Research Paper Informatization Policy Vol. 28, No.1 (2021), pp.064-076
https://doi.org/10.22693/NIAIP.2021.28.1.064

개인정보보호 활동 결정요인 연구: 개인정보처리자를 중심으로

장 철 호* · 차 윤 호**

요약 본 연구는 개인정보처리자 관점에서 개인정보보호 활동에 영향을 미치는 요인을 확인하고, 개인정보처리자 스스로 보호 활동을 강화하기 위한 방안을 모색하는데 있다. 요인 탐색을 위해 보호동기이론을 바탕으로 위협평가와 대처평가요인으로 대표되는 주요 요인을 선정하였으며, 요인별 영향분석을 위해 다항로짓모형을 활용하였다. 분석결과, 소규모 개인정보를 보유한 영세 개인정보처리자는 스스로 개인정보 보호 활동을 수행할 수 있도록 보호조치 점검도구 등 시스템 및 기술지원과 인식제고를 위한 교육지원이 필요하다. 그리고 대규모 개인정보를 보유한 개인정보처리자는 예산 및 조세지원 등 개인정보 보호 강화를 위한 투자를 장려하며, 실무 중심의 전문교육 지원이 필요한 것으로 나타났다.

주제어 : 개인정보처리자, 개인정보보호 활동, 다항로짓모형, 위협평가, 대처평가

A Study on the Determinants of Personal Information Protection Activities: With a Focus on Personal Information Managers

Jang, Chul-Ho* · Cha, Yun-Ho**

Abstract The purposes of this study are to identify factors that affect personal information protection activities from the perspective of personal information managers and explore ways of promoting such activities. The main factors examined by threat and response assessments were selected based on the protection motivation theory, and the effects of each factor were analyzed using a multinomial logit model.

The analysis results show that small-scale personal information managers need to be provided with both educational support to enhance their awareness and technical support, such as protection inspection tools, to help them carry out their own personal information protection activities. Personal information managers larger than a certain size also require tax support, including tax cuts, to support their budgets for and investments in personal information protection activities. In addition, they need professional education that emphasizes practice.

Keywords : personal information manager, personal information protection activity, multinomial logit model, threat appraisal, coping appraisal

Received Dec 22, 2020; Revised Jan 19, 2021; Accepted Feb 2, 2021

* First Author, Ph.D in Economics, General Researcher, Personal Data Strategy Team, Korea Internet & Security Agency
** Second Author, Manager, Personal Data Strategy Team, Korea Internet & Security Agency

Ⅰ. 서론

4차 산업 데이터 경제 시대의 도래로 데이터가 모든 산업의 발전과 새로운 가치 창출의 핵심 원천으로 부각되고 있다. 특히 가치 창출과 관련된 데이터 중 대부분을 차지하는 개인정보[1]는 의료, 금융, 마케팅 등 다양한 분야에서 활용되며 그 가치가 높아지고 있다.

최근에는 AI, 클라우드, 빅데이터 등 신기술 기반 서비스의 확대로 지능형 CCTV, AI 스피커와 같은 기기의 센서를 통해 정보주체가 인식하지 못하는 사이 음성, 영상정보 등 다양한 형태의 개인정보가 불법적으로 수집·저장·이용되는 사례가 증가하고 있다. 이에 정보주체[2] 스스로 자신의 개인정보를 보호할 수 있는 자기결정권 행사를 지원하는 제도[3]가 마련되고 있으나, 아직 실효적이지는 못하다. 또한 현행 동의제 하에서 비록 정보주체가 개인정보처리자[4]가 제시하는 개인정보처리방침에 동의하더라도 정보주체는 자신의 정보가 정확히 어떠한 방식으로 처리되고 활용되는지 확인하기는 쉽지 않다. 더욱이 빅데이터 기반 인공지능의 자동화된 개인정보 처리 시스템은 개인정보처리자 역시 이를 확인하지 못하는 경우가 있다.

카드사의 대규모 개인정보 유출사고, 공공기관의 시민 개인정보 노출사고 등과 같이 정보주체의 개인정보 보호활동과 무관하게 개인정보처리자가 개인정보를 수집, 저장, 가공, 유통 등 처리하는 과정에서 관리자 무관심, 부주의 혹은 시스템 설계 오류 및 관리소홀 등으로 인한 대규모 개인정보 유·노출 사고도 지속적으로 발생하고 있다.

이에 사회 전반적으로 개인정보를 안전하게 보호하며 활용하기 위해서는 정보주체의 개인정보 보호활동과 더불어 개인정보처리자 스스로 개인정보를 직접 처리하는 전체 과정에서 보호활동을 수행하는 것이 중요하게 되었다.

그동안 학계에서는 정보주체의 개인정보 보호활동과 관련된 요인연구가 활발하게 진행되었으나, 개인정보처리자의 개인정보 보호활동에 대한 요인연구는 영업 비밀 등의 이유로 자료 수집이 어려워 이에 대한 연구가 거의 이루어지지 못했다.

따라서 본 연구는 개인정보처리자가 개인정보 보호활동을 수행하도록 하는 결정요인을 분석하고, 개인정보처리자의 보호활동을 활성화하기 위한 정책적 방안을 모색하고자 한다. 이를 위해 Rogers(1975)의 보호동기이론(Protection Motivation Theory)을 기반으로 개인정보처리자의 보호활동에 관한 가설을 설계하고, 공공 및 민간 개인정보처리자를 대상으로 하는 한국인터넷진흥원의 2019년 개인정보보호 실태조사를 2차 자료(Secondary Data)로 활용하여 가설을 실증적으로 검증하였다.

연구순서는 다음과 같다. 제 Ⅱ장에서는 본 연구의 이론적 배경인 보호동기이론에 대해 간략하게 정리하고, 선행연구를 검토하였다. 제 Ⅲ장에서는 보호동기이론을 기반으로 연구모형을 설계하고, 제 Ⅳ장에서 실제 데이터를 활용하여 실증 검증하였다. 마지막으로 제 Ⅴ장에서 결론을 제시하였다.

