JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 19, No. 8, pp. 1515-1525, Aug. 2018

정보보호 투자의도에 영향을 미치는 요인에 대한 연구

이 홍 제[1] · 노 은 희[2] · 한 경 석[3*]
[1]숭실대학교 IT정책경영 박사과정 · [2]한성대학교 IT교육과정 조교수 · [3]숭실대학교 경영학부 교수

A Study on Factors Affecting the Investment Intention of Information Security

Hong-Je Lee[1] · Eun-Hee Roh[2] · Kyeong-Seok Han[3*]

[1]Department of IT Policy Management, Soongsil University, Seoul 06978, Korea
[2]Department of College of Liberal Arts & Sciences, Hansung University, Seoul 02876, Korea
[3]Department of Business Administration, Soongsil University, Seoul 06978, Korea

[요 약]

4차 산업혁명 시대의 보안은 안전의 문제로 확대되고 있으나, 기업의 정보보호 제반환경은 여전히 열악한 수준이다. 본 연구는 정보보호 투자의도 요인을 실증 분석하여 정책적 시사점을 제안 하고자 한다. 이에 정보보호 실태, 보호 행동이론을 고찰하고 UTAUT를 확장하여 연구 모델을 설계하고 가설을 검증하였다. 분석 결과는 정보 자산이 촉진조건에 영향을 미치고, 인지된 우려와 신규 우려가 사회적 영향에 영향을 미치는 것으로 나타났다. 사회적 영향은 경험과 습관에 영향을 미치지만, 정보보호 투자 의도에 미치는 영향은 기각되었다. 촉진조건, 경험 및 습관이 정보보호와 신규서비스 정보보호 투자의도에 가장 높은 영향을 미치는 것으로 나타났다. 하지만, 인지된 우려와 신규 우려가 정보보호 투자의도에 미치는 영향은 낮거나 기각되었다. 업종, 규모, 정보보호 조직 구성, 침해사고 경험, 정보보호 인력 비율, 개인정보 건수에 따라 집단 간 조절 효과가 있었다. 본 연구가 기업의 정보보호 수준 제고를 위한 정책 수립에 도움을 줄 수 있기를 기대한다.

[Abstract]

Security threats in the 4th Industrial Revolution have expanded to the issue of safety, but the environment for information security of domestic companies is still at a low level. This study aims to propose policy implications by empirically analyzing factors affecting investment intention. We investigated the state of information security and protection behavior and expanded UTAUT to investigate correlations. The results showed that information assets affect facilitating conditions, and perceived and new concerns have impacts on social influence. Social influence affect experience and habits, but the impact on security investment intentions was rejected. Facilitation conditions, previous experiences and habits have great influences on investment intention, new service security investment intention. The influence of perceived and new concern are low or rejected. There are moderating effects between types of business, size, security organization, experience of infringement, security personnel ratio, and personal information collection. This study will help to establish policies for enhancing the level of information security.

색인어 : 정보보호, 투자의도, UTAUT, 보호동기이론, 정보보호 실태조사
Key word : Information Security, Intention to Invest, UTAUT, Protection Motivation, Survey on Information Security

http://dx.doi.org/10.9728/dcs.2018.19.8.1515

Received 20 July 2018; **Revised** 20 August 2018
Accepted 28 August 2018

***Corresponding Author;** **Kyeong-Seok Han**

Tel: +82-2-820-0585
E-mail: kshan@ssu.ac.kr

Ⅰ. 서 론

4차 산업혁명 시대의 핵심 기술(IoT, 클라우드, 빅데이타, 모바일)들은 지금과 비교할 수 없는 다양한 행태의 보안 위협이 발생할 것으로 우려된다. 사이버 상의 정보 유출 등의 위협이 현실 세계의 안전(safety)문제로 확대되고, 위협 또한 고도화, 지능화 되어 가고 있어 침해사고 발생 시 커다란 재앙으로 다가 올수 있다. 가트너(Gartner)에서는 오는 2020년까지 전체 보안 위협의 20%가 IoT와 연관된 위협이 될 것으로 전망하고 있다(안랩, 2017). 차량, 홈 가전, 건강 의료 서비스 등과 결합한 IoT 기기의 오작동, 불법 조작, 정보 유출 등의 보안 위협은 기존의 위협과 달리, 대규모의 신체적(생명), 재산적 피해 발생이 우려될 뿐만 아니라, 일부 공격은 이미 현실화되고 있다. 국내 기업들은 모바일, 클라우드, 빅 데이터, IoT 등의 신규 서비스 도입 시 '정보유출'을 가장 큰 위협으로 인식하고 있다.

한국인터넷진흥원(KISA)이 발표한 '2017년 정보보호 실태조사(기업부문)'[18]에 따르면, 국내 기업의 정보보호 제반 환경, 정보보호 예산, 침해사고 예방 등 기업들의 정보보호 대응 환경은 매우 열악한 수준이라고 할 수 있다.

국내 기업의 9.9%만이 정보보호 조직을 운영하고 있으며, 정보보호 담당 인력이 없는 기업은 81.1%나 되었고, 정보보호 인력의 비중이 '1% 미만'이 11%로 가장 많았다[18]. 정보보호 예산을 수립한 기업은 48.1%였으며, IT 예산대비 정보보호 관련 예산의 비중은 '1% 미만'이 36.8%로 가장 높았고, 정보보호 예산 비중이 5% 이상인 기업은 2.2%에 불과한 것으로 조사되었다. 정보보호 책임자(CISO) 임명, 정보보호 교육 시행, 침해사고 대응 협력 채널 등 대응 환경 수준 역시 여전히 낮은 것으로 조사되었다. 국내 기업은 온·오프라인으로 개인정보를 수집·이용하고 있고, 개인정보 침해사고 예방을 위한 기술적 조치를 도입하고 있지만, 여전히 정보보호 예산, 보안 전문인력 확보 및 운용 등의 애로사항이 많다. 대기업과 금융 및 보험업, 정보서비스 업종의 경우, 정보보호 대응 제반 환경, 정보보호 제품과 서비스의 이용률이 높지만, 중소기업, 소상공인과 농림수산업, 제조업, 건설업, 숙박 및 음식점, 개인 서비스 업종 등은 정보보호에 대한 인식 부족과 예산 확보 어려움으로 보안 위협에 충분히 대응하지 못하고 있다.

국내 기업의 2.2%가 지난 1년간 해킹, 악성코드, 랜섬웨어 등의 보안 침해사고를 경험하였으며. 건설업, 제조업, 기술서비스 업종의 침해사고가 높았고, 특히 종업원 250명 이상인 기업의 침해사고 피해 경험 비율이 높게 나타났다[18]. 그럼에도 침해사고 예방을 위한 정보보호 제품과 서비스의 이용률은 전체적으로 낮게 나타나고 있다. 클라우드, 빅 데이터 등 신규 서비스를 이용하거나 이용하려는 기업은 매년 증가하고 있지만, 신규 서비스의 정보보호에 투자하는 사업체는 13.9%에 불과한 것으로 조사 되었다.

국내 기업은 보안 침해 사고가 발생한 후에야 후속 보안 조치로 정보보호에 투자하는 악순환이 반복되고 있어서 4차 산업혁명시대의 기업의 정보보호 수준 향상을 위해서는 정보보호 투자에 대해 적극적이고 선제 대응을 위한 새로운 접근 방법이 필요한 시점이라고 할 수 있다.

본 연구는 국내 기업의 정보보호 실태, 정보보호 행동 관련 연구 고찰을 바탕으로, 기업의 정보보호 투자 의도에 미치는 요인을 분석하여, 정보보호 수준 향상을 위한 정보보호 투자 활성화의 정책적 시사점을 제시하고자 한다.

