

기업의 개인정보 보호에 대한 사용자 인식 연구: 다차원 접근법(Analytic Hierarch Process)을 활용한 정보보안 속성 평가 및 업종별 비교

User Perception of Personal Information Security: An Analytic Hierarch Process (AHP) Approach and Cross-Industry Analysis

박 종 화 (Jonghwa Park) 경북대학교 경영학부 조교수
한 승 민 (Seoungmin Han) 고려대학교 미디어학부 박사과정
정 윤 혁 (Yoonhyuk Jung) 고려대학교 미디어학부 교수, 교신저자

요 약

최근 지능정보기술의 활용이 확산되면서 개인정보 침해에 대한 위험이 더욱 증가하고 있다. 특히, 기업이 디지털 환경에서 개인정보의 수집과 활용에 중점을 두면서, 기업의 고객정보 보호에 대한 사회적 관심이 증가하고 있다. 비록 인터넷 사용자들의 개인정보 보호에 대한 인식은 광범위하게 연구되어 왔으나, 특정 업종의 문맥, 더 나아가 업종별 개인정보 보호에 대한 비교 연구는 아직 부족한 실정이다. 본 연구는 기업의 개인정보 보안 특성에 대한 사용자 인식을 바탕으로, 업종별 개인정보 보호 수준을 비교 분석하고자 한다. 이를 위해 인터넷 사용자 498명을 대상으로 국내 포털사이트, 해외 포털사이트, 소셜미디어, 온라인 쇼핑몰, 은행, 정부기관, 온라인 사행성 게임 등 다양한 업종에 대한 개인정보 보안 특성에 대한 분석을 실시하였다. 설문을 통해 수집된 데이터를 분석적 계층 과정(Analytic Hierarch Process, AHP)을 이용하여 각 보안 특성의 상대적 중요도를 도출하였다. 연구 결과, 사용자들은 기업의 개인정보 보호를 평가할 때 기술적 보안과 투명성을 가장 중요한 요소로 간주하였다. 기술적 보안면에서는 은행과 국내 포털사이트가, 투명성 면에서는 은행과 정부기관이 우수한 성과를 보였다. 반면, 소셜미디어는 기술적 보안과 투명성 모두에서 가장 부진한 성과를 보였다. 본 연구는 개인정보 보안에 대한 다차원적 접근법을 제시하고, 사용자 관점에서 각 보안 특성에 대한 업종별 차이를 조명함으로써 연구적 의의를 가진다.

키워드 : 개인정보, 기술적 보안, 투명성, 기업 보안, 업종별, 분석적 계층 과정(Analytic Hierarch Process)

† 본 연구는 한국연구재단의 지원을 받아 수행되었음(2020S1A5A2A01046509).

I. 서론

지능정보기술의 발달에 힘입어 사용자는 보다 다양하고 풍족한 인터넷 서비스를 향유할 수 있게 되었지만, 다른 한편으로 정보 주체인 사용자의 동의없이 개인정보가 언제 어디서든 수집될 수 있는 정보보호에 취약한 환경에 놓이게 되었다. 또한, 기업들은 개인화된 인터넷 서비스를 제공하기 위해 사용자들의 개인정보를 광범위하게 수집하고 있어 사용자들의 개인정보 침해 위협에 대한 불안이 증가하고 있다(김상현, 박현선, 2013). 실제로 인터넷 서비스 기업에 의한 사용자들의 개인정보 유출 사례가 급증하고 있으며, 이에 대한 심각성이 부각되고 있다(이택현, 2019; 정혜림, 2019). 개인정보 보안 문제가 더욱 심각해질 경우 사용자들은 지능정보기술 기반의 혁신적인 서비스에 대해 기피할 가능성이 높아지게 된다(정원진, 정석균, 2012). 결국 지능정보기술 발달의 부작용인 개인정보 보호의 취약성 심화는 사용자의 개인정보 보안의 중요성을 환기시키면서 주요한 사회문제로 간주되고 있다(차인환, 김정덕, 2009).

지능정보사회에서 개인정보 보호가 화두로 등장함에 따라 기업들의 사용자 정보보안이 주목받고 있다. 사용자의 인터넷 서비스 이용 행태는 기업의 사용자 정보보안에 대한 인식에 영향을 받을 수 있다. 예컨대 인지된 기술 보안(perceived technology security)은 인터넷 서비스 이용의도에 유의미한 영향을 미쳤고(Oliveira et al., 2016), 김종기, 이동호(2005)는 전자상거래에 대한 정보 보안의 위협이 서비스 신뢰와 이용 의도에 영향을 미침을 보였다. 게다가 인터넷 서비스는 낮은 전환 비용을 갖기 때문에 사용자 정보보안에 불안을 느끼는 사용자는 서비스 변경을 고민하고, 더 좋은 보안을 제공하는 서비스로 전환하거나 서비스 이용을 중단할 수 있다(Bright et al., 2022; Jiang et al., 2016). 또한 사용자의 디지털 기술 이용 역량과 활용 수준에 따라 개인정보위험에 대한 인식은 증가하였는데(김시정, 최상욱, 2019), 이러한 양상은

사용자의 디지털 기술 이용 역량이 지속해서 상승하는 상황에서 개인정보위험에 대한 인식 또한 증가할 수 있음을 시사한다. 사용자의 개인정보 보안 행동은 정보 관리의 투명성, 제공한 개인정보의 관리 용이성 및 제공한 개인정보 대비 얻을 수 있는 이익에 영향을 받는다(Son and Kim, 2008). 요컨대 정보 보안에 대한 기존 문헌은 정보 보안에 대한 개인의 평가가 다차원으로 구성되어 있다는 것을 시사한다. 이러한 각각의 보안 속성은 상대적 중요도에 차이가 있을 수 있고(Zhang et al., 2017), 나아가 각 보안 속성에 따른 사용자들의 인터넷 서비스 기업에 대한 평가 역시 업종별로 다를 수 있다(Chang and Ho, 2006). 예를 들어 보안 속성 중 기술적 보안성이 상대적 이익성에 비해 중요할 수 있다(Morosan, 2018). 보다 구체적으로, 사용자들은 기술적 보안성 측면에서 은행업이 온라인쇼핑몰보다 상대적으로 안전하다고 느낄 수도 있다(Kankanhalli et al., 2003). 하지만 정보 보안에 대해 진행된 연구에서 인터넷 기업의 보안 속성에 대한 사용자의 인식은 주로 인지된 정보 보안 혹은 인지된 프라이버시 등의 형태로 연구되고 있다(Alkhowaiter, 2020; Gautam and Malik, 2022; Kajol et al., 2022; Merhi et al., 2019). 혹은 사용자의 개인 정보에 대한 인식을 다차원적으로 살펴본 연구에서는 금융, 소셜 미디어 등 단일 업종을 분석한 연구가 이루어졌다(이석호, 장항배, 2022; Merhi et al., 2019). 이렇듯 보안 속성에 대한 인식의 차이 및 업종별 보안 평가에 있어 차이가 분명한 점에도 불구하고, 사용자의 다차원적인 보안 속성 평가와 업종별 인식 차이에 대한 연구는 미흡한 실정이다.

