韓國IT서비스學會誌
第13卷 第2號
2014年 6月, pp.1-17
http://dx.doi.org/10.9716/KITS.2014.13.2.001

소셜 네트워크 서비스의 보안기능 사용의도에 영향을 미치는 요인 : Facebook을 중심으로

김 협* · 김경규** · 이 호***

Factors Affecting Intention to Use Security Functions in SNS

Hyeob Kim* · Kyung Kyu Kim** · Ho Lee***

■ Abstract ■

Social networking service (SNS) is a service that allows people to share information, manage relationships with others, and express themselves on the Internet. The number of SNS users have increased explosively with the growth of mobile devices such as smartphones. As the influence of SNS has grown extensively, potential threats to privacy have also become pervasive. The purpose of this study is to empirically examine the main factors that affect users' intentions to use security functions provided by their SNS. The main theories for this study include the rational choice theory and the theory of planned behavior. This study has identified the factors that affect intention to use security functions. In addition, security function awareness and information security awareness are found to be important antecedents for intention to use security functions. The results of this study implies that when SNS providers develop security policies, they should consider the ways to improve users information security awareness and security function awareness simultaneously.

Keyword : Social Networking Service, Facebook, Safety of Information, Privacy Concern, Security Vulnerability, Information Security Awareness, Security Function Awareness

논문투고일 : 2014년 01월 24일 논문수정완료일 : 2014년 04월 01일 논문게재확정일 : 2014년 04월 04일

* 연세대학교 정보대학원 석사
** 연세대학교 정보대학원 교수, 교신저자
*** 연세대학교 정보대학원 박사

1. 서 론

소셜 네트워크 서비스(Social networking service, SNS)는 웹 2.0의 확산 및 스마트기기의 보급으로 주요 커뮤니케이션 채널로서 각광받고 있다. SNS는 인터넷을 기반으로 사람과 사람을 연결하고 정보공유, 인맥관리, 자기표현 등을 통해 타인과의 관계를 관리할 수 있는 서비스로서, 사람들의 생각이나 감정 등을 쉽게 표현할 수 있는 의사소통 수단으로써 사용되고 있다[14].

ECAR(EDUCAUSE Center for Applied Research)에서 진행한 연구에 따르면 85.2%의 응답자들이 SNS를 사용한 경험이 있고, 56.8%의 응답자들은 SNS를 매일 사용하는 것으로 조사되었다[16]. 링크드인(LinkedIn), 마이스페이스(Myspace), 페이스북(Facebook) 등의 다양한 SNS 중에서도 2004년부터 시작된 페이스북은 전 세계적으로 10억 명 이상의 이용자를 보유하고 있으며 가장 인기 있는 SNS로 각광받고 있다[28]. 특히, 페이스북은 SNS의 기본적인 기능 및 특성과 더불어 사회적 상호작용을 반영하고, 개인의 정체성을 나타내는 창구의 역할을 함으로써, 사람간의 관계 형성에 큰 역할을 하고 있다[1, 16].

SNS의 활용 및 중요성이 점차 커짐에 따라 2011년 페이스북에서 악성 웹 링크를 이용하는 쿱페이스(koobface) 등의 악성코드에 의한 공격, 2010년 트위터로 위장한 성인 약품광고 스팸 메일 유포, 트위터를 이용한 봇넷 구성과 조정 등 개인정보의 부적절한 접근, 루머나 가십과 같은 평판의 손상, 스토킹, 제 3자에 의한 개인정보의 사용 그리고 해킹과 ID 탈취, 사생활 침해, 개인정보 유출 등 보안 관련 문제들이 증가하게 되었다[14].

이러한 보안 위협에 대응하기 위해 SNS 제공자들은 다양한 보안정책을 수립하고 보안 기능을 이용자에게 제공하고 있다[2]. 하지만 개인 이용자 차원에서의 Security, Privacy 등 SNS 보안에 관한 실증적 연구는 아직까지 미미한 상황이다. 기존 SNS에 관한 연구는 기업조직에서 마케팅 활용, 기술 개발적인 차원에 초점이 맞추어져 있었기 때문이다[26]. 더욱이, 기존에 있는 소수의 개인 이용자 차원에서의 보안 관련 연구들조차, 정보보안 인식의 영향력에만 초점을 맞추고 있다[15]. 그러나 정보보안 자체에 대한 인식뿐만 아니라 실제 보안을 가능하게 하는 보안 기능에 대한 인식 또한 중요한 변수이다. 이러한 보안 기능 인식의 중요성에도 불구하고 관련 연구가 매우 부족한 상황이다. 때문에, 본 연구는 정보보안 인식과 더불어 보안 기능 인식에도 초점을 맞추어 진행하려고 한다. 이는 기존의 정보보안 자체에 편향된 연구에서 보안 기능을 함께 고려하여 보안에 대한 이해를 강화하는 학술적 의의가 기대된다. 실무적으로는 실제 이용자를 대상으로 한 실증적인 분석을 통해 SNS 제공자가 효과적인 보안 정책을 수립하여 운영하는 측면에 도움이 될 것이다.

본 연구는 페이스북 사용 경험이 있는 이용자를 대상으로 보안기능을 사용하는 주요 요인들을 계획된 행동 이론(The Theory of Planned Behavior)과 합리적 선택 이론(Rational Choice Theory)을 접목시켜 만든 프레임워크를 적용하여 검증하고자 한다. 본 연구의 연구 질문은 다음과 같다.

첫째, 이용자들이 SNS의 보안기능을 사용하려는 의도에 영향을 주는 주요 요인은 무엇인가?

둘째, 정보보안 인식, 보안기능 인식이 보안기능 사용의도에 영향을 주는 주요 요인과 보안기능 사용에 대한 태도를 형성하는데 어떠한 영향을 주는가?

2. 이론적 배경

2.1 소셜 네트워크 서비스의 보안기능

SNS 관련 보안위협의 증가에 따라 EU 보안전문기관인 유럽 네트워크 정보보안청(ENISA)에서는 SNS에서의 보안 위협을 다음 <표 1>과 같이 네 가지의 범주로 분류하고 있다[4].

〈표 1〉 SNS에서의 주요 보안 위협분류

보안위협	세부내용
프라이버시 위협	◦ 개인프로파일 수집 ◦ 2차 데이터 수집 ◦ 얼굴 인식 ◦ 콘텐츠 기반 이미지 검색 ◦ 완전한 계정 삭제의 어려움
기존 네트워크 보안 위협	◦ SNS 스팸 ◦ XSS, 웜, 바이러스
ID 관련 위협	◦ SNS를 이용한 피싱 ◦ 네트워크 침입을 통한 정보유출 ◦ ID 도용에 의한 프로파일 위조 및 명예훼손
사회적 위협	◦ 사이버 스토킹 ◦ 사이버 괴롭힘 ◦ 산업스파이

따라서 <표 1>과 같은 보안위협들에 대응하여 SNS 제공자들은 다양한 보안정책을 수립하고 있다. 하지만 다양한 보안위협으로부터 이용자들을 보호하기에 보안정책만으로는 충분하지 않다[6]. 이는 실제 이용자가 보안 정책을 인지한다고 해서 제공된 보안 기능들이 어떠한 역할을 하는지는 알 수 없기 때문이다. 따라서 보안위협에 대응하기 위해서는 보안정책 인식과 더불어 보안 기능에 대한 인식을 동시에 고려할 필요가 있다. 보안기능은 SNS의 안전한 참여를 장려하기 위해 사용자 친화적인 프로필 제어 및 설정을 가능하게 도움을 주는 개인정보 보호의 통제 기술의 구현이다[35].