Ⅱ. 관련 연구

2.1 보호동기 이론 (Protection Motivation Theory)

공포 소구(Fear Appeal)는 권고되는 행동을 따르지 않을 경우 발생하는 좋지 않은 결과를 불안이나 공포를 통해 묘사하여, 수용자들에게 공포 반응을 유발하고, 그들의 태도와 행동을 변화시키려고 한다[25, 26, 33]. 공포 소구는 비듬방지 샴푸, 구강청정제, 보험 같은 상품 광고나 금연, 마약 예방에서 수용자들의 관심을 유도하는 설득 커뮤니케이션 분야에 널리 이용되고 있다.

보호 동기는 위협 평가(threat appraisal)와 대처 평가(coping appraisal)의 인지적(cognitive) 평가를 통해 보호 동기를 일으키고 보호하고자 하는 행동 변화를 가져온다. 위협 평가는 인지된 취약성(perceived vulnerability)과 인지된 심각성 (perceived severity)으로 구성된다[12, 29].

□ 인지된 취약성- 위협에 노출될 가능성에 대한 평가

□ 인지된 심각성- 위협이 성공할 경우 개인에게 미치는 피해의 정도

대처 평가는 손실을 방지하고 위협을 대처하는 능력에 대한 개인의 평가로, 자기 효능감(self efficacy), 인지된 대응 효능감(perceived response effectiveness), 인지된 장애(perceived barriers)로 구성된다[29].

□ 자기 효능감- 위협 대응 행동을 할 수 있는 능력에 대한 개인의 믿음

□ 인지된 대응 효능감- 대응 행동이 위협에 효과적일 것이라고 믿는 정도

□ 장애- 대응 행동을 방해하는 요인(금전적 비용, 시간, 어려움, 부작용 등)

보호 동기는 보안 위협에 대한 위험분석, 위험평가, 보안 위험을 수용 가능한 수준으로 완화하기 위한 보안 대응책(보안제품이용, 보호행동, 정책 등)을 채택하는 정보보호 위험관리와도 관계된다. 그래서 정보보호에 보호동기이론을 이용하여 개인의 정보보호 행동 및 조직의 보안정책 준수행동을 설명하는 연구들을 많이 수행하였다.

표 1. 보호동기를 활용한 정보보호 행동 관련 연구
Table 1. Security Behavior Researches based on PMT

Research (year)	Result
Siponen (2007)	Perceived severity, self-efficacy and response efficacy and sanctions have a significant impact on compliance with information security policies [27]
Gurung (2009)	The perceived severity, self-efficacy, and response efficacy are significantly related to use anti-spyware tools [5]
Johnston (2010)	Fear appeals do impact end user behavioral intentions to comply with recommended individual acts of security. Perception of self-efficacy, response efficacy, threat severity, social influence affect security behavior intent [14].
Ifinedo (2012)	Subjective norms, attitude toward compliance, self-efficacy, and response efficacy and perceived vulnerability positively influence on compliance behavior of information system security policy [10].
Hanus, Wu (2016)	Security awareness significantly affects perceived severity, response efficacy, self-efficacy and response cost. Constructs in coping appraisal process (except response cost) significantly impact recommended security behavior [6].
Park, H.S (2013)	Self-efficacy, response efficacy, and perceived severity are significantly related to privacy awareness, and privacy protection awareness have a positive effect on protection behavior on SNS [23].
Park, C.U (2014)	Perceived vulnerability, severity, self-efficacy, and Privacy rights awareness have a positive impact on privacy behavior. Perceived barriers has a negative impact on privacy behavior[22]
Kim, S.H (2015)	The higher subjective norm, perceived usefulness, technology awareness, self-efficacy, the more intent to use security technology[16]

2.2 기술수용모델(TAM)과 통합 기술 수용 이론 (UTAUT)

IT 기술의 수용에 미치는 요인을 분석하기 위한 기술수용모델(Technology Acceptance Model)은 정보기술 이용 의도로 지각된 유용성(Perceived Usefulness), 지각된 사용 용이성(Perceived Ease of Use)의 개념을 합리적 행동이론의 관점에서 설명하고 있다[3].

□ 지각된 사용 용이성 - 새로운 정보 기술을 사용하는데 필요한 노력에 대해서 개인이 느끼는 정도

□ 지각된 유용성 - 새로운 정보기술을 사용해서 사용자의 직무 성과가 향상할 것이라는 사용자의 주관적인 믿음, 정보기술을 사용하여 업무 성과를 향상할 수 있다고 생각하는 정도

Johnson & Alice M.(2005)는 조직의 정보보호 투자 동기를 설명하기 위해 TAM을 이용한 모델을 제안하였다[13]. 정보보호의 인지된 유용성과 사용 용이성에 영향을 주는 외부 변수로 외부 환경, 이전의 정보보호 경험, 보호하지 않은 IT의 인지된 위험(perceived risks), 정보보호 예산, 정보보호 계획, 정보보호에 대한 확신(confidence), 정보보호 인식 및 교육훈련을 설정하였다. 이러한 외부 변수가 정보보호의 지각된 유용성과 사용 용이성을 매개하여 정보보호 투자에 영향을 준다고 하였다.

통합기술 수용 이론(Unified Theory of Acceptance and Use of Technology)은 사용자의 정보기술 이용 의도와 행동을 설명하기 위해 TAM, MM(motivation model), TPB, MPCU(model of PC utilization), 혁신확산이론 (IDT), SCT(social cognitive theory) 등을 통합하여, 성과기대(Performance expectancy), 노력기대(Effort expectancy), 사회적 영향(Social influence), 촉진조건(Facilitating conditions)으로 구성하였다[28].

□ 성과 기대 - 새로운 IT시스템 사용이 업무 성과를 높이는데 도움을 될 것이라고 믿는 정도

□ 노력 기대 - 새로운 IT시스템 사용이 쉽거나 어려운 정도

□ 사회적 영향 - 다른 중요한 사람들이 새로운 시스템을 사용하는 것이 중요하다고 믿는 정도

□ 촉진조건 - 새로운 정보기술을 사용하기 위한 조직적 자원과 기술적 기반이 갖춰져 있다고 믿는 정도

보호 동기와 UTAUT, 기술 수용모델을 비교해보면 기술수용 모델들은 정보보호 위험(인지된 취약점, 심각성)과 관련된 요소가 없다. 반면에 보호동기 이론은 UTAUT의 사회적 영향이나 촉진조건과 같은 요소를 포함하지 않는다. 많은 기술수용 연구들에서 사회적 영향과 촉진조건이 정보기술의 사용 의도에 긍정적 영향을 미치는 것으로 나타나고 있어, 정보보호 투자 의도에도 그러한 인과 관계가 존재할 것으로 보인다.

표 2. 정보보호 투자 의도 관련 연구 모델 비교
Table 2. Comparison of study models

UTAUT	PMT	Security Investment based on TAM
	Vulnerability, Severity	Perceived Risk
Performance expectancy	Perceived response effectiveness	Perceived Usefulness, Confidence in Information Security
Effort expectancy	Perceived Barriers	Perceived Ease of Use
Social Influence		External Environment, Security Awareness &Training
Facilitating Conditions	Self Efficacy	Security Planning
Experience, Habit		Prior Information Security Experience
Behavioral Intention	Behavioral Intention	Information Security Budget

Ⅲ. 연구모델 및 가설

연구 모델은 관련 연구의 이론적 배경을 기반으로 UTAUT를 확장하여 인지된 위험(Perceived Risk), 성과기대, 사회적 영향, 촉진조건, 이전 정보보호 제품의 이용 경험과 습관(Experience & Habit), 정보보호 투자 의도(Intention to invest),

신규서비스 정보보호 투자 의도(New service security investment intention)로 구성하였다. 또한 기업의 업종, 규모, 정보보호 정책 유무, 조직, 침해사고 경험 여부, 개인정보 보유 건수, 정보보호 인력 비율을 조절변수로 설정하여 집단 간 차이가 있는지에 대해 규명하고자 한다.

