

제재 및 보호동기와 정보보호정책 준수 의도에 관한 연구: 주관적 규범을 매개로

신 혁*

요 약

본 연구에서는 Fishbein & Ajzen(1975)이 제창한 합리적 행위이론을 근거이론으로 활용하였다. 그리고 억제 이론의 구성요인인 제재와 보호동기이론의 보호동기 일부요인을 선행변수로 채택하여 이론적 확인과 정보보호 분야에서 인용된 사례를 제시하였다. 합리적 행위이론의 변수인 주관적 규범을 매개변수로 채택하여 제재와 지각된 취약성, 반응비용 및 자기효용성과 정보보호정책 준수 행위 의도간의 인과관계를 분석하였다. 연구가설 검증 결과 제재를 제외한 지각된 취약성, 반응비용과 자기효용성은 행동 의도와 유의미한 인과관계가 있었으며, 주관적 규범은 선행요인과 의도 간에 매개효과를 입증하였다.

The Influence of Sanctions and Protection Motivation on the Intention of Compliance with Information Security Policies: Based on Parameter of Subjective Norm

Hyuk Shin*

ABSTRACT

This study applied the Theory of Reasoned Action by Fishbein & Ajzen(1975) as the grounded theory and adopt sanctions of the General Deterrent Theory and protection motivation of the Protection Motivation Theory as the antecedents to discuss the theoretical factors and the cases of application in the field of information security. Then, it adopted subjective norm, a variable of the Theory of Reasoned Action, as a parameter to analyze the causality of sanctions, perceived vulnerability, response cost, and self-efficacy with the intention to follow the information security policies. As a result, all of the antecedents except for sanctions had causality with the intention and subjective norm proved its mediating effect as a parameter between the antecedents and the intention.

Keywords : Information Security Policy, The Theory of Reasoned Action, Sanctions, Protection Motivation, Subjective Norm

1. 서 론

산업현장에서 정보보호를 위하여 방화벽 등 정보보안시스템의 설치와 관련 프로그램의 운용도 중요한 정보보호 활동이지만 조직의 핵심 자산인 종업원으로 하여금 정보보호정책 준수를 위한 자발적인 활동을 이끌어 내는 것이 더욱 중요하고 필수적이다. 기업에서 종업원의 안이한 정보보호 인식과 정보보호정책 준수 위반으로 정보자산의 침해 또는 유출 사고로 유발될 수 있는 유형적 또는 무형적 피해는 단시일에 회복하기 어려운 상황이 될 수 있다. 최근의 언론에서 자주 보도되는 랜섬웨어 또는 악성코드 침해 등으로 인한 정보보안사고가 중요한 예시로서 이를 증명하고 있다[7]. 최근의 정보보호정책과 관련한 선행연구에서는 정보보호 강화를 위한 수단이 기술적 보안조치가 조직에서 정보보호에 있어서 가장 효과적인 수단으로 인정하고 있지 않은 흐름을 보여주고 있다. 기업을 구성하는 핵심자산인 종업원 등 인적요인과 정보보호 역량과의 인과관계 분석과 검증이 증가하고 있기 때문이다[8]. Boss et al.(2009)는 정보보호와 관련하여 조직에서 경영진을 포함한 종업원의 행동에 관한 연구가 다양화되면서 정보보호정책 준수 의도 및 행동에 대한 요인 분석 연구에도 집중되고 있다고 하였다[14].

본 연구의 목적은 조직에서 정보보호정책 준수 의도 영향요인을 도출하고 가설검증을 통하여 종업원들로 하여금 정보보호정책 준수 의도를 적극 유발하도록 이론적으로 제안하기 위한 것이다. 이를 위해 다양한 정보보호분야 선행연구에서 검증된 Ajzen & Fishbein(1977)이 제창한 합리적 행위이론(Theory of Reasoned Action)을 근거이론으로 사용하였다[10]. 그리고 주관적 규범이 정보보호정책 준수 의도 사이의 인과관계 분석과 주관적 규범을 종속변수로 제재와 보호동기와의 각각의 인과관계를 분석하였다. 이를 위해 억제이론(General

Deterrence Theory)과 보호동기이론(Protection Motivation Theory)을 인용하였다. 아울러 정보보호정책 준수 행위 의도 연구를 위해 제재와 보호동기를 독립변수로 활용하고 합리적 행위이론의 변수인 주관적 규범과의 인과관계를 분석하고 인과관계를 검증하였다.

2. 이론적 배경

2.1. 정보보호정책 개념 및 특성

정보보호정책은 정보보호에 대한 목표와 방향을 제시하고 조직의 사업목표와 일관성을 유지하며 정보보호와 관련된 조직 및 종업원이 지켜야 하는 필수항목 등에 대한 전반적이며 정리된 규정이다. 정보보호정책은 조직에서 종업원이 스스로 준수하도록 경영진의 방침과 요구에 의하여 정보보호에 대한 비전 또는 목표, 기본 방향 및 규정 그리고 지침 및 가이드 또는 절차서가 포함된다. 이를 구체적으로 뒷받침하고 실제로 준수하도록 지원하기 위해서는 정보보안정책에 의한 표준과 세부절차가 확보되어야 한다[6]. 심준보와 황경태(2015)는 정보보호정책은 조직에서 정보보호에 대한 기본적인 방향과 이를 위한 추진 목표와 함께 지침, 규정과 가이드 및 매뉴얼 등으로 이루어진다고 하였다[5].