하지만 전술한 바와 같이 다수의 이용자들은 정보보안에 대한 인식뿐만 아니라 보안기능 자체에 대한 인식이 부족한 상황이다. 이렇게 보안 기능 인식이 보안에 중요한 영향을 미침에도 불구하고, 기존의 연구들에서는 보안 기능 인식에 대한 중요성을 간과하고 있다. 페이스북과 관련한 연구에서는 소수의 이용자들만이 기본 보안설정을 변경한 것으로 나타났다[5]. 따라서 본 연구에서는 이용자들의 정보보안 인식과 더불어 보안기능 인식에도 초점을 맞추어 연구를 진행하고자 한다.

다음의 <표 2>는 본 연구의 대상인 페이스북의 보안기능 및 내용이다.

〈표 2〉 페이스북의 보안기능 및 내용

구 분	기능	내용
보안 설정	안전한 브라우징	가능한 경우에는 언제나 보안 연결 상에서 페이스북을 이용
	로그인 알림	이전에 사용하지 않은 컴퓨터나 휴대 장치에서 계정이 접속되면 알림 ⇒ 이메일, SMS, 푸시
	로그인 승인	알 수 없는 브라우저에서 계정에 접속하려면 보안 코드가 필요. ⇒ 보안 코드는 SMS로 전달
	코드 생성기	보안 코드를 받기 위한 것
	앱 비밀번호	계정 비밀번호 외에 개별적인 앱을 사용 시에 적용하는 비밀번호
	믿을 수 있는 연락처	계정에 접근하는 데 문제가 있을 때 안전하게 도울 수 있는 친구 리스트
	인증 기기	페이스북에 접속한 기록이 있는 기기 내역
	로그인 내역	기기 이름, 위치, 기기 유형 별 로그인 내역
공개 범위 설정	콘텐츠 공개 범위 설정	향후 게시물을 볼 수 있는 대상을 분류
		본인의 게시물과 본인이 태그 된 게시물 검토
		지금까지 친구의 친구 또는 전체 공개로 공유한 게시물의 공개 대상을 제한하는 여부
	연락 가능 범위 설정	본인에게 친구 요청을 보낼 수 있는 대상 분류
		본인에게 페이스북 메시지를 보낼 수 있는 대상 분류
	검색 가능 범위 설정	본인이 제공한 이메일 주소로 본인을 찾을 수 있는 대상 분류
		본인이 제공한 전화번호로 본인을 찾을 수 있는 대상 분류
		다른 검색 엔진을 타임라인과 연결 여부

2.2 계획된 행동 이론

Ajzen[7]은 합리적 행동 이론(TRA : Theory of Reasoned Action)을 보완하기 위해 지각된 행동통제(Perceived behavioral control)를 포함시켜 계획된 행동 이론을 개발하였다. 계획된 행동 이론에

서는 행동을 하려는 의도에 따라 직접적인 행동이 결정된다고 가정하였고, 이러한 행동을 하려는 의도가 행동에 대한 태도(attitude toward the behavior), 주관적 규범(subjective norm), 지각된 행동 통제(perceived behavioral control)의 세 가지 요인에 의해서 결정된다고 보았다[8].

Technology Acceptance Model(TAM)과 같이 계획된 행동 이론에 기반 한 정보시스템 관련 기존연구들은 행동에 대한 태도(attitude toward the behavior)와 이러한 태도를 결정하는 선행 변수들에만 초점을 맞추고 있다. 이는 TRA나 TAM이 개발될 당시에는 대부분의 정보시스템이 무조건 적으로 수용해야하는 필수재적인 성격보다는 상황에 따라 수용 할 수 있는 보완재적인 성격을 가지고 있었기 때문이다. 현재 정보시스템이 필수재가 되고 있는 현재에는 주관적 규범(subjective norm), 지각된 행동 통제(perceived behavioral control)등의 사회적 영향에 의한 변수들도 추가적으로 고려한 연구들이 많아지고 있다[8, 10, 12].

그러나 본 연구의 대상인 SNS, 특히 페이스북, 의 경우에는 자발적인 이용을 전제로 하기 때문에 필수재라고 보기는 어렵다. 따라서 본 연구에서는 행위의 태도가 행위를 하려는 의도를 결정하는 주요 요소라는 관점을 가지고 진행하려고 한다. 하지만 계획된 행동 이론은 행동의 태도를 결정하는 선행 요소들을 구체적으로 제시하지 못했다는 부분을 단점으로 지적받고 있다[15]. 따라서 본 연구에서는 계획된 행동 이론을 기반으로 혜택과 비용의 이성적 판단에 따라 행위가 결정된다는 합리적 선택 이론을 본 연구의 프레임 워크에 추가하였다.

2.3 합리적 선택 이론

합리적 선택 이론(Rational Choice Theory, RCT)에 따르면, 행위자가 어떠한 행동을 할때, 혜택(benefit)과 비용(cost)의 균형(Balancing)에 의해 그 행동을 결정한다고 보고 있다[29].

행위자는 합리적 결정 과정에서 행동을 선택하게 되는데, 우선 다양한 방안을 인식하게 되고 그 이후에 행동에 대한 결과를 고려하게 된다[32]. 마지막으로 최적의 대안을 결정하기 위해 혜택과 비용의 전반적인 평가를 통해 최종적인 행동을 결정하게 된다.

본 연구에서는 태도를 결정하는 선행 요소들을 구체적으로 제시하지 못했다는 계획된 행동 이론을 보완하기 위해, 합리적 선택 이론의 관점에서 SNS의 보안에 대한 인식과 보안 기능에 대한 인식이 어떠한 혜택과 비용을 발생하는 지를 범주화 고 이것이 결국 행위자의 태도를 결정한다고 보았다. 또한 보안 기능에 대한 인식의 경우, 사용 후에만 그 비용을 사용자들이 인식할 수 있기 때문에 미사용 시의 비용(Costs of Nonuse)과 사용 시의 비용(Costs of use)을 구분하여 살펴보았다. 이는 합리적 선택 이론을 채용한 기존의 대부분의 연구들이 혜택과 비용의 단순한 구분만을 한 것에서 확장하여, 사용 시 고려되는 비용과 미사용 시에도 예상 될 수 있는 비용으로 구분하여 합리적 선택이론의 비용 부분을 확장한 의의도 기대된다.

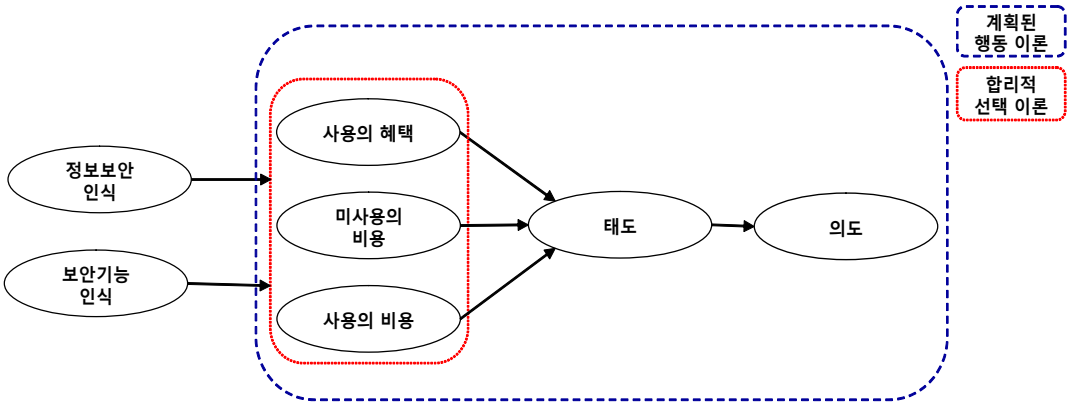
2.4 개념적 프레임워크

본 연구의 전체 개념적 프레임워크(Conceptual Framework)는 다음의 [그림 1]과 같다.