Ⅱ. 이론적 배경 및 선행연구

Rogers(1975)에 의해 처음 소개된 보호동기이론은 개인이 건강의 위험 신호에 반응하여 어떠한 변화와 행동하는지 설명하기 위해 고안되었다. 이후 개인이 인식

1) 개인정보는 살아있는 개인에 관한 정보로 성명, 주민등록번호 및 영상 등을 통해 개인을 식별할 수 있는 정보를 말하며, 해당 정보만으로 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있으면 개인정보에 포함된다.

2) 정보주체는 처리되는 정보에 의해 알아볼 수 있는 사람으로 그 정보의 주체가 되는 사람을 말한다.

3) 정보주체의 개인정보 자기결정권 행사 지원을 위해 개인정보침해 신고센터, 개인정보 분쟁조정, e프라이버시 클린서비스, 개인정보보호 포털 등 개인정보 피해구제 및 권익보호 서비스가 운영되고 있으며, 개인정보 보호에 대한 인식제고를 위해 국민 참여 캠페인 및 취약·소외계층을 위한 맞춤형 교육 등이 실시되고 있다.

4) 개인정보처리자는 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인을 말한다.

한 정보와 기대가치를 바탕으로 특정 신호를 두려움 또는 공포로 인식하고 행동을 변화시키는 과정을 설명하는 일반 이론으로 발전하였으며, 심리학, 교육학 등 다양한 분야에서 보호행동 연구에 활용되었다.

보호동기이론은 개인이 특정 메시지 또는 신호에 노출된 경우 이를 심각하거나 위협적인 상황으로 인식하였다면 이를 회피하기 위한 행동으로 연결된다는 것을 전제하고 있다. 하지만 행동의 변화는 단순히 메시지에 대한 노출 자체가 아니라 인지적 매개과정을 통해 일어난다. 즉, 개인이 메시지 또는 신호를 위협적인 상황으로 인식해야 하며, 이러한 인식을 위해서는 자신에 대한 위협적인 요인과 이에 대한 대처 방안을 평가하고 보호행동을 결정한다는 것이다. 위협적인 요인을 평가하는 위협평가(Threat Appraisal) 요인과 대처방안을 평가하는 대처평가(Coping Appraisal) 요인은 일반적으로 다음 〈표 1〉과 같다.

위협평가 요인은 특정 신호가 향후 사건으로 확대될 가능성을 나타내는 인지된 취약점(Perceived Vulnerability)과 실제 사건으로 연결되었을 때 발생하는 피해의 정도를 나타내는 인지된 심각성(Perceived Severity)으로 구성된다. 대처평가 요인은 위협적인 사건이 발생했을 경우 대처할 수 있는 개인의 능력을 나타내는 자기 효능감(Self Efficacy)과 자신의 대처 능력에 대한 신뢰를 나타내는 반응효능감(Response Efficacy), 그리고 대처행동을 수행할 때 소요되는 시간, 금전, 노력 등 기회비용을 나타내는 대처 비용(Response Cost)으로 구성된다.

이러한 보호동기이론이 개인정보보호 분야까지 응용되어 정보주체가 인식하는 특정 요인이 개인정보보호 활동에 미치는 영향을 연구하는데 활용되고 있다. 보호동기이론을 기반으로 한 개인정보보호 분야 초창기 연구에서는 정보주체의 개인정보 유·노출에 대한 위험 인식이 보호 활동에 미치는 영향이 주로 연구되었다. Kim and Kim(2013)는 프라이버시 침해 위험이 개인의 개인정보보호 활동에 주요한 요인으로 분석하였으며, Kim and Park(2013)는 SNS 서비스 이용 시 자기효능감과 반응효능감, 그리고 침해심각성이 보호 활동의 주요 요인으로 분석하였다. 또한 Park and Lee(2014)는 지각된 취약성, 심각성, 자기효능감 그리고 지각된 장애가 보호 활동에 영향을 미치는 요인으로 분석되었다. Kim, et al.(2016)는 SNS 서비스 이용자의 자기효능감과 대응성이 보호 활동에 영향을 미치는 것으로 분석되었다. 그리고 Bae(2016)은 위협심각성, 위협 발생가능성, 반응효능감, 자기효능감, 주관적 규범이 보호 활동에 영향을 미치는 것으로 분석하였다.

최근 연구에서는 정보주체를 세분화하여 특정 계층을 대상으로 개인정보보호 활동에 영향을 미치는 요인을 분석하거나 연구대상을 정보주체에서 개인정보처리자로 확대한 연구가 진행되고 있다. Park(2019)는 보호동기이론을 기반으로 청소년의 보안인식이 개인정보보호 활동에 미치는 영향을 연구하였으며, 청소년의 주관적 규범과 보안 태도가 보호 활동에 중요 요인으로 분석하였으며, Tian, et al. (2020)는 한국 중·노년층의 경우 지각된 취약성, 지각된 심각성 그리고 교육경험이 보호

〈표 1〉 평가 요인
〈Table 1〉 Appraisal factors

Factors	Threat appraisal	perceived vulnerability
		perceived severity
	Coping appraisal	self efficacy
		response efficacy
		response cost

활동의 동기로 분석하였다.

그리고 개인정보처리자를 대상으로 한 연구는 Lee, et al. (2016)는 개인정보처리자 중 공공기관 담당자를 대상으로 개인정보정책에 대한 태도, 규범적 신념, 자기효능감, 지각된 염려수준, 대처효능감이 개인정보 보호에 주요 요인으로 분석하였다. Kim and Lee(2011)는 개인정보처리자 중 민간기업 담당자를 대상으로 개인정보보호가 아닌 정보보호 정책 준수 의도에 미치는 영향을 분석하였으며, 정보보안 정책에 대한 태도와 기회비용, 정책 미준수에 대한 비용, 대처효능감이 정보보호 정책 준수에 영향을 주는 것으로 검증하였으며, Lee, et al.(2018)는 민간기업의 정보보호에 대한 투자의지를 분석하여 정보 자산, 인지된 우려, 인지된 위험 등이 투자의지에 영향을 주는 것으로 검증되었다.

