

개인정보 침해 관련 정보 제공 서비스 사용 의도 분석*

김택영,^{1*} 전효정,² 김태성^{1*}

¹충북대학교 경영정보학과/보안경제연구소,

²충북대학교 글로벌보안컨설팅전문인력양성사업단/보안경제연구소

An Analysis on Intention to Use Information Service for Personal Information Breach*

Taek-Young Kim,^{1*} Hyo-Jung Jun,² Tae-Sung Kim^{1*}

^{1,2}Chungbuk National University/Cybersecurity Economics Research Institute(CERI)

요 약

2008년부터 대규모 개인정보 유출사고들이 빈번히 발생하면서 이를 해결하고자 국가적 차원의 교육, 정책, 법률 등이 제정 및 시행되고 있다. 현재까지 개인정보 침해와 유출사고는 지속적으로 발생하고 있지만, 개인이 개인정보 침해에 대한 상세 정보를 확인하고 추정 및 대처 할 수 가 없는 실정이다. 이에 본 연구는 개인 정보 침해 및 유출 사고 등 개인정보 침해에 예방 및 대응하기 위한 여러 가지 방법 중 일반인을 대상으로 하여 개인정보 침해에 관한 정보가 제공 및 전달된다면, 개인은 개인정보 침해 정보를 얼마나 받아들이고 개인정보보호 행동으로 옮겨질지에 대하여 연구하고자 한다. 개인정보 침해와 관련된 정보를 제공하는 것이 어떠한 의미를 가지고 있으며, 어떠한 기능을 수행해야 하는지 정의하고, 정보 제공에 대한 일반인의 수용 영향에 대하여 분석하고자 한다. 이를 통해 개인정보 관련 정보 제공에 대한 필요성 및 가이드라인을 제시하고, 개인의 주동적인 정보보호 활동을 장려하는데 도움이 되 고자 한다.

ABSTRACT

Since 2008, large-scale personal information breach incidents have occurred frequently. Even though national education, policy, and laws have been enacted and implemented to resolve the issue, personal information breaches still occur. Currently, individuals cannot confirm detailed information about what personal information has been affected, and they cannot respond to the breaches. Therefore, it is desirable to develop various methods for preventing and responding to personal information infringement caused by breach and leakage incidents and move to privacy protection behaviors. The purpose of this study is to create understanding of personal information security and information breach, to present services that can prevent breaches of personal information, to investigate the necessity of and analyze the potential public demand for such services, and to provide direction for future privacy-related information services.

Keywords: Information Breach, Social Disaster, Service Acceptance, Personal Information Security

Received(09. 22. 2017), Modified(12. 14. 2017),
Accepted(12. 15. 2017)

* 본 연구는 미래창조과학부 및 한국인터넷진흥원의 "고용계약
형 정보보호 석사과정 지원사업"의 연구결과로 수행되었음
(과제번호 H2101-16-1001). 이 논문은 2015년 대한민국

교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF
-2015S1A5A2A01009763).

† 주저자, ecac5732@gmail.com

‡ 교신저자, kimts@cbnu.ac.kr(Corresponding author)

I. 서 론

인터넷 기술의 발전과 활성화로 인하여 누구든지 장소와 시간에 구애받지 않고 개인정보를 포함한 정보를 생산, 유통, 공유할 수 있는 환경이 되었다[1]. 하지만 정보통신 기술 기반 서비스가 활성화되고, 정보의 유통범위가 넓어지면서, 그에 따른 해킹, 악성코드, 피싱, 파밍 등 역기능의 범주도 넓어지고 있으며, 이와 관련된 개인정보 침해 사고가 끊임없이 발생하고 있다[2].

개인정보 침해 사고는 사생활 침해와 더불어 금융 피해까지 일으킬 수 있는 심각한 사고이다. 하지만 사고 발생 시 구체적인 피해 규모와 발생내역 등 상세한 정보를 파악하는 것은 어렵다[3]. 그 이유는 개인정보 침해와 관련하여 정보가 충분히 제공되지 않기 때문이다. 현재 개인정보 관련 법률에 따라, 개인정보 침해 사고가 발생하게 되면 사고 발생에 대한 내용을 한국인터넷진흥원에 신고하고, 개인정보 침해에 대한 정보를 온라인, 오프라인으로 개인정보가 유출된 회원에게 공지하게 되어있다. 하지만 정보가 상세하지 않기 때문에, 일반 개인이 개인정보 침해에 대하여 정보를 확인하고 개인정보 침해 사고에 대처할 수 없는 실정이다[4].

이에 본 연구에서는 개인정보 침해에 관한 정보 부족 현상을 해결하고, 개인정보 침해를 예방하고 대처할 수 있도록 일반인을 대상으로 개인정보 침해에 관한 정보를 제공한다면 개인이 정보를 얼마나 수용하고, 보호 행동으로 옮길지에 대하여 연구하고자 한다.

본 연구를 위해, 개인정보 침해 정보 제공에 대한 서비스와 그에 따른 기능을 정의하고, 서비스에 대한 일반 개인들의 수용, 더 나아가 개인정보보호 행동에 어떠한 요인들이 영향을 미치는 지에 대하여 도출하고자 한다. 이를 통해 개인정보 관련 정보 제공과 이와 관련된 기능을 수행하는 서비스의 필요성을 제시하고, 정보 제공 서비스가 개인의 주동적인 정보보호 활동을 장려할 수 있다는 것에 대하여 검증하고자 한다.

II. 개인정보 침해 관련 정보 제공 서비스 정의

2.1 정보보호 관련 정보 제공 사례

현재 개인정보보호 분야 내에서 개인정보 침해 관련 정보 제공에 대하여 직접적으로 제공하고 있지 않다. 하지만 정보보호 분야에서 정보보호 관련 정보

(사이버 위협, 유출, 대응 방침 등)를 개인·기업·조직에게 제공하고 있다. 국내의 경우, 개인정보 침해 사고 신고 서비스, e프라이머시 클린서비스, 인터넷 침해사고 경보, 사이버 위기 경보 등 4개의 서비스가 운영되고 있으며, 국외에서는 미국, 중국, 일본 등에서 CERT를 통해 정보보호 관련 정보가 제공되고 있다.

개인정보 침해사고 신고 서비스는 한국인터넷진흥원에서 운영하는 서비스로서, 개인정보침해 발생 신고 접수 및 상담, 민원 등 개인정보 침해에 관한 도움을 주는 서비스를 운영하고 있다. 신고 절차에 따라 신고자의 이메일로 결과 및 정보를 제공하고 있다. 해당 서비스의 경우, 개인정보 침해 사고가 발생 후 개인이 직접 신고를 해야 하는 서비스이다[5].

e프라이머시 클린 서비스는 한국인터넷진흥원에서 운영하는 서비스로서, 개인정보(주민등록번호, I-PIN)가 어떠한 웹사이트에서 어떠한 용도로 사용되는지를 조회하고, 불필요할 시 회원탈퇴를 할 수 있도록 제공하는 서비스이다. 또한, 공지사항을 통해 본인확인서비스에 대한 기업별 서비스 현황 정보(순간 중단·스팸차단 방법 등)를 게시하고 있다[6].

인터넷 침해사고 경보는 한국인터넷진흥원에서 운영하는 서비스로서, 민간분야의 인터넷 침해 우려 위협에 대하여 경보 및 정보를 제공하는 서비스이다. 제공하는 정보는 일자별로 사이버 위협에 대한 경보, 악성코드 발견 홈페이지 수, 신종 스미싱 악성 앱 수, 피싱·파밍 차단 사이트 수, 소프트웨어 보안 업데이트 권고 공지 등을 제공하고 있다. 인터넷 침해사고 경보 단계는 5단계로 정상, 관심, 주의, 경계, 심각으로 구성되어 있다[7].

