면 PC와 비교하여 휴대의 편리성이 가장 큰 차이로 볼 수 있으며, 스마트폰의 휴대 편리성으로 인하여 스마트폰 도난 및 분실이 쉽게 발생할 것이다. 이상으로 사용자가 기기의 특징 때문에 추가된 위협에 대해 익숙하지 않아 정보보안 위협의 이해도 측면에서 PC와 스마트폰 간에는 차이가 있을 것이다. 이에 따라 본 연구의 H2c을 설정하였다.

H2a: 정보보안 위협의 이해도는 사용자의 PC 정보보안 인식에 긍정적인(+) 영향을 끼칠 것이다.

H2b: 정보보안 위협의 이해도는 사용자의 스마트폰 정보보안 인식에 긍정적인(+) 영향을 끼칠 것이다.

H2c: 사용자의 PC와 스마트폰에 대한 정보보안 위협의 이해도는 차이가 있을 것이다.

3.2.3 정보보안 의도에 대한 가설

장명희, 강다연(2012)의 연구에서는 정보보안 의도는 조직 환경에서 정보보호를 위해 개인이 중요시 하는 정보보안 방안의 중요성을 의식하여 보호하려는 행동의지 정도로 정의하였다. Petrova and Sinclair(2003)의 연구에서는 정보보안 의도를 보안 위협적인 요소들과 보안대응을 위한 방안 및 보안 기술을 적용하여 정보를 보호하려는 행동의지로 분석하였다. 또한, 사용자의 보안에 대한 행동의지가 정보보안 인식에 긍정적인 영향을 주는 것으로 나타났으며, Hawkins *et al.*(2000)의 연구에서는 정보보안 의도를 네트워크 환경에서 인터넷을 통해 유출되는 위험에서 보호하려는 의지로 보았으며 네트워크 환경이 발달함에 따라 정보유출이 될 수 있는 확률이 높아지기에 이에 따른 명확한 정보보안 인식의 중요성을 언급하였다.

정보보안 의도가 높은 사용자는 정보보안을 강화하기 위하여 정보보안 절차에 따라 관련 작업을 잘 실행하려는 의지가 높을 것이며 정보보안을 더욱 중요하다고 인식할 것이다. 예를 들면 주기적인 바이러스 검사 및 백업 등에 대한 의지가 높은 사용자는 정보보안 인식이 높을 것이다. 이에 따라 H3a를 설정하였다. 그리고 스마트폰 측면에서도 PC 측면의 정보보안 의도와 동일하게 정보보안 의도가 높은 사용자가 스마트폰 정보보안을 더욱 중요하게 인식할 것이다. 하지만 스마트폰은 언제 어디에서도 사용할 수 있기 때문에 사용자의 PC와 스마트폰 정보보안 의도에는 차이가 있을 수도 있다. 이에 따라 본 연구에서 가설 H3b 및 H3c를 설정하였다.

H3a: 정보보안 의도는 사용자의 PC 정보보안 인식에 긍정적인(+) 영향을 끼칠 것이다.

H3b: 정보보안 의도는 사용자의 스마트폰 정보보안 인식에 긍정적인(+) 영향을 끼칠 것이다.

H3c: 사용자의 PC와 스마트폰에 대한 정보보안 의도는 차이가 있을 것이다.

3.2.4 정보보안 정책에 대한 가설

Wolf(2010)의 연구에서는 정보보안 정책을 강조하여 정보보안 정책이 조직 구성원의 행위를 변화시킨다고 주장하였으며, Bulgurcu *et al.*(2010)의 연구에서는 정보보안 정책 및 정보보안 인식의 관계를 설명하였다. 즉, 조직의 정보보안 정책이 조직 구성원의 정보보안 인식에 긍정적인 영향을 끼친다는 것을 검증하였다. 또한, Ryan(2006), Solms and Kerry(2005) 등의 연구에서도 정보보안 정책을 정식적인 정책 및 비 정식적인 정책으로 구분하여 정보보안 정책의 중요성을 강조하였으며, 정보보안 정책이 정보보안 인식에 정의 영향을 미친다고 주장하였다.

정보보안 정책을 중요하다고 생각한 사용자들은 정보보안 정책에 많은 관심을 가지고 있고 시대에 따라 정보보안 정책에 대한 지식을 지속적으로 업데이트 할 것이다. 항상 정보보안에 관련된 최신의 규정을 알고 있을 것이며 정보보안 인식도 높을 것이다. 이에 따라 H4a를 설정하였다. 그리고 PC 정보보안 정책 측면과 동일하게 정보보안 정책을 중요하게 생각하는 스마트폰 사용자는 허용되는 스마트폰의 규정에 많은 관심을 가지고 있을 것이고 쉽게 규정에서 제시된 내용과 일치하지 않은 상황을 발견할 것이다. 이러한 사용자들은 스마트폰 정보보안이 더욱 중요하다고 인식할 것이다. 이에 따라 H4b를 설정하였다. 또한, 스마트폰의 정보보안 이슈는 최근에 많이 발생하여 스마트폰 정보보안에 대한 정책은 PC보다 부족할 수밖에 없다. 따라서 사용자가 스마트폰 정보보안 정책에 대해서는 상대적으로 생소하기 때문에 PC 정보보안 정책과 차이가 있을 것이다. 이에 따라 본 연구

에서는 가설 H4c를 설정하였다.

H4a: 정보보안 정책은 사용자의 PC 정보보안 인식에 긍정적인(+) 영향을 끼칠 것이다.
H4b: 정보보안 정책은 사용자의 스마트폰 정보보안 인식에 긍정적인(+) 영향을 끼칠 것이다.
H4c: 사용자의 PC와 스마트폰에 대한 정보보안 정책은 차이가 있을 것이다.

3.2.5 정보보안 교육에 대한 가설

Decker(2008)는 정보보안 교육의 중요성이 많은 정보보안 인식에 대한 연구에서 정보보안 교육을 통해 정보보안 인식을 정의 및 제고하는 것을 강조하였으며, 백민정(2010)의 연구에 의하면 정보보안 교육도 정보보안 인식을 측정할 때 중요한 요인으로 강조되어 정보보안 인식에 긍정적인 영향을 끼친다고 하였다.