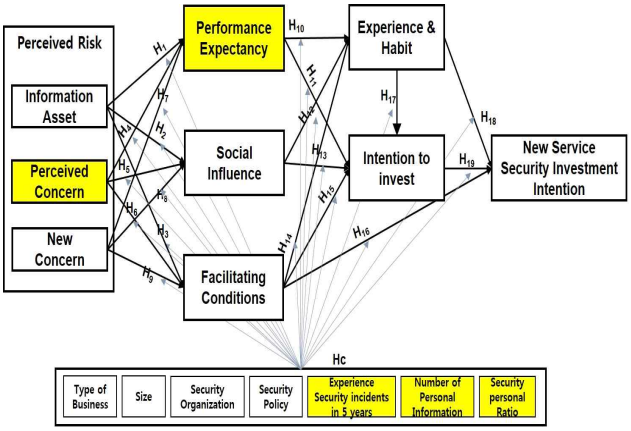

그림 1. 연구 모델
Fig. 1. Research Model

[연구문제 1] 기업의 정보보호 투자 의도에 영향을 주는 요인들은 무엇이며, 어떠한 요인들이 높은 영향을 미치는가? 기업들은 어떤 요인들의 경로(path)를 통해 정보보호 제품과 서비스에 투자하는가?

먼저, 보호 동기의 인지된 취약성과 심각성은 정보보호 행동에 영향을 미치는 것으로 나타나고 있어서, 정보보호 투자 의도에 보호 동기의 위협 평가 요소를 적용하는 것이 필수라고 할 수 있다. Chenoweth(2007) 연구에서 위험에 대한 결정이 위험분석(risk analysis)보다는 일관성이 없는 감정, 신념, 인지에 근거를 두고 있다고 지적하였다[2]. 따라서 본 연구에서는 정보보호 위험관리 표준 ISO/IEC 27005의 위험 구성 요소인 정보 자산, 위협, 취약점에 대해 위협과 취약점을 우려(concern)로 통합하여, 인지된 위험을 정보자산, 인지된 우려, 신규 우려로 정의하였다. 정보 자산은 정보 자산 평가 항목의 동일성과 측정 가능성 등을 고려하고 기밀성, 무결성, 가용성 측면에서 가장 중요한 데이터(개인정보)에 한정하여 조작적 정의(operational definition) 하였다.

정보보호는 위험을 완화하기 위한 활동으로, 보호 동기의 인지된 취약점과 심각성이 개인의 정보보호 행동에 영향을 미치는 것처럼, 조직의 인지된 위험(정보 자산, 인지된 우려, 신규 우려)이 기업의 정보보호 제품과 서비스 사용 의도에 영향을 미치는 것으로 보인다. Wang(2010)은 정보보호 지식과 행동에 관한 연구에서 정보보호 기술의 인지된 유용성과 인지된 사용용이성보다 정보보호 기술을 사용하지 않음으로 발생하는 결과에 대한 인식이 태도와 사용 의도에 더 큰 영향을 미친다고 하였다[31]. 이처럼, 인지된 위험이 높을수록 정보보호 투자 의도는 높을 것이며, 정보보호 투자 의도에 요인이 되는 사회적 영향, 촉진조건, 성과기대도 증가할 것으로 판단하여 다음의 가설을 설정하였다.

H1 : 정보 자산은 성과기대에 정(+)의 영향을 미칠 것이다.
H2 : 정보 자산은 사회적 영향에 정(+)의 영향을 미칠 것이다.
H3 : 정보 자산은 촉진조건에 정(+)의 영향을 미칠 것이다.
H4 : 인지된 우려는 성과기대에 정(+)의 영향을 미칠 것이다.
H5 : 인지된 우려는 사회적 영향에 정(+)의 영향을 미칠 것이다.
H6 : 인지된 우려는 촉진조건에 정(+)의 영향을 미칠 것이다.
H7 : 신규 우려는 성과기대에 정(+)의 영향을 미칠 것이다.
H8 : 신규 우려는 사회적 영향에 정(+)의 영향을 미칠 것이다.
H9 : 신규 우려는 촉진조건에 정(+)의 영향을 미칠 것이다.

보호 동기 이론의 지각된 효율성이 정보보호 제품이나 개인정보 보호 행동에 영향을 미치는 것으로 나타났으며[5, 19], 정재원(2012)의 연구에서도 성과기대가 개인정보보호 기술 수용과 이용에 긍정적 영향을 미치는 것으로 나타났다[15]. 2016년 정보보호 실태조사에 따르면, 정보보호 투자 목적으로 기업 가치 보호 및 제고가 법률 등의 의무사항 이행(22.2%)을 위해 투자하는 사업체에 비교해 14.0%p 높은 것으로 나타났다[17]. UTAUT를 적용한 연구들에서 성과기대는 정보시스템의 사용의도에 가장 영향력이 높은 예측변수 중 하나로 나타나고 있다. 정보보호 제품 또한 정보시스템 일부분으로 인식할 수 있기 때문에, 정보보호에 대한 성과기대(조직의 위험 감소, 규제대응, 기업 가치 보호, 침해사고 신속 대응 등)가 정보보호 투자 의도에 영향을 미칠 것으로 판단하여 다음의 가설을 설정하였다.

H10 : 성과기대는 경험 및 습관에 정(+)의 영향을 미칠 것이다.
H11 : 성과기대는 정보보호 투자 의도에 정(+)의 영향을 미칠 것이다.

국내 기업은 법·규제 대응을 위해 정보보호에 투자하는 경향이 강한 편이다. 2016년 정보보호 실태조사에서도 정보보호 제품 이용률이 높은 금융보험업, 정보서비스업, 대기업(종업원 250명 이상)은 사전 규제에 더 동의하는 반면에, 이용률이 낮은 기업과 중소기업은 사후 규제를 더 동의하고 있었다[17]. 경영진과 직원의 정보보호나 개인정보의 중요성 인식에서도 금융보험업, 정보서비스 업종은 높지만, 이용률이 낮은 기업은 중요성 인식 또한 낮은 편이다. 보호 동기 이론에 기초한 관련 연구에서도 사회적 영향의 요소인 주관적 규범(social norm)이 높을수록 보안 행동은 높게 나타나고 있다[10, 16, 23, 27]. 따라서 경영진과 직원들의 정보보호에 대한 중요성 인식이 정보보호에 중요한 요인으로 판단하여 다음의 연구 가설을 설정하였다.

H12:사회적영향은 경험 및 습관에 정(+)의 영향을 미칠 것이다.
H13:사회적영향은 정보보호 투자 의도에 정(+)의 영향을 미칠 것이다.

보호 동기 이론과 병행과정 확장모델(EPPM)에서 자기 효능감이 높을수록 정보보호 행동은 증가 하였고[10, 16, 23, 27],

UTAUT의 촉진조건은 정보시스템 이용 의도와 이용에 가장 높은 영향을 미치는 요소라고 할 수 있다.

