Journal of Digital Convergence
Vol. 19. No. 2, pp. 169-174, 2021

ISSN 2713-6434 / eISSN 2713-6442
https://doi.org/10.14400/JDC.2021.19.2.169

억제이론 기반의 정보보안 행동의도에 대한 메타분석

김종기
부산대학교 경영학과 교수

Analysis of MASEM on Behavioral Intention of Information Security Based on Deterrence Theory

Jongki Kim
Professor, Dept. of Business Administration, Pusan National University

요 약 효과적인 정보보안관리의 핵심요소인 정보보안 정책의 중요성이 고조되는 가운데, 조직 구성원의 보안정책 준수 여부에 영향을 미치는 요인에 대하여 다양한 이론에 기반한 실증연구가 다수 수행되었다. 억제이론은 사용자의 보안행동을 설명하는 연구에서 널리 사용되었다. 그러나, 여러 연구들이 일관적이지 않거나 서로 상충되는 결과를 보여 주었다. 이에 따라, 기존의 연구결과를 종합하는 연구들이 수행되었으나, 정성적인 문헌검토 차원이거나 개별 효과크기에 대한 단순한 정량적 분석에 그쳐 억제이론의 전반적인 모형을 대상으로 기존 연구결과를 종합적으로 분석하는 메타분석의 필요성이 대두되었다. 본 연구는 28편의 기존연구를 대상으로 다변량 메타분석의 일종인 TSSEM 기법을 R 기반의 metaSEM 패키지를 활용하여 분석하였다. 무선효과모형을 활용한 분석결과, 전반적인 억제이론 모형의 적합성은 만족스러운 수준이었으며, 억제이론을 구성하는 공식적인 세 가지 요인인 처벌의 확실성, 엄격성 및 신속성 모두 유의하게 나타났다. 향후 연구에서는 비공식적 억제요인에 대한 추가적인 분석과 함께 상황적 변수를 조절변수로 고려할 필요가 있다.

주제어 : 보안행동, 보안정책, 억제이론, 메타분석, MASEM, TSSEM

Abstract While the importance of information security policies is heightened, numerous empirical studies have been conducted to investigate the factors that influence employee's willingness to comply organizational security policies. Some of those studies, however, were not consistent and even contradictory each other. Synthesizing research outcomes has been resulted as qualitative literature reviews or quantitative analysis on individual effect sizes, which leads to meta-analyze on whole research model. This study investigated 28 empirical research based on the deterrence theory with sanction certainty, severity and celerity. The analysis with random effect model resulted in well-fitted research model as well as all of significant paths in the model. Future research can include informal deterrent factors and contextual factors as moderator variables.

Key Words : Security Behavior, Security Policy, Deterrence Theory, Meta-analysis, MASEM, TSSEM

*This study was supported by the Fund for Humanities & Social Studies at Pusan National University 2020.
*Corresponding Author : Jongki Kim(jkkim1@pusan.ac.kr)
Received January 18, 2021 Revised February 1, 2021
Accepted February 20, 2021 Published February 28, 2021

1. 서론

정보보안에 있어서 조직 구성원은 조직 외부에서의 공격에 가장 취약한 요소이며, 보안기술, 보안정책 및 지침, 관련 법규 등을 포함하는 보안관리의 효과가 조직 구성원의 노력에 의해 결정된다[1]. 따라서 조직 구성원의 보안 관련 행동에 영향을 미치는 요인이 무엇인지에 대한 많은 연구가 진행되었다. 이들 연구들은 억제이론, 합리적 행동이론, 계획된 행동이론, 보호동기이론, 기술수용모형 등 다양한 이론적 기반을 두고 있다[2]. 그 중에서 억제이론은 정보보안 문헌에서 가장 많이 언급된 이론이다[3,4].

정보보안 분야에서 보안정책의 준수행동에 영향을 미치는 요인을 탐색하기 위하여 억제이론을 기반으로 한 다수의 연구가 수행되었으나, 많은 경우 연구결과의 일관성이 없거나 심지어 상충되기도 하였다[5]. 이에 따라 기존의 연구결과를 종합하기 위한 다양한 시도가 있었는데, 이런 노력들은 기존 연구결과에 대한 서술적인 분석기법인 체계적인 문헌검토를 기반으로 정성적으로 분석하거나, 정량적인 분석인 경우에도 하나의 독립변수와 하나의 종속변수 사이의 경로계수나 상관관계 계수와 같은 개별 효과크기에 대한 분석에 그쳐 전반적인 연구모형에 대한 체계적인 분석의 필요성이 대두되고 있다.