지침은 규정과 같이 종업원이 반드시 지켜야 하는 내용보다는 준수를 권고하는 내용을 구체화한 것으로, 정보보호정책에 따라서 보안시스템 또는 특정 영역에 대해 정보보호 활동에 필요 및 도움이 되는 내용을 제공한다. 세부절차서는 정책 준수를 위해 준수하여야 하는 항목을 단계적이고 구체적으로 이행하는 절차를 나열한 것이다. Sommestad et al.(2014)에 따르면 정보보호정책은 조직의 정보보호 역량을 제고를 위하여 경영진에게 가이드 하는 것을 포함하고 있다[35]. 심준보와 황경태(2015)는 정보보안 위험수준에 따라 정보보호정책을 보완하고

점검하고 측정하여야 한다고 주장하였다[4].

정보보호정책이 미비한 조직은 기술적 보안 및 물리적 보안영역의 정보보호는 가능할 수 있으나, 종업원의 보안활동을 통제하는 인력보안과 보안사고 예방 또는 대응에서는 어려움이 존재할 수 있다. 따라서 효율적인 정보보호 및 통제와 정보자산을 유지하고 관리하는 데 있어서 조직 전반의 정보보호정책 수립 및 절차에 근거한 실행은 필수적이다.

2.2 정보보호정책 선행연구

정보보호정책 준수에 대한 행동 연구는 국내 외에서 다양하게 연구되고 있으며, 정보보호정책 준수에 대한 선행요인 또한 다양하게 채택하고 있다. Sommestad et al.(2014)은 그간의 정보보호정책 준수에 대한 선행요인으로 변화에 대한 개방성, 태도 및 주관적 규범과 지각된 행동통제, 처벌에 대한 지각된 정의, 보상, 지각된 정당성, 정보보안 의식, 위협평가, 반응 효용성, 반응비용, 자기효용성, 지각된 가치 적합성, 정보보안정책 품질이 높은 영향을 주는 것으로 나타났으나, 정보보호정책 준수 위반에 대한 영향 요인으로는 훈련, 지각된 처벌의 심각성, 처벌의 확실성, 중화기술, 주관적 규범, 도덕적 신념, 지각된 편인, 참여도, 자기방어의도 등이 나타났다고 제시하였다[35]. 정보보호정책 연구동향을 보면 주로 다수의 선행연구가 정책 준수에 관한 것을 확인할 수 있다.

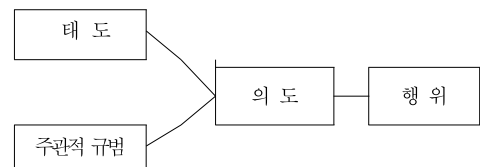
Herath & Rao(2009)는 정보보호정책에 대한 연구는 선행연구에서 검증된 근거이론과 함께 변수를 활용하여 다양하게 연구되었다고 하였다[20][21]. 그리고 Sommestad et al.(2014)은 정보보호정책 준수 또는 위반에 미치는 영향에 대한 선행요인을 조사하여 분석하고 각각의 선행요인에 대한 중요성과 인과관계 여부를 규명하였다[35]. 그간 선행연구에서 선행변수의 근거이론은 합리적 행위이론, 계획행동이론, 억제이론, 사회통제이론, 보호동기이론, 중화이론

등이다.

2.3 합리적 행위이론

Ajzen & Fishbein(1977)이 주장한 합리적 행위이론은 개인의 행위와 행위에 대한 의도 또는 의지간의 근본적 원인 측정이 가능한 연구 모델로서 많이 인용되었다[10]. Ajzen & Fishbein(1977)과 Ajzen(1991)은 태도와 행위에 관한 상호 인과관계 연구에서 태도와 합리적 행위 간의 상호대응 관점에서 연관성을 이론으로 제시하고, 그리고 의욕이 있는 행위를 실현하고자 하는 개인 스스로의 태도와 일정한 정도로 지각된 주관적 규범이 동시에 함께 포함된 결과가 개인적으로 의지 또는 의도로 나타난다고 정의하였다[9][10].

Ajzen(1991)은 합리적 행위이론을 바탕으로 연구한 결과, 신념에서 태도로, 태도에서 의도로, 그리고 의도는 행위로 영향을 미치는 것으로 제시하였다[9]. 이정하와 이상용(2015)은 합리적 행위이론은 개인이 어떠한 행위를 실천하기 위한 결정은 개인이 실행하고자 하는 의도에 의해 결정되고, 그러한 의도는 지각된 주관적 규범과 태도에 의해 생성된다고 요약하였다[6]. 이와 같이 합리적 행위이론은 (그림 1)과 같이 표현할 수 있다.



(그림 1) 합리적 행위이론
Ajzen & Fishbein(1977), 연구자 재구성

합리적 행위이론은 사회심리학 분야의 일부 이론으로 조직에서의 행동통제, 의료분야에서의 의사결정, 정보통신기술 활용 등과 같은 다양한 영역에서 개인 또는 종업원의 행위를 분석하기 위한 기초이론으로 다양하게 활용하였다고 Ajzen & Fishbein(1977)은 주장하였다

[10]. Ifinedo(2014)는 종업원과 사용자의 태도, 주관적 규범이 정보보호정책 준수 행동 의도에 영향을 미친다고 제시하였다[22].

2.4. 억제이론 및 제재

Bankston & Cramer(1974)에 의한 억제이론은 인간의 자유에 대한 의지와 합리적인 의사결정을 기초로 하는 일반적인 범죄이론으로, 개인 스스로의 행동은 자유의사에 의하여 범죄행위를 저지를 것인가 아니면 그렇지 않을 것인가를 자신 스스로 선택하고 행동한다는 것이다[13]. 그러므로 국가 또는 조직은 범죄를 저지른 개인을 제재하거나 또는 처벌함으로써 상응한 대가를 받게 하고, 이러한 제재를 활용하여 미래에 발생가능한 범죄를 사전에 예방 또는 억제할 수 있다는 것이다[1].