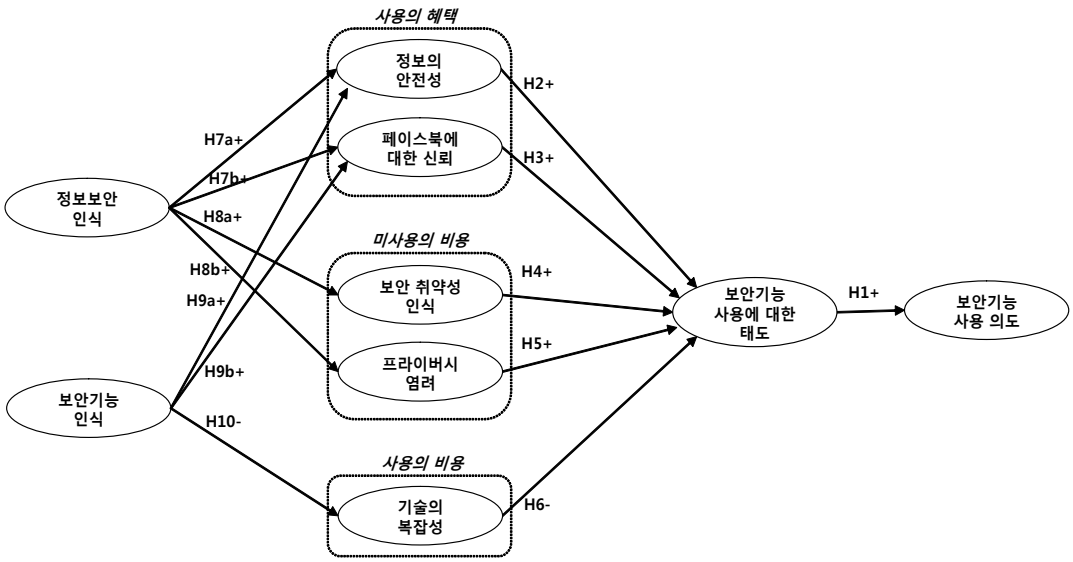
3. 연구 설계

3.1 연구 모형

본 연구는 지금까지 논의된 개념들과 이론들을 고려하여 SNS의 보안기능 사용의도에 관한 연구모형을 개발하였다. 보안기능 사용의 혜택으로 정보의 안전성과 페이스북에 대한 신뢰를 설정하였다. 또한 보안기능 사용의 비용과 관련하여 정보보안 인식에 영향을 받는 비용 요인들을 미사용의 비용으로 실제 사용을 해야 느끼는 보안 기능 인식에 영향을 받는 비용 요인을 사용의 비용으로



[그림 1] SNS 보안기능 사용의도에 관한 요인 프레임워크 구성



[그림 2] 연구 모형

구분 하였다. 또한, 보안기능 미사용 비용에는 보안 취약성 인식, 프라이버시 염려의 요인을, 보안기능 사용 비용에는 기술의 복잡성을 주요 요인으로 보았다. 이를 정리하면 [그림 2]와 같다.

3.2 연구 가설 설정

3.2.1 보안기능 사용에 대한 태도(Attitude)

보안기능 사용에 대한 태도는 페이스북의 보안기능에 대한 이용자의 성향(dispositions)을 나타낸다[13]. 계획된 행동 이론에 기반 한 기존의 선행연구들에서는 태도(attitude)가 의도(intention)에 긍정적인 영향을 미친다는 결과들이 다수 존재한다[8, 9, 21]. 또한 조직에서의 정보보안 정책 준수와 관련한 연구에서는 정책 준수에 대한 태도가 정보보안 정책 준수의도에 긍정적인 영향을 미치는 것으로 나타났다[15]. 특정 행위를 하려는 의도는 결국 그 행위에 대해 어떠한 태도를 갖느냐에 따라 결정되게 된다. 이를 바탕으로 다음과 같은 가설을 설정하였다.

H1 : 보안기능 사용에 대한 태도는 보안기능 사용의도에 긍정적인 영향을 미칠 것이다.

3.2.2 정보의 안전성(Safety of Information)

정보의 안전성은 페이스북의 보안기능을 사용함으로써 이용자의 정보가 안전하게 보호된다고 느끼는 인식의 정도를 의미한다[15]. 일반적으로 행동을 수행함에 있어 좀 더 안전성을 느끼게 되는 방법에 대해 긍정적인 태도를 형성하게 된다[15, 36]. 결국, 보안기능을 사용함으로써 얻는 혜택인 개인정보에 대한 안전성이 보안기능을 사용하려는 태도에 긍정적인 영향을 미칠 것이다. 이를 바탕으로 다음과 같은 가설을 설정하였다.

H2 : 정보의 안전성은 보안기능 사용에 대한 태도에 긍정적인 영향을 미칠 것이다.

3.2.3 페이스북에 대한 신뢰(Trust in Facebook)

페이스북에 대한 신뢰는 이용자가 보안위험 상황하에서 페이스북을 사용함에 따라 발생할 수 있는 위험을 감수하려는 정도를 의미한다[16, 34].

SNS 환경에서는 사이버 스토킹(cyber Stalking), 피싱(phishing) 등의 보안위험이 내포되어 있기 때문에 신뢰는 정보시스템 연구에서 정보시스템이나 서비스의 사용의도에 영향을 미치는 주요 요인 중의 하나로 여겨지고 있다[14, 24, 36]. 이용자들은 특정 서비스를 이용할 때 어느 정도의 보안 위험을 인지하게 된다. 이러한 보안 위험의 정도는 보안 기능에 대한 신뢰라기보다는 서비스 자체에 대한 신뢰에 영향을 받게 된다. 예를 들어, 특정 서비스에 개인 정보를 입력하지 않는 것은 서비스가 제공하는 보안기능에 대한 신뢰가 존재하지 않는 것이 아니라, 특정 서비스에 대한 신뢰가 없기 때문이다. 결국, 서비스 자체에 대한 신뢰는 보안 기능사용에 대한 태도를 결정을 짓는 주요 요인이 될 것이다. 이를 바탕으로 다음과 같이 가설을 설정하였다.

H3 : 페이스북에 대한 신뢰는 보안기능 사용에 대한 태도에 긍정적인 영향을 미칠 것이다.

3.2.4 보안 취약성 인식(Perceived Security Vulnerability)

취약성은 정보보안에서 중요한 개념으로 위협이 발생한 상태에서 현재 상태를 잃어버리거나 안전하게 관리할 수 없는 상태이거나 통제를 할 수 없는 상태를 말한다. 특히, 보안 취약성 인식은 페이스북의 보안기능을 사용하지 않음으로써 이용자의 정보가 보안 위험에 노출된다는 인식의 정도이다[15, 33]. 결국, 보안기능을 사용하지 않을 때 발생할 수 있는 위험이 늘어나면 날수록, 예상되는 위험을 방지하기 위해 보안기능을 사용하려고 한다. 따라서 보안 취약성 인식이 증가한다면 보안기능에 대한 태도를 형성하는데 긍정적인 영향을 미칠 것이다. 이를 바탕으로 다음과 같이 가설을 설정하였다.

H4 : 보안 취약성 인식은 보안기능 사용에 대한 태도에 긍정적인 영향을 미칠 것이다.

3.2.5 프라이버시 염려(Privacy Concern)

프라이버시 염려는 이용자의 정보가 저장, 감시, 검색 등에 이용될 것이라고 느끼는 염려의 정도를 의미한다[18, 19, 30]. SNS 환경에서는 개인 사진의 공개 등을 통한 자발적인 정보공개를 통해 프라이버시 염려가 더욱 증가하고 있는 추세이다.