따라서 본 연구는 사용자의 관점에서 인터넷 서비스 기업의 다양한 보안 속성들의 우선순위를 도출하고, 나아가 각 보안 속성에 대한 기업 업종별 차이를 살펴보고자 한다. 이를 위해 쌍대비교를 통해 각 속성의 상대적 중요도를 평가하는 계층적 분석방법(analytic hierarchy process; 이하 AHP)를 활용하였다. 본 연구는 사용자들이 평가

하는 인터넷 서비스 기업의 보안 속성에 대한 상대적으로 중요도를 파악하여, 이를 토대로 인터넷 서비스 기업이 보다 집중해야 할 보안 속성에 대해 제시하고자 하였다. 나아가 사용자들의 개인정보 보안에서 중요하게 평가하는 속성에 대한 우선순위를 인터넷 서비스 업종별로 제시하여 인터넷 기업이 개인정보 보안을 강화하기 위한 전략을 제시하고자 한다.

II. 선행연구

2.1 개인정보 보안

온라인 환경에서 인터넷 사용자의 정보 프라이버시는 다양한 목적에 의해 수집 및 활용되고 있기 때문에 정보 프라이버시는 자신의 정보를 스스로 통제할 수 있는 정보의 통제권을 강조해왔다. 하지만 정보기술이 발전함에 따라 다량의 정보를 저장 및 공유할 수 있는 환경이 조성되면서, 정보 프라이버시의 정의는 기존의 개인이 단순히 자신의 정보를 통제할 수 있는 권리 뿐 아니라 자신의 개인정보를 편리함과 같은 이익을 얻기 위한 교환 수단으로 간주하고 적극적으로 활용할 수 있는 권리까지 포함하는 넓은 범위로 확장되었다. 요즘대 사용자는 자신의 개인정보를 상품(*commodity*)으로 간주하고 개인정보를 제공하는 대가로 어떤 이익을 얻을 수 있는지 고려한다(*Smith et al., 2011*). 하지만 최근 지능정보기술의 비약적인 발전은 인터넷 기업이 사용자의 동의 없이 개인정보를 언제 어디서든 수집할 수 있는 환경을 가능케 함으로써 서비스 사용자의 정보 프라이버시를 저해하고 있다. 또한, 인터넷 서비스 기업 역시 사용자의 개인정보 보호보다 개인정보를 수집하는 역량에만 초점을 맞추고 있어, 사용자의 개인정보 침해 위험이 증가하고 있다(*김상현, 박현선, 2013*). 이에 사용자의 개인정보 보안에 대한 중요성이 점점 증가하고 있으며, 사용자의 개인정보 보안은 정보시스템분야에서 주요 연구주제가 되어왔다(*Park et al.,*

2012).

전통적으로 개인정보 보안은 인터넷 기업이 얼마나 안전하게 수집된 사용자의 개인정보를 보호하는지에 대한 정도라고 정의된다(*Parasuraman et al., 2005*). 그러나 정보기술이 발달하여 개인정보 활용의 중요성이 부각되면서, 개인정보보호의 의미는 단순히 수집된 정보를 안전하게 보호하는 것을 넘어 수집된 개인정보를 어떻게 안전하게 활용하고 공개할지까지 포함하게 되었다(*Minkkinen, 2019*). 이에 따라 본 연구에서는 개인정보 보안을 기업이 얼마나 안전하고 투명하게 사용자의 수집된 개인정보를 관리하고 활용하는지에 대한 정도로 정의한다.

정보시스템 분야에서는 다양한 맥락에서 인터넷 사용자의 개인정보 보안과 관련된 연구를 다양하게 수행해왔다. 박경아 등(2012)의 연구는 인터넷 맥락에서 사용자의 역량과 주관적 규범이 사용자의 보안태도 및 보호행동 간의 관계에 대해 검증했다. 스마트폰 맥락에서도 개인정보 보안에 대한 연구가 진행되었는데, 김종기 등(2016)의 연구는 스마트폰 사용자의 인지된 보안취약성, 자기효능감 및 반응효능감이 사용자의 보안태도 및 보호행동에 영향을 미치는 것을 증명했다. 또한 유은술, 김병조(2018)의 연구는 온라인플랫폼의 소셜 로그인서비스 맥락에서 사용자의 편의와 개인정보 보안 사이의 관계에 대해 분석하였는데, 해킹에 대한 기대손실이 낮을 경우 서비스 사용자의 수가 증가함을 밝혀냈다. 최근 정승민(2019)의 연구는 모바일 지문암호 결제 맥락에서 보안문제 발생 가능성, 문자암호 보안 취약성, 인지된 보안성이 사용자의 보안태도 및 보호행동에 영향을 미치는 것을 밝혀냈다. 이러한 기존 연구들은 다양한 인터넷 서비스에 대한 사용자의 개인정보 보안 인식과 사용자의 보안태도 및 보호행동의 관계를 탐색했다는 점에서 의의가 있지만, 사용자가 인터넷 서비스 기업의 개인정보 보안에 대해 평가할 때 실질적으로 중요하게 여기는 보안 속성들에 대한 실증적인 연구는 거의 이루어지지 않았다. 나아

가, 그러한 보안 속성들이 서비스 업종별로 차이가 있는지에 대한 연구 역시 검증되지 않고 있다. 따라서 본 연구에서는 사용자가 평가하는 인터넷 서비스 기업에 대한 개인정보 보안 속성에 대한 상대적 중요도를 도출하고 각 보안 속성에 대한 인터넷 서비스 업종별 차이점을 제시하고자 한다.

2.2 개인정보 보안 속성

개인정보 보안 속성은 다양한 맥락에서 탐색되어 왔다. 기업의 개인정보 보호와 관련하여 전영은, 김정연(2014)는 금융회사의 정보보안을 평가에 있어 주요한 요인(예, 지문인증보급화, 즉각적인 정보폐기)임을 탐색하였고, 최원녕 등(2018)는 기업의 정보보호를 위한 활동을 정보보호투자활성화 실적, 정보보호 인식 향상교육, 정보보호인력 사기진작 활동 및 대국민 인지도 제고활동을 통해 평가하였다. 하지만, 기존 연구들은 정책적 혹은 전문가적 관점에서 기업의 개인정보 관리를 평가하는 데에는 기여하고 있으나, 서비스 사용자 관점에서 기업의 개인정보 보안에 대한 구체적인 평가기준을 제시하고 있지 못하다. 개인정보 보호에 대한 사용자의 관심이 증폭하고 있으며 서비스 제공자의 사용자 정보보호에 대한 인식이 서비스 제공자를 선택하는데 영향을 줄 수 있다는 점에서, 사용자들이 실제로 어떤 개인정보 보안 속성을 중요하게 인식하는지에 대한 연구가 필요하다.

