「정보시스템연구」 제26권 제1호
한국정보시스템학회
2017년 3월, pp. 53~73
http://dx.doi.org/10.5859/KAIS.2017.26.1.53

전자정부서비스에 대한 개인정보제공의 영향요인

박 정 애* · 손 달 호**

〈목 차〉

Ⅰ. 연구의 필요성

공공기관의 전자정부서비스에서 시민들의 개인정보는 필수적인 자료로 인식되고 있다. 그럼에도 불구하고, 최근 민간 부문에서 잇달아 터진 개인정보 유출 사건으로 인해 많은 시민들이 공공기관의 정보서비스에 조차도 개인정보를 제공하는 것을 꺼리고 있다. 이는 우선적으로 개인정보 유출에 대한 프라이버시 염려가 주된 원인이 될 수 있으며, 공공기관의 정보보안에 대한 신뢰성을 가지지 못하는 것이 중요한 원인이라 할 수 있다(김기열, 2010).

정보기술의 발전과 인터넷 이용이 일상화됨에 따라서 공공서비스나 인터넷을 통한 편의서비스를 이용하기 위해서 개인정보의 제공은 필수적인 조건으로 인식되고 있다(곡민 등, 2015). 그러나 개인의 중요한 사생활 정보가 수차례에 걸쳐 반복적으로 다양한 분야에 제공되는 상황에서 개인들은 개인정보 제공에 대한 우려가 점차적으로 높아지고 있는 실정이다(심재윤 등, 2015). 이는 지식정보 활용성제고 측면에서 개인정보의 제공과 이러한 개인정보가 유출되어 사생활의 침해라는 패러독스 상황이 작용하고 있다는 것을 보여주는 것이다(Lin et al, 2015).

지금까지, 공공부문에서 개인정보 보호는 예방적인 성격의 입법이나 정책 때문에, 민간부문과는 달리 개인정보의 유출로 인한 심각한 피해

* 대구광역시청, parkjungae@korea.kr(주저자)
** 계명대학교 경영정보학과, dhshon@kmu.ac.kr(교신저자)

가 발생하지 않았다(민현홍 등, 2016). 그럼에도 불구하고 금융사를 비롯하여 각 분야의 민간부문에서의 개인정보 유출을 경험한 국민들은 공공부문에서 조차 개인정보 제공에 대해서 거부감을 보이고 있는 실정이다. 일례로 전자주민카드, 전자건강보험증, NEIS 등 국가적인 차원에서 진행하는 정보화 사업을 둘러싸고 많은 혼란과 사회적 비용을 경험하고 있다(임병화 등, 2014). 특히, 스마트 시대와 전자정부 중심사회로 이행되면서 스마트카드, 무선인터넷, LBS, RFID 등 첨단 스마트 공공서비스가 확대 추진되는 과정에서 개인정보의 제공과 관련된 문제가 중요한 이슈로 대두되고 있다(Miltgen and Smith, 2015).

학술적인 측면에서는 지난 10여년 동안 프라이버시에 대한 연구들을 바탕으로 온/오프라인 상에서 사용자들의 프라이버시 보호를 위한 정책 및 기술적 수단들이 다양하게 제시되었다(안수미 등, 2014). 그럼에도 불구하고 프라이버시 침해에 대한 우려는 감소되지 않고, 오히려 더욱 증폭되고 있는 실정이라 할 수 있다(Cavusoglu et al, 2015). 이는 정보기술의 발전과 확산이 가속화되면서 침해위협 역시 증가한 결과로 볼 수 있으나, 기존의 프라이버시 연구가 가지고 있는 한계에서도 그 이유를 찾을 수 있다(이환수 등, 2013). 기존의 정보 프라이버시 관련 연구들은 기술적 또는 도구적 관점에서 사용자 위험과 효익에 대한 판단을 중심으로 정보 프라이버시 관련 태도, 의도 및 행위를 설명하는데 집중해 왔다. 또한 대부분의 연구들이 개인수준에서 사용자들의 프라이버시 염려 또는 정보제공 의도 등에 영향을 미치는 요인들의 인과관계 규명에 초점을 맞추고 있다(Czernek et al, 2016).

전자정부 시대의 프라이버시 문제에 관한 연구는 초기에는 주로 입법을 중심으로 하는 법제도적인 측면에서 다루어져 오다가, 최근에는 경영분야에서 민간 기업부문을 중심으로 실증연구를 통한 접근이 진행되고 있다(Miltgen and Smith, 2015). 그러나 여전히 공공부문을 대상으로 하는 개인정보에 대한 연구는 공공부문의 특수성으로 인해 주로 법학 및 행정학 분야에서 정보보호 차원의 연구가 수행되고 있으나(장혜진, 2016), 경영학 분야에서는 아직도 공공부문의 개인정보와 관련된 연구는 활용 현황 분석 및 단순 비교 수준의 기초연구 수준에 머무르고 있다(임진택 등, 2015). 따라서 공공부문의 개인정보 제공과정에 대한 심층적인 연구는 찾아보기 힘든 상황이며, 개인정보 제공과 같은 시민의 참여행동을 포함하는 연구가 매우 미흡한 실정이다(김상희 등, 2015). 특히 공공기관을 중심으로 개인정보 제공에 대한 심층적인 연구가 필요하며, 디지털 정부로의 급격한 이행 과정에서 공공기관의 프라이버시와 신뢰를 중심으로 하는 개인정보 제공 과정을 연구하는 노력이 필요하다.

이상의 논의와 같이 프라이버시 침해를 둘러싼 심각한 사회적 이슈 상황에서 공공기관의 전자정부서비스에 있어서 개인정보를 어떻게 획득할 것인가는 전자정부가 풀어야 할 중요한 과제이다. 따라서 본 연구는 경영정보학 관점에서 전자정부의 활성화 차원에 목적을 두고, 공공부문의 전자정부서비스에 있어서 개인의 프라이버시 염려와 공공기관 신뢰를 중심으로 개인정보 제공 의도에 영향을 미치는 요인들의 영향력을 실증적으로 규명하고자 한다. 특히 본 연구

에서는 법제도적 강제장치가 작용하는 공공부문에 있어서, 개인의 정보제공을 어떻게 효과적으로 획득할 수 있는지를 연구하고자 한다. 이와 함께 공공 전자정부서비스 이용자 관점에서 개인이 인식하는 프라이버시 염려가 형성되는 과정과 정보서비스 제공자 관점에서 공공기관의 신뢰 요인을 중심으로 개인정보 제공의도에 영향을 미치는 과정을 심층적으로 연구하는데 주된 목적을 두고 있다.

Ⅱ. 이론적 배경

2.1 개인정보 제공의 영향요인

개인정보 제공에 대한 개인적 관점의 영향요인은 정보보호에 대한 인식, 조직문화, 개인 혁신성, 훈련 또는 교육, 정보보호 이슈에 대한 커뮤니케이션 역량 등의 요인이 있다(김유정 등, 2015). 심리학, 의학, 그리고 정보시스템 분야에서 널리 사용되고 있는 개념인 인식은 각 개인의 자각으로 정의될 수 있다. 특히 정보보호 인식은 이슈에 대한 개인의 관심정도로 정보보호에 대한 자각 및 정보보호 활동에 대한 관심을 의미하며, 조직구성원의 정보보호에 대한 일반적 지식과 조직의 정보보호 정책에 대한 인식 정도를 나타낸다(민현홍 등, 2016). 또한 정보보호 인식은 구성원들이 자신의 직무를 수행하는데 있어 정보보호의 관리상태를 알 수 있도록 하는 프로세스로 여기에는 정보보호의 중요성, 보안사고가 발생할 때 이에 대한 대응방안과 보고체계 등이 포함된다(임진택 등, 2015).

조직문화는 조직의 구성원이 어떤 일을 함에 있어서 구성원이 공유하고 있는 신념, 가치관 또는 체계이다(장혜진 등, 2014). 전사적 차원에서 구성원의 보안인식 증진과 기업보안활동에 대한 참여도 제고를 통하여, 기업의 보안활동에 대한 구성원들의 행동을 변화시킬 수 있다(김희선, 2015). 이와 함께 구성원들에게 회사의 장기적 보안전략과 비전을 이해하도록 하는 정보보호 인식 및 문화 프로그램의 운영이 중요하다.