본 연구는 다수의 기존 연구결과를 종합하는 분석기법 중에서 다변량 메타분석 기법 중의 하나인 TSSEM (Two-Stage Structural Equation Modeling)을 활용하여 분석한다. TSSEM은 메타분석과 구조방정식모형을 결합한 분석기법으로서 연구모형 전체의 적합성 뿐만 아니라 개별 경로의 유의성을 평가할 수 있다[6]. 따라서, 이 연구를 통하여 억제이론의 전체 모형을 통합적으로 검토함으로써 정보보안 분야에서 어떻게 적용되었는지 확인할 수 있다.

2. 억제이론과 메타분석 선행연구

2.1 억제이론

억제이론은 범죄학 분야에서 가장 널리 검증된 이론 중의 하나이다[5]. 이 이론은 개인은 자기이익을 추구하는 경향이 강하며, 불법적인 행동의 수행에 따른 비용과 효익의 평가에 따른 합리적인 의사결정을 하는 합리적 선택이론(rational choice theory)에 근거하고 있다[7].

전통적인 억제이론은 범죄행위를 억제하기 위하여 다음의 Figure 1과 같이 처벌의 엄격성(sanction severity), 처벌의 확실성(sanction certainty), 그리고 처벌의 신속성(sanction celerity)과 같은 공식적인 처벌에 중점을 둔다[5]. 처벌의 엄격성은 위법한 행위에 대한 처벌의 강도를 말하여, 처벌의 확실성은 위법한 행위가 발각된 경우에 처벌될 가능성을 의미한다[4]. 처벌의 신속성은 얼마나 빠르게 처벌의 집행이 이루어지는지에 대한 평가인데, 측정이 쉽지 않거나 이론적인 중요성이 결여되었다는 이유로 연구에 잘 포함되지 않았다[5].

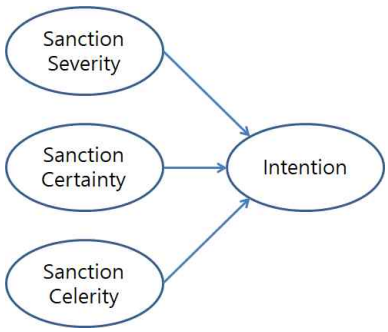

Fig. 1. Deterrence Theory

최근에는 공식적인 처벌에 의한 불이익에 대한 평가 이외에도 비공식적인 처벌에 의한 손실을 같이 고려하는 확대한 억제이론이 대두되었다[8]. 다수의 연구들이 모욕, 주관적 규범, 도덕적 신념 등과 같은 비공식적 처벌이 공식적인 처벌보다 강력한 억제효과가 있다는 결과를 보여주었다[9].

억제이론을 적용한 보안 관련 선행 연구들은 조직이 보다 엄격한 보안 준수 제재 정책을 제시하고, 보안 준수 결과에 대한 평가를 함으로써 보안 미준수에 대한 부정적 결과를 조직원에 인식시키는 것이 목표하는 보안 준수 행동을 유도할 수 있다고 본다[10]. 억제이론의 획일적인 적용에 대한 우려도 있는데, 범죄행위로 인한 이익과 손실이 객관적으로 측정되기 어렵고 당사자의 인지적 판단과정을 거치기 때문에 특정 대상자의 성향에 따라 달라진다는 문제가 있다. 또한 처벌대상 범죄의 성격과 처벌대상 범죄자의 특징에 따라 처벌의 효과가 달라진다는 다수의 선행연구들이 있다[8].

2.2 억제이론 기반의 메타분석 선행연구

Abed & Weistroffer[11]는 억제이론을 구성하는 요인과 직원의 보안준수행동 사이의 관계를 분석하기 위하여 13편의 연구를 메타분석하였다. 분석결과에 따르면 억제이론을 구성하는 세 가지 공식적인 처벌 요인의 효과크기가 모두 작은 것으로 나타나, 억제이론이 직원의

보안준수행동을 확실하게 설명하지 못한다고 보았다.