정보보안 교육이 중요하다고 생각한 사용자들은 정보보안 교육을 통하여 정보보안에 관련된 지식이나 기술을 습득할 것이며 정보보안 수준을 강화할 것이며, 이러한 사용자들은 정보보안 교육에 관심이 없는 사용자들보다 정보보안 인식이 더욱 높을 것이다. 이에 본 연구에서는 정보보안 교육을 추가하여 H5a를 설정하였다. 그리고 PC 정보보안 교육 측면과 동일하게 스마트폰 정보보안 교육에 관심을 가지고 있는 사용자가 교육이 중요하다고 생각하여 교육을 통하여 많은 스마트폰 정보보안에 관련한 지식을 습득하고자 하는 의지가 있을 것이며, 이러한 사용자들은 정보보안 인식이 높을 것으로 생각한다. 이에 따라 본 연구에서는 H5b를 설정하였다. 또한 사용자의 스마트폰 사용기간이 PC보다 짧아서 스마트폰 정보보안에 관한 지식이 상대적으로 부족할 것이며, 스마트폰 정보보안 이슈가 점점 심각해지는 추세에서 사용자가 스마트폰 정보보안의 수준을 강화하기 위하여 PC보다 스마트폰 정보보안 교육을 더 많이 받고 싶을 것이고 더욱 중요하다고 인식할 것이다. 이에 따라 가설 H5c를 설정하였다.

H5a: 정보보안 교육은 사용자의 PC 정보보안 인식에 긍정적인(+) 영향을 끼칠 것이다.
H5b: 정보보안 교육은 사용자의 스마트폰 정보보안 인식에 긍정적인(+) 영향을 끼칠 것이다.
H5c: 사용자의 PC와 스마트폰에 대한 정보보안 교육은 차이가 있을 것이다.

3.2.6 정보보안 인식에 대한 가설

PC가 도입된 지 오래되어 사용자가 PC 정보보안에 대해 더욱 잘 이해한다고 볼 수 있다. 스마트폰은 2007년부터 유행하여 사용자가 스마트폰 정보보안에 대한 인식이 상대적으로 부족하다고 볼 수 있다. 그리고 대학교 혹은 기업에서는 사용자가 PC 정보보안에 대하여 어느 정도는 인식하고 있지만 그의 스마트폰 정보보안에 대한 인식은 상대적으로 부족하다고 느끼고 있다. 또한, 최근에 심각해진 스마트폰 정보보안 이슈로 인하여 사용자가 스마트폰 정보보안에 대하여 더욱 중요하다고 생각할 것이며 스마트폰 정보보안에 관련한 지식이나 기술을 많이 습득하고자 할 것이다. 이러한 환경에서 H6과 같이 사용자의 PC와 스마트폰 정보보안에 대한 인식은 차이가 있을 것이라고 예상할 수 있다.

H6: 사용자의 PC와 스마트폰에 대한 정보보안 인식은 차이가 있을 것이다.

3.3 연구 변수의 조작적 정의 및 측정

3.3.1 기술적 요인

기술적 요인에서는 두 가지 변수가 있다. 즉, 보안 기술의 이해도 및 정보보안 위협의 이해도이다. Ryan(2006)의 연구에서는 사용자의 정보보안에 관련된 기본적인 지식 및 기술에 대한 이해 정도로 보안 기술의 이해도를 정의하였으며 관련

하여 설문기반의 측정 항목을 제시하였으며, 백신 프로그램 및 방화벽 소프트웨어는 정보보안에 관련된 기본적인 지식 및 기술로서 사용자의 이에 대한 이해 수준을 측정하였다. Dinev and Hart(2006)의 연구에서는 기술 인식도를 사용자가 기술적 이슈와 그것을 다루는 전략에 대하여 아는 것에 흥미를 느끼고 의식을 높이게 되는 것이라고 정의를 내리고 있으며, 사용자가 정보보안 기술에 대하여 얼마나 이해하고 있는지를 보고자 하였다. 이에 본 연구에서도 사용자의 PC 및 스마트폰에 대한 기본적인 기술을 측정하기 위하여 Ryan(2006)의 연구에서와 같이 5점 척도로 측정하고자 한다.

또한, Ryan(2006)의 연구에서 정보보안 위협은 정보보안 위협에 대한 지식, 즉 위협의 유형, 영향 등으로 정의하였으며, 정보보안 위협의 이해도에는 이러한 위협에 대한 적절한 대책도 포함된다고 하였다. 그리고 이 연구에서 도출한 항목으로 첫째는 정보보안 위협의 중요성을 제시하였으며, 둘째로는 정보보안 위협에 대한 적절한 대책, 즉, 백업, 패스워드 설정, 소프트웨어 업데이트를 제시하였다. 그리고 셋째로는 정보보안 위협이 시스템에 끼치는 영향을 강조하였다. 아울러 Huang *et al.*(2010)의 연구에서도 정보보안 위협에 대한 영향과 대책을 강조하였다. 본 연구에서도 Ryan(2006), Dinev and Hart(2006)의 연구에서 제시한 항목에 따라 5점 척도로 측정하고자 한다.

3.3.2 인적 요인

인적 측면의 변수는 정보보안 의도이다. 정보보안 (준수)의도는 잠재적 보안 위협으로 인한 피해로부터 조직의 핵심 정보 및 기술 자원을 보호하기 위한 조직 구성원의 의도로 정의되었다(Bulgurcu *et al.*, 2010; Vance *et al.*, 2012). 이에 대하여 황인호 등(2016)은 조직 구성원의 정보보안(준수)의도는 자발적인 보안 활동을 위한 조직 구성원의 의지이기 때문에, 조직이 요구하는 정보보안 수준을 달성하기 위해서는 조직 구성원의 정보보안 준수의도를 지속적으로 높이기 위한 노력이 필요하다고 주장하였다. 또한, Hawkins *et al.*(2000), Petrova and Sinclair(2003), 장명희, 강다연(2012)의 연구에서는 정보보안 의도는 조직의 내부의 정보보호를 위해 개인이 중요시 하는 정보보안 방안의 중요성을 의식하여 보호하려는 행동의지 정도로 정의하였다. 이 연구에서는 바이러스 검사, 자료의 백업, 패스워드의 변경 등과 같은 정보보안 의도를 측정항목으로 설정하였다. 본 연구에서도 이와 같이 5점 척도로 측정 항목을 제시하였다.