금융보험 업종의 경우, 전자금융 감독 규정에서 정보보호 위원회 운영, IT 인력대비 5% 이상 정보보호 인력 확보, 조직(정보보호 책임자(CISO) 지정, 전담 조직 구성), IT 예산 대비 7% 이상의 정보보호 예산 확보, 정보보호 교육 등을 의무화하고 있다. 대부분의 금융보험 업종은 정보보호 조직적 기반 확보로 인해 정보보호 제품과 서비스 이용률이 타 업종에 비교해 높게 나타나는 것으로 보인다. 따라서 기업의 촉진조건(정보보호 조직, 인력, 교육, 정책 등)이 정보보호 투자 의도에 매우 중요한 요인으로 판단되어 다음과 같은 가설을 설정하였다.

H14: 촉진조건은 경험과 습관에 정(+)의 영향을 미칠 것이다.
H15: 촉진조건은 정보보호 투자 의도에 정(+)의 영향을 미칠 것이다.
H16: 촉진조건은 신규서비스의 정보보호 투자 의도에 정(+)의 영향을 미칠 것이다.

[연구문제 2] 이전의 정보보호 제품의 이용과 주기적 취약점 점검 활동 등은 신규 위험에 대응하기 위한 새로운 정보보호 투자 의도에 어떤 영향을 미치는가?

정보보호는 외부 위협에 대해 일회성으로 정보보호 제품을 설치하는 것으로 끝나는 것이 아니라, 체계적이고 지속해서 이루어져야 하는 프로세스(process) 중심 활동이다. 정보보호 관리는 PDCA(Plan-Do-Check-Act) 기반의 반복적인 활동으로, ISO/IEC 27001이나 정보보호 관리체계 인증은 조직이 체계적이고 지속해서 관리 가능한 정보보호를 하도록 하고 있다.
조직은 위험을 분석하고 위험평가 결과에 따라, 위험 완화를 위한 중·단기 정보보호 이행 계획을 수립하고 이에 따라 정보보호에 대한 투자를 진행한다. 따라서 이전의 정보보호 제품과 서비스의 이용 경험과 주기적인 취약점 점검 등의 습관이 정보보호 투자에 영향을 미칠 것으로 보인다. 이홍제(2018) 연구에서도 경험과 습관은 촉진조건과 함께 정보보호 투자 의도와 신규서비스의 정보보호 투자 의도에 높은 영향을 미치는 요소 중 하나로 나타나고 있다[7,8].

H17 : 경험과 습관은 정보보호 투자 의도에 정(+)의 영향을 미칠 것이다.
H18 : 경험과 습관은 신규서비스의 정보보호 투자 의도에 정(+)의 영향을 미칠 것이다.

[연구문제 3] 업종, 규모, 침해사고 경험, 정보보호 조직, 정보보호 정책 유무, 정보보호 조직 구성 여부, 대량의 개인정보 보유는 정보보호 투자 의도에 집단 간 조절 효과가 있는가?

국내 기업은 업종과 규모에 따라 정보보호 제품/서비스의 이용에 차이가 나타난다. 전체적으로, 금융보험업, 정보서비스업 등은 이용률이 높지만, 농림수산업, 제조업, 건설업, 운수업 등은 낮다. 또한 기업 규모가 클수록 정보보호 제품/서비스의 이용률이 높은 경향이 있고, 중소기업은 정보보호 예산과 인력 부족 등으로 낮은 편이다.

정보보호 조직 구성, 정보보호 정책(계획), 정보보호 인력에 따라 정보보호 투자 의도에 차이가 있을 것으로 보이며, 대량의 개인정보를 보유하고 있는 기업과 개인정보를 거의 수집하지 않는 기업은 정보보호 투자 의도에 차이가 있을 것으로 판단하였다. 정보보호 관리체계 인증 심사 기준(일일 이용자 수가 100만 명 이상)과 개인정보 보호법의 안전성 확보 조치(대기업, 중견기업, 공공기관은 10만 건 이상, 중소기업과 단체는 100만 건 이상 보유하는 경우 '강화' 안전성 확보 조치) 따라 보호 수준이 달라진다. 또한 침해사고를 경험한 기업은 침해 사고 대응 후속 조치로 정보보호 투자(예산)를 증가할 가능성이 높다.

Ⅳ. 실증분석

4.1 표본의 특성

본 연구의 자료는 네트워크에 연결된 컴퓨터를 보유하고 있는 사업체(기관)의 정보보호 업무를 총괄하는 담당자(개인정보보호, 정보보호, 전산, IT 등)를 대상으로 설문조사를 하였다. 설문지는 전체 241부를 회수하였으며, 불성실한 응답자의 설문지 32개를 제외한 209개를 실증분석에 사용하였다.

표 3. 인구통계학적 특성
Table 3. The Demographic Characteristic of Data

Category			%	Category			%
Type of Business	T1*	38	18.1	A	~ 1	77	36.8
	T2*	7	3.3		1~10	29	13.9
	T3*	39	18.6		10~50	16	7.7
	T4*	37	17.7		50~500	17	8.1
	T5*	51	24.4		500~1,000	11	5.3
	T6*	10	4.7		10000~	59	28.2
	T7*	27	12.8	B	No	28	13.4
Size (employee)	1~49	27	12.9		Yes	181	86.6
	50~249	50	23.9	C	No	50	23.9
	250~499	28	13.4		Yes	159	76.1
	500~999	26	12.4	D	No	167	79.9
	1,000~	78	37.3		Yes	42	20.1

* T1 - Agriculture,Forestry and Fisheries/Manufacturing /Construction
T2 - Wholesale/Retail & Accommodation
T3 - Information service industry
T4 - Financial insurance business
T5 - Professional scientific and technical services
T6 - Associations/Business Facility Support
T7 - etc
A: number of personal Information (unit :thousand)
B: Have information security policies
C: Have information security organizations ?
D: Have experience of security incidents in 5 years?

본 연구의 정보보호 투자 의도에 영향을 미치는 요인 변수에 대한 측정 항목은 KISA의 정보보호 실태조사 항목, 관련연구 표2의 정보보호 투자 공통 항목 등을 고려하여 다음과 같이 설정 하였다.

표 4. 측정항목

Table 4. Measurement of the Constructs

Construct	Measure
Asset (AST)	AST1-degree of general personal information
	AST2-degree of sensitive personal information
	AST3-degree of personal information to encrypt
	AST4-purpose of collecting personal information
	AST5-number of collected personal information
Perceived Concern (CON)	CON1-Hacking threat concerns
	CON2-Malicious code threat concerns
	CON3-Information leakage concerns
	CON4-service disruption concerns such as DDoS
	CON5-Latest concerns such as APT, Ransomware
New Concern (NEW)	NEW1-Concerns about mobile security threats
	NEW2-Cloud service security threat concerns
	NEW3-Big data security threat concern
	NEW4-Concerns about IoT security threats
	NEW5-WLAN security threat concerns
Performance Expectation (EXP)	EXP1-Reduce security risk of organization
	EXP2-Effect of legal / regulatory compliance
	EXP3-Protect organization value
	EXP4-Effect of quick response to accidents
	EXP5-Efficient security management
Social Influence (SOC)	SOC1-recognizing importance of information security by management
	SOC2-recognizing importance of personal information by management
	SOC3-recognizing importance of information security by employees
	SOC4-recognize importance of personal information by employees
	SOC5-management leadership level of security
Facilitation Conditions (FAC)	FAC1-information security organization (CISO, CPO)
	FAC2-degree of security policy establishment
	FAC3-degree of information security education
	FAC4-collaborative channel for incident response
	FAC5-percentage of security personnel
USE Experience and Habit (USE)	USE1-Wired network security product utilization ratio
	USE2-data leak prevention product use ratio
	USE3-security management product usage ratio
	USE4-periodic security vulnerability checks
	USE5-Security service utilization ratio
Intention to Invest (INT)	INT1-information security budget ratio
	INT2-degree of increase of security budget
	INT3-budget adequacy of security products
	INT4-budget adequacy of security services
	INT5-degree of ease of security budget
New Service Security Investment Intention (VST)	VST1-WLAN security investment/investment plan
	VST2-Mobile security investment/ investment plan
	VST3-Investing or planning Cloud, Big data, IoT security

4.2 측정 항목의 타당성 및 신뢰도 분석

먼저 SPSS 프로그램의 탐색적 요인 분석(Exploratory Factor Analysis, EFA)을 통해 신뢰도 분석을 하였다. 측정 항목에서 INT2(정보보호 예산 증가 정도), FAC5(정보보호 담당 인력 비율), SOC5(경영진의 정보보호 리더십), CON4(보안 위협 우려 -DDoS 등 서비스 장애), USE1(유선 네트워크 보안 제품 이용), FAC4(침해사고 대응 협력 채널 구축), EXP5(보안관리 효율화)는 제거하는 경우 신뢰도가 더 높게 나타나 삭제하였다.