D'Arcy & Herath[9]는 정보시스템 보안 연구에서 억제이론이 어떻게 적용되었는지 분석하였다. 많은 연구들이 묵시적으로 처벌의 효과가 모든 개인에게 동등하게 적용된다는 가정을 전제로 함에도 불구하고 억제이론에 기반을 둔 연구들에서 처벌의 억제효과가 개인 사이에 매우 다르게 나타나는 경우가 많았다. 이를 바탕으로 자기통제, 컴퓨터 자기효능감, 그리고 도덕적 신념과 같은 개인적 요인과 함께, 가상지위(virtual status)와 직원의 지위를 맥락적 요인으로 핵심적인 상황변수로 식별하였다. 비일관적인 연구결과를 설명하는 다른 원인으로 표본의 차이, 비응답편차 문제, 설문의 특성, 분석기법 등과 같은 방법론적 문제를 열거하였다.

Trang & Brendel[4]은 정보보안 정책준수에 대한 억제이론의 적용가능성을 살펴보기 위하여 2003년부터 2018년까지 게재된 34편의 연구를 대상으로 메타분석을 수행하였다. 일관적이지 않은 연구결과를 설명하는 데는 상황적 조절변수와 연구방법론적 조절변수의 역할이 중요한 것으로 보았다. 상황적 조절변수에는 악의적 행동과 비악의적 행동, 정책준수 행동과 정책비준수 행동, 낮은 권력거리와 높은 권력거리, 그리고 낮은 불확실성 회피와 높은 불확실성 회피로 구분하였다. 방법론적 조절변수로는 행동 기반과 시나리오 기반 측정, 그리고 보편적 상황과 구체적 상황으로 구분하였다. 분석결과에 따르면 처벌은 전반적으로 일탈행동에 영향을 미치지만 연구의 상황에 따라 달라지는 것으로 나타났다. 악의적인 상황, 높은 권력 거리, 그리고 높은 불확실성 회피의 상황에서 억제이론이 일탈행위를 더 잘 설명하였다.

Kuo et al.[5]은 기존의 관련 연구들이 대부분 보안준수행위에 중점을 두고 있다고 주장하면서, 정보시스템 보안 관련 행동을 긍정적인 행동과 부정적인 행동으로 구분한 Guo[12]의 분류방법에 따라 정보보안정책 준수행위와 위험행위로 나누고 이에 대한 영향요인을 억제이론을 근간으로 설명하였다. 특히, 억제이론을 구성하는 공식적인 처벌요인 이외에도 망신, 주관적 규범, 설명적 규범, 도덕적 신념과 같은 비공식적 처벌을 포함하여 연구모형을 구성하였다. 40편의 실증연구에서 모두 108개의 효과크기를 도출하여 각각의 공식적 및 비공식적 처벌요인과 보안준수행위와 보안위험행위와의 경로분석을 수행하였다. 분석결과를 바탕으로 억제이론이 조직의 정보보안정책을 통하여 구성원의 정보보안행위에 영향을 미치는 요인을 이해하는데 도움이 되는 유용한 프레임워크를 제공한다고 주장하였다. 또한, 각 요인의 설명력에 대한 비교를 통하여 공식적 처벌요인보다 비공식적 처벌요인이 보다 더 효과가 크다고 보았다.

Bok[13]은 KCI 등재학술지에 2011년부터 2019년까지 게재된 논문 146편을 대상으로 개인정보 보안정책의 연구동향에 대하여 체계적 문헌분석을 수행하였다. 연구주제의 측면에서는 해외 사례와의 비교 연구와 핀테크 분야에서의 정책의 비중이 높았으며, 보안과 해킹 문제에 대한 기술적 연구도 많이 수행되었다. 연구의 성격 측면에서는 정책 및 법률에 대한 질적 연구가 60% 이상을 차지했다.

이상과 같이 정보보안 정책준수에 대한 종합적인 연구가 일부 수행되었으나, 정성적인 문헌분석에 그치거나 정량적인 분석인 경우에도 개별 효과크기에 대한 유의성 분석에 그치고 있어 억제이론의 전체적인 차원에서 모형분석은 수행되지 못하였다.