관련 연구에 기반하여 본 연구에서는 개인정보 보안 속성으로 기술적 보안성, 투명성, 관리 용이성, 상대적 이익성을 제시한다. 각 개인정보 보안 속성에 대한 개념을 살펴보면, 기술적 보안성은 기존 정보시스템분야에서 가장 많이 이용하고 있는 보안 속성으로서 인지된 보안성은 주로 기술적 보안을 의미한다(Ogbanufe and Kim, 2018). 따라서 본 연구는 기술적 보안성을 인터넷 서비스 사용자의 주요 보안 속성으로 선정하고, 인터넷 서비스 기업이 수집된 개인정보가 해킹 등 외부에 의해 불법적으로 접근되거나 이용되는 것을 방어할 수

있는 기업의 역량을 기술적 보안성이라 조작적으로 정의한다.

한편 인터넷 서비스 사용자의 정보보호 행동에 영향을 미치는 속성으로 상호작용 공정성(interactive justice), 절차 공정성(procedural justice) 및 분배 공정성(distributive justice)이 제시되었는데(Son and Kim, 2008), 상호작용 공정성은 인터넷 서비스 기업이 사용자의 개인정보를 얼마나 투명하게 관리하고 있는지를 의미하며 절차 공정성은 기업에 제공한 자신의 개인정보를 얼마나 관리하기 용이한지를 의미하고 분배공정성은 자신이 제공한 개인정보 대비 얼마나 이익을 얻을 수 있는지를 의미한다. 사용자들은 앞서 언급한 세 가지 공정성이 낮다고 인지하면 적극적으로 정보보호 활동을 하려고 하기 때문에(Son and Kim, 2008), 세 가지 공정성은 인터넷 서비스 사용자가 생각하는 주요 보안 속성이라 볼 수 있다. 본 연구에서는 앞서 언급한 세 가지 공정성을 바탕으로 나머지 세 가지 보안 속성(투명성, 관리 용이성 및 상대적 이익성)을 선정하였다. 구체적으로 투명성은 상호작용 공정성(interactive justice)과 관련된 속성으로 인터넷 서비스 기업이 수집한 정보를 얼마나 정직하고 투명하게 관리하고 있는지를 의미한다. 관리 용이성은 절차 공정성(procedural justice)에 기초한 속성으로 사용자가 인터넷 서비스 기업에 제공한 개인정보를 얼마나 용이하게 통제할 수 있는지를 뜻한다. 마지막으로 상대적 이익성은 분배 공정성(distributive justice)에 근거한 속성으로 인터넷 서비스 기업에 제공한 개인정보의 종류 혹은 양과 비교하여 기업이 사용자에게 제공하는 이익 및 효용을 의미한다.

III. 연구방법

본 연구에서는 AHP를 활용하여 인터넷 서비스에 대해 사용자가 인식하는 개인정보 보안 속성의 중요도와 우선순위를 도출하고자 했다. AHP 분석 방법은 가장 높은 계층에 있는 목표를 달성하기

위해 각 계층 내의 속성들을 쌍대비교(pairwise comparison)하여 계층별로 각 속성의 상대적 중요도 및 우선순위를 산출하는 방법이다(Satty, 1982).

3.1 측정모형 설계

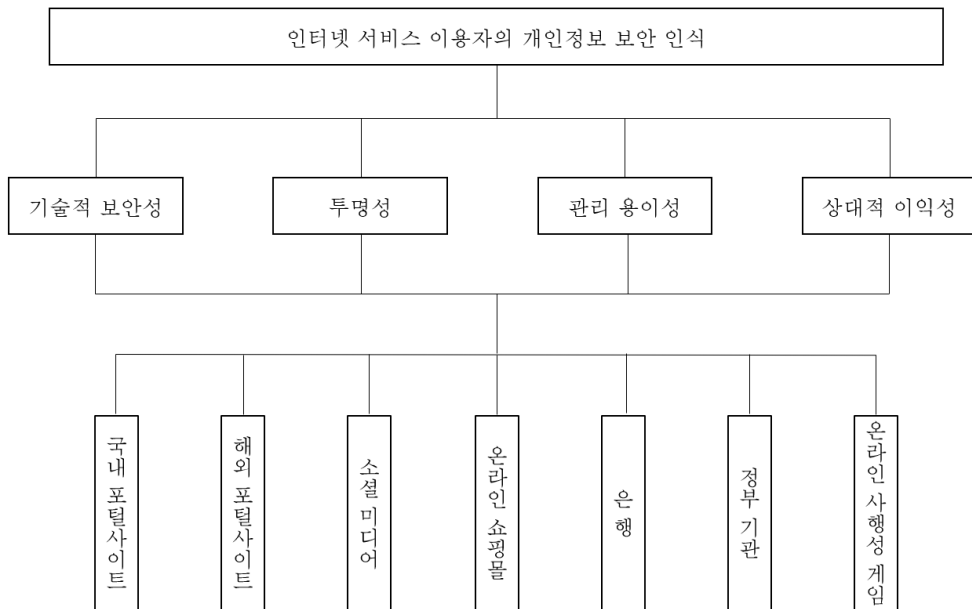
<그림 1>에서와 같이 본 연구에서는 사용자의 개인정보 보안 속성에 대한 중요도 및 우선순위를 도출하기 위해 기존 문헌을 바탕으로 주요 보안 속성 네 가지(기술적 보안성, 투명성, 관리 용이성, 상대적 이익성)를 선정하였다. 또한 각각의 개인정보 보안 속성에 대한 서비스 업종별 인식을 평가하기 위해 사용자의 개인정보를 취급하는 7개의 업종을 선택하였다. 동일 업종이더라도 사업자간 차이가 크다는 점에서 응답자에게 각 업종을 대표하는 기업의 명을 제시하여 평가하도록 하였다. 서비스 업종은 국내외 포털사이트, 소셜미디어, 온라인쇼핑몰, 은행, 정부기관 및 온라인 사행성 게임을 선택하였고, 각각의 대표적인 기업명은 <표 1>과 같다.