SNS 이용자들은 서비스 이용과정에서 어느 정도의 프라이버시 염려를 가지게 되면서 자신의 프라이버시 보호를 위한 다양한 행동을 취하게 된다[22]. 다시 말해, SNS 서비스를 이용하면 할수록 공개된 개인 정보의 양은 늘어나게 되고, 이에 따른 프라이버시 침해에 대한 우려는 증가하게 된다. 결국, 프라이버시 침해를 방지하지 위해, 이용자는 보안기능 사용에 긍정적인 태도를 가지게 된다. 이를 바탕으로 다음과 같이 가설을 설정하였다.

H5 : 프라이버시 염려는 보안기능 사용에 대한 태도에 긍정적인 영향을 미칠 것이다.

3.2.6 기술의 복잡성(Technical Complexity)

특정 기술이나 서비스의 사용이 쉽다면, 다시 말해 사용 용이성이 확보된다면 당연히 그 기술이나 서비스 사용에 대한 태도는 긍정적일 것이다[20, 25]. 반면에 특정 기술이나 서비스가 이해하거나 사용하기가 어렵다고 느낀다면, 그 기술이나 서비스 사용에 대한 태도 또한 부정적일 수밖에 없다. 기술 복잡성은 페이스북의 보안기능을 이해하고 사용하기가 상대적으로 어려운 것으로 인식되는 정도를 의미한다[20, 25]. 특히, 강제성이 없는 선택적인 서비스의 경우, 이러한 기술 복잡성은 기술 사용에 대한 태도에 막대한 영향을 주게 된다. 따라서 이용자들이 보안기능 사용 시에 정신적이나 물리적으로 어려움을 느낀다면 많은 사용을 기대할 수 없을 것이다. 이를 바탕으로 다음과 같이 가설을 설정하였다.

H6 : 기술의 복잡성은 보안기능 사용에 대한 태도에 부정적인 영향을 미칠 것이다.

3.2.7 정보보안 인식(Information Security Awareness; ISA)

정보보안 인식(ISA)은 이용자가 일반적으로 인식한 정보보안과 관련된 지식의 정도이다[15]. 페이스북 보안기능 사용에 있어 정보보안 인식은 중요한 역할을 수행한다[5]. 정보보안 인식은 발생할 가능성이 있는 보안 위협을 이용자들에게 인지시켜 보안기능의 사용을 유도 시킬 수 있다. 또한, 정보 보안에 대한 인식이 높으면 높을 수록정보 보안기능을 사용 할 때 생기는 혜택과 보안 기능을 사용하지 않았을 때 발생하는 비용에 대한 정확한 판단을 할 수 있게 된다. 따라서 정보보안 인식은 보안기능 사용의 혜택과 보안 기능 미사용의 비용 영향을 미치게 된다.

3.2.7.1 정보보안 인식과 보안기능 사용의 혜택

이용자들이 정보보안과 관련된 지식의 수준이 높다면, SNS에서 제공하는 보안관련 기능, 정책이 적절한지에 대한 판단의 기준이 될 수 있을 것이다. 예를 들어, 특정 SNS에서 제공하는 보안 기능이 가져다주는 혜택(프라이버시 보호 등)에 대해 인지하기 쉬울 것이다[5]. 특정 SNS가 적절한 정보보안을 제공한다면, 많이 알아야 많이 볼 수 있다는 말과 같이, 정보보안에 대한 인식이 높을수록 이용자의 정보가 안전하게 보호된다고 느끼는 인식인 정보의 안정성에 긍정적인 영향을 미칠 것이다. 또한, 높은 정보보안 지식수준은 SNS 자체에 대한 신뢰도 강화 시킬 것이다. 이를 바탕으로 다음과 같이 가설을 설정하였다.

H7a : 정보보안 인식은 정보의 안전성에 긍정적인 영향을 미칠 것이다.

H7b : 정보보안 인식은 페이스북에 대한 신뢰에 긍정적인 영향을 미칠 것이다.

3.2.7.2 정보보안 인식과 보안기능 미사용의 비용

이용자들이 정보보안에 대해 일반적으로 인식하고 있는 지식의 정도가 클수록 보안 침해시의 피해에 대한 인지가 커지게 된다[3, 15]. 결국 보안에 대한 지식이 크면 클수록 보안 기능을 사용하지 않았을 때 발생할 수 있는 보안 취약성 인식이나 프라이버시 침해 등을 더욱 심각하게 생각하게 된다. 이를 바탕으로 다음과 같이 가설을 설정하였다.

H8a : 정보보안 인식은 보안 취약성 인식에 긍정적인 영향을 미칠 것이다.

H8b : 정보보안 인식은 프라이버시 염려에 긍정적인 영향을 미칠 것이다.

3.2.8 보안기능 인식(Security Function Awareness; SFA)

보안기능 인식(SFA)은 페이스북에서 제공하는 보안기능에 대해 이용자가 인식한 이해의 정도이

다. 본 연구에서 보안기능이란 페이스북에서 제공하고 있는 보안 설정 및 프라이버시 설정(공개 범위설정)의 16가지 기능을 의미한다[2]. 어떠한 보안 기능이 있는지, 혹은 보안 기능이 어떠한 역할을 하는지 모르는 이용자들은 SNS 제공자들이 설정해 놓은 기본 값을 변경하지 않을 가능성이 높다[35]. 또한, 보안 기능을 설정하는 방법이 어렵거나 보안 기능 설정 위치를 찾기 힘들다면, 보안 기능의 존재 여부 자체도 모를 수 있다. 결국 보안기능은 실제 보안 기능이 어떠한 역할을 하는지 사용해 보거나 혹은 보안 기능을 설정하기 위해 찾아보지 않는 다면, 그 기능을 사용했을 때 또는 찾기 위해 발생할 수 있는 어려움(비용)을 알 수 없게 된다. 따라서 본 연구에서는 보안기능에 대한 인식이 보안기능 사용의 혜택과 사용의 비용에 영향을 주는 요인으로 보았다.

3.2.8.1 보안인식 기능과 보안기능 사용의 혜택

이용자들이 SNS 보안위협에 대응할 수 있는 유일한 방법은 SNS에서 제공하는 보안기능을 사용하는 것이다. 이용자들이 보안기능에 대한 인식의 정도가 크다면 보안기능을 사용함으로써 얻는 혜택에 대한 이해도가 높아 질 것이다[3]. 페이스북에서 제공하는 보안 기능에 대한 이해가 높을수록 보안 기능을 사용함으로써 얻게 되는 정보의 안전성에 대한 인식이 높아지게 된다. 또한, 이러한 보안 기능에 대한 이해는 페이스북의 보안 유지 노력을 이해하게 됨으로써 페이스북 신뢰에도 긍정적인 영향을 미칠 것이다. 이를 바탕으로 다음과 같이 가설을 설정하였다.

H9a : 보안기능 인식은 정보의 안전성에 긍정적인 영향을 미칠 것이다.

H9b : 보안기능 인식은 페이스북에 대한 신뢰에 긍정적인 영향을 미칠 것이다.

3.2.8.2 보안인식 기능과 보안기능 사용의 비용

보안기능에 대한 인식의 정도가 높다는 것은 SNS 사이트에서 제공하는 보안기능에 대한 지식이 많다는 것이다[2, 3]. 지식의 정도에 따라 보안기능을 사용할 때 발생하는 비용인 기술의 복잡성(사용의 어려움)을 감소시켜주는 역할을 할 수 있을 것이다. 이를 바탕으로 다음과 같이 가설을 설정한다.

H10 : 보안기능 인식은 기술의 복잡성에 부정적인 영향을 미칠 것이다.