3. 데이터 분석

3.1 데이터

메타분석에서 어떤 연구가 분석에 포함되는가에 따라 결과의 신뢰성에 영향을 미친다. 이를 출판편향의 문제라고 하며, 이를 회피하기 위한 방법으로 다양한 유형의 연구를 포함하여 분석을 수행한다[14]. Cram et al.[3]에서 식별한 억제이론 기반 연구는 29편이다. 그중에서 억제이론을 구성하는 독립변수가 없거나[15-18], 처벌을 엄격성이나 확실성과 같은 세부 항목으로 구분하지 않고 하나의 변수로 설정하거나[12,19], 공식적 처벌과 비공식적 처벌로만 구분한 경우[20]는 제외하였다. 또한, 처벌의 확실성 대신에 발각 가능성이나 발각 확실성을 쓴 경우[21,22]에는 이 변수를 분석에서 제외하였다.

Arunothong[23]과 Hovav & D'Arcy[24]의 연구에서는 두 개의 표본집단이 사용되어 별개의 연구로 구분하였다. Cram et al.[3]의 연구는 2018년 초반까지 발표된 연구만 포함되어 있어, Cram et al.[3]의 검색기준에 따라 그 이후에 발표된 연구 네 편[25-28]을 포함하였다. 이에 따라 모두 28편의 연구가 식별되었으며, 연구의 특성은 Table 1과 같다.

종속변수인 정보보안 행위를 Guo[12]의 분류에 따라 구분하면 보안준수행위와 보안위험행위가 각각 50%이다. 연구의 발표시기를 살펴보면 시간이 흐름에 따라 점차 늘어나는 추세를 보이고 있다. 출판 형태별로 구분하면 대부분이 학술지(22편)이며, 일부가 학위논문(4편)이나 학술회의(2편)로 나타났다.

Table 1. Characteristics of studies

Characteristic		N	Percent
Security behavior	Compliant	14	50%
	Risk	14	50%
Publication years	~ 2005	2	7.14%
	2006 ~ 2010	5	17.86%
	2011 ~ 2015	10	35.71%
	2016 ~ 2019	11	39.29%
Publication type	Conference	2	7.14%
	Dissertation	4	14.29%
	Journal	22	78.57%

억제이론을 구성하는 요인들의 경로에 대한 기술적 통계를 살펴보면 Table 2와 같다. 보안위험행위를 종속변수로 사용한 연구는 상관계수 값을 역코딩하여 사용하였다. 먼저, 엄격성은 본 연구에 포함된 모든 논문에서 연구모형에 포함하고 있으며, 총 표본 수는 8,183개이다. 처벌의 확실성은 평균 상관계수 값이 0.314로 가장 크다. Kuo et al.[5]의 언급과 같이 처벌의 신속성을 포함하는 연구는 그리 많지 않으며, 본 연구에서도 3편에 그친다.

출판편향(publication bias) 문제를 검토하기 위하여 Rosenthal[14]의 Fail-safe N(FSN) 값을 계산하였다. 출판편향 문제는 유의적인 분석결과를 무력화하기 위하여 필요한 비유의적인 결과를 갖는 연구가 얼마나 더 필요한가를 분석하는 것으로, 현재의 분석에 포함된 논문편수보다 최소한 (5배 + 10)개 만큼의 추가적인 연구가 필요하다[14]. Table 2의 FSN 행에 나타난 바와 같이 세 가지 요인 모두 최소한의 필요 논문 수를 초과하여 출판편향의 문제는 없다고 볼 수 있다.

Table 2. Statistics for correlation coefficients

Path	Severity	Certainty	Celerity
K	28	23	3
N	8183	7023	998
Mean	0.252	0.314	0.227
Min	−0.066	−0.054	0.117
Max	0.54	0.7	0.409
FSN	264	281	25

3.2 데이터 분석

본 연구는 Cheung & Chan[6]의 TSSEM(Two-Stage Structural Equation Modeling)을 이용하여 Fig. 1의 연구모형을 분석하였다. 분석도구는 R 기반의 metaSEM을 사용하였다. TSSEM은 다변량 메타분석의 일종인 MASEM(Meta-Analytic Structural Equation Modeling) 기법 중의 하나이며, 메타분석에 포함된 각 연구의 상관관계 행렬을 통합하는 1단계와 구조방정식을 이용하여 연구모형을 분석하는 2단계로 구분하여 분석을 진행한다. Table 3은 본 연구에 포함된 연구들의 상관관계를 통합한 결과를 보여준다.