<표 1> 인터넷 서비스 업종 및 기업명

업종	설문에 포함된 기업명
국내 포털사이트	네이버
해외 포털사이트	구글
소셜미디어	페이스북
온라인쇼핑몰	쿠팡
은행	국민은행
정부기관	국세청
온라인 사행성 게임	스포츠토토

3.2 자료 수집 및 대상

본 연구는 인터넷 서비스 사용자의 개인정보 보안에 대한 네 가지 속성의 상대적 중요도 및 인터넷 서비스 업종별 보안 속성 평가를 위해 현재 인터넷 서비스를 이용하고 있는 사용자를 표본으로 추출하였다. 본 연구를 위한 자료 수집은 온라인 조사 전문기관인 마크로밀엠브레인의 온라인 패널을 대상으로 실시되었다. 본 연구는 20대 이상 59세 이하 성인남녀를 대상으로 성별 및 연령



<그림 1> 인터넷 서비스에 대한 사용자의 개인정보 보안 인식 계층도

<표 2> 설문조사 참여자의 인구통계학적 특성

분류		빈도	%
성별	남성	247	49.6
	여성	251	51.4
연령	20대	122	24.5
	30대	123	24.7
	40대	127	25.5
	50대 이상	126	25.3
학력	고졸 이하	65	13.1
	대학 재학	42	8.4
	대학 졸업	332	66.7
	대학원 졸업	59	11.8
월소득	100만원 미만	58	11.6
	100~200만원	64	12.9
	200~300만원	114	22.9
	300~400만원	107	21.5
	400~500만원	70	14.1
	500만원 이상	85	17.1
하루 평균 로그인 횟수	1~2회	70	14.1
	3~4회	126	25.3
	5~6회	135	27.1
	7회 이상	167	33.5

별 할당표본추출(quota sampling)을 사용하여 총 498명을 설문조사 하였다. 설문참여자의 인구통계학적 특성은 <표 2>와 같다. 한편 본 연구를 위한 설문지는 <부록>의 예시와 같이 각 속성별 상대적 중요도에 대한 쌍대비교로 구성하였으며, 각각의 쌍대비교는 1부터 9까지 리커트 척도로 측정되었다.

IV. 연구결과

4.1 AHP 일관성 검증결과

본 연구는 회수한 응답을 일관성 비율(consistency ratio)에 근거하여 응답의 일관성을 확인하였고, 다수 응답을 가중치로 종합하기 위해 기하평균을 사용하여 각각 속성별 상대적 가중치를 산출하였다(Aczel and Satty, 1983). 각 계층에 대한 항목별 가중치에 대한 일관성 비율은 <표 3>과 같다. 본

연구의 각 요인에 대한 일관성 비율은 모두 0.1 미만으로 회수한 응답이 상대적 가중치를 분석하기에 충분히 일관성이 있다고 판단된다(Saaty, 1986).

<표 3> 일관성 비율

구분		일관성 비율
상위 요인	프라이버시 보호 평가	0.01
	기술적 보안성	0.04
하위 요인	투명성	0.04
	관리 용이성	0.02
	상대적 이익성	0.01

4.2 AHP 가중치 분석 결과

본 장에서는 앞서 제안된 AHP 계층에 속한 보안 속성들 및 인터넷 서비스 업종들을 쌍대비교하여 각 보안 속성별 상대적 중요도(가중치)를 계산하고, 순위를 평가하였다. 분석은 크게 두 부분

으로 나누어서 수행되었다. 첫 번째는 인터넷 서비스 사용자의 개인정보 보안에 대한 속성별 중요도를 비교 분석하였고, 두 번째는 기술적 보안성, 투명성, 관리 용이성 및 상대적 이익성에 대한 사용자의 인터넷 기업 업종별 인식 차이를 비교 분석하였다.

우선 인터넷 서비스 사용자의 개인정보 보안에 대한 속성들의 상대적 중요도 및 우선순위에 대한 결과는 <표 4>와 같다. 인터넷 서비스 사용자가 생각하는 가장 중요한 보안 속성은 기술적 보안성(39%)이 가장 높고, 그 다음으로 투명성(28%), 상대적 이익성(19%), 관리 용이성(14%)순으로 나타났다. 이는 인터넷 서비스 사용자들은 인터넷 기업이 제공하는 기술적 보안이 가장 중요한 보안 속성으로 인식하고 있으며, 사용자가 제공한 개인정보를 손쉽게 통제할 수 있는 관리 용이성은 상대적으로 중요치 않게 인식하고 있음을 나타낸다.

<표 4> 인터넷 서비스 사용자의 개인정보보호에 대한 속성의 상대적 중요도

평가 지표	상대적 중요도	순위
기술적 보안성	0.39	1
투명성	0.28	2
관리 용이성	0.14	4
상대적 이익성	0.19	3

다음으로 각 보안 속성에 대한 인터넷 업종별

인식 차이를 분석하였다. 우선 기술적 보안성에 대한 사용자의 인터넷 업종별 인식의 차이는 <표 5>와 같다. 인터넷 서비스 사용자들은 은행(25%)이 가장 높은 기술적 보안성을 제공한다고 평가했으며, 그 다음으로 국내 포털사이트(16%), 온라인쇼핑몰(15%), 해외 포털사이트(14%), 온라인 사행성 게임(13%), 정부기관(10%), 소셜미디어(7%) 순으로 평가했다. 이는 인터넷 서비스 사용자들은 은행이 다른 인터넷 업종에 비해 상대적으로 높은 기술적 보안성을 제공한다고 평가하고 있으며, 정부기관 및 소셜미디어에 대해서는 상대적으로 낮은 기술적 보안 신뢰도를 갖고 있음을 의미한다.

투명성의 경우, 은행(22%)이 가장 높은 투명성을 갖고 있다고 평가했으며, 그 다음으로 정부기관(16%), 국내 포털사이트(15%), 온라인쇼핑몰(13%), 온라인 사행성 게임(12%), 해외 포털사이트(12%), 소셜미디어(10%) 순으로 나타났다. 인터넷 서비스 사용자들은 민감한 정보를 다루는 은행 및 정부기관이 가장 높은 투명성을 갖고 있다고 인식하며, 해외 플랫폼사업자(해외 포털사이트, 소셜미디어)의 경우 낮은 투명성을 보인다고 평가했다.

국내 포털사이트(20%)가 가장 높은 관리 용이성을 갖고 있다고 평가했으며, 그 다음으로 해외 포털사이트(17%), 소셜미디어(15%), 온라인쇼핑몰(14%), 은행(13%), 온라인 사행성 게임(11%), 정

<표 5> 업종별 인터넷 서비스 사용자의 개인정보보호 평가

업종	기술적 보안성		투명성		관리 용이성		상대적 이익성	
	상대적 중요도	순위	상대적 중요도	순위	상대적 중요도	순위	상대적 중요도	순위
국내 포털사이트	0.16	2	0.15	3	0.20	1	0.18	1
해외 포털사이트	0.14	4	0.12	5	0.17	2	0.17	2
소셜미디어	0.07	7	0.10	7	0.15	3	0.11	6
온라인쇼핑몰	0.15	3	0.13	4	0.14	4	0.15	4
은행	0.25	1	0.22	1	0.13	5	0.16	3
정부기관	0.10	6	0.16	2	0.10	7	0.10	7
온라인 사행성 게임	0.13	5	0.12	6	0.11	6	0.13	5

부기관(10%) 순으로 나타났다. 인터넷 서비스 사용자는 국내외 포털사이트에서 개인정보를 손쉽게 통제할 수 있다고 생각하고 있으며, 정부기관에서 상대적으로 개인정보를 관리하기 어렵다고 평가한다.