개인혁신성은 사회시스템에서 개인이 다른 구성원보다 기술적 혁신을 상대적으로 빨리 수용하는 정도를 의미하는 것으로, 다른 사람의 조언이나 도움 없이 새로운 제품 혹은 기술을 수용하려는 정도를 나타낸다(박성희, 2014). 즉 개인혁신성은 개인이 새로운 것을 얼마나 쉽고 빠르게 수용 또는 새로운 것을 시도하고자 하는 의지를 지칭한다(곡민 등, 2015). 정보기술 분야에서 개인혁신성은 새로운 정보기술에 대한 개인의 인식뿐만 아니라 사용의도에까지 유의한 영향을 미치는 것으로 연구되었다(Miltgen and Smith, 2015). 이러한 개인혁신성은 프라이버시 염려를 감소시키고 정보서비스의 지속적인 사용의도를 더욱 촉진시키는 역할을 한다(김상현 등, 2013).

IT관리는 비즈니스와 IT의 전략적 통합이라는 전제 아래 기업의 운영탁월성을 확보할 수 있다는 것을 의미한다(임진택 등, 2015). 정보보호 관점에서 IT관리책임의 분산은 보안통제 수단을 적용함에 있어 조직역량의 저하를 초래할 수 있다(Cavusoglu et al, 2015). 또한 IT관리책임의 분산은 다른 외부조직과의 상호작용 시에도 문제가 발생할 수 있으며, 조직 내 정보시스템의 복잡성, 보안 이슈의 소통 관점에서도

부정적 영향을 줄 수 있다.

취약점 분석/평가, 침해행위 대응활동과 같은 기술적 요인이 개인정보 제공에 중대한 영향을 미칠 수 있다(Jarvelainen, 2013). 취약점 분석/평가는 악성코드 유포, 해킹 등 사이버 위협에 대한 정보 및 정보시스템의 취약점을 종합적으로 분석, 평가, 개선하는 일련의 과정으로, 평가에 대한 준비, 수행과 더불어 결과공유 및 평가 유지활동 등이 포함된다(Wu et al, 2012). 특히 평가수행 단계는 보안위협이 되는 원천과 이벤트의 식별, 취약점과 유발요인의 식별, 보안사고 발생의 가능성, 보안사고 영향의 정도 및 위험에 대한 결정 등의 활동으로 이루어진다.

정보보호 컴플라이언스 및 환경 불확실성과 같은 사회적 요인도 개인정보 제공행위에 영향을 미칠 수 있다(임진택 등, 2015). 정보보호 컴플라이언스는 일반적으로 조직에서 공식적인 의무사항에 대한 준수 그리고 합법성을 유지하는 것을 의미한다(심재윤 등, 2015). 정보보호 관련 법규를 위반하여 발생되는 컴플라이언스 위험에 적극적으로 대처하지 못하는 경우 기업은 중대한 위기상황에 직면하게 된다. 따라서, 기업의 비즈니스 연속성을 보장하는데 정보보호 컴플라이언스는 선택이 아닌 필수사항으로 반드시 해결해야 하는 과제로 인식되고 있다(Irwin et al, 2014).

환경 불확실성은 기술의 급격한 변화, 경쟁자 행동, 고객의 보안 요구사항, 제도변경에 의해 야기된다(Lin et al, 2015). 정보기술의 발전으로 인해 정보를 이용하게 되는 다양한 유형의 사용자들이 있으며, 이에 따라 기존에 안전했던 정보에 취약점이 발생하게 되며, 이러한 위협에 대응할 수 있는 보안시스템이 필요하다(김유정 등, 2015). 특히 보안시스템 자체를 새로운 환경에 끊임없이 적응하게 해야 하며, 따라서, 외부로부터의 환경확실성은 정보보호 관리의 필요성에 영향을 미치는 중요한 요인 중 하나가 될 수 있다(민현홍 등, 2016).

2.2 개인정보 제공모형

사람들이 특정행위의 결과로 야기되는 이득과 손실을 평가하는 과정은 사회적 교환이론, 기대이론, 프라이버시 계산모형 등 여러 이론에서 설명되고 있다(김상현 등, 2013). 사회적 교환이론은 사람의 관계에서 발생하는 잠재적 보상과 손실을 식별한 후 보상이 손실을 초과하는 경우에 사회적 상호작용이 진행된다는 것을 나타낸다. Vroom(1964)으로 대표되는 기대이론은 인간은 본질적으로 긍정적인 결과를 최대화하는 반면 부정적인 결과를 최소화하는 방향으로 행동한다는 것을 기본 전제로 하고 있다.

개인정보 제공에 관한 사용자들의 의사결정을 이해하기 위한 대표적인 이론적 기반은 프라이버시 계산모형(Privacy Calculus Model)이다(민진영 등, 2013). 프라이버시 계산모형은 사회적 교환이론과 기대이론의 논리를 프라이버시 관련 행동에 접목시켜, 인간이 특정 경제적 또는 사회적 이득을 획득하기 위해서 일정 수준의 프라이버시를 희생하게 되는 것을 설명한다. 기대이론에 따르면 사람들은 일반적으로 긍정적인 결과를 최대화하고, 부정적인 결과를 최소화하는 방향으로 행동한다는 것이다(Vroom, 1964).

프라이버시 계산모형은 특정 개인이 현재의 프라이버시 관련 행위가 가져 올 미래의 잠재적

이익과 손실을 비교하여 개인정보 제공여부를 결정하는 것으로 경제적인 관점에서 프라이버시를 다루는 이론이다(Miltgen and Smith, 2015). 이러한 맥락에서 프라이버시 계산모형은 자신에 대한 정보수집과 사용을 통제하는 정보 프라이버시 개념에서 접근된다. 프라이버시 계산모형에서 잠재적 이익은 경제적 또는 사회적 보상을 의미하며, 여기에서 잠재적 손실은 프라이버시 침해가 되는 프라이버시 패러독스를 담고 있다(안수미 등, 2014).

개인정보 제공에 관한 의사결정은 비용-혜택의 상충관계를 포함하고 있으며, 정보제공은 약간의 불확실성을 내포하고 있지만, 여기에는 정보제공자의 기회주의적 행동이 포함된다(김상희, 2015). 개인정보 제공 및 교환은 표면적으로 법적 계약에 의해 규제받지는 않지만, 전자상거래의 경우 정보제공 및 교환은 일종의 암묵적 계약에 의해 지배받는 비금전적 교환의 한가지 형태로 생각된다. 사회적 계약은 당사자의 권한 및 책임과 관련된 당사자 사이의 공유된 규범으로 구성된다(박찬욱 등, 2014). 이러한 측면에서 사회적 계약이론은 기업과 고객 사이의 정보제공 및 교환관계를 설명할 수 있으며, 주로 마케팅 분야에서 많이 적용되고 있다(민현홍 등, 2016).

Ⅲ. 연구모형구축 및 가설설정

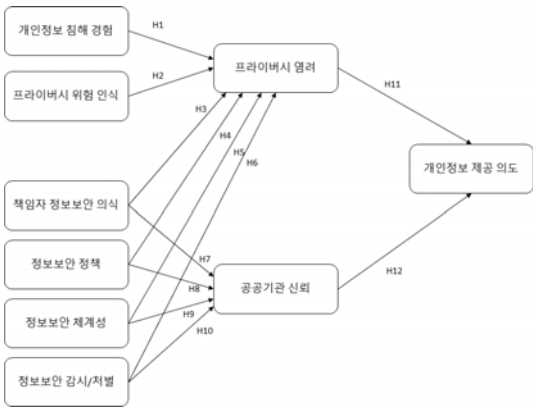
3.1 연구모형구축

최근의 인터파크를 비롯하여 각종 금융 및 카드회사, 대형 인터넷 쇼핑몰 등 공공서비스 성격을 지닌 조직에서 정보서비스의 개인정보 유출 사건이 빈번하게 발생하여 이와 같은 서비스를 이용하는데 필수적 요소인 개인정보 제공을 사용자들이 꺼려하고 있는 실정이다(박성희, 2014). 이와 같은 상황에서도 공공행정 서비스의 인터넷 또는 모바일 서비스가 급속하게 확산되고 있으며, 공공행정 서비스에 있어서 개인의 정보제공은 필수적인 요건으로 인식되고 있다(김기열, 2010). 이러한 개인정보 제공의도와 관련하여 본 연구에서는 공공기관 서비스에 대해 프라이버시 염려를 중심으로 하는 사용자 측면과 정보서비스를 제공하는 공공기관의 신뢰 측면에서 접근하고자 한다.

개인정보의 제공은 정보를 제공하는 대상측면을 살펴볼 필요가 있다. 공공행정 기관과 같이 신뢰도가 높은 조직에서 정보서비스를 실시하는 경우 프라이버시 위험인식이 낮아지게 되어 개인정보를 제공하고자 하는 의도가 증가하게 된다(김유정, 2015). 이는 공공기관이 지니고 있는 높은 신뢰의 속성이 내재되어 있기 때문이다. 따라서 프라이버시 위험을 낮게 인식하는 것은, 이에 따른 프라이버시 염려를 감소시켜, 민간서비스 보다 공공기관의 정보서비스에 대해서 이용자들이 개인의 정보를 손쉽게 제공하게 된다. 이는 공공기관의 경우 높은 신뢰도를 기반으로 하고 있기 때문에, 자신이 공개한 개인정보가 손실될 가능성이 낮을 것이라고 생각하기 때문이다(곡민 등, 2015).