억제이론에 근거하면 제재의 범죄억제 효과를 극대화하기 위해서는 제재의 신속성은 범죄가 발생한 시점부터 그러한 범죄에 제재 또는 벌칙이 가해지는 시간과 연관되어 있다. 확실성은 범죄 행동이 적발된 경우 제재 가능성을 의미하고, 심각성은 범죄 행동의 경중에 따른 제재의 규모와 관련이 있다. Straub(1990)은 제재의 신속성과 심각성 및 확실성이 반영된 조직에서 정보보호정책을 준수하지 않은 종업원에 대한 제재는 준수 행동을 적절히 증가시킨다고 하였다[37]. Herath & Rao(2009)는 제재의 확실성과 심각성을 정보보호정책 준수 관점에서 그간의 정보보호정책 준수에 대한 선행연구를 재정리하고 행동 의도와 의 인과관계를 검증하였다[20][21].

2.5. 보호동기이론 및 구성 요인

보호동기이론은 원래에는 개인의 건강과 관련한 태도와 행동에 영향을 미치는 위협 또는 위협요인의 규명을 위해 연구되었으며, 개인의 부상예방과, 환경 및 보안문제 해결 등에서도 보호이론이 검증되었다[19]. 보호동기이론은 일

정 상황에서의 위협과 위험한 행동에 대해 어떻게 판단하고 대응하도록 동기부여가 제기되는 가를 나타내고 있다. Zhang et al.(2009)은 개인의 위협에 대한 대처에 관한 연구를 위해 지각된 보호동기 요인을 채택하였다. 위협 대처는 지각된 위협의 정도인 위협성, 지각된 위협에 민감한 정도인 취약성을 포함한다[41].

그리고 Rogers(1975)의 보호동기이론은 위협에 대처하기 위한 개인능력을 나타내는 선행요인을 포함한다[30]. Rogers(1975)는 위협의 제거에 따른 대처에 의해 지각되는 편익에 대한 믿음인 반응효용성, 위협에 대한 보호행동에 따라 부과되는 반응비용과 스스로 보호행동 실천이 가능하다고 믿는 정도인 자기효용성으로 정의하였다[30][31].

정보보호 선행연구에서 보호동기이론의 변수는 독립변수로 많이 인용되고 있으며, 정보보호 행동 의도 또는 태도 등과 보호동기 요인간의 인과관계 또는 영향 여부 검증에 있다. Ifinedo(2012)는 정보보호정책 준수 연구에서 보호동기 요인 대부분의 독립변수가 종업원의 행동 의도에 인과관계가 있는 것으로 증명하였다[23]. 그간의 보호동기를 선행요인으로 인용하고 종속변수인 행동 의도간의 인과관계 설정과 영향여부에 대한 검증이 다수였다[28]. 그리고 정보보호정책 준수 행동 연구에서 보호동기 요인을 변수로 채택하여 준수 행동을 위한 의도에 대하여 보호동기가 실증적으로 유의미하게 활용한 결과를 제시하였다[11][12].

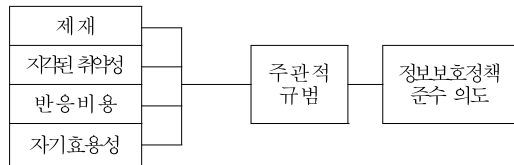
3. 연구가설 및 방법

3.1. 연구가설 설정

본 연구는 산업현장에서 종업원의 정보보호정책 준수 요구가 강화하고 있음에 이를 제고하기 위하여 선행연구를 기초하여 연구가설을 설정하였다. 그리고 종업원의 정보보호정책 준

수 행동 의도에 대한 변화에 대한 설명이 가능한 합리적 행위이론을 토대이론으로 연구가설을 분석하였다. 연구가설은 합리적 행위의 선행요인인 주관적 규범과 억제이론의 변수인 제재와 보호동기이론 변수인 지각된 취약성, 반응비용 및 자기효용성과 상호 간 영향 여부를 실증하는 것이다.

실증연구 분석을 위한 수단으로 다중적 회귀분석 등 통계기법을 사용하여 각각의 연구가설의 유의성 여부를 검증하였다.



(그림 2) 연구모형

3.2. 제재와 주관적 규범간의 연구가설

Kankanhalli et al.(2003)은 제재심각성이 정보보호 활동의 효과에 대비하여 선행요인이 될 수 있다는 것을 확인하였다[24]. Straub (1990)는 정보보호정책 미준수에 대한 적절한 제재의 부과는 적절한 정보보안 행동을 증가시킨다고 주장하였다[37]. Herath & Rao(2009)는 조직에서의 제재는 억제이론에서 시작한다고 제시하였다[21]. D'arcy et al.(2011)은 정보보호정책 위반에 대한 제재심각성은 종업원으로 하여금 정보보호 행위의 미숙함이 감소될 수 있다고 제시하였다[17]. 한편 Herath & Rao(2009)는 제재확실성과 심각성은 종업원의 정보보호정책 준수 의도에 유의미한 영향을 준다고 설명하였다[20]. 그리고 Son(2011)은 종업원의 정보보호정책 준수 의도에 대하여 위반하는 경우 제재심각성은 유의미한 영향을 주는 것으로 제시하였다[36]. 이와 같이 억제이론과 선행연구 가설에 대한 검증결과를 근거로 제시한 연구가설은 다음과 같다.

가설1. 제재는 정보보호정책 준수 의도에 대한 주관적 규범에 정(+)의 영향을 미칠 것이다.