AMOS 확인적 요인 분석을 통해 집중타당성과 판별타당성을 평가한 결과는 표5, 표6과 같다. 집중타당성 검증 기준은 표준화 계수가 0.5이상, 개념 신뢰도 (Composite Reliability)값이 0.7 이상, 평균분산추출(Average Variance Extracted)값이 0.5 이상이면 측정 도구의 신뢰성이 있는 것으로 볼 수 있다.

표 5. 집중 타당성 분석 결과

Table 5. The result of Convergent Validity

Constructs	Measure	Factor Loading	CR	AVE
AST	AST1	.946	.887	.663
	AST2	.884		
	AST3	.958		
	AST4	.979		
CON	CON2	.936	.898	.644
	CON1	.924		
	CON5	.876		
	CON3	.760		
NEW	NEW3	.900	.864	.635
	NEW4	.876		
	NEW5	.822		
	NEW2	.806		
SOC	SOC3	.861	.902	.697
	SOC1	.908		
	SOC2	.921		
	SOC4	.885		
FAC	FAC1	.953	.882	.714
	FAC2	.972		
	FAC3	.873		
USE	USE2	.880	.875	.637
	USE3	.879		
	USE4	.909		
	USE5	.925		
INT	INT3	.888	.949	.847
	INT2	.987		
	INT4	.985		
	INT5	.929		
VST	VST3	.874	.849	.652
	VST1	.898		
	VST2	.949		

표 6은 각 구성 개념 간의 상관행렬을 나타내는 것으로, 상관계수가 가장 높은 관계는 촉진조건과 경험 및 습관 사이의 관계(.781)이다. 판별타당성을 위해서는, 변수 간의 평균분산추출(AVE) 값이 상관계수의 제곱값 보다 반드시 커야 한다. 각 요인 사이의 AVE 값이 상관계수를 제곱한 값보다 모두 크므로 구성 개념 간에 판별 타당성이 확인되었다고 할 수 있다.

표 6. 판별 타당성 분석 결과
Table 6. The result of discriminant Validity

	AST	CON	NEW	EXP	SOC	FAC	INT	USE	VST
AST	.663								
CON	.262	.644							
NEW	.235	.484	.635						
EXP	.214	.311	.266	.699					
SOC	.177	.292	.314	.409	.697				
FAC	.448	.319	.244	.370	.513	.714			
INT	.353	.238	.260	.190	.335	.577	.847		
USE	.425	.378	.330	.360	.541	.781	.629	.637	
VST	.215	.363	.432	.296	.479	.589	.506	.580	.652

4.3 가설 검증

경로 분석을 통한 연구 가설 검증 결과는 다음의 표7과 같다.

표 7. 가설 검증 결과
Table 7. The Result of Path Analysis

Hypothesized Path		Standardized Estimate	S.E	C.R.	p-value	Result
H1	AST→EXP	.101	.031	1.464	.143	NOT
H2	AST→SOC	.084	.038	1.184	.236	NOT
H3	AST→FAC	.349	.047	5.859	***	Supported
H4	CON→EXP	.160	.068	2.010	.044	Supported
H5	CON→SOC	.169	.083	2.067	.039	Supported
H6	CON→FAC	.120	.100	1.755	.079	NOT
H7	NEW→EXP	.061	.063	.750	.453	NOT
H8	NEW→SOC	.214	.077	2.591	.010	Supported
H9	NEW→FAC	-.019	.094	-.278	.781	NOT
H10	EXP→USE	.044	.082	.822	.411	NOT
H11	EXP→INT	-.059	.090	-.939	.348	NOT
H12	SOC→USE	.180	.082	2.992	.003	Supported
H13	SOC→INT	-.022	.087	-.308	.758	NOT
Ha	SOC→FAC	.426	.092	6.724	***	Supported
Hb	SOC→EXP	.328	.061	4.494	***	Supported
H14	FAC→USE	.676	.056	11.24	***	Supported
H15	FAC→INT	.242	.079	2.545	.011	Supported
H16	FAC→VST	.305	.083	3.050	.002	Supported
H17	USE→INT	.470	.089	4.669	***	Supported
H18	USE→VST	.227	.094	2.136	.033	Supported
H19	INT→VST	.184	.076	2.430	.015	Supported

χ^2=688.141, CMIN/df=1.521, RMSEA=.05 GFI=.837
AGFI=.801,PGFI=.685,CFI=.968,NFI=.913
PNFI=.793,PCFI=.841

*** p-values < 0.01
Not = Not Supported (기각), Supported (채택)

인지된 위험에서 H1:정보 자산→성과기대, H2:정보 자산→사회적 영향, H6:인지된 우려→촉진조건, H7:신규 우려→성과기대, H9:신규 우려→촉진조건 연구 가설이 기각 되었다. 성과기대에서는 H10:성과기대→경험 및 습관, H11:성과기대→정보보호 투자의도 가설이 모두 기각되었다. 사회적 영향은 H13:사회적 영향→정보보호 투자 의도 가설이 기각되었고, 촉진조건, 경험 및 습관, 정보보호 투자 의도의 연구 가설은 모두 채택되었다.

부트스트래핑(bootstrapping)을 이용한 총 효과(직접 효과, 간접 효과)의 분석 결과에서는 촉진조건에 사회적 영향, 정보 자산, 인지된 우려 순서로 높은 영향을 미치는 것으로 나타났다. 경험 및 습관은 촉진조건, 사회적 영향, 정보 자산, 인지된 우려 순으로 높은 영향을 미치는 것으로 나타났다. 정보보호 투자 의도에는 촉진조건, 경험 및 습관이 높은 영향을 미치고 있으며, 사회적 영향과 정보 자산이 영향을 미치는 것으로 나타났다. 신규서비스의 정보보호 투자 의도에는 촉진조건이 가장 높은 영향을 미쳤으며, 다음으로 경험과 습관, 사회적 영향, 정보 자산, 정보보호 투자 의도 순서로 큰 영향을 미치는 것으로 나타났다. 하지만 성과기대가 정보보호 투자의도에 미치는 영향은 모두 기각되었고, 신규 우려는 사회적 영향에만 영향을 미치는 것으로 나타났다.

4.4 조절효과 분석

조절효과 분석은 대응별 모수 비교 (pairwise parameter comparison) 방법을 이용하였는데, 모수의 차이(critical ratio for difference between parameters)가 ±1.96 이상이거나 또는 ±2.58 이상이면 α=0.05, α=0.01에서 유의한 차이가 있다고 할 수 있다.