사이버 위기 경보는 국가정보원에서 운영하고 있는 사이버안전센터에서 제공하는 서비스로서, 공공분야의 사이버 위기 경보와 이에 대한 정보를 제공하는 서비스이다. 국가사이버안전관리규정 제 11조에 의거하여 해당 홈페이지를 통해 사이버 위기 경보를 발령하고 있다. 국가 차원에서의 효율적인 경보 업무 수행을 위해 경보 관련 정보를 발령 전에 민간 분야를 담당하는 과학기술정보통신부와 상호 교환하여 업무를 수행한다. 사이버 위기 경보 단계는 5단계로 정상, 관심, 주의, 경계 심각으로 구성됨으로써 인터넷 침해사고 경보와 동일하다[8].

미국의 US-CERT는 홈페이지를 통해 최신 보안 이슈 외 취약점 및 공격 등에 관한 정보 서비스를 제공하고 있다. 해당 정보는 홈페이지를 통해 게시하고

있으며, 메일링 서비스 신청자들에게는 보안 경고 정보 메일을 보내는 서비스를 운영하고 있다. 다른 국가의 CERT에서 제공하는 서비스와 달리 각 취약점 및 공격에 대한 코드화가 되어 있다[9].

중국의 CNCERT의 경우, 국내와 유사하게 사이버 위기 경보에 대해 5단계로 정보를 제공하고 있다. 이외에 취약점과 악성코드 등 보안 위협에 대한 경고 사항 및 정보를 홈페이지를 통해 제공하고 있으며, 미국과 동일하게 신청자에게 별도의 메일링 서비스를 제공하고 있다[10].

일본의 JPCERT의 경우, 타 국가와 동일하게 위협 및 취약점에 대한 정보 및 취약점 조치 방안에 대한 정보를 제공하고 있다. 해당 정보는 공공·민간 분야 모두 해당되며, 주로 조직을 대상으로 정보를 제공하고 있다[11].

현재 정보보호 분야 내 정보 제공은 웹 홈페이지와 이메일을 통해 정보를 제공하고 있으며, 이메일의 경우 신청자에 한해 정보를 제공하고 있다. 이를 통해 소극적으로 정보를 제공하고 있음을 알 수 있다. 일부 정보 제공 사례의 경우, 사이버 위협을 지속적으로 파악하고 위험한 정도를 단계로 구분하여, 정보를 제공하고 있다. 제공하는 내용은 주로 개인정보 침해가 우려되는 정보시스템 및 네트워크에 대한 기술적 취약점, 취약점을 제거할 수 있는 보호기술, 취약점에 발생할 수 있는 위협 등 기술적인 정보에 초점을 두고 있다.

2.2 개인정보 침해 관련 정보 제공 서비스 정의

국내·외 정보보호 분야의 정보 제공 서비스 사례 분석을 통해 개인정보 침해 관련 정보 제공 서비스를 정의하였다.

개인정보 침해 관련 정보 제공 서비스는 현재 실시되고 있지 않은 개념적인 서비스라고 할 수 있다. 본 연구를 통해 명확히 정의하고자 한다. 개인정보 침해 관련 정보 제공 서비스는 공공분야의 개인정보 보호 관련 기관(주관 기관)에서 개인정보 침해 전·후(제공 시기)로 개인정보 위협 및 침해와 이에 대한 보호·대처 방법(제공 정보)에 대하여 문자, 이메일, 웹 홈페이지(제공 방법)를 통해 일반인(제공 대상)에게 제공하는 서비스이다. 개인정보 침해 관련 정보 제공 서비스는 서비스의 목적은 개인정보 유출사고를 줄일 수 있고 일반 국민들 및 정부기관이나 민간업체들이 개인정보 침해에 보다 더 관심을 가지고 행동할

수 있도록 하는 것이다.

III. 문헌연구

3.1 개인정보 유출·침해

인터넷은 우리 생활의 필수 매체가 되었으며, 인터넷 이용자의 수는 기하급수적으로 증가하여, 대부분의 일반인들이 인터넷을 사용하고 있다. 인터넷 사용자 수의 증가는 정부나 기업에서 일반적으로 정보를 제공하던 기존 방식에서 탈피하여, 일반 인터넷 사용자가 직접 정보를 생산하고 공유가 가능한 시대를 만들었다[1]. 하지만 이면에서는 대량의 정보 생산 및 유통이 쉬워지면서, 개인정보의 무분별한 수집 및 이용과 개인정보 유출 및 침해 등이 지속적으로 발생하고 있다[12]. 이러한 개인정보의 유출과 침해는 일반 사용자의 물리적·정신적 피해를 초래하고 있다[13]. 이전 연구들에서는 개인정보의 중요성과 개인정보 침해의 악영향에 대한 내용을 행동적·기술적·관리적·정책적·경제적 분야 등 다양한 관점으로 다루고 있다. Crespo & del Bosque(2009)는 일반 사용자의 개인정보 유출에 대하여 위협을 인식하였고, 이를 해결하기 위한 예방 활동에 영향을 미치는 요인들을 제시하였다[14]. Heatherly et. al.(2012)은 소셜 네트워크를 통한 공격 대상인 개인정보는 보호해야하며, 개인정보를 보호하기 위한 보안 시스템을 개발하고 이에 대한 효과를 분석하였다[15]. 이충훈 등(2011)은 미국의 46개주와 다른 주요 국가에서 실시하고 있는 개인정보 유출 통지 및 신고 관련 법률을 분석하여, 국내 개인정보 유출 통지 및 신고 프레임워크를 도출하고, 이에 대한 가이드라인을 제시하였다[16].

현재 국내·외에서 개인정보 유출에 대하여 대응할 수 있는 기술, 개인정보 침해를 일으키는 공격 등에 대한 연구와 법적·정책적 구조에 대한 연구, 개인정보의 유출 및 침해로 인한 피해 가치 등의 경제적 연구, 개인의 개인정보보호에 대한 영향 요인 및 행위적 연구 등이 진행되었다. 하지만, 일반 사용자(개인)의 개인정보보호를 위한 정보 제공에 대한 체계 및 그에 대한 필요성 등에 대한 연구된 바 없다. 이에 본 연구에서는 개인정보에 관한 정보 제공의 필요성을 연구하여 서비스를 정의하고, 최종적으로 일반 사용자들을 대상으로 서비스 수용 의도에 대하여 분석하고자 한다.

3.2 개인 대상 정보 제공 및 알림

정보 제공 및 알림에 대한 연구는 기술, 디자인, 소비자의 수용 등 다양한 측면에서 연구되었다. Hauswirth & Jazayeri(1999)는 정보 알림을 위한 시스템 중 푸시 시스템에 대하여 제시하고, 다른 시스템과 비교하여 효과적인 푸시 시스템을 위한 통신 체계 및 구성 요소, 제공 채널에 대하여 제시하였다[17]. Juvva & Rajkumar(1999)는 통신 패턴과 이중 노드를 활용하여, 실시간으로 정보 제공을 할 수 있는 푸시 서비스를 제시하였다[18]. Lepori et. al.(2002)은 일반 사용자가 서비스에 가입만 하면 적절한 시간에 정보를 제공 받을 수 있는 푸시 서비스를 제시하였다. 이를 통해 이러한 정보 제공 서비스가 시장에서 필요하다는 것을 증명하였다[19]. Us et. al.(2011)는 기존의 경보 시스템이 공정 및 제어시스템 설계상 많은 위험이 존재하기 때문에, 정보 알림을 활용함으로써, 산업에서 사용되는 경보 시스템의 문제를 해결할 수 있다고 주장하였다[20]. 임미나와 이중식(2013)은 스마트폰 이용자의 푸쉬 정보 알림에 대한 수용과 태도에 대하여 연구하였으며, 자신과의 접근성, 다양한 형태, 사회적 상호 작용 등의 요인들로 인하여 태도가 형성되고 행동이 발현된다고 주장하였다[21].

3.3 정보 제공 서비스에 대한 영향 요인

문헌 연구와 사례 조사를 통해 정의하고자 하는 개인정보 침해 관련 정보 제공 서비스에 대하여 어떠한 요인들이 서비스 수용과 개인정보보호 행동에 영향을 미치는지 확인하고자 한다. 이를 위해 서비스 수용과 보호 동기 이론에 대한 문헌 연구를 진행하여, 연구 모형을 설계하고자 한다.