4. 연구 분석 및 결과

4.1 자료수집 및 표본의 특성

4.1.1 자료의 수집

본 연구에서는 연구 가설의 실증을 위하여 설문서를 통해 연구 자료를 수집하였다. 본 연구의 설문서에 사용된 척도는 모두 선행연구를 통해 검증된 설문항목들로 응답자의 인구통계학적인 사항들을 제외한 모든 문항은 리커트(Likert) 7점 척도를 사용하여 측정하였다.

설문항목은 문헌연구 및 기존 조사도구들을 참고로 연구목적에 맞게 작성하였고, 설문항목의 타당성과 신뢰성을 검증하기 위해 페이스북을 사용해본 경험이 있는 대학원생 30명을 대상으로 사전조사(pretest)를 실시하여 응답자가 명확하게 이해하기 힘들다고 지적하거나, 영문 척도를 한글로 번역하는 과정에서 어색한 느낌을 주는 항목은 원문을 참고하여 본 연구에 적합하게 수정하였다.

연구 자료의 수집을 위해 설문 대상자는 페이스북을 사용하고 있거나 경험이 있는 개인을 대상으로 하였고, 구글 문서도구(Google Docs)를 이용하여 온라인 방식으로 설문을 진행하였다.

본 연구의 설문대상에 적합하도록 페이스북을 사용한 경험여부를 먼저 파악한 뒤 설문을 진행하였으며 본 연구의 대상인 페이스북에 설문지를 업로드한 뒤 지인들을 통한 공유와 뉴스피드, 카카오톡을 활용하여 이용자들에게 설문을 의뢰하였다. 설

문조사는 2013년 11월 15일부터 11월 19일까지 5일 동안 수행되었고, 회수된 설문지는 총 314부이며 회수된 설문지 중에서 같은 척도로만 응답하거나 미 기입한 경우 등 불성실한 응답으로 사용이 불가능하다고 판단되는 64부를 통계 분석 대상에서 제외하여 최종적으로 250부의 설문서를 통계 자료 분석에 사용하였다.

4.1.2 표본 집단의 특성

설문 응답자들을 인구 통계학적 특성으로 구분한 결과는 다음과 같다. 응답자의 남녀 비율은 남성이 58.8%, 여성이 41.2%로 남성의 비율이 17.6% 차이로 높았다. 연령대는 20대가 56%, 30대가 38.8%, 40대가 4% 20대가 가장 많았으며 50대 이상은 1.2%였다. 학력의 경우는 대졸 63.6%, 대학원졸 16%, 고졸 14%, 전문대졸 6.4%의 순으로 나타났으며 직업을 보면 직장인이 61.2%로 가장 많았고 다음으로 대학원생 17.2%, 대학생 16.8%, 주부 3.2%, 기타 1.6% 순이었다.

페이스북 접속 빈도는 하루에 한 번 초과가 48.8%로 가장 높게 나왔고, 다음으로 하루에 한 번과 2~3일에 한 번, 한 달에 한 번이 12%로 동일한 분포를 보였다. 다음으로 일주일에 한 번은 10.4%를 보였고, 기타는 4.8% 순이었다.

페이스북 사용기간은 2년 이상~3년 미만이 33.6%, 1년 이상~2년 미만이 30.8%, 4년 이상이 13.2%, 6개월 이상~1년 미만이 12.4%, 6개월 미만이 10% 순으로 나타났다.

4.2 측정 모형의 검증

수집된 데이터는 SPSS 18.0과 PLS(Partial Least Squares) 2.0을 사용하여 분석하였다. 측정항목의 타당성(validity)과 신뢰성(reliability)을 검증하기 위해 SPSS 18.0을 사용하여 크롬바흐 알파계수 분석과 탐색적 요인분석(exploratory factors analysis; EFA)을 실시하였으며, 더불어 PLS 2.0을 사용하여 확인적 요인분석(confirmatory factors analysis; CFA)을 병행하여 실시하였다. 최종적인 가설의 실증분석을 위해 PLS를 사용한 구조방정식 모형을 분석하였다. PLS는 정보기술 관련 연구에 적합하며 전체 이론의 검증보다는 인과관계 예측에 유용한 도구로 정보시스템 관련 연구에 많이 사용되고 있다[11].

4.2.1 타당성 및 신뢰성 분석

주성분 분석과 배리맥스(varimax) 방법에 따른 직교회전 방식을 사용한 요인 분석 결과 8개의 요인으로 구분되었으며, 총 분산의 77.656%를 설명하고 있다. 측정 항목들의 타당성을 검증하기 위해 요인적재값(factor loading)이 0.5 이상이고 교차요인적재값(cross loading)이 0.4 미만인 측정 항목과 중복되는 의미의 측정 항목(ATT3, TRU6)은 제외하였다[38]. 측정 항목들의 요인적재값은 ATT3과 TRU6를 제외한 모든 측정 항목들은 0.5 이상으로 측정 항목들의 집중타당성이 있는 것으로 나타났다.

본 연구에서 활용한 측정 도구에 대한 신뢰도는 크롬바흐 알파계수에 대한 0.7을 기준으로 판단하였으며[31], <표 3>에서 알 수 있듯이 모든 구성 신뢰성 지수와 크롬바흐 알파계수가 0.7 이상으로 각 측정항목은 신뢰도가 있다고 볼 수 있다.

<표 4>의 대각선 행렬은 각 개념의 상관계수 행렬(correlation)에서 추출된 평균분산의 제곱근 값을 동일 변수의 상관계수의 자리에 입력한 것으로 인접한 다른 상관계수들보다 모두 높게 나타났다. 이 결과는 본 연구의 측정 항목들이 판별타당성을 확보하였다고 판단할 수 있다[17, 23].

4.3 가설검증

잠재변수들 간의 인과관계를 분석한 구조모형의 결과를 정리하면 [그림 3]과 같다.

분석 결과에 의하면, 매개변인인 보안기능 사용에 대한 태도는 보안기능 사용의도에 통계적으로 유의한 영향을 미쳤으며(가설 1의 채택, $\beta = 0.602$,