마지막으로 상대적 이익성에 대한 인터넷 서비스 사용자의 인터넷 업종별 인식의 경우, 국내 포털사이트(18%)가 가장 높은 상대적 이익성을 제공한다고 평가했으며, 그 다음으로 해외 포털사이트(17%), 은행(16%), 온라인쇼핑몰(15%), 온라인 사행성 게임(13%), 소셜미디어(11%), 정부기관(10%) 순서로 평가했다. 인터넷 서비스 사용자는 국내 포털사이트가 제공한 개인정보 대비 가장 큰 이익을 준다고 평가하고 있으며, 상대적으로 정부기관에서 개인정보 제공 대비 낮은 이익을 돌려받는다고 평가한다.

V. 결론 및 시사점

본 연구는 인터넷 서비스 사용자의 개인정보 보안에 대해 상대적으로 중요하게 인지하고 있는 속성들을 파악하고, 각 보안 속성에 대한 인터넷 서비스 업종별 인식의 차이를 비교 분석하고자 하였다. 이러한 연구 목적을 달성하기 위해 본 연구는 기존 연구를 바탕으로 개인정보 보안에 대한 주요 속성들을 구조화하고 개인정보 보안 속성들의 상대적 중요도를 계량화하여 각 보안 속성별 우선순위를 도출하였다. 이를 통해 개인정보 보안 속성들 중에서 인터넷 서비스 사용자가 가장 중요하게 평가하고 우선적으로 고려하는 보안 속성이 무엇인지 입증하였다. 또한 본 연구는 각 보안 속성에 따른 인터넷 서비스 업종별 사용자의 인식의 차이를 규명함으로써 인터넷 서비스 사용자가 실질적으로 인지하고 있는 인터넷 서비스 업종에 대한 보안 평가 또한 밝혀냈다.

보다 구체적으로 각각의 결과를 살펴보면, 인터넷 서비스에서 개인정보 보안에 관련해 중요하게 고려되는 네 가지의 속성을 제시하고, 이를 바

탕으로 사용자가 가장 중요하게 인지하는 개인정보 보안 속성에 대한 상대적 중요도를 밝혀냈다. 본 연구 결과는 인터넷 서비스 맥락에서 가장 중요한 보안 속성은 기술적 보안성이라는 것을 확인했는데, 이는 기술적 보안성이 중요하다는 기존의 문헌을 뒷받침한다(Ogbanufe and Kim, 2018). 또한 은행이 기술적 보안성에 대해 가장 높은 수치를 보였는데 이는 사용자의 개인정보 보안과 위협 지각이 인터넷뱅킹 사용 의도에 미치는 영향을 제시한 이용규(2007)의 연구와 일치한다. 투명성은 두 번째로 중요한 개인정보 보안 속성으로 나타났는데, 이는 앞서 언급한 공정성 중 상호작용 공정성이 제일 큰 영향력을 갖는다는 기존의 연구와 맥락을 같이한다(Son and Kim, 2008). 한편, 인터넷 서비스 사용자들은 관리 용이성을 보안 속성들 중 가장 낮게 평가했는데, 이는 인터넷 서비스 업종이 이미 편리한 관리 용이성을 제공하고 있기 때문에 상대적으로 중요도가 낮게 평가된다고 해석될 수 있을 것이다(Scott *et al.*, 2016).

각 보안 속성들에 대한 인터넷 서비스 사용자들의 업종별 인식 차이를 살펴보면, 기술적 보안성 측면에서 사용자들은 인터넷 서비스 업종 중 은행이 가장 기술적으로 안전하다고 평가하고 있고, 다음으로 국내 포털사이트가 안전하다고 판단한다. 이는 인터넷 서비스 사용자들이 이체 및 결제 등 다양한 금전거래를 영위하는 인터넷 서비스 기업일수록 더 높은 기술적인 보안성을 제공할 것이라는 믿음으로 해석될 수 있다. 왜냐하면 온라인 재무정보는 가장 중요한 온라인 정보로서(Bruwer and Wood, 2005; Masoud, 2013), 사용자들이 가장 안전하게 보안이 이루어져야 한다고 생각하는 정보이기 때문이다. 한편 소셜미디어 업종의 경우 가장 낮은 기술적 보안성을 갖고 있다고 평가했는데, 이는 소셜미디어 상에서 사용자는 자신의 개인정보를 스스로 드러내고 있을 뿐 아니라 빈번하게 발생하는 소셜미디어 개인정보유출 사건이 역시 영향을 미치는 것으로 해석될 수 있다(권혜림, 2019; 이택현, 2019). 투명성 측면에서는 인터넷 서

비스 사용자들은 은행과 정부기관이 가장 투명하게 개인정보를 관리한다고 평가한다. 이는 민감한 개인정보를 다루는 기관에 대한 신뢰가 작용한 것으로 해석된다. 또한 인터넷 서비스 사용자들은 전반적으로 국내 사이트가 해외 사이트에 비해 투명하게 개인정보를 관리하고 있다고 평가하였다. 이는 해외 인터넷 기업이 국내 개인정보 침해 사건에 대해 정부의 관리나 규제의 영향을 받지 않기 때문에 서비스 사용자들의 개인정보를 불투명하게 관리할 것이라는 불신으로 해석될 수 있다. 이는 국내 규제가 해외 인터넷 기업에 대해 제대로 작동할 수 없음을 반영하는 인식이라고도 할 수 있다(김현아, 2018). 이는 국내 포털사이트의 경우 정보 공개 범위를 설정할 수 있고, 정보 수정이 용이하기 때문이라고 추측할 수 있다. 관리 용이성 측면에서는 인터넷 서비스 사용자는 국내외 포털사이트가 전반적으로 개인정보를 관리하기 용이하다고 평가했다. 한편 정부기관의 경우 가장 낮은 관리 용이성을 보였는데, 이는 공인인증서 등 여러 가지 제약으로 인해 상대적으로 개인정보를 관리하기 어려운 것으로 해석할 수 있다. 마지막으로 상대적 이익성 측면에서는 국내외 포털사이트가 다양한 서비스를 동시에 제공함으로써 사용자들이 제공한 개인정보 대비 상대적으로 높은 효용을 준다는 것으로 해석할 수 있었다. 반면 정부기관은 사용자들이 필요시에만 제한적으로 사용하기 때문에 다른 인터넷 업종 대비 낮은 효용을 준다고 해석할 수 있다.