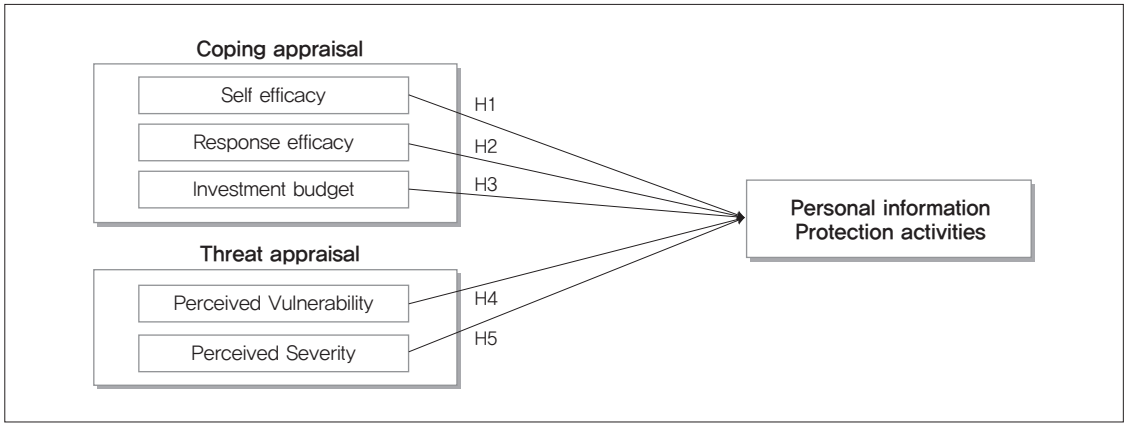
개인정보보호 분야에서 보호동기이론을 적용한 기존 선행연구는 대부분 정보주체를 대상으로 진행되어, 본 연구에서는 개인정보처리자의 보호 활동 연구에도 보호동기이론이 일반적으로 적용될 수 있는지 여부를 우선적으로 확인하고자 하였다. 또한 비록 본 연구와 동일하게 개인정보처리자를 대상으로 한 선행연구에서도 자료 수집 등의 어려움으로 인해 소수 표본을 대상으로 연구가 진행되었다. 하지만 본 연구는 개인정보보호 실태조사 자료를 활용함으로써 중앙행정기관 및 지자체, 공공기관 전체, 전국 초·중·고 및 대학교 일부를 포함한 공공부문 1,500개 표본 자료와 전국 17개 시·도 54만 사업체 중 종사자 규모와 업종을 고려하여 선정된 민간 2,000개 표본 자료를 활용하여 소수의 법칙에 따른 대표성 오류를 최소화하고자 하였다.

Ⅲ. 연구 설계

1. 연구모형

본 연구는 국내 공공 및 민간 개인정보처리자의 개인정보보호 활동에 영향을 주는 요인을 실증 분석하였다. 특히 개인정보보호 활동 연구의 대부분을 차지하는 정보주체에 관한 선행연구와 같이 개인정보처리자의 연구에 있어서도 보호동기이론이 적용가능한지 확인하기 위해 Rogers(1975)의 연구를 기본 이론적 틀로 적용하였다.

개인정보처리자의 개인정보보호 활동에 미치는 요인으로 대처평가 요인인 자기효능감, 반능효능감, 투자예산과 위협평가 요인인 침해취약성, 침해심각성을 독립변수로 다음 〈그림 1〉과 같이 연구모형을 설정하였다.



〈그림 1〉 연구모형
〈Fig. 1〉 Research model

2. 연구가설

1) 자기효능감

Bandura, et al.(1977, 2001)은 자기효능감을 특정 목표를 달성하기 위해 필요한 행동을 조직하고 이를 수행할 수 있는 판단과 신념으로 정의하였으며, Kline(2007), Bulgurcu, et al.(2010)은 상황에 대처할 수 있는 대응 능력과 관계가 있다고 정의하였다. 개인정보처리자의 자기효능감은 개인정보를 안전하게 보호하기 위해 갖추고 있는 개인정보 침해사고에 대한 대처 능력으로 정의하고 가설을 설정하였다. 개인정보처리자의 자기효능감을 측정하기 위해 개인정보보호 책임자 지정 유무[5], 개인정보보호 전담부서 인력 수[6], 담당자의 업무경력[7]을 활용하였다.

가설 1 : 자기효능감은 개인정보보호 활동에 긍정적인 영향을 미칠 것이다.

가설 1-1 : 개인정보보호 책임자가 지정되어 있으면 개인정보 보호 활동에 긍정적인 영향을 미칠 것이다.

가설 1-2 : 개인정보보호 전담부서 인력 수는 개인정보 보호 활동에 긍정적인 영향을 미칠 것이다.

가설 1-3 : 개인정보 담당자의 업무경력은 개인정보보호 활동에 긍정적인 영향을 미칠 것이다.

2) 반응효능감

Workman, et al.(2009), Johnston, et al.(2010)은 반응효능감을 위험에 대응할 수 있는 권고된 활동이 효과적일 것이라는 믿음으로 정의하였으며, 개인정보처리자의 반응효능감은 개인정보처리자의 개인정보보호 활동이 개인정보 침해사고를 예방할 수 있을 것이라는 믿음으로 정의하고 가설을 설정하였다. 개인정보처리자의 반응효능감을 측정하기 위해 담당자의 개인정보 보호에 대한 중요도 인식 정도[8]를 활용하였다.

가설 2 : 반응효능감은 개인정보 보호활동에 긍정적인 영향을 미칠 것이다.

가설 2-1 : 담당자의 개인정보보호에 대한 중요도 인식은 개인정보 보호활동에 긍정적인 영향을 미칠 것이다.

3) 투자예산

투자예산은 개인정보처리자가 위협에 대처하기 위한 활동에 소요되는 예산으로 정의하고 가설을 설정하였다. Rogers(1975)는 위기에 대응하기 위한 기회비용으로 위협 대처비용으로 정의하였으나, 자료 수집 등의 현실적 한계로 인해 대처비용이 아닌 투자예산으로 변수를 변경하였다. 투자예산은 각 기관의 개인정보보호 예산[9]으로 측정하였다.

가설 3 : 투자예산은 개인정보보호 활동에 긍정적인 영향을 미칠 것이다.

가설 3-1 : 개인정보보호 예산규모는 개인정보보호 활동에 긍정적인 영향을 미칠 것이다.