〈표 3〉 연구 변수의 신뢰도 및 타당성 분석 결과

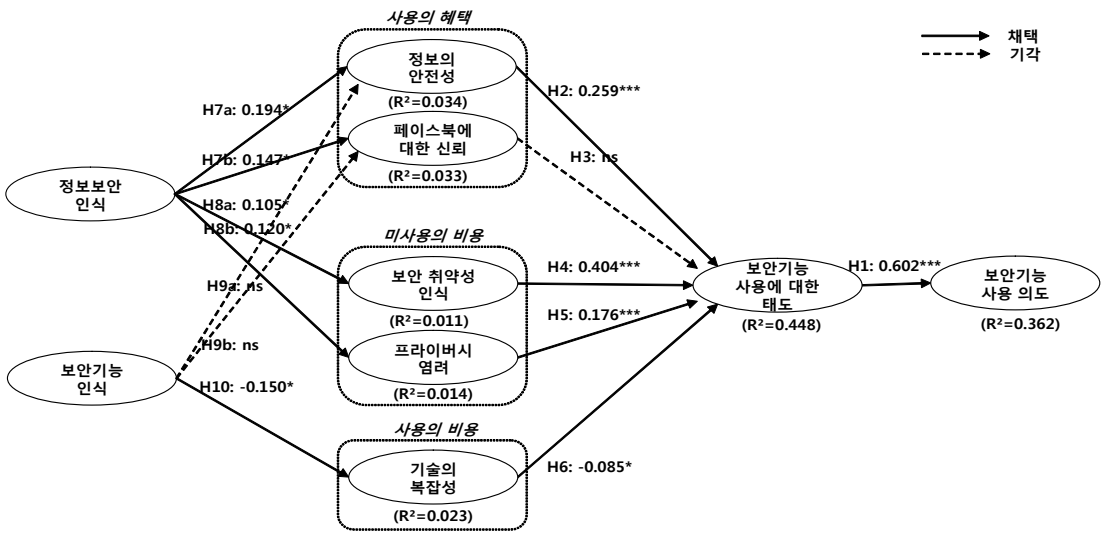
연구변수	측정 항목	Std. Loading	t-value	AVE	Construct Reliability	Cronbach's α
보안기능 사용에 대한 태도	ATT1	0.902	47.782	0.829	0.936	0.897
	ATT2	0.913	68.954			
	ATT4	0.916	53.278			
보안기능 사용의도	INT1	0.936	62.121	0.855	0.947	0.914
	INT2	0.911	49.213			
	INT3	0.928	83.574			
정보보안 인식	ISA1	0.894	28.196	0.812	0.928	0.882
	ISA2	0.890	26.323			
	ISA3	0.918	42.247			
프라이버시 염려	PRC1	0.813	26.253	0.773	0.932	0.902
	PRC2	0.899	50.467			
	PRC3	0.909	70.633			
	PRC4	0.893	49.681			
정보의 안전성	SAF1	0.840	30.444	0.712	0.937	0.915
	SAF2	0.881	56.707			
	SAF3	0.879	24.826			
	SAF4	0.755	16.732			
	SAF5	0.809	22.267			
	SAF6	0.893	46.703			
보안 취약성 인식	SEV1	0.912	70.004	0.815	0.957	0.942
	SEV2	0.817	23.869			
	SEV3	0.932	85.654			
	SEV4	0.921	76.707			
	SEV5	0.927	91.920			
보안기능 인식	SFA1	1.000	-	1.000	1.000	-
기술의 복잡성	TEC1	0.850	4.358	0.704	0.905	0.867
	TEC2	0.820	3.937			
	TEC3	0.875	6.557			
	TEC4	0.810	5.144			
페이스북에 대한 신뢰	TRU1	0.694	4.706	0.631	0.894	0.865
	TRU2	0.665	4.237			
	TRU3	0.849	6.189			
	TRU4	0.881	5.987			
	TRU5	0.858	6.031			

Note) ATT = 보안기능 사용에 대한 태도, ISA = 정보보안 인식, INT = 보안기능 사용의도, PRC = 프라이버시 염려, SFA = 보안기능 인식, SAF = 정보의 안전성, TEC = 기술의 복잡성, TRU = 페이스북에 대한 신뢰, SEV = 보안 취약성 인식

〈표 4〉 연구 변수의 상관관계 분석

연구변수	Mean	S.D	ATT	ISA	INT	PRC	SFA	SAF	TEC	TRU	SEV
ATT	5.764	1.174	**0.910**								
ISA	4.141	1.593	0.130	**0.901**							
INT	5.735	1.176	0.602	0.132	**0.925**						
PRC	5.330	1.503	0.435	0.120	0.421	**0.879**					
SFA	3.816	1.637	0.146	0.340	0.166	-0.046	**1.000**				
SAF	5.029	1.380	0.489	0.162	0.305	0.286	-0.029	**0.844**			
TEC	3.768	1.662	-0.024	0.053	-0.087	0.137	-0.113	0.017	**0.839**		
TRU	3.766	1.439	-0.006	0.167	-0.060	-0.180	0.120	0.255	0.077	**0.794**	
SEV	5.431	1.482	0.601	0.107	0.435	0.479	0.001	0.459	0.085	-0.042	**0.903**

Note) 대각선의 굵은 숫자는 AVE 값의 제곱근 값.



Note) * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$.

[그림 3] PLS 분석 결과

$p < 0.001$) 보안기능 사용의도의 36.2%를 설명하였다. 정보의 안전성은 보안기능 사용에 대한 태도에 통계적으로 유의한 영향을 미쳤으며(가설 2의 채택, $\beta = 0.259$, $p < 0.001$), 보안 취약성 인식도 보안기능 사용에 대한 태도에 유의한 영향을 미치는 것으로 나타났다(가설 4의 채택, $\beta = 0.404$, $p < 0.001$). 또한 프라이버시 염려가 보안기능 사용에 대한 태도에 미치는 영향은 통계적으로 유의한 것으로 분석되었고(가설 5의 채택, $\beta = 0.176$, $p < 0.001$), 이들 정보의 안전성, 보안 취약성 인식, 프라이버시 염려는 보안기능 사용에 대한 태도의 44.8%를 설명하였다.

선행요인인 정보보안 인식은 정보의 안전성(가설 7a의 채택, $\beta = 0.194$, $p < 0.05$), 페이스북에 대한 신뢰(가설 7b의 채택, $\beta = 0.147$, $p < 0.05$), 보안 취약성 인식(가설 8a의 채택, $\beta = 0.105$, $p < 0.05$), 프라이버시 염려(가설 8b의 채택, $\beta = 0.120$, $p < 0.05$)에 통계적으로 유의한 영향을 미치는 것

으로 나타났다. 또한 보안기능 인식은 기술의 복잡성(가설 10의 채택, $\beta = -0.150$, $p < 0.05$)에 유의한 영향을 미치는 것으로 나타났다. 그 밖의 변수 간 관계에 있어서 페이스북에 대한 신뢰는 보안기능 사용에 대한 태도에 미치는 영향은 통계상 유의하지 않은 것으로 나타났다(가설 3의 기각). 또한 보안기능 인식과 정보의 안전성, 페이스북에 대한 신뢰에 미치는 영향 역시 통계상 유의하지 않은 것으로 나타났다(가설 9a, 가설 9b의 기각).

본 연구의 분석 결과, SNS의 보안기능 사용의도에 선행요인인 정보보안 인식이 정보의 안전성, 페이스북에 대한 신뢰, 보안 취약성 인식, 프라이버시 염려에 영향을 미치며, 보안기능 인식은 기술의 복잡성에 유의한 영향을 미침을 알 수 있다. 또한 정보의 안전성, 보안 취약성 인식, 프라이버시 염려, 기술의 복잡성은 보안기능 사용에 대한 태도에 영향을 미치며, 보안기능 사용에 대한 태도는 보안기능 사용의도에 유의한 영향을 미침을 알 수 있다.

가설에 대한 검정 결과는 <표 5>에 요약되어 있다.

5. 결 론

5.1 연구 결과 및 시사점

SNS의 확산이 사회적으로 크게 영향력을 가지면서 이용자들의 개인정보 관리가 중요한 이슈로 대두되었다. 본 연구는 SNS에서 정보보안 인식과 보안기능 인식을 동시에 고려하여 SNS의 보안기능 사용의도에 관한 선행요인들을 알아보았다.

SNS 이용자들의 보안기능 사용의도에 관한 요인들과 정보보안 인식, 보안기능 인식과의 관계를 살펴보았고, 두 가지 인식이 영향을 주는 요인들 간의 차이가 있다는 점을 경험적으로 검증하였다.

본 연구의 결과는 다음과 같다.