본 연구는 인터넷 서비스 맥락에서 개인정보 보안 속성들을 구조화하고 계량화하여 인터넷 서비스 사용자가 실질적으로 중요하게 생각하는 개인정보 보안 속성들을 제시했다는 점에서 학문적 기여도가 있다. 특히 제시된 각각의 보안 속성은 이용 의도와 같은 다양한 결과변수들을 도출하는데 활용될 수 있을 것이다. 또한 본 연구의 결과는 인터넷 서비스 업종별 취약한 보안 속성을 보여줌으로써 기업의 고객정보 보호에 대한 전략을 수립하는데 도움이 될 수 있을 것으로 기대한다. 예를

들어 인터넷 서비스 사용자들은 기술적 보안성이 가장 중요하다고 평가하는데, 이러한 기술적 보안성은 서비스 이용에 대한 인지된 위험을 낮춰줄 뿐만 아니라 서비스에 대한 신뢰 및 이용의도를 높일 수 있다(Damghanian *et al.*, 2016). 따라서 기술적 보안성이 낮다고 평가된 인터넷 서비스 업종은 지속적으로 기술적 보안에 투자하고 이를 사용자들에게 고지함으로써 서비스에 대한 사용자들의 기술적 보안 인식을 높일 필요가 있다. 또한 본 연구 결과에 따르면 투명성은 두 번째로 중요한 개인정보 보안 속성으로 나타났다. 이는 인터넷 서비스 기업이 사용자들의 개인정보를 보다 투명하고 정직하게 관리해야 한다는 것을 의미한다. 투명성 역시 개인정보보호에 대한 신뢰와 밀접한 관련이 있고(Son and Kim, 2008), 이러한 인터넷 서비스 기업에 대한 신뢰는 사용자의 인터넷 서비스 사용의도를 높일 수 있다(Dimitriadis and Kyrezi, 2010). 따라서 인터넷 서비스 기업은 사용자의 개인정보를 지속적으로 투명하게 관리하는 것이 기존 사용자의 이탈을 방지할 수 있을 뿐만 아니라 새로운 사용자의 확보하는데도 도움이 될 것이라 기대된다. 나아가, 업종별로 정보보안에 취약하다고 인식되고 있는 부분을 강화하고 이를 홍보함으로써 해당 기업의 개인정보 보안에 대한 소비자 인식을 제고할 수 있을 것이다.

본 연구에서 가장 큰 한계점은 보안 속성별 우선순위 차이를 설명하기 위한 뒷받침할 설명이나 심층자료가 부족하다는 점이다. 따라서 향후 연구에서는 인터뷰 방법을 함께 사용하여 보안 속성별 우선순위 차이에 대한 이유를 좀 더 심층적으로 설명할 수 있는 연구가 필요하다. 또한 본 연구에서 선정한 업종은 제한적일 수 있으며, 각 업종에 대해 대표 기업을 하나만 선정하였기 때문에 대표성에 문제가 있을 수 있다. 따라서 향후 연구에서는 다양한 인터넷 업종 및 기업을 포함하여 좀 더 포괄적으로 각 보안 속성들을 검증할 필요가 있다. 마지막으로 연구 방법적인 측면으로 AHP 분석 이외에 분석 네트워크 프로세스(analytic net-

work process)와 같은 다른 분석 방법을 활용하여 사용자들의 개인정보 보안 속성 중요도를 평가하여 본 연구 결과와 차이가 있는지 살펴보는 후속 연구가 이어질 필요가 있다.

참고문헌

- [1] 김종기, 이동호, “전자상거래 사용자의 신뢰에 영향을 미치는 정보보안위험 기반의 선행요인 연구”, *경영정보학연구*, 제15권, 제2호, 2005, pp. 65-96.
- [2] 김시정, 최상욱, “디지털 이용 역량과 활용이 개인정보위험 인식에 미치는 영향 연구”, *한국사회와 행정연구*, 제30권, 제2호, 2019, pp. 257-284.
- [3] 김상현, 박현선, “프라이버시 보호인식 및 보호행동의도에 미치는 영향 요인과 프라이버시 침해경험의 조절효과에 관한 연구”, *인터넷전자상거래연구*, 제13권, 제4호, 2013, pp. 79-105.
- [4] 김종기, 김지윤, 리첸첸, “스마트폰 사용자의 보안행위의도에 영향을 미치는 요인에 관한 연구”, *인터넷전자상거래연구*, 제16권, 제6호, 2016, pp. 115-136.
- [5] 김현아, “국내외 인터넷기업 역차별 해소 노력..내년에도 계속된다, 이데일리, 2018, Available at <https://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=105&oid=018&aid=0004280174>.
- [6] 박경아, 이대용, 구철모, “최종사용자의 인터넷과 소셜 네트워크 보안 행동에 대한 실증 연구”, *정보시스템연구*, 제21권, 제4호, 2012, pp. 1-1.
- [7] 유은솔, 김병조, “플랫폼의 소셜로그인 서비스 (Authing Service): 보안과 편의 사이의 적절성”, *Information Systems Review*, 제20권, 제1호, 2018, pp. 137-158.
- [8] 이석호, 장항배, “정보보호 관점의 금융 마이데이터 서비스 수용 요인에 관한 연구”, *한국전자거래학회지*, 제27권, 제2호, 2022, pp. 137-152.
- [9] 이용규, “보안과 위협의 지각이 인터넷 बैं킹 재사용 의도에 미치는 영향”, *경영정보학연구*, 제17권, 제1호, 2007, pp. 77-93.
- [10] 이택현, ““폐북이 개인정보 통제력을 잃었다” 사용자 정보 5억건 아마존 유출, 국민일보, 2019, Available at <http://news.kmib.co.kr/article/view.asp?arcid=0924071352&code=11141100&cp=nvhttp://news.kmib.co.kr/article/view.asp?arcid=0924071352&code=11141100&cp=nv>.
- [11] 전영은, 김정연, “금융회사의 사이버 보안 위협에 따른 개인정보보호 실태에 관한 연구”, *한국IT서비스학회지*, 제13권, 2014, pp. 79-89.
- [12] 정석균, 정원진, “스마트폰 사용자가 지각한 모바일 쇼핑몰의 정보보안 수준이 쇼핑몰 이용의도에 미치는 영향”, *기업경영연구*, 제19권, 제4호, 2012, pp. 261-282.
- [13] 정승민, “모바일결제 시 지문암호 사용의도에 영향을 미치는 보안관련 요인과 비 보안관련 요인에 관한 연구”, *전문경영인연구*, 제22권, 제3호, 2019, pp. 207-228.
- [14] 정혜림, “페이스북이 또...“2억 6,000만 명 개인정보 유출”, *중앙일보*, 2019, Available at <https://news.joins.com/article/23663090>.
- [15] 차인환, 김정덕, “정보보호를 위한 인적자산 관리지표 실증 연구”, *정보보호학회논문지*, 제19권, 제6호, 2009, pp. 153-160.
- [16] 최원녕, 김우제, 국광호, “기업의 정보보호활동의 효율성 평가”, *융합보안논문지*, 제18권, 제5호, 2018, pp. 25-32.
- [17] Aczél, J. and T. L. Saaty, “Procedures for synthesizing ratio judgements”, *Journal of Mathematical Psychology*, Vol.27, No.1, 1983, pp. 93-102.
- [18] Alkhowaiter, W. A., “Digital payment and banking adoption research in Gulf countries: A systematic literature review”, *International Journal of*