4) 침해취약성

Rogers(1975), Youn(2009), Ifinedo(2012)는 침해취약성은 인지된 위협에 대한 평가로 개인정보처리자의 침해취약성은 개인정보가 노출될 위험과 노출 가능성에 대한 인지정도로 정의하고 가설을 설정하였다. 이

5) "귀 기관은 개인정보보호 책임자가 있습니까?" ① 예 ② 아니요

6) "귀 기관은 개인정보보호담당자(책임자 제외)는 몇 명이며, 전담으로 업무를 수행합니까?" 현 인원 수 ( )명, 전담여부 전담 ( )명, 타 업무 병행 ( )명

7) "귀 기관의 개인정보보호 업무 경력은 얼마나 되었습니까?" ① 1년 미만 ② 1년~2년 미만 ③ 2년~3년 미만 ④ 3년~5년 미만 ⑤ 5년 이상

8) "귀 기관은 고객 등의 개인정보보호를 얼마나 중요하게 생각하고 있습니까?" ① 전혀 중요하지 않다 ② 중요하지 않다 ③ 보통이다 ④ 중요하다 ⑤ 매우 중요하다

9) "귀 기관의 2019년 개인정보보호 예산은 어느 정도 입니까?" ① 10만원 미만 ② 10만원~100만원 미만 ③ 100만원~1,000만원 미만 ④ 1,000만원~1억원 미만 ⑤ 1억원 이상

는 외부의 위험에 노출될 가능성이 얼마나 있는가에 대한 것으로 우연한 노출, 내부자에 의한 개인정보 유·노출, 해킹 등 통제되지 않는 침해 등으로 개인정보가 노출될 수 있다. 이러한 침해사고의 위험을 높게 인지하는 개인정보처리자는 자발적으로 개인정보 보호행동을 수행할 가능성이 높다. 침해취약성은 기관별 고유식별정보 보유 규모[10]와 개인정보 유출에 대비하기 위한 노력[11]으로 측정하였다.

가설 4 : 침해취약성은 개인정보보호 활동에 긍정적인 영향을 미칠 것이다.

가설 4-1 : 고유식별정보 보유 규모는 개인정보보호 활동에 긍정적인 영향을 미칠 것이다.

가설 4-2 : 개인정보 유출에 대비하기 위한 노력은 개인정보 보호 활동에 긍정적인 영향을 미칠 것이다.

5) 침해심각성

Rogers(1975)는 침해심각성을 위협 발생되는 피해의 정도로 정의하였으며, Grrung, et al.(2009)은 개인정보 침해로 인한 발생하는 부정적 결과에 대한 인지로 정의하였다. 또한 Kim and Lee(2011)와 Lee, et al.(2016)은 침해심각성을 보호정책 미준수 시 발생할 수 있는 비용으로 정의하였다. 선행연구를 참고하여 본 연구에서도 침해심각성을 개인정보 침해사고에 따른 부정적 인지로 정의하고 가설을 설정하였다. 침해에 대한 심각성을 높게 인지할수록 개인정보를 보호하려는 동기요인으로 작용될 수 있으며, 위협적인 상황에 대처하기 위한 활동을 수행하려는 의지가 강해질 것으로 예상된다. 침해심각성은 개인정보 침해사고 발생 기관과 해당 책임자에 대한 처벌 및 손해배상 강도 인식[12]으로 측정하였다.

〈표 2〉 변수 및 측정항목
〈Table 2〉 List of the variables and its measurement items

variables		Measurement items
DV	personal information protection activities	number of implementation measures for personal information protection
IV	self efficacy	whether or not a person in charge of privacy is designated, number of dedicated personnel, employee experience
	response efficacy	degree of importance recognition about personal information protection
	investment budget	budget size for personal information protection
	perceived vulnerability	amount of unique identifying information holdings, number of efforts to prepare for leakage
	perceived severity	degree of recognition about punishment and damages to the leaked company and the person in charge

10) "귀 기관은 몇 명의 고유식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호)를 보유하고 있습니까?" ① 1천명 미만 ② 1천명 이상~1만명 미만 ③ 1만명 이상~5만명 미만 ④ 5만명 이상~10만명 미만 ⑤ 10만명 이상~50만명 미만 ⑥ 50만명 이상~100만명 미만 ⑦ 100만명 이상

11) "귀 기관은 개인정보 유출에 대비하여 어떤 대응 노력을 하고 있습니까?" ① 유출사고 대응 계획 수립 ② 배상 책임 보험 가입 ③ (피해 보상 등을 위한) 준비금 등 재원마련 ④ 전문가 채용 등 인력 체계 마련 ⑤ ISMS-P 등 인증 취득 ⑥ 기타 ⑦ 별도의 대응방안 없음

12) "귀 기관은 개인정보 유출사고 발생 시 개인정보 유출업체(기관), 책임자 등에 대한 현재의 처벌 및 손해배상 강도가 어떻다고 생각하십니까?" ① 매우 부족하다 ② 부족하다 ③ 적당하다 ④ 과하다 ⑤ 매우 과하다

가설 5 : 침해심각성은 개인정보보호 활동에 긍정적인 영향을 미친 것이다.

가설 5-1 : 개인정보 침해사고 발생 기관과 해당 책임자에 대한 처벌 및 손해배상 강도 인식은 개인정보보호 활동에 긍정적인 영향을 미칠 것이다.

6) 개인정보보호 활동

개인정보보호 활동은 개인정보처리자가 개인정보를 안전하게 관리하기 위해 수행하고 있는 보호조치로 정의하였다. 각 기관마다 수행하고 있는 보호조치를 객관적 기준으로 산정하기 위해「개인정보보호법」과 「개인정보의 안전성 확보조치 기준」에서 필수적으로 조치하여야 하는 최소한의 보호조치인 내부 관리계획의 수립·시행, 접근 권한의 관리 및 통제, 개인정보 암호화 등 총 8개의 카테고리로 나누어 범주형으로 측정하였다.

또한 본 연구에서는 개인정보처리자가 현재 수행 중인 보호조치는 처리자에게 개인정보보호를 위한 파레토 최적(Pareto optimality)인 상태로 가정하였다. 따라서 개인정보처리자는 현재 상황에서 가용가능한 자원을 가장 효율적으로 배분하여 각 카테고리별 보호조치를 수행하며, 그 보호조치 수를 개인정보보호 활동의 수준 또는 정도로 측정하였다.