3.3.3 제도적 요인

제도적 요인의 변수는 정보보안 정책 및 정보보안 교육이다. Bulgurcu *et al.*(2010)의 연구는 정보보안 정책을 측정하기 위하여 3가지 항목을 도출하였으며, 정보보안 정책에 대한 이해, 자신의 책임 및 얼마나 정보보안 정책을 알고 있는가를 측정하였다. 그리고 Ryan(2006)의 연구에서는 정보보안 정책을 측정하기 위하여 정책에 대한 관심도 및 비 정식적인 정책을 측정항목으로 적용하였다. 이에 본 연구에서는 두 연구자의 항목들을 종합하여 5점 척도로 측정하고자 한다. 또한, 이선중, 이미정(2008)의 연구에서는 정보보안 교육을 측정하기 위하여 정보보안 교육의 참여성 및 중요성을 측정항목으로 도출하였으며, 송은수(2006)의 연구에서는 정보보안 교육의 효과성을 강조하였다. 본 연구에서는 연구의 목적에 맞게 정보보안 교육의 필요성을 추가하여 제시한 제도적 측면의 측정 항목으로 사용하였다.

3.3.4 정보보안 인식

Wolf(2010)의 연구에서는 정보보안 인식은 정보보안의 중요성을 의미한다고 주장하였으며, 백민정(2010)의 연구에서는 정보보안 인식을 측정하기 위하여 6가지 항목을 도출하였다. 그리고 정해철, 김현수(2000)의 연구에서는 정보보안 인식을 정보보안의 필요성, 정보보안 의지, 정보의

가치인식 정도로 나누어 측정하였으며, 박일형 등(2009)은 정보보안 이해 수준, 정보의 중요성을 인지하는 정도, 보안에 대한 필요성으로 자각하는 정도를 통해서 정보보안 인식 수준을 측정하였다. 또한, 장명희, 강다연(2012)의 연구에서는 정보보안 인식을 조직 구성원의 정보보안의 중요성을 알고 있는 정도로 정의하여 정보보안 인식을 측정하기 위하여 4가지 항목을 도출하였다. 이러한 선행연구에 따라 본 연구의 목적에 맞게 정보보안 인식의 측정 항목을 사용하였다.

3.4 연구 방법

본 연구는 보안 기술의 이해도, 정보보안 위협의 이해도, 정보보안 의도, 정보보안 정책, 정보보안 교육의 5가지 변수들이 조직 구성원의 PC 및 스마트폰 정보보안 인식에 끼치는 영향을 측정 및 분석한다. 그리고 어떠한 요인으로 인하여 사용자의 PC와 스마트폰 정보보안 인식 간에 차이가 있는지를 분석한다. PC 및 스마트폰을 많이 이용하고 있는 대학생 및 대학원생을 본 연구의 설문대상으로 적용하였다. 이들을 선정한 이유는 학교 혹은 회사에서 PC 및 스마트폰을 자주 사용하고 특히 스마트폰을 초기 보급 시기부터 이용하고 있기 때문이다.

본 연구에서는 선행연구를 통하여 도출된 설문 문항들이 정확하게 구성되었는가를 확인하고 설문조사 대상자들이 이러한 설문 문항에 대하여 잘 이해하고 있는지를 측정하기 위하여 사전 조사를 2번 수행하였다. 1차 사전 조사는 대학(원)생을 대상으로 수행하였으며 응답자가 이해하기 어려운 문항들을 수정하였고 본 연구의 목적에 맞게 문항을 추가 및 수정하였다. 2차 사전 조사는 설문 문항들에 있어 기술용어들에 대한 추가 설명을 제공하여 응답자가 설문내용을 이해하기 쉽도록 설문지를 수정하는데 중점을 두었다.

본 조사에서는 온라인 설문 조사 및 오프라인 설문 조사를 활용하여 대학생 179명 및 대학원생 40명으로부터 총 219부의 설문지를 수집하였다. 이 중에 8부의 설문지는 무효설문지로 제외하였다. 설문지는 PC 및 스마트폰 부분으로 구분하여 크게 3가지 측면으로 작성되었다. 즉, 정보보안 인식을 측정하기 위한 3가지 측면은 기술적 요인, 인적 요인, 제도적 측면이다. 따라서 각 측면의 독립변수는 보안 기술의 이해도, 정보보안 위협의 이해도, 정보보안 의도, 정보보안 정책, 정보보안 교육이다. 설문지는 PC 및 스마트폰 부분에서 각 35개 문항이며 인구 사회학적 통계를 추가하여 총 79개 문항으로 구성하였다. 각 변수를 측정하기 위하여 '전혀 그렇지 않다'는 1점이고 '매우 그렇다'는 5점으로 표시하여 5점 리커트(Likert) 척도를 사용하였다. 수집된 설문조사 데이터의 분석은 SPSS 22.0 for Windows 통계 패키지 프로그램을 사용하여 수행하였다.

Ⅳ. 연구 데이터 분석

4.1 표본의 인구통계학적 특성

설문 응답자의 인구 통계학적 분석을 실시한 결과는 다음과 같다. 응답자는 남성 108명(51.2%)과 여성 103명(48.8%)으로 구성되어 있으며, 연령은 20세부터 26세까지가 89.6%이고 27세부터 39세까지가 10.4%를 차지하였다. 또한, PC 사용기간은 13년부터 16년까지 사용하고 있었던 응답자가 102명(48.3%)으로 가장 많은 비율을 차지하고 있었다. 스마트폰 사용기간은 109명(51.7%)이 4년부터 6년까지로 나타났다. 또한, 응답자가 제시한 정보기술(IT)의 중요성에 대한 인식은 대부분 높은 수준(그렇다 41.7%, 매우 그렇다 49.3%)으로 나타났다.

4.2 타당성 및 신뢰성 분석

본 연구에서는 개념타당성을 측정하기 위해 주성분 분석을 실시하였으며 Rotation은 Varimax 방

법을 선정하였다. 타당성 분석 결과를 살펴보면 독립변수 중에 정보보안 위협의 이해도 3개 항목, 정보보안 의도 3개 항목, 정보보안 인식 1개 항목을 제외하여 요인 적재량이 0.5 이상으로 나타났다. 하지만 정보보안 의도 변수에서 1개 항목은 0.495이며 전반적인 고려를 위하여 유지하였다.

통계적으로 KMO(Kaiser-Meyer-Olkin) 값은 0.6 이상이면 요인분석의 타당성 분석결과가 유의미하다고 볼 수 있고 0.8 이상이면 좋다고 볼 수 있다. 본 연구의 결과를 살펴보면 PC 부분의 KMO 값은 0.840, 스마트폰 부분 KMO값은 0.861로 좋은 요인분석으로 확정되었다. 또한 본 연구의 신뢰도를 측정하기 위하여 Cronbach's α분석을 이용하였다. 통계적으로 α계수가 0.7 이상이면 신뢰도가 높다고 볼 수 있다. 본 연구의 신뢰도 결과를 살펴보면 모두 0.7 이상으로 높은 신뢰도를 확보하였다. 요인 및 신뢰도 분석 결과는 <표 1>과 같다.