본 연구에서는 공공기관의 신뢰에 영향을 미치는 요인으로 정보보안에 초점을 두어 책임자의 보안의식, 정보보안 정책, 정보보안의 체계성, 정보보안 감사 및 처벌 등을 중심으로 연구모형을 구축하고자 한다(Cavusoglu et al, 2015;

Jarvelainen, 2013). 즉, 본 연구는 공공서비스에 대한 개인정보 제공과 관련하여, 사용자 측면에서 프라이버시 염려와 공공기관 신뢰를 매개변수로 하여 이들에 대한 영향요인들의 영향력을 파악하고자 한다. 특히, 프라이버시 염려의 영향요인으로 개인정보 침해와 프라이버시 위험을 중심으로 접근하고자 한다. 또한 공공기관 신뢰의 영향요인으로 책임자 정보보안 의식, 정보보안 정책, 정보보안 체계성, 정보보안 감시 및 처벌 등의 측면에서 접근하고자 한다. 이와 같은 점들을 고려하여 공공서비스의 개인정보 제공의도에 대해 구축된 실증 연구모형을 <그림 1>에 나타내었다.



<그림 1> 연구 모형

3.2 가설설정

프라이버시 염려

프라이버시 침해가 발생하는 경우 민간서비스 상황에서는 법적 소송을 거쳐야 하지만, 공공서비스의 경우 내부 프라이버시 규정이 잘 확립되어 있고, 공신력을 바탕으로 하기 때문에, 법적 소송과 관련없이 이를 보상하는 것을 사용자들에게 전제함으로써 프라이버시 염려가 줄어들 수 있다(심재윤 등, 2015). 또한 프라이버시 계산모형의 논리에 따라서 공공서비스의 경우 개인정보 침해가능성에 따른 위험보다 개인정보 제공에 따른 효익이 높다고 인식하는 경우 프라이버시에 대한 염려가 줄어들게 된다(안수미 등, 2014). 이와는 반대로, 프라이버시 노출에 대한 개인경험이 프라이버시 위험인식을 불러일으켜 프라이버시 염려를 초래하며, 이러한 프라이버시 염려가 개인정보 제공의도에 영향을 미치게 된다(민현홍 등, 2016). 이상의 논의를 토대로 공공서비스에 있어서 개인정보 침해경험과 프라이버시 염려에 관하여 다음과 같은 가설을 설정하였다.

H1: 개인정보 침해경험은 프라이버시 염려에 정(+)의 영향을 미칠 것이다.

공공서비스에 있어서도 밴드나 트윗기능을 담은 SNS 서비스를 실시하는 경우, 타인의 정보수집 행위를 통제하는 기능이 취약하기 때문에 개인정보 노출이 쉽게 이루어지고 있다(Knijnenburg and Kobsa, 2013). 이로 인해서 프라이버시 위험인식이 발생하고, 이에 따른 프라이버시 위험이 제고될 여지도 있다. 특히, 공공기관의 온라인 게시판 등에서 실명인증이 존재하고 있어, 프라이버시의 위험과 염려가 높아지고 있는 상황이다(Miltgen and Smith, 2015). 이와 같이 SNS 또는 인터넷 게시판 등 공공서비스 사용자가 개인정보 제공결정 과정에서 프라이버시 위험인식이 높아지며, 이에 따른 프라이버시 염려 또한 높아지게 된다. 이상의 논의를 토대로 공공서비스에 있어서 프라이버시 위험

인식과 프라이버시 염려에 관하여 다음과 같은 가설을 설정하였다.

H2: 프라이버시 위험 인식은 프라이버시 염려에 정(+)의 영향을 미칠 것이다.

개인정보의 유출에 대한 책임은 원천적으로 최고 경영자에게 있다. 따라서 온라인 서비스를 통해서 정보를 제공하는 기업 혹은 기관의 최고 경영자는 이러한 정보보안 침해에 대해 많은 관심을 가지고 있다(김유정, 2015). 온라인 서비스 기관의 책임자가 정보보안 통제능력을 인식하고, 이용자에게 공지하는 등 의사소통의 노력을 기울이고, 개인정보 유출이 발생할 시 이에 대한 금전적 보상까지 제시한다면, 이용자들의 프라이버시에 대한 염려를 줄여주게 된다(심재윤 등, 2015). 따라서 다음과 같은 가설을 설정하였다.

H3: 책임자 정보보안 의식은 프라이버시 염려에 부(-)의 영향을 미칠 것이다.

정부나 지자체와 같은 공공기관은 개인정보보호에 대한 내용과 기술적인 방안, 그리고 이에 대한 책임 규정이 일반적으로 잘 갖추어져 있으며, 이를 공식적으로 공시하고 있다(Wu et al., 2012). 이와 같은 프라이버시 인증과 같은 정보보안 정책을 공시하고, 규칙과 제도가 제대로 확립되어 있는 경우에 웹 사이트를 이용하는 사용자의 프라이버시 염려를 감소시켜 줄 수 있다(Cavusoglu et al., 2015). 즉 정보 프라이버시 정책이 체계적으로 확립되어 있는 경우에 이용자들은 프라이버시 염려가 줄어들어 자신의 의견을 적극적으로 개진할 수 있게 된다(Miltgen and Smith, 2015). 따라서 다음과 같은 가설을 설정해 볼 수 있다.

H4: 정보보안 정책은 프라이버시 염려에 부(-)의 영향을 미칠 것이다.

프라이버시 보안 절차에 대해 조직내부 규정을 명확하게 확립하여 개인정보 관리를 철저하게 하는 정보보안 시스템이 체계적으로 구축되어 있으면 조직 내부적으로 개인정보 유출을 사전에 방지할 수 있다(박찬욱 등, 2014). 정보보안 체계성은 정보보안 자원의 가용성을 제고시켜 구성원들과 조직전반에 정보보안 활동에 대한 자기 효능감을 높여주는 역할을 한다(박성희, 2014). 이러한 조직 내부에 구축된 정보보안 체계는 이용자들의 프라이버시 염려를 감소시키게 되며, 따라서 다음과 같은 가설을 설정해 볼 수 있다.

H5: 정보보안 체계성은 프라이버시 염려에 부(-)의 영향을 미칠 것이다.

철저한 감시를 통해 실시간으로 개인정보 유출을 감시하고, 이를 어기는 경우 강력하게 처벌하는 시스템이 조직 내부에 확립되어 있는 경우 정보보안의 침해를 빠르게 인지하게 된다(Jarvelainen, 2013). 따라서 이와 같은 정보보안 감시/처벌체제가 잘 확립되어 있는 경우 이용자들에게 개인정보 보안에 대한 확신을 심어주게 되어 프라이버시에 대한 염려를 줄일 수 있도록 해준다(Miltgen and Smith, 2015). 정보보안과 관련된 책임자의 의식, 정보보안 정책, 정보보

안의 체계성, 정보보안에 대한 감시/처벌은 프라이버시 염려를 줄일 수 있을 것이며, 따라서 다음과 같은 가설을 설정해 볼 수 있다.

H6: 정보보안 감시/처벌은 프라이버시 염려에 부(-)의 영향을 미칠 것이다.

공공기관 신뢰

최고경영층의 지원은 조직의 정보보호정책 성숙도에 영향을 미치는 가장 중요한 요인으로 작용하고 있다(Knijnenburg and Kosba, 2013). 최고경영자가 정보보안 관리에 적극적으로 참여하는 경우에 정보보안 시스템이 성공적으로 구축되고, 대외적으로 정보서비스에 대한 신뢰를 확보할 수 있게 된다. 이러한 맥락에서 공공서비스의 책임자 보안의식은 개인정보와 관련하여 해당 공공기관의 신뢰에 결정적인 영향을 미치게 된다(김상희, 2015). 정보보안 책임자가 정보보안 전략에 대한 명확한 비전, 목적 및 목표 설정을 조율하고 구성하는 지원활동을 하게 되면, 명료하고 실행가능한 정보보안 정책이 수립되게 된다. 따라서, 정보보안 정책을 실행하기 위한 정보보안 자원의 가용성이 높아지기 때문에, 이를 이용하는 사용자의 소속 조직에 대한 신뢰가 높아질 수 있다(김유정, 2015). 따라서 다음과 같은 가설을 설정해 볼 수 있다.

H7: 책임자 정보보안의식은 공공기관 신뢰에 정(+)의 영향을 미칠 것이다.