- Information Management*, Vol.53, 2020, p. 102102.
- [19] Bright, L. F., K. Logan, and H. S. Lim, "Social media fatigue and privacy: An exploration of antecedents to consumers' concerns regarding the security of their personal information on social media platforms", *Journal of Interactive Advertising*, Vol.22, No.2, 2022, pp. 125-140.
- [20] Bruwer, J. and G. Wood, "The Australian online wine-buying consumer: Motivational and behavioural perspectives", *Journal of Wine Research*, Vol.16, No.3, 2005, pp. 193-211.
- [21] Chang, S. E. and C. B. Ho, "Organizational factors to the effectiveness of implementing information security management", *Industrial Management & Data Systems*, Vol.106, No.3, 2006, pp. 345-361.
- [22] Damghanian, H., A. Zarei, and M. A. Siah Sarani Kojuri, "Impact of perceived security on trust, perceived risk, and acceptance of online banking in Iran", *Journal of Internet Commerce*, Vol.15, No.3, 2016, pp. 214-238.
- [23] Dimitriadis, S. and N. Kyrezis, "Linking trust to use intention for technology-enabled bank channels: The role of trusting intentions", *Psychology & Marketing*, Vol.27, No.8, 2010, pp. 799-820.
- [24] Gafni, R. and D. Nissim, "To social login or not login? Exploring factors affecting the decision", *Issues in Informing Science and Information Technology*, Vol.11, No.1, 2014, pp. 057-072.
- [25] Gautam, S. and P. Malik, "Importance of perceived security, perceived privacy and website design of active online investors: an Indian market perspective", *International Journal of Electronic Finance*, Vol.11, No.1, 2022, pp. 30-48.
- [26] Jiang, L., M. Jun, and Z. Yang, "Customer-perceived value and loyalty: how do key service quality dimensions matter in the context of B2C e-commerce?", *Service Business*, Vol.10, 2016, pp. 301-317.
- [27] Kajol, K., R. Singh, and J. Paul, "Adoption of digital financial transactions: A review of literature and future research agenda", *Technological Forecasting and Social Change*, Vol.184, 2022, p. 121991.
- [28] Kankanhalli, A., H. H. Teo, B. C. Tan, and K. K. Wei, "An integrative study of information systems security effectiveness", *International Journal of Information Management*, Vol.23, Vol.2, 2003, pp. 139-154.
- [29] Masoud, E. Y., "The effect of perceived risk on online shopping in Jordan", *European Journal of Business and Management*, Vol.5, No.6, 2013, pp. 76-87.
- [30] Merhi, M., K. Hone, and A. Tarhini, "A cross-cultural study of the intention to use mobile banking between Lebanese and British consumers: Extending UTAUT2 with security, privacy and trust", *Technology in Society*, Vol.59, 2019, p. 101151.
- [31] Minkkinen, M., "Making the future by using the future: A study on influencing privacy protection rules through anticipatory storylines", *New Media & Society*, Vol.21, No.4, 2019, pp. 984-1005.
- [32] Morosan, C., "Information disclosure to biometric e-gates: The roles of perceived security, benefits, and emotions", *Journal of Travel Research*, Vol.57, No.5, 2018, pp. 644-657.
- [33] Ogbanufe, O. and D. J. Kim, "Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment", *Decision Support Systems*, Vol.106, 2018, pp. 1-14.
- [34] Oliveira, T., M. Thomas, G. Baptista, and F. Campos, "Mobile payment: Understanding the

- determinants of customer adoption and intention to recommend the technology”, *Computers in Human Behavior*, Vol.61, 2016, pp. 404-414.
- [35] Parasuraman, A., V. A. Zeithaml, and A. Malhotra, “ES-QUAL: A multiple-item scale for assessing electronic service quality”, *Journal of Service Research*, Vol.7, No.3, 2005, pp. 213-233.
- [36] Park, Y. J., S. W. Campbell, and N. Kwak, “Affect, cognition and reward: Predictors of privacy protection online”, *Computers in Human Behavior*, Vol.28, No.3, 2012, pp. 1019-1027.
- [37] Saaty, T. L., “Axiomatic foundation of the analytic hierarchy process”, *Management Science*, Vol.32, No.7, 1986, pp. 841-855.
- [38] Scott, C., D. Wynne, and C. Boonthum-Denecke, “Examining the privacy of login credentials using web-based single sign-on-are we giving up security and privacy for convenience?”, In *2016 Cybersecurity Symposium (CYBERSEC)*, IEEE, 2016, pp. 74-79.
- [39] Smith, H. J., T. Dinev, and H. Xu, “Information privacy research: an interdisciplinary review”, *MIS quarterly*, Vol.35, No.4, 2011, pp. 989-1016.
- [40] Son, J. Y. and S. S. Kim, “Internet users’ information privacy-protective responses: A taxonomy and a nomological model”, *MIS quarterly*, 2008, pp. 503-529.
- [41] Sun, S. T., E. Pospisil, I. Muslukhov, N. Dindar, K. Hawkey, and K. Beznosov, “What makes users refuse web single sign-on? An empirical investigation of OpenID”, In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, 2011, pp. 1-20.
- [42] Urueña, M., A. Muñoz, and D. Larrabeiti, “Analysis of privacy vulnerabilities in single sign-on mechanisms for multimedia websites”, *Multimedia Tools and Applications*, Vol.68, No.1, 2014, pp. 159-176.
- [43] Yang, K. C., “Exploring factors affecting the adoption of mobile commerce in Singapore”, *Telematics and informatics*, Vol.22, No.3, 2005, pp. 257-277.
- [44] Zhang, M., M. Luo, R. Nie, and Y. Zhang, “Technical attributes, health attribute, consumer attributes and their roles in adoption intention of healthcare wearable technology”, *International Journal of Medical Informatics*, Vol.108, 2017, pp. 97-109.

〈부록〉 설문지 예시

다음은 개인정보 보호 평가지표의 중요도에 대한 질문입니다.

1은 동일하게 중요함, 5는 상대적으로 더 중요함, 9는 매우 더 중요함을 의미합니다.

예를 들어 **좌측의 속성이 우측의 속성보다 상대적으로 더 중요하다고 판단되는 경우 좌측의 5에 체크**해주시면 됩니다.

각 항목의 설명은 다음과 같습니다.