3.3.1 서비스 수용

정보기술수용모형(Technology Acceptance Model, TAM)은 사회심리학분야의 합리적 행위이론(Theory of Reasoned Action, TRA)을 기초로 정보기술 이용자의 행위를 설명하고 예측하는 모형이다. 합리적 행위 이론에서의 행위에 대한 태도와 행위 의도 간 관계를 정보기술 이용자의 정보 기술 채택 연구로 확장한 모형이다. 합리적 행위 이론은 사회 심리학 분야에서 Fishbein(1967)에 의해 처음

으로 개발된 이후 여러 차례에 걸쳐 검증되었으며, 인간의 행위를 이해하고 예측하는데 유용하게 사용되고 있다. 사람의 특정행동은 행동을 수행하려는 행동 의도에 의해서 결정되고, 행동 의도는 대상에 대한 태도와 주관적 규범에 결정된다는 이론이다[22]. 계획적 행위 이론은 Ajzen(1985)에 의해 발표된 모형으로서, 기존의 합리적 행위이론에서 지각된 행동 통제라는 개념을 추가하였다. 행동은 행동의도와 지각된 행동통제에 의해 결정되고, 행동 의도는 태도, 주관적 규범, 지각된 행동통제 등에 의해서 결정된다는 이론이다[23]. 분해된 계획적 행위 이론(Decomposed Theory of Planned Behavior, DTPB)은 많은 행위 이론들이 활용되는 가운데, Taylor & Todd에 의하여 컴퓨터 자원 센터 사용을 설명하고 예측하기 위해 제시된 이론이다. 자신감과 관련된 내적 자원 측면과 이용 가능한 자원인 외적 자원(시간, 돈)으로 나눌 수 있다고 제시하였다[24].

Hsu & Chiu(2004)는 인터넷을 통한 지식의 경우, 서비스 도입 초기 자기 효능감이 적어서 사용자들이 만족을 느끼지 못하는 경우가 발생한다고 주장하였다. 또한, 온라인 서비스 도입에 대한 인터넷 사용자의 자기 효능감의 역할에 대하여 수용 패턴을 계획적 행위 이론(Theory of Planned Behavior, TPB)을 활용하여 검증하였다[25]. Shih(2004)는 B2C 대상 전자 상거래 시장의 온라인 쇼핑은 커뮤니케이션에 의존하고 있음을 주장하면서, 온라인 쇼핑에 대한 고객의 수용 요인을 도출하고, 이에 대하여 검증하였다[26]. Hung & Chang(2005)의 연구에서는 어플리케이션 프로토콜의 수용 모형을 도출하기 위해, 기술 수용 모형과 계획적 행위 이론을 활용하였다. 두 모형을 통해 연구 모형 설계와 설문 조사를 실시하고, 검증을 통해 최종적으로 무선 어플리케이션 프로토콜(Wireless Application Protocol, WAP) 수용에 미치는 영향 요인을 도출하였다[27]. Hung et. al(2006)는 전자정부 서비스에 관한 연구와 계획적 행위 이론에 관한 문헌 연구를 통해 전자정부 서비스에 적합한 계획적 행위 이론 모형을 도출하고 검증하였다[28].

3.3.2 보호 동기 이론

보호 동기 이론(Protection Motivation Theory, PMT)은 의학과 보건학에서 건강에 대한

위험에 노출되었을 시, 보호 동기를 일으켜 자신의 건강을 보호하고자 하는 행동에 변화를 가져온다는 가정을 기반으로 위협배제지의 효과를 설명하는 이론이다. 정보보호 분야에서도 보호 동기이론을 활용한 연구되어 왔다. Rogers(1975)는 보호동기이론의 변인들을 공포소구의 세 가지 중요 변인인 유해함의 정도, 발생 가능성, 권장 반응의 효능감이 인지적 매개 과정을 통해 보호동기이론의 위협 평가와 대처 평가라는 새로운 변인으로 변형되어, 이를 통해 공포소구의 영향으로 인한 태도 변화의 과정을 더욱 깊게 이해할 수 있다고 주장하였다[29]. 이민규와 김영은(2009)은 건강과 질병이 주요 쟁점으로 부각되는데 있어서, 미디어는 건강 관련 정보를 제공하고 있으며, 정보 전달의 순기능과 선정적인 보도로 인한 불필요한 공포감을 조성하는 역기능을 동시에 수행하고 있다고 주장하였다. 이에 따라 보호동기이론을 바탕으로 하여 질병에 관한 정보 이용의 다양한 효과에 대해서 살펴보고, 이 같은 정보가 이용자의 공포감과 보호동기추구를 이끌어내고 궁극적으로 건강 증진 의사를 유도하는 요소임을 실증하였다[30]. 박찬욱과 이상우(2014)는 정보 주체인 개인을 대상으로 개인 정보보호 행동을 유도하는 방안에 대한 연구가 부족한 실정이라고 주장하였다. 이를 보완하기 위해 보호 동기이론을 기반으로 온라인 사용자들의 개인정보보호 행동의 변화를 설명하였다[31].

개인정보 침해 관련 정보 제공 서비스의 수용과 행동에 미치는 영향에 대하여 연구하기 위해, 정보 기술 관련한 서비스 수용과 보호 동기 이론과 관련된 선행 연구들을 살펴보았다. 서비스 수용에 관한 선행 연구들은 기술 수용 이론으로부터 출발하여, 합리적 행위 이론, 계획적 행동 이론 등 여러 이론과 관련되어 연구가 진행되었고, 더 나아가 제품이나 기술과 관련된 수용 이외에 서비스의 수용에 대하여 연구되었다. 본 논문에서 연구하고자 하는 개인정보 침해와 정보 제공에 대한 서비스 수용 연구는 피해를 방지하는 정보를 개인에게 제공하고, 개인이 정보를 수용할 것인지, 더 나아가 정보를 활용하여 행동으로 이어질 것인지에 대하여 면밀히 살펴보고자 한다. 이러한 내용은 외부 요인이 개인의 인지 요인과 연결되고, 개인의 인지 요인이 태도, 이용 의사, 실제 행동으로 까지 영향을 미친다는 기술 수용 모형의 연구 내용과 관련된다는 것을 확인하였다. 이를 통해 기술 수용 모형을 기초로 개인정보 침해 정보 제공 서비스에 대한 수용 연구 모형을 설계하였다.

서비스 수용 관점 이외에 개인 정보 침해와 관련된 요인들에 대하여 보호 동기 이론과 관련된 선행연구들을 살펴보았다. 문헌 연구를 진행하였다. 보호 동기 이론과 관련한 연구들은 질병과 주로 관련된 연구가 진행되었다. 개인정보 침해가 질병과 달리 직접적인 신체적 피해 및 정신적인 피해를 입히지 않는다. 하지만 개인에게 미칠 수 있는 금전적 피해와 정신적 피해 등을 직·간접적으로 발생 시킬 수 있으며, 이러한 결과가 개인의 인식 및 행동으로 변화가 가능하며 확산될 수 있다. 본 연구에서는 진행하고자 하는 개인정보 침해 관련 정보 제공 서비스는 개인정보 침해로부터 일반인이 스스로의 개인정보를 보호할 수 있도록 정보를 제공한다는 점에서, 보호 동기를 일으키고 태도와 행동의 변화를 일으킨다는 점에서 보호 동기 이론과 관련이 있다. 이에 보호 동기 이론에 대한 문헌 연구 결과를 바탕으로 서비스 수용과 연결하여 연구 모형을 설계하였다.

IV. 연구 모형 및 설계

4.1 연구 모형

사례 연구를 통해 정의한 서비스에 대하여 수용 의도와 개인정보보호 행동에 미치는 영향 요인을 분석하기 위해 연구 모형을 설계하였다. 본 연구의 모형은 기술 수용 모형을 기반으로 연구된 서비스 수용 연구 모형을 기반으로 하였으며, 개인정보보호 분야의 특성을 반영하기 위해 보호 동기 이론을 활용하여 연구 모형을 보강하였다.