Table 3. Pooled correlation coefficients

	Severity	Certainty	Celerity
Severity			
Certainty	0.3608*		
Celerity	0.2642*	0.0958*	
Intention	0.5906*	0.3139*	0.2321*

* p-value < 0.001

1단계에서 상관관계를 통합하면서 개별 연구들의 상관관계의 동질성 여부에 따라 고정효과모형이나 무선효과모형을 사용할지 결정한다. 먼저, 고정효과모형의 χ^2값이 1079.787로서 $p<0.01$(df=37) 수준에서 유의하며, RMSEA가 0.3106으로 유의수준인 0.08보다 크다 (95% 신뢰구간은 (0.2952, 0.3272)). 무선효과모형의 동질성 지표인 Q값이 406.129로 유의하게 나타났다 (df=37, $p<0.01$). 따라서 통합된 상관관계 행렬 데이터에 심각한 이질성이 있어 무선효과모형을 사용해야 함을 의미한다.

2단계에서 추정한 경로모형의 적합도를 살펴보면, 먼저 $\chi^2(3) = 15.703$(p값 = 0.0013)이나, RMSEA는 0.0227(95% 신뢰구간 (0.0125, 0.0344)), TLI = 0.8974, CFI = 0.9487으로 전반적인 모형 적합도는 우수하다고 볼 수 있다. 정보보호정책 준수의도에 대한 각 요인의 경로계수 추정치와 표준편차, 95% 신뢰구간의 하한과 상한, 그리고 z-값은 다음의 Table 4와 같다. 세 요인의 경로계수는 모두 유의한데, 경로계수의 크기를 비교하면 처벌의 엄격성이 가장 크고, 처벌의 신속성이 가장 작다.

Table 4. Parameter estimates and 95% CI

Path	Estimate (Std.Err)	lower	upper	z-value
Severity→ Intention	0.5548 (0.0542)	0.4662	0.6433	12.2780
Certainty→ Intention	0.3137 (0.0334)	0.2483	0.3792	9.4008
Celerity→ Intention	0.2204 (0.0685)	0.0863	0.3546	3.2201

4. 결론

정보보안정책은 조직의 보안성과를 결정하는 매우 중요한 요소이다. 조직 구성원의 정책준수 여부에 영향을 미치는 요인을 설명하기 위하여 다양한 이론이 적용되었다. 그 중에서 억제이론은 가장 널리 적용된 이론 중의 하나이다. 억제이론을 적용한 연구들의 분석결과가 일관적이지 않고, 때로는 상충되기도 하였다[4,5].

본 연구는 정보보안 행동의도에 영향을 미치는 요인을 억제이론을 기반으로 실증연구를 수행한 28편의 연구에서 도출한 데이터를 이용하여 다변량 메타분석의 일종인 TSSEM을 이용하여 분석을 수행하였다. 분석 결과에 따르면, 공식적인 처벌에 대한 요인을 포함하는 전통적인 억제이론의 전반적인 모형 적합도는 우수하게 나타났다. 이는 기존의 연구들이 억제이론의 전체적인 모형을 잘 뒷받침하고 있다고 볼 수 있다. 개별 요인의 유의성을 살펴보면, 처벌의 엄격성, 확실성, 신속성의 순으로 크다. 처벌의 정도보다는 처벌의 실행 여부가 더 중요하다는 측면에서 확실성이 엄격성보다 준수행동을 더 잘 설명한다고 보는 관점[8,11]이 있으나, 다수의 연구결과를 종합한 본 연구의 메타분석의 결과는 이와는 달리 처벌의 엄격성이 보다 큰 영향을 미친다고 나타났다.