소비자들은 정보 프라이버시 정책에 대한 인식여부에 따라 정보 프라이버시 신뢰에 대한 영향에 차이가 나타난다(민진영 등, 2013). 정보보안 정책은 정부나 기업에서 개인정보의 보호를 위해 수집하는 개인정보에 대한 내용, 보호를 위한 기술적 방안 및 개인정보 관리에 대한 책임규정을 지칭한다(Wu et al., 2012). 정보보안 정책이 모호하고 어렵게 기술되어 있을 경우 소비자들은 정책을 신뢰하지 않게 된다(김유정, 2015). 반면에, 정보보안 정책이 잘 정의되고 검증될 경우 사용자들로 부터 안전성과 신뢰성을 확보할 수 있다. 또한 개인정보 보호를 위한 규정, 시스템 존재여부, 적절성 등의 정보보안 정책이 기업의 정보보안 신뢰에 영향을 줄 수 있다(Miltgen and Smith, 2015). 이상의 논의를 토대로 공공서비스에 있어서 정보보안 정책과 공공기관의 신뢰에 관하여 다음과 같은 가설을 설정하였다.

H8: 정보보안 정책은 공공기관 신뢰에 정(+)의 영향을 미칠 것이다.

민현홍(2016)은 관리적 정보보안 자원이 조직의 신뢰 형성에 영향을 미친다는 것을 발견하였다. 정보보안에 대한 취약점 분석/평가, 침해행위 대응활동과 같은 기술적 요인은 공공기관의 신뢰와 이를 통한 개인정보 제공의도에 영향을 미칠 수 있다(안수미 등, 2014). 헬프데스크, 온라인 정보보안정책 이용지원, 정보보안 정책에 대한 홍보 및 교육 등 정보보안 체계가 제대로 확립되면, 공공기관의 구성원들이 정보보안 정책을 준수하게 되고, 이를 통해 개인정보와 관련된 공공기관의 전반적 신뢰를 제고시킬 수 있게 된다(심재윤 등, 2015). 이상의 논의를 토대로 공공서비스에 있어서 정보보안 정책과 공공기관의 신뢰에 대하여 다음과 같은 가설을 설

정하였다.

H9: 정보보안 체계성은 공공기관 신뢰에 정(+)의 영향을 미칠 것이다.

일반적으로 사람들은 협력적 행동을 통해 목표를 달성해야 하는 상황에서 신뢰가 부족할 경우 처벌시스템의 도입을 희망한다(Cavusoglu et al, 2015). 조직에서 처벌시스템이 작동하면 기회주의적 행동을 하는 사람들에 의해 자신이 피해를 보지 않을 것이라는 신뢰가 형성되기 때문이다. Irwin et al.(2014)은 처벌시스템과 보상시스템이 그룹내 구성원들 간 신뢰와 협력에 긍정적으로 영향을 미친다고 주장하였다. 결국 정보보안에 대한 감시와 처벌시스템이 잘 갖추어질수록 공공기관의 내적신뢰와 협력이 강화되어, 개인정보 보안을 취급하는 공공기관 전반에 대한 신뢰가 제고된다(김상희, 2015). 이상의 논의를 토대로 공공서비스에 있어서 정보보안 감시 및 처벌과 공공기관의 신뢰에 관하여 다음과 같은 가설을 설정하였다.

H10: 정보보안 감시 및 처벌은 공공기관 신뢰에 정(+)의 영향을 미칠 것이다.

개인정보 제공의도

최근 정보기술의 발전으로 인해 자신의 의지와 상관없이 자신의 개인정보가 광범위하게 수집되는 경우가 빈번하게 발생하고 있으며, 자신의 개인정보가 언제 어디에서 어떻게 사용되고 있는지 규제할 수 없다는 점에서 개인의 프라이버시 염려가 더욱 증가하고 있는 실정이다(임진택 등, 2015). 이러한 부정적인 요소가 증가하게 되면, 프라이버시 계산 모형의 논리에서 혜택보다 위험이 커지게 되어 결국 개인정보 제공을 포기하게 된다(심재윤 등, 2015). 이상의 논의를 토대로 공공서비스에 있어서 사용자가 인식하는 프라이버시 염려와 개인정보 제공의도에 관하여 다음과 같은 가설을 설정하였다.

H11: 프라이버시 염려는 개인정보 제공의도에 부(-)의 영향을 미칠 것이다.

공공기관에 대한 조직신뢰가 높은 사용자는 신뢰성에 대한 확신을 가지고 있기 때문에, 개인정보 침해의 우려에도 불구하고 잔류해야 한다는 당위성과 책임감 차원에서 지속적으로 개인정보를 제공하는 규범적 몰입의 성향이 나타나게 된다(김유정, 2015). 특히, 온라인에서 거래할 때 조직에 대한 신뢰는 사용자의 긍정적인 태도를 형성시켜, 개인정보침해나 프라이버시 위험의 불확실성을 감소시켜주며 만족스러운 거래를 도와준다(곡민 등, 2015). 기존 조직신뢰에 대한 연구들은 강한 신뢰성을 가지고 있는 사용자들이 조직에서 요구하는 개인정보를 제공하고자 하는 의지가 높다는 것을 보여주고 있다(김희선, 2015). 이상의 논의를 토대로 공공서비스에 있어서 공공기관에 대한 신뢰와 개인정보 제공의도에 관하여 다음과 같은 가설을 설정하였다.

H12: 공공기관 신뢰는 개인정보 제공의도에 정(+)의 영향을 미칠 것이다.

Ⅳ. 방법론

실증연구 모형에 포함하고 있는 변수에 대해서 <표 1>과 같이 기존 선행연구를 토대로 개인정보 제공의도, 프라이버시 염려 및 영향요인(개인정보 침해 경험, 프라이버시 위험인식), 공공기관 신뢰 및 영향요인(책임자의 정보보안 의식, 정보보안 정책 및 체계성, 감시 및 처벌)에 대해서 조작적 정의에 따른 설문지항목을 구성하였다. 각 측정 항목은 5점 Likert 척도로 구성하였다.

<표 1> 설문지의 설문항목

변수	항목	선행연구
개인정보 침해경험	온라인이나 SNS에서 프라이버시를 침해당했다고 느낄 정도의 침해가 있다 온라인이나 SNS에서 부당하게 프라이버시 침해를 당한 사용자라고 느낀적이 있다 온라인이나 SNS에서 해킹을 당해 개인신상정보를 유출당한 경험이 있다 온라인이나 SNS에서 인터넷 계정을 해킹당한 경험이 있다	Wu et al(2011) 민현홍등(2016)
프라이버시 위험인식	우리사회가 가지고 있는 프라이버시 문제와 관행에 대해 알고 있다 프라이버시 문제와 프라이버시 침해에 관한 뉴스와 사건을 유심히 지켜본다 공공기관이 개인의 프라이버시 문제를 취급하는데 이용하는 방법과 해결책들을 알고 있다 공공기관이 개인의 프라이버시 문제를 중요하게 취급하고 있다	Wu et al(2011) 김상희(2015) 민현홍등(2016)
책임자 정보보안 의식	공공기관의 정보보안 책임자들은 정보보안에 대한 명확한 비전을 가지고 있다 공공기관의 정보보안 책임자들은 체계적인 정보보안을 달성하기 위한 명확한 전략을 가지고 있다 공공기관의 정보보안 책임자들은 체계적인 정보보안을 달성하기 위한 명확한 목표와 목적을 가지고 있다 공공기관의 정보보안 책임자들은 체계적인 정보보안을 달성하는데 필요한 지식을 가지고 있다	Wu et al(2012) 박성희(2014)
정보보안 정책	공공기관은 정보시스템의 적절한 사용방법을 명확하게 기술한 가이드라인을 가지고 있다 공공기관은 정보시스템에 권한없는 사람이 접근하는 것을 제한하는 매뉴얼이 있다 공공기관은 정보보안 담당자들이 정보시스템 비밀번호를 적절하게 사용하도록 하는 가이드라인이 있다 공공기관은 정보시스템 관련 담당자들의 업무를 명확하게 정의한 가이드라인이 있다	Wu et al(2012) 김유정(2015)
정보보안 체계성	온라인에서 공공기관의 정보보안 정책을 확인할수 있다. 공공기관의 정보보안 정책은 온라인에서 명료하고 이해가능한 형태로 작성되어 있다 공공기관의 정보보안 담당자들은 컴퓨터계정을 받기전에 적절한 정보보안교육을 받는다 공공기관에서 정보보안인식제고를 위한 다양한 커뮤니케이션(뉴스레터, 프로터, 공지등)이 이루어지고 있다.	곡민등(2015) 김유정(2015)
정보보안 감시/처벌	공공기관은 정보보안규칙을 위반하는 행위를 항상 적발한다. 공공기관은 정보보안규칙을 위반하는 담당자를 반드시 적발한다. 공공기관은 정보보안규칙을 반복적으로 위반하는 담당자를 반드시 처벌한다. 공공기관은 정보보안규칙의 실행정도를 감시하기 위한 감사활동이 정기적으로 이루어지고 있다 공공기관은 정보보안규칙의 위반행위발견시 반드시 대처활동이 이루어지고 있다.	김상희등(2015) 김유정(2015)
프라이버시 염려	온라인에서 공공기관에 개인정보를 제공하는 것은 위험이 수반된다. 온라인에서 공공기관에 개인정보를 제공하는 것은 예상치못한 문제를 발생시킬수 있다 온라인에서 공공기관에 개인정보를 제공하는 것은 불확실성의 요소가 많다. 온라인에서 공공기관에 개인정보를 제공하는 것은 나에게 손실이 발생할수 있다. 온라인에서 공공기관에 개인정보를 제공하는 것은 안전하지 못하다.	Wu et al(2010) 김상희(2015) 민현홍등(2016)
공공기관 신뢰	개인정보를 요구한 공공기관은 개인정보보안과 관련된 안전한 환경이 구축되어 있다. 개인정보를 요구한 공공기관은 체계적인 방법으로 개인이 제공한 정보를 처리할수 있다 개인정보를 요구한 공공기관은 개인정보보호를 위해 신뢰할수 있는 유능한 책임자를 배치할 것이다 개인정보를 요구한 공공기관은 개인정보를 보관하고 있는 컴퓨터시설이 외부 침입자로부터 안전하게 보호될 것이다. 개인정보를 요구한 공공기관은 개인정보를 안전하게 관리할 것이다.	Lin et al(2015) 박천웅(2014)
개인정보 제공의도	공공기관에서 기본정보를 요청하면 제공할 의향이 있다 공공기관에서 기본정보외에 추가정보(자격, 소득, 신용)를 요청하면 제공할 의향이 있다 공공기관에서 기본정보외에 민감정보(정치성향, 병력, 생활방식)릉 요청하면 제공할 의향이 있다 공공기관에서 정보제공에 대한 혜택을 제공한다고 하면 개인정보를 좀더 정확하게 제공할 의향이 있다	Knijnenburg et al(2013) 박천웅(2014)