3.3. 보호동기와 주관적 규범간의 연구가설

Lee & Lee(2002)는 지각된 취약성은 조직에서 컴퓨터 활용에 있어서 보안위반에 대한 전반적 분석에서 준수 행동을 위한 의도에 중요한 영향을 제공하는 연구결과를 제시하였다[26]. Pahlila et al.(2007)은 지각된 위험성과 지각된 취약성은 정보보호정책 준수를 위한 태도에 유의미한 관계가 있다고 증명하였다[28][29]. Ifinedo(2012)는 보호동기 가운데 위협대처 요인인 지각된 취약성은 정보보안정책 준수 의도에 유의미한 영향을 미치는 것으로 보았다[22]. Siponen et al.(2014, 2007)의 정보보호정책에 대한 종업원의 준수 연구에서도 보호동기 요인인 지각된 취약성은 준수 의도에 유의미한 영향을 미치는 것으로 검증하였다[32][33]. 이와 같이 보호동기이론과 선행연구 가설에 대한 검증결과를 근거로 제시한 연구가설은 다음과 같다.

가설2. 지각된 취약성은 정보보호정책 준수 의도에 대한 주관적 규범에 정(+)의 영향을 미칠 것이다.

반응비용은 개인의 행동의 결과에 따라 소요되는 금전적 비용 소요, 시간적 불편하기, 어려운 환경조성 또는 부정적 결과를 포함할 수 있다고 Pahlila et al.(2007)은 요약하였다[28][29]. 선행연구에서 반응비용은 정보보호 조치를 이행하는 데 있어서의 행동 의도에 대해 부정적 인과관계로 제시하였다. Vance(2010)의 연구에서도 반응비용이 정보보호를 위한 행동 의도에 부정적 인과관계를 제시하였다[38]. Bulburcu et al.(2010)은 지각된 취약성은 보안행동을 위한 태도에 부정적으로 영향을 미친다고 하였다[15]. Ifinedo(2012)는 정보보호정책 준수 의도에 반응비용이 미치는 영향을 검증하고 준수

의도에 긍정적으로 미친다는 가설을 설정하여 인과관계를 분석하였다[22]. Vance et al.(2012)은 반응비용은 정보보호정책을 준수 의도간의 부정적인 인과관계로 있다고 제시하였다[39]. 이와 같이 보호동기이론과 선행연구 가설에 대한 검증결과를 근거로 제시한 연구가설은 다음과 같다.

가설3. 반응비용은 정보보호정책 준수 의도에 대한 주관적 규범에 정(+의 영향을 미칠 것이다.

Siponen et al.(2010)은 자기효용성과 정보보호정책 준수 의도간의 유의미한 인과관계를 실증하고 자기효용성의 중요성을 강조하였다[33]. 그리고 Whitman(2004)은 자기효용성이 정보보호를 위한 직무행동을 수행하는 데 개인의 수행능력에 심각한 영향을 준다고 검증한 바 있다[40]. Compeau et al.(1995)은 정보보호에 대하여 자기효용성이 강한 종업원이 자기효용성이 약한 종업원보다 직무수행에서 더 많은 정보시스템을 활용한다고 주장하였다[16]. 박찬욱과 이상욱(2014)은 보호동기이론을 중심으로 한 인터넷상에서의 개인정보 보호행동에 관한 연구에서 자기효용성과 개인정보보호 행동과의 상호 간의 인과관계에 대한 영향을 분석하였다[2]. 위와 같이 선행연구에서 정보보호정책 준수 행동 의도에 영향 여부에 대하여 자기효용성을 선행요인으로 제시하였다. 보호동기이론과 선행연구 가설에 대한 검증결과를 근거로 제시한 연구가설은 다음과 같다.

가설4. 자기효용성은 정보보호정책 준수 의도에 대한 주관적 규범에 정(+의 영향을 미칠 것이다.

3.4. 주관적 규범과 준수 의도간의 연구가설

Fishbein과 Azen(1975)에 의하면 합리적 행위이론 의하면 주관적 규범은 특정행위 의도에 영향을 미치는 주변에서의 규범적인 자극, 신

뢰 및 동기이다. 즉, 개인의 행동은 주변에서 규범이라고 지각되는 것에 의해 동기부여가 되거나 영향을 받는다는 것이다[18]. Vance & Siponen(2012)의 정보보호정책 준수 연구에서는 주관적 규범과 태도는 행동 또는 의도에 영향을 미치는 요인으로 인용되었다[39]. Rogers & Prentice-Dunn(1997)은 보호동기를 변수로 채택한 연구에서 결과측정 수단은 행동 또는 의도라고 주장하였다[31]. Somestad et al.(2014)은 정보보호정책 준수에 미치는 선행요인에 대한 메타분석에서 합리적 행위이론에 의한 주관적 규범은 정보보안정책 준수 행동과의 의도에 유의미한 영향을 미치는 변수로서 정리하였다[35]. 이와 같이 합리적 행위이론과 선행연구에 의한 검증결과를 근거로 제시한 연구가설은 다음과 같다.

가설1.5. 주관적 규범은 정보보호정책 준수 의도에 정(+의 영향을 미칠 것이다.

3.5. 변수 측정 및 인구통계학적 분석

각각의 변수간의 인과관계 측정을 위한 측정항목은 선행연구에서의 정의를 근거하여 요인별 타당성과 신뢰성이 검증된 설문을 작성하였다. 설문은 인구통계학적 분석을 위한 문항 이외에는 리커트(Likert) 5점 척도로 구성하여 측정하였다.