〈표 1〉 PC 및 스마트폰 부분 요인 및 신뢰성 분석 결과

구 분	PC 부분			스마트폰 부분		
	측정항목	요인적재량	Cronbach's α	측정항목	요인적재량	Cronbach's α
보안 기술의 이해도	Isa6	.799	0.734	Isa2	.822	0.828
	Isa4	.778		Isa3	.808	
	Isa1	.764		Isa5	.805	
	Isa5	.736		Isa4	.784	
	Isa3	.736		Isa6	.753	
	Isa2	.719		Isa1	.722	
보안 위협의 이해도	Pol2	.843	0.801	Pol2	.882	0.768
	Pol5	.803		Pol3	.860	
	Pol3	.732		Pol1	.852	
	Pol1	.724		Pol4	.815	
	Pol4	.717		Pol5	.765	
정보보안 정책	Thr3	.753	0.852	Thr3	.792	0.904
	Thr2	.681		Thr1	.645	
	Thr1	.656		Thr4	.637	
	Thr4	.626		Thr2	.606	
정보보안 교육	Beh8	.778	0.788	Beh8	.719	0.855
	Beh7	.722		Beh3	.697	
	Beh6	.676		Beh7	.672	
	Beh3	.565		Beh2	.668	
	Beh2	.495		Beh6	.629	
정보보안 의도	Edu2	.807	0.777	Edu2	.819	0.815
	Edu1	.778		Edu3	.802	
	Edu4	.653		Edu1	.797	
	Edu3	.652		Edu4	.715	
정보보안 인식	Gen3	.712	0.886	Gen3	.808	0.915
	Gen1	.712		Gen2	.776	
	Gen4	.649		Gen1	.756	
	Gen2	.627		Gen4	.667	

4.3 연구가설 검증

독립변수가 종속변수에 미치는 영향을 측정하기 위하여 회귀분석을 활용하였다. 먼저, 모형의 적합도에 대한 분석 결과는 조정된 R^2가 PC 부분에서 0.346, 그리고 스마트폰 부분에서 0.406으로 나타났다. 통계적으로 R^2가 0.26 이상이면 내적 변수별 경로모형의 적합도가 높다고 판단할 수 있다. 최종 회귀 분석 결과는 <표 2>, <그림 2>와 같다.

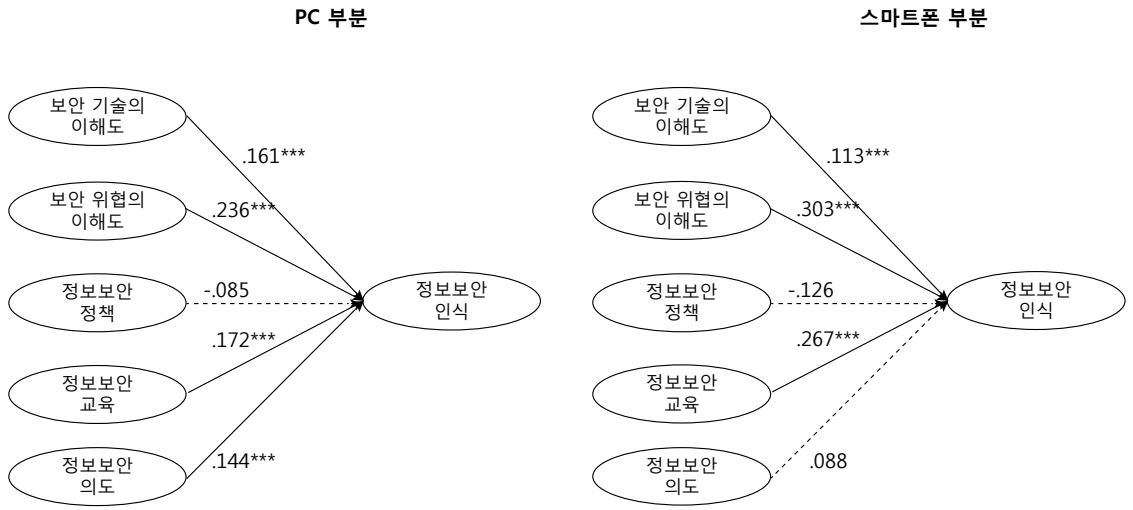
4.3.1 각 요인과 정보보안 인식의 관계

각 요인과 정보보안 인식의 관계는 살펴보면, 먼저 PC 부분은 통계적으로 유의수준 0.01에서 보안 기술의 이해도는 정보보안 인식에 영향을 끼치는 것으로 나타났다. 그리고 스마트폰 부분에서는 통계적으로 유의수준 0.05에서 보안 기술

〈표 2〉 회귀분석 결과

구 분	종속변수 / 독립변수	정보보안 인식		F	R^2
		β	t		
PC	보안 기술의 이해도	.161	2.713**	21.718***	.346
	보안 위협의 이해도	.236	4.049***		
	정보보안 정책	-.085	-1.597		
	정보보안 교육	.172	3.173**		
	정보보안 의도	.144	2.768**		
스마트폰	보안 기술의 이해도	.113	2.166*	29.666***	.406
	보안 위협의 이해도	.303	4.843***		
	정보보안 정책	-.126	-2.907		
	정보보안 교육	.267	5.230***		
	정보보안 의도	.088	1.786		

*p < 0.5, **p < 0.01, ***p < 0.001.



*p < 0.5, **p < 0.01, ***p < 0.001.

〈그림 2〉 연구결과 모형

의 이해도는 정보보안 인식에 영향을 끼치는 것으로 나타났다. 즉, 사용자의 PC 및 스마트폰에 대한 보안 기술의 이해도가 높을수록 정보보안 인식이 더 높다고 볼 수 있다. PC 부분의 결과는 김종기, 전진환(2006), Ryan(2006)의 연구와 같게 나타났다. 또한, 스마트폰 부분에서도 PC 부분과 같이 유의한 결과가 나타났다. 즉, H1a(보안 기술의 이해도는 사용자의 PC 정보보안 인식에 긍정적인(+) 영향을 끼칠 것이다) 및 H1b(보안 기술의 이해도는 사용자의 스마트폰 정보보안 인식에 긍정적인(+) 영향을 끼칠 것이다)의 두 개 가설이 지지되었다.