기존의 기술 수용 모형은 외부요인으로 인하여, 인지된 유용성, 인지된 이용 용이성, 이용 태도, 행동적 이용 의사, 실제 시스템 이용이 영향 관계에 따라 연결되어 있다. 본 연구에서는 기술 수용 모형의 기반으로 하지만 영향 요인 중 인지된 이용 용이성을 제외하였다. 정보 제공에 대한 서비스는 서비스 자체에서의 이용이 발생하는 것이 아니라, 정보 전달에 초점을 두고 있다. 이에 따라 이용 용이성 보다는 인지된 신뢰성이 서비스에 대한 태도에 영향을 미칠 것이라는 연구 의도를 가지고 기존 기술 수용 모형을 수정하여 본 연구의 모형을 설계하였다. 이에 따라 인지된 유용성과 인지된 신뢰성은 태도에 영향을 미치고, 태도는 서비스 수용의도에 영향을 미치며, 더 나아가 수용 의도는 실제 개인의 개인정보보호 행동으로 영향을 미친다는 연구 모형을 설계하였다.

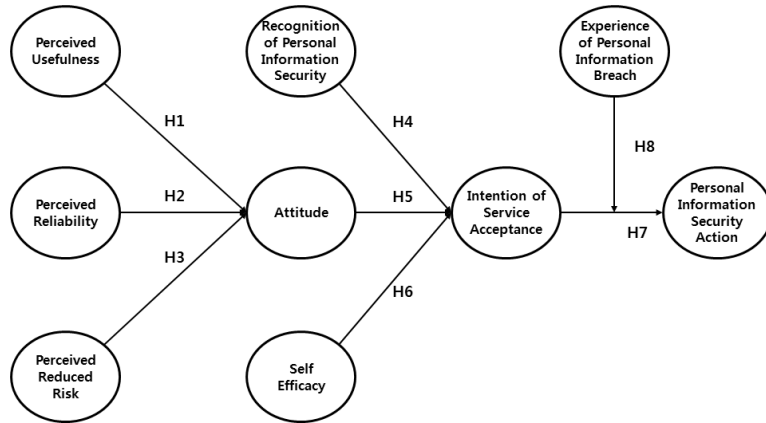


Fig. 1. Research Model

보호 동기 이론에 대한 문헌 연구를 통해 인지된 위험 감소, 자기 효능감, 개인정보보호 인식 수준, 개인정보 침해 경험을 연구 변인으로 도출하였다. 인지된 위험 감소는 정보 제공을 통해 위험이 감소할 것이라는 기대를 뜻하며 위험에 대한 보호 기대와 관련 있다. 자기 효능감은 개인정보 침해라는 위협으로부터 자신의 정보를 보호할 수 있는 능력에 대한 개인의 믿음을 뜻한다. 이는 보호 동기 이론의 대처 평가로부터 도출하였다. 개인정보보호 인식 수준과 개인정보 침해 경험은 자신의 위험에 대한 인식 수준과 실제 위험에 닥친 경험이 각각 태도와 행동에 영향을 미칠 수 있기 때문에 본 연구의 변인으로 도출하였다. 개인정보보호 인식 수준은 위험에 대한 인식 수준이기 때문에 태도와 함께 수용 의도에 영향을 미치며, 개인정보 침해 경험은 수용 의도가 형성된 이후 개인정보보호 행동을 할 때, 개인정보 위협과 개인(자신)과의 직접적인 연관성이 개인정보보호 행동에 영향을 미칠 것으로 추측하였다. 이를 바탕으로 본 연구의 모형을 설계하였다(Fig 1).

4.2 연구가설

본 연구의 서비스는 태도에 인지된 유용성, 신뢰성, 위험감소가 영향을 미친다. 그 중에서도 태도는 서비스 수용에 중요한 요소이며, 주관적인 규범과 행동 통제가 영향을 미친다. 태도에 미치는 영향 요소 중 인지된 유용성(Perceived Usefulness)은 서비스를 이용할 예정인 일반인에게 있어 중요한 요소이다[18]. 따라서 다음과 같은 가설을 도출하였다.

가설 1: 개인정보 침해 정보 제공 서비스에 대한

인지된 유용성(Perceived Usefulness)은 태도에 영향(+)을 미칠 것이다

인지된 신뢰성(Perceived Reliability)는 정보를 전달 및 제공하는 매체에 대한 태도를 형성하는 중요한 요소 중 하나이다. 정보를 전달하는 서비스는 신뢰성이 중요하다. 또한, 서비스의 인지된 신뢰성은 태도를 형성하는데 유용성만큼 중요한 요소이다. 신뢰를 갖추지 못한 정보는 일반인의 부정적인 의도를 형성할 수 있도록 하며, 사용하지 않는 현상이 발생할 수 있다[21]. 따라서 다음과 같은 가설을 도출하였다.

가설 2: 개인정보 침해 정보 제공 서비스에 대하여 인지된 신뢰성(Perceived Reliability)은 태도에 영향(+)을 미칠 것이다.

인지된 위험 감소(Perceived Reduced Risk)는 정보보호 서비스에서 중요한 요소이다. 서비스의 핵심 기능은 정보를 보호할 수 있고, 정보 자산을 위협하는 위험 요소를 감소시키는 것이다[34]. 따라서 다음과 같은 가설을 도출하였다.

가설 3: 개인정보 침해 정보 제공 서비스에 대하여 인지된 위험 감소(Perceived Reduced Risk)는 태도에 영향(+)을 미칠 것이다.

개인정보보호 인식 수준(Recognition of Personal Information Security)은 서비스를 사용할 것인지 여부에 영향을 미친다. 개인정보보호에 대한 인식 수준이 낮다면, 서비스에 대한 태도가 좋을 수 있음에도 서비스 수용까지 영향을 미칠 수 없

게 된다. 이렇듯 개인정보보호에 대한 인식하는 정도는 개인정보보호와 관련된 서비스를 수용하는데 있어 중요한 요소로서 작용한다[24]. 따라서 다음과 같은 가설을 도출하였다.

가설 4: 개인정보보호 인식 수준(Recognition of Personal Information Security)은 수용 의도에 영향(+)을 미칠 것이다.

태도(Attitude)는 수용 의도에 영향을 미치는 중요한 요소이다. 일반인의 서비스에 대한 태도는 서비스 수용에 직접적으로 영향을 미친다. 서비스에 대한 수요를 파악할 시 태도를 파악하는 것은 중요하며, 도입 후 의도를 파악하는 중요한 영향 요소이다[32]. 따라서 다음과 같은 가설을 도출하였다.

가설 5: 개인정보 침해 정보 제공 서비스에 대하여 태도(Attitude)는 수용 의도에 영향(+)을 미칠 것이다.

자기 효능감(Self Efficacy)은 본인이 적절하게 행동할 것이라는 기대감과 자신감으로서, 서비스에 대하여 일반인이 적절하게 행동할 지에 대한 기대와 자신은 서비스 수용 의도에 영향을 미친다[33]. 따라서 다음과 같은 가설을 도출하였다.

가설 6: 개인정보 침해 정보 제공 서비스에 대하여 자기 효능감(Self Efficacy)은 수용 의도에 영향(+)을 미칠 것이다.

서비스 수용 의도(Intention of Service Acceptance)는 실제 이용에 영향을 미친다. 태도가 수용 의도에 영향을 미치고, 수용 의도가 개인정보보호 행동으로 이동되는 지에 대하여 분석이 필요하다. 이를 통해 영향이 미치는 것 뿐 만 아니라, 결과로서 발휘될 수 있는 요소이다[32]. 따라서 다음과 같은 가설을 도출하였다.

가설 7: 개인정보 침해 정보 제공 서비스에 대한 수용 의도(Intention of Service Acceptance)는 개인정보보호 행동(활동)에 영향(+)을 미칠 것이다.