<표 1> 인구통계학적 분석

	구분	구성비
성별	남성 / 여성	51% / 49%
학력	~학사 / 석·박사	90% / 10%
소속	중소벤처기업 / 중견기업	54% / 13%
	대기업 / 연구기관 및 기타	11% / 22%
부서	총무 및 관리 / 연구개발	32% / 12%
	기술생산 / 영업마케팅	12% / 13%
	기타	31%
직급/직급	CEO~임원급 / 수석~책임급	7% / 22%
	선임급 / 주임급이하	16% / 55%

설문문항은 매우 그렇다(5)에서부터 매우 그

렇지 않다(1)까지로 구성하였으며, 연구가설에 대한 인과관계 분석 및 검증을 위해 통계패키지 SPSS 20을 활용하였다. 설문응답 대상자는 305명이며 분석한 결과 인구통계학적 특성은 <표 1>과 같다.

4. 실증 분석 및 가설 검증

4.1. 신뢰도 및 타당성 분석

설문결과에 대한 실증분석에 앞서 요인별 타당성 분석과 신뢰도 분석을 각각 진행하여 실증분석을 위한 정교화 과정을 실시하였다. 탐색적 요인분석은 측정항목별 개별타당성 검증을 위하여 주성분 분석 방식과 고유값이 1.0 이상인 요인을 선정하고 항목간 해석은 배리맥스 회전방식(Varimax rotation)으로 실시하였다. 송지준(2017)은 신뢰도 측정은 연구 개념과 설문에 대한 응답결과 각각의 변수와 얼마만큼 내적일관성이 있게 측정되었는지 검증하고자 하는 것으로 설명하였다[3].

<표 2> 연구모형 요인분석 및 신뢰도 분석

변수	측정항목	요인 적재량	고유값	신뢰도 (α)
정보보호 정책 준수 행동 의도	의도3	0.840	3.135	0.893
	의도2	0.801		
	의도4	0.799		
	의도1	0.785		
주관적 규범	주관적규범3	0.810	2.813	0.860
	주관적규범4	0.795		
	주관적규범1	0.759		
	주관적규범2	0.686		
지각된 취약성	지각된취약성2	0.852	2.484	0.897
	지각된취약성1	0.838		
	지각된취약성3	0.804		
반응 비용	반응비용2	0.815	2.203	0.802
	반응비용3	0.792		
	반응비용1	0.747		
제재	제재2	0.869	2.192	0.904
	제재3	0.813		
	제재1	0.808		
자기 효용성	자기효용성2	0.867	2.191	0.802
	자기효용성3	0.844		
	자기효용성1	0.827		

일반적으로 설문에 대한 신뢰도 검증을 위하여 크론바하 알파값으로 평가한다[3]. Nunnally (1978)에 따르면 크론바하 알파값이 0.6~0.7이면 허용 가능, 0.7~0.9이면 적절 그리고 0.9 이상이면 양호한 것으로 간주한다[27]. 7개 변수에 대한 신뢰도 측정결과는 0.802~0.904로서 모두 0.8 이상으로 변수 각각의 측정항목들 신뢰수준을 만족한다고 할 수 있다. 각각의 변수별 측정항목과 변수와 대한 요인분석 결과값 및 검증된 신뢰성 분석 결과는 <표 2>로 나타났다.

탐색적 요인분석과 신뢰도 분석에 이어 변수간의 상관관계 분석을 통한 타당성 분석을 추가하였다. 변수간의 상관관계는 복수의 변수에서 한 개의 변수가 변화함에 따라서 이외의 변수가 변화하는 강도를 제시한다고 볼 수 있다 [3]. 변수간의 상관관계 결과는 절대값이 1에 가까울수록 변수간의 상관관계가 크다고 볼 수 있다[3]. 상관관계 분석에 의한 타당성 검증결과는 <표 3>으로 나타났다.

<표 3> 변수간 상관관계 분석

구분	반응 비용	자기 효용성	주관적 규범	지각된 취약성	행동 의도	제재
반응비용	1**	.377**	.353**	.520**	.263**	-.064
자기효용성	.377**	1	.418**	.456**	.498**	-.035
주관적규범	.353**	.418**	1	.542**	.542**	.013
지각된취약성	.520**	.456**	.542**	1	.444**	-.031
행동의도	.263**	.498**	.542**	.444**	1	.059
제재	-.064	-.035	.013	-.031	.059	1

** .상관계수는 0.01 수준(양쪽)에서 유의합니다.

4.2. 연구가설 검증

본 연구는 제재 및 보호동기와 정보보호정책 준수 의도 간의 인과관계 분석을 위해 주관적 규범을 매개로 검증하고 기업 등 조직에서 정보보호정책 준수를 제고하는 데 각각의 요인별 영향을 검증하고자 하는 것이다. 연구가설 검증을 위하여 단순회귀분석 방법과 다중회귀분

석 방법을 실시하였다. <표 4>는 지각된 취약성과 반응비용 및 자기효용성과 주관적 규범과의 관계에 t값과 유의확률이 각각 정(+)의 값을 나타내고 있어 인과관계가 있다고 보여주었다. 반면에 제재는 주관적 규범과 t값(0,978), 유의확률(0,329)로서 인과관계가 없음을 보여주었다. 따라서 연구가설2와 연구가설3 및 연구가설 4는 채택이 되었으나 연구가설 1은 채택되지 못하였다. 주관적 규범과 정보보호정책 준수 의도와와의 연구가설 검증결과 t값(11.225), 유의확률(0.000)로 정(+)의 값으로 연구가설 5는 채택되었다.