정보보안 위협의 이해도를 살펴보면 PC 부분 및 스마트폰 부분에서는 통계적으로 유의수준 0.01에서 정보보안 위협의 이해도가 정보보안 인식에 영향을 미치는 것으로 나타났다. 즉, 사용자가 PC 및 스마트폰 정보보안 위협에 대한 지식, 기술 등이 높을수록 정보보안 인식이 더 높다고 볼 수 있다. PC 부분의 결과는 Bulgurcu *et al.*(2010), Huang *et al.*(2010)의 연구와 동일하게 나타났다. 따라서, 스마트폰 부분의 결과도 PC 부분과 같이 유의하게 설명되었다. 즉, H2a(정보보안 위협의 이해도는 사용자의 PC 정보보안 인식에 긍정적인(+) 영향을 끼칠 것이다) 및 H2b(정보보안 위협의 이해도는 사용자의 스마트폰 정보보안 인식에 긍정적인(+) 영향을 끼칠 것이다)의 두 개 가설이 지지되었다.

정보보안 정책을 살펴보면 PC 부분 및 스마트폰 부분에서는 통계적으로 유의수준 0.05에서 정보보안 정책이 정보보안 인식에 영향을 끼치는 것으로 나타나지 않았다. 선행연구에서 Bulgurcu *et al.*(2010), Ryan(2006), Wolf(2010)의 연구와 결과가 일치하지 않아 H3a(정보보안 정책이 사용자의 PC 정보보안 인식에 긍정적인(+) 영향을 끼칠 것이다) 및 H3b(정보보안 정책이 사용자의 스마트폰 정보보안인식에 긍정적인(+) 영향을 끼칠 것이다)의 두 개 가설이 기각되었다. 이러한 결과가 나타난 이유는 학생들이 정보보안 정책에 대하여 잘 모르고 대학교에서도 정보보안 정책의 전달과 교육이 잘 이루어 지지 않았기 때문이라고 볼 수 있다.

정보보안 교육을 살펴보면 PC 부분 및 스마트폰 부분에서는 통계적으로 유의수준 0.01에서 정보보안 교육이 정보보안 인식에 영향을 끼치는 것으로 나타났다. PC 부분의 분석결과가 Decker(2008)의 연구와 일치하여 H4a(정보보안 교육이 사용자의 PC 정보보안 인식에 긍정적인(+) 영향을 끼칠 것이다)를 지지되었다. 또한, 스마트폰 부분에서도 PC 부분과 같이 유의하게 설명되었다. 즉, H4b(정보보안 교육이 사용자의 스마트폰 정보보안 인식에 긍정적인(+) 영향을 끼칠 것이다)가 지지되었다.

마지막으로 정보보안 의도를 살펴보면 PC 부분에서 통계적으로 유의수준 0.01에서 정보보안 의도는 정보보안 인식에 영향을 끼치는 것으로 나타났다. 이 결과는 장명희, 강다연(2012)의 연구와 일치하며 H5a(정보보안 의도는 사용자의 PC 정보보안 인식에 긍정적인(+) 영향을 끼칠 것이다)가 지지되었다. 하지만 스마트폰 부분은 통계적으로 유의수준 0.05에서 정보보안 의도는 정보보안 인식에 영향을 끼치는 것으로 나타나지 않았다. 즉, H5b(정보보안 의도는 사용자의 스마트폰 정보보안 인식에 긍정적인(+) 영향을 끼칠 것이다)가 기각되었다. 이 결과를 자세히 살펴보면 통계적으로 유의수준 0.1에서는 유의하다고 볼 수 있다. 즉, 유의수준 0.1에서 정보보안 의도는 스마트폰 정보보안 인식에 영향을 끼칠 것이다. 하지만 PC와 비교하면 사용자가 스마트폰 정보보안에 대해 중요하다고 생각하지만 실제로는 스마트폰에 대한 정보보안 의도가 부족하다고 볼 수 있다.

4.3.2 요인별 차이 비교

사용자의 PC 및 스마트폰에 대한 기본적인 기술, 정보보안 위협, 정보보안 정책, 정보보안 교육, 정보보안 행동, 정보보안 인식을 포함하는 6개 변수의 차이를 파악하기 위하여 대응표본 T 검증

〈표 3〉 T-Test 결과

구 분		Mean	Std. Deviation	Std. Error Mean	t
정보보안 인식	PC - 스마트폰	-.00602	.54392	.03744	-0.161
보안 기술의 이해도	PC - 스마트폰	.26303	.78498	.05404	4.867
보안 위협의 이해도	PC - 스마트폰	.07583	.71892	.04949	1.532
정보보안 정책	PC - 스마트폰	-.17062	.77858	.05360	-3.183
정보보안 교육	PC - 스마트폰	-.10782	.53222	.03664	-2.943
정보보안 의도	PC - 스마트폰	-.05024	.60280	.04150	-1.211

(Paired T-Test)을 실시하였다. 정보보안 인식, 기본적인 기술, 정보보안 위협, 정보보안 정책, 정보보안 교육, 정보보안 행동에 대한 T 검증의 결과는 <표 3>과 같다.

정보보안 인식을 살펴보면 PC와 스마트폰의 정보보안 인식은 차이가 있다고 볼 수 없다(t = -0.161). 즉, 사용자의 PC 정보보안에 대한 인식과 스마트폰 정보보안에 대한 인식이 비슷하게 나타났다. 이에 따라 가설 6(사용자의 PC와 스마트폰에 대한 정보보안 인식은 차이가 있을 것이다)은 기각되었다.

선행요인을 살펴보면 PC와 스마트폰에 대한 보안 기술의 이해도(t = 4.867), 정보보안 정책(t =-3.183), 정보보안 교육(t = -2.943)은 차이가 있다고 볼 수 있다. 따라서 정보보안 위협의 이해도(t = 1.532), 정보보안 의도(t = -1.211)는 차이가 있다고 볼 수 없다. 즉, H1c(사용자의 PC와 스마트폰에 대한 보안 기술의 이해도는 차이가 있을 것이다), H4c(사용자의 PC와 스마트폰에 대한 정보보안 정책은 차이가 있을 것이다), H5c(사용자의 PC와 스마트폰에 대한 정보보안 교육은 차이가 있을 것이다)는 지지되었고 H2c(사용자의 PC와 스마트폰에 대한 정보보안 위협의 이해도는 차이가 있을 것이다), H3c(사용자의 PC와 스마트폰에 대한 정보보안 의도는 차이가 있을 것이다)는 기각되었다.