개인정보 침해 및 유출에 대한 걱정과 염려가 커질수록 일반인의 개인정보보호 행동에 긍정적인 영향을 미친다. 우려와 더불어, 개인정보 침해 경험(Experience of Personal Information Breach)은 이러한 정보보호 활동에 영향을 미친다. 또한, 정보보호 서비스에 대한 수용 의도가 정보보호

활동에 영향을 미치는데 개인정보 침해 경험이 영향을 미친다[24]. 따라서 다음과 같은 가설을 도출하였다.

가설 8: 개인정보 침해 경험(Experience of Personal Information Breach)은 수용 의도와 개인정보보호 행동 사이의 상관관계에 영향(+)을 미칠 것이다.

4.3 연구변수의 조작적 정의

인지된 유용성(Perceived Usefulness)은 개인 정보 침해 관련 정보 제공 서비스는 가치가 있으며, 적절한 기능을 수행할 것이라는 신념의 정도를 뜻한다.

인지된 신뢰성(Perceived Reliability)은 개인 정보 침해 관련 정보 제공 서비스에 대하여 신뢰할 수 있다고 믿는 정도를 뜻한다.

인지된 위험 감소(Perceived Reduced Risk)는 서비스를 이용함으로써, 일반인의 개인정보를 다양한 위협들로부터 보호하고, 위험한 상황을 완화 시켜줄 것이라고 믿는 정도를 의미한다.

개인정보보호 인식 수준(Recognition of Personal Information Security)은 개인이 지켜야 할 자산이며, 보호하기에 충분한 가치가 있는 자산을 인지하는 정도이다.

태도(Attitude)는 개인정보 침해 관련 정보 제공 서비스에서 제공하는 정보와 서비스에 대한 개인의 태도를 뜻한다. 태도는 개인의 행동과 행동을 실시하기 이전 그에 대한 의도를 구성하는데 중요한 요소이다.

자기 효능감(Self Efficacy)은 개인이 개인정보 침해 관련 정보 제공 서비스를 이용함에 있어 원활하게 이용할 수 있는 내적 자원을 가지고 있음을 의미하며, 이에 대한 자신감 혹은 기대감을 뜻한다.

서비스 수용 의도(Intention of Service Acceptance)는 개인정보 침해 관련 정보 제공 서비스를 이용하고자 하는 일반인의 가능성을 뜻한다.

개인정보 침해 경험(Experience of Personal Information Breach)은 개인정보 침해 경험을 뜻한다. 개인정보 침해 경험은 일반인의 실제 침해 경험 뿐 만 아니라, 유출 사실 여부를 조회하거나 통보를 받은 경험을 뜻한다.

개인정보보호 행동(Personal Information Security Action)은 개인정보 자산을 보호하기 위

해 수행하는 활동으로서, 기초적인 예방, 대처 활동과 더불어 개인정보 침해 신고, 손해 배상 청구 등 모든 개인정보보호 행동을 뜻한다. 서비스를 통해 태도를 구성하고, 의도가 있으며, 더 나아가 행동으로 옮기기까지의 일련의 연결을 뜻한다.

V. 가설검증 및 분석 결과

5.1 표본 구성과 분석방법

5.1.1 자료 수집 및 표본의 특성

연구가설의 검증을 위해 휴대폰을 사용하는 일반인을 대상으로 설문조사를 실시하였다. 구글 설문지를 구성하여 배포하였다. 총 434부를 회수하여 분석에 사용하였다. 응답자 중 남성은 193명(44.4%), 여성은 241명(55.6%)이었다(Table 1).

Table 1. Feature of Respondents by Gender

Gender	# of Respondents	Ratio(%)
Male	193	44.4%
Female	241	55.6%
Total	434	100.0%

연령대는 20대가 전체 434명 중 369명(85.0%)로 가장 높았다. 나머지 연령대는 19세 미만 6명(1.4%), 30~39세 30명(6.9%), 40~49세 19명(4.4%), 50세 이상 10명(2.3%)으로 나타났다(Table 2).

Table 2. Feature of Respondent by Age

Age	# of Respondents	Ratio(%)
~19	6	1.4%
20~29	369	85.0%
30~39	30	6.9%
40~49	19	4.4%
50~	10	2.3%
Total	434	100.0%

개인정보 침해 경험이 있는 응답자는 280명(64.5%)이다. 개인정보 유출 조취를 해본 적이 있는 응답자는 221명(50.9%)이다. 이는 자신의 개인정보가 유출되었음을 인지하고 있는 사람이 인지 못하는 사람보다 더 많다는 것을 알 수 있다. 하지만,

유출 조취 경험은 221명(50.9%)으로, 인지하였어도 실제 조취하여 확인하지 않는 인원이 있다는 것을 알 수 있다(Table 3).

Table 3. Experience of Personal Information Breach and Breach Recognition

Experience	Yes(%)	No(%)	Total(%)
Personal information breach	280 (64.5%)	154 (35.5%)	434 (100.0%)
Personal information breach recognition	221 (50.9%)	213 (49.1%)	434 (100.0%)

개인정보 침해 관련 정보 제공 서비스 혹은 유사한 서비스가 있다면 사용할 의사가 있는 응답자는 전체 434명 중 300명(69.1%)로 나타났다. 이는 개인정보와 개인정보보호에 대하여 중요하게 인식하는 수준이 높아짐에 따라, 사용 의도 역시 높게 나타난 것을 알 수 있다. 이를 통해 개인정보 침해 관련 정보 제공 서비스가 도입 될 경우, 일반인의 인식이 긍정적인 방향으로 나타날 수 있음을 알 수 있다. 의도가 없는 응답자는 30.9%로 나타났다(Table 4).

Table 4. Intention of Service Acceptance

Intention	Yes(%)	No(%)	Total
Result	300(69.1)	134(30.9)	434

개인정보 침해 관련 정보 제공 서비스와 요인간의 상관관계 여부와 영향을 도출하기 위하여 Smart PLS 2.0을 사용하여 분석하였다. 분석을 위하여 총 434부 중 서비스 사용 의도가 없다고 응답한 134부를 제외한 300부를 사용하였다.

5.1.2 분석방법

연구모형의 분석을 위해 Smart PLS(Partial Least Square) 2.0을 활용하였다. PLS 분석은 다변량 분석을 위한 구조방정식 모델의 하나로 요인 분석법을 활용하여 구조방정식 방법의 큰 제약이었던 수집된 자료의 정규분포에 대한 엄격한 가정으로부터 자유로운 방법이다. 또한 이론적인 구조에 대한 평가와 측정모형에 대한 평가가 가능하다[35]. 이에 연구 구성 요인들의 설명력을 측정하고자 본 연구의 분

Table 5. Analysis of Internal Consistency

Component	Composite Reliability	Cronbachs Alpha
Perceived Usefulness	0.9060	0.8443
Perceived Reliability	0.9363	0.9089
Perceived Reduced Risk	0.9331	0.9035
Recognition of Personal Information Security	0.9486	0.9186
Attitude	0.9360	0.9085
Self Efficacy	0.9258	0.8931
Intention of Service Acceptance	0.9458	0.9139
Personal Information Security Action	0.9402	0.9153
Experience of Personal Information Breach	0.9437	0.9105

석방법으로 채택하였다.

5.2 타당성과 신뢰성 검증

PLS 분석은 측정문항과 구성개념에 대해 내적일관성, 집중타당성, 판별타당성 검증을 요구한다. 내적일관성 검증을 위해 인지된 유용성, 인지된 신뢰성, 인지된 위험 감소, 태도, 인지된 용이성, 개인정보보호 인식 수준, 서비스 수용 의도, 개인정보보호 행동을 대상으로 Fornell & Larcker(1981)의 복합신뢰도(Composite Reliability)와 신뢰성을 분석하였다[36]. 복합신뢰도는 Thompson 등(1995)이 주장하는 기준치인 0.7 이상으로 나타났고, 신뢰성 검증에 널리 사용되는 크론바하 알파 값은 0.7 이상으로 나타났[37]. 따라서 내적일관성은 적합한 것으로 나타났다(Table 5).