<표 4> 연구가설 검증 회귀분석

종속 변수	독립변수	표준 오차	베타 (β)	t값	유의 확률	공차 한계
주관적 규범	제재	0.042	0.046	0.978	0.329	0.992
	지각된취약성	0.046	0.406	7.541	0.000	0.747
	반응비용	0.042	0.147	3.025	0.003	0.910
	자기효용성	0.048	0.210	4.011	0.000	0.790
R=0.593, R ² =0.353, 수정된 R ² =0.345 F=9.9563, p=0.000, 더빈윌슨=2.042						
행동 의도	주관적 규범	0.051	0.542	11.225	0.000	1.000
	R=0.542, R ² =0.067, 수정된 R ² =0.087 F=12.275, p=0.000, 더빈윌슨=1.822					

정보보호정책 준수 의도에 대한 주관적 규범에 미치는 영향은 지각된 취약성(β=0.406)이 가장 크며 자기효용성(β=0.210)과 반응비용(β=0.147) 순서로 나타났다.

4.3. 매개효과 및 총효과 분석

매개효과분석은 일반적으로 SPSS에 의한 위계적 회귀분석 측정방법을 사용한다. 또한 매개효과 값은 간접효과로 활용되어 경로계수값(β)을 측정값으로 검증한다[3]. 본 연구는 주관적 규범을 매개변수로 채택하여 정보보호정책 준수 의도에 제재, 지각된 취약성, 반응비용 및 자기효용성에 의한 매개효과를 검증하였다. 검

증결과 유의수준에서 제재에 대한 매개효과는 표준화 경로계수값(β)이 0.007로 나타났고, 지각된 취약성은 0.231로 나타났으며, 반응비용은 0.166으로 그리고 자기효용성은 0.169로 각각 <표 5>과 같이 나타났다. 더빈윌슨 통계량이 각각의 변수 검증결과에서 1.786에서 1.845로 모두 2.0 근처에 있으므로 모두 상관관계가 없음을 검증하였다.

<표 5> 매개효과 분석

독립 변수	매개 변수	종속 변수	매개효과(유의수준)	더빈 윌슨
제재	주관적 규범	행동 의도	0.013x0.541=0.007(****)	1.845
지각된 취약성	주관적 규범	행동 의도	0.542x0.427=0.231(****)	1.786
반응 비용	주관적 규범	행동 의도	0.295x0.566=0.166(****)	1.801
자기 효용성	주관적 규범	행동 의도	0.418x0.405=0.169(****)	1.796

이와 같이 매개효과는 지각된 취약성, 자기효용성, 반응비용 및 제재 순으로 검증되었다.

정보보호정책 준수 의도에 미치는 영향에 대한 각각의 독립변수에 의한 총효과 분석을 위하여 직접효과와 간접효과를 검증하였다. 총효과는 각각의 독립변수가 종속변수에 미치는 영향에 대한 직접효과를 보여주는 표준화 경로계수값(β)과 매개변수로 채택한 주관적 규범을 경유하는 간접효과 표준화 경로계수 값(β값)을 합한 결과로 나타낼 수 있다. 총효과 분석에서 유의할 것은 β값의 측정에서 유의확률이 0.05보다 큰 경우에는 유의하지 않으므로 채택하지 않는다. 검증결과 제재와 행동의도간의 가설경로에 대한 총효과는 직접효과 0.052, 간접효과 0.007로서 합하여 0.059의 β값을 보여주었다. 지각된 취약성과 행동 의도간의 가설경로에 대한 총효과는 직접효과 0.427, 간접효과 0.231로 합하여 0.658의 경로계수 값(β)을 보여주었다. 반응비용과 행동 의도간의 총효과는 직접효과는 유의수준에 미치지 못하여 없으며 간접효과

0.328로서 0.328의 β 값을 보여주었다. 그리고 자기효용성과 행동 의도간의 총효과는 직접효과 0.328, 간접효과 0.169로 합하여 0.497의 β 값을 보여주었다. 이와 같이 총효과 결과는 지각된 취약성, 자기효용성, 반응비용 및 제재 순으로 나타났으며 그 결과는 <표 6>으로 요약하였다.

<표 6> 총효과 분석

독립 변수	매개 변수	종속 변수	총효과	간접효과	직접효과	유의 수준
제재	주관적 규범	행동 의도	0.059	0.007	0.052	***
지각된 취약성	주관적 규범	행동 의도	0.658	0.231	0.427	***
반응 비용	주관적 규범	행동 의도	0.166	0.166	-	***
자기효용성	주관적 규범	행동 의도	0.497	0.169	0.328	***

5. 결론 및 시사점

5.1. 결론

본 연구는 기업 등 현업에서 종업원이 정보보호정책을 준수하고자 하는 행동 의도에 대한 영향요인을 분석하고 행동 의도를 강화하기 위하여 그간의 다양한 선행연구에서 검증된 합리적 행위이론과 억제이론 및 보호동기이론을 이론적 근거와 변수로 활용하였다. 이와 같은 결과에서 정보보호정책 준수 의도를 강화하고자 종업원 개인의 주관적 규범은 매우 중요한 요인으로 작용하는 것이 검증되었다. 정보보호정책 위반에 대한 제재와 인지된 정보보안 위협에 대한 지각된 취약성 및 반응비용과 자기효용성 요인도 주관적 규범을 자극하는 영향요인임을 가설검증에 의한 인과관계 분석결과에서 확인할 수 있었다. 가설검증과 연구모형에 대한 통계분석으로 검증된 결과를 바탕으로 다음과 같이 정보보호정책 준수 의도에 대한 연구

결과를 요약할 수 있다.