Ⅴ. 결과 분석

5.1 표본의 특성

본 연구의 표본설계 방법은 무작위 추출방법을 이용하였고 설문 조사는 2016년 4월-6월 동안 총 400명을 대상으로 설문지를 배포하였으며, 이 중 375부를 회수하였다. 회수된 설문지 중 불성실한 설문지를 제외하고 332부를 실증분석에 활용하였다.

<표 2> 표본의 인구통계적 특성

변 수 명		빈도(명)	비율(%)
성별	남자	185	55.7
	여자	147	44.3
	전체	332	100.0
연령	20대 미만	2	.6
	20대	94	28.3
	30대	84	25.3
	40대 이상	152	45.8
	전체	332	100.0
교육수준	고졸	62	18.7
	대학/전문대 재학	66	19.9
	대학/전문대 졸업	191	57.5
	대학원 재학/졸업	13	3.9
	전체	332	100.0
직업	학생	46	13.9
	사무/관리/전문직	206	62.0
	자영업	9	2.7
	주부	21	6.3
	기타	50	15.1
	전체	332	100.0

응답자 332명 중 남성이 55.7%, 여성이 44.3%를 차지하였다. 연령대의 경우 40대 이상이 45.8%로 가장 많은 비율을 차지하였으며, 20대 28.3%, 30대 25.3%의 순으로 구성되었다. 교육수준은 대학 및 전문대 졸업자가 전체의 57.5%로 가장 많은 비율을 차지하였으며, 대학 및 전문대 재학 19.9%, 고졸 18.7%, 대학원 이상이 3.9%를 차지하였다. 직업의 분포의 경우 사무/관리/전문직이 전체의 62%로 가장 많은 비율을 차지하였으며, 학생 13.9%, 주부 6.3%, 자영업자 2.7% 등의 순으로 구성되었다. 실증조사 분석에 활용된 표본특성은 <표 2>에 나타낸 바와 같다.

5.2 측정모형의 평가

변수의 신뢰도 및 타당도, 측정모형을 평가하기 위해서 SPSSWIN과 AMOS를 사용하여 탐색적 요인분석 및 확인적 요인분석을 실시하였다. 탐색적 요인분석 방법은 실증연구 모형에 포함하고 있는 모든 변수를 투입하여, Varimax 회전방법과 주성분분석을 실시하였다. 요인분석결과 실증 연구모형에서 설계한 바와 같이 9개의 요인이 도출되었다. 이들 9개 요인에 의한 전체 설명력은 약 75.8%로 나타났다. 각 요인의 고유값은 정보보안 체계성이 .956으로 조금 낮게 나타났으나, 다른 요인들은 모두 기준값인 1.0을 상회하는 것으로 나타났다. 요인분석과정에서 프라이버시 염려 요인의 2개 문항과 정보보안 체계성의 2개 문항이 교차부하 및 적재값이 낮아서 제외되었다.

탐색적 요인분석을 통해 구성타당성이 확인된 항목과 요인을 대상으로 AMOS를 활용하여 확인적 요인분석을 실시하였다. 또한 확인적 요인분석 결과 최종 타당성이 확인된 항목을 대상으로 신뢰도 검증을 실시하였다. 신뢰도 검증은 Cronbach's α 값, AVE, 합성신뢰도를 통해 실시하였다. 확인적 요인분석결과와 신뢰도 분석결과는 <표 3>에 나타난 바와 같다. 확인적 요인

<표 3> 확인적 요인분석 및 신뢰도검증 결과

변수		추정값	S.E.	C.R.	AVE	크론바하α	합성신뢰도
개인정보 침해 경험	A1	.910			.613	.876	.859
	A2	.917	.050	2.577			
	A3	.671	.060	14.071			
	A4	.578	.064	11.462			
프라이버시 염려	B1	.676			.539	.759	.774
	B2	.879	.132	1.621			
	B3	.624	.107	9.721			
프라이버시 위험인식	C1	.783			.718	.931	.927
	C2	.854	.047	22.884			
	C3	.900	.063	18.254			
	C4	.832	.068	16.563			
	C5	.866	.066	17.442			
책임자 정보보안 의식	D1	.842			.760	.926	.926
	D2	.891	.050	2.999			
	D3	.897	.046	21.255			
	D4	.857	.051	19.669			
정보보안 정책	E1	.888			.667	.886	.888
	E2	.864	.044	2.980			
	E3	.780	.047	17.642			
	E4	.726	.052	15.737			
정보보안 체계성	F1	.897			.561	.672	.709
	F2	.565	.083	7.898			
정보보안 감시/처벌	G1	.778			.548	.875	.858
	G2	.752	.057	16.793			
	G3	.728	.076	13.072			
	G4	.712	.073	12.668			
	G5	.731	.069	13.053			
공공기관 신뢰	H1	.867			.722	.928	.928
	H2	.867	.048	21.349			
	H3	.807	.050	18.725			
	H4	.816	.051	19.114			
	H5	.891	.045	22.505			
개인정보 제공의도	J1	.738			.633	.869	.873
	J2	.879	.079	15.194			
	J3	.770	.072	13.526			
	J4	.789	.08	13.870			

χ^2(df)=102.231(554), χ^2/df=1.842, RMR=.037, GFI=.857, AGFI=.829, NFI=.889, IFI=.946, TLI=.938, CFI=.946, RMSEA=.050

분석 결과는 탐색적 요인분석 결과와 마찬가지로 모든 요인에 대한 구성 항목들이 유의한 구성타당성이 있는 것으로 나타났다.