먼저, 정보보안 인식 측면에서 살펴보면 사용자의 PC 및 스마트폰 정보보안 인식에 대한 수준이 모두 높게 분석되었다. 즉, 사용자는 PC 및 스마트폰 정보보안이 모두 중요하며, 필요하다고 생각한다. 따라서 비슷한 정보보안 인식수준에서 세부적으로 각 요인별 PC와 스마트폰 간의 차이가 있을 것인지를 살펴볼 필요가 있다. 보안 기술의 이해도에서 보면 PC가 스마트폰 보다 더 높다는 결과가 나타났다. Ryan(2006)의 연구에서 그는 사용자가 기술/도구 등에 대한 사용기간이 길수록 보안 기술의 이해도가 더 높다고 주장하였다. 사용자가 스마트폰 보다는 PC의 사용기간이 훨씬 더 길어 보안 기술의 이해도가 더 높다고 확신할 수 있다. 정보보안 위협의 이해도에서 살펴보면 사용자는 PC 및 스마트폰 정보보안 위협에 대해 모두 중요하다고 생각한다. 즉, 사용자는 PC 및 스마트폰 정보보안 위협의 중요성을 이해하며 두 플랫폼(Platform) 기반의 정보보안 위협에 대한 대응방법 등에 대한 지식 혹은 수준이 비슷하다고 볼 수 있다. 따라서 정보보안 정책측면에서 살펴보면 사용자는 PC 정보보안 정책 보다 스마트폰 정보보안 정책에 대하여 더 많이 알고 있으며 상대적으로 중요하다고 생각한다. 스마트폰은 편의성 때문에 PC보다 사용빈도가 더 높다. 또한, 스마트폰의 경우는 연락처, 사진 등의 개인 정보가 많아 사용자가 스마트폰 보안을 강화하기 위한 정보보안 정책에 더 많은 관심을 갖고 있다. 정보보안 교육 측면에서 보면 정보보안 정책과 동일하게 사용자는 스마트폰 정보보안 교육에 대해 더 많은 관심을 갖고 있으며 교육에 대한 수용의사가 높다. 마지막으로 정보보안 의도 부분에서는 PC 및 스마트폰이 비슷하게 나타났다. 이는

사용자가 PC보다는 스마트폰에 대한 정보보안 정책 및 교육이 더 중요하다고 생각하지만 실질적인 보안관련 의도에 있어서는 미흡하다는 의미로 해석할 수 있다.

V. 결 론

본 연구는 PC 및 스마트폰 중심으로 기술적 요인, 인적 요인 및 제도적 요인들에 있어 조직 구성원의 정보보안 인식에 끼치는 영향력을 살펴보고자 하였다. 따라서 보안 기술의 이해도, 정보보안 위협의 이해도, 정보보안 정책, 정보보안 교육 및 정보보안 의도의 5개 요인별로 조직 구성원에 대한 PC와 스마트폰 간의 차이를 분석하였다. 연구결과를 요약하면 다음과 같다. 첫째, 선행연구에서 도출된 보안 기술의 이해도, 보안 위협의 이해도 및 정보보안 교육 3가지 변수는 PC 및 스마트폰 정보보안 인식에 유의한 영향을 끼치는 것으로 검증되었다. 즉, 정보보안에 관련된 기술 및 위협에 대한 이해도가 높은 사용자는 정보보안 인식이 높다는 것이 확인되었다. 둘째, 정보보안 의도는 PC 정보보안 인식에 유의한 영향을 끼치는 것으로 밝혀졌다. 즉, 정보보안을 위하여 정보보안 절차나 정책을 잘 준수하고자 하는 사용자는 PC의 정보보안 인식이 더욱 높다는 점이 확인되었다. 셋째, 보안 기술의 이해도, 정보보안 정책 및 정보보안 교육에 있어 PC와 스마트폰 간의 차이가 있는 것으로 나타났다. 보안 기술의 이해도는 스마트폰보다 PC가 더 높고 정보보안 정책 및 정보보안 교육은 스마트폰이 더 높다는 것으로 분석되었다. 사용자의 스마트폰에 대한 보안 기술의 이해도는 부족하고 정보보안 정책 및 교육은 더욱 중요하게 인식하며 이에 대한 수용의사가 높다는 것으로 해석된다.

기존의 PC 정보보안에 대한 이슈가 지속적으로 발생하고 있지만 스마트폰의 발전 및 유행에 따라 정보보안 이슈가 더욱 빠르게 증가하고 있다. 선행연구를 살펴보면 스마트폰 정보보안 인식에 관한 연구가 드물다. 또한, PC 정보보안 인식에 관한 연구가 많지만 대부분 기업 차원에서 이루어진 연구다. 본 연구에서는 정보보안 인식에 관한 선행연구를 통하여 대학교의 학생을 대상으로 PC 및 스마트폰 두 부분에 적용할 수 있는 정보보안 인식 모델을 제시하였다. 따라서 이 모델을 활용하여 PC와 스마트폰 간의 차이를 분석할 수 있었다. 즉, 현재 상황에서 어떠한 요인에서 정보보안 인식에 대한 차이가 있는지를 검증하였으며 이를 통하여 사용자가 더욱 명확하게 요인별 차이를 파악하고 부족한 부분에 대한 정보보안 인식을 강화할 수 있다.

본 연구의 결과에 의하면 정보보안 정책이 정보보안 인식에 영향을 미치지 않는 것으로 나타났다. 이러한 결과가 나타난 이유는 설문조사가 주로 대학생을 대상으로 이루어졌으며 대학생들이 정보보안 정책을 상대적으로 잘 모르기 때문이라고 할 수 있다. 즉, 대학생들은 정보보안 정책의 중요성, 필요성 등에 대한 지식이 부족하다. 따라서 대학생들의 정보보안 정책에 대한 지식 혹은 인식을 높이기 위해서는 학교 및 관련 전문기관이 정보보안 정책을 효율적으로 전달 및 교육해야 한다고 생각한다. 또한, 정보보안 의도는 스마트폰 정보보안 인식에 영향을 미치는 것으로 나타나지 않았다. 이는 스마트폰 사용자가 정보보안이 중요하다고 생각하지만 실질적인 정보보안 의도는 부족하다고 볼 수 있다. 스마트폰 기능이 많아지면서 보안이슈가 더 심각해지는 추세이지만 아직까지 스마트폰 회사들은 기능 강화 및 다양화에 중점을 두고 있어 보안문제에 대한 사고의 전환 및 대처는 미흡하다. 향후 스마트폰 회사가 자사의 스마트폰 사용절차 등을 명확하게 명시하고 전달하면 사용자의 정보보안 의도가 더욱 높아 질 것이다. 마지막으로 사용자는 PC 및 스마트폰 정보보안에 대하여 중요하다고 생각하지만 실질적인 결과는 각 요인별로 차이가 있게 나타났다. 사용자가 스마트폰의 정보보안 정책 및 정보보안 교육에 대하여 더욱 중요하게 인식

하지만 보안 기술의 이해도는 PC가 더 높다. 이에 따르면 대학생 및 대학원생의 스마트폰 보안 기술의 이해도가 부족하여 다양한 채널을 통하여 보안 기술을 배우는 것이 중요하다고 할 수 있다.