기술적 보안성 - 수집된 개인정보가 해킹 등 외부에 의해 불법적으로 접근되거나 이용되는 것을 기술적으로 방어할 수 있는 기업의 역량

투명성 - 기업이 수집한 개인정보를 허가 받지 않은 대상에게 공유하지 않는 등 기업이 얼마나 수집한 개인정보를 투명하게 관리하는지를 의미

통제가능성 - 기업에 제공한 개인정보를 사용자가 용이하게 관리할 수 있는지 여부를 의미

상대적이익성 - 기업에 제공한 개인정보의 종류/양과 비교하여 기업이 사용자에게 제공하는 이익/효용을 의미

기업에 제공한 개인정보의 보안 측면에서	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	기업에 제공한 개인정보의 보안 측면에서
기술적 보안성이 더 중요하다																		투명성이 더 중요하다
기술적 보안성이 더 중요하다																		관리 용이성이 더 중요하다
기술적 보안성이 더 중요하다																		상대적 이익성이 더 중요하다
투명성이 더 중요하다																		관리 용이성이 더 중요하다
투명성이 더 중요하다																		상대적 이익성이 더 중요하다
관리 용이성이 더 중요하다																		상대적 이익성이 더 중요하다

다음은 각 평가지표의 중요도를 평가하는 설문입니다.

1은 동일한 수준, 5는 상대적으로 더 그렇다, 9는 매우 더 그렇다를 의미합니다.

예를 들어 좌측의 기업이 우측의 기업보다 상대적으로 더 안전하다고 판단되는 경우 좌측의 5에 체크해주시면 됩니다.

개인정보 보안측면에서 **기술적 보안성**이란 수집된 개인정보가 해킹 등 외부에 의해 불법적으로 접근되거나 이용되는 것을 기술적으로 방어할 수 있는 기업의 역량을 의미합니다.

개인정보 보안 기술적 보안성 측면에서

기업에 제공한 개인정보 보안 기술적인 측면에서	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	기업에 제공한 개인정보 보안 기술적인 측면에서
네이버가 더 안전하다																		구글이 더 안전하다
네이버가 더 안전하다																		페이스북이 더 안전하다
네이버가 더 안전하다																		쿠팡이 더 안전하다
네이버가 더 안전하다																		국민은행이 더 안전하다
네이버가 더 안전하다																		국세청이 더 안전하다
네이버가 더 안전하다																		스포츠토토(스포츠편팅게임)가

기업에 제공한 개인정보 보안 기술적인 측면에서	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	기업에 제공한 개인정보 보안 기술적인 측면에서
																		더 안전하다
구글이 더 안전하다																		페이스북이 더 안전하다
구글이 더 안전하다																		쿠팡이 더 안전하다
구글이 더 안전하다																		국민은행이 더 안전하다
구글이 더 안전하다																		국세청이 더 안전하다
구글이 더 안전하다																		스포츠토토(스포츠베팅게임)가 더 안전하다
페이스북이 더 안전하다																		쿠팡이 더 안전하다
페이스북이 더 안전하다																		국민은행이 더 안전하다
페이스북이 더 안전하다																		국세청이 더 안전하다
페이스북이 더 안전하다																		스포츠토토(스포츠베팅게임)가 더 안전하다
쿠팡이 더 안전하다																		국민은행이 더 안전하다
쿠팡이 더 안전하다																		국세청이 더 안전하다
쿠팡이 더 안전하다																		스포츠토토(스포츠베팅게임)가 더 안전하다
국민은행이 더 안전하다																		국세청이 더 안전하다
국민은행이 더 안전하다																		스포츠토토(스포츠베팅게임)가 더 안전하다
스포츠토토(스포츠베 팅게임)가 더 안전하다																		스포츠토토(스포츠베팅게임)가 더 안전하다

Information Systems Review

Volume 25 Number 4

November 2023

User Perception of Personal Information Security: An Analytic Hierarch Process (AHP) Approach and Cross-Industry Analysis

Jonghwa Park* · Seoungmin Han** · Yoonhyuk Jung***

Abstract

The increasing integration of intelligent information technologies within organizational systems has amplified the risk to personal information security. This escalation, in turn, has fueled growing apprehension about an organization's capabilities in safeguarding user data. While Internet users adopt a multifaceted approach in assessing a company's information security, existing research on the multiple dimensions of information security is decidedly sparse. Moreover, there is a conspicuous gap in investigations exploring whether users' evaluations of organizational information security differ across industry types. With an aim to bridge these gaps, our study strives to identify which information security attributes users perceive as most critical and to delve deeper into potential variations in these attributes across different industry sectors. To this end, we conducted a structured survey involving 498 users and utilized the analytic hierarchy process (AHP) to determine the relative significance of various information security attributes. Our results indicate that users place the greatest importance on the technological dimension of information security, followed closely by transparency. In the technological arena, banks and domestic portal providers earned high ratings, while for transparency, banks and governmental agencies stood out. Contrarily, social media providers received the lowest evaluations in both domains. By introducing a multidimensional model of information security attributes and highlighting the relative importance of each in the realm of information security research, this study provides a significant theoretical contribution. Moreover, the practical implications are noteworthy: our findings serve as a foundational resource for Internet service companies to discern the security attributes that demand their attention, thereby facilitating an enhancement of their information security measures.

Keywords: *Personal Information, Technological Security, Transparency, Corporate Security, Cross-Industry, Analytic Hierarch Process (AHP)*

* Assistant Professor, School of Business Administration, Kyungpook National University

** Ph.D. Student, School of Media & Communication, Korea University

*** Corresponding Author, Professor, School of Media & Communication, Korea University

◎ 저자 소개 ◎



박종화 (jonghwapark@knu.ac.kr)

울산과학기술원에서 경영과학(Management Engineering)으로 박사학위를 받았으며, 현재 경북대학교 경영학부 조교수로 재직하고 있다. 주요 연구분야로는 프라이버시, 인공지능, 사용자 정보 기술 수용 등이며, International Journal of Information Management, Telematics & Informatics, Computers in Human Behavior, International Journal of Human - Computer Interaction 등 다수의 학술지에 논문을 게재하였다.



한승민 (han9102@korea.ac.kr)

울산과학기술원에서 경영공학(Management Engineering)으로 석사학위를 받았고, 현재 고려대학교 미디어학부에서 박사과정을 진행 중이다. 주요한 연구 분야로는 디지털 미디어, 디지털 플랫폼, 가상 세계, 사물인터넷 등이다.



정윤혁 (beyond@korea.ac.kr)

미국 Louisiana State University에서 경영정보 및 의사결정(Information Systems & Decision Science)으로 박사학위를 받았고, 현재 고려대학교 미디어학부 교수로 재직하고 있다. 주요한 연구분야는 디지털 미디어, 디지털 플랫폼, 가상세계, 프라이버시 등이고, Information & Management, Information Systems Journal, European Journal of Information Systems, International Journal of Information Management 등 다수의 학술지에 논문을 게재하였다.

논문접수일 : 2023년 06월 23일

1차 수정일 : 2023년 08월 07일

게재확정일 : 2023년 10월 06일

2차 수정일 : 2023년 09월 15일