종업원 수가 250명보다 작은 기업(중소기업)과 250명보다 큰 대기업의 집단 간 모수 차이를 비교하였는데, 대기업은 중소기업보다 사회적 영향이 경험과 습관에 더 큰 영향을 미치고 있으며, 촉진조건이 경험과 습관에 더 큰 영향을 미치는 것으로 나타났다. 중소기업은 가설이 기각되는데, 경영진과 직원의 정보보호 중요성 인식이 높다 하더라도, 정보보호 조직, 인력, 정책, 교육 등의 촉진조건을 동인하지 못함을 실증하고 있다.

표 8. 규모에 따른 조절 효과 분석
Table 8. Moderating Effects of Size

Hypothesized Path	Size				Critical Ratio for Difference
	Small Business (n=77)		Major (n=132)		
SOC→FAC	.191	.108	.469	***	2.266
FAC→USE	.546	***	.741	***	2.472

정보보호 제품/서비스 이용률이 높은 금융보험업, 정보서비스 업종과 나머지 업종의 기업 집단으로 나누어 조절 효과를 분석한 결과 인지된 우려→사회적 영향 가설에서 유의미한(99%

신뢰수준) 차이가 있었고, 나머지 가설에서는 유의한 차이가 없었다. 정보서비스, 금융보험 업종은 인지된 우려(해킹, 악성코드, 정보유출, 시스템 장애 등)가 경영진과 직원의 정보보호 중요성 인식에 영향을 미치지만, 다른 업종의 기업 집단의 경우 기각(p-value=.855)되었다.

최근 5년간 심각한 침해사고를 경험한 기업의 경우 사회적 영향(정보보호 중요성 인식)이 정보보호 제품과 서비스의 이용 경험과 습관(주기적인 보안 점검 및 취약점 점검)에 높은 영향(표준화 계수=.522, p-vale=***)을 미치지만, 침해사고를 경험하지 않은 기업은 기각(p-value=.342)되었다. 침해사고를 경험한 기업은 경영자와 직원의 정보보호 인식이 침해사고 대응 후속 조치로 정보보호 제품과 서비스의 투자와 주기적 취약점 점검을 동인한 것으로 보인다.

공식적인 정보보호 조직 구성 여부나 정보보호 인력비율에 따른 집단 간 차이가 있을 것으로 판단하여 대응별 모수 차이를 비교하였다. 정보보호 조직을 구성한 기업 집단은 사회적 영향이 성과기대와 촉진조건에 미치는 영향이 높게 나타났지만, 정보보호 조직이 없는 기업 집단은 사회적 영향이 성과기대, 촉진조건에 미치는 영향이 모두 기각되었다.

표 9. 정보보호 조직 구성여부에 따른 조절 효과 분석
Table 9. Moderating Effects of security organization

Hypothesized Path	Have security organization ?				Critical Ratio for Difference
	N(n=50)		Y(n=159)		
AST→SOC	.312	.035	-.031	.706	-2.145
SOC→EXP	-.050	.636	.434	***	3.438
SOC→FAC	.020	.911	.617	***	3.231

정보보호 인력 비율에 따른 조절 효과분석에서 IT 인력 대비 정보보호 인력이 5% 이하인 집단은 정보 자산이 촉진조건에 영향을 미치지만, 5% 이상인 집단에서는 기각(p-value=.208)되었다. 사회적 영향이 촉진조건에 미치는 영향에서는 정보보호 인력이 5% 이하인 기업 집단이 5% 이상인 기업보다 더 높은 영향을 미치는 것으로 나타났으며, 촉진조건이 경험 및 습관에 미치는 영향에서는 정보보호 인력이 5% 이상인 기업 집단이 5% 이하인 기업보다 더 높은 영향을 미치는 것으로 나타났다.

표 10. 정보보호 담당 인력 비율에 따른 조절 효과 분석
Table 10. Moderating Effects of security personnel ratio

Hypothesized Path	Have more than 5% security personnel in IT				Critical Ratio for Difference
	No (n=142)		Yes(n=67)		
AST→FAC	.359	***	.140	.208	-3.882
SOC→FAC	.655	***	.436	.001	-2.429
FAC→USE	.555	***	.783	***	2.342
EXP→INT	-.015	.851	-.345	.03	-1.833

정보 자산의 규모(개인정보 보유 건수)에 따른 집단 간 조절 효과 분석이 의미가 있을 것으로 판단하였으며, 기업이 보유한 개인정보 건수가 100만 건 이하인 그룹과 100만 건 이상인 기업 집단으로 나누어 대응별 모수 차이를 비교하였다.

표 11. 개인정보 보유 건수에 따른 조절 효과 분석
Table 11. Moderate Effects of the number of personal information

Hypothesized Path	Have more than one million personal information				Critical Ratio for Difference
	No (n=150)		Yes (n=59)		
AST → FAC	.256	***	.005	.968	-2.403
FAC → USE	.640	***	.410	.002	-2.129
USE → INT	.363	.002	.678	***	2.203
INT → VST	.262	.002	-.097	.499	-2.246

개인정보 보유 건수가 100만 건 이하인 기업 집단에서는 정보 자산이 촉진조건에 영향을 미치고, 정보보호 투자 의도가 신규 서비스의 정보보호 투자 의도에 영향을 미치는 것으로 나타났지만, 100만 건 이상인 집단에서는 모두 기각(p-value=.968, p-value=.499)되었다. 촉진조건이 경험 및 습관에 미치는 영향은 100만 건 이하인 기업 집단에서 더 높게 나타났고, 경험 및 습관이 정보보호 투자 의도에 미치는 영향은 100만 건 이상인 기업 집단에서 더 높게 나타났다.

본 연구의 분석 결과를 요약하면 다음과 같다.

첫째, 정보 자산, 인지된 우려, 신규 서비스의 보안 우려로 구성된 인지된 위험은 경험 및 습관, 사회적 영향, 촉진조건에 긍정적 영향을 미치는 것으로 검증되었다. 인지된 우려는 성과기대, 사회적 영향에 긍정적 영향을 미치며, 신규 우려는 사회적 영향에 영향을 미치는 것으로 나타났다. 사회적 영향은 경험 및 습관, 성과기대, 촉진조건에 긍정적 영향을 미치지만, 정보보호 투자 의도에 미치는 영향은 기각되었다. 촉진조건은 경험 및 습관, 정보보호 투자 의도, 신규서비스의 정보보호 투자 의도에 가장 높은 영향을 미치는 것으로 나타났다.

둘째, 이전의 정보보호 제품 이용 경험과 습관은 정보보호 투자 의도, 신규 서비스의 정보보호 투자 의도에 매우 긍정적 영향을 미치는 것으로 검증되었다. 이는 정보보호 제품 및 서비스의 이용에 대한 피드백(feedback)이 새로운 정보보호 제품과 서비스의 투자를 촉진한다는 것을 의미한다. UTAUT 연구들에서처럼, 정보보호 역시 이전 정보보호 제품과 서비스의 경험이 신규 정보보호 투자의도에 중요한 요인임을 나타내고 있다.

셋째, 총 효과 분석에서 정보 자산, 사회적 영향, 촉진 조건, 경험 및 습관이 정보보호 투자 의도, 신규 서비스의 정보보호 투자 의도에 높은 영향을 미치지만, 인지된 우려와 신규 우려가 미치는 영향은 기각되었다. 정보 자산이 촉진조건에 영향을 미쳐 정보보호에 투자하거나 경험 및 습관을 매개하여 정보보호 제품과 서비스에 투자하는 것으로 나타났다. 또한 인지된 우려, 신규 우려가 사회적 영향에 영향을 미치고, 사회적 영향이 촉진

조건을 거쳐 정보보호에 투자하는 것으로 검증되었다. 그러나 성과 기대가 정보보호 투자 의도에 미치는 영향은 기각되었다.