본 연구의 학술적 의의를 살펴보면, 먼저 억제이론을 정보보안 정책준수행동에 적용한 다양한 연구들의 일관되지 않거나 상충된 연구결과들을 통합하여 살펴보았다는 점이다. 또한, 연구방법론적 차원에서는 정보보안 정책준수 행동에 대한 기존의 연구들이 정성적인 체계적 문헌분석이나 단변량 메타분석을 적용한 반면, 본 연구는 각 연구내의 상관관계를 고려하는 다변량 메타분석의 일종인 TSSEM을 적용하여 억제이론 모형을 통합하여 분석하였다.

본 연구의 한계와 향후 연구방향은 다음과 같다. 구조방정식과 메타분석을 결합한 분석기법인 TSSEM을 적용하기 위해서는 연구모형에 포함된 연구변수 모두를 포함한 연구가 적어도 한 편 이상 있어야 한다. 향후 추가적인 연구가 수행되어 비공식적인 억제요인을 포함한 표본의 수가 다수 확보되면 연구모형을 확장하여 분석할 수 있다.

두 번째는 공식적인 억제요인 중에서 처벌의 신속성을 연구모형에 포함한 연구가 매우 적다는 점에서 이 요인을 포함하는 후속연구에 대한 관심이 필요하다. 더불어 세 가지 공식적인 억제요인 이외에 발각 가능성과 같은 유사요인에 대해서도 추가적인 분석이 필요가 있다.

마지막으로 조절변수의 추가가 필요하다는 점이다. 정책 준수와 위반행위는 이익과 손실에 대한 인지적 판단 과정이기 때문에 행동을 선택하는 의사결정자의 특성을 고려할 필요가 있다[8]]. 이에 따라, 종속변수의 유형(정책준수 또는 정책위반), 발각 가능성이나 발각 확실성과 같은 공식적인 억제 요인과 유사한 변수, 정책의 유형(일반적 정책 또는 구체적 정책), 문화적 차이에 따른 특성[3] 등이 고려될 수 있다.

REFERENCES

[1] Q. Hu, Z. Xu, T. Dinev & H. Ling. (2011). Does deterrence work in reducing information security policy abuse by employees?. *Communications of the ACM, 54(6)*, 54-60.
DOI: 10.1145/1953122.1953142

[2] J. Kim & J. Mou. (2020). Meta-analysis of Information Security Policy Compliance Based on Theory of Planned Behavior. *Journal of Digital Convergence, 18(11)*, 169-176.
DOI: 10.14400/JDC.2020.18.11.169

[3] W. A. Cram, J. D'Arcy & J. G. Proudfoot. (2019). Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. *MIS Quarterly, 43(2)*, 525-554.
DOI: 10.24251/hicss.2017.489

[4] S. Trang & B. Brendel. (2019). A meta-analysis of deterrence theory in information security policy compliance research. *Information Systems Frontiers, 21(6)*, 1265-1284.
DOI: 10.1108/ICS-09-2016-0073.

[5] K. M. Kuo, P. C. Talley & C. H. Huang. (2020). A Meta-analysis of the Deterrence Theory in Security-compliant and Security-risk Behaviors. *Computers & Security*, 101928.
DOI: 10.1016/j.cose.2020.101928

[6] M. W. L. Cheung. & W. Chan. (2005). Meta-Analytic Structural Equation Modeling: A Two-Stage Approach. *Psychological Methods, 10(1)*, 40-64.
DOI: 10.1037/1082-989x.10.1.40

[7] I. Onwudiwe, J. Odo & E. Onyeozili. (2005). Deterrence Theory. In: Bosworth, M. (Ed.), *Encyclopedia of Prisons & Correctional Facilities*. Sage Publications, Inc, Thousand Oaks, CA, 234-238.
DOI: 10.4135/9781412952514

[8] D. Shin. (2009). The Effect of Punishment: A Critique of Deterrence Theory. *Korean Journal of Criminology, 21(2)*, 191-216.
UCI: I410-ECN-0102-2012-320-002372416

[9] J. D'Arcy & T. Herath. (2011). 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)*, 643-658.
DOI: 10.1057/ejis.2011.23

[10] I. Hwang & H. Lee. (2016). The Employee's Information Security Policy Compliance Intention: Theory of Planned Behavior, Goal Setting Theory, and Deterrence Theory Applied. *Journal of Digital Convergence, 14(7)*, 155-166.
DOI: 10.14400/JDC.2016.14.7.155

[11] J. Abed & H. R. Weistroffer. (2016). Understanding deterrence theory in security compliance behavior: a quantitative meta-analysis approach. *SAIS 2016*.