5.2.1 집중타당성

집중타당성은 AVE(average variance extracted)와 구성개념에 대한 요인적재값으로 검증하였다. AVE는 Fornell & Larcker(1981), Chin(1998) 등이 주장하는 기준치인 0.5 이상으로 나타났고, 구성개념의 요인적재값은 모두 Fornell & Larcker(1981)의 검증 기준치인 0.7 이상으로 나타났[36].

5.2.2 판별타당성

판별타당성은 구성개념 간의 상관계수 값들의 대

각선 축에 표시되는 AVE의 제곱근 값이 다른 구성개념 간의 상관계수 값보다 큰가의 여부로 검증하였다[36]. 분석결과, AVE의 제곱근 값 중 가장 작은 값(0.8701)이 가장 큰 상관계수 값(0.7432)보다 상회하였기 때문에 판별타당성은 적합한 것으로 나타났다.

5.3 가설 검증

PLS 분석에서 경로모형의 설명력은 분산설명력(Explained Variance)인 R²값으로 표현된다. PLS의 R² 분석결과, 서비스 수용의도는 개인정보보호활동의 55.50%를 설명하였다. 이는 Falk & Miller가 제시한 적정 검정력 10%를 상회하는 것이다[38].

다음으로, 연구모형의 적합도(goodness-of-fit, GoF)를 검증한 결과, GoF 영향도는 0.5853으로서, Wetzels et. al이 제시한 강(large)보다 크기 때문에 모형의 적합도가 매우 높은 것으로 나타났다[39](Fig 2).

PLS 분석을 통해 경로계수와 경로계수의 유의성을 검증하였다. 이를 위해 전체표본을 이용하여 구조모형에 대한 β value(경로계수)를 구하고, PLS에서 제공하는 부스트랩 방식을 이용하여 독립변수와 종속변수 간에 성형관계(관련성)이 존재하는 정도를 나타내는 t-value를 산출하였다. 또한 각 t-value에 대한 신뢰도를 나타내는 p-value를 산출하였다. 신뢰도는 3구간으로, $p < 0.001$ (***)이 가장 높으며, $p < 0.01$ (**), $p < 0.05$ (*) 순으로 신뢰도를 나타낸다(Table 6).

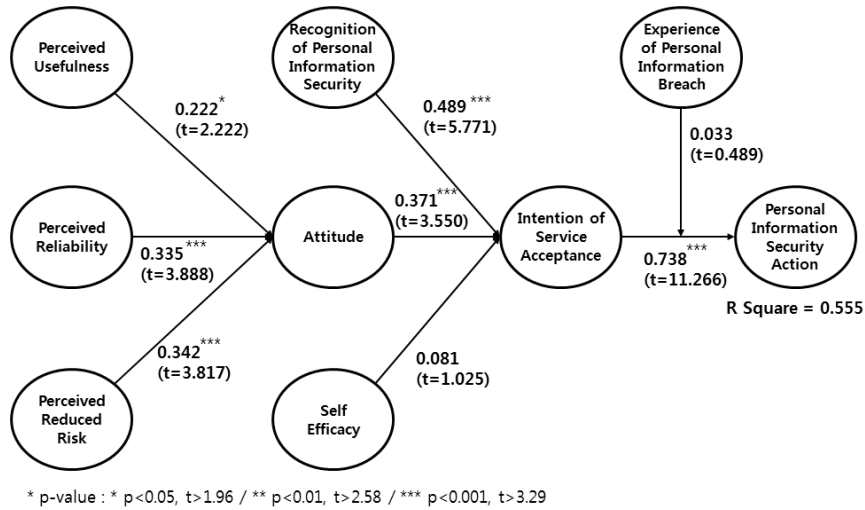


Fig. 2. Analysis Results

Table 6. Analysis Result

Hypothesis	β value (Path coefficient)	t-Value	p-Value	Result
Hypothesis 1	0.222	2.222	*	Adopt
Hypothesis 2	0.335	3.888	***	Adopt
Hypothesis 3	0.342	3.817	***	Adopt
Hypothesis 4	0.489	5.771	***	Adopt
Hypothesis 5	0.371	3.550	***	Adopt
Hypothesis 6	0.081	1.025	0.085	Reject
Hypothesis 7	0.738	11.266	***	Adopt
Hypothesis 8	0.033	0.489	0.412	Reject

가설1 채택: 개인정보 침해 관련 정보 제공 서비스에 대한 인지된 유용성(Perceived Usefulness)이 태도(Attitude)에 영향을 미친다는 가설을 분석한 결과 β값은 0.222, t값은 2.2220(p < 0.05)으로 유의하게 나타나 가설1을 채택하였다.

가설2 채택: 개인정보 침해 관련 정보 제공 서비스에 대한 인지된 신뢰성(Perceived Reliability)이 태도(Attitude)에 영향을 미친다는 가설을 분석한 결과 β값은 0.335, t값은 3.8880(p < 0.001)으로 유의하게 나타나 가설2를 채택하였다.

가설3 채택: 개인정보 침해 관련 정보 제공 서비스에 대한 인지된 위험 감소(Perceived Reduced Risk)가 태도(Attitude)에 영향을 미친다는 가설을 분석한 결과 β값은 0.342, t값은 3.8170(p < 0.001)으로 유의하게 나타나 가설3을 채택하였다.

가설4 채택: 개인의 개인정보보호 인식 수준 (Recognition of Personal Information Security)이 개인정보 침해 관련 정보 제공 서비스 수용 의도(Intention of Service Acceptance)에 영향을 미친다는 가설을 분석한 결과 β값은 0.489, t값은 5.7710(p < 0.001)으로 유의하게 나타나 가설4를 채택하였다.

가설5 채택: 개인정보 침해 관련 정보 제공 서비스에 대한 태도(Attitude)가 서비스 수용 의도(Intention of Service Acceptance)에 영향을 미친다는 가설을 분석한 결과 β값은 0.371, t값은 3.5500으로 유의하게 나타나 가설5(p < 0.001)를 채택하였다.

가설6 기각: 개인정보 침해 관련 정보 제공 서비스에 대한 자기 효능감(Self Efficacy)이 개인정보

침해 관련 정보 제공 서비스 수용 의도(Intention of Service Acceptance)에 영향을 미친다는 가설을 분석한 결과 β 값은 0.081, t 값은 1.0250($p < 0.085$)으로 유의하게 나타나지 않아 가설6을 기각하였다.

가설7 채택: 개인정보 침해 관련 정보 제공 서비스에 대한 수용 의도(Intention of Service Acceptance)가 실제 개인정보보호 활동(Personal Information Security Action)에 영향을 미친다는 가설을 분석한 결과 β 값은 0.738, t 값은 11.266($p < 0.05$)으로 유의하게 나타나 가설7을 채택하였다.

가설8 기각: 개인정보 침해 관련 정보 제공 서비스에 대한 수용 의도(Intention of Service Acceptance)가 실제 개인정보보호 활동(Personal Information Security Action)에 영향을 미치는데 개인정보 침해 경험(Experience of Personal Information Breach)이 영향을 미친다는 가설을 분석한 결과 β 값은 0.033, t 값은 0.4890으로 유의하게 나타나지 않아 가설8을 기각하였다.

따라서 본 연구에서 제시한 8개의 가설 중 가설6과 가설8의 경우 유의하지 않을 것으로 나타났고, 나머지는 모두 유의한 것으로 나타났다. 유의하게 나타난 가설 6개를 채택하였다.

5.4 연구결과와 논의

연구결과의 의미를 태도, 수용 의도, 개인정보보호 활동에 미치는 영향 순으로 살펴보면 다음과 같다.