3. 자료수집

본 연구는 「2019 개인정보보호 실태조사」의 공공·민간 총 3,500개 개인정보처리자 데이터를 활용하여 실증분석하였다. 개인정보보호 실태조사는 한국인터넷진흥원에서 국내 개인정보보호 수준 및 조치현황, 담당자의 인식과 정책적 요구사항 등을 조사하기 위해 공공 1,500개 기관과 전국 17개 시·도 종사자 수 5인 이상, 개인정보 1,000개 이상 보유 사업체 중 임의추출(Random Sampling) 방식으로 선정된 민간 2,000개 기업을 대상으로 매년 조사되고 있다. 본 연구의 각 변수 측정항목에 대한 설문 역시 실태조사 항목을 활용하였다.[13)]

4. 분석방법

본 연구와 같이 종속변수가 범주형(Categorical) 또는 이산적(Discrete) 특성을 가질 경우 다항로짓모형을 이용하는 것이 바람직하다.(Wooldrigde, 2010) 다항로짓모형을 살펴보면, 확률효용(Random Utility)이론을 기초로 개인정보처리자 n이 개인정보보호 활동 m으로부터 얻는 개인정보보호 활동의 정도 $U_{n,m}$를 식(1)과 같이 나타낼 수 있다.

$$U_{n,m} = V_{n,m} + \epsilon_{n,m} \quad (1)$$
$$= \beta_1 X_{n,1} + \beta_2 X_{n,2} + \cdots + \beta_m X_{n,m} + \epsilon_{n,m}$$

식(1)에서 $V_{n,m}$은 관측된 독립변수의 속성 및 속성수준에 의해 설명되는 효용의 결정부분(Deterministic Part)을 의미하며, $\epsilon_{n,m}$는 결정부분에 의해 설명되지 못한 부분이나 관측되지 않은 요소들에 의한 오차항(Error Term)을 의미한다. 즉, $V_{n,m}$은 기관의 개인정보보호 활동에 대한 자기효능감, 반응효능감, 투자예산, 침해취약성, 침해심각성으로 설명 가능한 부분을 의미한다. 또한 β는 개인정보처리자 n의 관측된 독립변수 X_n이 효용에 미치는 영향을 반영하는 추정계수이다. 통계적으로 유의한 양(+)의 β값은 각 요인으로 인해 보호활동을 증가시킬 가능성이 높으며 음(-)의 β값은 그 역에 해당하며, 유의하지 않는 값은 개인정보보호 활동에 영향을 미치지 않는 것으로 해석할 수 있다.

다항로짓모형에서 오차항 $\epsilon_{n,m,t}$는 I.I.D(Independent, Identically, Distributed) Ⅰ형 극한값분포(type Ⅰ Extreme Value Distribution)를 따른다고 가정하며, 개인정보처리자 n이 i를 선택할 확률은 다음 식(2)와 같다.

13) 본 연구의 설문지는 한국지능정보사회진흥원 대표 홈페이지에서 확인할 수 있다. (http://www.nia.or.kr/site/nia_kor/ex/bbs/List.do?cbldx=65684)

$$\Pr(U_{n,i}=i|X_i)=\frac{\exp(\beta_i X_{n,i})}{1+\sum_{m}^{M}\exp(\beta_m X_{n,m})} \quad (2)$$

식(2)와 같이 각 처리자의 개인정보보호 활동에 대해 정의된 선택확률을 활용하여 전체 연구대상 N개, 처리자에 의해 선택된 보호활동인 I번, 보호활동 전체 범주 M개일 경우를 로그우도함수(Loglikelihood Function)로 표현하면 다음 식(3)과 같다.

$$LL(\beta)=\sum_{n=1}^{N}\sum_{i=1}^{I}\sum_{m}^{M}\ln P_{n,i,m} \quad (3)$$

최종적으로 최우추정법(Maximum Likelihood)을 활용하여 식(3)의 로그우도함수 값을 극대화하는 계수 β를 도출하였다.

Ⅳ. 분석결과

본 연구는 개인정보처리자를 「개인정보의 안전성 확보조치 기준」 제3조[14]에 따라 세 그룹을 분류하여 분석하였다. 해당 법령은 개인정보처리자를 기관의 유형(공공기관, 민간기업), 규모 기준(대기업, 중견기업, 소상공인)과 개인정보 보유량(1만 명, 10만 명, 100만 명)에 따라 국내 개인정보처리자를 세 그룹으로 분류하여 각기 다른 수준의 개인정보보호 의무를 부여하고 있다. 아직까지 개인정보처리자의 보호 활동은 기관의 자율적 수행보다 관련법에 의해 강제 의무적으로 수행하는 경우가 많아, 그룹을 분류하지 않고 분석할 경우 통계적 편의가 발생할 가능성이 높다. 따라서 본 연구의 분석대상 3,500개 개인정보처리자를 이 기준에 따라 그룹 Ⅰ 86개 사업자, 그룹Ⅱ 2,647개 사업자, 그룹 Ⅲ 767개 사업자로 분류 후 각 그룹별로 분석을 진행하였다.

각 유형별 개인정보처리자의 개인정보보호 활동에 미치는 요인을 분석한 결과는 다음 〈표 3〉과 같다.

먼저 그룹 Ⅰ의 분석결과, 모형의 적합성을 나타내는 분산분석 F값은 13.508($p<0.001$)로 유의하게 나타났으며 모형의 설명력을 나타내는 R^2값은 0.853으로 설명력이 높은 것으로 나타났다. 독립변수 중 책임자 지정유무와 전담인력 수 그리고 중요도 인식, 투자예산, 처벌 및 배상에 대한 강도 인식은 신뢰수준 99%에서 유의한 것으로 분석되었다. 특히 상대적 중요도는 자기효능감 중 전담 인력 수 변수가 0.615로 가장 높은 중요도를 차지하였으며, 다음으로 반응효능감인 개인정보보호에 대한 중요도 인식이 0.154로 중요한 변수로 분석되었다.

따라서 1만 명 미만의 개인정보를 보유한 소상공인, 단체, 개인이 속한 그룹 Ⅰ의 개인정보보호 활동에는 자기효능감, 반응효능감, 투입예산, 침해심각성이 주요 동기요인으로 작용함을 확인할 수 있다. 특히 동기요인 중 전담 인력 수와 개인정보보호에 대한 중요도 인식이 상대적으로 중요한 요인으로 분석되었다.