[12] K. H. Guo. (2013). Security-related behavior in using information systems in the workplace: a review and synthesis. *Computers & Security, 32*, 242-251. DOI: 10.1016/j.cose. 2012.10.003

[13] J. Bok. (2020). An Study on Privacy Policy Research Trend : Focused on KCI Published. *Journal of Digital Convergence, 18(4)*, 81-89.
DOI: 10.14400/JDC.2020.18.4.081

[14] R. Rosenthal. (1979). The File Drawer Problem and Tolerance for Null Results. *Psychological Bulletin, 86(3)*, 638-641.
DOI: 10.1037/0033-2909.86.3.638

[15] K. H. Guo & Y. Yuan. (2012). The Effects of Multilevel Sanctions on Information Security Violations. *Information & Management, 49(6)*, 320-326.
DOI: 10.1016/j.im.2012.08.001

[16] F. J. Haeussinger & J. J. Kranz. (2013). Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant. *34th International Conference on Information Systems*, Milan, Italy.

[17] B. T. Hanus. (2014). *The Impact of Information Security Awareness of Compliance with Information Security Policies: A Phishing Perspective*. unpublished doctoral dissertation, University of North Texas.

[18] S. J. Harrington. (1996). The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgements and Intentions. *MIS Quarterly, 20(3)*, 257-278.
DOI: 10.2307/249656

[19] S. Kinnunen. (2016). *Exploring Determinants of Different Information Security Behaviors*. unpublished doctoral dissertation, University of Jyväskylä.

[20] M. Siponen & A. Vance. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly, 34(3)*, 487-502.
DOI: 10.2307/25750688

[21] H. Li, J. Zhang, & R. Sarathy. (2010). Understanding Compliance with Internet Use Policy from the Perspective of Rational Choice Theory. *Decision Support Systems, 48(4)*, 635-645.
DOI: 10.1016/j.dss.2009.12.005

[22] W. Li & L. Cheng. (2013). Effects of Neutralization Techniques and Rational Choice Theory on Internet Abuse in the Workplace. *Pacific Asia Conference on Information Systems*, Jeju Island, South Korea.

[23] W. Arunothong. (2014). *Three Research Essays on Propensity to Disclose Medical Information through Formal and Social Information Technologies*. unpublished doctoral dissertation, University of Wisconsin-Milwaukee.

[24] A. Hovav & J. D'Arcy. (2012). Applying an Extended Model of Deterrence Across Cultures: An Investigation of Information Systems Misuse in the US and South Korea. *Information & Management, 49(2)*, 99-110.
DOI: 10.1016/j.im.2011.12.005

[25] X. Chen, D. Wu, L. Chen & J. K. L. Teng. (2018). Sanction severity and employees' information security policy compliance: investigating mediating, moderating, and control variables. *Information & Management, 55(8)*, 1049-1060.
DOI: 10.1016/ j.im.2018.05.011.

[26] M. I. Merhi & P. Ahluwalia. (2019). Examining the impact of deterrence factors and norms on resistance to Information Systems Security. *Computers in Human Behavior. 92*, 37-46.
DOI: 10.1016/j.chb.2018.10.031

[27] M. Rajab & A. Eydgahi. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security. 80*, 211-223.
DOI: 10.1016/j.cose.2018.09.016

[28] N. S. Safa, C. Maple, S. Furnell, M. A. Azad, C. Perera, M. Dabbagh & M. Sookhak. (2019). Deterrence and prevention-based model to mitigate information security insider threats in organisations. *Future Generation Computer Systems. 97*, 587-597.
DOI: 10.1016/j.future.2019.03.024

김 종 기(Jongki Kim) [정회원]

· 1987년 2월 : 부산대학교 경영학과(경영학사)
· 1988년 12월 : 미국 아칸소 주립대 경영대학원(경영학석사)
· 1992년 12월 : 미국 미시시피 주립대 경영학과(경영학박사)
· 1999년 3월 ~ 현재 : 부산대학교 경영학과 교수
· 관심분야 : 정보 프라이버시, 정보보안, 메타분석
· E-Mail : jkkim1@pusan.ac.kr