5.4.1 인지된 위험 감소

인지된 위험 감소(Perceived Reduced Risk)는 서비스에 대한 태도에 가장 큰 영향($\beta=0.342$)을 미치는 것으로 나타났다. 이는 개인정보 침해 관련 정보 제공 서비스의 주목적인 위험 감소가 서비스에 대한 태도가 가장 영향을 미치고, 밀접한 관계가 있음을 나타낸다. 개인정보 침해 관련 정보 제공 서비스가 도입된다면, 주목적과 주요 전달 정보가 서비스에 대한 태도를 형성하는 데에 가장 많은 영향을 미칠 수 있음을 의미한다. 즉 서비스를 도입하기 이전에, 해당 서비스가 인지된 위험을 감소시킬 수 있는지를 사전에 파악한 후 도입해야 함을 알 수 있다.

5.4.2 인지된 신뢰성

인지된 신뢰성(Perceived Reliability)은 서비스에 대한 태도에 두 번째로 큰 영향($\beta=0.335$)을 미치는 것으로 나타났다. 이는 개인정보 침해 관련 정보 제공 서비스에서 제공하는 정보와 서비스 자체에 대한 신뢰가 태도에 많은 영향을 미치고, 밀접한 관계가 있음을 나타낸다. 개인정보 침해 관련 정보 제공 서비스가 도입 될 시, 일반인의 신뢰를 확보할 수 있도록 서비스가 제공되어야 한다. 또한 제공되는 정보는 일반인들에게 신뢰를 가지고 수용하고, 활용할 수 있도록 해야 함을 알 수 있다.

5.4.3 인지된 유용성

인지된 유용성(Perceived Usefulness)은 서비스에 대한 태도에 영향($\beta=0.222$)을 미치는 것으로 나타났다. 이는 개인정보 침해 관련 정보 제공 서비스에서 제공하는 정보와 서비스가 활용도가 있어야 하고, 개인정보보호의 목적에 적합하도록 기능을 수행해야 한다. 개인정보 침해 관련 정보 제공 서비스가 도입될 경우, 개인정보를 보호할 수 있도록 적합한 기능을 수행 할 수 있어야 한다.

5.4.4 개인정보보호 인식 수준

개인정보보호 인식 수준(Recognition of Personal Information Security)은 서비스 수용 의도에 가장 큰 영향($\beta=0.489$)을 미치는 것으로 나타났다. 본 결과를 통해 일반인의 개인정보보호 인식 수준이 높을수록 개인정보 침해 관련 정보 제공 서비스를 수용할 의도가 높다는 것을 나타낸다. 개인정보보호 인식 수준이 높을 경우 정보를 보호하고자 하는 의도가 있음을 의미한다. 이를 통해 개인정보보호 인식 수준이 높은 일반인을 물론, 낮은 일반인도 개인정보 침해 관련 정보 제공 서비스를 수용할 수 있도록 노력해야 한다는 것을 알 수 있다.

5.4.5 태도

개인정보 침해 관련 정보 제공 서비스에 대한 태도(Attitude)는 서비스 수용 의도에 영향($\beta=0.371$)을 미치는 것으로 나타났다. 이는 서비스에 대한 태도가 긍정적일수록 서비스 수용 의도가 높다

는 것을 나타낸다. 서비스 수용에 관한 선행 연구들의 결과와 동일하게 태도가 수용 의도로 밀접하게 연결된다는 것을 알 수 있다.

5.4.6 서비스 수용 의도

개인정보 침해 관련 정보 제공 서비스에 대한 수용 의도(Intention of Service Acceptance)는 개인정보보호 활동에 가장 큰 영향($\beta=0.738$)을 미치는 것으로 나타났다. 이는 일반인이 서비스 수용 의도가 있다면, 서비스를 활용하여 개인정보보호 활동을 수행한다는 것을 나타낸다. 개인정보 침해 관련 정보 제공 서비스가 개인정보보호 활동으로 직접적으로 연결될 수 있다는 것을 나타내며, 더 나아가 개인정보보호 수준을 향상시킬 수 있는 수단임을 의미한다. 개인정보 침해 관련 정보 제공 서비스가 개인정보보호 활동을 수행하는데 기준이 될 수 있음을 알 수 있다.

5.4.7 자기 효능감

자기 효능감(Self Efficacy)은 개인정보 침해 관련 정보 제공 서비스의 수용 의도에 영향($\beta=0.081$)을 미치지 않는 것으로 나타났다. 일반인의 서비스 및 정보 활용 능력을 가지고 있고, 이에 따른 행동을 할 수 있다는 기대와 신념이 수용 의도에 영향을 미치지 않는다는 것을 의미한다.

5.4.8 개인정보 침해 경험

개인정보 침해 관련 정보 제공 서비스에 대한 수용 의도와 개인정보보호 행동 사이에 개인정보 침해 경험(Experience of Personal Information Breach)이 영향($\beta=0.033$)을 미치지 않는 것으로 나타났다. 이는 서비스에 대한 수용 의도가 개인정보보호 행동으로 이어지는데 개인정보 침해 경험에 차가 없이 중요하다는 것을 나타낸다. 또한, 개인정보 침해 경험 유·무와 관계없이 개인정보보호 활동이 이루어짐을 알 수 있다.

VI. 결 론

본 연구를 통해 개인정보 침해와 관련된 정보를 제공하는 것이 중요하며, 이러한 정보가 주어진다면

일반 개인들은 사용할 의사가 있다는 것으로 확인하였다. 더 나아가, 개인정보 침해 정보 제공 서비스가 개인의 개인정보보호 활동으로까지 연결될 수 있음을 검증하였다. 따라서 개인정보보호와 관련된 정보를 제공하는 활동이 개인정보보호 수준을 향상시키는데 도움을 줄 것이다.

본 연구의 시사점은 다음과 같다. 첫째, 개인의 개인정보보호 인식이 있음에도 불구하고, 개인정보 유출 사실을 확인하지 않고 있는 것으로 나타났다. 이는 개인이 개인정보보호에 대하여 수동적인 태도를 가지고 있는 것으로 해석될 수 있다. 하지만 응답자들은 개인정보 침해 관련 정보가 제공된다면, 정보를 수용하고 개인정보보호 활동을 수행할 것으로 결과가 도출되었기 때문에, 개인정보 침해 관련 정보 제공 서비스가 개인정보보호에 대한 수동적인 태도도 일부 적극적인 태도로 전환시킬 수 있는 방안이 될 것이다. 둘째, 개인정보 침해 관련 정보를 제공하는 것에 대한 중요성을 파악함으로써 개인정보보호 관련 정책 수립에 도움을 줄 수 있을 것이다. 셋째, 개인정보 침해와 관련된 정보 제공에 대하여 개인의 영향과 활용 가능성을 검증하였다는 것이다. 정보보호 분야에서 보호기술, 제품, 취약점, 바이러스 등의 정보를 제공하는데 초점을 두었기 때문에 연구의 범위를 확장하였다는 점에서 의의를 갖는다.

본 연구에서는 가상의 서비스에 대하여 일반인을 대상으로 사용 의도를 물었기 때문에 조사결과의 활용에는 어느 정도 한계가 있을 수 있다. 또한 서비스의 가격이 무료라는 가정 하에 물었기 때문에 유료 서비스일 경우 다르게 응답할 수 있다.