첫째, 페이스북 이용자들이 일반적으로 인식하고 있는 정보보안과 관련된 지식의 정도가 높아질수록 보안위협에 대응하여 개인정보가 안전하게 보호될 것으로 이용자들이 인식하였다. 보안위협에 대응하여 페이스북이 제공하는 보안기능의 적절성을 판단하여 페이스북에 대한 신뢰가 증가하는 것으로 보인다. 보안기능을 사용하지 않을 때

〈표 5〉 연구 모형의 가설검증 결과

가설	경로	경로계수	t-값	p-값	채택여부
H1	보안기능 사용에 대한 태도 → 보안기능 사용의도	0.602	12.091	0.000***	채택
H2	정보의 안전성 → 보안기능 사용에 대한 태도	0.259	3.842	0.000***	채택
H3	페이스북에 대한 신뢰 → 보안기능 사용에 대한 태도	-0.017	0.307	0.380	기각
H4	보안 취약성 인식 → 보안기능 사용에 대한 태도	0.404	4.538	0.000***	채택
H5	프라이버시 염려 → 보안기능 사용에 대한 태도	0.176	3.134	0.001***	채택
H6	기술의 복잡성 → 보안기능 사용에 대한 태도	-0.085	1.739	0.042*	채택
H7a	정보보안 인식 → 정보의 안전성	0.194	2.792	0.003*	채택
H7b	정보보안 인식 → 페이스북에 대한 신뢰	0.147	1.666	0.048*	채택
H8a	정보보안 인식 → 보안 취약성 인식	0.105	1.648	0.050*	채택
H8b	정보보안 인식 → 프라이버시 염려	0.120	1.839	0.034*	채택
H9a	보안기능 인식 → 정보의 안전성	-0.095	1.426	0.078	기각
H9b	보안기능 인식 → 페이스북에 대한 신뢰	0.069	0.751	0.227	기각
H10	보안기능 인식 → 기술의 복잡성	-0.150	2.046	0.021*	채택

Note) df = 249, one-tailed test, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$.

발생할 수 있는 보안 취약성 인식과 프라이버시 염려에 대한 경각심이 고취됨으로써 긍정적인 영향을 미치는 것으로 나타났다. 따라서 SNS 사이트에서는 제공하는 보안 정책 및 보안 기능들에 대해서 사용자가 좀 더 이해하기 쉽고 홍보방안을 설정한다면, 서비스가 제공하는 보안에 대한 신뢰뿐만 아니라 서비스 자체에 대한 신뢰도 증가 할 수 있을 것이다.

둘째, 페이스북에서 제공하는 보안기능에 대한 인식의 정도가 클수록 정보시스템 활용능력이 배양된 상태라고 판단할 수 있다[24]. 본 연구의 응답자 86% 이상이 전문대학 이상의 학력을 보유하고 있으며, 80% 정도가 직장인, 대학원생으로 업무 및 학업과정에서 정보시스템 활용능력이 배양되어 있다고 판단할 수 있으며 SNS 보안기능을 사용하는데 필요한 기술적인 어려움을 감소시켜 준다고 볼 수 있다. 따라서 SNS 사이트에서 보안위협에 대응한 적절한 보안기능 개발과 더불어 이용자들이 보안기능 자체에 대한 이해를 돕기 위한 노력이 필요할 것이다.

셋째, 최근 KB카드, 롯데카드, NH카드 등 많은 기업들의 개인정보 유출과 관련된 사건들을 접하면서 이용자들은 보안 취약성 인식과 프라이버시 염려로부터 개인정보를 안전하게 지키고 싶다는 인식이 보안기능 사용에 대한 태도를 형성하는 것과 유의미한 연관관계를 찾을 수 있었다. 서비스 제공자가 보안 기능을 사용 하지 않았을 때 발생할 수 있는 피해를 이용자에게 인지 시킨다면, 좀 더 보안기능 사용의 활성화를 기대할 수 있을 것이다.

마지막으로, 예상과 달리 페이스북에 대한 신뢰가 보안기능 사용에 대한 태도에 유의미한 영향을 미치지 못하는 것으로 나타났다. 또한, 보안 기능 인식이 페이스북에 대한 신뢰에는 유의미한 영향을 미치지 못하였다. 이는 서비스 자체에 대한 신뢰, 즉 페이스북에 자체에 대한 신뢰와 보안기능이 제 기능을 하는 지에 대한 믿음 및 태도와는 상관 관계가 없다는 것을 의미한다. 추후 연구에는 페이스북에 대한 신뢰보다는 보안 기능 자체에 대한 신뢰와의 관계 검증이 필요할 것이다.

이에 더하여, 보안 기능 인식이 정보의 안정성에는 유의미한 영향을 미치지 못하는 것으로 나타났다. 보안 기능에 대해 많은 지식을 가지고 있다고 하여, 정보가 안전하게 지켜질 수 있다는 믿음이 올라가는 것은 아닐 수 있다. 보안 기능에 대한 지식이 높아지면 보안 기능이 제 기능을 하는지에 대한 판단력이 올라 갈수는 있으나, 이러한 판단력의 증가가 정보의 안전성에 대한 믿음의 증가에 직접적인 영향은 미치지 않을 수 있다. 추후 연구에서는 보안 기능 인식과 정보의 안전성 사이의 매개변수에 대해 고민 할 필요가 있다.

본 연구를 통해 기존의 기업위주의 보안 관련 연구의 편향성을 없애고 개인 단위의 보안 연구를 진행함으로써 보안 관련 연구 대상의 편향성을 없앴다는 학술적 의의가 있다. 또한, 태도를 결정하는 구체적인 선행 요인이 없다는 계획된 행동 이론의 단점을 해결하기 위해 합리적 선택 이론을 도입하여 이론의 강화를 가져 왔다. 이에 더하여, 합리적 선택이론에서 비용의 측면을 사용 시의 비용과 미사용 시의 비용으로 확장하여 이론의 다양화를 이루어 내었다는 추가적 학술적 의의가 있다.

실무적으로는 SNS 제공자들이 경험적으로 검증된 요인들을 고려하여 정책을 수립하고 사용자의 보안 정책 및 기능의 인식을 고취한다면 보안기능사용의 활성화뿐만 아니라 이용자의 서비스 자체에 대한 신뢰도 강화시킬 수 있을 것이다.

5.2 연구의 한계점 및 향후 연구 방향

본 연구는 몇 가지 한계점을 가지고 있으며, 한계점을 극복하기 위한 추가적인 연구가 이루어져야 할 것이다.

첫째, SNS에서 보안기능 사용의도에 관한 초기의 연구로 선행연구가 풍부하지 못하여 사용자가 느끼는 혜택 및 비용에 영향을 미치는 선행 요인들에 대한 다양한 변수를 포함시키지 못했다. 이에 따라 정보의 안전성(R^2 = 0.034), 페이스북에 대한

신뢰(R^2 = 0.033), 보안 취약성 인식(R^2 = 0.011), 프라이버시 염려(R^2 = 0.014), 기술의 복잡성(R^2 = 0.023)의 설명력이 3% 이하의 값들로 설명력은 있지만 충분하다고 보기는 어렵다. 향후 연구에서는 SNS 상황에서 정보보안 인식과 보안기능 인식의 특성뿐만 아니라 보안기능을 사용함으로써 발생하는 해택과 비용에 대한 추가적인 선행 변수들의 개발이 이루어져야 할 것으로 생각한다.

둘째, SNS의 보안기능 사용의도에 영향을 미치는 요인을 고려함에 있어 서비스 제공업체의 특성, 보안관련 상황 등 다양한 특성에 따른 차이를 고려해 연구해보는 것도 이용자들의 SNS의 보안기능 사용의도를 파악하는데 새로운 시사점을 제공해 줄 수 있을 것이다.

마지막으로 SNS 보안기능과 관련하여 산업보안 측면, 기술 개발자 측면 등 다각적으로 연구를 진행할 필요가 있다.

참 고 문 헌

[1] 심은선, 이정훈, 정법근, "기업 SNS 이용자(고객)의 지속적 사용의도에 관한 연구 : Facebook 팬페이지 운영 목적을 조절변수로", 「한국IT서비스학회지」, 제12권, 제4호(2013), pp.41-57.

[2] 한국인터넷진흥원, 「페이스북 이용자를 위한 개인정보보호 안내서」, 2012.

[3] 한국인터넷진흥원, 「2012년 정보보호 실태조사(개인편)」, 2013.

[4] 한국정보보호진흥원, 「온라인 소셜 네트워크(Social Network) 환경에서의 보안 위협과 시사점」, 2008.