다음으로 그룹 Ⅱ의 분석결과, 분산분석 F값은 83.982 ($p<0.000$)로 유의하게 나타났으며 R^2값 역시 0.746으로 설명력이 높은 것으로 나타났다. 그룹 Ⅱ

14) 개인정보의 안정성 확보조치 기준(개인정보보호위원회 고시) 제3조

구분	분류 기준
그룹 Ⅰ	- 1만 명 미만의 개인정보를 보유한 소상공인, 단체, 개인
그룹 Ⅱ	- 100만 명 미만의 개인정보를 보유한 중소기업 - 10만 명 미만의 개인정보를 보유한 대기업, 중견기업, 공공기관 - 1만 명 이상의 개인정보를 보유한 소상공인, 단체, 개인
그룹 Ⅲ	- 10만 명 이상의 개인정보를 보유한 대기업, 중견기업, 공공기관 - 100만 명 이상의 개인정보를 보유한 중소기업, 단체

〈표 3〉 분석결과
〈Table 3〉 Result of anlysis

variable	group Ⅰ		group Ⅱ		group Ⅲ	
	β	importance	β	importance	β	importance
whether or not a person in charge of privacy is designated	1.085**	0.025	0.450**	0.320	0.267**	0.123
number of dedicated personnel	1.145**	0.615	0.082**	0.043	-0.046	0.009
employee experience	0.207	0.035	0.298**	0.057	0.444**	0.527
degree of importance recognition	0.239**	0.154	0.251**	0.238	0.100**	0.067
budget size	-0.199**	0.088	0.260**	0.285	0.181**	0.170
number of unique identifying information holdings	-0.083	0.027	0.079**	0.016	-0.092**	0.044
number of efforts to prepare for leakage	-0.060	0.008	0.014	0.003	0.069**	0.018
degree of recognition about punishment and damages	0.174**	0.048	0.086**	0.038	0.086**	0.042
R^2	0.853		0.746		0.783	
F	13.508**		83.982**		25.895**	

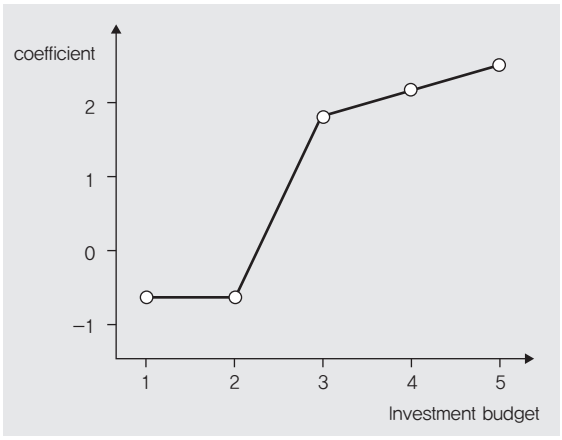
**p〈0.01, *p〈0.05

는 유출대비 노력을 제외나 나머지 변수 모두 신뢰수준 99%에서 유의한 것으로 분석되었다. 상대적 중요도는 자기효능감 중 책임자 지정 유무가 0.320으로 가장 높게 나타났으며, 투자예산 0.285, 개인정보보호에 대한 중요도 인식 0.238 순으로 분석되었다.

1만 명 이상 개인정보를 보유한 소상공인, 단체, 개인과 10만 명 미만 개인정보를 보유한 대기업, 중견기업, 공공기관, 그리고 100만 명 미만의 개인정보를 보유한 중소기업이 속한 그룹 Ⅱ는 자기효능감, 반응효능감, 투자예산, 침해취약성, 침해심각성 모두 개인정보보호 활동에 주요 동기요인으로 분석되었으며, 동기요인 중 기관 내 개인정보보호 책임자[15] 지정과 일정 규모의 개인정보보호 예산 책정, 담당자의 개인정보보호에 대한 중요도 인식이 상대적으로 중요한 요인으로 분석되었다.

특히 예산 책정 규모에 따른 개인정보보호 활동에 미치는 영향을 추가적으로 분석한 결과는 〈그림 2〉와 같다. 예산 규모 2(10만 원 이상~100만 원 미만)보다 3(100만 원 이상~1,000만 원 미만)에서 급격한 증가 추세를 확인할 수 있어 그룹 Ⅱ의 경우 개인정보보호 활동을 위한 예산은 최소 1,000만 원 이상 규모로 책정하는 것이 바람직할 것으로 판단된다.

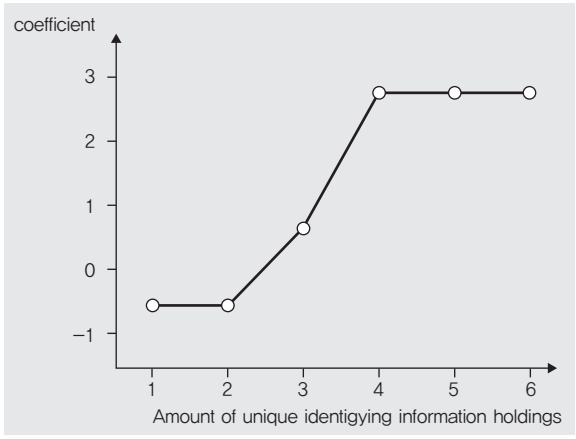
15) 개인정보보호법 제31조(개인정보 보호책임자의 지정)는 개인정보 처리에 관한 업무를 총괄하고 이를 책임지기 위해 개인정보 보호책임자 지정을 규정하고 있으며, 시행령에서 개인정보보호 책임자의 지정요건, 업무, 자격요건, 그밖에 필요한 사항을 규정하고 있다.