먼저 본 연구가 그간의 선행연구와 같이 합리적 행위이론, 억제이론 및 보호동기이론에 따른 각각의 변수 간의 유의미한 인과관계를 형성하고 있다는 것을 실증적으로 보여주고 있다는 것이다. 이것은 합리적 행위이론은 토대이론으로 선택된 다양한 선행요인이 실증적으로 인과관계를 검증할 수 있다는 것을 다시 한번 확인하였다.

본 연구결과 매개변수 채택에 있어서 합리적 행위이론에서 태도를 매개요인으로 한 다양한 연구가 있었으나 주관적 규범을 매개요인으로 합리적 행위이론의 이론적 다양성과 확장성 검증에도 의의를 찾을 수 있다. 그리고 정보보호정책 준수 의도에 대한 요인 분석에서 종업원의 준수 의도를 강화하는 데 있어서 조직차원에서 위반에 대한 제재의 강화 등의 경영활동보다는 종업원 스스로 보안위협에 대한 스스로 취약점을 지각할 수 있도록 다양하고 정기적인 교육의 실시와 예방적 활용을 시행토록 하여 종업원에게 할 수 있다는 자신감을 제공하는 정책적 배려를 적극 추진하여야 한다고 볼 수 있다. 또한 정보보호정책 준수에 대한 행동을 하는 데 있어서 수반되는 비용 또는 소요시간 등에 대한 종업원의 부담을 제거하거나 최소화하는 노력을 정책적 뒷받침으로 제도화하는 것이 더욱 중요하다고 볼 수 있다.

5.2. 연구 시사점

이를 바탕으로 다음과 같은 실무적 관점에서 시사점을 마련하여 제시하고자 한다. 첫째, 정보보호정책을 수립하고 준수하도록 추진하는 데 있어서 경영진의 참여는 가능한 최소화 하여 간접적인 방법을 활용하여야 한다. 회의 방식을 활용하거나 외부전문가 등을 활용하는 것이 방법일 수 있을 것이다. 둘째, 선행연구 결과와 같이 본 연구에서도 보호동기 요인을 적극 활용하여 정보보호정책 준수를 위한 행동

의도가 사전에 종업원 스스로 부여될 수 있도록 조직차원에서의 제재 강화보다 행동 실천에 따른 보상과 다양한 동기부여 조치가 우선적으로 고려되어야 한다는 것이다.

이와 같은 실증결과에도 불구하고 본 연구에 일정부분 연구의 한계가 있다는 것을 확인할 수 있었다. 먼저 연구를 위한 설문조사를 실시함에 있어 설문응답대상자를 현장방문을 활용하여 종업원으로부터 실제 응답을 통한 직접적인 조사이어야 함에도 인터넷을 활용한 간접방식의 활용으로 설문응답자의 설문에 대한 보다 솔직한 견해와 평소 습득한 지식에 의한 응답 결과를 이끌어 내지 못하였다는 것이 아쉽다고 할 수 있다. 아울러 종업원의 정보보호정책 준수 행동 의도를 유인하는 데 있어서 일부 제한적인 선행요인을 변수로 채택하여 보다 포괄적이고 충분한 분석을 하지 못했다고 하는 것이 아쉽다고 할 수 있으나 주관적 규범을 매개변수로 선행변수와 독립변수간의 인과관계 분석을 다양하게 시도하고 검증하였다는 점을 제시할 수 있다.

참고문헌

- [1] 기광도, “법위반에 대한 처벌의 억제효과분석:인지적 측면을 중심으로”, 한국형사정책학회, 형사정책 제16권 제2호, pp. 9-35, 2004.
- [2] 박찬욱과 이상욱, “인터넷상의 개인정보 보호행동에 관한 연구: 보호동기이론을 중심으로”, 한국인터넷정보학회. 제15권 제2호. pp. 171-199, 2015.
- [3] 송지준, “SPSS/AMOS 통계분석방법,” 21세기사, 2017.
- [4] 신혁, 강민형, 이철규, “경영진 역할과 보호 동기 요인이 정보보안정책 준수에 미치는 영향: 계획행동이론을 기반으로”, 융합보안논문지, 제18월 제1호, pp.69-84, 2018.
- [5] 심준보, 황경태, “은행 IT인력의 정보보호 정책 준수에 영향을 미치는 정보보호 대책에 관한 연구”, 한국테이타비이스학회, 제22권, 제2호.
- [6] 이정하, 이상용, “금융회사 보안정책의 위반에 영향을 주는 요인 연구: 지각된 고객정보 민감도에 따른 조절효과”, 한국테이타비이스학회, 22(4), pp.225-251, 2015.
- [7] 이창훈, 하옥현, “기밀유출 방지를 위한 융합보안 관리체계”, 융합보안논문지, 제10권 제4호, pp. 61-67, 2010.
- [8] 정재원, 이정훈, 김채리, “기업의 정보보안 활동이 구성원의 정보보안 준수 의도에 미치는 영향 연구”, 융합보안논문지, 제16권 제7호, pp. 51-59, 2016.
- [9] Ajzen, I. “The theory of planned behavior,” *Organizational Behavior and Human Decision Processes*, Vol.50, pp. 179-211. 1991.
- [10] Ajzen, I., and Fishbein, M., “Attitude - Behavior Relations: A theoretical analysis and review of empirical research”, *Psychological Bulletin*, 84(5), pp.888 - 918, 1977.
- [11] Aurigemma, S., “A composite framework for behavioral compliance with information security policies,” *Journal of Organizational and End User Computing*, Vol. 25, No. 3, pp. 32-51. 2013.
- [12] Aurigemma, S., and Panko, R., “A composite framework for behavioral compliance with information security policies”, 2012 45th Hawaii International Conference on System Science, pp. 3248-3257, 2012.
- [13] Bankston, W. B., & Cramer, A. (1974). “Toward a Macro-Sociological Interpretation of General Deterrence”, 「*Criminology*」. 12: 251-280.
- [14] Boss, S., Kirsch, L., Angermeier, I., Shingler, R., and Boss, R., “If Someone Is Watching,