나아가 본 연구에서는 대학생 및 대학원생의 PC 및 스마트폰 정보보안 인식을 측정하기 위하여 기존의 선행연구를 바탕으로 정보보안 인식을 측정할 수 있는 모형들을 살펴보았다. 그러나 선행연구에서는 대부분의 정보보안 인식에 대한 모형을 PC 중심으로 제시하였으며 스마트폰 정보보안 인식에 대한 모형은 제한적이었다. 그리고 대부분의 PC 정보보안 인식에 관한 연구들은 기업 차원에서 수행되었으며, 연구의 표본 대상이 한정된 대학생 및 대학원생 211명으로 구성되어 일반화에 대한 한계점이 있을 수도 있다. 또한, 응답자가 대부분 경영학과 학생이라 정보기술 및 정보보안에 대한 관심 및 지식이 상대적으로 많지 않아 정보보안 의도 수준이 낮을 수 있기 때문에 정보보안 인식에 부정적인 영향을 미칠 수 있다. 모든 응답자가 대학생이나 대학원생이라서 정보보안 정책을 상대적으로 중요하게 인식하지 않아 정보보안 인식에 부정적인 영향을 미쳤다고 볼 수 있다.

이상으로 향후 연구의 제안을 하면 다음과 같다. 먼저 표본의 수를 넓히고 다양한 학과, 직업, 국가 등을 포함하여 국가별 직업별로 보안 인식에 대한 차이를 비교할 수 있을 것이다. 본 연구에서는 대학생 및 대학원생의 PC 및 스마트폰 정보보안 인식을 측정하였으나 향후 연구에서는 좀 더 구체적인 영역에서 연구를 수행할 필요가 있다. 예를 들면 회사 내에서의 회사원에 대한 PC와 스마트폰 정보보안 인식간의 차이를 분석할 수 있다. 마지막으로, 스마트폰 기능의 다양화로 인하여 다양한 비즈니스 영역에서 스마트폰을 활용하고 있다. 최근 스마트폰 결제기능이 확산되어 정보보안 이슈가 더욱 증가할 것으로 예측되어 향후 4차 산업혁명의 추세에 맞는 스마트폰 정보보안 인식에 대한 연구를 추가적인 요인들을 고려하여 수행할 필요할 있을 것이다.

참 고 문 헌

[1] 강다연, 장명희, “정보보안정책 준수가 정보보안능력 및 행동에 미치는 영향 분석: 해운항만조직 구성원을 대상으로”, *한국항만정제학회지*, 제30집, 제1호, 2014, pp. 97-118.

[2] 김종기, 김재현, “개인사용자의 보안행위의도에 관한 실증연구: 개인 컴퓨터와 스마트폰의 비교를 중심으로”, *인터넷전자상거래연구*, 제14권, 제6호, 2014, pp. 45-69.

[3] 김종기, 전진환, “대기업과 중소기업 간의 정보보안 요소에 대한 사용자의 인지 비교: 컴퓨터 바이러스를 중심으로”, *한국정보보호학회지*, 제16권, 제5호, 2006, pp. 79-92.

[4] 박일형, 서승우, 이은동, “정보보안 향상을 위한 보안의식 조사결과 분석”, *한국경영학회 통합학술발표논문집*, 2009, pp. 1-7.

[5] 박진완, *스마트폰 악성코드 감염시 스마트폰 이용자의 피해 가능성 연구* (석사학위논문), 인천대학교, 2011.

[6] 박호현, *모바일 온리로 급변하는 ICT 시장*, 서울경제, 2014.

[7] 백민정, 손승희, “조직의 정보윤리실천이 구성원의 정보보안 인식과 행동에 미치는 영향에 관한 연구”, *한독경상논총*, 제28권, 제4호, 2010, pp. 119-145.

[8] 백민정, *정보윤리활동이 정보보안 성과에 미치는 영향에 관한 연구* (박사학위논문), 단국대학교, 2010.

[9] 송은수, *일반 컴퓨터 사용자의 정보보안에 대한 인식* (석사학위논문), 중앙대학교, 2006.

[10] 신현민, *정보보안 인식수준 평가 사례를 통한 측정지표 체계 수립에 관한 연구* (석사학위논문), 동국대학교, 2009.

[11] 신호영, *스마트폰 이용자들의 정보보안 행위에 관한 실증연구* (석사학위논문), 영남대학교, 2012.

[12] 안랩, *2014년 스마트폰 악성코드 통계*, 연구보고서, 2015.

[13] 왕혜민, “3세 이상 국민 인터넷 이용률 88.3% 육박 ‘스마트폰 직접적 영향’”, Break News, 2017. 02. 01., Available at http://www.breaknews.com/sub_read.html?uid=489441.

[14] 이기정, *정보보호관리체계 기반의 강화된 스마트폰 보안모델 연구* (석사학위논문). 서울과학기술대학교, 2012.

[15] 이기주, “스마트 사회의 보안 위협과 정보보호 정책추진에 관한 제언”, *한국인터넷진흥원 발표논문*, 2013, pp. 24-32.

[16] 이선중, 이미정, “정보보호문화의 평가지표에 관한 탐색적 연구”, *정보화정책*, 제15권, 제3호, 2008, pp. 100-119.

[17] 이중정, 김진, 이충훈, “정보보호관리체계(ISIS) 항목의 중요도 인식과 투자의 우선순위 비교 연구”, *한국정보보호학회지*, 제24권, 제5호, 2014, pp. 919-929.

[18] 이초희, “일상생활의 모바일化…스마트폰·태블릿 보유↑ 데스크톱↓”, 아시아경제 뉴스, 2014. 12. 30., Available at http://www.asiae.co.kr/news/view.htm?idxno=2014123010462842248.

[19] 이현동, *스마트폰 환경에서 MAUT와 퍼지 알고리즘을 이용한 상황인식 보안 시스템* (석사학위논문), 부경대학교, 2012.

[20] 장명희, 강다연, “항만기업 종사자들의 정보보안인식과 지각된 정보보안위험에 영향을 미치는 요인”, *한국항해항만학회지*, 제36권, 제3호, 2012, pp. 261-271.