Investment budget

1 : less than 100,000 won
2 : more than 100,000 won and less than 1million won
3 : more than 1million won and less than 10million won
4 : more than 10million won and less than 100million won
5 : more than 100million won

〈그림 2〉 그룹 II의 예산 규모별 영향도
〈Fig. 2〉 Impact of Group 2 on Budget size



Amount of unique identigying information holdings

1 : less than 100,000 won
2 : more than 1,000 and less than 10,000
3 : more than 10,000 and less than 50,000
4 : more than 50,000 and less than 100,000
5 : more than 100,000 and less than 500,000
6 : more than 500,000 and less than 1million

〈그림 3〉 그룹 III 개인정보처리자의 고유식별정보 보유규모별 영향도
〈Fig. 3〉 Impact of Group 3 personal information manager on unique identifying information holdings size

마지막으로 그룹 Ⅲ을 분석한 결과는 다음과 같다. 분산분석 F값은 25.895($p<0.001$)로 유의하게 나타났으며 값은 0.783으로 설명력이 높은 것으로 나타났다. 그룹 Ⅲ은 전담 인력 수를 제외한 나머지 변수 모두 신뢰수준 99%에서 유의한 것으로 분석되었다. 상대적 중요도는 담당자의 업무 경력이 0.527로 가장 높게 나타났으며, 투자예산 0.170, 개인정보보호 책임자 지정 유무 0.123 순으로 나타났다.

따라서 10만 명 이상 개인정보를 보유한 대기업, 중견기업, 공공기관과 100만 명 이상의 개인정보를 보유

한 중소기업, 단체가 속한 그룹 Ⅲ은 자기효능감, 반응효능감, 투자예산, 침해취약성, 침해심각성 모두 개인정보보호 활동에 주요 동기요인으로 분석되었으며, 동기요인 중 담당자의 업무 경력, 투자예산, 개인정보보호 책임자 지정이 상대적으로 중요한 요인으로 분석되었다.

특히 고유식별정보 보유 규모에 따른 개인정보보호 활동에 미치는 영향을 추가적으로 분석한 결과는 〈그림 3〉과 같다. 5만 명이상을 초과하여 개인정보를 보유하는 기관은 보유량과 관계없이 추가적인 보호 활동을 수행하지 않는 것으로 나타났다. 이는 개인정보보호법 시행령 제21조에서 안전성 확보조치 기준을 5만 명 이상으로 규정하고, 5만 명 초과 보유에 대한 추가적인 보호조치가 필요하지 않기 때문으로 판단된다.

Ⅴ. 결론

본 연구는 보호동기이론을 기반으로 개인정보처리자의 개인정보보호 활동에 미치는 주요 요인을 규명하고, 보호활동 활성화 지원을 위한 효율적 방안을 모색하고자 하였다. 분석결과를 정리하면 다음과 같다.

첫째, 기존 정보주체에 대한 선행연구와 같이 개인정보처리자의 개인정보보호 활동에 영향을 미치는 주요 요인 분석에 보호동기이론의 적용이 가능하다.

둘째, 소규모 개인정보를 보유한 소상공인 집단인 그룹 Ⅰ의 보호 활동에 주요 요인은 자기효능감과 반응효능감, 침해심각성으로 분석되었다. 이는 정보주체에 대한 선행연구의 분석과도 일치하는 결과로, 그룹 Ⅰ의 보호 활동을 강화하기 위해서는 금전적인 재정 지원보다 인적 자원에 대한 지원이 필요하며 담당자의 개인정보보호에 대한 인식교육이 우선되어야 한다. 특히 1인 혹은 소규모 업체에서 개인정보를 전담하는 인력을 지정하기 어려운 현실을 감안하여 업체 스스로 정기적인 보호조치를 수행할 수 있도록 점검도구를 무상으로 제작·배포하거나 원격으로 전문 서비스를 제공받을 수 있는 지원책이 마련되어야 할 것으로 판단된다.

셋째, 중간 규모 개인정보를 보유하는 집단인 그룹 Ⅱ의 보호 활동에는 상대적으로 자기효능감, 반응효능감, 투자예산이 중요 요인으로 분석되었으며, 특히 그룹Ⅱ는 국내 개인정보처리자의 가장 기본적인 속성을 가진 집단으로 향후 개인정보보호에 관한 정책 수립 시 준거 집단으로 활용 할 수 있을 것으로 판단된다. 그룹 Ⅱ의 보호 활동을 강화하기 위해서는 개인정보보호 책임자를 지정하고, 개인정보보호와 관련한 예산 책정 및 투자를 유도하기 위한 세액 감면 등 조세지원 정책이 필요할 것으로 판단된다. 또한 기관 내 정기 혹은 상시 개인정보보호 교육이 가능한 환경을 조성하기 위해 사내 교육 강사 양성을 지원할 필요가 있다.

마지막으로 대규모 개인정보를 보유하고 처리하는 집단인 그룹 Ⅲ의 보호 활동에는 상대적으로 자기효능감과 투자예산이 주요한 영향을 미치는 것으로 분석되었으며, 특히 담당자의 업무 경험과 개인정보보호 예산, 책임자 지정이 핵심 요인으로 나타났다. 그룹 Ⅲ은 개인정보보호 활동을 위한 기본적인 인적, 물적 기반은 이미 충족된 상태로, 보호 활동을 강화하기 위해서는 갖추어진 자원을 보다 효율적으로 활용할 수 있도록 보호체계 개선이나 운용에 대한 컨설팅 등의 지원이 필요할 것으로 판단된다. 또한 EU GDPR(General Data Protection Regulation)의 DPO(Data Protection Officer)와 같이 높은 수준의 전문 교육이 필요할 것으로 판단된다.

본 연구는 실태조사의 표준화된 설문양식으로 조사된 결과를 활용하여 개인정보처리자의 보호 활동과 관련된 다양한 변인을 발굴하지 못하였으며, 이로 인해 변인 간 매개로 발생하는 직·간접 효과 등을 연구모형에 반영하지 못하였다. 특히 본 연구는 실태조사의 설문 항목 및 결과를 2차 데이터로 활용하여, 연구모형 설계에서 정보프라이버시, 신뢰-위험 모델, 계획된 행동이론 등 개인정보보호 활동 연구에 적용가능한 추가적 이론을 고려하지 못한 한계가 있다. 향후 연구에서는 이러한 한계를 보완하여 국내 개인정보처리자에 대한 보다 심층적인 연구가 이루어질 필요가 있다.

■ References

Bae, J. (2016). "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 theroy." *The e-business studies, 17*(3), 191-208.

{배재권 (2016). 빅데이터 환경에서 개인정보유출 위협이 정보보호행위에 미치는 영향에 관한 연구 = 건강심리이론과 보호동기이론을 중심으로. 〈국제e-비지니스 연구〉, 17권 3호, 191-208.}

Bandura, A. (2001). "Social Cognitive theory : An Agentive Perspective" *Annual Review of Psychology, 52*, 1-26.