확인적 요인분석결과 측정모형에 대한 적합도의 경우, 샘플 수에 민감하게 반응하는 χ^2의 값이 1,020으로 나타났지만, 이에 대한 대안값인 χ^2/df이 1.842로 적합하다는 것을 보여주고 있다. 또한 GFI .857, AGFI .829, NFI .889, TLI

<표 4> 판별타당성 분석결과

변 수	1	2	3	4	5	6	7	8	9
1. 개인정보 침해 경험	.782								
2. 프라이버시 위험 인식	.279**	.734							
3. 프라이버시 염려	.247**	.296**	.847						
4. 책임자 정보보안 의식	.131*	.127*	-.273**	.871					
5. 정보보안 정책	.141*	.245**	-.058	.613**	.816				
6. 정보보안 체계성	.108*	.180**	-.026	.465**	.487**	.748			
7. 정보보안 감시/처벌	.161**	.189**	-.156**	.630**	.574**	.442**	.740		
8. 공공기관 신뢰	.146**	.144**	-.191**	.674**	.665**	.470**	.706**	.849	
9. 개인정보 제공의도	.018	.028	-.226**	.368**	.273**	.299**	.348**	.418**	.795
평균	2.624	3.393	3.483	2.949	3.240	2.809	2.983	3.040	2.507
표준편차	1.011	.705	.817	.785	.728	.725	.723	.740	.856

* p<.05, **p<.01
대각선 값은 AVE의 제곱근 값

.938, CFI .946, RMSEA .050 등으로 대체로 양호한 적합도 지수를 나타내었다. 신뢰도 검증결과, 내적 일관성을 나타내는 Cronbach α값이 .672 이상으로 나타났으며, AVE는 최소 .548, 합성신뢰도는 .709 이상으로 나타나, 모두 기준값을 넘고 있어서 신뢰도에 문제가 없음을 확인할 수 있다.

판별타당도를 검증하기 위해서 구성변수 사이의 상관계수와 AVE 제곱근값을 비교하였으며, 이에 대한 분석결과는 <표 4>에 나타낸 바와 같다. 판별타당성 분석결과를 살펴보면, 상관관계표의 대각선에 위치한 AVE 제곱근값이 모두 상관계수의 값을 상회하고 있어 판별타당성에 문제가 없음을 보여주고 있다.

5.3 구조모델분석 및 가설검증

연구모형과 가설을 검증하기 위해서 개인정보 제공의도에 대한 프라이버시 염려와 공공기관 신뢰를 매개변수로 하는 구조모델 분석을 실시하였다. 구조모델 분석방법은 ML추정에 의한 Bootstap 방법을 실시하였다. 구조모델의 적합도는 샘플수에 민감한 x2값이 950.736으로 높게 나타났지만, 대안값인 χ^2/df값 1.701로 기준값을 충족하는 것을 보여주고 있다. 이외에 GFI .865, AGFI .839, NFI .897, TLI .949, CFI .954, RMSEA .046으로 나타나 대체로 양호한 모델적합도를 나타내고 있는 것을 확인할 수 있다. 이러한 구조모델 분석결과를 토대로 가설검증 결과를 정리하면 <표 5>와 같다.

프라이버시 염려와 영향요인에 관련된 가설을 살펴보면, 개인정보 침해 경험과 프라이버시 염려에 관한 가설 H1은 개인정보 침해 경험이 프라이버시 염려에 유의한 정(+)의 영향을 미치는 것으로 나타났다(β=.174, t=2.848). 이는 개인정보 침해 경험이 많을수록 공공서비스에 대

<표 5> 가설검증결과

가설	내용			표준화된 Estimate	비표준화 Estimate	S.E.	t	P	채택 여부
H1	개인정보 침해경험	→	프라이버시 염려	.214	.153	.042	3.674	***	채택
H2	프라이버시위험 인식	→	프라이버시 염려	.299	.391	.087	4.477	***	채택
H3	책임자 정보보안 의식	→	프라이버시 염려	-.391	-.371	.088	-4.208	***	채택
H4	정보보안 정책	→	프라이버시 염려	.153	.171	.105	1.634	.102	기각
H5	정보보안 체계성	→	프라이버시 염려	.053	.080	.117	.677	.498	기각
H6	정보보안 감시/처벌	→	프라이버시 염려	-.153	-.184	.113	-1.629	.103	기각
H7	책임자 정보보안 의식	→	공공기관 신뢰	.198	.185	.059	3.143	.002	채택
H8	정보보안 정책	→	공공기관 신뢰	.203	.223	.070	3.188	.001	채택
H9	정보보안 체계성	→	공공기관 신뢰	.126	.187	.082	2.287	.022	채택
H10	정보보안 감시/처벌	→	공공기관 신뢰	.452	.532	.084	6.369	***	채택
H11	프라이버시 염려	→	개인정보 제공의도	-.167	-.188	.062	-3.032	.002	채택
H12	공공기관 신뢰	→	개인정보 제공의도	.427	.489	.068	7.231	***	채택

χ^2(df)=950.736(559), χ^2/df=1.701, RMR=.037, GFI=.865, AGFI=.839, NFI=.897, IFI=.955, TLI=.949, CFI=.954, RMSEA=.046

한 사용자가 인식하는 프라이버시 염려가 높아지는 것을 의미한다.

프라이버시 위험 인식과 프라이버시 염려에 관한 가설 H2는 프라이버시 위험 인식이 프라이버시 염려에 정(+)의 영향을 미치는 것으로 나타났다(β=.260, t=3.926). 이러한 결과는 공공서비스에 대해 개인이 인식하는 프라이버시 위험이 높을수록 이에 따른 프라이버시 염려 또한 제고되는 것을 의미한다. 프라이버시 염려와 영향요인에 관한 분석결과를 살펴보면, 개인정보 침해경험과 프라이버시 위험인식 모두 프라이버시 염려에 유의한 정(+)의 영향을 미치며, 특히 공공기관 정보서비스에 있어서 프라이버시 위험인식이 프라이버시 염려에 미치는 영향의 강도가 상대적으로 강하다는 것을 보여주고 있다.

책임자의 정보보안 의식과 프라이버시 염려에 관한 가설 H3은 책임자의 정보보안 의식이 프라이버시 염려에 부(-)의 영향을 미치는 것으로 나타났다(β=-.391, t=-4.208). 이러한 결과는 공공기관의 책임자가 정보보안에 대한 의식이 높을수록 이에 따른 프라이버시 염려가 감소되는 것을 의미한다. 그러나 프라이버시 염려에 대한 정보보안 정책(β=.151, t=1.634)의 영향 관한 가설 H4, 정보보안 체계성(β=.053, t=.677)의 영향에 관한 가설 H5, 정보보안 감시

및 처벌(β=-.153, t=-1.629)의 영향에 관한 가설 H6은 통계적으로 유의하지 않은 것으로 나타났다.

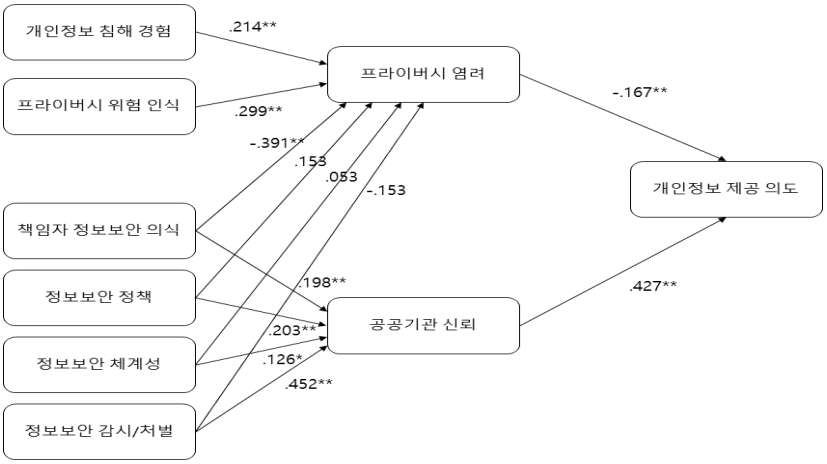
다음으로 공공기관 신뢰와 영향요인에 관련된 가설을 살펴보면, 책임자의 정보보안 의식과 공공기관 신뢰에 관한 가설 H7은 책임자의 정보보안 의식이 공공기관 신뢰에 유의한 정(+)의 영향을 미치는 것으로 나타났다(β=.198, t=3.143). 이는 책임자의 정보보안 의식수준이 높을수록 사용자가 지각하는 공공기관에 대한 신뢰수준이 제고되는 것을 의미한다. 정보보안 정책과 공공기관 신뢰에 관한 가설 H8은 정보보안 정책이 공공기관 신뢰에 정(+)의 영향을 미치는 것으로 나타났다(β=.203, t=3.188). 이러한 결과는 공공서비스에 있어서 책임자의 정보보안 의식이 높을수록 사용자들이 인식하는 공공기관 신뢰가 제고되는 것을 의미한다.

정보보안 체계성과 공공기관 신뢰에 관한 가설 H9는 정보보안 체계성이 공공기관 신뢰에 정(+)의 영향을 미치는 것으로 나타났다(β=.126, t=2.287). 이러한 결과는 공공서비스에 있어서 정보보안 체계성이 높을수록 사용자들이 인식하는 공공기관 신뢰가 제고되는 것을 의미한다. 정보보안 감시 및 처벌과 공공기관 신뢰에 관한 가설 H10은 정보보안 감시 및 처벌이 공공기관 신뢰에 정(+)의 영향을 미치는 것으로 나타났다(β=.452, t=6.369). 이러한 결과는 공공서비스에 있어서 정보보안 감시 및 처벌 강도가 높을수록 사용자들이 인식하는 공공기관 신뢰가 제고되는 것을 의미한다. 이러한 결과를 검토하면, 공공기관의 정보보안 관리적 요인 모두가 공공기관 신뢰에 긍정적으로 작용하며, 특히 정보보안 감시 및 처벌시스템이 미치는 영향이 가장 강하게 나타나고 있음을 보여준다.