넷째, 집단 간 조절 효과 분석에서 대기업, 정보보호 조직을 구성한 기업, 금융보험업과 정보서비스 업종, 침해사고를 경험한 기업이 정보보호 투자 의도에 영향을 미치는 요인들의 상관계수가 그렇지 않은 집단보다 높게 나타났다. 정보보호 인력을 5% 이상 보유한 기업은 촉진조건이 경험 및 습관에 미치는 영향이 더 높았으며, 100만 건 이상 대량의 개인정보를 보유한 기업은 이전의 경험 및 습관이 정보보호 투자 의도에 미치는 영향이 더 높게 나타났다.

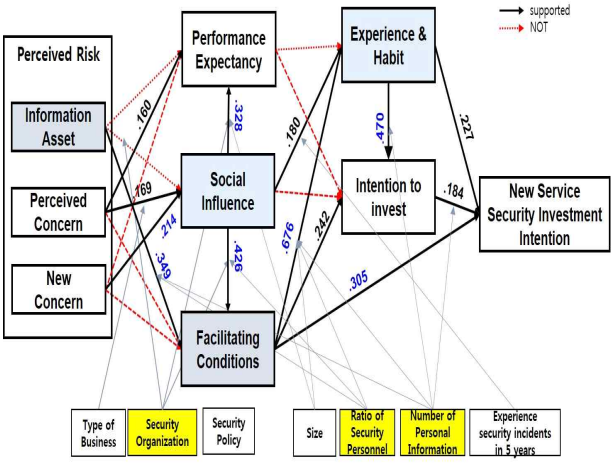

그림 2. 가설 및 조절효과 검증 결과
Fig. 2. Hypothesis and Moderating Effects Result

Ⅴ. 연구결과

본 연구 분석결과는 기업의 정보보호 투자 의도는 외부 요인(인지된 우려, 신규 우려)보다는 내부 요인(정보 자산, 사회적 영향, 촉진조건, 경험 및 습관)이 더 높은 영향을 미치고 있음을 실증하고 있다. 이는 4차 산업혁명 시대의 정보보호는 내부 요인인 정보 자산에 따른 법·규제 강화, 정보보호 조직과 인력, 정보보호에 대한 경영진의 책임, 정보보호 제품 이용 활성화 등의 정책적 변화가 필요함을 의미한다.

첫째, 정보 자산(개인정보 보유 건수, 유형 등)이 해킹, 악성코드, 정보유출 등의 위협보다 정보보호 투자 의도에 더 많은 영향을 미치는 것으로 나타남에 따라, 기업이 보유한 정보 자산(예: 개인정보 보유 건수, 정보 유형 등)의 수준에 따라 정보보호 관련 법·규정을 강화하거나 정보보호 투자를 활성화할 필요가 있다. 빅 데이터 시대에 데이터는 기업의 가장 중요한 정보자산일 뿐만 아니라, 정보 유출시 대규모의 피해 발생이 우려된다. 하지만, 많은 기업이 침해 사고가 없어서 정보보호 예산을 수립하지 않고 있는 것으로 나타나고 있어서 선제적 보안 대응을 위해서는 수집 정보량, 민감 정보 등에 따라 정보보호 기술적 조치를 강화하는 방안이 필요하다.

둘째, 경영진/직원의 정보보호나 개인정보의 중요성 인식이 높을수록, 정보보호 제품과 서비스의 이용은 증가하지만, 정보보호 중요성 인식에 비해 투자 예산의 정도는 낮게 나타나고 있으며, 여전히 정보보호 예산 확보가 정보보호의 가장 어려운 사항으로 나타나고 있다[17,18]. 국내 기업의 경우, 침해사고 발생 시 경영자나 정보보호 책임자의 처벌 수준이 낮은 것이 원인 중 하나라고 파악된다. 사회적 규범(제재)이 정보보호 수준 향상에 긍정적인 영향을 미친다는 관련 연구를 고려해 보면, 경영자나 책임자의 책임과 처벌을 강화하는 방안이 필요하다. 유럽 연합(EU)의 GDPR 규정은 침해사고 시 강력한 제재를 하고 있는데 비해, 국내 개인정보 보호법의 벌칙 조항은 낮아 낮은 수준으로 볼 수 있다. 침해사고를 경험한 기업의 경우 경영진의 정보보호 중요성 인식이 정보보호 제품과 서비스의 이용에 매우 높은 영향을 미치는 것으로 나타나고 있어, 보안사고 시 경영진의 책임 강화가 정보보호 투자에 매우 긍정적 영향을 줄 것으로 보인다.

셋째, 정보보호 수준을 향상하는 가장 효과적인 요인은 촉진조건(정보보호 조직(정보보호 책임자 지정), 정보보호 전문 인력 채용, 정보보호 교육)을 강화하는 것이다. 하지만, 여전히 많은 기업이 낮은 수준의 정보보호 조직과 인력을 구성하고 있어서, 정보보호 수준을 저해하는 가장 큰 요인으로 보인다. GDPR 규정과 국내 개인정보 보호법 모두 개인정보에 대한 책임성 및 거버넌스를 강화하고 있지만, 국내 기업의 실태는 정보보호 책임자가 지정되지 않거나 대부분 겸직하고 있다. 4차 산업 혁명이 가속화될수록, 정보보호 위협은 증가할 것이고, 이에 따라 정보보호 조직과 인력 확보를 위한 제도적 강화가 필요하다. 정보 자산(개인정보 수집 건수, 정보 유형 등)의 수준에 따라 정보보호 책임자 지정, 정보보호 담당 인력 비율 등을 강화하는 방안이 필요할 것이다. 공공기관의 경우, 정부의 정보 분야의 일자리 창출에 맞추어 신규 채용이 필요하며, 정보보호 인력 채용에 어려움을 겪고 있는 중소기업의 경우 보안 인력 채용 활성화 정책(예: 보조금 지급)과 더불어, 정보보호 아웃소싱(보안관제, 정보보호 컨설팅 등) 확대를 통해 부족한 정보보호 조직과 인력의 보완이 필요하다.

넷째, 정보보호 제품/서비스의 이용 경험이 정보보호 예산과 신규 서비스의 정보보호 투자 의도에 높은 영향을 미치는 것으로 나타남에 따라, 국내 정보보호 시장의 확대 및 정보보호 투자 활성화를 위해서는 기업들의 정보보호 제품/서비스 이용을 촉진할 수 있는 정책이 필요하다. 현행 조세특례제한법 제 25조(안전설비 투자 등에 대한 세액공제)에서는 기술 유출 방지 설비 제품 투자 시, 일반 기업의 경우 3%, 중견기업의 경우 5%, 중소기업의 경우 투자금의 10%에 해당하는 금액을 법인세(소득세) 세액 공제를 해주고 있다. 현재 국내 기업의 정보보호 제품 이용률(94.9%)은 매우 높지만, 정보보호 서비스(유지보수, 교육훈련, 보안관제, 보안 컨설팅)의 이용률은 낮다. 정보보호 제품, 서비스 이용 활성화를 위해서는 정보보호 제품 투자 시 세제 감면 혜택의 비율 증가와 더불어, 정보보안 서비스 투자에 대한 세제 감면 혜택 신설이 필요하다.

본 연구에서는 기업의 여러 정보 자산 중에서 개인정보에 한정하였다. 또한, 설문 조사의 시간적, 비용 한계 등으로 다양한 업종과 규모의 표본 집단에 대한 의견이 반영되지는 못하였다. 향후 연구에서는 개인정보 이외에 정보 자산(예: 정보처리 시스템의 수, 기밀 자료 등)을 확대하고 다양한 업종의 기업으로 설문 조사를 확대한 연구가 필요하다고 생각한다.