- I'll Do What I'm Asked : Mandatoriness, Control, and Information Security”, *European Journal of Information Systems*, Vol. 18, No. 2, pp. 151 - 164. 2009,
- [15] Bulgurcu, B., Cavusoglu, H., and Benbasat, I., “Information security policy compliance : An empirical study of rationality-based beliefs and information security awareness,” *MIS quarterly*, Vol. 34, No. 3, 2010, pp. 523-548. 2010.
- [16] Compeau, D. R. and Higgins, C. A., “Computer Self-Efficacy: Development of a Measure and Initial Test”, *MIS Quarterly*, Vol. 19, No. 2 (1995, Jun.), pp. 189-211.
- [17] D'Arcy, J. and Herath, T., “A review and analysis of deterrence theory in the IS security literature : Making sense of the disparate findings”, *European Journal of Information Systems*, 20(6), pp.643-658, 2011.
- [18] Fishbein, M. and Ajzen, I., “Belief, attitude, intention and behavior: An introduction to theory and research”, Reading, MA: Addison- Wesley, 1975.
- [19] Gochman (Ed.), *Handbook of health behavior research I: Personal and social determinants*, New York, NY: Plenum Press. pp.113-132, 1997.
- [20] Herath, T., and Rao, H. R., “Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness,” Vol.40, pp. 154-165. 2009a.
- [21] Herath, T., and Rao, H. R., “Protection motivation and deterrence: A framework for security policy compliance in organizations,” *European Journal of Information Systems*, Vol.18, pp. 106-125. 2009b.
- [22] Ifinedo, P., “Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition,” *Information & Management*, Vol. 51, No. 1, pp.69-79, 2014.
- [23] Ifinedo, P., “Understanding information systems security policy compliance: An integration of the theory of planned theory and protection motivation theory,” *Computers and Security*, Vol. 31, pp. 83-95. 2012.
- [24] Kankanhalli, A., Teo, H. H., Tan, B. C., and Wei, K. K., “An integrative study of information systems security effectiveness”, *International Journal of Information Management*, 23(2), pp.139-154, 2003.
- [25] Katsikas, S. K., “Health care management and information systems security: Awareness, training or education?” *International Journal of Medical Informatics*, Vol. 60, No. 2, pp.129-135. 2000.
- [26] Lee, J., and Lee Y., “A holistic model of computer abuse within organizations,” *Information Management & Computer Security*, Vol.10, No.2, pp. 57-63. 2002.
- [27] Nunnally, J. C., *Psychometric Theory*, New York, McGraw-Hill, 1978.
- [28] Pahnla, S., Siponen, M., and Mahmood, A., “Employees’ behavior towards IS security policy compliance,” *System Sciences, 2007 HICSS 2007 40th Annual Hawaii International Conference on*, pp. 156b. 2007a.
- [29] Pahnla, S., M Siponen, M., and Mahmood, A., “Which factors explain employees’ adherence to information security policies? An empirical study,” *Pacific Asia Conference on Information Systems(PACIS), 2007b Proceedings*, aisel.aisnet.org.
- [30] Rogers, R. W., “A protection Motivation Theory of fear appeals and attitude change,” *The Journal of Psychology*, Vol.91, pp. 93-114. 1975.

[31] Rogers, R. W., & Prentice-Dunn, S. "Protection motivation theory. In D. S., 1997.

[32] Siponen, M., Mahmood, A., and Pahnla, S., "Employees' adherence to information security policies: An empirical field study," *Information Management*. Vol.51, pp. 217-224. 2014.

[33] Siponen, M., Pahnla, S., and Mahmood, A., "Employees' adherence to information security policies: An empirical study," *IFIP International Federation for Information Processing*. Vol.232, pp. 133-144. 2007.

[34] Siponen, M., and Vance, A., "Neutralization: New insights into the problem of employee systems security policy violation," *MIS Quarterly*, Vol.34, No.3, pp. 487-502. 2010.

[35] Sommestad, T., Hallberg, J.,Lundholm, K., and Bengtsson, J., "Variables influencing information security policy compliance." *Information Management & Computer Security*, Vol.22, No.1, pp. 44-75. 2014.

[36] Son, J. Y., "Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies," *Information & Management*, Vol.48, pp. 296-302. 2011.

[37] Straub, D. W., "Effective IS security: An empirical study", *Information Systems Research*, 1(3). pp.255-276, 1990.

[38] Vance, A., "Neutralization: New Insights into the Problem of Employee Systems Security Policy Violations," *Management information Systems Quarterly*, Vol. 34, Np. 3, pp. 487-502, 2010.

[39] Vance, A., Siponen, M., and Pahnla, S., "Motivating IS security compliance: Insights from habit and protection motivation theory." Vol.49, pp. 190-198. 2012.

[40] Whitman, M. E., "In defense of the realm

: Understanding the threats to information security", *International Journal of Information Management*, 24(1), pp.43-57, 2004.

[41] Zhang. J., Reithel, P. J, and Li, H, "Impact of perceived technical protection on security behavior", *International Management & Computer Security*, 17(4), pp.330-340, 2009.

[저 자 소 개]



신 혁 (Hyuk Shin)
 1995년 8월 건국대학교 산업공학
 석사
 2006년 6월 Kansas State University
 MBA
 2018년 8월 건국대학교 경영공학
 박사
 2007년 10월~현재 한국산업기술보호
 협회 산업기술보호실장
 email : shhy0422@hanmail.net