마지막으로 프라이버시 염려 및 공공기관 신뢰와 개인정보 제공의도와 관련된 가설을 살펴보면, 프라이버시 염려와 개인정보 제공 의도에 관한 가설 H11은 사용자의 프라이버시 염려가 개인정보 제공의도에 부(-)의 영향을 미치는 것으로 나타났다(β=-.167, t=-3.032). 이는 사용자의 프라이버시 염려가 높아질수록 자신의 개인정보를 공공기관에 제공할 의도가 낮아진다는 것을 의미한다. 공공기관 신뢰와 개인정보 제공의도에 관한 가설 H12는 공공기관 신뢰가 개인정보 제공 의도에 정(+)의 영향을 미치는 것으로 나타났다(β=.427, t=7.231). 이는 사용자가 공공기관을 신뢰하는 수준이 높아질수록 자신의 개인정보를 제공할 의도가 높아지는 것을 의미한다. 이러한 결과를 살펴보면, 사용자의 프라이버시 염려와 공공기관의 신뢰 모두 개인정보 제공에 긍정적으로 작용하며, 특히 공공기관의 신뢰도가 개인정보 제공의도에 미치는 영향이 매우 강하다는 것을 보여준다. 연구모형에 대한 구조모델 분석 결과를 도식화하면 <그림 2>와 같다.

5.4 분석결과의 의미

실증 연구의 결과를 요약하면 다음과 같다. 공공서비스에 대한 개인정보 제공의도에 있어서 사용자 개인적 관점에서 프라이버시 염려와 조직관점에서 공공기관 신뢰 모두 유의한 영향력을 보이고 있으며, 특히 조직관점에서 공공기관의 신뢰가 매우 강한 영향을 미치고 있다는 것을 확인하였다. 이러한 결과를 고려할 때, 공



* p<.05, **p<.01

<그림 2> 구조모델 분석결과

공기관 정보서비스의 상황에서 기존의 개인적 관점에서 주로 많이 다루어 왔던 프라이버시 계산모형 등의 경제적 효익과 비용의 논리보다는 조직신뢰의 논리가 더욱 중요한 요인으로 작용하고 있음을 알 수 있다.

공공기관 정보서비스에 대한 프라이버시 염려에 대해서 개인정보 침해경험과 프라이버시 위험인식 모두 정(+)의 영향을 미치는 것을 확인할 수 있었다. 특히, 기존의 개인정보 침해경험보다는 프라이버시 위험인식이 프라이버시 염려에 더욱 많은 영향을 미친다는 사실이 중요하다. 그동안 민간분야의 개인정보 유출사건이 언론을 통해 대서특필되어 사회적으로 이슈화된 반면에, 공공기관의 개인정보 노출은 아직까지 크게 이슈화되지 않았다. 그러나 최근 행정자치부의 자체 감사결과에 대한 보도에서 나타난 바와 같이 공공서비스, 특히 지자체의 개인정보 노출은 심각한 수준에 이르고 있는 실정이다. 그럼에도 불구하고 직접적인 개인정보의 침해경험이 간접적인 프라이버시 위험인식보다 프라이버시 염려에 약한 영향을 미치는 이유는 일반시민이 공공서비스에서 개인정보 노출과 같은 부분을 제대로 인식하지 못하는 데서 그 원인을 찾을 수도 있다.

이러한 맥락에서 공공기관은 프라이버시 위험을 줄이기 위한 노력이 필요하다. 일례로 기술적인 측면에서 공인인증 시스템 방법을 활용하거나, 개인 모바일인증과 같은 편리한 방법을 활용하는 등 사용자의 참여를 높여 시민 스스로 프라이버시 위험을 통제할 수 있는 부분을 강화할 필요가 있다. 또한 프라이버시 위험을 줄이기 위해서 사용자와 공공기관의 상호 협력 활동을 높일 필요가 있다. 현재 행정자치부를 중심으로 하는 공공기관자체의 감사이외에 시민이 참여하여 타인의 개인정보를 수집하는 위법행위에 대한 자체 감시활동 등과 같은 개인정보 노출에 대비한 노력이 필요하다. 또한 개인정보 유출이 가장 심각하게 나타나고 있는 지자체와

교육청의 경우 자치단체장과 교육감이 솔선수범하여 정보보안에 대한 관심과 노력을 기울일 필요가 있다.

마지막으로 개인정보 제공의 조직측면인 공공기관의 신뢰에는 책임자의 정보보안 의식, 정보보안 정책, 정보보안 체계성, 정보보안 감시 및 처벌 등 모든 요인들이 긍정적으로 작용하고 있음이 확인되었다. 특히 공공기관의 정보서비스에 있어서 신뢰요인에 정보보안에 대한 감시 및 처벌요인이 매우 강한 영향을 미치고 있음이 나타났다. 이는 중앙정부를 비롯한 개인정보 노출이 가장 높은 지자체, 그리고 교육기관에서 정보보안 위법행위에 대한 상시적인 실시간 모니터링과 이에 따른 엄격한 처벌시스템을 강화해야 할 필요성을 보여준다. 최근 행정자치부의 자체 정보보안 감사보고에 나타난 바와 같이 공공기관의 개인정보 노출에 대한 자체 모니터링 시스템이 미흡하며, 또한 정보유출시 이에 대한 책임과 처벌이 미약한 상황이다. 이러한 이유로 행정자치부는 공공기관의 지속적인 개인정보 보안시스템과 실시간 모니터링 확산을 위해 노력하고 있는 실정이다.

Ⅵ. 결 론

본 연구는 개인관점에서 그동안 프라이버시 연구에서 기반이론으로 이용되고 있는 프라이버시 계산모형을 공공기관 정보서비스에 적용하여 실증적 규명하였다는 점에서 이론적 시사점이 있다. 특히, 본 연구는 공공기관의 프라이버시 연구가 실증적으로 거의 이루어지지 않은 상황에서 개인정보의 침해와 프라이버시 위험인식을 통해 일반 시민들이 민간부분의 정보서비스에서 겪고 있는 프라이버시 염려를 실증적으로 규명하였다. 또한 개인적 차원의 프라이버시와 함께 조직 차원에서 공공기관의 조직신뢰를 함께 포함하여 개인정보 제공행위를 규명하는 이론적 접근을 시도하였다는 점에서 시사점을 지닌다.

그동안 개인정보 제공과 관련된 대부분의 연구들이 정보제공자의 속성에 초점을 둔 개인차원의 프라이버시를 중심으로 다루어 온 것과는 달리 정보서비스 공급자, 즉 정보를 활용하는 조직속성 차원에서 개인정보 제공의도를 규명하는 접근을 시도하였다는 점에서 이론적 시사점을 찾을 수 있다. 본 연구에서는 공공부문의 정보서비스에 있어서 개인적 차원의 프라이버시보다 제도기반의 신뢰, 즉 조직속성 차원의 공공기관의 신뢰성이 더욱 중요하다는 것을 확인하였다는 점에서 이론적으로 시사하는 바가 크다. 따라서 조직신뢰 차원에서 정보보안과 관련된 다차원적인 연구의 필요성이 있다고 생각된다.

본 연구의 결과는 실무적으로도 몇 가지 시사하는 바가 있다. 무엇보다도, 공공기관의 정보서비스에 있어서 개인정보 제공기반을 확보하기 위해서 개인적 차원의 프라이버시 강화도 중요하지만, 공공기관과 자치단체장이 솔선수범하여 조직 내부에서 스스로 신뢰를 구축하여 프라이버시 염려를 줄여주는 것이 필요한 것으로 나타났다. 따라서 공공기관이라는 조직적 특수성에 적합한 조직신뢰를 위한 다각적인 노력의 필요성이 제기된다. 실무적으로는 현재 제도적인 차원에서 정부가 중점적으로 추진하고 있는 정보보안 정책을 지속적으로 확산하고 홍보함

으로써 공공기관의 신뢰성을 제고할 수 있음을 확인할 수 있었다. 그러나, 공공기관의 개인정보 노출이 더욱 심화되는 상황에서 이보다 더욱 중요한 것은 개인정보 보안에 대하여 실시간으로 탐지하는 시스템의 구축이 더욱 시급한 것으로 나타났다.