참고문헌

[1] Anderson, Catherine L., and Ritu Agarwal. "Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions." MIS quarterly 34.3 (2010): 613-643.

[2] Chenoweth, Tim, Robert Minch, and Sharon Tabor, "Expanding views of technology acceptance: seeking factors explaining security control adoption," AMCIS 2007 Proceedings, 2007.

[3] Davis, Fred D., Richard P. Bagozzi, and Paul R. Warshaw. "User acceptance of computer technology: a comparison of two theoretical models." Management science 35.8 (1989): 982-1003.

[4] Fruin, Donna J., Chris Pratt, and Neville Owen, "Protection motivation theory and adolescents' perceptions of exercise," *Journal of Applied Social Psychology*, Vol. 22, No. 1, pp. 55-69, 1992.

[5] Gurung, Anil, Xin Luo, and Qinyu Liao, "Consumer motivations in taking action against spyware: an empirical investigation," *Information Management & Computer Security*, Vol. 17, No. 3, pp. 276-289, 2009.

[6] Hanus, Bartlomiej, and Yu and Wu, "Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective," *Information Systems Management*, Vol. 33, No. 1, pp.2-16, 2016.

[7] Hong Je Lee, Eun Hee Roh and Kyeong Seok Han, "A Study on Factors of Information Security Investment in the Fourth Industrial Revolution," *International Journal of Advanced Science and Technology*, Vol 111, pp.157-174, 2018.

[8] Hong-Je Lee, Eun-Hee Roh, Kyeong-Seok Han, "A Study on the Factors of Experience and Habit on Information Security Behavior of New Services - based on PMT and UTAUT2," *Journal of Digital Contents Society*, Vol 19.1, pp. 93-102, 2018.

[9] Hsu, Chien-Lung, Ming-Ren Lee, and Chien-Hui Su, "The role of privacy protection in healthcare information systems adoption," *Journal of medical systems*, Vol. 37, No. 5, 2013.

[10] Ifinedo, Princely, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Computers & Security*, Vol. 31, No. 1, pp. 83-95, 2012.

[11] Jae Kwon Bae, "An Empirical Study on the Effect of Leakage Threat of Personal Information on Protective Behavior Intention in Big Data Environment: Based on Health Psychology Theory and Protection Motivation Theory," *The e-Business Studies*, Vol. 17, No. 3, pp.191-208

[12] Jee, B. S., Fan, L., Lee, S. C., & Suh, Y. H., "Personal Information Protection Behavior for Information Quality: Health Psychology Theory Perspectives," *Journal of the Korean society for quality management*, Vol. 39, No. 3, pp. 432-443, 2011.

[13] Johnson, Alice M. (2005). The technology acceptance model and the decision to invest in information security. Southern Association of Information Systems Conference, pp. 114-118.

[14] Johnston, Allen C., and Merrill Warkentin, "Fear appeals and information security behaviors: an empirical study," MIS quarterly, pp. 549-566, 2010.

[15] Jung, J. W, Empirical study on acceptance of personal information protection technology in the 'Smart' era, Ph.D. dissertation, Busan University, Busan, 2012.

[16] Kim, Sang-Hoon, and Gab-Su Lee, "An Empirical Study on Influencing Factors of Using Information Security Technology," *Journal of Society for e-Business Studies*, Vol. 20, No. 4, pp. 151-175, 2016.

[17] KISA. 2016 Survey on Information Security Individual. Available:https://isis.kisa.or.kr/board/?pageId=060200.

[18] KISA. 2017 Survey on Information Security Individual. Available:https://isis.kisa.or.kr/board/?pageId=060200.

[19] LaRose, R., Rifon, N., Liu, S., & Lee, D., "Understanding online safety behavior: A multivariate model," The 55th annual conference of the international communication association, New York, 2005.

[20] Maddux, James E., and Melinda A. Stanley, "Self-efficacy theory in contemporary psychology: An overview," *Journal of Social and Clinical psychology*, Vol. 4, No. 3, pp. 249-255, 1986.

[21] Maddux, James E., and Ronald W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *Journal of experimental social psychology*, Vol. 19, No. 5, pp. 469-479, 1983.

[22] Park, Chanouk, 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, Vol. 15, No. 2, pp. 59-71, 2014.

[23] Park, H. S., and S. Kim, "An Empirical Study on SNS Users' Privacy Protection Behaviors," *Management and Economics*, Vol. 46, No. 2, pp. 69-91, 2013.

[24] Posey, Clay, Tom L. Roberts, and Paul Benjamin Lowry. "The impact of organizational commitment on insiders' motivation to protect organizational information assets." *Journal of Management Information Systems* 32.4 (2015): 179-214.

[25] Rogers, Ronald W, "A protection motivation theory of fear appeals and attitude change," *The journal of psychology*, Vol. 91, No. 1, pp. 93-114, 1975.

[26] Rogers, Ronald W, "Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation," Social psychophysiology: A sourcebook, pp. 153-176, 1983.

[27] Siponen, Mikko, Seppo Pahnila, and Adam Mahmood, "Employees' adherence to information security policies: an empirical study, in " IFIP International Information Security Conference, Boston, 2007.

[28] Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D., "User acceptance of information technology: Toward a unified view," MIS quarterly, pp. 425-478, 2003.

[29] Venkatesh, Viswanath, James YL Thong, and Xin Xu, "Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology," *MIS Quarterly,* Vol. 36, No. 1, pp. 157-178, 2012.

[30] Wang, Ping An, "Assessment of cyber security knowledge and behavior: An anti-phishing scenario, in " Proc. IEEE Int. Conf. Internet Monitor. Protection (ICIMP), p. 1-7, 2013.

[31] Wang, Ping An, "Information security knowledge and behavior: An adapted model of technology acceptance," *in 2010 2nd International Conference on Education Technology and Computer*, Vol. 2, pp. 364-367, 2010.

[32] Wang, Ping An, and Easwar Nyshadham, "Knowledge of online security risks and consumer decision making: An experimental study," in 2011 44th Hawaii International Conference on System Sciences, 2011.

[33] Witte, Kim, "Fear control and danger control: A test of the extended parallel process model(EPPM)," *Communications Monographs*, Vol. 61, No. 2, pp. 113-134, 1994.

이홍제 (Hong-Je Lee)

1998년: 고려대학교 대학원(이학 석사)
2015년: 고려대학교 정보보호대학원 박사수료
2017년: 숭실대학교 일반대학원 재학중 정보관리기술사,정보시스템감리사

※관심분야 : 정보보안, 데이터베이스, 빅데이타, HTML5, 디지털 콘텐츠 등

노은희 (Eun-HeeShin Roh)

2001년 : 숙명여자 대학교 대학원 (교육학 석사)
2015년 : 숭실대학교 일반대학원 (공학박사)

2017년～현 재 : 한성대학교 상상력교양교육원 조교수
※관심분야 : HTML5, 하이브리드 앱, 스마트러닝, 디지털 콘텐츠, 정보보안 등

한경석 (Kyeong-Seok Han)

1979년 : 서울대학교 문학사 졸업
1983년 : 서울대학교 경영학과 (경영학 석사)
1989년 : 미국 퍼듀대에서 MIS 박사

1993년～현 재: 숭실대학교 경영학부 교수
※관심분야 : 경영정보시스템,Digital Economy, Agent-Based Simulation, Web Programming,ERP, C++,회계정보시스템, e-Business, 전자상거래, 중소기업 정보화, 기업자금지원. 정책 연구, ERP 등