Bulgurcu, Burcu Cavusoglu, Hasan Benbasat & Izak (2010). "Information Security Policy Compliance : An Empirical Study of Rationality-Based Beliefs and Information Security Awareness." *MIS Quarterly, 34*(3), 523-A7.

Crossler, R. & Blanger, F. (2014). "An extended perspective on individual security behavior : Protection motivation theory and a unified security practices(USP) instrument." *ACM SIGMIS Databases, 45*(4), 51-71.

Floyd, D. L., Prentice-Dunn,S. & Rogers, R.W. (2000). "A meta analysis of research on protection motivation theory." *Journal of Applied Social Psychology, 30*, 407-429.

Gurung, Anil, Xin Luo & Qinyu Liao (2009). "Consumer motivations in taking action against spyware : an empirical investigation." *Information Management & Computer Security, 17*(3), 276-289.

Ifinedo, P. (2012). "Understanding information systems security policy compliance : An integration of the theory of planned behavior and the protection motivation theory." *Computers & Security, 31*(1), 83-95.

Kim, M. & Kim, S. (2014). "A study on Intention to Accept the Right to be Forgotten Associated with Exposure of Personal Data." *Korean Journal of Journalism & Communication Studies, 58*(2), 307-336.

{김민성·김성태 (2014). 개인정보 노출이 잊혀질 권리 수용의도에 미치는 영향에 관한 연구. 〈한국언론학보〉, 58권 2호, 307-336}

Kim, S & Lee, K. (2011). *An empirical study on perception factors influencing information security behavior*. Paper prsented at the Korea IT service society, Nov.30.

{김상훈·이갑수 (2011). "정보보호행동에 영향을 미치는 인지요인에 관한 실증적 연구." 한국IT서비스학회 학술대회 발표논문.}

Kim, S. & Park, H. (2013). "An Analysis of Influence Factor on Privacy Protection Awareness and Protection Behavior and moderating Effect of Privacy Invasion Experience." *Internet e-commerce Studies, 13*(4), 79-105.

{김상현·박현선 (2013). 프라이버시 보호인식 및 보호행동의도에 미치는 영향 요인과 프라이버시 침해경험의 조절효과에 관한 연구. 〈인터넷전자상거래연구〉, 13권 4호, 79-105.}

Kim, J. & Kim, S. (2013). "Privacy Behavioral Intention in Online Environment : Based on Protection Motivation Theory." *Informatization policy, 20*(3), 63-85.

{김종기·김상희 (2013). 온라인 환경에서 프라이버시 행동의도에 미치는 영향 : 보호동기이론을 중심으로. 〈정보화정책〉, 20권 3호, 63-85.}

Kim, J., Kim, S. & Kwon, D. (2016), "Study on Social Network Service(SNS) Users' Privacy Protection Behavior : Focusing on the protection motivation theory." *Journal of information systems, 25*(3), 1-30.

{김정은·김성준·권두순 (2016). 소셜 네트워크 서비스 이용자들의 개인정보보호 행동에 관한 연구-보호동기이론을 중심으로. 〈정보시스템 연구〉, 25권 3호, 1-30.}

Lee, H., Roh, E. & Han, K. (2018). "A study on factors affecting the investment intention of information security." *Korea digital contents society, 19*(8), 1515-1525.

{이홍제·노은희·한경석 (2018). 정보보호 투자의도에 영향을 미치는 요인에 대한 연구. 〈한국디지털콘텐츠학회논문지〉, 19권 8호, 1515-1525.}

Lee, K., Han, K. & Jung, J. (2016). "A study of influencing factors for compliance intention of personal information protection policy of public institution employees." *Entrue Journal of Information Technology, 15*(1), 75-94.

{이기호·한경석·정진섭 (2016). 공공기관 종사자의 개인정보보호정책 준수의도에 영향을 미치는 요인에 관한 연구. 〈엔트루정보기술지〉, 15권 1호, 75-94.}

Ministry of the Interior and Safety & Personal Information Protection Commission (2020). 2019 Survey on the Personal information Protection. Seoul

{행정안전부·개인정보보호위원회 (2020). 〈2019 개인정보보호 실태조사〉, 서울.}

Park, J. (2019). "A study on the influence of the perception of personal information security of youth on security attitude and security behavior." *Journal of the Korea industrial information systems society, 24*(4), 79-98.

{박경아 (2019). 청소년의 개인정보보안 의식이 보안의도와 보안행동에 미치는 영향에 관한 연구. 〈한국산업정보학회논문지〉, 24권 4호, 79-98.}

Park, C. & Lee, S. (2014). "A study of the user privacy protection behavior in online Environment : Based on protection motivation theory." *Journal of Internet Computing and Services, 15*(2), 57-71.

{박찬욱·이상우 (2014). 인터넷상에서의 개인정보 보호행동에 관한 연구: 보호동기이론을 중심으로. 〈인터넷정보학회논문지〉, 15권 2호, 59-71.}

Rogers, R. W. (1975). "A protection motivation theory of fear appeals and attitude change." *Journal of Psychology, 91*(1), 93-114.

Rogers, R. W. (1983). "Cognitive and physiological processes in fear appeals and attitude change : A revised theory of protection motivation." *Social Psychophysiology : A sourcebook*. 153-177. New York : Guilford Press.

Tian, Y., Park, M. & Chai, S. (2020). "A Study on the Factors of Online Information Security Behavior Failure : Focused on the Elderly." *Journal of information systems, 29*(1), 51-74.

{전양·박민정·채상미 (2020). 중·노년층의 온라인 개인정보보호 행동에 영향을 미치는 요인에 관한 연구, 한국과 중국 인터넷 사용자를 중심으로. 〈정보시스템연구〉, 29권 1호, 51-74.}

Wooldridge, J. (2010). *Econometric analysis of cross section and panel data*. MIT press.

Workman, M. & Bommer, W. H. & Straub, D. (2009). "The Amplification Effects of Procedural Justice on a Threat Control Model of Information Systems Security Behaviours." *Behaviour & Information Technology, 28*(6), 563-575.

Youn, Seounmi (2005). "Teenagers' perceptions of online privacy and coping behaviors : a risk-benefit appraisal approach." *Journal of Broadcasting & Electronic Media, 49*(1), 86-110.