[21] 정보통신부, *2006 국가정보보호백서*, 정보통신부, 2006.

[22] 정해철, 김현수, “조직구성원의 정보보안 의식과 조직의 정보보안 수준과의 관계 연구,” *정보기술과 데이터베이스 저널*, 제7권, 제2호, 2000, pp. 117-134.

[23] 진성철, “스마트폰 사용자 보안 불감증 심각”, LA중앙일보, 2017. 03. 16., Available at http://www.koreadaily.com/news/read.asp?art_id=5090368.

[24] 최민지, “절반 이상 개인 이용자, PC·스마트폰 보안피해 경험”, 디지털데일리, 2016.07. 14., Available at http://www.ddaily.co.kr/news/article.html?no=145311.

[25] 황인호, 김대진, 김태하, 김진수, “조직의 정보보안 문화 형성이 조직 구성원의 보안 지식 및 준수의도에 미치는 영향 연구”, *Information Systems Review*, 제18권, 제1호, 2016, pp. 1-23.

[26] KT경제경영연구소, *2015년 모바일 트렌드 전망*, 연구 보고서, 2015.

[27] 360 Internet Security Center, *2014 Smartphone Security Reports in China*, 360 Reports, 2015.

[28] Bulgurcu, B., H. Cavusoglu, and I. Benbasat, “Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness”, *MIS Quarterly*, Vol.34, No.3, 2010, pp. 523-548.

[29] Cavusoglu, H., J. Son, and I. Benbasatm, “Information Security Control Resources in Organizations: A Multidimensional View and Their Key Drivers”, *UBC Working Paper*, 2009.

[30] Choi, N., D. Kim, and A. Whitmore, “Knowing is doing”, *Information Management and Computer Security*, Vol.16, No.5, 2008, pp. 484-501.

[31] Decker, L. G., *Factors Affecting the Security Awareness of End-Users* (Doctoral Dissertation), Capella University, 2008.

[32] Dinev, T. and P. Hart, “Internet privacy concerns and social awareness as determinants of intention to transact”, *International Journal of E-Commerce*, Vol.10, No.2, 2006, pp. 7-31.

[33] Facebook, “Financial results for the quarter ended September 30”, 2014, Facebook Reports Third Quarter 2014 Results, 2014.

[34] Hawkins, S., D. C. Yen, and D. C. Chou, “Awareness and challenges of internet security”, *Information Management & Computer Security*, Vol.8, No.3, 2000, pp. 131-143.

[35] Holbert, D. A., *Factors Contributing to Security*

Awareness of the end User (Doctoral Dissertation), Capella University, 2013.

[36] Huang, D. L., P. L. Rau, and G. Salvendy, "Perception of information security", *Behaviour & Information Technology*, Vol.29, No.3, 2010, pp. 221-232.

[37] Petrova, K. and R. Sinclair, "Expanding the understanding: Transactions and security awareness for eBusiness students", *New Zealand Journal of Applied Computing and Information Technology*, Vol.7, No.1, 2003, pp. 82-88.

[38] Rhee, H. S., C. Kim, and Y. U. Ryu, "Self-efficacy in information security: Its influence on end users' information security practice behavior", *Computers & Security*, Vol.28, No.8, 2009, pp. 816-826.

[39] Ryan, J. E., *A Comparison of Information Security Trends between Formal and Informal Environments* (Doctoral Dissertation), Auburn University, 2006.

[40] Solms, V. and T. Kerry, "Information security obedience: A definition", *Computers & Security*, Vol.24, No.1, 2005, pp. 69-75.

[41] Spurling, P., "Promoting security awareness and commitment", *Information Management & Computer Security*, Vol.3, No.2, 1995, pp. 20-26.

[42] Vance, A., M. Siponen, and S. Pahnila, "Motivating IS security compliance: Insights from habit and protection motivation theory", *Information & Management*, Vol.49, No.3-4, 2012, pp. 190-198.

[43] Wiant, T. L., "Information security policy's impact on reporting security incidents", *Computer & Security*, Vol.24, No.6, pp. 448-459.

[44] Wolf, M. J., *Measuring an Information Security Awareness Program* (Master's Thesis), University of Nebraska, 2010.

Information Systems Review
Volume 19 Number 3
September 2017

The Study on the Difference of Information Security Awareness between PC and Smartphone

Piao Zhengxian* · Sungmin Kang**

Abstract

In the information age, the rapid development of information technology provides people with an enriching experience yet also causes them harm because of information security (IS) issues. The IS of smartphones faces great challenges. Although many studies on IS awareness have been conducted, most of them have focused on PCs and do not consider the security issues of smartphones. In this study, we focus on those factors that affect IS awareness for both PCs and smartphones. We also analyze the differences in the impacts of certain factors on PCs and smartphones based on the proposed research model.

The results are summarized as follows. First, the understanding of security technique, understanding of IS threat, and IS education have significant impacts on IS awareness for PCs and smartphones, while IS intention has a significant impact on IS awareness for PCs but not for smartphones. Moreover, IS policy has no significant impact on IS awareness. Second, PCs and smartphones show no significant differences in IS awareness, IS threat, and IS intention, but show significant differences in understanding of security technique, IS education, and IS policy.

Keywords: Smart Age, IS Threat, IS Education, IS Intention, IS Policy, IS Awareness

* Graduate of Dept. of Business Administration, Graduate School, Chung-Ang University
** Corresponding Author, College of Business and Economics, Chung-Ang University

◐ 저 자 소 개 ◑

박 정 현 (zh-park@hotmail.com)

중앙대학교에서 일반대학원 경영학과 석사(MIS)를 취득하였으며 현재 cafe24에서 근무하고 있다.

강 성 민 (smkang@cau.ac.kr)

현재 중앙대학교 경영경제대학 경영학부 교수로 재직 중이며, 미국의 카네기멜론 대학에서 경영학 학사 및 석사(MBA) 학위를 받았으며 텍사스 주립대에서 경영정보학(MIS) 박사학위를 취득하였다. 연구 관심 분야는 전자상거래, 정보기술의 전략적 활용, 사용자 편의성 및 컴퓨팅, 모바일 컴퓨팅, 지식경영, 정보기술 도입 및 조직적 영향 등이며, 관련 논문들을 국내/외 학술지 및 컨퍼런스에 실은 바 있다.

논문접수일 : 2017년 03월 27일 **게재확정일 : 2017년 09월 08일**
1차 수정일 : 2017년 06월 27일