[5] Acquisti, A. and R. Gross, "Imagined communities : Awareness, information sharing, and privacy on the Facebook", *In Privacy enhancing technologies*, Springer Berlin Heidelberg, (2006), pp.36-58.

[6] Aimeur, E., S. Gambs, and A. Ho, "Towards a privacy-enhanced social networking site. In Availability, Reliability, and Security", *ARES International Conference on IEEE*, (2010), pp.172-179.

[7] Ajzen, I., *From intentions to actions : A theory of planned behavior*, Springer Berlin Heidelberg, 1985.

[8] Ajzen, I., "The theory of planned behavior", *Organizational behavior and human decision processes*, Vol.50, No.2(1991), pp.179-211.

[9] Ajzen, I. and M. Fishbein, "Understanding Attitudes and Predicting Social Behavior", *Journal of Experimental Social Psychology*, Vol.22(1980), pp.453-474.

[10] Ajzen, I. and D. Albarracin, *Chapter 1 : Predicting and Changing Behavior : A Reasoned Action Approach, in Prediction and Change of Health Behavior : Applying the Reasoned Action Approach*, I. Ajzen, D. Albarracin, and R. Hornik(eds.), Hillsdale, NJ : Lawrence Erlbaum and Associates, 2007.

[11] Barclay, D., C. Higgins, and R. Thompson, "The Partial Least Squares(PLS) Approach to Causal Modelling : Personal Computer Adoption and Use as an Illustration", *Technology Studies*, Vol.2, No.2(1995), pp.285-309.

[12] Bhattacherjee, A. and G. Premkumar, "Understanding changes in belief and attitude toward information technology usage : a theoretical model and longitudinal test", *MIS Quarterly*, Vol.28, No.2(2004), pp.229-254.

[13] Bhattacherjee, A. and C. Sanford, "Influence processes for information technology acceptance : an elaboration likelihood model", *MIS Quarterly,* (2006), pp.805-825.

[14] Boyd, D. M. and N. B. Ellison, "Social Network Sites : Definition, History, and Scholarship", *Journal of Computer-mediated*

Communication, Vol.13, No.1(2007), pp.210-230.

[15] 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.

[16] Caruso, J. B. and G. Salaway, "The ECAR study of undergraduate students and information technology, 2008", Retrieved December, 8, 2007.

[17] Churchill Jr, G. A., "A Paradigm for Developing Better Measures of Marketing Constructs", *Journal of Marketing Research*, Vol.16, No.1(1979), pp.64-73.

[18] Culnan, M. J., "How did they get my name? : An exploratory investigation of consumer attitudes toward secondary information use", *MIS Quarterly*, Vol.17, No.3(1993), pp.341-363.

[19] Culnan, M. J. and P. K. Armstrong, "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust : An Empirical Investigation", *Organization Science*, Vol.10, No.1(1999), pp.104-115.

[20] DeLone, W. H. and E. R. McLean, "Information systems success : the quest for the dependent variable", *Information systems research*, Vol.3, No.1(1992), pp.60-95.

[21] Fishbein, M. and I. Ajzen, *Belief, attitude, intention, and behavior : An introduction to theory and research, Reading,* MA : Addison-Wesley, 1975.

[22] Fogel, J. and E. Nehmad, "Internet social network communities : Risk taking, trust, and privacy concerns", *Computers in Human Behavior*, Vol.25, No.1(2009), pp.153-160.

[23] Gefen, D., D. W. Straub, and M. C. Boudreau, "Structural Equation Modeling and Regression : Guidelines for Research Practices", *Communications of AIS*, Vol.4, No.7 (2000), pp.1-79.

[24] Hewett, K. and W. O. Bearden, "Dependence, trust, and relational behavior on the part of foreign subsidiary marketing operations : implications for managing global marketing operations", *The Journal of Marketing*, (2001), pp.51-66.

[25] Kim, H. W., H. C. Chan, and S. Gupta, "Value-based adoption of mobile internet : an empirical investigation", *Decision Support Systems*, Vol.43, No.1(2007), pp.111-126.

[26] Kwon, O. and Y. Wen, "An empirical study of the factors affecting social network service use", *Computers in Human Behavior*, Vol.26, No.2(2010), pp.254-263.

[27] Laudon, K. C. and J. P. Laudon, *Management information systems : managing the digital firm*, Pearson, Vol.12(2012).

[28] Lee, S., Oh, Y. Kang, and Y. Lee, "Design principles of social network based learning based on analysis of participation motivation of social network", *The Korean Association of Educational Methodology Studies*, Vol.23, No.4(2011), pp.729-754.

[29] McCarthy, B., "New Economics of Sociological Criminology", *Annual Review of Sociology*, Vol.28, No.1(2002), pp.417-442.

[30] Mohamed, N. and I. H. Ahmad, "Privacy measures awareness, privacy setting use and information privacy concern with Social Networking Sites", *In Research and Innovation in Information Systems(ICRIIS), International Conference on IEEE*, (2011), pp. 1-6.

[31] Nunnally, J. C., Psychometric Theory, Mc-Graw-Hill, New York, 1978.

[32] Paternoster, R. and G. Pogarsky, "Rational Choice, Agency and Thoughtfully Reflective Decision Making : The Short and Long-Term Consequences of Making Good Choices", *Journal of Quantitative Criminology*, Vol.25, No.2(2009), pp.103-127.

[33] Peltier, T. R., *Information Security Risk Analysis(2nd ed.)*, Boca Raton, FL : CRC Press, 2005.

[34] Shu, W. and Y. H. Chuang, "The perceived benefits of six-degree-separation social networks", *Internet Research*, Vol.21, No.1(2011), pp.26-45.

[35] Tuunainen, V. K., O. Pitkanen, and M. Hovi, "Users' Awareness of Privacy on Online Social Networking sites-Case Facebook", *22nd Bled eConference eEnablement : Facilitating an Open, Effective and Representative eSociety, Bled, Slovenia*, (2009), pp. 1-16.

[36] Wang, Y. D. and H. H. Emurian, "An overview of online trust : Concepts, elements, and implications", *Computers in human behavior*, Vol.21, No.1(2005), pp.105-125.

[37] West, R., "The Psychology of Security", *Communications of the ACM*, Vol.51, No.4 (2008), pp.34-40.

[38] Zikmund, W. G., J. C. Carr, and M. Griffin, *Business research methods*, Cengage Brain, com, 2012.

◈ 저 자 소 개 ◈

김 협 (hyubiii@yonsei.ac.kr)

연세대학교 정보대학원에서 정보시스템 석사 학위를 취득하였으며, 현재 내부보안 전문기업인 지니네트웍스(주) 경영기획실에 재직 중이다. 학사는 연세대학교 문헌정보학과에서 취득하였다. 주요 관심분야는 u-biz Strategy, Information Security, Social Networking Services, Network Access Control 등이다.

김 경 규 (kyu.kim@yonsei.ac.kr)

미국 Utah 대학에서 경영정보 전공으로 박사를 취득하였으며, 현재 연세대학교 정보대학원 교수로 재직 중이다, MIS Quarterly, Journal of MIS, Information and Management, Accounting Review, Database 등의 국제학술지 및 경영학연구, 경영정보학 연구, 중소기업 연구 등의 국내학술지에 논문을 게재한 바 있다. 주요 관심분야는 e-Business Strategy, Trust in B2C e-Commerce, SCM, Evaluation of Industrial Informatization, u-biz Strategy 등이다.

이 호 (leeho32@gmail.com)

연세대학교 정보대학원 디지털 비즈니스 전공으로 박사를 취득하였으며, 현재 연세대학교 정보대학원 박사 후 연구원으로 재직 중이다. 주요 관심분야는 Ubiquitous Computing, u-Business Model, u-Business Strategy 등이다.