본 연구는 사용자의 프라이버시와 조직신뢰 맥락을 포함하여, 공공기관 정보서비스에 있어서 개인정보 제공에 대한 연구를 수행하였다. 이러한 개인차원과 조직차원의 연구를 수행하면서 본 연구는 시간과 비용의 한계로 인해 개인속성 차원에서는 핵심요인인 프라이버시 염려와 조직속성 차원에서 정보보안에 초점을 둔 공공기관의 신뢰에 초점을 두고 진행할 수 밖에 없었다. 따라서 본 연구를 통해 공공기관 정보서비스에 있어서 개인차원과 조직차원의 핵심 속성들이 개인정보제공에 미치는 영향을 실증적으로 규명하였다는데 의의가 있지만, 이론적 배경에서 취급하였던 개인차원과 조직차원에서 주요하게 다루어진 다차원적인 속성들을 함께 포함하지 못한 한계점이 있다. 추후 연구에서는 본 연구의 이론적 논리를 토대로 다차원적인 속성을 포함해 나가는 연구의 노력이 필요할 것이다.

프라이버시 이론적인 측면에서 본 연구는 프라이버시 계산모형에서 취급하는 위험과 이익 측면중 위험에 주력하고 있다. 즉 공공기관 정보서비스 이용에 따른 편의와 비용절감 같은 혜택 측면을 고려하지 못하였다. 프라이버시 계산모형의 논리를 제대로 적용하기 위해서는 위험과 이익에 대한 차이분석을 통해 개인정보 제공행위의 의사결정을 규명할 필요가 있으며, 추후 연구에서는 이러한 공공기관 정보서비스의 혜택요소를 함께 포함하는 연구가 필요하다.

조직신뢰 측면에서 본 연구는 정보보안이라는 신뢰에 초점을 두고 접근하였다. 공공기관 맥락에서 조직신뢰는 경제적 호황 및 불황과 같은 거시적 환경요인을 비롯하여 외부신뢰, 내부신뢰, 종합신뢰 등 다양한 요인들이 영향을 미치게 된다. 따라서 추후 연구에서는 공공기관의 상황에 적합한 조직신뢰의 다양한 요인들을 함께 고려하는 연구로 확장해나갈 필요성이 있다.

참고문헌

곡민, 최수정, 김재전, “소셜 네트워킹 사이트에서 자기정보공개 연구 : 계획된 행위이론(TPB)을 적용하여,” 인터넷전자상거래연구, 제15권, 제4호, 2015, pp.1-24.

김기열, "공공부문에 관한 외국의 개인정보보호 법제와 국내 입법의 검토 방향," 법제, 통권 633, 2010, pp.5-48.

김상현, 박현선, "프라이버시 보호인식 및 보호행동의도에 미치는 영향 요인과 프라이버시 침해경험의 조절효과," 인터넷전자상거래연구, 제13권, 제4호, 2013, pp.79-105.

김상희, 정보제공 의도와 실제 정보제공행동 간의 프라이버시 역설에 대한 연구, 부산대학교 박사학위논문, 2015.

김유정, "조직구성원이 지각하는 기업 정보보안 관리에 대한 신뢰 형성 요인," 인터넷전자상거래연구, 제15권, 제4호, 2015, pp.247-264.

김희선, 외식기업의 경영자특성이 조직신뢰, 조

직몰입 및 직무만족에 미치는 영향, 단국대학교 석사학위논문, 2015.

민진영, 김병수, "프라이버시 계산모형을 적용한 SNS 지속 사용 의도에 대한 연구: 페이스북과 카카오톡 사례 중심으로," Information System Review, 제15권, 제1호, 2013, pp.105-122.

민현홍, 박성배, 정진섭, 한경석, "빅데이터 시대의 개인정보 제공의도에 영향을 미치는 요인," 인터넷전자상거래연구, 제16권, 제1호, 2016, pp.95-117.

박성희, "효과적인 정보시스템 보안을 위한 통합적 모형의 연구," 경영교육연구, 제35권, 2014, pp.271-298.

박찬욱, 이상우, “인터넷상에서의 개인정보 보호행동에 관한 연구-보호동기이론을 중심으로,” 인터넷정보학회논문지, 제15권, 제2호, 2014, pp.59-71.

심재윤, 노영희, "학교도서관 이용자의 프라이버시에 대한 인식 조사연구," 한국비블리아학회지. 제26권, 제4호, 2015, pp.31-63.

안수미, 정재영, 김지동, 김범수, "SNS에서 프라이버시 침해의도에 영향을 미치는 요인," Information System Review, 제16권, 제2호, 2014, pp.1-23.

이환수, 임동원, 조항정, "빅데이터 시대의 개인정보 과잉이 사용자 저항에 미치는 영향," 지능정보연구, 제19권, 제1호, 2013, pp.125-139.

임병화, 강동원, "폐쇄형 SNS에서 프라이버시가 지속적인 사용의도에 미치는 영향에 관한 연구: 밴드 사용자를 중심으로," Informations Systems Reviews, 제16권, 제3호, 2014, pp.191-214.

임진택, 김양우, "공공도서관의 개인정보보호 현황분석 및 개선방안 연구: 서울・경기 지역을 중심으로," 정보관리학회지, 제31권, 제4호, 2015, pp.85-108.

장혜진, "컨벤션 종사자의 조직신뢰가 직무만족과 조직몰입에 미치는 영향 연구," 관광연구저널, 제28권, 제3호, 2014, pp.161-179.

Cavusoglu, H., Cavusoglu, H., Son, J.Y. and Benbasat, I., "Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources," Information and Management, Vol.52, 2015, pp.385-400.

Czernek, K. and Czakon, W., "Trust-building processes in tourist cooperation: The case of a Polish region, Tourism Management, Vol.52, 2016. pp.380-394.

Irwin, K., Mulder, L. and Simpson, B., "The detrimental effects of sanctions on intragroup trust: Comparing punishments and rewards," Social Psychology Quarterly, Vol.77, No.3, 2014, pp.253-272.

Jarvelainen, J., "IT incidents and business impacts: Validating a framework for continuity management in information systems," International Journal of Information Management, Vol.33, 2013, pp.583-590.

Knijnenburg, B.P. and Kobsa, A., "Making decisions about privacy: Information disclosure in context-aware recommender systems," ACM Transactions on Interactive Intelligent Systems, Vol.3, No.3, 2013, pp.20-29.

Lin, C.P., Tsai, Y.H., Chiu, C.K. and Liu, C.P., "Forecasting the purchase intention of IT product: Key roles of trust and environmental consciousness for IT firms," Technological Forecasting and Social Change, Vol.99, 2015, pp.148-155.

Miltgen, C.L. and Smith, H.J., "Exploring information privacy regulation, risks, rrust, and behavior," Information and Management, 2015, pp.1-19.

Vroom. V.H., Work and motivation, John Wiley and Sons, 1964.

Wu, K.W., Huang, S.Y., Yen, D.C. and Popova, I., "The effect of online privacy policy on consumer privacy concern and trust," Computers in Human Behavior, Vol.28, 2012, pp.889-897.

박 정 애 (Park, Jung Ae)

계명대학교에서 석사와 박사학위를 취득하였다. 현재 대구광역시청에서 공무원으로 재직하고 있으며, 주요 관심분야는 클라우드, 사물인터넷 등이다.

손 달 호 (Son, Dal Ho)

경북대학교에서 학사, Texas Tech에서 석사와 박사학위를 취득하였다. 현재 계명대학교 경영정보학과 교수로 재직하고 있으며, 주요 관심분야는 모바일 상거래, 빅데이터, 사물인터넷 등이다.

<Abstract>

Factors Influencing the Provision of Personal Information in Electronic Government Services

Park, Jung Ae · Son, Dal Ho

Frequent outbreak of intrusion of private information is occurring recently not only at portal sites but also in electronic information service of public agencies. Due to these intrusions, it is observed that the citizens tend to avoid providing their private information even to the service for public agencies. Therefore, the object of this research can be explained as demonstrating the influence of the intention of provision for private information to foster the selectronic information ervice of the public agencies. In order to achieve this, this research intends to demonstrate how the experience of the intrusion of the private information affects the concern about the privacy and how the information factor from the public electronic information service has influence on the reliability toward the public. The results showed that the experience of intrusion of privacy, awareness of the danger of privacy, and the sense protection of the information from the manager at public agencies have direct influence on the concern of privacy. Meanwhile, it has been verified that the awareness of information protection of a manager, the systemicity of information protection, and the surveillance and punishment of information protection have influence on the reliability of public agencies.

Keyword: Electronic Government Service, Personal Information, Provision

* 이 논문은 2016년 12월 26일 접수, 2017년 2월 14일 1차 심사, 2017년 3월 10일 게재 확정되었습니다.