References

- [1] Bo-Mi Choi, Min-Jung Park, and Sang-Mi Chai, "An investigation of users' privacy protection behaviors : Factors affecting privacy protection technology adoption," *Information Systems Review*, 17(30), pp. 77-94, Dec. 2015.
- [2] Young-Soo Son, and Jin-Ho Yu, "Consideration of privacy infringement and utilization of information security service," *Proceedings of the Korea Society of Management information*

- Systems*, pp. 355-359, Nov. 2014.
- [3] Soo-Jung Kim, and Min-Jung Sung, "The effects of the perception of and online risk and prior knowledge on public's communication behavior," *The Korean Journal of Advertising and Public Relations*, 13(4), pp. 528-567, Oct. 2011.
- [4] Jeong-Gyu Kim, and Kyung-Ho Lee, "FAIR-based loss measurement caused by personal information breach of a company," *Journal of the Korea Institute of Information Security & Cryptology*, 27(1), pp. 129-145, Feb. 2017.
- [5] <http://www.privacy.kisa.or.kr/kor/main.jsp>(accessed on 2016.10.12.)
- [6] <http://www.eprivacy.go.kr/introCleanCenter.do>(accessed on 2016.10.12.)
- [7] <http://www.krcert.or.kr/main.do>(accessed on 2016.10.12.)
- [8] http://www.nis.go.kr/AF/1_7.do(accessed on 2016.10.12.)
- [9] <http://www.us-cert.gov/ncas>(accessed on 2016.10.12.)
- [10] <http://www.cert.org.cn>(accessed on 2016.10.12.)
- [11] <http://www.jpCERT.or.jp>(accessed on 2016.10.12.)
- [12] R. Whitaker, *The End of Privacy: How Total Surveillance is Becoming a Reality*, The New Press, 2010.
- [13] Kyoung-Jin Choi, "Right to be forgotten-A personal information perspective," *Korea Association for Informedia Law*, 16(2), pp. 97-120, Aug. 2012.
- [14] A. H. Crespo, I. R. del Bosque, and M. G. de los Salmones Sanchez, "The influence of perceived risk on Internet shopping behavior: a multidimensional perspective," *Journal of Risk Research*, vol. 12, no. 2, pp. 259-277, Feb. 2009.
- [15] R. Heatherly, M. Kantarcioglu, and B. Thuraisingham, "Preventing private information inference attacks on social networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 8, pp. 1849-1862, Jun. 2012.
- [16] Chung-Hun Lee, Yu-Mi Ko, and Beom-Soo Kim, "A framework and guidelines for personal data breach notification act," *Journal of the Korea Institute of Information Security & Cryptology*, 21(5), pp. 169-179, Oct. 2011.
- [17] M. Hauswirth, and M. Jazayeri, "A component and communication model for push systems," *Software Engineering-ESEC/FSE'99*, pp. 20-38, Aug. 1999.
- [18] K. Juvva, and R. Rajkumar, "A real-time push-pull communications model for distributed real-time and multimedia systems," *No. CMU-CS-99-107. Carnegie-mellon Univ pittsburgh Pa Dept of Computer Science*, Jan. 1999.
- [19] B. Lepori, L. Cantoni, and R. Mazza, "Push communication services: a short history, a concrete experience and some critical reflections," *Studies in Communication Sciences*, vol. 2, no. 1, pp. 149-164, Feb. 2002.
- [20] T. Us, N. Jensen, M. Lind, and S. B. Jorgensen, "Fundamental principles of alarm design," *International Journal of Nuclear Safety and Simulation*, vol. 2, no. 1, pp. 44-51, Feb. 2011.
- [21] Mi-Na Im and Jung-Sik Lee, "A study on usage of smartphone push notification," *HCI 2013*, pp. 388-392, Jan. 2013.
- [22] M. E. Fishbein, *Readings in Attitude Theory and Measurement*, Wiley, 1967.

- [23] I. Ajzen, "From intentions to actions: A theory of planned behavior," *In Action Control*, Springer Berlin Heidelberg, pp. 11-39, 1985.
- [24] S. Taylor and P. A. Todd, "Understanding information technology usage: A test of competing models," *Information Systems Research*, vol. 6, no. 2, pp. 144-176, Jun. 1995.
- [25] M. H. Hsu and C. M. Chiu, "Internet Self Efficacy and electronic service acceptance," *Decision Support Systems*, vol. 38, no. 3, pp. 369-381, Dec. 2004.
- [26] H. P. Shih, "An empirical study on predicting user acceptance of e-shopping on the web," *Information & Management*, vol. 41, no. 3, pp. 351-368, Jan. 2004.
- [27] S. Y. Hung and C. M. Chang, "User acceptance of WAP services: test of competing theories," *Computer Standards & Interfaces*, vol. 27, no. 4, pp. 359-370, Apr. 2005.
- [28] S. Y. Hung, C. M. Chang, and T. J. Yu, "Determinants of user acceptance of the e-Government services: The case of online tax filing and payment system," *Government Information Quarterly*, vol. 23, no. 1, pp. 97-122, 2006.
- [29] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change," *The Journal of Psychology*, vol. 91, no. 1, pp. 93-114, June. 1975.
- [30] Min-Kyu Lee and Young-Eun Kim, "A study on effects of disease information use on the internet: Based on the protection motivation theory," *Journal of Communication Science*, 9(4), pp. 506-539, Dec. 2009.
- [31] Chan-Ouk Park and Sang-Woo Lee, "A study of the user privacy protection behavior in online environment: Based on protection motivation theory," *Journal of Internet Computing and Services*, 15(2), pp. 59-71, Apr. 2014.
- [32] H. F. Lin, "Predicting consumer intentions to shop online: An empirical test of competing theories," *Electronic Commerce Research and Applications*, vol. 6, no. 4, pp. 433-442, Feb. 2008.
- [33] T. D. Susanto and R. Goodwin, "User acceptance of SMS-based e-government services," In *International Conference on Electronic Government*, pp. 75-87, Aug. 2011.
- [34] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," *MIS Quarterly*, vol. 27, no. 3, pp. 425-478, Sep. 2003.
- [35] R. Noonan and H. Wold, "PLS path modeling with indirectly observed variables: a comparison of alternative estimates for the latent variable," *Systems under Indirect Observation*, Part II, pp. 75-94, 1982.
- [36] C. Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," *Journal of Marketing Research*, vol. 18, no. 1, pp. 39-50, Feb. 1981.
- [37] C. B. Thompson, "Apoptosis in the pathogenesis and treatment of disease," *Science*, vol. 267, no. 5203, pp. 1456-1462, Mar. 1995.
- [38] R. F. Falk and N. B. Miller, *A Primer for Soft Modeling*, University of Akron Press, 1992.
- [39] M. Wetzels, G. Odekerken-Schröder, and C. Van Oppen, "Using PLS path modeling for assessing hierarchical

construct models: Guidelines and empirical illustration," *MIS Quarterly*, vol. 33, no. 1, pp. 177-195, Mar. 2009.

〈저자소개〉



김택영 (Taek-Young Kim) 학생회원
 2015년 2월: 충북대학교 경영정보학과 학사
 2017년 2월: 충북대학교 정보보호경영학과 석사
 2017년 3월~현재: 충북대학교 경영정보학과 박사과정
 <관심분야> 정보보호 교육 및 인력, 정보보호정책, 개인정보보호



전효정 (Hyo-Jung Jun) 정회원
 2001년 2월: 충북대학교 경영정보학과 학사
 2003년 8월: 충북대학교 경영정보학과 석사
 2003년 9월~2007년 5월: 한국전자통신연구원 사업기획팀 기술원
 2014년 2월: 충북대학교 경영정보학과 박사
 2014년 3월~2017년 2월: 충북대학교 정보보호경영학과 Post-Doc
 2018년 1월~현재: 충북대학교 글로벌 보안컨설팅 전문인력 양성사업단 Post-Doc
 <관심분야> 정보보호정책, 정보보호인력, 정보자원관리, 보안경제성



김태성 (Tae-Sung Kim) 종신회원
 1997년 2월: KAIST 산업경영학과 박사
 1997년 2월~2000년 8월: 한국전자통신연구원 정보통신기술경영연구소 선임연구원
 2005년 1월~2006년 2월: Univ. of North Carolina at Charlotte 방문교수
 2010년 7월~2012년 7월: Arizona State University 방문연구원
 2000년 9월~현재: 충북대학교 경영정보학과 교수, 보안경제연구소장, 보안컨설팅연계전공 주임교수, 일반대학원 정보보호경영전공 주임교수, 국가정보원 보안관리실태평가 자문 및 평가위원, 행정안전부 전자정부 민관협력포럼 자문위원, 국방부 사이버보안 자문위원, KISA ISMS/PIMS 인증위원회 위원, 한국전력 정보보안 자문위원
 <관심분야> 정보통신과 정보보호 분야의 경영 및 정책의사결정

